On the QKD relaying models and building QKD networks

Quoc Cuong Le

THESE

Présenté pour l'optention du diplôme de

Docteur de l'Ecole Nationale Supérieure des Télécommunications

Spécialité : Informatique et Réseaux

Par

Quoc-Cuong LE

Autour des réseaux quantiques et des modèles de relais pour la clé quantique

Soutenue le 1 Octobre 2009 à E.N.S.T

Devant le jury composé de :

Rapporteurs :	Marc BUI
	Daniel OI
Examinateurs :	Akim DEMAILLE
	Philippe GALLION
	Elham KASHEFI
Directeur de thèse :	Patrick BELLOT

RESUME ETENDU

Dans l'information classique, il y a de plusieurs années où la distribution de clé secrète pour deux parties lointaines était bien connue comme un défi difficile. L'histoire pourrait commencer en 1948 lorsque Shannon introduit un concept fondamental de la théorie de l'information classique: l'entropie H, ou également nommé par « Entropie de Shannon ». L'entropie de Shannon de la variable aléatoire X, classiquement notée H (X), est pour but de quantifier, en moyenne, la quantité d'information qu'on gagne lorsqu'on apprend la valeur de X. En d'autres termes, H (X) mesure l'incertitude de X avant que l'on apprend sa valeur. Avec la notion d'entropie, Shannon a montré qu'il est possible de construire un canal virtuel sans bruits et sans perte à partir d'un canal réel bruité et présenté des pertes. Ce résultat est maintenant bien connu sous le nom « le théorème de codage des canaux sans bruit de Shannon ». Inspiré de ce travail, en 1949, Shannon a continué à mettre en place un modèle de communication sécurisé dans lequel le canal entre Alice et Bob est sans bruit et sans perte. Cependant, Eve peut écouter le canal, c'est à dire que, Eve peut recevoir des copies identiques de tous les messages reçus par Bob. Grosso modo, Alice chiffre le message en texte brut M à un mot de code C, elle envoie C sur le canal. Tous les deux Bob et Eve reçoivent C. Dans ce contexte, Shannon a montré que M serait parfaitement en secret si l'information mutuelle de M et C, notée I(M ; C), est égal à zéro, en d'autres mots, le code C donne aucune information sur la texte M. Un tel secret parfaite est appellé « sécurité de l'information théorique » ou « sécurité inconditionnelle », par le fait qu'il ne dépend pas de la puissance de calcul de l'ennemi. Shannon a montré que la sécurité inconditionnelle de M peut être obtenu en utilisant le schéma « masque jettable », à condition que Alice et Bob ont été partagés une clé secrète K, qui a au moins la même longueur de M, en d'autres termes, $H(K) \geq H(M)$. Malheureusement, une telle condition est difficile à obtenir auprès des situations de communication réelle. Par conséquent, la question d'intérêt est de savoir comment les deux parties éloignées peuvent faire s'ils ne partagent pas à priorité une clé secrète assez longue? Peuvent-

ils, Alice et Bob, générer une clé plus longue à partir d'une clé secrète initiale plus courte ?

Dans le modèle de communication sécurisé de Shannon, l'inégalité $H(K) \geq H(M)$ s'agit d'une réponse négative à la question au-dessus, c'est à dire qu'il est impossible de générer une clé secrète plus longue à partir d'une clé secrète initiale plus courte. Toutefois, on devrait noter que cette impossibilité prend effet sous l'hypothèse de base de Shannon qui suppose que le canal est réduit à être parfait (sans bruit et sans perte) et l'ennemi peut obtenir exactement les choses que la partie légitime Bob peut obtenir. Ainsi, on pense à modifier le modèle de Shannon, plus précisément, à une modification de l'hypothèse de Shannon. En effet, on essaie de construire d'autres modèles qui sont plausibles et dans lesquels l'information obtenu par l'espion est différent de celui obtenu par le destinataire légitime. Jusqu'à présent, c'est connu qu'il y a au moins deux tels modèles: l'un est d'utiliser directement des canaux classiques bruités et l'autre d'exploiter les canaux quantiques.

Cette thèse a pour but d'examiner la distribution de clé quantique, ou Quantum Key Distribution (QKD) en termes d'anglais. C'est une technique qui promet un moyen parfait de distribuer la clé secrète pour les deux personnes à courte distance. Malheureusement, la QKD n'est pas disponible aux communications à grande distance. Pour remédier ce problème, les modèles de relais ont été étudiés et proposés. Ces modèles peuvent être classifiés en deux catégories principales :

- Modèles de confiance : les noeuds intermédiaires ont été assumés d'être sécurisés. Cela rend un effet indésirable que la sécurité finale se baissera en fonction du nombre des noeuds intermédiaires dans les cas réels.

- Modèles d'utiliser les paires d'EPR : ces modèles ne réduisent pas la sécurité des schémas originaux de QKD. Cependant, c'est très difficile à manipuler les paires d'EPR pendant une longue durée qui est nécessaire pour effectuer et terminer un protocole de distribution de la clé.

Évidement, un modèle efficace à étendre la portée de QKD est toujours manqué. Motivé par ce fait, cette thèse a pour but de chercher et proposer les nouveaux modèles de relais pour la distribution de clé quantique. Nous avons abordé le problème par deux approches : « classique » et « quantique ».

I. Approche « classique »

Nous avons étudié la distribution des clés extrêmement secrètes dans un réseau quantique à grand échelle. Les liens sont inconditionnellement sécurisés grâce à la technologie QKD qui permet à détecter efficacement les attaques aux liens. Par contre, les noeuds restent sujet des attaques et aucune architecture ne permet de les protéger. Les attaques aux noeuds sont soit détectables, soit indétectables. Les attaques détectables sont faciles à traiter. Lors qu'on a détecté une attaque parue à un noeud, on peut simplement enlever ou mettre en garantaine ce noeud pour maintenir les autres opérations du réseau. Les attaques indétectables sont très graves. Personne ne peut les détecter jusqu'au moment où un dommage terrible était paru. Les transmissions de clé quantique à longue distance présentent plus de risques à cause des attaques indétectables. La vulnérabilité s'augmente en fonction du nombre des noeuds intermédiaires. Il faut envisager les méthodes qui permettent de traiter contre les attaques indétectables aux noeuds intermédiaires. Une méthode remarquable est d'utiliser des algorithmes de routage stochastique qui obligeraient l'espion à réussir les attaques indétectables sur une proportion importante de la totalité du réseau pour être sûr de pouvoir intercepter l'échange de secrets.

Nous avons modélisé le problème par le modèle suivant (voir Fig. 1):

- Un grand réseau à maille carrée dans lequel chaque noeud est connecté à ses quatre voisins par la technologie QKD ;
- Chaque noeud est sûr avec probabilité p_s où $0 \leq p_s \leq 1$. Autrement dit, chaque noeud est espionné sans aucune trace avec probabilité $p_e = 1 - p_s$;

- Alice et Bob ne connaissent pas les noeuds sûrs et les nœuds espionnés. Ils ne connaissent que p_s et p_e.
- Alice envoie à Bob N sous-clés K_1, K_2, .., K_N par N chemins différents π_1, π_2, .., π_N. La clé finale K est calculée par une opération XOR au niveau du bit sur toutes les sou-clés K_1, K_2, .., K_N.

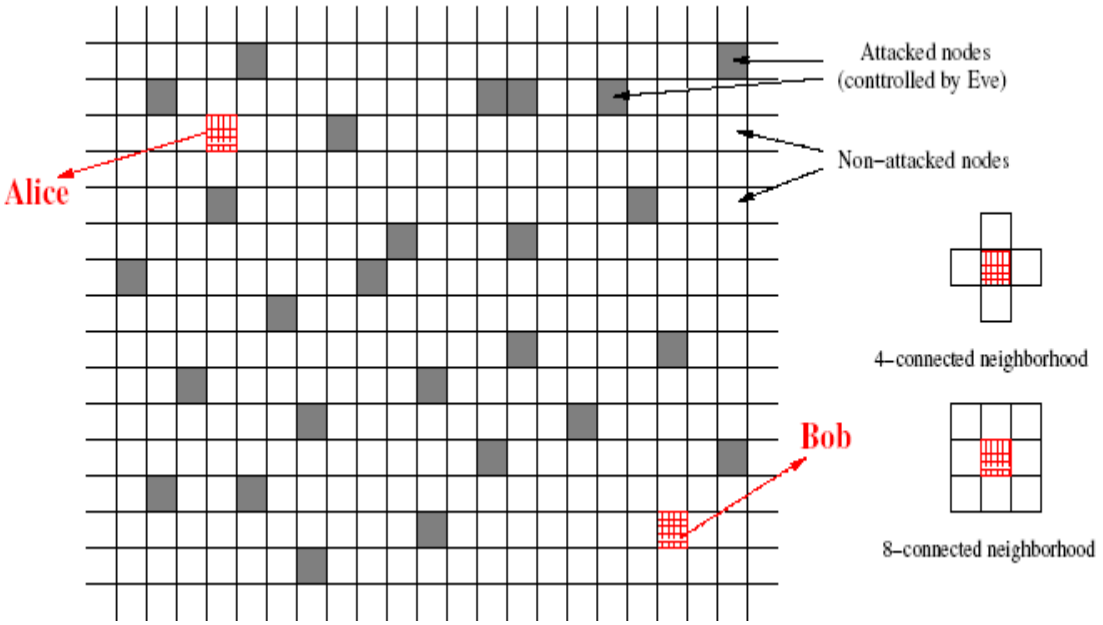


Fig. 1 – Two-dimensional lattice network

Dans le cadre proposé, les deux questions suivantes sont essentielles :

1. Quelle est la condition de p_s telle que tous les nœuds sûrs soient presque certainement liés ?
2. Etant donné un algorithme de routage stochastique, et une ε arbitrairement proche de 0, comment peut-on estimer la value N des chemins (π_1, π_2, .., π_N) telle que la sécurité de la clé final K est égale à 1- ε ?

Pour répondre à la première question, notre approche est basée sur la « théorie de percolation ». En effet, le cadre de la percolation 2-dimensionnel est semblable à notre modèle proposé au-dessus. Le problème de percolation peut être enoncé comme la suivante. Etant donnée un graphe G = (V, E) où V est l'ensemble des

sommets et E est l'ensemble des arêtes. Tous les arrêts sont ouverts. Chaque sommet est soit ouvert ou soit fermé. On fournit de l'eau au centre du graphe G. Les arrêts et les sommets dans l'état ouvert permettent à l'eau de traverser et les faire devenir mouillés. Sinon, ils ne permettent pas le passage de l'eau. Chaque sommet est ouvert avec probabilité p_o, où $0 \leq p_o \leq 1$. On considère la probabilité de percolation θ, qui est mesurée par la proportion de sommets mouillés sur les sommets ourverts. Fig. 2 montre le comportement de $\theta(p_o)$. La valeur p_c, également nommée la probabilité critique, est la valeur minimum de p_o telle que $\theta(p_o) > 0$.

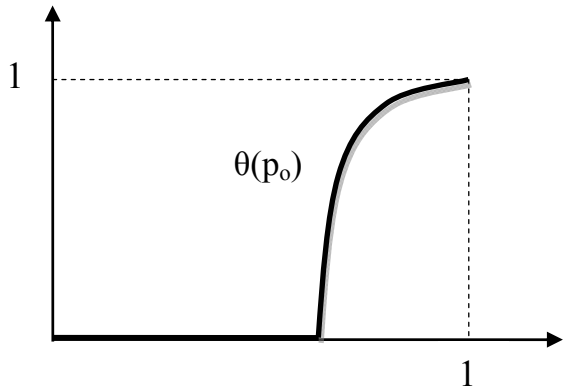


Fig. 2 – Probabilité de percolation $\theta(p_o)$

Nous avons trouvé que les deux probabilités p_o (ouvert) et p_s (sûr) jouent un rôle équivalent dans les deux contextes. Si nous fixons $p_s = p_o$ et supposons que le sommet A envoie à le sommet B un ensemble infini des sous-clés K_1, K_2, .., par une infinité de chemins différents π_1, π_2, .., π_N, alors la sécurité de la clé finale K est identique à la probabilité existant au moins un chemin sûr entre A et B. D'autre côté, une telle probabilité est équivalente à la probabilité que un sommet ouverte appartient à la grappe géante des sommets ouverts du graphe. Nous avons pu retirer deux caractéristiques importantes de la théorie de percolation :

1. θ est une fonction non-décroissante et continue dans le droit de p_c (voir Fig. 2).
2. Le nombre des grappes ouverts géantes est soit 0 ou soit 1 pour $\theta = 0$ ou $\theta > 0$, respectivement.

En basant sur les deux résultats importants au-dessus, nous avons trouvé une méthode d'heuristique pour déterminer la condition sur p_s telle qu'on soit sûr qu'il existe au moins un chemin non-espionné entre les nœuds sûrs avec une probabilité δ arbitrairement proche de 1. Nous avons pu formuler mathématiquement la relation entre δ et p_s comme la formule ci-après :

$$1-(1-p_s)^4 \leq \delta \leq \begin{cases}(1-p_s^8)^4 \; if \; 0.8 \leq p_s < 0.9, \\ (1-p_s^6)^4 \; if \; 0.9 \leq p_s < 1.\end{cases}$$

Pour valider notre formule trouvée, nous avons implémenté des simulations et fait des statistiques.

Lorsque la condition sur p_s étant satisfaite, nous nous sommes intéressés aux algorithmes de *routage stochastique* qui permettent de réaliser la distribution de clé à un niveau de sécurité 1-ε où ε arbitrairement proche de 0. L'idée est simple. Si on envoie un assez grand N des secrets par des chemins aléatoires, alors il y aurait un secret qui échappe à l'espion avec probabilité 1-ε. Les algorithmes que nous avons étudiés sont :

- Un algorithme de routage d'ivrogne adaptatif, ou ***Adaptive Drunkard Routing Algorithm (ADRA)*** en termes d'Anglais. Cet algorithme a pour but d'examiner le phénomène « percolation » de notre carde de travail proposé. La distribution de probabilité pour le nœud suivant est sans biais dans le problème de marche de l'ivrogne classique. Ici, nous avons proposé un algorithme de routage d'ivrogne, nommé ADRA, qui est biaisé. L'idée est de donner une plus grande chance, mais toujours au hasard, pour le sommet qui est plus proche du destinataire, afin d'augmenter la convergence de l'algorithme.

- Un algorithme de routage stochastique avec longueur constante, ou ***Constant-Length Stochastic Routing Algorithm (l-SRA)*** en termes d'Anglais. Tout d'abord, nous devrions définir quelques nouvelles notions. *La longueur d'un chemin* est le nombre de sommets appartenant à ce chemin-là. Un sommet peut être compté autant de fois que le chemin passe par ce sommet. *La distance entre deux sommets* est la longueur du plus court chemin entre ces sommets. Alors, l'algorithme de routage *l*-SRA est un algorithme stochastique qui prend un paramètre d'entrée l et tente de transmettre le message par un chemin aléatoire mais ayant la longueur l.

- Un algorithme de routage stochastiques ave longueur paramétrée, ou ***Parameterized-Length Stochastic Routing Algorithm (k-SRA)***. Cet algorithme prend un paramètre d'entrée $k > 1$, et essaie de transmettre le message par un chemin de longueur $l \leq k \times d$. Nous avons pu construire l'algorithme *k*-SRA en basant sur l'algorithme *l*-SRA. L'idéee est comme la suivante. Lorsqu'un message a besoin d'être envoyé, nous choisissons aléatoirement une valeur $l \leq k \times d$, puis nous utilisons l'algorithme *l*-SRA pour déterminer sur quel chemin ayant la longueur l le message va être transmis.

Nous avons considéré également deux stratégies d'attaque d'Eve:

- ***Attaque dynamique :*** Eve re-sélectionne fréquement des nœuds attaqués en essayant d'attraper quelques messages envoyés.
- ***Attaque statique:*** Eve maintient son choix des nœuds attaqués jusqu'au moment où tous les N messages ont été envoyés.

Parce que l'ADRA algorithme est totalement basé sur la marche aléatoire, un tel algorithme n'a pas pu donner des résultats mathématiques rigoureux. Son rendement ne donne qu'une estimation statistique expérimentale. L'algorithme *l*-SRA n'est pas une vraie solution de routage. Cet algorithme a pour but d'exécuter la sous-tâche de l'algorithme *k*-SRA. L'algorithme *k*-SRA a pu présenter quelques

bornes rigoureuses. Nous avons trouvé la formule qui décrit la dépendance de N à ε et à l'algorithme de routage :

$$N \geq \frac{\lg \varepsilon}{1 - \lg \lambda}$$

Où λ dépend de caractéristiques spécifiques de l'algorithme de routage.

Nous avons implémenté les simulations pour valider les conclusions et formules obtenues.

- Nous avons noté que pour l'algorithm ADRA, le calcul des probabilités pour choisir le nœud suivant peuvent varier d'entraîner de nombreuses variantes. Nous avons conduit les simulations dans un réseau quarré de taille 600 × 600, en faisant varier la probabilité sécurité p_s, $0.93 \leq p_s < 1$, et la distance entre Alice et Bob $d_{(AB)}$. Pour chaque p_s, nous avons généré des attaques au hasard d'Eve. Pour chaque distance $d_{(AB)}$, nous avons généré 400 paires (Alice, Bob). Pour chaque paire, nous avons conduit 400 expériences. Dans chacun, nous avons généré des chemins stochastiques d'Alice à Bob jusqu'à trouver un chemin sûr (c'est-à-dire un chemin sans Eve). Pour chaque ensemble des 400 expériences nous avons ramassé le plus grand nombre des messages qui ont eu besoin. Pour éviter d'envoyer un nombre infini de messages, nous avons mis un effort maximal à 10^4 messages. Le résultat de simulations donne à penser qu'il existe un seuil du nombre des messages d'envoyer au-dessus duquel on peut être presque certain qu'il existe au moins un message échappé à Eve.

- Pour l'algorithme *k*-SRA, les simulations ont été mises en œuvre également dans un réseau quarré de taille 600 × 600. Nous avons performé 10^4 expériences. Nous avons pu collecter et comparer les bornes inférieures, valeurs réels sorties de simulations, et bornes supérieures pour le cas auquel k = 2, d = 10 et p_s = 0,93; 0,95; 0,97; 0,99. Nous avons noté que la borne

inférieure est toujours possible si tous les N messages prennent un seule chemin. La convergence de résultats expérimentaux aux bornes supérieures est importante. Nous avons constaté que la secrète de la clé finale est une fonction non décroissante. Comme le nombre de messages envoyés s'augmente, la secrète converge vers sa borne supérieure. En outre, les deux ont tendance à 1, lorsque N tente à l'infini.

En bref, l'originalité de notre modèle ``classique'' proposé est de faire émerger la question sur les attaques indétectables aux noeuds intermédiaires dûs d'une transmission de clé à long distance, et de proposer une solution correspondante. Notre travail est interessant lorsquqqu'il ouvre une autre porte qui permet d'enquêter les réseaux QKD en utilisant la théorie de la percolation et le routage stochastique. La recherche sur le modèle proposé nous avons rendu cinq papiers présentés dans les congrès internationaux avec comité de programme (voir Chapitre 1.3). Cependant, beaucoup de travail reste à faire dans le fuure. Par exemple, nous devons tenir compte de l'authentification de clé pour compléter notre système d'échange des clés. La distribution d'attaque était uniforme dans notre présent travail. Plus d'autres distributions de probabilité complexes semblent plus intéressantes. Étudier d'autres topologies est aussi de l'importance, les grilles quarrés ne sont que la première étape. Nous visons également à trouver des formules plus rigoureuses et bien serrés. D'ailleurs, nous devrions améliorer notre propositions de routage stochastique, par exemple, cacher les informations de routage comme dans le routage en pelure d'oignon. Nous devrions attacher une importance au débit et aux charges de calcul dans la pratique. Nous avons également l'intention de procéder à une estimation des coûts à l'égard de la technologie QKD aujourd'hui.

II. Approche « quantique »

1. Modèles QQTB et QQTR

Nous avons abordé le problème par proposer une nouvelle définition du relais quasi-confiant. Les relais quasi-confiant que nous nous sommes intéressés sont définies comme la suivante t: (i) être assez honnête pour bien suivre un protocole de communication multi-partie en temps fini, (ii) cependant, étant sous la surveillance d'Eve. En basant sur une telle nouvelle définition, nous avons pu développer une modèle simple de 3-parties appellé le pont quantique quasi-confiant, ou Quantum quasi-Trusted Bridge (QQTB) en terme d'Anglais (voir Fig. 3). Dans ce modèle, Alice et Bob sont pris hors de portée de la distribution de clés quantique (QKD). Carol est un relais quasi-confiant qui peut partager des liens QKD avec tous les deux Alice et Bob. Nous avons pu montrer que le protocole QQTB permet à Alice et Bob, en collaboration avec Carol, de bien établir des clés secrètes. L'originalité du protocole QQTB est que nous n'avons pas besoin de paires de photons intriqués invoquer.

Ensuite, nous avons élaboré le modèle QQTB au modèle relais quantique quasi-confiant, ou Quantum Quasi-Trusted Relais (QQTR) en termes d'Anglais (voir Fig. 4). Le modèle QQTR est capable de distribuer des clés secrètes sur une distance arbitrairement lointaine. Bien que le modèle QQTB exige les sources de photons intriqués, l'originalité est que nous n'avons pas invoqué la technique d'entanglement swapping.

En effet, l'idéee de fond de nos deux modèles au-dessus est simple. Nous avons remarqué que dans le modèle de 3-parties comme le modèle QQTB, si Alice et Bob arrivent à donner la valeur $C = A \oplus B$ (l'opération XOR) en gardant en secret les deux valeurs A et B, alors Alice et Bob peuvent utiliser le schéma *masque jetable* afin de protéger la transmission de la clé finale K. Nous avons cherché et arrivé à réaliser notre remarque par proposer le circuit quantique CNOT-M comme être décrit dans Fig. 5. Les caractéristiques du circuit CNOT-M sont :

1. Si $|a\rangle$ et $|b\rangle$ ont été préparés dans la base $|\times\rangle = \{|\tilde{0}\rangle, |\tilde{1}\rangle\}$, alors $c1 = a \oplus b$ et $c2$ est aléatoire.
2. Si $|a\rangle$ et $|b\rangle$ ont été préparés dans la base $|+\rangle = \{|0\rangle, |1\rangle\}$, alors $c2 = a \oplus b$ et $c1$ est aléatoire.

Où $|\tilde{0}\rangle = \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right\}, |\tilde{1}\rangle = \left\{\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$.

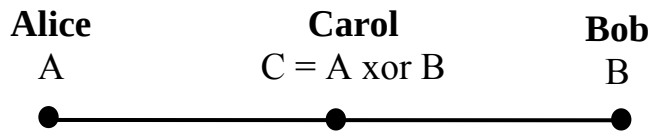


Fig. 3 – Modèle QQTB : la communication entre Alice, Carol et Bob : Carol joue le rôle d'une personne intermédiaire quasi-confiant.

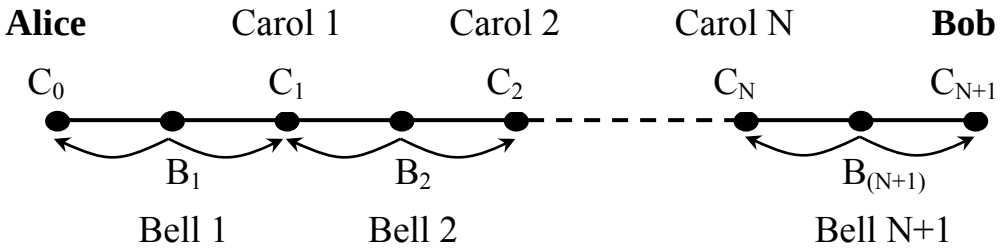


Fig. 4 – Modèle QQTR: Bell 1, Bell 2, .., Bell N sont EPR sources; Carol 1, Carol 2,.., Carol N jouent le rôle de Carol dans la modèle QQTB.

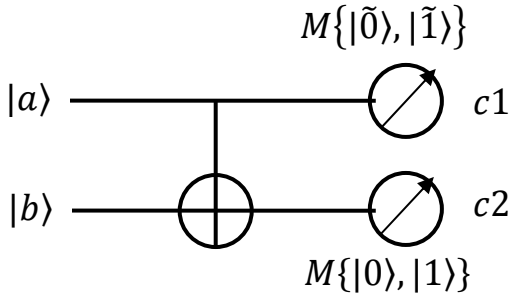


Fig. 5 – Le circuit CNOT-M se compose d'une porte C-NOT et deux mesures en bases différentes. Les deux sorties garantissent soit $c1$= a xor b, soit $c2$ = a xor b.

Le protocole du modèle QQTB se compose de 4 étapes :

Étape 1: Préparer, échanger, et mésurer des qubits.

- Alice crée les *2n* bits aléatoires $ra_1, .., ra_{2n}$ et choisit une chaîne b_A de *2n* bits aléatoires. Pour chaque bit ra_i, Alice crée un état quantique correspondant $|\widehat{ra_i}\rangle = |ra_i\rangle$ dans la base $|+\rangle = \{|0\rangle, |1\rangle\}$ si rangle $b_A[i] = 0$, ou $|\widehat{ra_i}\rangle = |\widehat{\widetilde{a_i}}\rangle$ dans la base $|\times\rangle = \{|\widetilde{0}\rangle, |\widetilde{1}\rangle\}$ si $b_A[i] = 1$. Alice envoie $|\widehat{ra_i}\rangle, |\widehat{ra_2}\rangle, .., |\widehat{ra_{2n}}\rangle$ à Carol.
- De même, Bob crée les 2n bits aléatoires $rb_1, .., rb_{2n}$, un chaîne b_B de *2n* bits aléatoires. Bob génère et envoie $|\widehat{rb_i}\rangle, |\widehat{rb_2}\rangle, .., |\widehat{rb_{2n}}\rangle$ à Carol.
- Carol reçoit deux chaînes de 2n qubits, l'une d'Alice et l'autre de Bob, d'une manière synchrone. Cela veut dire que Carol reçoit un par un tous les *2n* paires $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. Pour recevoir une paire$|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle$, Carol se tourne au hasard dans une de deux modes, soit Check-Mode (CM) ou soit Message-Mode (MM).
    - Dans la mode CM, Carol mesures indépendamment $|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle$ dans deux bases aléatoires $|+\rangle$ ou $|\times\rangle$. Carol enregistre les deux bits classique du résultat et conserve leurs bases correspondantes.
    - Dans la mode MM, Carol utilise le circuit CNOT-M (voir Fig. 5) pour mesurer $|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle$. Elle enrigistre les deux valeurs de sortie.
- Après d'avoir reçu tous les paires de qubits, les choix de CM et MM produit grosso modo deux chaînes : l'une indiquant les positions de Check-Mode CP = $cp_1, .., cp_n$ et l'autre indiquant les positions de Message-Mode MP = $mp_1, .., mp_n$.

Étape 2 : Détecter la présence d'Eve.

- Pour le canal Alice-Carol: Alice et Carol communiquent leurs bases utilisées dans les check-positions $cp_1, .., cp_n$ et leurs valeurs correspondantes. Alice et Bob écartent des positions où leurs bases sont différentes. Ils comparent les valeurs aux positions restantes. Si quelques-uns des ces valeurs sont en désaccord, alors le canal devrait être compromise. Dans ce cas, Alice et Carol informent à Bob pour annuler la transaction.

- Pour le canal Bob-Carol: Bob et Carol font comme Alice et Bob dans le processus de vérification ci-dessus.

Étape 3 : Créer les masques jetables pour Alice, Carol et Bob.

- Alice et Bob annoncent leurs bases en message-positions mp_1, .., mp_n. Si leurs bases sont différentes à la position mp_i, alors qu'ils informent à Carol d'écarter ce position.
- À chaque position restant, Carol jette la première sortie du circuit CNOT-M si la base commune de Alice et Bob est $|+\rangle$. Sinon, Carol jette la deuxième sortie.
- Les valeurs restant d'Alice, Carol et Bob se forment les trois masques A = A_1, .., A_m ; C = C_1, .., C_m; B = B_1, .., B_m à Alice, Carol et Bob, respectivement. Ces masques tiennent la condition $C_i = A_i \oplus B_i$ pour i=1, .., m où $m \approx \frac{n}{2}$.

Étape 4 : Transmettre la clé secrète K.

- Carol annonce publiquement C = C_1, .., C_m.
- Alice crée la clé secrète K. Elle envoie $K \oplus A \oplus C = K \oplus B$ à Bob.
- Bob reçoit $K \oplus B$, récupère $K = K \oplus B \oplus B$.

Nous avons considé la sécurité de notre protocole. À l'étape 1, quand une paire $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$ arrive de manière synchrone à Carol, elle se tourne par hasard soit dans le Check-Mode (CM) ou soit dans le Message-Mode (MM). Parce qu'Eve ne sait pas le mode choisi par Carol, Eve ne peut pas traiter différemment les paires $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. Ainsi, le taux d'erreur dans le Check-Mode doit se comporter d'une même façon par rapport à cela dans le Message-Mode. En revanche, la procédure de détection d'Eve dans les canaux (Alice, Carol) et (Carol, Bob) fonctionnent exactement comme celle du protocole BB84. Par conséquence, la sécurité du protocole QQTB devrait être exactement celle du protocole BB84. Cela implique que le protocole QQTB est inconditionnellement sûr.

Le protocole QQTR se compose de 5 étapes:

Étape 1 : Prépare, échanger et mesurer des qubits.

- Chaque B_i, pour i = 1,.., N+1, prépare n états Bell $(\Phi^+)^{\otimes n}$.
- B_1 envoie la première moitié de chaque état Bell à Alice (la station précédente), et la deuxième moitié à C_1 (la station suivante). B_{n+1} envoie la premère moitié de chaque état Bell à C_n (la station précédente), et la deuxième moitié à Bob (la station suivante).
- Chaque B_i, pour i = 1,.., N+1, envoie la première moitié de chaque état Bell à C_{i-1} (la station précédente), et la deuxième moitié C_i (la station suivante).
- Alice (ou C_0) et Bob (ou C_{n+1}), chacun reçoit n qubits. Ils choisissent au hasard et indépendamment des bases de measurement.
- Chaque C_i, pour i = 1,.., N, reçoit 2n qubits vient de B_i et B_{i+1} de manière synchrone. Cela signifie qu'elle reçoit n fois, et pour chaque fois qu'elle reçoit une paire de qubits: l'un vient de B_i et l'autre de B_{i+1}. Elle la mesure en utilisant le circuit CNOT-M (voir Fig. 5). Elle conserve les valeurs mesurées et les bases correspondantes. En bref, C_i fait exactement comme Carol dans le Message-Mode du protocole QQTB.

Étape 2 : Tamiser.

- Alice et Bob annoncent leurs bases.
- Si leurs bases sont différentes à la position i, Alice, Bob, C_1, .., C_n rejettent cette position.
- Pour chaque position restante i, C_1, .., C_n rejettent la première ou la deuxième sortie du circuit CNOT-M si la base commune de Alice et Bob est soit $|+\rangle$ ou soit $|\times\rangle$, respectivement.
- Les valeurs restantes se forment N +2 chaînes de 2m-bits a = a_1, .., a_{2m}, c(i) = $c(i)_1$, .., $c(i)_{2m}$, pour i = 1, .., N, b = b_1, .., b_{2m} pour Alice, C_1, .., C_n, et Bob, respectivement. Ces N+2 chaînes devraient tenir $\bigoplus_{i=1}^{N} c(i)_j = a_j \oplus b_j$, pour j= 1,.., 2m où m ~ n/4.

Étape 3 : Détecter la présence d'Eve.

- Alice, Bob et C_1, .., C_n se mettent en accord alératoirement *m* positions dans *2m* positions totales pour vérifier la présence d'Eve. Cela forme les deux chaînes indiquant m-positions: l'une pour vérification CP = cp_1, .., CP_m et l'autre pour information MP = mp_1, .., mp_m.
- Alice, Bob, C_1, .., C_n annoncent les valeurs aux positions de vérification CP: a = a_{cp1}, .., a_{cpm}; b = b_{cp1}, .. , b_{cpm}; c(i) = $c(i)_{cp1}$,.., $c(i)_{cpm}$, pour i = 1,.., N, respectivement. Ils vérifient si $\bigoplus_{i=1}^{N} c(i)_j = a_j \oplus b_j$, ou pas. Si certains des résultats négatifs, ils abandonnent la transaction.

Étape 4 : Créer les masques jetables.

- Les valeurs aux *m* positions MP forment N+2 chaînes de m-bits : $P^A = P^A_1$, .., P^A_m; $P^{C(i)} = P^{C(i)}_1$, .., $P^{C(i)}_m$, pour i = 1,.., N et $P^B = P^B_1$, .., P^B_m, pour Alice, C_1, .., C_n, et Bob, respectivement. Ces masques tiennent $\bigoplus_{i=1}^{N} P^{C(i)} = P^A \oplus P^B$.

Étape 5 : Transmettre la clé K.

- Chaque C_i, pour i = 1,.., N, annonce publiquement $P^{C(i)}$.
- Alice crée la clé secrète K de m-bit. Elle envoie $K \oplus P^A \oplus_{i=1}^{N} P^{C(i)} = K \oplus P^B$ à Bob.
- Bob reçoit $K \oplus P^B$, récupère $K = K \oplus P^B \oplus P^B$.

Nous avons pu montrer dans Section 10.4.3 que le protocole QQTR est correct et également inconditionellement sécurisé.

2. Modèles QUB et QUR

L'inconvénience de deux modèles QQTB et QQTR est d'obliger des intermédiaire stations (Carol 1, .., Carol N) être « quasi-confiant ». Nous avons pu évoluer ces deux modèles aux nouveaux modèles, nommés le pont quantique méfiqant ou

Quantum Untrusted Bridge (QUB) en termes Anglais, et les relais quantiques méfiants ou Quantum Untrusted Relay (QUR) en termes Anglais.

Ce que nous avons obtenu est :

1. Si on n'utilise que la source de photons simples, alors le modèle QUB peut étendre jusqu'à deux fois la portée de la QKD.
2. Si on utilise la source des paires d'EPR, alors le modèle QUR peut relayer la clé quantique à travers des distances arbitraires.

Le modèle QUB est très semblable au modèle QQTB (voir Fig. 3). Cependant, le pont Carol peut être contrôlé par Eve. Nous devons utiliser un autre protocole de communication pour garantir la sécurité de la clé transmise. Le protocole QUB est composé de 5 étapes :

Étape 1 : Préparer, échanger, et mesurer des qubits

- Alice crée *2n* bits $ra_1, .., ra_{2n}$ aléatoirement et choisit une chaîne b_A de *2n* bits aléatoires. Pour chaque ra_i, elle crée un état quantique correspondant $|\widehat{ra_i}\rangle = |ra_i\rangle$ dans la base $\{|0\rangle, |1\rangle\}$ si $b_A[i]=0$, ou $|\widehat{ra_i}\rangle = |\widetilde{ra_i}\rangle$ dans la base $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ si $b_A[i]=1$. Ensuite, Alice envoie $|\widehat{ra_1}\rangle, |\widehat{ra_2}\rangle, .., |\widehat{ra_{2n}}\rangle$ à Carol.
- De même, Bob crée *2n* bits $ra_1, .., rb_{2n}$ aléatoirement, une chaîne b_B de *2n* bits aléatoires, une chaîne des états quantiques $|\widehat{rb_1}\rangle, |\widehat{rb_2}\rangle, .., |\widehat{rb_{2n}}\rangle$ Ensuite, Bob envoie $|\widehat{rb_1}\rangle, |\widehat{rb_2}\rangle, .., |\widehat{rb_{2n}}\rangle$ à Carol.
- Carol reçoit $\{|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle\}$ pour *i=1,..,2n*, vient d'Alice et Bob. Pour chaque paire $\{|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle\}$, Carol utilise le circuit CNOT-M (voir Fig. 5) pour obtenir deux bits classiques à la sortie. Notez que ces deux bits classiques ne contiennent pas plus d'informations qu'un bit classique ra_i *XOR* rb_i.
- Carol envoie à Alice et Bob tous les *2n* paires de deux bits classiques obtenus. Le rôle de Carol s'arrête ici.

Étape 2 : Tamiser.

- Alice et Bob communiquent leurs bases b_A et b_B. Si leurs bases sont différentes à une position i, alors qu'ils abandonnent les données concernant cette position.
- A chaque position restant i, qu'ils rejettent un bit dans chaque paire reçue de Carol comme la suivante. Ils rejet soit le premier bit, soit le deuxième bit si leur base commune à la position i est soit $|+\rangle$ ou soit $|\times\rangle$, respectivement.
- Les bits restants forment les trois chaînes de $2m$ bits a, b, c où $a = a_1, .., a_{2m}$, $c = c_1, .., c_{2m}$, $b = b_1, .., b_{2m}$. Notons qu'Alice garde deux chaînes a, c et Bob garde deux chaînes b, c où dans le cas idéal (appareils parfaits, canaux parfaits, etc), ces trois chaînes devraient tenir $c_i = a_i \; XOR \; b_i$ où $i=1, ..,2m$ et $m \approx \frac{n}{2}$.

Étape 3 : Détecter la présence d'Eve.

- Alice et Bob choisissent par hasard m sur $2m$ positions afin de détecter la présence d'Eve. Il s'agit de deux chaînes de m-positions : la chaîne de Check-Position $CP=cp_1, .. ,cp_m$ et la chaîne de Message-Position $MP=mp_1, .. ,mp_m$.
- Alice et Bob annoncent les valeurs a_{cpi}, b_{cpi} aux check-positions cp_i, pour $i= 1, .., m$. Ils testent si $c_{cpi} = b_{cpi} \; XOR \; a_{cpi}$. Si le nombre des résultats négatifs est supérieur à un seuil pré-calculé alors ils interrompent la transaction.

Étape 4 : Créer des masques jetables pour Alice et Bob.

- Les bits dans les m-positions de Message-Position forment trois chaînes de m bits $A, B,$ et C où $A = A'_1, .., A'_m, C = C'_1, .., C'_m, B = B'_1, .., B'_m$. Nous notons que'Alice tient deux chaînes A, C et Bob tient deux chaînes B, C. Dans le cas où l'appareil quantique et les canaux sont parfaits, il devrait tenir $C'_i = A'_i \; XOR \; B'_i$, pour $i = 1,.., m$, et $m \approx \frac{n}{2}$.
- Avec les trois chaînes A', B' et C', Alice et Bob effectuent les schémas classiques de Correction d'Erreur et d'Amplification de Confidentialité pour obtenir les trois nouveaux chaînes plus courtes A, B et C qui tiennent

toujours *C = A XOR B* mais Eve a une quantité d'informations négligeable sur *A* et *B*.

Étape 5 : Transmettre la clé *K*.

- Alice crée la clé secrète *K* qui a la même longueur de *A, B* et *C*. Elle envoie *K XOR A XOR C = K XOR B* à Bob.
- Bob reçoit *K XOR B*, récupère *K = K XOR B XOR B*.

Nous avons justifié la sécurité du protocole QUR. Nous avons trouvé qu'à l'étape 3, le taux d'erreur dans les positions Check-Position doit se comporter comme cela dans les positions Message-Position. En effet, depuis Eve ne sait pas par avance le choix des positions Check-Position et Message-Position qui étaient choisis au hasard, elle ne peut pas traiter les paires circulantes $\{|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle\}$ différemment.

La preuve de sécurité du protocole QUR est très similaire à celle du protocole BB84 qui est le premier protocole pour la distribution de clé quantique. Nous avons pu montrer que toutes les attaques quantiques qui peuvent échapper à la détection sont celles qui ne donnent aucune information à Eve.

Nous notons qu'après l'étape 2 (tamisage) a été terminé, les paires restantes sont toujours être préparés dans la même base, soit $|++\rangle$ ou soit $|\times\times\rangle$. Considérons par exemple une paire de deux états $|xy\rangle$. Dans le cas sans écoute d'Eve, Carol s'applique la porte CNOT sur $|xy\rangle$ pour obtenir deux états ordonnés à la sortie $|c_1c_2\rangle$.

$$CNOT|xy\rangle = |c_1c_2\rangle, \qquad (1)$$

où $|x \oplus y\rangle = |c_1\rangle$ ou $|x \oplus y\rangle = |c_2\rangle$ dépend de $|xy\rangle$ sont été préparé dans $|++\rangle$ ou $|\times\times\rangle$, respectivement.

Eve peut avoir un contrôle total sur le site Carol. Supposons qu'Eve a un ordinateur quantique. Nous notons que toutes les transformations quantiques d'Eve, pas

seulement sur les canaux mais aussi sur le site Carol, peuvent être représentées par l'opérateur unitaire U. Désignons par $|E\rangle$ la sonde quantique d'Eve.

Alice et Bob utilisent la valeur $x \oplus y$ qui est extraite de deux états quantiques $|c_1 c_2\rangle$ pour détacter l'écoute d'Eve. La détection est décrite à l'étape 3 du protocole QUB. Depuis Eve ne connaît pas les bases de $|xy\rangle$, Eve ne sais pas si $|x \oplus y\rangle = |c_1\rangle$ ou $|x \oplus y\rangle = |c_2\rangle$. D'autre part, afin d'éviter la détection, Eve ne doit pas faire changer la valeur $x \oplus y$. Par conséquent, Eve devrait ne pas toucher à la fois tous les deux états ordonnés $|c_1 c_2\rangle$, c'est à dire,

$$U|xy\rangle|E\rangle = |c_1 c_2\rangle|E_1\rangle. \qquad (2)$$

Maintenant, nous considérons une autre paire de deux états $|uv\rangle$ qui n'est pas orthogonal avec $|xy\rangle$. De même, dans le cas sans écoute d'Eve, nous avons

$$CNOT|uv\rangle = |c_3 c_4\rangle. \qquad (3)$$

Dans le cas d'avoir la présence d'Eve, depuis Eve ne connaît pas les bases de $|xy\rangle$, Eve ne sais pas si $|u \oplus v\rangle = |c_3\rangle$ ou $|u \oplus v\rangle = |c_4\rangle$, afin d'échapper à la détection, Eve doit laisser les deux états de sortie $|c_3 c_4\rangle$ intacte, c'est à dire,

$$U|uv\rangle|E\rangle = |c_3 c_4\rangle|E_2\rangle. \qquad (4)$$

Depuis la porte CNOT est unitaire, à partir de (1) et (3), nous avons

$$\langle xy|uv\rangle = \langle c_1 c_2|c_3 c_4\rangle. \qquad (5)$$

Depuis l'opérateur *U* est unitaire, à partir de (2) et (4), nous avons

$$\langle xyE|uvE\rangle = \langle xy|uv\rangle\langle E|E\rangle =$$
$$\langle xy|uv\rangle = \langle c_1 c_2 E_1|c_3 c_4 E_2\rangle = \langle c_1 c_2|c_3 c_4\rangle\langle E_1|E_2\rangle. \qquad (6)$$

Appliquer (5) à (6), nous avons

$$\langle xy|uv\rangle = \langle xy|uv\rangle\langle E_1|E_2\rangle. \qquad (7)$$

Depuis $|xy\rangle$ et $|uv\rangle$ sont préparés dans les bases non-orthogonales $|+\rangle$ et $|\times\rangle$, donc $\langle xy|uv\rangle \neq 0$. Ainsi, $\langle E_1|E_2\rangle = 1$. D'autre part, $|E_1\rangle$ et $|E_2\rangle$ sont normalisées. Alors, $|E_1\rangle = |E_2\rangle$. Cela implique qu'Eve ne peut pas distinguer $|xy\rangle$ avec $|uv\rangle$ à l'aide de sa sonde. En d'autres termes, si une écoute peut éviter la détection, alors elle donne aucune information à Eve.

A côté des attaques quantiques, Eve peut également appliquer des attques classiques. La seule information qu'elle peut obtenir est la valeur classique *x XOR y* révélée au site Carol. Toutefois, Eve ne peut tirer les deux pièces d'information *x* et *y* à partir de *x XOR y*. La transmission de clé à l'étape 5 est inconditionellement garantie puisque nous utilisons le schéma incassable masque jetable, ou one-time pad en termes Anglais. Alors, le protocole QUB est inconditionnellement sûr comme les protocoles QKD originaux.

Bien que le modèle QUB puisse étendre la portée de QKD, sa capacité n'est que deux fois de la distance possible du modèle QKD original. Nous avons pu arriver au meilleur résultat. Le modèle des relais quantiques méfiants, ou Quantum Untrusted Relais (QUR) est très semblable au modèle QQTR (voir Fig. 4). Cependant, les relais Carol 1,.., Carol N peuvent être contrôlés par Eve. Nous devons utiliser un autre protocole de communication pour garantir la sécurité de la clé transmise. Pour plus de commodité, nous utilisons également C_0 et C_{N+1} pour désigner Alice et Bob, respectivement. Le protocole QUR est composé de 5 étapes:

Étape 1 : Prépare, échanger et mesurer des qubits.

- Chaque B_i, pour $i = 1,.., N+1$, prépare n états Bell $(\Phi^+)^{\otimes n}$.
- Chaque B_i, pour $i = 1,.., N+1$, envoie la première moitié de chaque état Bell à C_{i-1} (i.e. la station précédente), et la deuxième moitié à C_i (i.e. la station suivante).

- Alice (également connu comme C_0) et Bob (connu comme C_{n+1}), chacun reçoit n qubits. Ils choisissent au hasard et indépendamment des bases de measurement.
- Chaque C_i, pour $i = 1,.., N$, reçoit $2n$ qubits vient de B_i et B_{i+1} de manière synchrone. Cela veut dire qu'elle reçoit n fois, et pour chaque fois qu'elle reçoit une paire de qubits: l'un vient de B_i et l'autre de B_{i+1}. Elle les mesure en utilisant le circuit CNOT-M (voir Fig. 5). Elle envoie les valeurs de sortie et les bases correspondantes à Alice et Bob. *Après ça, le rôle de C_i s'arrête.*

Étape 2 : Tamiser.

- Alice et Bob annoncent leurs bases.
- Si leurs bases sont différentes à la position i, Alice et Bob rejettent cette position.
- Pour chaque position restante i, Alice et Bob rejettent soit la première ou soit la deuxième sortie du circuit CNOT-M si la base commune de Alice et Bob est soit $|+\rangle$ ou soit $|\times\rangle$, respectivement.
- Les valeurs restantes se forment $N+2$ chaînes de $2m$-bits $a = a_1, .., a_{2m}$, $c(i) = c(i)_1, .., c(i)_{2m}$, pour $i = 1, .., N$, $b = b_1, .., b_{2m}$. Alice garde N+1 chaînes a, $c(i)$ pour pour $i = 1, .., N$. Bob garde N+1 chaînes a, $c(i)$ pour pour $i = 1, .., N$. Ces $N+2$ chaînes devraient tenir $\bigoplus_{i=1}^{N} c(i)_j = a_j \oplus b_j$, pour $j= 1,.., 2m$ où $m \sim n/4$.

Étape 3 : Détecter la présence d'Eve.

- Alice et Bob se mettent en accord alératoirement m positions dans $2m$ positions totales pour vérifier la présence d'Eve. Cela forme les deux chaînes indiquant m-positions: l'une pour vérification $CP = cp_1, .., cp_m$ et l'autre pour information $MP = mp_1, .., mp_m$.
- Alice et Bob annoncent les valeurs aux positions de vérification CP: $a = a_{cp1}, .., a_{cpm}$; $b = b_{cp1}, .. , b_{cpm}$; $c(i) = c(i)_{cp1},.., c(i)_{cpm}$, pour $i = 1,.., N$, respectivement. Ils vérifient si $\bigoplus_{i=1}^{N} c(i)_j = a_j \oplus b_j$, ou pas. Si certains des résultats négatifs, ils abandonnent la transaction.

Étape 4 : Créer les masques jetables.

- Les valeurs aux *m* positions *MP* forment *N+2* chaînes de *m*-bits : $Q^A = Q^A_1$, .., Q^A_m; $Q^{C(i)} = Q^{C(i)}_1$, .., $Q^{C(i)}_m$, pour $i = 1,..,N$ et $Q^B = Q^B_1$, .., Q^B_m, où Alice garde *N+1* chaînes Q^A, $Q^{C(i)}$ et Bob garde *N+1* chaînes Q^B, $Q^{C(i)}$. Nous avons rémarqué que dans la cas idéal (appareils et canaux parfaits), ces *N+2* chaînes tiennent $\oplus_{i=1}^{N} Q^{C(i)} = Q^A \oplus Q^B$.
- Alice et Bob calculent $Q^C \oplus_{i=1}^{N} Q^{C(i)}$. Avec les trois chaînes Q^A, Q^B, Q^C, Alice et Bob performent les schémas classiques de Correction d'Erreur et d'Amplification de Confidentialité pour obtenir les trois nouveaux chaînes plus courtes P^A, P^B, P^C qui tiennent toujours $P^C = P^A \oplus P^B$ mais Eve a une quantité d'informations négligeable sur P^A, P^B.

Étape 5 : Transmettre la clé K.

- Alice crée la clé secrète K qui a la même longueur avec P^A, P^B, P^C. Elle envoie $K \oplus P^C \oplus P^A = K \oplus P^B$ à Bob.
- Bob reçoit $K \oplus P^B$, récupère $K = K \oplus P^B \oplus P^B$.

Nous avons pu montrer dans Section 11.3.3 et 11.3.4 que le protocole QUR est correct et également de garantir la sécurité inconditionelle sur la clé K.

3. Résultats principaux

L'objet central de de cette thèse est de dépasser la limitation de la portée d'application de la technique QKD. Nous avons attaqué le problème par deux approches directe et indirecte : d'une part, nous avons étudié la possibilité de construire un réseau QKD à grande échelle, et d'autre part, nous avons étudié de nouvelles méthodes directement à relayer la clé QKD sans réduire la sécurité finale. En effet, étendre la portée de la technique QKD et construire le réseau QKD à

grande échelle ont une corrélation étroite : si on peut résoudre ce premier alors on peut l'utiliser pour résoudre ce dernier, et vice-versa.

Afin de construire le réseau QKD à grande échelle, nous avons proposé un modèle de réseau de dense qui permet à deux nœuds QKD à distance arbitraire de partager les clés extrêmement secrètes. Nous avons montré que le réseau QKD proposé est capable de maintenir la sécurité inconditionnelle sur clé la transmission de clé sous la condition que chaque nœud du réseau doit se garantir un niveau de sécurité calculable qui fait apparaître la phénomène de percolation. Une fois que la percolation de sécurité est possible, nous avons examiné des algorithmes de routage stochastique et compte tenu des formules pour mesurer le nombre des sous-clés qui doivent être envoyés afin d'obtenir la clé finale secrète.

Afin d'élargir directement la portée de la technique QKD, nous avons proposé des nouveaux modèles qui permettent de relayer les clés QKD sans réduire la sécurité des systèmes QKD originaux. Les modèles QQTB et QQTR nécessitent des noeuds intermédiaires de suivre honnêtement leur protocole de communication. Dans un tel cas, même si la méchante Eve espionne les nœuds intermédiaires, elle ne peut obtenir aucune information sur la clé finale. Notre modèles QQTB et QQTR introduisent des caractéristiques importantes et intéressantes par rapport à les précédentes modèles de relais de QKD (voir notre discusion dans Sections 10.3.4, 10.4.3, et 10.5).

Les modèles QUB et QUR peuvent être considérés comme deux versions améliorées des modèles QQTB et QQTR. Dans ces modèles, Eve est autorisé à avoir un contrôle total sur les nœuds intermédiaires. Toutefois, si, dans le but de voler l'information de la clé finale, Eve n'a pas suivi le protocole de communication, elle est détectée. Sinon, elle ne peut avoir aucune information sur la clé finale. Une telle situation est totalement similaire à celle dans les protocoles QKD originaux. Notre modèles QUB et QUR introduisent des caractéristiques

importantes et intéressantes par rapport à la précédente QKD relayer les modèles (voir notre discusion dans Section 11.4).

Notre recherche a été les premières étapes pour aller vers les nouvelles solutions potentielles au problème de la portée d'application de QKD. Par conséquent, beaucoup de choses peuvent être exploités dans l'avenir.

Pour notre modèle proposé du réseau QKD à grande échelle, la topologie, à compter des algorithmes de routage spéciaux , des différentes stratégies d'attaque, et les scénarios d'application peuvent être les nouveaux sujets d'étude intéressant.

Pour nos modèles proposés de relayer des clés QKD, une estimation de ressources nécessaires dans le cas pratique en comptant des dispositifs quantiques imparfait est de d'intérêt. Une étude comparative sur la performance des modèles proposés avec celles de répéteur quantique standardisé basé sur entanglement swapping est aussi l'un de nos objectifs. D'ailleurs, nous sommes également s'intéresse à l'évolution de notre modèle QUB, c'est-à-dire d'une recherche sur une gamme des nouvelles modèles de relais QKD qui ne nécessitent pas de sources des photon d'intrication.

A présent, notre résultat de recherche nous avons rendu une série des articles et communications internationaux (voir Section 1.3).

4. Plan de thèse

Ce manuscrit est décomposé de 12 chapitres, y compris d'un chapitre d'introduction.

Chapitre 1 est une introduction courte qui présente la motivation et l'objectif de la thèse. Il donne une introduction concise mais utile pour des modèles classiques de

chiffrement et les caractéristiques de la théorie quantique qui conduit à la possibilité de distribution de clés au-delà des limites imposées par la théorie classique.

Chapitre 2 donne un bref aperçu des concepts et outils de base dans la théorie quantique de l'information. Les concepts essentielles, comme le qubit, les états quantiques, comment peut-on mesurer les états quantiques, comment évoluent-ils les états quantiques, comment peut-on calculer l'entropie d'un état quantique (l'entropie de Von Neumann), le modèle de computation basé sur les portes quantiques, etc., ont été exposées et détaillées.

Chapitre 3 introduit la distibution quantique de clé, Quantum Key Distribution ou QKD en termes Anglais, qui est la plus mûre application de la théorie de l'information quantique dans le domaine de la cryptologie. QKD aborde le problème de la distribution de la clé secrète entre deux parties à distance. Ses avantages et ses inconvénients par rapport à ceux de la contrepartie classique sont étudiés.

Chapitre 4 donne un état de l'art des réseaux QKD. L'architecture, la topologie et les protocoles qui rendent réseau des liens individuelles QKD sont étudiées.

Chapitre 5 discute les avantages et les inconvénients des réseaux QKD présents. Un nouveau cadre qui peut rendre possible la construction d'un réseau QKD à grande échelle est proposé. Chapitre 6 analyse la condition à laquelle les deux noeuds éloignés du réseau QKD à grande échelle peut établir des clés inconditionnellement sûr comme ceux de système QKD original. Une fois que la condition trouvée détient, Chapitre 7 étudie des algorithmes de routage sécurisé qui devraient être appliquées dans le réseau QKD afin d'obtenir la sécurité inconditionnelle. Chapitre 8 discute sur les scénarios d'application en réel des résultats obtenus dans Chapitres 5, 6 et 7.

Chapitre 9 introduit les éléments principaux et le principe de fonctionnement des répéteurs quantiques ainsi que des relais quantiques actuelles. Chapitre 10 propose deux nouveaux modèles de relais quantique qui nécessitent des nœuds intermédiaires étant quasi-confiance. Chapitre 11 évolue les deux modèles proposée dans Chapitre 10 à deux autres modèle dans lesquels les intermédiaires nœuds sont autorisés à être méfiants. Les modèles de relais proposés dans Chapitres 10 et 11 permettent d'étendre la portée de la technique QKD originale sans réduire sa sécurité d'origine.

Enfin, Chapitre 12 conclut la thèse par un résumé des résultats obtenus ainsi que des suggestions pour l'exploration plus loin.

ON THE QKD RELAYING MODELS AND BUILDING QUANTUM NETWORKS

by

Quoc-Cuong Le

DISSERTATION
Submitted in Partial Fulfillment of the
Requirements for the Degree of

Doctor of Philosophy

Network and Computer Science department
TELECOM ParisTech, Paris, France

2009

ACKNOWLEDGMENTS

In the first place, I'd like to thank my advisor, Professor Patrick Bellot, for giving me an invaluable opportunity to work with him on a challenging and extremely interesting subject over the past four years. His patience, support and advice have guided me going through the most difficult moments of my research. Without him, this thesis would never be possible.

I am grateful to Professor Michel Riguidel, Head of Department, for giving me the opportunity to work at the Network and Computer Science Department of Telecom ParisTech. I would like also to express my warmest thanks to other staff members as well as my colleagues Minh-Dung, Tan-Nguyen, Loïc, Linh-Tam for providing me an excellent working environment at Telecom ParisTech.

I would like to thank Professor Marc Bui and Doctor Daniel Oi for agreeing to serve on my thesis committee and for sparing their invaluable time reviewing the manuscript.

Lastly, I owe my deepest thanks to all my family, especially my father, mother and brother for their love, understanding, support and constant encouragement. Above all, I want to dedicate this thesis to my wife Minh-Khanh, my daughters Minh-Thao and Khanh-Linh who are always by my side.

Quoc-Cuong Le
Telecom ParisTech, Mars 2009

ON THE QKD RELAYING MODELS AND BUILDING QUANTUM NETWORKS

by

Quoc-Cuong Le

B. S., Hanoi University of Technology, 2001
M. S., Institut de la Francophonie pour l'Informatique, 2005

ABSTRACT

Quantum Key Distribution (QKD) is an unconditionally secure key-agreement scheme that promises worthwhile applications. One of the most critical drawbacks is the limitation of QKD's range. This Dissertation addresses two main topics: (1) how to build large-scale QKD networks, (2) how to securely relay the QKD keys. These two topics have a tight correlation: if one can solve the former then one can use its result to solve the latter, and vice-versa.

Quantum Key Distribution (QKD) networks are of much interest due to their capacity of providing extremely high security keys to network participants. Most QKD network studies so far focus on trusted models where all the network nodes are assumed to be perfectly secured. This restricts QKD networks to be small. In the first stage of our work, we develop a novel model dedicated to large-scale QKD networks, some of whose nodes could be secretly eavesdropped. We investigate the key transmission problem in the new model by an approach based on percolation theory and stochastic routing. Analyses show that under computable conditions, large-scale QKD networks could protect secret keys with an extremely high probability. Simulations validate our results.

In our second stage, we investigate the quasi-trusted QKD relaying model. We propose a new definition for quasi-trusted relays. Our quasi-trusted relays are defined as follows: (i) being honest enough to correctly follow a given multi-party finite-time communication protocol; (ii) however, being under the monitoring of eavesdroppers. Based on the new definition, we first develop a simple 3-party quasi-trusted model called Quantum Quasi-Trusted Bridge (QQTB) model. In this model, the origin Alice and the destination Bob are assumed out of range of Quantum Key Distribution (QKD). Carol is a quasi-trusted relay that can share QKD links with both Alice and Bob. We show that QQTB protocol allows Alice and Bob, in cooperation with Carol, to securely establish secret keys. The originality of QQTB protocol is that we do not need invoke entangled photon pairs. Then, we extend QQTB model to Quantum Quasi-Trusted Relay (QQTR) model that is capable of securely

distributing secret keys over arbitrarily long distances. Although QQTB model requires entangled photon sources, the originality is that we do not invoke entanglement swapping as in the current standard quantum repeater model.

In the final stage, we propose two novel untrusted QKD relaying models: Quantum Untrusted Bridge (QUB) and Quantum Untrusted Relay (QUR). Both QUB and QUR models provide unconditional security as the original QKD protocols. The QUB model works with single-photon sources. This model is capable of extending the range of single-photon based QKD schemes up to two times without invoking entangled photons. The QUR model works with entangled-photon sources and is capable of extending QKD's range up to an arbitrarily long distance. The originality is that the QUR method is not based on entanglement swapping as was the case of the current standard quantum repeater model. Indeed, our new untrusted QKD relaying models are built based on a new approach compared to that of the standard quantum repeater model: while the idea of the standard quantum repeater model is creating *entangled-state pairs* over the entire length of key distribution, our idea is to combine two facts: (1) enemies cannot gain information without disturbing *unknown quantum single-states*, (2) enemies cannot infer two partial pieces of *classical* information a and b from the global *classical* information $c = a$ XOR b.

Contents

Chapter 1

Introduction

1.1 Motivations and Objectives

In the classical information theory, communicating secret information between distant parties was known as a hard challenge from many years ago. The history might begin in 1948 when Shannon [83] introduced one central fundamental concept of the classical information theory: the entropy H, also well-known under the name "Shannon's entropy". Shannon's entropy of the random variable X, conventionally denoted by $H(X)$, quantifies on average how much information one gains when learning the value of X. Or in other words, $H(X)$ measures the *uncertainty* of X before one learns its value. With the concept of *entropy*, Shannon showed that it is possible to build a virtual noiseless and lossless channel from a realistic noisy and lossy one. This result is now well-known by the name *Shannon's noiseless coding theorem*. Inspired from this work, in 1949, Shannon continued to introduce a secure communication model in which the channel between Alice and Bob is noiseless and lossless. However, Eve can perfectly eavesdrop the channel, i.e. Eve can receive identical copies of all the messages received by Bob [84]. Roughly speaking, Alice encodes the plain-text message M into a codeword C, then sends C onto the channel. Both Bob and Eve receive C. In this context, Shannon showed that the secrecy of M is perfect if the mutual information of M and C, conventionally denoted by $I(M;C)$, is equal to 0, i.e. the codeword C gives no information about the plain-text M. Such a perfect secrecy is now known as *theoretic information security*, or so-called *unconditional security*, by the fact that it does not depend on the computational power of the enemy Eve. Shannon showed that the unconditional security on M can be achieved by using unbreakable one-time pad scheme [91], provided that Alice and Bob initially share the secret key K which has at least the same length of M, or in other words $H(K) \geq H(M)$. Unfortunately, this condition is hard for almost practical

communication applications. Hence, the question of interest is how two distant parties can do if they do not share previously the long enough key? Can Alice and Bob generate a longer secret key from the initial shorter secret key?

In Shannon's secure communication model [84], inequality $H(K) \geq H(M)$ implies a negative response to the above question, i.e. it is impossible to generate a longer secret key from the initial shorter secret key. However, notice that this impossibility takes effect under Shannon's basic assumptions that suppose that the channel is reduced to be perfect (noiseless and lossless) and the enemy Eve can get exactly any things got by the legitimate party Bob. Thus, in order to make it possible of extending an initial short key, one thinks of modifying Shannon's model, or precisely, modifying Shannon's assumptions. Indeed, one tries to build other plausible models in which information got by the eavesdropper is different from that got by the legitimate receiver. So far, one knows that there are at least two such models: one based on using directly noisy classical channels and the other based on exploiting quantum channels.

Let us take a glance at the secure communication model based on noisy channels. In 1975, A. D. Wyner introduced the wire-tap channel and showed that in his model it is possible to communicate the key K in secrecy with respect to some conditions [97]. Wyner's wire tap channel was deeply studied afterward by Csiszár and Körner [29], Maurer [69, 70], and Van Dijk [90]. Roughly speaking, the wire-tap channel model can be described as in Fig. 1.1. The sender and receiver, conventionally called Alice and Bob, share the channel $C1$. The eavesdropper Eve gets information transmitted by Alice through another channel $C2$, also called the wire-tapper's channel. Both channels $C1$ and $C2$ are discrete and memoryless. Suppose that Alice wants to send to Bob the secret message k-bit M. She encodes M into an n-bit codeword X, then transmits X. Due to the two different channels $C1$ and $C2$ Bob and Eve receive n-bit strings Y and Z, respectively. Thus, the model can be mathematically described as follows. The random variables X, Y, Z, that respectively take values in the finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, are considered. The security of communication between Alice and Bob is characterized by the conditional probability distribution $P_{YZ|X}$.

Alice focus on the two following goals:

1. Security: Eve has no knowledge on M, or in other words, the mutual information $H(Z; M) = 0$.

2. Reliability: Bob can, with a negligible small error, retrieve M from Y, or in other words, the mutual information $H(Y; M) \approx 1$.

The secrecy capacity C_s of the wire-tap model is the biggest $\frac{k}{n}$ with that the two above

goals are still achieved. Intuitively, C_s depends on the properties of the channels $C1$ and $C2$.

In [97], Wyner showed that if $C2$ is a degraded version of $C1$, e.g. $C2$ is $C1$ concatenated by another discrete and memoryless channel, then $C_s > 0$. In [29], Csiszár and Körner showed that if $C1$ is less noisy than $C2$ then $C_s > 0$. More precisely, for all distribution P_{XYZ} we have

$$C_s \geq \max(I(X;Y) - I(X;Z)) \tag{1.1}$$

where X, Y, Z are random variables that form a Markov chain. Notice that since $X \to Y \to Z$ is a Markov chain, $P_{Z|XY} = P_{Z|Y}$ and $I(X;Z|Y) = 0$.

Maurer [69, 70] considered a more general case of $C1$ and $C2$, as described in Fig. 1.1, and showed that even though $C1$ is noisier than $C2$ then C_s is still positive,

$$C_s \geq \max\{I(X;Y) - I(X;Z), I(Y;X) - I(Y;Z)\}. \tag{1.2}$$

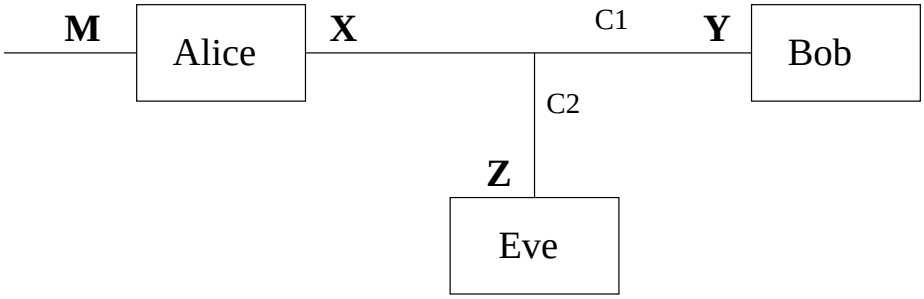


Figure 1.1: The wire-tap channel.

The modern quantum physics recognizes the world in a different way compared with the classical physics. The *Heisenberg uncertainty principle* states that the non-commuting observables, for instance position and momentum, cannot both have precisely defined values. This is the nature of a quantum physical system itself. Indeed, if two observables A and B do not commute than performing a measurement of A will necessarily influence the outcome of the measurement of B afterward. In others words, the act of acquiring information about a physical system will inevitably disturb the current state of the system. *There is no counterpart of uncertainty principle in the classical physics.*

Another distinguished property of quantum physics is the *no-cloning theorem*, stated by Wootters, Zurek and Dieks in 1982 [96, 35]. The no-cloning theorem forbids to make perfect copies of an unknown quantum state. Indeed, this theorem also concerns the trade-off

between acquiring information and making disturbance in the quantum world. Assume that we could make perfect copies of a quantum state, then we can measure an observable on the copy in order to do not disturb the original state. This will violate the uncertainty principle. Remind us that in the classical physics we can measure precisely all the observables that together completely describe a physical system. As a result, in principle one can make identical copies of the measured system.

In quantum physics, a system can be in a *superposition* of many different states at the same time, and exhibits the *interference effect* of these states during the evolution of the system. Besides, spatially separated quantum systems can be *entangled*, and the local operations on a system can have *non-local* effects on other distant systems. In 1964, J. Bell [4] showed that no physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics. This discovery is well-known under the name *Bell's theorem*. Bell's theorem introduces two major importances: on one hand, it proves that local hidden variables cannot remove the statistical nature of quantum mechanics; on the other hand, it implies that if quantum mechanics is correct then the universe is not locally deterministic. Bell's theorem also implies that quantum information can be encoded in *non-local* correlations of the spatially separated parts of a quantum system. Such information has no counterpart in classical information and brings a new potential resource to exploit.

In recent years, Quantum Key Distribution (QKD) emerges and draws many attention of cryptographic community by the fact that this technique, by exploiting special properties of quantum mechanics, can provide unconditional security of the key distribution [8,38,88]. In fact, QKD requires an initial short shared key to work. Hence, one can say that QKD allows to create a longer key from a shorter key, but not generate the key. This is impossible in classical mechanics, or in other words, QKD has no counterpart in the classical information processing theory. However, QKD has some own limitations, most prominently throughput and range [42, 56]. This makes harder the build of large QKD-based networks that enable a perfect distribution of secret key between network's participants. Notice that extending the range of QKD and building the large-scale QKD network have a tight correlation: the solution for the former can be applied in the latter, and vice-versa.

Attracted by their potentials, our research focus on extending the QKD's range and building the large-scale QKD network. Our objectives consist of studying then proposing new solutions for extending the QKD's range and building the large-scale QKD network.

1.2 Thesis Outline

This dissertation is organized into twelve chapters, including this introduction. The next chapter briefly reviews some of key concepts and principles of quantum mechanics, their advantages, drawbacks and prominent applications in the information processing theory.

Chapter 3 introduces QKD (QKD) that is the most matured application of quantum information in the field of cryptology. QKD addresses the problem of distributing the secret key between distant parties. Its advantages and drawbacks compared to those of the classical counterpart are studied.

Chapter 4 reviews current QKD networks. The architecture, topology and protocols that make networking from individual QKD links are investigated.

Chapter 5 discusses on the advantages and drawbacks of current QKD networks. A new framework that can make it possible building the world-wide QKD network is proposed. Chapter 6 investigates the condition on which two distant nodes of the world-wide QKD network can establish unconditionally secure keys as those of the original QKD schemes. Once the condition for unconditionally secure keys holds, chapter 7 proposes secure routing algorithms that should be applied in the world-wide QKD network in order to get unconditional security on the key distribution. Chapter 8 discusses on the scenarios of application for the results of Chapters 5, 6 and 7.

Chapter 9 introduces the main components and the operational principle of current quantum repeaters as well as current quantum relays. Chapter 10 proposes a new scheme of quantum relay that requires intermediate nodes being quasi-trusted. Chapter 11 evolves the scheme proposed in Chapter 10 to another scheme in which the intermediate nodes are allowed to be untrusted. Both relay schemes proposed in Chapters 10 and 11 allow to extend the range of the original QKD schemes without reducing their original security.

Finally, Chapter 12 concludes the dissertation with a summary of results as well as suggestions for the further exploration.

1.3 Related Publications

1. Quoc-Cuong Le and Patrick Bellot, "A novel approach to build QKD relaying models", ***accepted*** in International Journal of Security and Communication Networks.

2. Quoc-Cuong Le and Patrick Bellot, "How can quasi-trusted nodes help to securely relay QKD keys", International Journal of Network Security, ***vol. 9***, p.233-241 (2009).

3. Quoc-Cuong Le and Patrick Bellot, "On the QKD relaying models", e-print: http://arxiv.org/abs/0803.3699.

4. Quoc-Cuong Le and Patrick Bellot, "A new proposal for QKD relaying models", in *Proc. of the 17th Int. Conf. on Computer Communications and Networks (ICCCN'08)*, Track on Network Security, St. Thomas, Virgin Island, US, August 2008, doi:0.1109/ICCCN.2008.ECP.23. (*top 15%*)

5. Quoc-Cuong Le and Patrick Bellot, "How to use the quantum XOR gate as a relay to extend the QKD range", in *Proc. of the 4th Int. Conf. on Boolean Functions: Cryptography and Application (BFCA'08)*, Copenhagen, Denmark, May 2008.

6. Quoc-Cuong Le, Patrick Bellot and Akim Demaille, "Towards the World-Wide Quantum Network", in *Proc. of the 4th Information Security and Practice Conference (ISPEC'08)*, ***LNCS 4991***, p.218-232, Sydney, Australia, April 2008.

7. Quoc-Cuong Le, Patrick Bellot and Akim Demaille, "On the security of quantum networks: a proposal framework and its capacity" in *Proc. of Int. Conf. on New Technologies, Mobility and Security (NTMS'07)*, p.385-396, Paris, France, May 2007.

8. Quoc-Cuong Le, Akim Demaille and Patrick Bellot, "Stochastic routing in large grid shaped quantum networks", in *Proc. of the 5th IEEE Int. Conf. on Research, Innovation and Vision for the Future (RIVF'07)*, p.166-174, Hanoi, Vietnam, March 2007.

9. Quoc-Cuong Le and Patrick Bellot, "Enhancement of AGT Telecommunication Security using Quantum Cryptography" in *Proc. of the 4th Int. Conf. on Research, Innovation and Vision for the Future(RIVF'06)*, p.7-16, Ho Chi Minh, Vietnam, February 2006.

10. Minh-Dung Dang, Toan-Linh-Tam Nguyen, Quoc-Cuong Le, Thanh-Mai Nguyen and Patrick Bellot, "Usage of Secure Networks built using Quantum Technology" in *Proc. of the 3rd Int. Conf. on Research, Innovation and Vision for the Future(RIVF'05)*, Cantho, Vietnam, February 2005.

Part I

Quantum key distribution

Chapter 2

Quantum Information

2.1 Quantum state space, pure state and mixed state

2.1.1 Quantum state space: the Hilbert space

In quantum information, one usually uses the *complex* Hilbert space and Dirac's *bra-ket* notations to mathematically describe and work with quantum states. A Hilbert space $\mathcal{H}$ is a *complete* vector space with an *inner product*. Dirac's *ket* and *bra* notations are used to denote a vector and its conjugate, for instant, the vector $|\phi\rangle$ and its conjugate $\langle\phi|$. The inner product $\langle\cdot|\,\cdot\rangle$ is a map taking ordered pairs of vectors over the complex numbers $\mathcal{C}$,

$$\langle\cdot|\,\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathcal{C}.$$

The inner product has its own properties. For all $\psi, \phi, \phi_1, \phi_2 \in \mathcal{H}$ and $a, b \in \mathcal{C}$, this satisfies:

1. *Conjugate symmetry:* $\langle\psi|\,\phi\rangle = \langle\phi|\,\psi\rangle^*$, where the asterisk symbol denotes the conjugate transpose.
2. *Positivity:* $\langle\phi|\,\phi\rangle \geq 0$, the equality i.i.f $|\phi\rangle = 0$.
3. *Linearity:* $\langle\psi|\,\big(a\,|\phi_1\rangle + b\,|\phi_2\rangle\big) = a\,\langle\psi|\,\phi_1\rangle + b\,\langle\psi|\,\phi_2\rangle$.

The *completeness* of the vector space $\mathcal{H}$ in the *norm*, $\|\phi\| = \sqrt{\langle\phi|\,\phi\rangle}$, ensures that all Cauchy sequences will converge to some vector within $\mathcal{H}$. This property is used to

handle infinite-dimensional function spaces, for instant, Fourier analysis. However, it will be enough to work on finite-dimensional inner product spaces in this dissertation.

An important concept for describing and understanding a composite quantum system is the *tensor product*. In mathematics, this is a way of putting vector sub-spaces together to form a larger vector space. In quantum mechanics, the tensor product is also used to describe the structure of the multi-particle quantum system. Suppose V and W are m- and n-dimensional Hilbert spaces of $|\psi\rangle$ and $|\phi\rangle$, respectively. Then the tensor product of $|\psi\rangle$ and $|\phi\rangle$, denoted by $|\psi\rangle \otimes |\phi\rangle$ and often by $|\psi\rangle\,|\phi\rangle$ or $|\psi\phi\rangle$ for abbreviation, is an mn-dimensional Hilbert space $V \otimes W$. Notice that if $|i\rangle$ and $|j\rangle$ are orthonormal bases for V and W then $|\psi\rangle \otimes |\phi\rangle$ is a basis for $V \otimes W$.

By definition the tensor product satisfies the following basic properties. For an arbitrary scalar z and elements $|\psi\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$ of V and $|\phi\rangle$, $|\phi_1\rangle$, $|\phi_2\rangle$ of W,

1. $z(|\psi\rangle \otimes |\phi\rangle) = (z\,|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (z\,|\phi\rangle)$.
2. $(|\psi_1\rangle + |\psi_2\rangle) \otimes |\phi\rangle = |\psi_1\rangle \otimes |\phi\rangle + |\psi_2\rangle \otimes |\phi\rangle$.
3. $|\psi\rangle \otimes (|\phi_1\rangle + |\phi_2\rangle) = |\psi\rangle \otimes |\phi_1\rangle + |\psi\rangle \otimes |\phi_2\rangle$.

2.1.2 Qubit, pure and mixed states

The basic unit of classical information is the bit which is a binary system that can take either value 0 or 1. In quantum information a quantum mechanical two-level system, such as the two spin states of spin $\frac{1}{2}$ atoms or the horizontal and vertical polarizations of a single photon, is used to encode binary information. In reference to the classical bit, such a system is considered as the quantum bit or *qubit* whose two bound state levels encode the classical binary values 0 and 1. Mathematically, the qubit is represented by a vector in the two-dimensional Hilbert vector space $\mathcal{H}_2$. The state vector represents the full and complete knowledge of the system's state. Usually, one considers $|0\rangle$ and $|1\rangle$ as an *orthonormal basis* of $\mathcal{H}_2$. One of the surprising features is that the permitted *pure* states of a qubit $|\phi\rangle$ can be a *superposition* of the two basic states $|0\rangle$ and $|1\rangle$, i.e.

$$|\phi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle\,, \tag{2.1}$$

where α_0, α_1 are complex values, and $|\alpha_0|^2 + |\alpha_1|^2 = 1$. Thus, the set of all the pure states will form the *unit sphere* of $\mathcal{H}_2$. Notice that the two vectors $|\phi\rangle$ and $e^{i\theta}\,|\phi\rangle$ describe the same physical state where $e^{i\theta}$ is called *phase factor*. Once one measures $|\phi\rangle$ by projecting

it onto the basis $\{|0\rangle, |1\rangle\}$, the outcome will be $|0\rangle$ or $|1\rangle$ with probabilities $|\alpha_0|^2$ and $|\alpha_1|^2$, respectively.

A composite quantum system of n qubits spans the 2^n-dimensional vector space $\mathcal{H}_{2^n}$, and can be considered as a superposition of 2^n computational basis vectors. Since bit-strings of length n can be interpreted by numbers from 0 to $2^n - 1$, we can denote an orthogonal basis of $\mathcal{H}_{2^n}$ by $\{|0\rangle, |1\rangle, .., |2^n - 1\rangle\}$. Thus, a *pure* n-qubit system can be represented by

$$|\phi\rangle = \alpha_0 |0\rangle + .. + \alpha_{2^n-1} |2^n - 1\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \tag{2.2}$$

where α_i are complex values and $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$. Once one measures $|\phi\rangle$ by projecting it onto the basis $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$, the outcome will be one out of 2^n basis states $|0\rangle, \ldots, |2^n - 1\rangle$ with probabilities $|\alpha_0|^2, \ldots, |\alpha_{2^n-1}|^2$, respectively.

While a *pure* state can be described by a single ket vector, the *mixed* state is not so. A mixed quantum state is a statistical ensemble of pure states $\{p_k, |\phi_k\rangle\}$ where $\{p_k\}$ is the probability distribution of $\{|\phi_k\rangle\}$, $p_k \geq 0$, $\sum_k p_k = 1$. One describes a mixed state by its associated *density operator*, or also called to *density matrix*, usually denoted by ρ.

The *density operator*, or *density matrix* is defined as

$$\rho = \sum_k p_k |\phi_k\rangle\langle\phi_k| \tag{2.3}$$

where $\{p_k\}$ is a probability distribution and each $|\phi_k\rangle$ is a pure state. Notice that a pure state also can be described by its density matrix.

2.1.3 Measurement and Evolution

Quantum mechanics can be mathematically described by the Hilbert space $\mathcal{H}$ and its associated *linear operators*. If $\mathcal{H}$ is d-dimensional space then the space of linear operators, or *operators* for short, acting on $\mathcal{H}$ is a d^2-dimensional complex vector $L(\mathcal{H})$. The linear operator is a map taking vectors to vectors that preserves vector addition and scalar multiplication. For instant, $A : A|\phi\rangle \to |A\phi\rangle$ is a linear operator, then:

$$A(a|\phi_0\rangle + b|\phi_1\rangle) = a|A\phi_0\rangle + b|A\phi_1\rangle. \tag{2.4}$$

The properties of the quantum system, e.g. position, angular momentum, energy, spin,

etc.,that can be measured are called *observables*. As a quantum mechanical state is described by a vector in a Hilbert space $\mathcal{H}$ observables are represented by *self-adjoint* operators acting on $\mathcal{H}$. Remind us first that the *adjoint* or *Hermitian adjoint*, $A^\dagger$, of the operator A is a linear operator $A^\dagger : \mathcal{H} \to \mathcal{H}$ that satisfies

$$\forall \psi, \phi \in \mathcal{H} : \langle A\psi |\, \phi \rangle = \langle \psi |\, A^\dagger \phi \rangle . \tag{2.5}$$

Thus, A is called a *self-adjoint* operator if $A = A^\dagger$. A self-adjoint operator is also called *Hermitian* operator. Notice that a dynamical variable such as position, momentum, is seen as a corresponding physically meaningful observable, and represented by a Hermitian operator. But not every Hermitian represents for a physically meaningful observable. Indeed, physically meaningful observables must satisfy transformation laws between observations done by different observers in different frames of reference. Under a special relativity, e.g. Galilean invariance, the mathematics of frames of reference is particularly simple, hence, restricts considerably the set of physically meaningful observables.

Eigenstates and eigenvalues of a Hermitian operator A suggest possible numerical outcomes of the *measurement* of the observable A. For example, suppose $|i\rangle$ is an eigenstate of A with the corresponding eigenvalue a_i, then

$$A\,|i\rangle = a_i\,|i\rangle . \tag{2.6}$$

Eq. 2.6 means that if a measurement of the observable A is made on the system of interest being in the state $|i\rangle$ then the observed value must return the eigenvalue a_i. This is the simplest case of measurement in quantum mechanics. In general, the measurement process affects the system state in a non-deterministic but statistically predictable way. When one repeats the measurement of the same observable with the same state we will often get different results. Indeed, after the measurement has been done the initial state may be destroyed and replaced by a statistical ensemble. The measurement is an *irreversible* operation. One can mathematically describe this fact as follows. Consider the observable A,

$$A = \sum a_i P_i \tag{2.7}$$

where each a_i is an eigenvalue and P_i is the projection onto the space of eigenstates of A with its corresponding eigenvalue a_i. Notice that the eigenstates of A can form a complete orthonormal basis in $\mathcal{H}$. This implies that the sub-spaces V_i corresponding the projectors P_i are orthogonal. The measurement of the observable A is equivalent to the measurement

operator M

$$M = \sum P_i \tag{2.8}$$

where

$$\begin{cases} P_i P_j = & \delta P_i, \\ P_i^\dagger = & P_i \\ \sum_i P_i = I \end{cases} \tag{2.9}$$

where δ is the *Kronecker delta* and I is the identity operator.

Suppose that the system of interest is in an arbitrary state $|\phi_0\rangle$. Thus, the measurement M will return the eigenvalue a_i with probability

$$Pr(a_i) = \|P_i |\phi_0\rangle\|^2 = \langle\phi_0| P_i |\phi_0\rangle \tag{2.10}$$

If the obtained outcome is a_i then the quantum state becomes

$$\frac{P_i |\phi_0\rangle}{\sqrt{\langle\phi_0| P_i |\phi_0\rangle}}. \tag{2.11}$$

One can express the prediction of the measurement M in term of the mixed state as follows. Denote by $|\phi_1\rangle$ the state just after the measurement has been done, hence

$$|\phi_1\rangle = \sum_i Pr(a_i) \frac{P_i |\phi_0\rangle}{\sqrt{\langle\phi_0| P_i |\phi_0\rangle}} \tag{2.12}$$

where $Pr(a_i)$ is calculated by Eq. 2.10.

Notice that if one applies one more time again the measurement M on the post-measurement state $\frac{P_i|\phi_0\rangle}{\sqrt{\langle\phi_0|P_i|\phi_0\rangle}}$ then one always gets the outcome a_i and the state $\frac{P_i|\phi_0\rangle}{\sqrt{\langle\phi_0|P_i|\phi_0\rangle}}$. In other word,

$$MM|\phi_0\rangle = M|\phi_0\rangle . \tag{2.13}$$

In fact, the measurement operator M in Eq. 2.8 is known as a *projective* or *orthogonal* measurement. The projective measurement is concerned primarily with many applications of quantum information and quantum computation. The measurement of a qubit in the computational basis $\{|0\rangle, |1\rangle\}$ is a special case of the projective measurement $M = \{P_0, P_1\}$ where $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$ and $a_0 = 0$, $a_1 = 1$. For instance, let us try measure the qubit $|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$. Thus, the probability of obtaining the measurement outcome

$a_0 = 0$ is

$$Pr(\alpha_0) = Pr(0) = \langle\phi| P_0 |\phi\rangle = |\alpha_0|^2 . \tag{2.14}$$

The state after measurement of the outcome 0 is

$$\frac{P_0 |\phi\rangle}{|\alpha_0|} = \frac{\alpha_0}{|\alpha_0|} |0\rangle . \tag{2.15}$$

Similarly, the probability of obtaining the outcome $a_1 = 1$ is $|\alpha_1|^2$ and the corresponding state after measurement is $\frac{\alpha_1}{|\alpha_1|} |1\rangle$.

There is a more generalized measurement, called *Positive Operator-Valued Measure*, or *POVM* for short. However, in this dissertation, it is enough to consider only the orthogonal measurement. The readers interested in the POVM measurement is invited to refer to the standard books of the field such as [76].

How does the state $|\phi\rangle$ of a quantum mechanical system change with time? The response can be mathematically described by using the *time-evolution* operator. Notice that when observing the evolution of the quantum system it must assume that the system is *closed*. This means that the system of interest needs to be *non-relativistic* and *isolated*. Under this assumption the time-evolution operator describes an *unitary* transformation from the state $|\phi_0\rangle$ at time t_0 to the state $|\phi_1\rangle$ at time t_1

$$|\phi_1\rangle = U|\phi_0\rangle . \tag{2.16}$$

Remind us that if the operator U is *unitary* then $U^\dagger U = UU^\dagger = I$. This implies that its inverse equals its conjugate transpose, i.e. $U^{-1} = U^\dagger$. The unitary operator U preserves the norm of vectors, in other words, maps a vector of norm 1 to a vector of norm 1. As an unitary operator always has its inverse, it implies that *any* evolution operation of quantum states is *reversible*. One can apply the operation $U^\dagger$ to *undo* the effect of the operation U on the state $|\phi\rangle$,

$$U^\dagger |\phi_1\rangle = |\phi_0\rangle \text{ or } U^\dagger |U\phi\rangle = |\phi\rangle . \tag{2.17}$$

Notice that this is different compared to the measurement operation. The measurement is *non-reversible*.

2.1.4 No-cloning theorem

The *no-cloning* theorem states that it is *impossible* to make perfect copies of an *unknown* quantum state [96, 35]. This property is distinguished compared with the classical information processing. Remind us that the classical information is encoded by classical signals that may be difficult to copy in practice but can be perfectly copied in principle. The no-cloning theorem states one of the most interesting properties of quantum mechanics. It is exploited as a new rich resource in the information processing theory. Indeed, one has successfully applied the no-cloning theorem to build the inviolable communication channels [8, 38].

Let us show the essential reason that prevents us from making perfect copies of an unknown state. As we have seen in the previous section, we only can measure or make it evolving over time the quantum state. Since a measurement may destroy the initial state, it cannot be the cloning operation. Assume that the time-evolution operator U can produce the perfect copy of unknown states, thus, $U^\dagger U = 1$. We consider two unknown pure states $|\phi\rangle$ and $|\psi\rangle$. We have

$$\begin{cases} U|\phi\rangle|0\rangle &= |\phi\rangle|\phi\rangle \\ U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle . \end{cases} \tag{2.18}$$

Taking the inner product from side to side of Eq. 2.18, since U is unitary we have

$$\langle 0|\,0\rangle\,\langle\phi|\,\psi\rangle = \langle\phi|\,\psi\rangle\,\langle\phi|\,\psi\rangle \tag{2.19}$$

or:

$$\langle\phi|\,\psi\rangle = (\langle\phi|\,\psi\rangle)^2. \tag{2.20}$$

Notice that Eq. 2.20 holds i.i.f $\langle\phi|\,\psi\rangle$ equals either 0 or 1. This implies that the cloning operator U only works *perfectly* with orthogonal states such as $\{|0\rangle, |1\rangle\}$ or $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. The non-orthogonal states, for instant $\{|0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}\}$, cannot be *perfectly* cloned by U.

2.2 Entropy and Information

2.2.1 Shannon entropy

Historically, the classical information theory was developed to study fundamental limits on data compressions and communications. The classical information theory was based on the

probability theory and statistics. In 1948, Shannon proposed using *entropy* to measure the *uncertainty* of a random variable *before* this variable takes a real value. One can also consider *entropy* as an implication of the average amount of *information* that one can gain *after* the random variable reveals its real value. The entropy of a *random* variable is defined in terms of its probability distribution. Let $\mathbf{X}$ be a discrete random variable taking a finite number of possible values $x_1, .., x_n$ with probabilities $p_1, .., p_n$ respectively such that $\forall i : p_i \geq 0$ and $\sum_{i=1}^{n} p_i = 1$. The Shannon entropy of $\mathbf{X}$, conventionally denoted by $H(\mathbf{X})$, is defined by

$$H(\mathbf{X}) = -\sum_{i=1}^{n} p_i \log_2 p_i. \tag{2.21}$$

In the special case where the random variable $\mathbf{X}$ takes binary values with probabilities p and $1-p$, the entropy of $\mathbf{X}$ is measured by the *binary entropy function* $H_2(p)$, i.e.

$$H(\mathbf{X}) = H_2(p) = -p \log_2 p - (1-p) \log_2 (1-p). \tag{2.22}$$

The *joint entropy* of two independent discrete random variables $\mathbf{A}$ and $\mathbf{B}$ is defined by

$$H(\mathbf{X}, \mathbf{Y}) = -\sum_{x,y} p(x,y) \log_2 p(x,y). \tag{2.23}$$

The *conditional entropy* of $\mathbf{X}$ given $\mathbf{Y}$ is defined by

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y} p(y) \sum_{x} p(x|y) \log_2 p(x|y) = -\sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(y)}. \tag{2.24}$$

The *mutual information* of two random variables $\mathbf{X}$ and $\mathbf{Y}$ quantifies the amount of information that can be obtained from one of these variables by observing the other,

$$I(\mathbf{X}; \mathbf{Y}) = I(\mathbf{Y}; \mathbf{X}) = -\sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}. \tag{2.25}$$

From basic definitions we can obtain the following relations:

$$H(\mathbf{X}|\mathbf{Y}) = H(\mathbf{X}, \mathbf{Y}) - H(\mathbf{Y}), \tag{2.26}$$

$$I(\mathbf{X}; \mathbf{Y}) = I(\mathbf{Y}; \mathbf{X}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}), \tag{2.27}$$

$$I(\mathbf{X};\mathbf{Y}) = I(\mathbf{Y};\mathbf{X}) = H(\mathbf{X}) + H(\mathbf{Y}) - H(\mathbf{X},\mathbf{Y}). \tag{2.28}$$

2.2.2 Von Neumann entropy

The Shannon entropy measures the *uncertainty* associated to a probability distribution. Notice that quantum state introduces a nature feature of probability, represented by its associated density matrix instead of the classical probability distribution. The *Von Neumann entropy* is an extension of Shannon entropy that is dedicated to quantum mechanics.

Remind us that the *trace* of a linear operator A over the n-dimensional Hilbert space H is defined as

$$tr(A) = \sum_{i=0}^{n-1} \langle i| Ai\rangle \tag{2.29}$$

where $\{i\}$ is an orthonormal basis of H. Notice that $tr(A)$ is independent to the choice of the orthonormal basis over H. And if A is described by its representation matrix then $tr(A)$ is the sum of the elements on the main diagonal of A.

Consider a quantum state represented by its density operator $\rho = \sum_k p_k|\phi_k\rangle\langle\phi_k|$. As ρ is a density operator, ρ has *trace* equal to one and ρ is a positive operator. This implies that we can have the spectral decomposition $\rho = \sum_i \lambda_i|i\rangle\langle i|$, where $|i\rangle$ is an orthogonal basis, λ_i are real, non-negative eigenvalues of ρ and $\sum_i \lambda_i = 1$.

The *Von Neumann entropy* of ρ is defined by

$$S(\rho) = -tr(\rho \log_2 \rho) \tag{2.30}$$

Remind us that the logarithm of a diagonal matrix is computed by replacing each diagonal element by its logarithm. And if the representation matrix A is diagonalizable then its logarithm can be computed by

$$\log_2 A = V(\log_2 A')V^{-1} \tag{2.31}$$

where

- A' is the diagonal matrix whose diagonal elements are eigenvalues of A,
- V are eigenvectors of A, i.e. each column of V is an eigenvector of A,
- V^{-1} is the inverse of V.

Since we can re-write $\rho = \sum_i \lambda_i |i\rangle\langle i|$ where $\lambda_1, \lambda_2, ..$ are eigenvalues and $|i\rangle$ is an orthonormal basis,

$$S(\rho) = -\sum_i (\lambda_i \log_2 \lambda_i). \tag{2.32}$$

Similar to Shannon entropies it is possible to define quantum joint, quantum conditional entropies and quantum mutual information. The *joint entropy* of a composite system of two components A and B is defined by

$$S(A, B) = -tr(\rho^{AB} \log_2 \rho^{AB}) \tag{2.33}$$

where ρ^{AB} is the density matrix of the joint system AB.

The *conditional entropy* and the *mutual information* are defined in a biased way:

$$S(A|B) = S(A, B) - S(B), \tag{2.34}$$

$$\begin{aligned} S(A; B) = S(B; A) &= S(A) + S(B) - S(A, B) \\ &= S(A) - S(A|B) = S(B) - S(B|A) \end{aligned} \tag{2.35}$$

Let us now consider a mixed quantum state $\rho = \sum_i p_i \rho_i$ where $\{\rho_i\}$ are density operators and $\{p_i\}$ is a probability distribution of $\{\rho_i\}$, respectively. The relation between the entropy of the mixed state and those of elementary (mixed or pure) states and the probability distribution $\{p_i\}$ is described by the following inequality

$$S(\rho) \leq \sum_i p_i S(\rho_i) + H(\{p_i\}) \tag{2.36}$$

where the equality happens when $\{\rho_i\}$ are orthogonal.

Notice that some properties of Shannon entropies are not true for Von Neumann entropies, as the Von Neumann entropy can be known as a generalization of the Shannon entropy. For a more complete study about the properties of the Von Neumann entropy readers are invited to refer to some standard books such as [76].

2.2.3 The Holevo bound

The quantum states are not only impossible to be cloned but also cannot to be perfectly distinguished. The *Holevo bound*, denoted by χ, gives an upper bound of the amount of accessible information given a quantum state ρ,

$$\chi = S(\rho) - \sum_i p_i S(\rho_i) \tag{2.37}$$

where $S(\cdot)$ is the Von Neumann entropy and $\rho = \sum_i p_i \rho_i$.

The Holevo bound can be applied directly for the problem sending information over quantum channels. Suppose that Alice has a classical information source producing symbols $\mathbf{X} = \{0, \ldots, n\}$ with probabilities $p_0, \ldots, p_n$, respectively. With each symbol $\mathbf{X} = i$, Alice sends to Bob a quantum state $\rho_{\mathbf{X}} = \rho_i$. Bob receives and makes a measurement on ρ_i to get the value $\mathbf{Y}$. Based on $\mathbf{Y}$, Bob tries to guess the value $\mathbf{X}$. In reference to the classical information theory we can consider $\mathbf{X}$ and $\mathbf{Y}$ as two discrete random variables, and the capacity of guessing successfully the value of $\mathbf{X}$ can be represented by the mutual information $I(\mathbf{X}; \mathbf{Y})$ that holds

$$I(\mathbf{X}; \mathbf{Y}) \leq \chi \tag{2.38}$$

or

$$I(\mathbf{X}; \mathbf{Y}) \leq S(\rho) - \sum_i p_i S(\rho_i). \tag{2.39}$$

From Inequalities 2.36 and 2.39, we have

$$I(\mathbf{X}; \mathbf{Y}) \leq S(\rho) - \sum_i p_i S(\rho_i) \leq H(\mathbf{X}) \tag{2.40}$$

where the second equality happens i.i.f $\{\rho_i\}$ are orthogonal.

On the other hand, Bob can perfectly infer $\mathbf{X}$ from $\mathbf{Y}$ i.i.f $I(\mathbf{X}; \mathbf{Y}) = H(\mathbf{X})$. Thus, it is obvious that if $\{\rho_i\}$ are non-orthogonal then Bob cannot determine $\mathbf{X}$ with perfect reliability based on his measurement value $\mathbf{Y}$.

2.3 Quantum gates and circuits

Currently, the standard quantum mechanical computation model is the quantum circuit model where a sophisticated quantum computation is decomposed and described by a sequent chain of quantum elementary building blocks, or so-called quantum gates. Roughly describing, a quantum computation consists of three main stages:

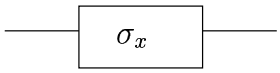
1. Preparing the quantum system in the initial state, normally, $|0\rangle$,
2. Evolving the initial system by letting it go through a quantum circuit that is a sequence of quantum gates,
3. Measuring the final state of the evolved system.

If one ignores the preparing and measuring stages then a quantum computation is represented by its corresponding quantum circuit that consists of a sequence of elementary quantum gates. Thus, what is this as the elementary quantum gates for quantum computation? This is the simplest quantum gates that can together compose the *universal computational sets*. It should first take a look on the single qubit gates due to their simplicity: they work on the simplest quantum mechanical system, one single qubit.

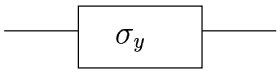
A single qubit is represented by a unitary two-dimensional vector $|\phi\rangle = a|0\rangle + b|1\rangle$ where a, b are complex values that satisfy the norm of 1: $|a|^2 + |b|^2 = 1$. Operations performed on $|\phi\rangle$ must preserve the unitary norm. Hence, they can be represented by the 2×2 unitary matrices. Some of most important one-qubit gates are the *Pauli gates*. Fig. 2.1 shows Pauli gates' representative symbols conventionally used in the design of quantum circuit. The effects of the Pauli gates on the qubit $|\phi\rangle$

$$\begin{aligned} \sigma_x|\phi\rangle &= \sigma_x(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle\,, \\ \sigma_y|\phi\rangle &= \sigma_y(a|0\rangle + b|1\rangle) = -ai|1\rangle + bi|0\rangle\,, \\ \sigma_z|\phi\rangle &= \sigma_z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle\,. \end{aligned} \tag{2.41}$$

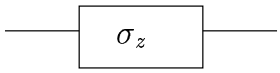
The other common useful one-qubit gates are the *Hadamard* and *α-phase shift* gates (see Fig. 2.2). The Hadamard gate transforms the input qubit $|x\rangle$, $x \in \{0, 1\}$, to the output qubit $(-1)|x\rangle + |1 - x\rangle$. One can also describe the effect of the Hadamard gate on an



$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

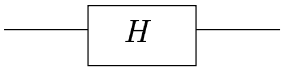


$$\sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

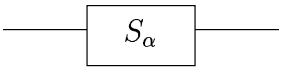


$$\sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Figure 2.1: Pauli gates and their transformation matrices.



$$H = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



$$S_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

Figure 2.2: Hadamard and Phase gates.

arbitrary pure qubit $|\phi\rangle = a|0\rangle + b|1\rangle$ as follows

$$H|\phi\rangle = H(a|0\rangle + b|1\rangle) = \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle . \tag{2.42}$$

The *α-phase shift* gate S_α is defined as a transformation $|x\rangle \to e^{ix\alpha}|x\rangle$ where $x \in \{0,1\}$. If one applies S_α on $|\phi\rangle = a|0\rangle + b|1\rangle$ then

$$S_\alpha|\phi\rangle = S_\alpha(a|0\rangle + b|1\rangle) = a|0\rangle + e^{i\alpha}b|1\rangle . \tag{2.43}$$

In [2], it is shown that all the one-qubit gates and the controlled-NOT gate make a universal set for quantum computation. By definition, the controlled-NOT, or CNOT for short, gate flips the second (target) qubit if the first (control) qubit is $|1\rangle$ and does nothing if the control qubit is $|0\rangle$. More generally, one has the controlled-U gate that applies the unitary operation U on the second (target) qubit if the first (control) qubit is $|1\rangle$ and does nothing if the control qubit is $|0\rangle$. Fig. 2.3 shows the graphical representations of the CNOT and controlled-U and their transformation matrices.

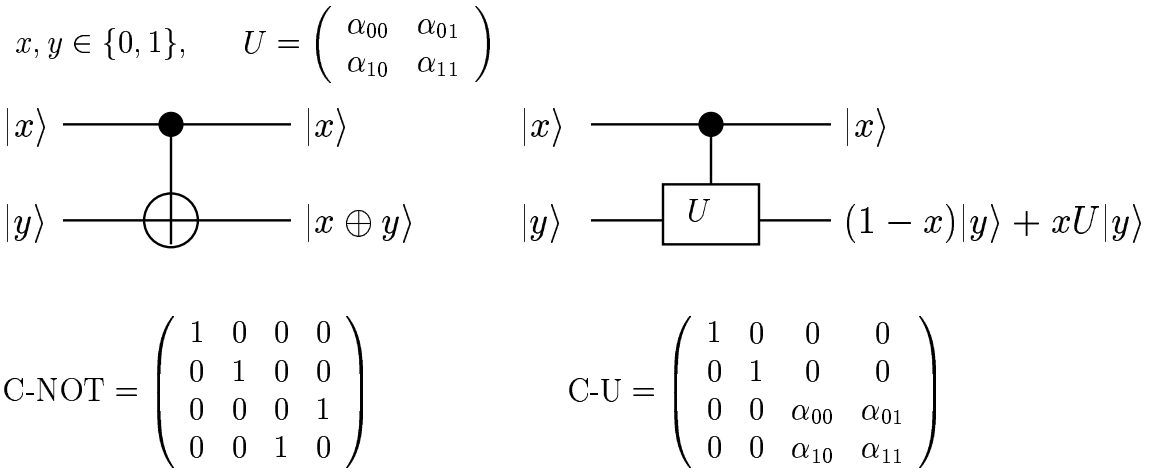


Figure 2.3: Controlled-NOT and Controlled-U gates.

2.4 Some prominent applications

2.4.1 Quantum computation

Consider a unitary transformation U which maps computational states to computational states as follows

$$U|i\rangle = |x_i\rangle \tag{2.44}$$

where $\{|i\rangle, i \in [0, 2^n - 1]\}$ is a computational basis and $x_i \in [0, 2^n - 1]$, $x_i = x_j$ iff $i = j$.

A quantum computation is roughly described by three stages. In the first stage, one prepares a system of n qubits in the initial state $|\phi_0\rangle = |i\rangle$. In the second stage, one applies U to $|\phi_0\rangle$. The initial state $|\phi_0\rangle$ will evolve to $|\phi_1\rangle = U|i\rangle = |x_i\rangle, x_i \in [0, 2^n - 1]$. In the final stage, one measures $|\phi_1\rangle$ by projecting each of n qubits onto the basis $\{|0\rangle, |1\rangle\}$. The measurement outcome x_i is the output of the computation. Hence, the final output is the classical information.

However, the initial state $|\phi_0\rangle$ of the n-qubit system can be prepared in a superposition of all the 2^n basis states, e.g. $|\phi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$. In such a case, the time-evolution of $|\phi_0\rangle$ that is represented by the unitary transformation $U|\phi_0\rangle$ exhibits an interference effect

of all the 2^n basis states in the same time, i.e.

$$|\phi_1\rangle = U|\phi_0\rangle = U(\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle) = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}U|i\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|x_i\rangle\,. \tag{2.45}$$

Eq. 2.45 shows that the evolution of the quantum mechanical system implies a potential parallelism paradigm. This can bring a superior computational power compared to the classical computation. However, if one measures the final state $|\phi_1\rangle$ of Eq. 2.45 in the basis $\{|i\rangle\}, i \in [0, 2^n - 1]$ then one gets only one out-of 2^n values $x_i, i = 0, \ldots, 2^n - 1$ with equal probabilities. In other words, one obtains different outputs while repeating the same computation process. This seems make no sense and gain nothing. Indeed, quantum computations are *probabilistic*. Quantum algorithms naturally generate a probability distribution of the possible outcomes. One needs appropriate quantum algorithms in order to gain quantum parallelism in specific problems, for example, the balanced black-box problem [27, 31], the search problem [49], or the number-factoring problem [85, 87].

2.4.2 Quantum communication

The beautiful idea of building a secret key exchange channel based on the no-cloning theorem of quantum mechanics was proposed by C. Bennett and G. Brassard in 1984 [8]. Although such a secret key exchange channel, largely well-known by the name *Quantum Key Distribution*, has some serious practical problems such as low transmission rate, limited range, etc., it presents a tremendous advantage since it guarantees the communicated secrets by quantum laws. This is, at least in principle, impossible to achieve in the classical information communication. We will see more about Quantum Key Distribution and its limit over range in the next chapters.

Super-dense coding is another example that illustrates interesting features of quantum information communication compared to ist classical counterpart. Suppose that Alice wants to send some classical information to Bob by transmitting quantum states. Super-dense coding allows Alice to send two classical bits by transmitting just only one qubit provided that Alice and Bob previously share a quantum entangled state [14].

In the opposite direction, suppose Alice wants to send an unknown quantum state to Bob by transmitting some classical information. *Teleportation* technique allows Alice to send one unknown quantum state (one qubit) to Bob by transmitting two classical bits provided that Alice and Bob previously share a quantum entangled state [9].

Chapter 3

Quantum Key Distribution

3.1 Key distribution problem

Unbreakable encryption scheme were invented by G. Vernam in 1917, now well-known under the name "one-time pad" scheme. The principle is to combine the plain-text with a random key or so-called a pad that is at least as long as the plain-text and just used once. Notice that it is important that the key is never re-used in order to ensure unbreakability. This is why it is called "one-time" pad. The one-time pad presents a serious drawback: two communication parties, conventionally called Alice and Bob, must pre-possess a random secret key as long as the message before actually communicating the message. Indeed, the presence of the one-time pad scheme leads to a transformation from the problem of secure communication to the problem of secure key distribution, or so-called of secret key agreement.

Most applications transport secret keys over the Internet using Public Key Infrastructure (PKI), more precisely, based on the Diffie-Hellman key agreement. They rely on assumptions about the limited computation power of eavesdroppers and the non-existence of effective algorithms for certain mathematical "hard" problems. These assumptions are critical, for instance, in 1994 Peter Shor [85,87] introduced an efficient quantum algorithm for the factoring problem that is considered as a "hard" problem in the conventional cryptography. Indeed, Public Key Infrastructure (PKI)-based key exchanges cannot provide information theoretic security, or so-called unconditional security.

In recent years, QKD emerges and draws attention of cryptographic community by the fact that this technique, by exploiting special properties of quantum mechanics, can provide unconditional security of the key transmission [8,38,88]. However, it has its own drawbacks,

most prominently throughput and range [42, 56]. The limitations of QKD makes it harder the construction of large QKD-based networks that enable the perfect distribution of secret key between network's participants.

3.2 BB84 protocol

Quantum Key Distribution allows two endpoints to agree a shared key with total confidentiality that can be afterward used for symmetric secret-key encryption algorithms. S. Wiesner described the idea in the 70's and officially published it in 1983 [95]. Wiesner's idea has been fully developed and finalized by Brassard and Bennett in 1984, therefore, it is well-known by the name the BB84 protocol [8].

BB84 Basics

The quantum law underlying QKD is *Heisenberg principle of uncertainty*: two non-commuting observables of a quantum system cannot be both accurately measured. It ensures that it is impossible to clone a quantum system as stated the no-cloning theorem [96, 35]. Otherwise, it would be possible to measure one observable on the original and the other observable on the clone.

The BB84 protocol is simple enough to be understood by a non-specialist of quantum physics. The idea can be roughly described as follows. Photons can have a *rectangular* or a *diagonal* polarization, two non-commutable observables. Rectangular polarization can be horizontal denoted by "$\rightarrow$" or vertical denoted by "$\uparrow$". Diagonal polarization can be left denoted by "$\nwarrow$" or right denoted by "$\nearrow$". Given a photon, the physical device can observe its polarization either rectangular or diagonal but not both. Moreover, if the physical device tries to measure the diagonal polarization over a photon that is rectangular-polarized, then a random outcome is made: either left or right with equals probabilities. And the measurement action changes the polarization of the photon corresponding with the outcome of the measurement. The situation is symmetric if the physical device measures the rectangular polarization of a photon that is diagonally polarized.

Session keys are made of bits, $\{0, 1\}^n$. One agrees that: a bit 0 can be encoded either by a horizontal ("$\rightarrow$") or a left ("$\nwarrow$") polarization of a photon and a bit 1 can be encoded either by a vertical ("$\uparrow$") or a right ("$\nearrow$") polarization of a photon. Such a polarized photon is considered as a *quantum bit* or *qubit*. Transmitting a key becomes transmitting a sequence of polarized photons.

Idealized BB84 Key Exchange

Alice and Bob are connected by using two channels. The first one is a quantum channel, typically an optical fiber. The second one is a classical channel, typically an Internet link, a telephone line, etc.

1. First, Alice generates a random sequence of bits, called the raw key. Randomness is crucial. For each bit, Alice randomly encodes it into a photon by using either rectangular or diagonal bases. And then, she sends the sequence of encoded photons to Bob over the quantum channel.

2. For each receiving photon, Bob randomly chooses either the rectangular or the diagonal bases to measure the polarization of the photon. Since Alice and Bob's choices of bases are random, the probability that they use the same basis on a given photon is 50%. If they use the same basis on a given photon, then Bob gets the right bit as Alice encoded. Otherwise, Bob gets a random bit.

3. Bob uses the classical channel to communicate to Alice which bases he used for the measurements. Alice, also by using the classical channel, answers which bases are correct according to her encoding bases, i.e. on which photons they used the same bases. They discard the photons on which their bases are different. This communication is public.

4. Once they used the same bases, the bits encoded by Alice are identical to the bits decoded by Bob. They get a shared sequence of bits, called a sifted key, that can be used to build a session key. The length of the sifted key is about half the length of the raw key.

Example. In table below, the rectangular and circular bases are denoted by $\oplus$ and $\otimes$. The 1^{st} line ARK contains Alice's randomly chosen sequence of bits. The 2^{nd} line ARB contains the encoding bases randomly chosen by Alice for each bit and the 3^{rd} line AQB contains the qubits, i.e. the polarized photons. The 4^{th} line BRB contains Bob's randomly chosen measurement bases and the 5^{th} line BQB contains the results of the measurements. We have put a symbol "?" to mention that Bob's measurement has a random result which will be discarded anyway.

The last line BSK contains the bits for which Alice and Bob have chosen the same basis, this is the sifted key which value is "00100100111" in our example.

ARK	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1	1	0	1
ARB	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
AQB	$\rightarrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	$\nearrow$	$\uparrow$	$\uparrow$	$\rightarrow$	$\uparrow$
BRB	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
BQB	$\rightarrow$	?	?	$\rightarrow$	?	?	$\nearrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	$\nwarrow$	$\nwarrow$	$\uparrow$	?	$\uparrow$	?	?	$\uparrow$
BSK	0			0			1	0	0	1	0	0	1		1			1

Eavesdroppers and Security

The eavesdropper, conventionally named Eve, has the access right to both channels. If Eve accesses a photon, she has no way to know the basis used by Alice to encode the bit. Thus, she has to guess a basis for measuring the photon. Then Eve resends the photon to Bob. This is the intercept-resend strategy. If Eve chooses the same basis as that of Alice for measurement, then Eve gets the right value and the photon's polarization is not changed. If Eve chooses the wrong basis then she destroys the initial polarization of the photon and afterward even if Bob chooses the right basis, Bob gets an incorrect bit with probability of 50%. On the average, Eve chooses the wrong bases for 50% of the cases. Thus, Eve's action introduces a supplementary error rate, about 25%. In such a case, Alice and Bob can detect the intrusion and know that the sifted key cannot be trusted.

Another strategy of Eve is the *man-in-the-middle* attack. In this attack, Eve gets control over the two channel and lets Alice thinks that she is communicating with Bob and conversely. Eve plays the role of Bob with respect to (w.r.t.) Alice and plays the role of Alice w.r.t. Bob. In such a case, one must rely on authentication algorithms stemmed from classical cryptography or recent quantum authentication algorithms.

Many papers give a rather complete description of the non-impossible quantum attack strategies, for instance, the beam splitting scheme, the entanglement scheme, the quantum copying scheme, or the collective attacks, in various configurations and to various QKD technologies, and why all of them cannot succeed. Formal proofs of security rely on protocols such as the following BB84. They uses Shannon's Information Theory and, most important, the laws of Quantum Physics.

Practical BB84 Protocol

The idealized BB84 protocol described above did not take into account losses and noises that are inevitable in any practical realizations. Hence, it will not work because Alice and

Bob always detect additional disturbances due to noises and losses, and they must to discard the transaction even if there are no eavesdropping actions.

On the other hand, single photon sources so far are not yet available in practice. Indeed, one uses altered single-photon sources, for instance, attenuated laser pulses that follow a Poissonian distribution in the number of photon, i.e. the probability of having n photon in a signal is given by $P_\mu(n) = \frac{e^{-\mu}\mu^n}{n}$ where μ, chosen by the sender Alice, is the average number of photons. For instance, if Alice chooses $\mu = 0.1$ then most of the pulses contain no photons, some contain single photon and a fraction of order 0.005 signals contains several photons. Notice that multi-photon signals can make it possible the photon-number-splitting (PNS) attack. The PNS attack can be roughly described as follows. Eve measures the number of photons on each signal sent by Alice. In principle, this measurement does not disturb the signal polarization, in other words, does not add any more disturbances into the signal. Thus, Eve can treat each signal differently according to its photon number. For vacuum signals, Eve does nothing and re-sends them to Bob. For multi-photon signals, Eve extracts one photon to keep it in her memory without disturbing other photons of the signal. Then, Eve re-sends the extracted signal to Bob by a lossless quantum channel. Hence, the extracted photon effectively pretends the loss on the original lossy quantum channel. The extraction of Eve does not affect the polarization of the initial signal. Later in the QKD protocol Alice announces the polarization basis of this signal. Knowing the polarization basis allows Eve to measure correctly the extracted photon to obtain the encoded information without any supplementary disturbances. For single-photon signals, since Eve uses a lossless quantum channel to re-send signals to Bob, Eve may suppress a proportion of single photons to pretend the effects of the original noisy and lossy channel. Obviously, limiting the presence of multi-photon signals is crucial in order to ensure the security of practical QKD. However, in practice multi-photon signals cannot be totally eliminated as well as the case of unavoidable noises and losses in the quantum channel. Indeed, Eve can get a little information of the raw key as well as Alice and Bob always can find some finite amount of disturbance in the intrusion-check phase. Hence, in order to work in the practical realization, the idealized BB84 protocol as described above needs to be added the following step.

1. *Sifting.* Alice sends a random string of bits, the raw key, as described above. Alice and Bob must be synchronized to detect photons that Alice did not send but Bob received and, conversely, photons that Alice sent but Bob did not receive. Then, they discard the photons that are not used the same bases for encoding and decoding. The result is the sifted key. The length of the *sifted key* is about a few percents of the length of the raw key.

2. *Bit reconciliation.* The sifted key is made of qubits on which Alice and Bob agree because they have used the same encoding basis. However, some bits may differ because the quantum apparatus is not reliable or because there has been a light intrusion of Eve which will not been recognized as so. The error elimination algorithm uses the public classical channel. Several algorithms have been proposed. For instance, it has been proposed that Alice and Bob use the same random permutation of bits to randomize the locations of errors. Then, the key is divided into small enough equalized-size blocks such that each block is unlikely to contain more than one error. Alice and Bob compare the parities of their respective blocks and discard blocks for which parities differ. After reconciliation, the sifted key has been often shortened but it is almost certainly shared between Alice and Bob.

3. *Eavesdropper detection.* At this step, Alice and Bob may detect Eve's intrusion because a significant intrusion must raise the usual error rate.

4. *Privacy amplification.* Eve may know some bits of the key from the previous steps. Privacy amplification is a technique reducing Eve's information. The cost is once again shortening the key. Again, several algorithms are available. For instance, Alice randomly chooses two bits and tells Bob the position of these bits. Alice and Bob replaces the two bits by the result of their XOR. If Eve has only partial information on these two bits, i.e. if she knows only one bit, then she has no information on the XOR result. Therefore, Eve's information becomes less than before. Alice and Bob may repeat this step to reduce Eve's knowledge down to a negligible amount.

5. *Authentication.* The two parties identify themselves. This may totally rely on classical algorithms such as Wegman-Carter's authentication scheme [93]. This algorithm assumes that a piece of information, an authentication key, is shared previously between Alice and Bob. Thus, Alice and Bob afterward can use an Universal Hash Function to create/verify the message-dependent tag. In fact, Alice and Bob may share a stack of authentication keys. This is subject to keys exhaustion by *Denial of Service* (DoS) attack where the eavesdropper simulates a lot of connections.

Then Alice and Bob share a key with a very high probability and Eve's information about the key is as small as wished. There are a number of successful implementations of the BB84 protocol in practice [5, 6, 7]. In [33], D. Gottesman *et al.* gave a security proof that takes into account all the practical imperfections. They showed that for low and intermediate losses one can ignore the effect of errors and the secret key rate R can be expressed in terms of the proportion of the multi-photon signals in the source p_m and the

rate of the received signals observed by receiver Bob p_r:

$$R \sim p_r - p_m \tag{3.1}$$

Once a Poissonian photon number distribution with mean photon number μ is used, one has

$$p_m = 1 - (1 + \mu)e^{-\mu} \tag{3.2}$$

and

$$p_r = 1 - \mu\eta e^{-\mu\eta} \tag{3.3}$$

where η is the photon transmissivity coefficient in a standard optical transmission.

Optimizing R over μ one has $\mu_{opt} \sim \eta$ and $R \sim \eta^2$. On the other hand, due to the photon detector imperfections, the effective distance of QKD is believed around 20 to 40 km.

3.3 Enhanced QKD schemes

The **decoy state QKD** [92, 68, 98] is the first and simplest enhanced version of QKD. The idea is to use additional decay states instead of decreasing the average photon number μ to defeat the photon-number-splitting (PNS) attack. As described above, in the PNS attack, Eve can make photon-number depending actions on each signal. Remark that Eve may suppress a proportion of single-photon signals to simulate the loss effect in the original lossy quantum channel. Remark also that if Alice sends either of two types of quantum states: signal states which have the average photon number μ_0, or decoy states which have various mean photon numbers $\mu_1, \mu_2, \ldots$, then Eve has no idea where comes from a given single-photon signal. Thus, the suppression of single-photon signals may lead to an abnormal transmission rate of multi-photon signals of the higher value μ_i compared to the lower value μ_j. By choosing appropriate values for $\mu_0, \mu_1, \ldots$, one can detect the PNS attack without decreasing dramatically the average photon number μ_0 of the signal state sources. Indeed, the decoy state QKD can improve the average photon number of signal states up to $\mu_0 \sim 1$. Remind us that the original QKD without decoy states require $\mu \ll 1$ in order to reduce the number of multi-photon signals, or in other words, to deal with the photon-number-splitting attack. [46] showed that improvements were roughly depicted as Fig. 3.1. Indeed, the decoy state QKD allows a higher key transmission rate $R = O(\eta)$, compared to $R = O(\eta^2)$ of the non-decoy QKD schemes. The decoy states QKD also can be implemented for longer effective distance.

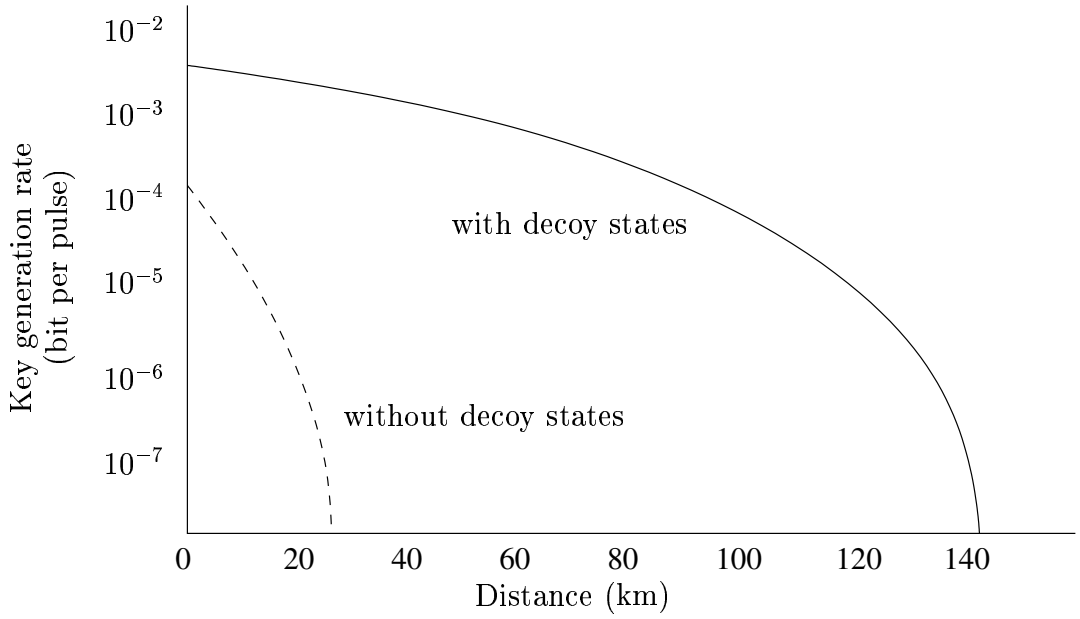


Figure 3.1: Distances and key rates in [46] using the results in [33] with and without decoy states.

The **QKD with strong reference pulses** [74] is another approach that is based on the strong phase-reference pulses idea. The idea is as follows. Besides a phase modulated weak signal pulse Alice sends a strong unmodulated reference pulse to Bob. On one hand, quantum information is encoded in the relative phase between the signal pulse and the strong reference pulse. On the other hand, Bob monitors the intensity of the strong reference pulses to detect Eve's single-photon signal suppressions in the PNS attack. As a result, Alice can send signal pulses of average photon number $\mu = O(1)$ and achieve the key transmission rate $R = O(\eta)$.

The third enhanced QKD version is the **differential phase shift (DPS) QKD** [55, 34, 79]. One encodes information into the relative phase between the consecutive pulses. Obviously, the PNS attack on each pulse is useless since information is encoded by two consecutive pulses. On the other hand, the PNS attack on two consecutive pulses will break the phase coherence between adjacent pulses and must induce additional perturbances. At present, a rigorous of the unconditional security of this approach is still missing.

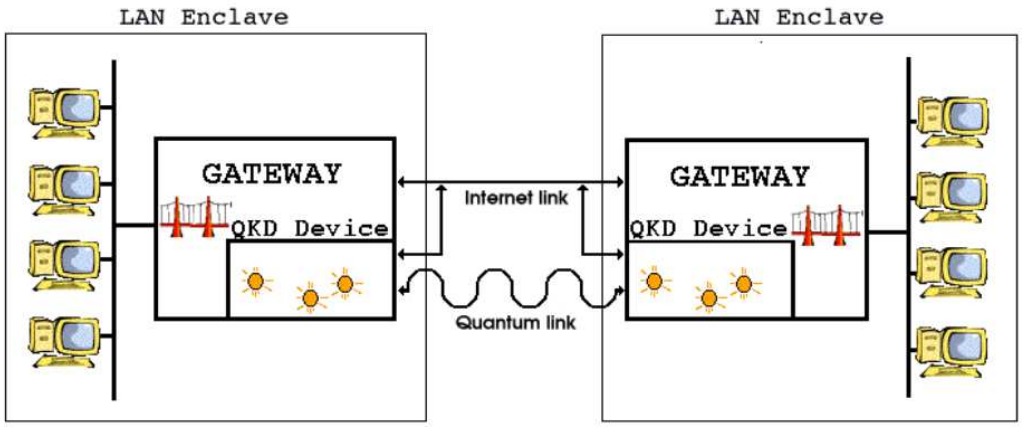


Figure 3.2: A single QKD Link

3.4 Current applications

A single QKD Link. The simpler network consists of a QKD link between two enclaves that marries QKD with classical Internet security protocol IPSec (see Fig. 3.2). QKD is used for key sharing between two enclave gateways.

The enclave, a *Local Area Network (LAN)*, is assumed to be already secured. An IPSec secured Internet link connects the two gateways. IPSec is a well-established Internet technology that allows traffic between two endpoints to be confidential provided the endpoints share an encryption key. The two gateways ensure the routing of IP communication. The only non-classical feature is that the keys necessary to IPSec are distributed using quantum technology. The two QKD devices produce continuous streams of bits, which can be used for regular key renewing.

A long QKD Link. Simple QKD links as above are limited to several tens of kilometers length. In order to extend the length, one may use QKD data relay (see Fig. 3.3). One must note that a QKD data relay is not a quantum repeater. A QKD data relay is a network apparatus able to establish a single QKD link with the previous element of the chain and another QKD link with the following element of the chain. It is a data relay with the following characteristics:

- Relay k establishes an encrypted communication, a QKD link, with relay k-1.
- Relay k receives encrypted data from relay k-1.
- Data are decrypted and stored in the memory of relay k.

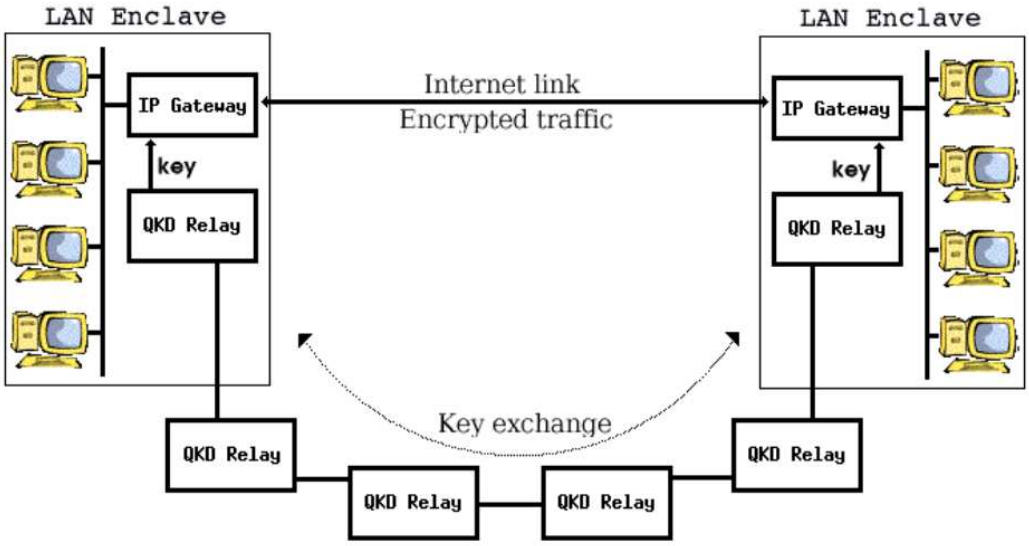


Figure 3.3: A QKD link using relays

- Relay k establishes an encrypted communication, a QKD link, with relay k+1.
- Data in memory are encoded and sent to relay k+1.

We can see that QKD data relays present a serious weakness: data appear unencrypted inside the relay memory. QKD data relays establish pair-wise secure communications using QKD in order to securely transport a randomly generated encryption key, hop-by-hop from one endpoint to the other as in figure below. The QKD relays network at the bottom of the figure is used to exchange an encryption key that used to encrypt the communication on the top Internet link.

Communication between QKD relays is done as the communication between LAN enclaves of section above. The encryption key that is exchanged using the QKD Relays Network appears unencrypted inside the relays. Thus, the relays must be seriously protected against eavesdropper. In Europe, due to the concentration of cities, such a scheme could be used by many institutions. This may not be applicable to larger countries such as USA, Canada or Russia where extended non-urban areas exist.

Chapter 4

Quantum Key Distribution Networking

From the point of view of security, QKD is a perfect tool to agree the session keys for two users at short distances. However, a stand-alone QKD link is subject to damage for some trivial reasons such as an accidental physical link failure or DoS attacks. Networking individual QKD links brings more attractive features since it introduces more physical ways between two end-users. For instance, QKD networks will allow us to think of improving the general traffic or replacing failed links by the other ones to ensure the quality of service for some specific end-to-end communications. In the conventional networks, networks devices as hubs, routers, etc., plays an important role. One of essential tasks of these network devices is to relay or repeat the signals that encode information. Notice that although repeaters and relay schemes for QKD have been yet proposed and feasible in theory but with today's quantum technology one cannot implement them in practice. Without these network devices, building the QKD network is a big challenge!

At present, the most practical solution to build the QKD network is networking the QKD individual links. In principle, one can focus only on the security aspect and do not take into consideration the cost aspect. Thus, this is acceptable if one assumes that all the participant network sites are *perfectly* protected by human security means, e.g. the military force. In such a case, one calls the *trusted* QKD network in which one can use long QKD links as described in the previous chapter in order to convey secret keys between two arbitrarily long sites. The perfect security of key transmission will be kept provided that intermediate nodes are perfectly protected. Currently, there are two such QKD networks: DARPA and SECOQC.

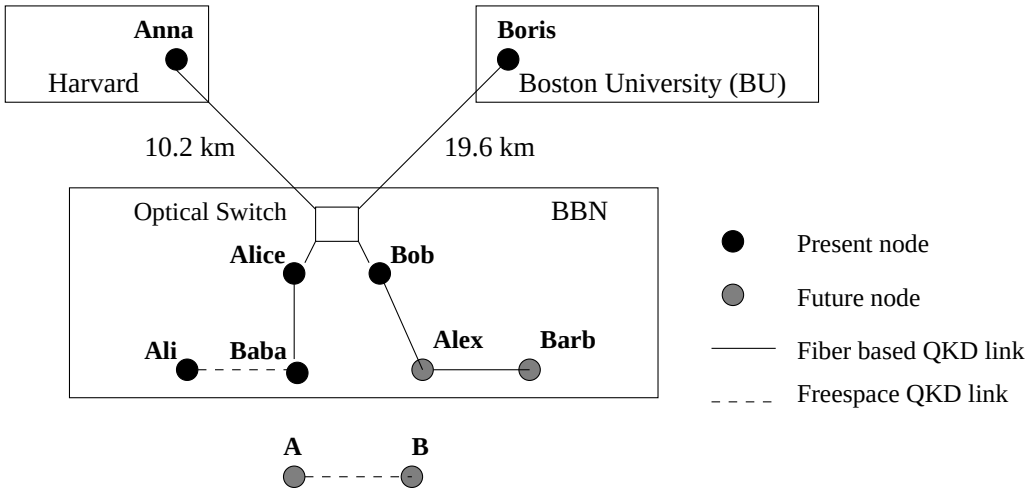


Figure 4.1: The DARPA quantum network topology. Alex and Bob are entanglement based nodes but not yet fully operational. A and B are two free-space nodes which have not yet been named [41].

4.1 DARPA quantum network

The DARPA quantum network is the first QKD network that became fully operational in October 2003 in BBN's laboratories, and in June 2004 was fielded through optical standard telecommunication fiber underneath the streets of Cambridge, Massachusetts, to link three sites: Harvard University, Boston University and BBN technology [40, 41]. In December 2004, the DARPA quantum network consists of six trusted QKD nodes. It is planned to build up to ten trusted QKD nodes connected by non-stop, twenty four hours per day QKD links, with a variety of QKD implementation technologies including phase-modulated laser through fiber, entanglement through fiber and free-space QKD (see Fig. 4.1).

The DARPA quantum network network uses the photonic switch to route encoded photons of the BB84 protocol. No signal amplification is made by the photonic switch. Indeed, such a photonic switch significantly reduce the geographic reach of QKD because it causes additional losses and noises along the photonic path. Fortunately, since all the nodes are trusted each node can play the role of QKD key relaying devices and make it possible to obtain a longer reach of QKD. In principle, the trusted architecture allows any two DARPA quantum network nodes establishing their shared secret keys without reducing the security of original QKD schemes. However, such a key is not a real end-to-end secret since necessary information needed to deduce the key is unavoidably appeared in all the relaying nodes'

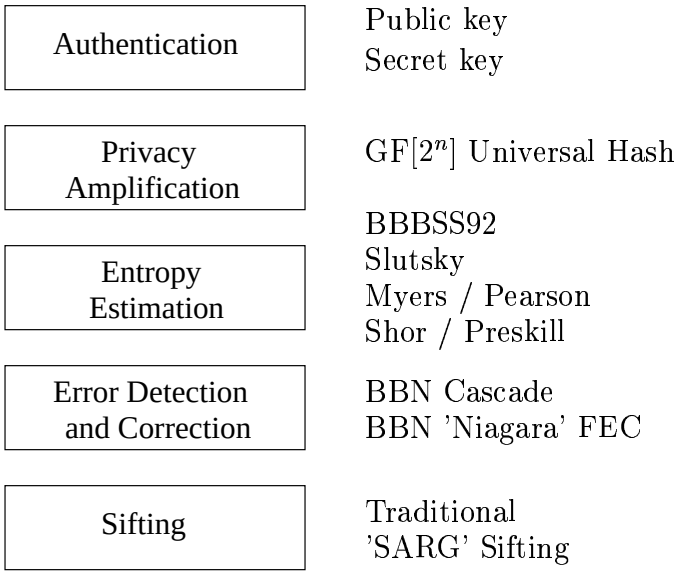


Figure 4.2: The architecture of the DARPA-QKD protocol software [41].

memories. Only one of the relaying nodes is compromised, the key will be compromised. One realizes that instead of exposing eavesdropping vulnerabilities on the entire length of the key transmission path, the DARPA quantum network makes vulnerabilities gathered at the relaying nodes. The security of key depends on the security of the relaying nodes along the transmission path.

Implementing QKD's protocols is an important part. Fig. 4.2 illustrates the DARPA-QKD software architecture in a high-level form. One can realize that the DARPA-QKD software aims at implementing every main algorithms for QKD rather than trying to pick the best ones. A simple configuration will be done afterward in order to indicate which algorithms are taken for a given operation on a given specific QKD system.

Remind us that the **Sifting** step is for Alice and Bob to reconcile their raw secret bits. Indeed, this step discards a proportion of the initial (raw) secret bit string to obtain the sifted key. Discarded bits are the bits at the positions where Alice and Bob used different bases, or there is no symbol clicked (photon detector does not fired), or there are multiple symbols clicked, etc. The DARPA-QKD network offers two sifting algorithms: classical and SARG04 [81]. In the classical sifting procedure,for each position Alice and Bob publicly announce the basis choice and Eve is permitted to listen to and know it. In the SARG04 sifting procedure introduced by V. Scarani *et al.* in 2004 the basis choice is not revealed. Instead, two possibilities are announced in which only one is compatible with the idealized

detection event. The advantage of the SARG04 sifting is reducing the knowledge of Eve about the encoding bases.

The **Error Detection and Correction** step is for eliminating the bits damaged in transmission, i.e. the flipped bits sent as 1 but received as 0 and vice-versa. Thus, one can estimate an important quantity called Quantum Bit Error Rate (QBER). Notice that after eliminating the damaged bits there is always some possibility that Alice and Bob do not share an identical bit string but they believe that they do. In fact, the error detection and correction process is only probabilistic unless all the bits are revealed. Besides, since this process requires a classical communication between Alice and Bob, in principle, Eve can get some more information about the sifted bits by eavesdropping.

The DARPA-QKD network offers two error detection and correction implementations: BBN Cascade and BBN Niagara. BBN Cascade is a modified version of Brassard and Salvail's Cascade [20]. BBN Niagara [77] is a novel type of Low-Density Parity Check (LDPC) code designed for the use in QKD applications. It is a type of Forward Error Correction codes that are mostly based on parity checks. BBN Niagara does not require multiple protocol interactions between Alice and Bob as does BBN Cascade.

The **Entropy Estimation** step aims at estimating the amount of entropy in the sifted and corrected bit string beyond what Eve may know. The DARPA-QKD network implemented four different entropy estimation techniques that were introduced by Bennett *et al.* [15], Slutsky *et al.* [89], Mayers *et al.* [75] and Shor-Preskill [41]. The choice of entropy estimation function is important because the estimated entropy quantity will be given as a key-control input parameter to the privacy amplification step. An incorrect entropy estimation may lead to an insufficient privacy amplification. As a result, the security of the final secret bits may be compromised.

The **Privacy Amplification** step is for reducing Eve's knowledge of the remaining shared bits up to a given arbitrarily small amount. This step uses a classical algorithm to shorten the remaining shared bit string across a shorter one. By that, Eve's knowledge can be reduced up to an arbitrarily small amount [10]. The DARPA-QKD network nodes perform privacy amplification by using a linear hash function over the Galois Field $GF[2^n]$.

The **Authentication** step is for Alice and Bob to ensure that they communicate with each other, not with Eve. The DARPA-QKD network uses the Wegman-Carter authentication scheme [93]. This requires Alice and Bob sharing beforehand a small secret key and afterward uses an Universal Hash Function to create/verify the message-dependent tag. Indeed, the DARPA-QKD network currently employs the standardized authentication mechanisms of the Internet security architecture (IPsec) and those provided by the Internet

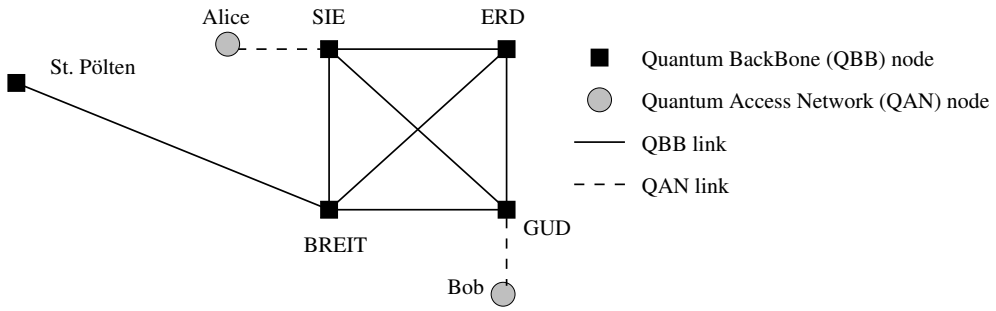


Figure 4.3: The topology of the SECOQC QKD's network.

Exchange Key (IKE) protocol. These mechanisms allow messages to be authenticated by public keys of the nodes or by pre-placed secret keys.

4.2 SECOQC quantum network

The SECOQC project is an European Union project that aims at the development of a global network for *SE*cure *CO*mmunication based on *Q*uantum *C*ryptography. The project was launched in 2004 and has obtained significant results [78].

In September 2008, the SECOQC QKD network had a successful demonstration in Vienna. This was a QKD network of five Quantum BackBone (QBB) nodes with sept Quantum BackBone (QBB) links (see Fig. 4.3). At present, the average distance of QBB link is around 25 km that is believed to be optimal with respect to the network building overall cost. Particularly, the QBB link to St. Pöelten city is of 85 km. Similar to the DARPA quantum network, the SECOQC network was developed based on the "trusted node" assumption. All the QBB nodes are assumed to be trusted by human means, e.g. the military forces. QBB nodes are connected together by QBB links that consist of a bunch of individual QKD links. QBB nodes can act as routers in the conventional communication network, as well as be used as the QKD network access entry for end-users such as Alice and Bob. End-users can also access to the SECOQC QKD network by a Quantum Access Network (QAN) node that does not support routing functionality but is more specialized to be an access point of many end-users. A new QAN node can be easily add into the SECOQC QKD network by using a QAN link that might be featured differently compared to a QBB link, e.g. a QAN connection can be a single QKD link. It is implicitly known that the QAN link is of lower cost and weaker performance than those of the QBB link, but this is not compelled [78]. One can realize that the SECOQC network architecture seems

to be hierarchical. This differs from the flat architecture of the DAPRA QKD network. In fact, although both are based on the crucial assumption of trusted nodes the SECOQC network is distinguished from the DARPA network in the point of view of architecture, management, strategy of generating, storing and using QKD keys. In other words, one can say that the two current QKD networks are similar in the basic level (based on the same crucial assumption), but they differ from each other in the engineering level.

Indeed, the SECOQC network introduces a new layer called "network of secrets". This layer is dedicated to the storing, forwarding and managing the secret key materials generated by QKD devices. Referred to the OSI 7-layer model the *network of secrets* layer is under the Network layer and from the Network layer all the upper layers (Transport, Session, etc.) are considered as to be independent of the quantum key generation process. In other words, the SECOQC network tries to make a view separately between the collection of QKD links and the classical network design and management. As a result, in the SECOQC network one can improve the global performance and reliability by exploiting path redundancy, designing new special-purpose routing algorithms, applying traffic engineering, etc. The network of secrets is based on the implementation of the *backbone QKD network* that consists of QBB nodes and QBB links. The topology of the backbone QKD network is proposed to be meshed that exhibits a high connectivity and redundancy. Such a meshed topology is expected to make available of multiple disjoint paths between any two network nodes. This property opens many possibilities to improve the global network performance. For instance, one can think of improving security of the final session key by applying a XOR operation over all the secret pieces send by a number of disjoint paths. The task of QBB links is to grow as much key material as possible for the network of secrets, no matter which end-user will request it afterwards.

Although allowing to include a variety of different QKD devices, the SECOQC network defines a common protocol designed to access services provided by the devices: the Quantum-Point-to-Point Protocol, or for shortness Q3P. This protocol serves as a point-to-point protocol between a pair of QBB nodes which enables the QKD devices underneath to carry out the classical tasks as key distillation, authentication, encryption for the upper layers of the network. By using the Q3P protocol as an uniform manner to interconnect a pair of QKD devices, one can now re-use traditional network protocols on the upper layers. However, since TCP/IP protocols are not compatible with the specific requirements for controlling QKD key traffic over network, one proposed new layered QKD network protocols as described in Fig. 4.4. The QKD Routing Layer (QKD-RL) protocol addresses the routing mechanism within the QBB nodes. This protocol follows the pattern of the Open Shortest Path First (OSPF) protocol but includes essential modifications to support the

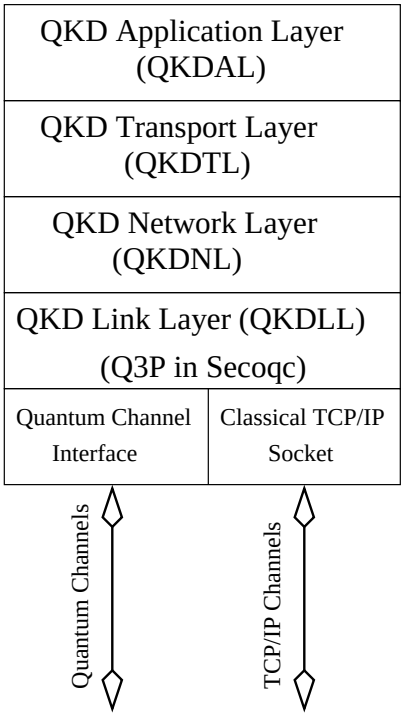


Figure 4.4: The layered protocol stack of the SECOQC QKD's network.

specific requirements arising from the sensitivity of the key material circulation. The QKD Transport Layer (QKD-TL) protocols adopts TCP/IP, however, introduces new approaches to deal with a high network congestion based on current key material resources. This protocol allows end-users to exchange information across the network with perfect confidentiality and authenticity based on a basic end-to-end pair [78].

4.3 Satellite free-space based quantum network

A QKD system consists of one transmitter (e.g. photon source), one receiver (e.g. photon detector) and one quantum channel. Fiber-based links is one of two solutions for quantum channel. The another is free-space links. Most of researches so far use optical fibers to guide the photons from Alice to Bob. Current fiber-based QKD systems are very advanced, however, such systems still cannot work over distance more than 150 km [56] due to the combination of fiber losses and detector noise. Besides, fiber-based links may not always be available due to some other reasons. Hence, there are more and more attentions focusing on free-space QKD links, where the photons are sent between remote telescopes.

Transmitting photons by free-space links has some advantages compared to that of fiber-based links. First of all, the atmosphere has a high transmission window at a wavelength of around 800 nm, where photons can easily be detected using commercial, high-efficiency photon detector. Furthermore, the atmosphere is weakly dispersive and essentially isotropic at these wavelengths. As a result, it will not alter the polarization state of a photon. There are some drawbacks of free-space links as well. In contrast to the signal transmitted in a optical fiber (guiding medium) where the energy is protected and remains localized in a small space, the energy transmitted via a free-space link spreads out, leading to higher and varying transmission losses. The background light such as ambient daylight or even moonlight at night can couple into the receiver, leading to dark-count errors. Besides, it is clear that the performance of the free-space QKDsystem depends dramatically on atmospheric conditions.

Photon sources and photon counters are the most important components of the QKD system. Optical quantum cryptography is based on the use of single-photon Fock states. Unfortunately, these states are difficult to realize experimentally. Nowadays, practical implementations rely on faint laser pulses or entangled photon pairs, in which both the photon and the photon-pair number distribution obey Poisson statistics. For large losses in the quantum channel, even small fractions of these multi-photons can have important consequences on the security of the key, leading to interest in "photon guns". As for the photon counter, in principle, this can be achieved using a variety of techniques, for instance, photon-multipliers, avalanche photo-diodes, multi-channel plates, and super-conducting Josephson junctions [45]. Today, the best choice of wavelength for free-space QKD systems is of 800 nm for which efficient *avalanche photo-diodes* (APD) counters are commercially available. In addition, the receiver uses a combination of spectral filtering, spatial filtering and timing discrimination using coincidence window of typically a few nanoseconds to decrease the dark-count errors. Free-space transmission is restricted to line-of-sight links. Thus, the beam-pointing is still difficult for moving targets. However, the theoretical estimation allows us to think of free-space communications up to 1600 km, suitable for satellite-based key exchange.

The very first demonstration of free-space QC system was a table-top experiment performed at the IBM Thomas J.Watson Research Center in 1989 over a distance of 32 cm [15]. After this, there are some others significant free-space experiments:

- 1998: Hughes *et al.*, Los Alamos : $\sim$1 km, night [22]
- 2000: Hughes *et al.*, Los Alamos : 1.6 km, daylight [23]

- 2001: Rarity *et al.*, QinetiQ : 1.9 km, night [47]
- 2002: Hughes *et al.*, Los Alamos : over 10 km [54]
- 2003: Kurtsiefer *et al.*: 23.4 km, night [58]

The result achieved of Kurtsiefer's QKD system is significant. Such a system using slightly bigger telescopes, optimized filters and anti-reflection coasting, combined with sophisticated automatic pointing and tracking hardware, could be stable up to 34dB of loss, the limitation of loss acceptable for the QKD system, and capable of maximum ranges exceeding 1600km. On the other hand, while this may not seem like much, a free-space QKD transmission between two ground-based locations 2km apart is equivalent to from a ground-based location to an orbiting satellite at 300km altitude. Hence, one can think of key transmissions between ground-based stations and low earth orbit satellites. Furthermore, one can also think of a satellite network that cover the whole wide world, in which each satellite can act as a secure "relay" station. This implies a potential of the global world-wide satellite-based QKD key distribution which is our ultimate goal.

4.4 Remarks

Both current QKD networks, the DARPA and SECOQC quantum networks, are based on the common essential assumption: all the participant nodes are trusted. Such an assumption is critical and seems not suitable to build a world-wide general-purpose QKD network. Indeed, the DARPA and SECOQC networks are currently limited in a small size of some nodes and capable of covering an area of several-tens of square kilometers. They are only understood as the metropolitan area networks (MANs). It seems that one has to wait for the new progress and new emergence in the development of QKD technologies in order to build the bigger QKD networks. One can realize that the two current QKD networks are only capable of approving the feasibility and of improving a little the performance of stand-alone QKD links. The crucial constraint on the reach of the original QKD schemes has not been yet broken out. The initial problem has not been yet thoroughly solved. Indeed, the question is always open.

The satellite-based QKD network is interesting. Each satellite acts as a trusted QKD relay. By its high altitude, such a relay is impossible to be eavesdropped and can cover a larger area. Indeed, a global world-wide satellite network such as the Global Positioning System (GPS) can consist of only 24 well-spaced satellites that orbit the Earth and make

possible for people with ground receivers to pinpoint their geographic location. The location accuracy of the GPS system is anywhere from 100 to 10 meters for most equipment. Accuracy can be pinpointed to within one meter with special military-approved equipment. Hence, the use of satellites to distribute photons seems a good choice for long-distance quantum communication networks. However, the cost of satellite-based experiments is very expensive. It needs to consider seriously before setting up such an experimental prototype.

In the next chapters, we will try to find new approaches that can help to build the bigger quantum network that is not based on the advantage of satellites. We will develop the solutions in two ways. The first one is to use additional engineering techniques to extend the current QKD networks, the DARPA and SECOQC quantum networks, becoming a world-wide quantum network. The second one is to seek for new relaying methods that can act as the conventional network relay/repeater devices without reducing the unconditional security of the original QKD schemes.

Part II

Towards the World-Wide Quantum Network

Chapter 5

Modeling the World-Wide Quantum Network

Chapter 5 begins for Part II of this Dissertation. As seen in the previous chapters, QKD networks are of much interest due to their capacity of providing extremely high security keys to network participants. However, two current QKD networks are based on trusted model where all the network nodes are assumed to be perfectly secured. This restricts QKD networks to be the small networks capable of several nodes. In this chapter, we propose a novel model dedicated to large-scale QKD networks. We consider a new assumption that is more suitable to large-scale QKD networks: nodes could be eavesdropped. Moreover, the nodes under eavesdropping operations are unknown and unknowable to the others. In the next chapters, Chapters 6 and 7, we will investigate the key transmission problem in the proposed model by an approach based on percolation theory and stochastic routing. Analysis shows that under computable conditions, large-scale QKD networks could protect secret keys with an extremely high probability. Simulations validate our results. In the last chapter of Part II, Chapter 8, we will provide a discussion about the application scenarios of the proposed world-wide quantum network. The material of Part II of this Dissertation primarily concerns with our publications [64, 63, 65].

5.1 Preliminary

The problem of transmitting a secret key from an origin to a destination over the network was considered for a long time, but cannot be thoroughly solved. The current solution in most of Internet applications is using Public Key Infrastructure (PKI). PKI relies on plau-

sible but unproven assumptions about the computation power of eavesdroppers and the non-existence of effective algorithms for some mathematical hard problems. As a result, PKI cannot meet the highest security level, also called *unconditional security*. Quantum Key Distribution (QKD) technology is a prominent alternative. It was proven that QKD can provide unconditional security [71, 66, 25]. It is also successfully implemented in some realistic applications [42, 41, ?, 79]. However, QKD only supports point-to-point connections and intrinsically causes serious limits on throughput and range [42, 56]. A long-distance QKD transmission must take an adequate number of intermediate nodes to relay the key. In realistic scenarios, however, some intermediate nodes could be controlled by eavesdroppers without the knowledge of the others. In consequence, the security of key will be compromised. For the large-scale context, moreover, the vulnerability of relay-based transmissions is more sharpened. The open question is: how to build large-scale QKD networks that are capable of enabling extremely high secret key for network participants?

In QKD networks, we can distinguish two types of links: the classical link and the QKD link. A classical link is easy and simple to be implemented, capable of providing high-speed but low-confidentiality communications. By contrast, a QKD link aims at the highest level of security, also called *unconditional security*. This causes its undesirable limitations over rate and range [42,56]. Conventionally, QKD networks are largely known as the special ones to which the primary goal is unconditional security. Indeed, QKD networks rather sustain QKD link's restrictions in order to support the security goal. Hence, there is no need to consider classical links in the design of the QKD network prototype. This implies that we can consider only QKD links in our works of Part II. We will simply write links instead of QKD links in Chapters 5, 6, 7 and 8.

Data can be perfectly secured on links connecting two adjacent nodes since the unconditional security of QKD was well proven [71, 66, 25]. The risk of data disclosure is with the case in which the origin (Alice) and the destination (Bob) are not connected by a direct link. Data must be relayed through some intermediate nodes to arrive its destination. The critical question is whether the intermediate nodes are vulnerable to the malicious person (Eve)? The feasibly-implemented model of QKD networks so far is the trusted network model. The two famous quantum networks, named SECOQC and DARPA, were planned to follow such a model [40, 41, 78].There, all the network nodes are assumed to be perfectly secured. This implies that we did not take into account the fact that Eve can ingeniously eavesdrop a proportion of networks nodes without leaving any trace. In the large-scale context, since the number of network participants is great such Eve's attacks become more realistic. Consequently, the security maybe compromised in practice. Our goal is to release the "trusted" constraint, and solve the secret key transmission problem over untrusted

network model.

Choosing an adequate topology is an important step in building a network. Restricted by a modest length of link, QKD networks have not many choices of topology. It is believed that a meshed topology would suit to QKD networks. Besides, the distributed architecture is believed to be good to improve the security. In Part II of this Dissertation, we follow such an idea of topology and architecture. However, we dedicate to design a global world-wide quantum network that is distinguished from the existing works, e.g. the DARPA and SECOQC networks. We will seek for conditions on that we can get unconditional security for key transmissions, and also solve the routing problem of secret keys in such a network. For simplicity, we focus on the 4-connected grid network. Fig. 5.1 roughly describes our proposed QKD network. Nodes are represented by squares. Links have no representation because they are perfectly secured and they have no effect on security analysis. Network connectivity is characterized by connections from one node to four adjacent neighbors.

Keeping confidentiality and secrecy on transmissions is a part of network security. There is a zero-sum game between two players: legitimate users and eavesdroppers. The former wants to protect as much as possible their exchanged data while the latter wants to gain as much as possible this data without revealing their presence. In QKD networks, we have not to worry about links. Thanks to the advantage of QKD technology! However, nodes are still vulnerable. Attacks are roughly divided into two categories: detectable or undetectable. In principle, if we can detect an attack then we can find out effective solutions to fix it. One of the simplest solutions is isolating contaminated components to keep the security of the remain components. Undetectable attacks are very dangerous. We cannot detect them until a terrible damage has been done. We must take into account such attacks in large-scale QKD networks. We assume that each node sustains a probability p_e with that the node is eavesdropped without knowledge of legitimate users. Imagine that legitimate users always try to detect attacks and unusual operations to repair them. This implies that p_e should be small unless eavesdropper resources are much more important than that owned by legitimate users. For simplicity, we focus on the context in which the probability p_e is the same for all the nodes. We will first investigate the decay of confidentiality caused by relaying nodes with respect to a given p_e. Then, we propose a solution that enhances confidentiality. We also seek conditions and means to achieve the unconditional security in QKD networks.

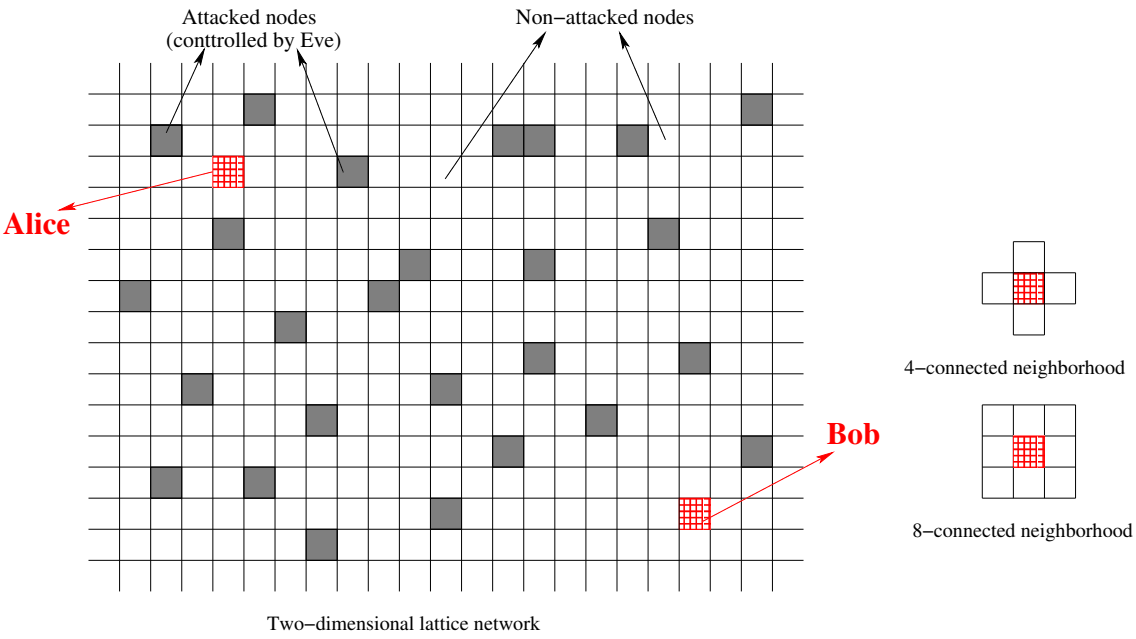


Figure 5.1: Two dimensional lattice network.

5.2 Modeling the World-Wide Quantum Network Problem

Consider a 4-connected grid lattice network (see Fig. 5.1). The network is large so that we can ignore its borders. Nodes are represented by squares. Each node is linked with its four nearest neighbors. We do not make representation of links since they have no effect on our security analysis. If we turn into the language of graph theory, then our network can be described as follows. The network is the set of vertices $V = Z^2$. Each vertex $v = (v_1, v_2)$ is the representation of one node being at its corresponding coordinates. A vertex is called as *safe* if there is no eavesdropping operation on it. Otherwise, it is called *unsafe*. By the fact that vertices can be eavesdropped without leaving any trace, we assume that all the vertices sustain a constant eavesdropping probability $p_e \in [0, 1]$. As mentioned above, we assume that all the vertices sustain the same eavesdropping probability p_e. Denote by p_s the probability that a vertex is safe, $p_s = 1 - p_e$.

Alice and Bob are two legitimate users, represented by two corresponding vertices v_A, v_B. Alice wants to convey a secret key K to Bob. The central object of study is the secrecy probability Σ that K is not revealed to the eavesdropper Eve. If v_A, v_B are adjacent then K is certainly safe, or $\Sigma = 1$. Otherwise, K must pass over some intermediate vertices $v_1, v_2, \ldots, v_l (l \geq 1)$ whose task is to relay K. In this case, K is revealed unless all the l

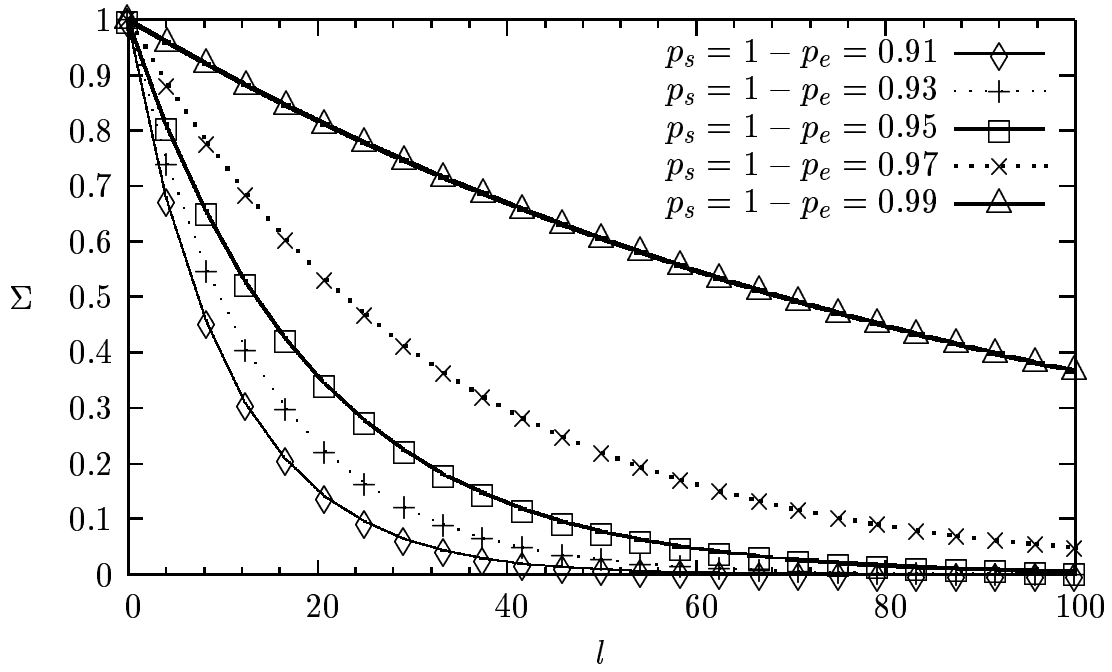


Figure 5.2: The secrecy probability Σ is dramatically attenuated with respect to (w.r.t) the number of relaying nodes l.

vertices $v_1, v_2, \ldots, v_l$ are not eavesdropped. We can measure Σ by the following formula:

$$\begin{aligned}
\Sigma &= Pr(\text{key in secrecy}) \\
&= Pr(v_1, v_2, \ldots, v_l \text{ are not eavesdropped}) \\
&= \prod_{i=1}^{l} Pr(v_i \text{ is safe}) \\
&= (1 - p_e)^l \\
&= (p_s)^l
\end{aligned} \tag{5.1}$$

If we focus on the probability of key disclosure:

$$\begin{aligned}
\overline{\Sigma} &= Pr(\text{key disclosure}) = 1 - \Sigma \\
&= 1 - (1 - p_e)^l \\
&= 1 - (p_s)^l
\end{aligned} \tag{5.2}$$

A sequence $\pi = v_A, v_1, v_2, \ldots, v_l, v_B$ is known as a path from v_A to v_B. Two succes-

sive vertices of the path are adjacent. We define the length of a path as the number of intermediate vertices in this path. For instance, the length of $\pi = v_A, v_1, v_2, \ldots, v_l, v_B$ is l.

We call *safe path* the one that has no vertex being intercepted by Eve. Otherwise, the path is called *unsafe path*. Fig. 5.2 shows that the secrecy quantity Σ of K is exponentially decreased with respect to (w.r.t) the length l. The advantage of QKD links is vanished just by some relaying nodes. We are interested in a simple way that possibly compensates the decay of Σ. This is to send a number of sub-keys $K_1, K_2, \ldots, K_N$ by different paths $\pi_1, \pi_2, \ldots, \pi_N$. The final key K is now computed by a bitwise XOR operation over $K_1, K_2, \ldots, K_N$. As such, K should be safe unless Eve intercepts all the paths $\pi_1, \pi_2, \ldots, \pi_N$. Assume that the graph presents somewhere safe paths from v_A to v_B. With a more bigger N, we can hope that the final key K has a more chance to be safe. The following questions are basic:

1. When all safe vertices are almost-certainly connected? In the mathematical expression, find the condition for p_s such that for any $\Delta \in [0, 1]$ we have:

$$\Sigma_\infty = \lim_{N \to \infty} (\Sigma) \geq 1 - \Delta$$

2. Assume that $\Sigma_\infty \geq 1 - \Delta$. Given a pair of vertices v_A, v_B, consider a finite number N of paths $\pi_1, \pi_2, \ldots, \pi_N$ from v_A to v_B generated by a proposed routing algorithm. Let $\lambda(N)$ be the secrecy probability of the final key if N sub-keys are sent by $\pi_1, \pi_2, \ldots, \pi_N$. Find N_0 such that for any $\epsilon \geq \Delta$, $\epsilon \in [0, 1]$, we have:

$$\forall N \geq N_0 : \lambda(N) \geq 1 - \epsilon$$

Chapter 6

Necessary Condition for Unconditional Security

6.1 Percolation theory based approach

First, we talk about percolation theory [48,52,53,1,3]. This theory investigates the transition phase from the non-existence to the existence of the giant wetted cluster when we supply water at the center of a graph. The 2-dimensional site percolation model can be roughly described as follows. Given the graph G with vertices set V and edges set E. Vertices and edges are either open or closed. In the open status, they allow water to pass through and water make them become wetted. Otherwise, they do not permit the passage of water. Edges are open. Vertices are not similar. Each vertex is open only with *open probability* $p_o \in [0,1]$. Let $\theta(p)$ be the *percolation probability* that measures the proportion of wetted vertices to open vertices. It is believed that θ has the form as roughly sketched in Fig. 6.1.

If G is infinite then θ implies the probability that exists an infinite wetted cluster. It turns out that θ follows Kolmogorov's one-zero law,

$$\theta(p_o) = \begin{cases} 1, & \text{if } p_o > p_c \\ 0, & \text{if } p_o \leq p_c. \end{cases} \tag{6.1}$$

Where p_c is called the critical probability that stands for the minimum value of p_o that holds $\theta(p_o) > 0$.

The framework of the 2-dimensional site percolation is very similar to that of our network model. It is not difficult to realize that the open probability p_o and the safe probability

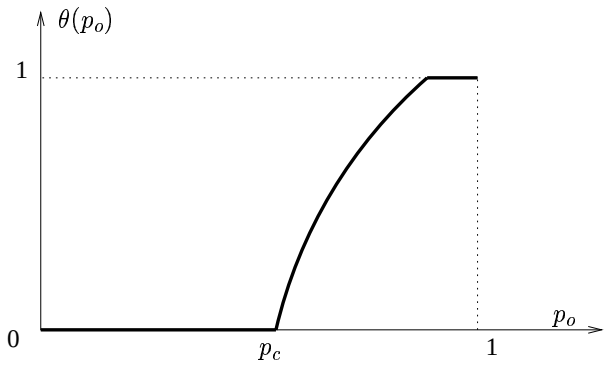


Figure 6.1: The percolation probability $\theta(p_o)$.

p_s play an equivalent role in two corresponding frameworks. If we always set $p_s = p_o$ and assume that Alice sends an infinite set of sub-keys $K_1, K_2, \ldots$ by an infinite set of different paths $\pi_1, \pi_2, \ldots$. Then, the secrecy quantity Σ of the final key K is identical to the probability that there exists a safe path between the origin v_A and the destination v_B. This probability is, however, equivalent to the probability θ that almost open vertices belong to the same infinite open cluster. We can use for Σ two important properties that have been proven in percolation [53]:

1. The percolation probability θ is a non-decreasing and continuous function w.r.t p_o, except possibly at the threshold p_c, where it is at least non-decreasing and continuous from the right (see Fig. 6.1).

2. The number of infinite open cluster k_0 is either 0 or 1, i.e.

$$k_0 = \begin{cases} 1, & \text{if } \theta > 0 \\ 0, & \text{if } \theta = 0. \end{cases} \tag{6.2}$$

The fundamental goal of quantum networks is to achieve the most highest security. Situations that lead to a small probability of having safe paths should be taken out of interest. Our network problem can be realized as a variant of percolation theory that presents its own challenges. Indeed, although of having the equivalence between Σ_∞ and θ, the intervals of interest over these functions are explicitly distinguished. The interest interval over θ is concerned with the transition point p_c where θ varies from 0 to the values greater than 0. As for Σ_∞, the interval of interest is close to 1. This formulates the first basic question stated in the end of Chapter 5. Besides, we must deal with another challenge. This is the routing problem that was stated as the second question at the end of Chapter 5.

Our network is large but not infinite. Let take a simple estimation about is possible size. Earth's surface is $510,065,600$ square kilometers. The optimal length of QKD links is so far believed to be around of 40 kilometers [78].Thus, the network size is approximately of 600×600. Consequently, the function $\Sigma_\infty(p_s)$ cannot follow Kolmogorov's one-zero law. This implies that the critical probability p_c of the 2-dimensional site percolation cannot be the good response for the critical value of p_s in our context. We must find the appropriate critical value for p_s.

6.2 Condition on the safety probability p_s

We investigate the secrecy probability Σ when Alice sends to Bob an infinite number of sub-keys $K_1, K_2, .., K_\infty$ by infinite corresponding paths $\pi_1, \pi_2, .., \pi_\infty$. This turns out the problem of the connectivity of safe vertices on the graph. Indeed, two vertices v_A and v_B (two vertices represent for Alice and Bob) are considered as safely connected together if there exists at least a safe path inside the infinite set of paths from v_A to v_B. In the percolation literature, $\Sigma_\infty(v_A, v_B)$ can be interpreted as the connectivity function $\tau(v_A, v_B)$. If Alice is far enough from Bob then we can use the following approximation [48],

$$\Sigma_\infty(v_A, v_B) = \tau(v_A, v_B) \sim \theta^2. \tag{6.3}$$

Unfortunately, the percolation theory did not give any estimate for θ in the region where θ is close to 1. In our context, we must study the interval of p_s such that the safe connectivity between two any Alice and Bob is almost certain. That is to say if given a non-negative small value Δ, we must show the interval $[p_{lc}, p_{uc}]$ such that $\forall p_s : p_{lc} \leq p_s \leq p_{uc}$, we have $\Sigma_\infty \geq 1 - \Delta$. Obviously, the upper critical bound p_{uc} is 1. Seeking for the lower critical bound p_{lc} is not easy. Our method is based on a heuristic and we use simulations to validate the results.

As is well-known, the critical probability for the 2-dimensional lattice percolation is about 0.6. From this value to 1, the percolation probability θ is greater than zero and increases continuously to 1. Let ξ be the probability that a given safe vertex is encircled by unsafe vertices. The relation between θ and ξ holds: $\theta = 1 - \xi$. Therefore, from Approximation 6.3 we can easily derive the condition on ξ w.r.t a given Δ as follows

$$\xi \leq 1 - \sqrt{1 - \Delta}. \tag{6.4}$$

Our task now is to investigate the behavior of ξ in the region close to 0. From the trivial case in which a given vertex is encircled by its four unsafe neighbor vertices, we have immediately the lower bound of ξ,

$$\xi \geq (1 - p_s)^4. \tag{6.5}$$

The equality holds if and only if $p_s = 1$. The directly subsequent corollary is $\xi = 0$ in this case. Otherwise, even though p_s is very close to 1, the probability ξ always is a non-negative value. If we set $p_s = 0.8$, then by applying Ineq. 6.5 we have $\xi > 1.6 \times 10^{-3}$. We temporarily set $p_{lc} = 0.8$ to continue an incremental study of ξ.

We first try to solve the problem of ξ in the one-dimensional case. To distinguish ξ in the one-dimensional and two-dimensional cases, we denote by $\xi^{(1)}$ and by $\xi^{(2)}$, respectively. We can easily measure $\xi^{(1)}$ for a given radius r (see Fig. 6.2),

$$\begin{aligned}
\xi^{(1)} &= Pr(\text{Both the left and right consist of unsafe vertices}) \\
&= \Big(Pr(\text{At least one unsafe vertex in the left})\Big) \times \\
&\quad \Big(Pr(\text{At least one unsafe vertex in the right})\Big) \\
&= \Big(1 - Pr(\text{All vertices in the left are safe})\Big) \times \\
&\quad \Big(1 - Pr(\text{All vertices in the right are safe})\Big) \\
&= (1 - p_s^r) \times (1 - p_s^r) \\
&= (1 - p_s^r)^2.
\end{aligned} \tag{6.6}$$

We now try to extend from $\xi^{(1)}$ to $\xi^{(2)}$. In the two-dimensional lattice, assume that we are focusing on a vertex O. Let $R(r)$ be the set of vertices that have the distance r from O. We are interested in unsafe circuits inside $R(r)$. Denote by:

- $G(r)$: the event that there is an unsafe circuit that encircles the considered vertex O and do not exceed $R(r)$ (see Fig. 6.2.C).
- $G_{LR}(r)$: the event that is an unsafe vertex in both the left and the right of the vertex O that do not exceed the length r (see Fig. 6.2.B).
- $G_{UD(r)}$: the event that is an unsafe vertex in both the left and the right of the vertex O that do not exceed the length r (see Fig. 6.2.B).

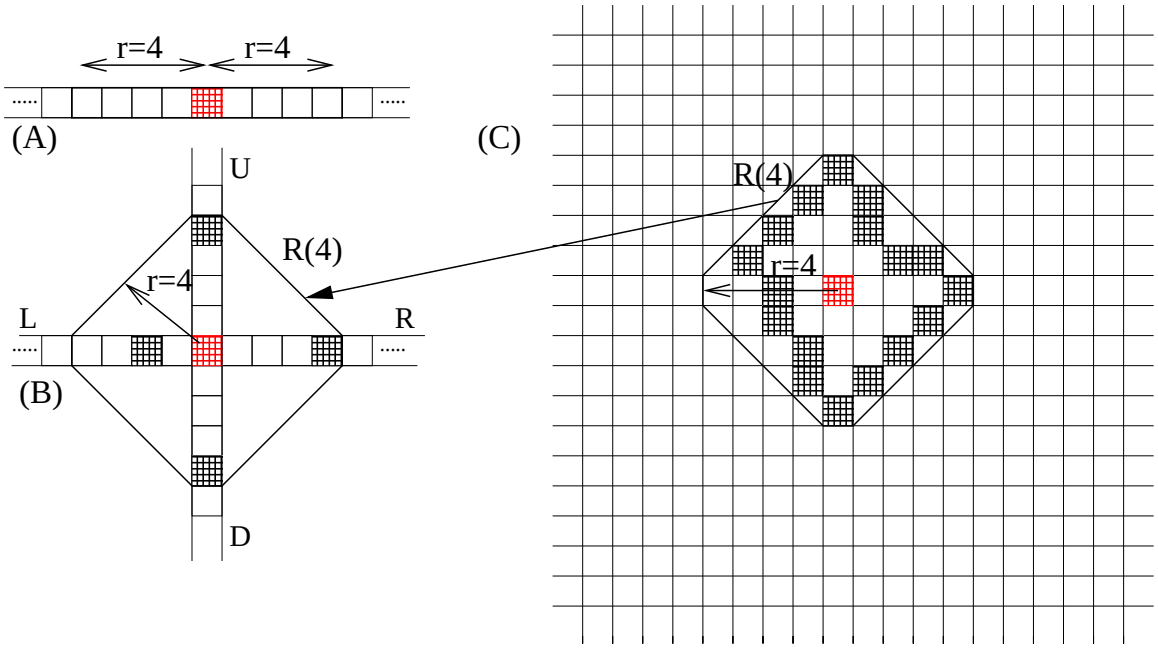


Figure 6.2: Unsafe circuits in the one-dimensional and two-dimensional cases.

Obviously, if we have the event $G(r)$ then we have two events $G_{LR}(r)$ and $G_{UD}(r)$, too. Thus,

$$Pr\Big(G(r)\Big) \leq Pr\Big(G_{LR}(r)\Big) \times Pr\Big(G_{UD}(r)\Big) \tag{6.7}$$

or

$$\xi(r) = \xi^{(2)}(r) \leq \Big(\xi^{(1)}(r)\Big)^2. \tag{6.8}$$

Applying Eq. 6.6 to Ineq. 6.8, we have:

$$\xi(r) \leq (1 - p_s^r)^4. \tag{6.9}$$

In the trivial case $r = 1$, the equality is always true. Otherwise, more r is bigger, more Ineq. 6.9 is looser. The reason is when r is bigger, besides of the condition on G_{LR} and G_{UD} hold, the event G needs more unsafe vertices to complete a circuit and to make itself appeared.

Based on $G(r)$ we define the event $G(r1, r2)$ is a event that there is no unsafe circuit inside the inferior $R(r_1)$ but there is an unsafe circuit inside the exterior $R(r_2)$. Let $\xi(r_1, r_2)$

be the probability that the event $G(r_1, r_2)$ appears. We have

$$\xi(r_1, r_2) = \xi(r_2) - \xi(r_1) \tag{6.10}$$

or:

$$\xi(r_2) = \xi(r_1, r_2) + \xi(r_1). \tag{6.11}$$

Let r_2 tend to infinity, we have

$$\xi = \xi(\infty) = \xi(r_1) + \xi(r_1, \infty). \tag{6.12}$$

Without loss of generality, we set $r_1 = r$ in Eq. 6.12. The upper bound of ξ could be estimated by applying Ineq. 6.9 to Eq. 6.12)

$$\xi = \xi(\infty) \leq (1 - p_s^r)^4 + \xi(r, \infty). \tag{6.13}$$

Note that if a circuit belongs to the set $G(r, \infty)$ then its length must be equal or greater than $2r$. As such, the minimum degree of p_e in the function $\xi(r, \infty)$ is $2r$. This implies that $\xi(r, \infty)$ is in the order of p_e^{2r}, or $\xi(r, \infty) = O\Big(p_e^{2r}\Big) = O\Big((1 - p_s)^{2r}\Big)$. In the other hand, we consider the limit of the ratio between ξ and the quantity $(1 - p_s)^{2r}$ as $r \to \infty$. From Ineq. 6.5, we have

$$\lim_{r \to \infty} \Big(\frac{\xi}{(1 - p_s)^{2r}}\Big) \geq \lim_{r \to \infty} \Big(\frac{(1 - p_s)^4}{(1 - p_s)^{2r}}\Big) = \infty. \tag{6.14}$$

This is to say $\xi >> (1 - p_s)^{2r} \sim \xi(r, \infty)$, or $\xi >> \xi(r, \infty)$ as $r \to \infty$. Fig. 6.3 roughly shows the ratio between two quantities $(1 - p_s)^4$ and $(1 - p_s)^{2r}$ with some values of p_s in $[0.8 : 1]$. We realize that in order to get an enough great ratio about 10^8, we can choose $r_1 = 8$ for the interval $p_s \in [0.8 : 0.9]$ and $r_2 = 6$ for the interval $p_s \in [0.9 : 1]$. By these choices of r, we ignore the quantity $\xi(r, \infty)$ in the formula of the upper bound of ξ. We derive from Ineq. 6.13 to the following approximation:

$$\xi \leq \begin{cases} (1 - p_s^8)^4, & \text{if } 0.8 \leq p_s < 0.9 \\ (1 - p_s^6)^4, & \text{if } 0.9 \leq p_s \leq 1. \end{cases} \tag{6.15}$$

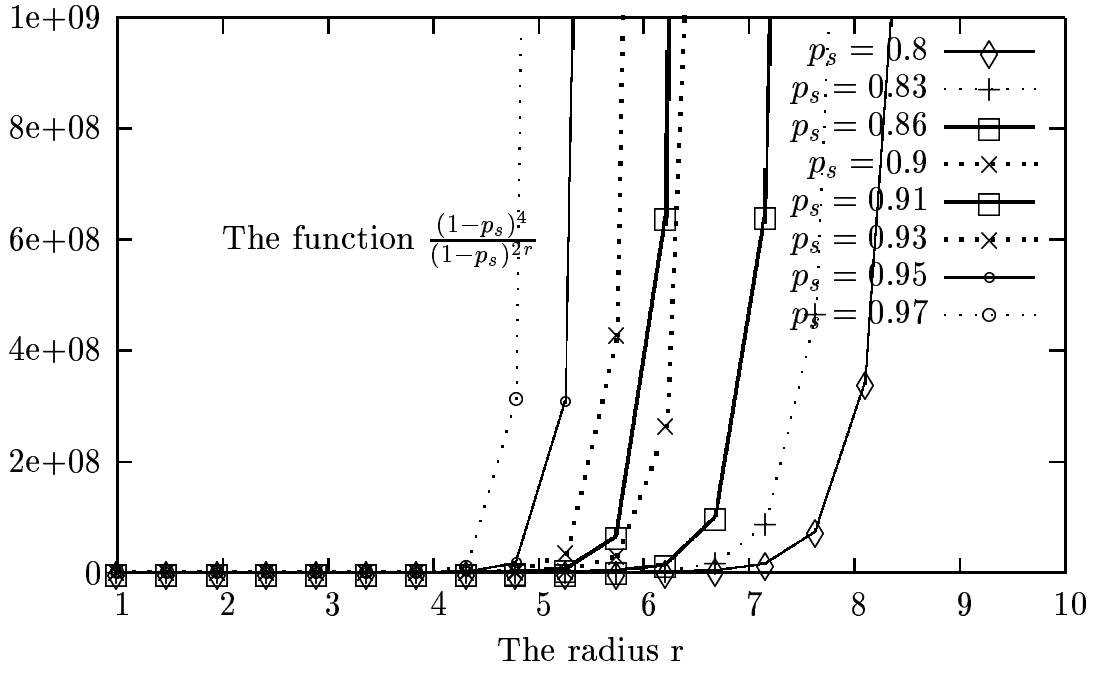


Figure 6.3: The ratio between $(1-p_s)^4$ and $(1-p_s)^{2r}$

6.3 Simulation results

We implemented simulations to examine our heuristic results. We investigated the two-dimensional lattice 600×600 that suits to the "size" of the whole wide-world quantum network. For each experiment, we generated randomly the untrusted network with a given value of p_s. Then, we used the spreading algorithm to find the greatest connected safe cluster. We denote by:

- A: the set of all the safe vertices.
- $C_{\max}$: the greatest connected safe cluster.
- ξ_{si}: the probability that a safe vertex does not belong to the greatest cluster $C_{\max}$.

We can calculate ξ_{si} for each experiment by the following formula:

$$\xi_{si} = \frac{1 - \|C_{\max}\|}{\|A\|} \tag{6.16}$$

where:

p_s	ξ_{lb}	$E(\xi_{si})$	ξ_{ub}
0.8	1.6×10^{-3}	2.14×10^{-3}	4.79×10^{-1}
0.83	8.35×10^{-4}	1.03×10^{-3}	3.6×10^{-1}
0.86	3.84×10^{-4}	4.47×10^{-4}	2.4×10^{-1}
0.9	1×10^{-4}	1.12×10^{-4}	4.82×10^{-2}
0.93	2.4×10^{-5}	2.7×10^{-5}	1.55×10^{-2}
0.95	6.25×10^{-6}	7×10^{-6}	4.92×10^{-3}
0.97	8.1×10^{-7}	1×10^{-6}	7.78×10^{-4}

Table 6.1: The lower bound ξ_{lb}, the expected value of simulation $E(\xi_{si})$ and the upper bound ξ_{ub}.

- $\|A\|$: the cardinality of A, or the number of safe vertices belonging to A.
- $\|C_{\max}\|$: the cardinality of $C_{\max}$, or the number of safe vertices belonging to $C_{\max}$.

We executed $10,000$ experiments for each chosen value of p_s. Table 6.1 shows our theoretic values and the simulation results. We realize that as p_s increases the expected value (or the mean) of ξ_{si} gets closer to its lower bound, and both tends to 0. We can realize also that for $p_s \in [0.8 : 0.9]$ the upper bound of ξ is important in comparison with the eavesdropping probability $p_e = 1 - p_s$ at each vertex. In the other word, the probability that the final key is eavesdropped in its transmission is greater than that of the final key being eavesdropped at the transmitter. This is out of our interest. By contrast, in the interval $p_s \in [0.93 : 1]$ the upper probability of a vertex being encircled is approximate or less than the probability of this vertex itself being unsafe. This seems more interesting. Table 6.1 also suggests that we can use a very quick estimation $\xi \sim \xi_{lb} = (1 - p_s)^4$ in the interval $p_s \in [0.93 : 1]$.

Note that for $p_s = 0.96$, we have $\xi \sim 2.56 \times 10^{-6}$. With our envisaged quantum network that is in 600×600, the number of safe vertices that are encircled is about

$$N_{\text{bounded}} \sim N_{\text{total}} \times p_s \times \xi \sim 0.88. \tag{6.17}$$

The above calculation can be interpreted that the expected number of safe vertices that are encircled by unsafe circuits is less than 1. Therefore, we can roughly derive another more powerful statement about the safe connectivity in our network: in the interval $p_s \in [0.96 : 1]$, all the safe vertices are almost-certainty connected.

Chapter 7

Security Routing Algorithms

7.1 Deterministic and stochastic routings

Routing algorithms can be classified into two main categories:

1. Deterministic routing algorithm (DRA): the path used to send a given message between one given pair of nodes is determined before the transmission and is usually always the same.

2. Stochastic routing algorithm (SRA): the path used to send a given message is randomly chosen among possible paths between one given pair of nodes. There is no need to determine the path before the transmission. The path can be incrementally determined at each relaying node.

Traditional routing algorithms, such as those used on the Internet, are mostly deterministic. As they are tailored to be efficient, they are guessable. This is not good to our model.

By contrast, stochastic routing algorithms seem better. The basic idea of stochastic routings is sending randomly a packet to one of possible routes. This can be implemented by a distributed way as follows. When the message holder forwards the message, it randomly chooses one among its neighbors, not necessarily the most "efficient" one. This gives birth to the new concept called next-hop probability distribution. Roughly speaking, the choice of next-hop is random, but according to a given next-hop probability distribution. From the end-to-end point of view, this results in the fact that each message will take a random path to go from origin to destination.

The main challenge in stochastic routing is how to determine the best next-hop probabilities that could optimize the given specific goal. Previous works on stochastic routing [17, 51, 18, 19] focus on performance metrics (latency, throughput, acceptance rate, etc.) which are not of major importance to QKD networks. As is well known, the most highest priority of QKD networks is the security. In other words, we could temporarily ignore other performance metrics to concentrate on the security goal. Besides, a special grid 4-connected topology as proposed can be well matched with QKD networks, but also make the previous optimization on stochastic routing became useless. We need to build our own appropriate stochastic routing.

7.2 Some proposed routing algorithms

7.2.1 An adaptive drunkard's routing algorithm

In the classic drunkard's walk problem, the next-hop probability distribution is uniform. This means there is no unbiased directions. Here, we propose an adaptive drunkard's routing algorithm, named ADRA, that is biased. The idea is to give the more chance for the vertex that is more closer to the destination vertex. Assume that the vertex v_A wants to send a message to the vertex v_B. The algorithm can be informally described as follows. The vertex v_A computes the next-hop probability for each neighbor to forward the message. These next-hop probabilities are determined with respect to the coordinates correlations of neighbors and v_B. To ensure that the message can finally reach v_B, we give a higher probability to the vertex that is closer to v_B. Then the vertex v_A randomly chooses one of its neighbors to forward the message, but according to the probability distribution that has been computed. As that, some vertices are more likely to be selected, but nothing is sure. Anyone that subsequently receives the message would do the same thing and the chain of communication would continue to reach to v_B.

Candidate selection and probability assignment can vary. Here, we propose a simple way:

- All the neighbors of the message holder (the current vertex) are selected to be candidates.
- Assume that there are m candidates in the candidate list. Do:
    1. Sort candidates in decreasing order of the distance to Bob. After sorted, let d_i

be the distance from the candidate i to Bob. We have:

$$\forall i = 1, \ldots, m-1 : d_i \geq d_{i+1}$$

2. Compute $w_1, \ldots, w_m$:

$$w_i = \begin{cases} 1, & \text{if } i = 1 \\ w_{i-1}, & \text{if } i > 1 \wedge d_i = d_{i-1} \\ w_{i-1} + 1, & \text{if } i > 1 \wedge d_i > d_{i-1} \end{cases}$$

3. Compute the next-hop probabilities $\Pr(i)$:

$$\Pr(i) = \frac{w_i}{\sum_{i=1}^{m} w_i}$$

7.2.2 A constant-length stochastic routing algorithm (l-SRA)

The *length* of a path is the number of the vertex belonging the path. A vertex may be counted as many times as the path runs through the vertex.

The *distance* between two vertices is the length of the shortest path from the origin vertex to the destination vertex.

Our *constant-length stochastic routing algorithm*, called l-SRA(l) or sometimes l-SRA for short, is a stochastic routing algorithm that takes a value l as input and tries to transmit a message in a random path having the length l.

Obviously, if l is less than the distance d between Alice and Bob then l-SRA(l) returns no path. Also, note that in the 4-connected grid lattice the difference of the length and the distance must be an event value.

We are interested in the cases $l \geq d$ and there are some different paths $\pi_1, \ldots, \pi_m$ that hold $l_{(\pi_1)} = \ldots = l_{(\pi_m)} = l$. Therefore, for each message l-SRA will choose randomly a path π_i among $\pi_1, \ldots, \pi_m$ according to a probability distribution that holds two following conditions:

1. $\forall i, 1 \leq i \leq m$:

$$0 \leq Pr(l\text{-SRA(l) takes } \pi_i) \leq 1$$

2.

$$\sum_{i=1}^{m} Pr(l\text{-SRA(l) takes } \pi_i) = 1 \tag{7.1}$$

It is clear that if $m = 1$, l-SRA(l) becomes a deterministic routing algorithm: the unique path is always chosen. However, as for $m \geq 2$, the message will be transmitted by an unpredictable path. It is different from the routing algorithm ADRA, we can compute the probability that l-SRA(l) chooses successfully a safe path to send one message.

In the two previous chapters, we are familiar with the notation p_s used to denote the safe probability of a node in the network or a vertex in the graph. For convenience, from here we also use p to denote the safe probability with the same meaning.

Theorem 7.1. *The probability that l-SRA(l) chooses successfully a safe path to send one message depends only on the safe probability p and the length l, not on the distance d between Alice and Bob:*

$$Pr(1, p, d, l\text{-}SRA(l)) = p^l. \tag{7.2}$$

Proof.

$$\begin{aligned}
\Pr\left(1, p, d, l\text{-SRA(l)}\right) &= \sum_{i=1}^{k} \Big(\Pr\left(l\text{-SRA(l) takes } \pi_i\right) \times \Pr(\pi_i \text{ is safe}) \Big) \\
&= \sum_{i=1}^{k} \Big(\Pr\left(l\text{-SRA(l) takes } \pi_i\right) \times p^l \Big) \\
&= \Big(\sum_{i=1}^{k} \Pr\left(l\text{-SRA(l) takes } \pi_i\right) \Big) \times p^l \\
&= p^l \quad (\text{ from Eq. 7.1}).
\end{aligned}$$

□

7.2.3 A parameterized-length stochastic routing algorithm (k-SRA)

We propose another routing algorithm that takes the distance between the origin and the destination as an input parameter. We call the algorithm k-SRA(k) or sometimes k-SRA for short. This is built based on l-SRA. The idea is as follows. k-SRA(k) receives an input value $k \geq 2$, and then considers only the paths with lengths less than or equal to $k \times d$. Note that the difference between the length and the distance cannot be an odd number.

Therefore, the possible lengths are $d, (d+2), \ldots, (d+2\times\lfloor\frac{(k-1)\times d}{2}\rfloor)$. For each message, k-SRA(k) chooses randomly a value l among $d, (d+2), \ldots, (d+2\times\lfloor\frac{(k-1)\times d}{2}\rfloor)$ according to the uniform distribution, i.e.

$$\forall i, 0 \leq i \leq u :$$
$$Pr\Big((d+2\times i) \text{ is taken for } l\Big) = \frac{1}{(k+1)\times d}$$

where $u = \lfloor\frac{(k-1)\times d}{2}\rfloor$.

Once l was chosen, k-SRA uses l-SRA to send the message. This implies that the message will take a random path that has the length l.

Theorem 7.2. *The probability that k-SRA(k) chooses successfully a safe path to send one message depends on the safe probability p, the input parameter k, and also the distance d between Alice and Bob,*

$$\lambda = \Pr(1, p, d, k\text{-}SRA(k)) = \frac{p^d \times (1-p^{2\times(u+1)})}{(u+1)\times(1-p^2)}. \tag{7.3}$$

Proof.

$$\begin{aligned}
\lambda &= \Pr\big(1, p, d, k\text{-SRA(k)}\big) \\
&= \sum_{l=d,\ldots,d+2u} \Big(\Pr\big(k\text{-SRA(k) takes } l\big) \times \Pr\big(l\text{-SRA}(l) \text{ takes a safe path}\big)\Big) \\
&= \sum_{l=d,\ldots,d+2u} \left(\frac{1}{(u+1)} \times \Big(\Pr\big(1, p, d, l\text{-SRA(l)}\big)\Big)\right) \\
&= \frac{1}{(u+1)} \times \left(\sum_{l=d,\ldots,d+2u} \Big(\Pr\big(1, p, d, l\text{-SRA(l)}\big)\Big)\right) \\
&= \frac{1}{(u+1)} \times \Big(\sum_{l=d,\ldots,d+2u} p^{(l)}\Big) \\
&= \frac{p^d \times (1-p^{2(u+1)})}{(u+1)\times(1-p^2)}
\end{aligned}$$

□

7.3 Proposed routing algorithms in different attack strategies

We consider two attack strategies of Eve:

1. Dynamic attack: Frequently, Eve changes nodes being attacked. Roughly speaking, to catch one message, Eve re-chooses the set of nodes being attacked.
2. Static attack: Once Eve has chosen some nodes to attack, she keeps these nodes in eavesdropping for a long time. Roughly speaking, Eve keeps her choice of the nodes being attacked until all N messages have been sent.

Note that we cannot formulate rigorous mathematical results for the algorithm ADRA. We are only able to estimate the effect of this algorithm by statistics. This is a trivial but essential method in the random walk literature. The algorithm l-SRA is not a real routing solution. The goal of this algorithm is to execute the sub-task of the algorithm k-SRA. The algorithm k-SRA presents some rigorous bounds.

Theorem 7.3. *If Eve executes a dynamic attack, then the probability that there is at least one safe path in N routings of k-SRA(k) depends on N, the safe probability p, the input parameter k, and the distance d between Alice and Bob:*

$$\Pr(N, p, d, k\text{-}SRA(k)) = 1 - (1 - \lambda)^N \tag{7.4}$$

where λ is evaluated by Eq. 7.3.

Proof. It is a memoryless system. From Eq. 7.3),

$$\begin{aligned}\Pr(\text{All the N trials are failed}) &= \big(1 - \Pr(\text{A trial is successful})\big)^N \\ &= (1 - \lambda)^N.\end{aligned}$$

Hence,

$$\begin{aligned}\Pr(N, p, d, k\text{-SRA(k)}) &= \Pr(\text{At least one of N trials is successful}) \\ &= 1 - \Pr(\text{All the N trials are failed}) \\ &= 1 - (1 - \lambda)^N.\end{aligned}$$

□

We have a lemma derived directly from Theorem 7.3.

Lemma 7.4. *If Eve executes a dynamic attack, given ϵ and k-SRA(k), then we have the threshold N_0 responding to the second basic question stated at the end of Chapter 5,*

$$N_0 = \frac{\lg(\epsilon)}{\lg(1-\lambda)} \tag{7.5}$$

where λ is evaluated by Eq. 7.3.

Theorem 7.5. *If Eve executes a static attack, then the upper bound of the probability that there is at least one safe path in N routings of k-SRA(k) depends on N, the safe probability p, the input parameter k, and the distance d between Alice and Bob:*

$$Pr(N, p, d, k\text{-}SRA(k)) \leq 1 - (1-\lambda)^N \tag{7.6}$$

where λ is evaluated by Eq. 7.3. The equality is possible when $N \leq 4$.

Proof. We must take into account the path dependence of N paths taken by N messages sent. The probability that k-SRA(k) takes an unsafe path for each trial is:

$$\begin{aligned}\overline{\Pr(1, p, d, k\text{-SRA(k)})} = \sum_{d \leq l \leq k \times d} \Big(&\Pr\left(k\text{-SRA(k) takes } l\right) \times \\ &\Pr\left(l\text{-SRA}(l) \text{ takes an unsafe path}\right)\Big) = 1 - \lambda\end{aligned} \tag{7.7}$$

The probability of N messages being intercepted is:

$$\begin{aligned}\overline{\Pr(N, p, d, k\text{-SRA(k)})} = \sum_{\substack{d \leq l_1 \leq k \times d \\ \cdots \\ d \leq l_N \leq k \times d)}} &\Bigg(\Pr\left(k\text{-SRA(k) takes } (l_1, \ldots, l_N)\right) \times \\ &\Bigg(\sum_{\substack{l_{\pi_1} = l_1, \\ \cdots \\ l_{\pi_N} = l_N}} \Big(\Pr(l\text{-SRA takes } \pi_1 \ldots \pi_N) \times \Big(\Pr(\pi_1 \ldots \pi_N \text{ are failed})\Big)\Big)\Bigg)\end{aligned} \tag{7.8}$$

For a given path set $(\pi_1, \ldots, \pi_N)$, we can prove the following inequality:

$$\Pr(\pi_1, \ldots, \pi_N \text{ are failed}) \geq \prod_{i=1}^{N} \Pr(\pi_i \text{ is failed}) \tag{7.9}$$

Where the equality holds i.i.f $\pi_1, \ldots, \pi_N$ are independent.

We first prove with $N = 2$. Assume that π_1, π_2 have the length l_1, l_2 respectively, and have l common nodes ($0 \leq l \leq \min(l_1, l_2)$). We have:

$$\begin{aligned}
&\Pr(\pi_1, \pi_2 \text{ are failed}) = p^l \times (1 - p^{(l_1 - l)}) \times (1 - p^{(l_2 - l)}) + (1 - p^l) \\
&= (1 - p^{(l_1)}) \times (1 - p^{(l_2)}) + (p^{(l_1 + l_2 - l)} - p^{(l_1 + l_2)}) \\
&\geq (1 - p^{(l_1)}) \times (1 - p^{(l_2)}) = \Pr(\pi_1 \text{ is failed}) \times \Pr(\pi_2 \text{ is failed})
\end{aligned}$$

Ineq. 7.9 was proven with $N = 2$. We iterate this to obtain (7.9) for $\forall N$. Note that the equality holds iff $\pi_1 \ldots \pi_N$ are separated. In the square 4-connected lattice there are maximum 4 separated paths between Alice and Bob. Thus, if $N > 4$, the equality for (7.9) cannot appear. By applying (7.9) to (7.8), we have:

$$\begin{aligned}
\overline{\Pr(N, p, d, k\text{-SRA(k)})} &\geq \sum_{\substack{d \leq l_1 \leq k \times d \\ \cdots \\ d \leq l_N \leq k \times d)}} \Big(\Big(\prod_{i=1}^{N} \Pr\left(k\text{-SRA(k) takes } l_i\right) \Big) \times \\
&\qquad \Big(\sum_{\substack{l_{\pi_1} = l_1, \\ \cdots \\ l_{\pi_N} = l_N}} \big(\prod_{i=1}^{N} \Pr(l\text{-SRA takes } \pi_i) \big) \times \big(\prod_{i=1}^{N} \Pr(\pi_i \text{ is failed}) \big) \Big) \Big) \\
&= \sum_{\substack{d \leq l_1 \leq k \times d \\ \cdots \\ d \leq l_N \leq k \times d)}} \Big(\Big(\prod_{i=1}^{N} \Pr\left(k\text{-SRA(k) takes } l_i\right) \Big) \times \\
&\qquad \Big(\prod_{l_j = l_1}^{l_N} \Big(\sum_{l_{\pi_i} = l_j} \big(\Pr(l\text{-SRA takes } \pi_i) \times \Pr(\pi_i \text{ is failed}) \big) \Big) \Big) \Big) \\
&= \sum_{\substack{d \leq l_1 \leq k \times d \\ \cdots \\ d \leq l_N \leq k \times d)}} \Big(\prod_{i=1}^{N} \Pr\left(k\text{-SRA(k) takes } l_i\right) \times \prod_{l_j = l_1}^{l_N} \Pr\left(l\text{-SRA}(l_j) \text{ takes an unsafe path}\right) \Big) \\
&= \sum_{\substack{d \leq l_1 \leq k \times d \\ \cdots \\ d \leq l_N \leq k \times d)}} \Big(\Big(\prod_{i=1}^{N} \Pr\left(k\text{-SRA(k) takes } l_i\right) \times \Pr\left(l\text{-SRA}(l_j) \text{ takes an unsafe path}\right) \Big) \Big) \\
&= \prod_{i=1}^{N} \Big(\Big(\sum_{d \leq l_i \leq k \times d} \Pr\left(k\text{-SRA(k) takes } l_i\right) \times \Pr\left(l\text{-SRA}(l_i) \text{ takes an unsafe path}\right) \Big) \Big) \\
&= \prod_{i=1}^{N} \Big(\Pr\left(k\text{-SRA(k) takes an unsafe path}\right) \Big) = (1 - \lambda)^N \text{ (from (7.7))}
\end{aligned}$$

Thus,

$$\Pr(N, p, d, k\text{-SRA(k)}) = 1 - \overline{\Pr(N, p, d, k\text{-SRA(k)})} \leq 1 - (1 - \lambda)^N$$

□

We have a lemma derived directly from Theorem 7.5.

Lemma 7.6. *If Eve executes a static attack, given ϵ and k-SRA(k), we have the threshold N_0 responding to our initial question:*

$$N \geq \frac{\lg(\epsilon)}{\lg(1 - \lambda)} \tag{7.10}$$

Where λ is evaluated by Eq. 7.3. And the equality is possible when $N \leq 4$.

7.4 Simulation results

We implemented simulations to focus on several goals: study the effect of the algorithm ADRA and validate our results on the algorithm k-SRA. Simulations were done in the lattice 600×600 that is the size of our envisaged quantum network.

ADRA's simulations. We ran simulations in varying the safety probability $p_s \in [0.93 : 1]$ and the distance d_{AB} between Alice and Bob [64, 63]. For each p_s, we generated a network with randomly spread eave-droppers. For each distance d_{AB}, we generated 400 (Alice, Bob) pairs. For each such pair, we ran 400 experiments. In each one we generated stochastic routes from Alice to Bob until we find a safe one (i.e., a route with no Eve). For each 400 experiments we gathered the largest number of messages that were needed. Finally, we computed $N_0(p_s, d_{AB})$ (abbreviated N_0), the largest of these figures (i.e., the maximum number of messages that each 400×400 experiment required).

The routing algorithm ADRA may not be able to find any safe path in a reasonable amount of times, in particular when d_{AB} is great. We set the maximum effort to $10,000$ times: Alice sends at most $10,000$ messages, if all are intercepted by Eve, then we declare that the routing algorithm ADRA is not capable to find any safe path. Anyway, real world constraints (time and money) are likely to require a much smaller threshold.

Worst case study reveals $N_{max}(p_s, d_{AB})$ (abbreviated N_{max}) such that (at least for 1.6×10^5 trials):

	p_s						
d	0.99	0.98	0.97	0.96	0.95	0.94	0.93
1	8	12	12	22	14	12	14
2	44	105	122	68	82	425	106
3	87	51	273	99	122	233	439
4	95	171	160	408	244	1125	476
5	66	61	186	917	286	967	2149
6	34	397	356	377	644	583	921
7	43	194	155	395	625	420	2102
8	72	1645	224	414	936	773	1663
9	53	185	477	386	585	717	2794
10	149	169	340	1267	3731	1267	2854
20	127	338	829	9300	×	×	×
30	315	1987	2908	×	×	×	×
40	386	4111	×	×	×	×	×
50	437	×	×	×	×	×	×
60	656	×	×	×	×	×	×
70	1911	×	×	×	×	×	×
80	3117	×	×	×	×	×	×
90	7039	×	×	×	×	×	×
100	4117	×	×	×	×	×	×
110	×	×	×	×	×	×	×

Table 7.1: Worst cases's experiment results. Symbol × stands for more than 10,000.

$$\Sigma(\pi_1, \ldots, \pi_n) = \begin{cases} 1, & \text{if } n \geq N_{max} \\ \tau : 0 \leq \tau < 1, & \text{if } n < N_{max} \end{cases}$$

Table 7.1 gives the worst cases. Fig. 7.1 plots these results and reveals a chaotic behavior. However, this suits with the classical drunkard's walk chaos. Particularly, this suggests the idea about the existence of a threshold of the number of sending messages from that we can be almost certain that there exists at least one message not being intercepted by Eve.

k-SRA's simulations. If the algorithm ADRA and its simulations only support the idea about the existence of a threshold of the number of messages needed, then k-SRA gives more explicitly the bounds of this threshold with respect to a given coefficient security ϵ. We implemented simulations to validate our results.

Simulations were implemented in the lattice 600×600. We ran 10^4 experiments and gathered the results. Table 7.2 show lower bounds, simulation values, and upper bounds of

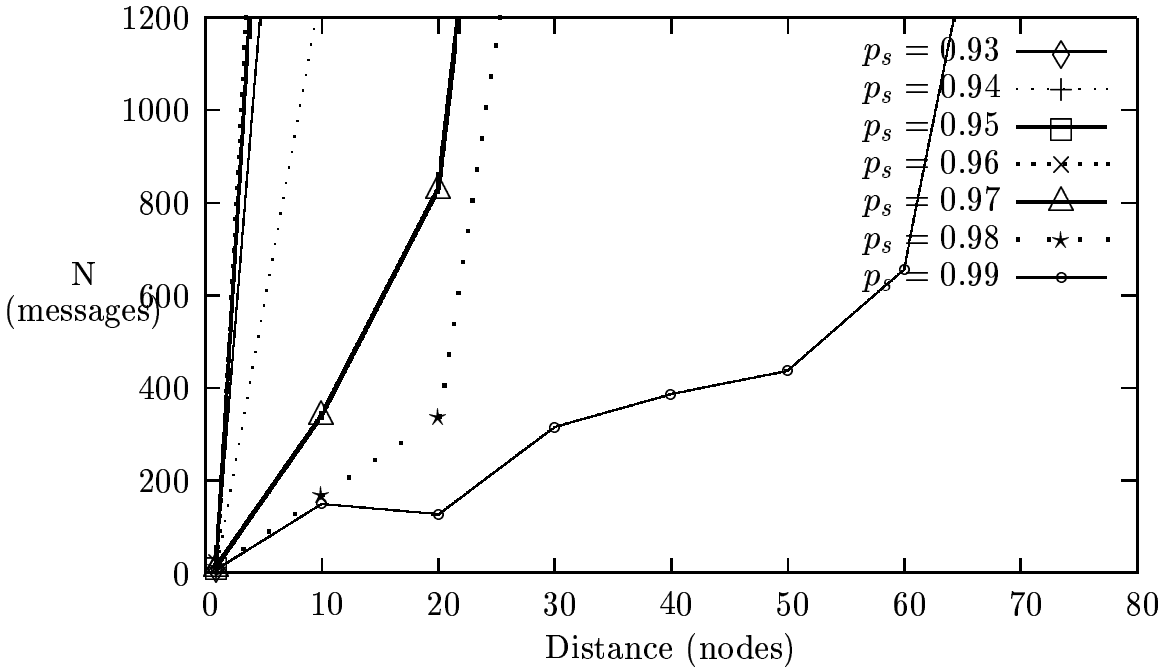


Figure 7.1: The number of messages N in the worst cases for some varying values of p_s.

the case of $k = 2$ and $d = 10$ with $p_s = 0.93; 0.95; 0.97; 0.99$. Note that the lower bound holds if N messages have taken the only one path. The convergence of the experimental results to their upper bound is more significant. Figs. 7.2, 7.3, 7.4, 7.5 draw the upper bounds and the experimental results for a visual comparative study. We realize that the secrecy probability of the final key is a non-decreasing function. As the number of messages being sent increases, this probability converges to its upper bound. Moreover, both tend to one as $N \to \infty$.

	$p_s = 0.93$				$p_s = 0.97$		
N	$\lambda_{lb}(\%)$	$\lambda_{si}(\%)$	$\lambda_{ub}(\%)$	N	$\lambda_{lb}(\%)$	$\lambda_{si}(\%)$	$\lambda_{ub}(\%)$
1	34.71	42.54	34.71	1	63.66	69.99	63.66
10	34.71	80.57	98.59	10	63.66	93.84	98.59
100	34.71	95.36	100	100	63.66	98.94	100
1000	34.71	99.52	100	1000	63.66	99.94	100
10000	34.71	99.96	100	10000	63.66	100	100
	$p_s = 0.95$				$p_s = 0.99$		
N	$\lambda_{lb}(\%)$	$\lambda_{si}(\%)$	$\lambda_{ub}(\%)$	N	$\lambda_{lb}(\%)$	$\lambda_{si}(\%)$	$\lambda_{ub}(\%)$
1	47.04	54.31	47.04	1	86.05	88.75	86.05
10	47.04	87.96	98.59	10	86.05	98.40	100
100	47.04	97.59	100	100	86.05	99.81	100
1000	47.04	99.84	100	1000	86.05	99.99	100
10000	47.04	100	100	10000	86.05	100	100

Table 7.2: Lower bounds, experimental results and upper bounds of the key secrecy for $p_s = 0.93; 0.95; 0.97; 0.99$. λ_{si} is the percentage in 10^4 experiments done.

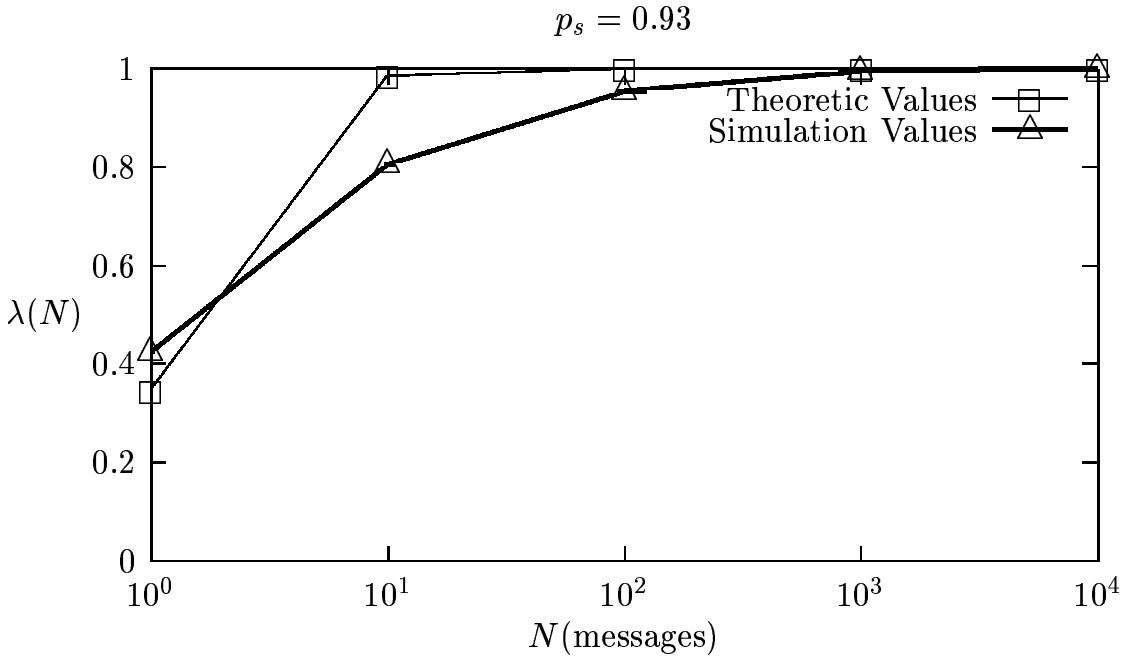


Figure 7.2: Theoretic upper bound and simulation result for $p_s = 0.93$.

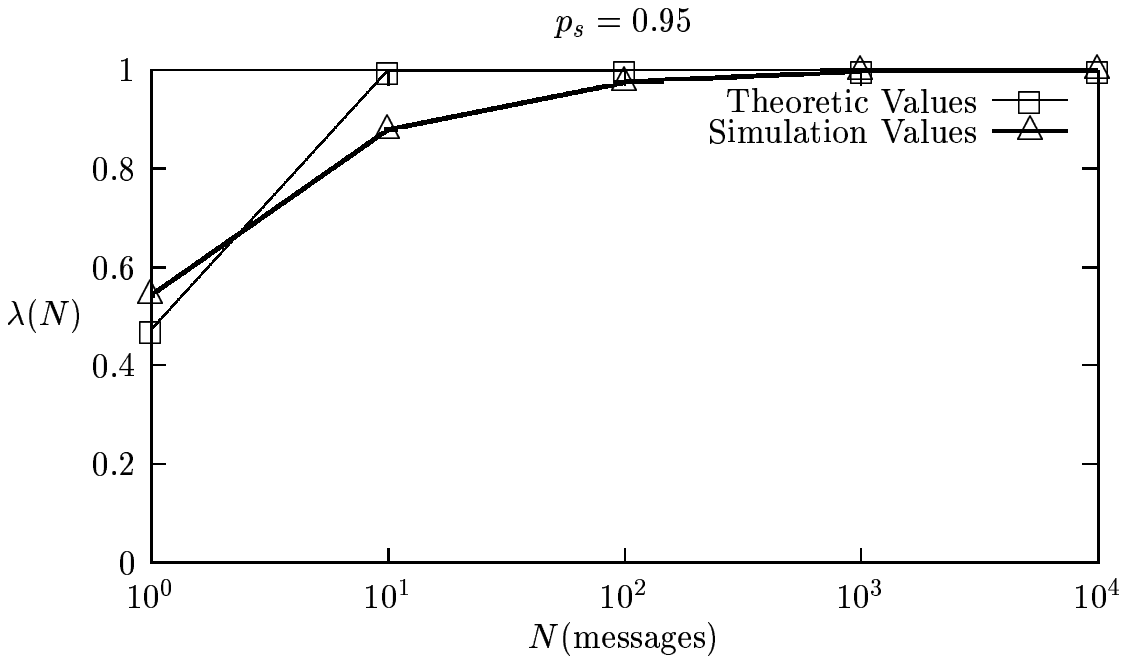


Figure 7.3: Theoretic upper bound and simulation result for $p_s = 0.95$.

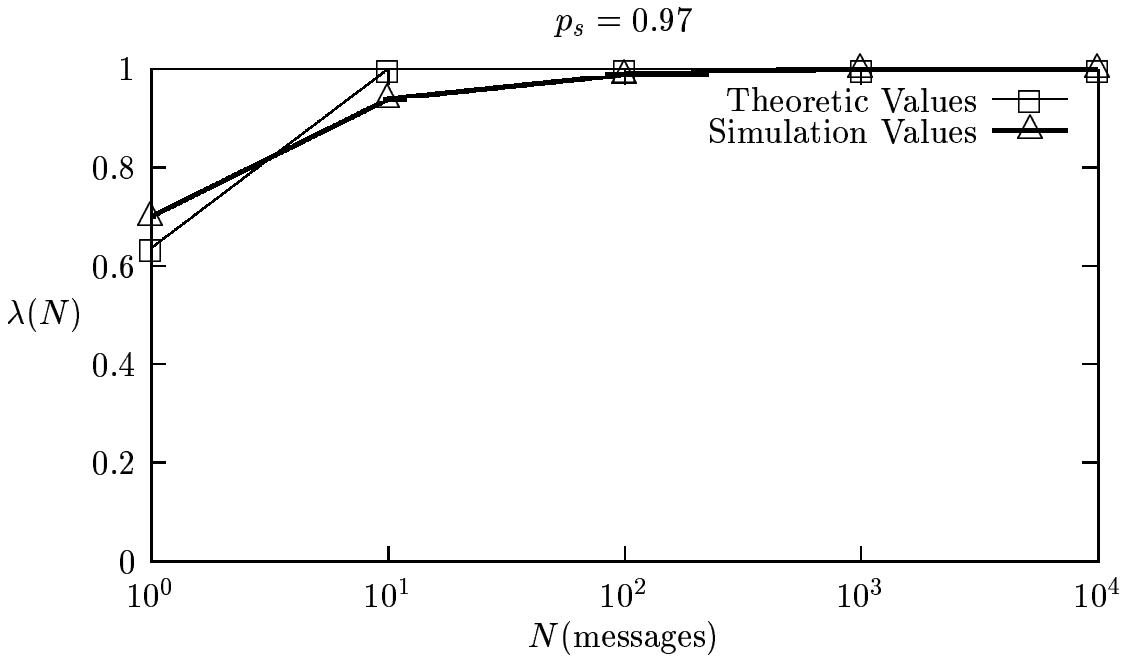


Figure 7.4: Theoretic upper bound and simulation result for $p_s = 0.97$.

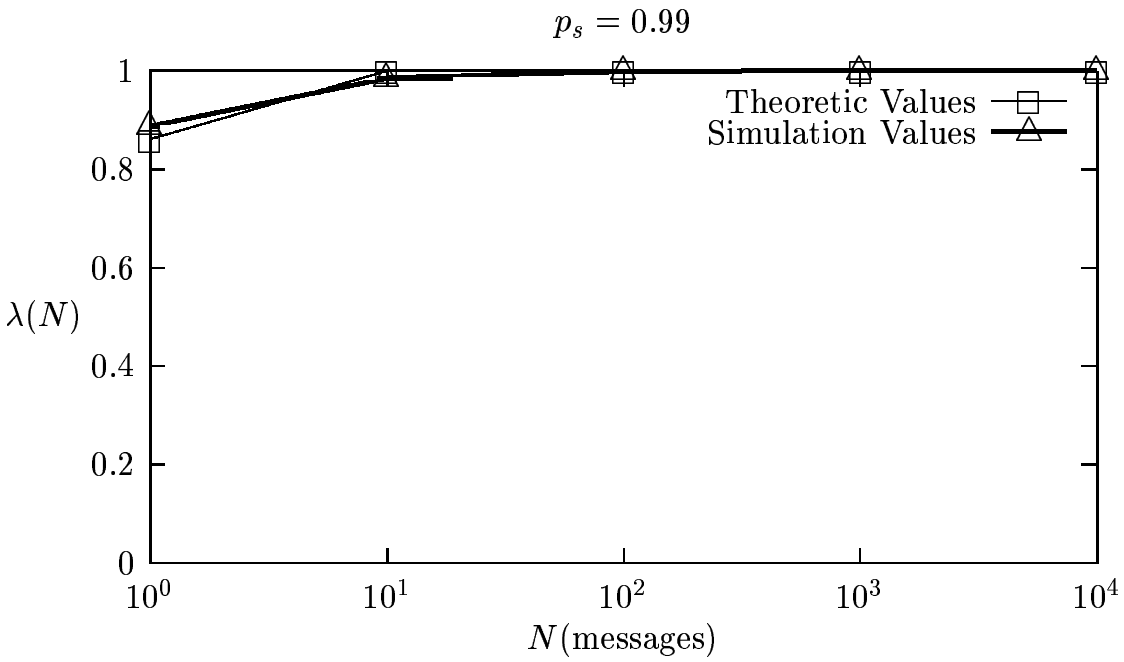


Figure 7.5: Theoretic upper bound and simulation result for $p_s = 0.99$.

Chapter 8

Discussions

In the previous chapters of Part II of this Dissertation we have studied a partially compromised QKD network model that allows any pair of members to establish a common key with almost certainty that the final key will not be disclosed. Our contributions are (i) a model of partially compromised QKD networks, (ii) the use of percolation theory techniques to find where almost-certainty can be achieved, (iii) stochastic routing proposals capable of achieving a given high secrecy level. Indeed, we investigated the constraints of quantum networks, particularly, ineluctable probability that some nodes are compromised. We proposed a secure key exchange scheme that scales well with distance. It is based on stochastic routing, and was analyzed using percolation-theory based methods. Not only did it validated our solution, it also gave figures allowing to engineer various parameters given others. For instance, given the probability that nodes are compromised and the distance between source and destination, it gives the the number of pieces the message must be broken into.

Our proposed framework opens a new door to study the large-scale QKD network. We can think of many things to do in order to improve the performance of the proposed QKD network. For instance, studying more general topologies is of primary importance: grids are only the first stab. The node safety-probability might also varying between regions. Finding formulas (explicit or implicit via equations) is also of interest, as they usually provide more powerful results than simulations do. We can also work to improve our stochastic routing proposal.

It is easy to realize that the key question of the proposed QKD network model is how to force Eve's attack probability of each node to be less than or equal to p_e? If we can measure the vulnerability index of each node in the network, then we can exclude the

nodes of vulnerability greater than p_e before applying the proposed QKD network model. Unfortunately, measuring the vulnerability of a network node is still an open problem so far. In our approach, we assume that for a QKD network of N nodes, Eve has a maximum resource of eavesdropping n nodes, i.e. $p_e = \frac{n}{N}$ if Eve's attack follows a uniform distribution. Thus, beside of depending on each specific routing algorithm, the number of pieces of secret that needs to be sent in order to create a secret shared key depends also on the attack strategy of Eve as analyzed in Section 7.3. However, if Eve knows the position of her target on the network then she certainly does not want to follow the uniform attack distribution. She will use her resource, capable of eavesdropping n nodes, to surround her target. In such a case, even if Alice sends an infinite number of pieces of secret, the final key is always compromised. Hence, in order to bring the proposedQKD network model to practical applications, it is necessary to do further serious analysis, for instance, how to make nodes being anonymous, i.e. the different political and economical role of each nodes is transparent to Eve. In other words, studying application scenarios that suit to the proposed QKD network in practice is important.

Part III

On the QKD relaying models

Chapter 9

Teleportation, entanglement purification and quantum repeater

9.1 Bell states

The originality of quantum entanglement was first observed by Einstein, Podolsky and Rosen (EPR) in 1935 [37]. Their observation is now well-known under the name "EPR paradox". The paradox raises once two following criterias of "local realism" are applied to quantum theory, more precisely to entanglement correlation:

1. Realism criteria: all real things exist regardless of whether or not we observe them. In other words, all possible observables have their pre-existing values before the measurements are made.

2. Locality criteria: the acts upon the distant objects cannot have direct influence on the local one. In other words, an object only is influenced directly by its immediate surroundings.

Einstein, Podolsky and Rosen tried to explain their paradox by invoking "hidden variables". In 1964, however, J. S. Bell introduced an inequality, now well-known by the name "Bell's inequality", that distinguishes entanglement correlations from hidden variable systems. Bell's inequality gives the upper bound of the correlation of the measurement outcomes in any local hidden-variable system, and this bound is violated by the outcomes of the measurements on entangled state pairs. Indeed, as it is well-known today, quantum mechanics is not described by a realistic-local model, and thus the EPR-paradox is resolved [4].

The object observed in Bell's experiment is a joint system maximally entangled quantum state of two qubits. These qubits could be spatially separated, however, they always exhibit perfect correlations. Assume that Alice and Bob share one of four Bell states $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow_A\downarrow_B\rangle - |\downarrow_A\uparrow_B\rangle)$. If Alice and Bob measure their qubits in any common basis, then Alice will get a random logical outcome either 0 or 1 with equal probabilities but the outcome of Bob is always anti-parallel with that of Alice (the same value). Thus, the EPR state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow_A\downarrow_B\rangle - |\uparrow_A\downarrow_B\rangle)$ introduces the non-locality property itself: the quantum state of Bob, previously undefined, becomes completely specified by Alice's local measurement that is spatially separated with Bob.

The four Bell states form an orthogonal basis of the two-qubit joint quantum state, also called the Bell basis. If we consider the logical values encoded in two different bases $|+\rangle = \{|0\rangle, |1\rangle\}$ and $|\times\rangle = \{|\tilde{0}\rangle, |\tilde{1}\rangle\}$, where $|\tilde{0}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\tilde{1}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, then we can re-write Bell states as follows

$$\begin{cases} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = \frac{1}{\sqrt{2}}\big(|\tilde{0}\tilde{0}\rangle + |\tilde{1}\tilde{1}\rangle\big) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big) = \frac{1}{\sqrt{2}}\big(|\tilde{0}\tilde{1}\rangle + |\tilde{1}\tilde{0}\rangle\big) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big) = \frac{1}{\sqrt{2}}\big(|\tilde{0}\tilde{0}\rangle - |\tilde{1}\tilde{1}\rangle\big) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big) = -\frac{1}{\sqrt{2}}\big(|\tilde{0}\tilde{1}\rangle - |\tilde{1}\tilde{0}\rangle\big). \end{cases} \tag{9.1}$$

From Eq. 9.1, we realize that two states $|\Phi^+\rangle$ and $|\Psi^-\rangle$ give the same phenomenon dominated on the measurement outcomes regardless of which basis, either $\{|0\rangle, |1\rangle\}$ or $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$, was used: two outcomes will be parallel if the state is $|\Phi^+\rangle$ and anti-parallel if the state is $|\Psi^-\rangle$. As for two states $|\Phi^-\rangle$ and $|\Psi^+\rangle$, this is not so. For instance, once we measure the state $|\Phi^-\rangle$, if we use the basis $\{|0\rangle, |1\rangle\}$ then we will get two outcomes parallel; otherwise, we will get two outcomes anti-parallel. In other words, the two outcomes depends also on which basis, $\{|0\rangle, |1\rangle\}$ or $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$, was used. Indeed, in quantum information applications such as quantum cryptography one does not use neither $|\Phi^+\rangle$ or $|\Psi^-\rangle$ as the initial states to avoid unnecessary complications raised from such a basis-dependence measurement property.

Bell's states, or so-called EPR pairs, are considered as a new fascinating non-classical resource that promise many potential applications and need to be exploited. In 1991, A. Ekert introduced the first entanglement-based QKD protocol [38] that is a variation of the original single-photon based QKD protocol. Roughly describing, the idea is as follows. Assume that Alice and Bob share many EPR pairs. In order to establish a secret key Alice and Bob measure singlets by using their random bases, then they discard the measurement outcomes of the EPR pairs whose singlets were not measured by the same basis. These

measuring and discarding steps are very similar to those of the original QKD protocol. Then, Alice and Bob check for the interception of Eve by testing Bell's inequality for EPR pairs: if EPR pairs maximally violate Bell's inequality then they were not disturbed by Eve. Other applications exploiting EPR pairs are in quantum computation [87, 31, 16] and quantum error correction [86, 26, 57, 24, 80].

9.2 Teleportation of an unknown quantum state

Suppose that Alice wants to transmit to Bob an unknown qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ but does not want to send the original qubit $|\phi\rangle$ itself. One can think of a classical solution as follows. Alice measures her qubit $|\phi\rangle$ to obtain information featuring $|\phi\rangle$, then sends this information to Bob. Bob receives the information featuring $|\phi\rangle$, then according to this information he forges an exact copy of $|\phi\rangle$ from another qubit in his possession. Unfortunately, such a classical method does not work! The quantum mechanics forbids Alice to acquire the full description of $|\phi\rangle$ by measurements, unless Alice has an infinite numbers of copies of the unknown state $|\phi\rangle$. It should insist here that the state $|\phi\rangle$ is unknown to Alice because if Alice knows beforehand to which orthonormal basis the state $|\phi\rangle$ belongs then she can make a measurement whose result will allow Bob to forge an exact copy of $|\phi\rangle$ from another qubit.

In 1993, Bennett *et al.* presented a non-classical solution, called *quantum teleportation*, that requires the assistance of quantum entanglement [9]. Quantum teleportation strikingly underlines one peculiar feature of the quantum world. It is one of the most fascinating discoveries relied on EPR pairs. This is a process of transmission of an *unknown* quantum state, $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, from one system to another distant system via a previously shared EPR pair and two classical bits transmitted by a classical channel. The destination system becomes the new original as it carries all information the original did and the original destroy all initial information it carried, as required by the quantum no-cloning theorem. Assume that Alice and Bob share previously an EPR pair $|\Phi^+\rangle_{AB}$, where the subscripts indicate the state's owners, $_A$ for Alice and $_B$ for Bob. We have the global system

$$\begin{aligned} |\phi\rangle_A \otimes |\Phi^+\rangle_{AB} &= \big(\alpha|0\rangle_A + \beta|1\rangle_A\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\big) \\ &= \frac{1}{\sqrt{2}}\big(\alpha|00\rangle_A \otimes |0\rangle_B + \alpha|01\rangle_A \otimes |1\rangle_B + \beta|10\rangle_A \otimes |0\rangle_B + \beta|11\rangle_A \otimes |1\rangle_B\big). \end{aligned} \tag{9.2}$$

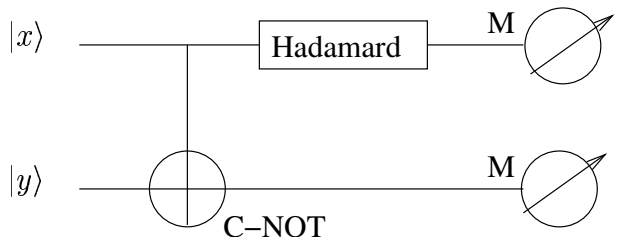


Figure 9.1: An implementation of the Bell measurement: a C-NOT gate followed by a Hadamard rotation and two single qubit measurement.

From the definition of Bell's states, $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $|\Phi^-\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$, $|\Psi^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$, $|\Psi^-\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$, we can re-write the states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ as follows

$$\begin{cases} |00\rangle &= \frac{|\Phi^+\rangle+|\Phi^-\rangle}{\sqrt{2}}, \\ |11\rangle &= \frac{|\Phi^+\rangle-|\Phi^-\rangle}{\sqrt{2}}, \\ |01\rangle &= \frac{|\Psi^+\rangle+|\Psi^-\rangle}{\sqrt{2}}, \\ |10\rangle &= \frac{|\Psi^+\rangle-|\Psi^-\rangle}{\sqrt{2}}. \end{cases} \tag{9.3}$$

Applying (9.3) into (9.2) we have

$$\begin{aligned} |\phi\rangle_A \otimes |\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}\Big(\frac{\alpha}{\sqrt{2}}(|\Phi^+\rangle_A + |\Phi^-\rangle_A) \otimes |0\rangle_B + \frac{\alpha}{\sqrt{2}}(|\Psi^+\rangle_A + |\Psi^-\rangle_A) \otimes |1\rangle_B \\ &\quad + \frac{\beta}{\sqrt{2}}(|\Psi^+\rangle_A - |\Psi^-\rangle_A) \otimes |0\rangle_B + \frac{\beta}{\sqrt{2}}(|\Phi^+\rangle_A - |\Phi^-\rangle_A) \otimes |1\rangle_B\Big) \\ &= \frac{1}{2}\big(|\Phi^+\rangle_A \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + |\Phi^-\rangle_A \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \\ &\quad + |\Psi^+\rangle_A \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) + |\Psi^-\rangle_A \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)\big) \\ &= \frac{1}{2}\big(|\Phi^+\rangle_A \otimes I|\phi\rangle_B + |\Phi^-\rangle_A \otimes \sigma_z|\phi\rangle_B + |\Psi^+\rangle_A \otimes \sigma_x|\phi\rangle_B + |\Psi^-\rangle_A \otimes \sigma_z\sigma_x|\phi\rangle_B\big) \end{aligned} \tag{9.4}$$

where σ_x and σ_z are Pauli's rotations.

Once Alice does a joint measurement on her two qubits in the Bell basis, she gets one of four Bell states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ or $|\Psi^-\rangle$ with equal probabilities. A Bell measurement can be realized by a controlled-NOT (CNOT) gate followed by a Hadamard rotation and two single qubit measurements as described in Fig. 9.1.

Eq. 9.4 indicates that the Bell measurement on Alice's side will make the qubit on Bob's

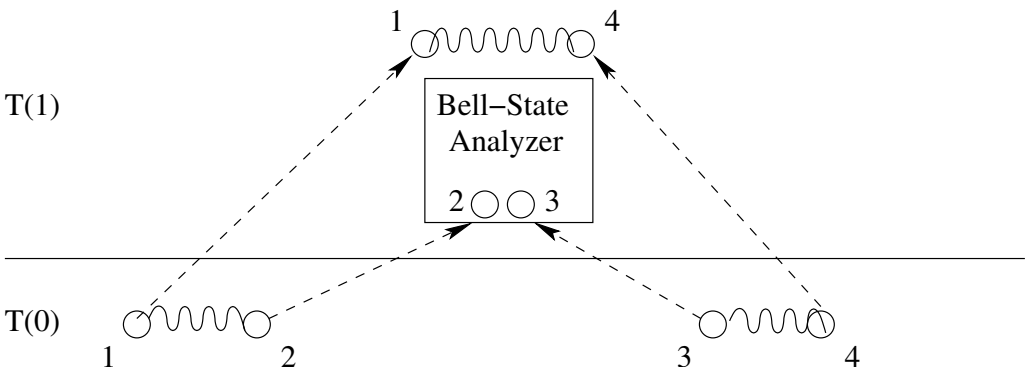


Figure 9.2: Entanglement Swapping: teleportation either of the state of particle 1 to particle 3 or of the state of particle 2 to particle 4.

side collapsed into one of four following states

$$\begin{cases} |\phi\rangle_B & \text{if Alice got } |\Phi^+\rangle \\ \sigma_z|\phi\rangle_B & \text{if Alice got } |\Phi^-\rangle \\ \sigma_x|\phi\rangle_B & \text{if Alice got } |\Psi^+\rangle \\ \sigma_z\sigma_x|\phi\rangle_B & \text{if Alice got } |\Psi^-\rangle. \end{cases} \tag{9.5}$$

Obviously, if Bob knows Alice's measurement outcome than he can recover $\alpha|0\rangle + \beta|1\rangle$ by applying an appropriate inverse rotation on his qubit. Notice that four possible outcomes of Alice can be indexed by two classical bits, and Alice can send these two classical bits to Bob by using a classical channel (telephone, Internet, etc.). Notice also that σ_x, σ_z are Hermitian operators, thus, $\sigma_x = \sigma_x^\dagger$ and $\sigma_z = \sigma_z^\dagger$.

In summary, quantum teleportation is a technique that allows Alice to send an unknown qubit to Bob provided that they share beforehand a Bell state and Alice can send to Bob two classical bits. The minimal resources required for quantum teleportation are one EPR pair and two classical bits. This is rather mysterious because a qubit requires two real numbers to be geometrically represented on the Bloch sphere, not two bits. Besides, even though Alice and Bob know two result bits of measurement they still cannot learn anything about the unknown state $|\phi\rangle$.

9.3 Entanglement swapping

The most interesting case of quantum teleportation is when one tries to teleport an entangled quantum state [99]. This process is called *Entanglement Swapping*. It is the essential

ingredient in quantum repeaters [21]. We consider a system of two Bell's states $|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}$ where the subscripts indicate the qubit numberings. Obviously, the qubits 1 and 4 have not any correlation. However, if we perform a Bell measurement on the qubit 2 and the qubit 3 then the qubit 1 and the qubit 4 become entangled. This is roughly described as in Fig. 9.2. We try to understand this fact by a mathematical manner. We can re-write the global system as follows

$$\begin{aligned} |\Phi^+\rangle_{12}|\Phi^+\rangle_{34} &= \frac{1}{2}(|0000\rangle_{1234} + |0011\rangle_{1234} + |1100\rangle_{1234} + |1111\rangle_{1234} \\ &= \frac{1}{2}(|00\rangle_{23}|00\rangle_{14} + |01\rangle_{23}|01\rangle_{14} + |10\rangle_{23}|10\rangle_{14} + |11\rangle_{23}|11\rangle_{14}. \end{aligned} \tag{9.6}$$

By applying (9.3) on the qubits 2 and 3 in (9.6), we have

$$\begin{aligned} |\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\Big(&\frac{|\Phi^+\rangle_{23} + |\Phi^-\rangle_{23}}{\sqrt{2}} \otimes |00\rangle_{14} + \frac{|\Psi^+\rangle_{23} + |\Psi^-\rangle_{23}}{\sqrt{2}} \otimes |01\rangle_{14} + \\ &\frac{|\Psi^+\rangle_{23} - |\Psi^-\rangle_{23}}{\sqrt{2}} \otimes |10\rangle_{14} + \frac{|\Phi^+\rangle_{23} - |\Phi^-\rangle_{23}}{\sqrt{2}} \otimes |11\rangle_{14}\Big) \\ = \frac{1}{2}(&|\Phi^+\rangle_{23} \otimes |\Phi^+\rangle_{14} + |\Psi^+\rangle_{23} \otimes |\Psi^+\rangle_{14} + |\Psi^-\rangle_{23} \otimes |\Psi^-\rangle_{14} + |\Phi^-\rangle_{23} \otimes |\Phi^-\rangle_{14}). \end{aligned} \tag{9.7}$$

Eq. 9.7 explicitly indicates that if the qubits 2 and 3 are jointly measured in the Bell basis (i.e. projected into one of four Bell states) then the qubits 1 and 4 collapse to be an entanglement. Two qubits 1 and 4 that previously have no correlation become an entangled pair after the result of Bell measurement has already been registered. We can say that the Bell measurement makes teleporting either the state of the qubit 1 to the qubit 3, or the state of the qubit 2 to the qubit 4.

9.4 Entanglement purification

Entanglement purification is a process of distilling few near-perfect EPR pairs out of many imperfect pairs. In other words, this is a process of producing higher-fidelity EPR pairs from lower-fidelity EPR pairs. Fig. 9.3 roughly describes the entanglement purification scheme proposed by Bennett *et al.* in [12,13]. This scheme works on two Werner states [94] ρ_{12} and ρ_{34} where the subscripts indicate the particle (qubit) numberings. Assume that ρ_{12} and ρ_{34}

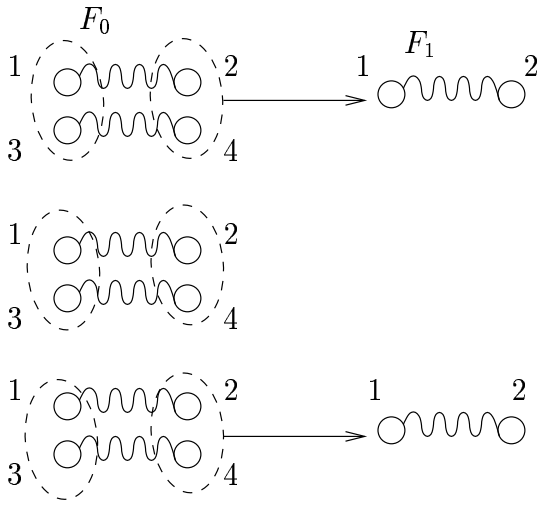


Figure 9.3: The entanglement purification of Bennett *et al.* [12,13] : two CNOT operations are applied on the particles 1 and 3, and the particles 2 and 4, then, the particles 3 and 4 are measured. If the measurement result either 00 or 11 then the particles 1 and 2 are kept and $F_1 \geq F_0$. Otherwise, the particles 1 and 2 are discarded.

describe $|\Phi^+\rangle$ with fidelity F_0,

$$\rho_{12} = \rho_3 4 = F_0 \left|\Phi^+\right\rangle \left\langle\Phi^+\right| + \left(\frac{1-F_0}{3}\right)\left(\left|\Phi^-\right\rangle \left\langle\Phi^-\right| + \left|\Psi^+\right\rangle \left\langle\Psi^+\right| + \left|\Psi^-\right\rangle \left\langle\Psi^-\right| \right). \quad (9.8)$$

In the purification scheme of Bennett *et al.*, one performs two CNOT operations on the particles 1 and 3, and the particles 2 and 4, followed by measuring two particles 3 and 4. If the measurement result shows that the particles 3 and 4 are on the same state (00 or 11) then the remaining pair, described by the state ρ'_{12} is kept, otherwise it is discarded. One can iterate this scheme for N time until the remaining pairs have the fidelity of F_N significantly greater than F_0. However, it must take in attention that the entanglement purification process works if and only if $F_0 \geq F_{min}$ where F_{min} is the minimal required fidelity that depends on the protocol used and specific physical devices.

9.5 Quantum repeater

In practice, quantum communication is realized via noisy and lossy quantum channel where noise and loss scale exponentially with the length of the channel. Indeed, in an optical

fiber of length l, when transmitting a photon without absorption the number of trials scales exponentially with l; even if a photon arrives the destination, the fidelity of the transmitted state decreases exponentially with l. The most essential component of long-distance QKD communication is the quantum repeater. Repeating an arbitrary quantum signal while preserving its proper nature cannot be accomplished by re-applying classical signal processing methods. This is a big challenge, however, this is feasible at least in principle. In 1998, Briegel *et al.* introduced a scheme of quantum repeater that tolerates the general error on the percent level with a polynomial overhead in time and a logarithmic overhead in the number of particles that need to be locally controlled [21]. This method so far is still considered as a standard scheme for quantum repeater and for arbitrarily long QKD systems.

Briegel's scheme is based on three main operations: entanglement swapping, entanglement purification and storing qubits. The operational mechanism can be roughly described as follows [36]:

1. Between two remote nodes Alice and Bob, one puts supplementary nodes as connection points in order to divide the total length into a number of shorter segments such that any two adjacent nodes can share together EPR pairs with an enough fidelity F_0.

2. One performs entanglement swapping, that consists of a Bell measurement and a classical transmission of two result bits, at each connection point to create new EPR pairs shared between non-adjacent node pairs. Since quantum apparatus are imperfect, the fidelity of new EPR pairs roughly decreases to $F_0' < F0$.

3. Entanglement purification is an important step in quantum communication [12, 13, 44, 32]. This step allows to create EPR pairs with fidelity $F_1 \approx F_0$ from a number of EPR pairs with fidelity $F_0' < F_0$.

4. One re-defines new connections points: between Alice, Bob and new connection points now share EPR pairs with fidelity $F_1 \approx F_0$, but the distance between two adjacent nodes has significantly been extended.

5. Return to Step 2 until there is no connection point between Alice and Bob and they share EPR pairs with fidelity $F_N \approx F_{N-1} \approx \ldots \approx F_0$. Once Alice and Bob share EPR pairs with fidelity $F_N \approx F_0$, they can do a entanglement-based QKD protocol to establish their secret key.

In the quick description of the EPR repeating process above, it seems no need to storing quantum states. However, a quantum memory device is indispensable to storing quan-

tum states because without it both the processes of entanglement swapping and quantum purification cannot be accomplished. Indeed, the requirement for quantum memory in entanglement swapping is due to the fact that Bell measurements in linear optics cannot be achieved with arbitrarily high probability, in contrast, they can fail with large probability. Also there is the problem of synchronization of the respective Bell pair halves arriving at the immediate nodes, and the requirement that the total swapping probability does not fall off exponentially with distance. Besides, in some protocols one can consider entanglement swapping and quantum purification as sequential time-dependence processes, i.e. the current step needs some outcomes of its previous step to run. For instance, in order to accomplish an entanglement swapping operation, one needs to known two classical bits resulted from the Bell measurement that indicates explicitly which Pauli's rotation will be applied. The time interval between the Bell measurement and Pauli's rotation steps implies a classical communication (of two classical bits) that can be important for the lifetime of quantum states. As for a long quantum communication that consists of several shorter segments, the accumulated latency due to such classical communications will lead to the requirement of quantum memory devices to store quantum states during the period of gathering Bell measurement's results. This explains why quantum memory devices are one of three main ingredients of Briegel's quantum repeater scheme. Unfortunately, such quantum devices are not available with the current technology. This is one of main reasons responding to the unavailability of quantum repeater in practice so far, although the idea is very beautiful in theory.

In the next chapters, we will introduce the new approaches to securely relay QKD keys. We will start from a new point of view compared the standard quantum repeater based on entanglement swapping, quantum purification and quantum memory. We will also present some novel schemes that can extend the range of original QKD schemes without reducing their original security.

Chapter 10

Quantum Quasi-Trusted relaying models

10.1 Introduction

The limited range of Quantum Key Distribution (QKD) link is one of the most headache-questions to many researchers for a long time. The earliest QKD protocol [8] is the BB84 protocol that was proposed by Bennett and Brassard in 1984. Then, this protocol is proven to be unconditionally secure [88, 66, 25, 71], and promises many worthful applications. Unfortunately, QKD owns undesirable restrictions over range and rate [42, 56]. In order to improve QKD's range approaches can be roughly divided into two categories. The first one focus on improvements over direct QKD links, for instance, perfecting quantum sources and quantum detectors. The second one is to develop QKD relaying methods. This chapter addresses the latter one. For simplicity, we focus on perfect quantum devices, free-error quantum channels to focus on the "relaying" aspect.

Since the range of QKD is limited, QKD relaying methods are necessary. Those become indispensable when one wants to build QKD networks as in recent years. All current QKD relaying models introduce some undesirable features. The most practical QKD relaying model is *trusted model*. It has been applied in two famous QKD networks, DARPA and SECOCQ [40,41,78],The drawback is that all the relaying nodes must be perfectly secured. Such an assumption is critical since passive attacks on intermediate nodes are difficult to be detected by the origin and destination nodes. Few "trusted" intermediaries can lead to terrible security holes in practice.

Theoretically, the most strong QKD relaying models so far are the ones that are based

on Entanglement Swapping (ES) operation [21, 36, 67, 28]. ES-based relaying models allow to achieve an arbitrarily long distance QKD. The idea is roughly described as follows. One can incrementally build a longer distance EPR pair from two shorter distance EPR pairs by a number of complex quantum operations as entanglement purification, entanglement swapping, etc. Thus, one can create shared EPR pairs for two target nodes (origin and destination) regardless of their distance. After having shared EPR pairs, origin and destination can do an entanglement-based BB84 protocol to establish the secret key. ES-based relaying models are considered as *untrusted model* since they allow effectively detecting malicious operations on intermediate nodes. Although ES-based relaying models introduce a beautiful result in theory, unfortunately, the nowadays technologies is not ready to implement such models in practice.

In fact, our work presented in Part II of this dissertation can be considered as based on "quasi-trusted" idea. However, the quasi-trusted property has been characterized differently and analyzed in a different context: each node was assumed to be trusted with a high probability $p \sim 1$, and the main focus was the global security of a very large network. In this chapter, we propose a new definition for quasi-trusted relays. Our quasi-trusted relays are defined as follows: (i) being honest enough to correctly follow a given multi-party finite-time communication protocol; (ii) however, being under the monitoring of eavesdroppers. From the new definition, we first develop a simple 3-party quasi-trusted model called Quantum Quasi-Trusted Bridge (QQTB) model. In this model, the origin Alice and the destination Bob are assumed out of range of Quantum Key Distribution (QKD). Carol is a quasi-trusted relay that can share QKD links with Alice and Bob. We show that QQTB protocol allows Alice and Bob, in cooperation with Carol, to securely establish secret keys. The originality of QQTB protocol is that we do not need invoke entangled photon pairs. Then, we extend QQTB model to Quantum Quasi-Trusted Relay (QQTR) model that is capable of securely distributing secret keys over arbitrarily long distances. Although QQTB model requires entangled photon sources, the originality is that we do not invoke entanglement swapping and entanglement purification as in [21, 36, 67, 28]. The content of this chapter concerns primarily with out publications [60, 61, 62].

10.2 Background

10.2.1 The controlled-NOT (C-NOT) gate

Our models need to use the quantum controlled-NOT (C-NOT) gate (see Fig. 10.1). Original BB84 protocols do not need this gate. However, the C-NOT gate is one of the most popular

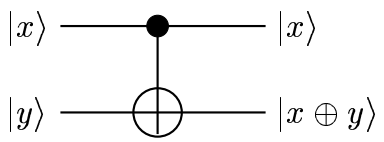


Figure 10.1: The two-qubit controlled-NOT (C-NOT) gate, also called the XOR gate.

two-qubit quantum gates and advanced QKD protocols require this gate [82, 43, 76]. We consider the basis $|+\rangle = \{|0\rangle, |1\rangle\}$. By definition, the C-NOT gate flips the second (target) qubit if the first (control) qubit is $|1\rangle$ and does nothing if the control qubit is $|0\rangle$.

We also consider the basis $|\times\rangle = \{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ where $|\tilde{0}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\tilde{1}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Note that the two bases $|+\rangle$ and $|\times\rangle$ are maximally conjugate.

Proposition 10.1. *If two input qubits of the C-NOT gate are prepared in one common basis, then:*

1. *If the common input basis is $|+\rangle$, then the XOR of two input qubits appears at the second output.*
2. *If the common input basis is $|\times\rangle$, the XOR of two input qubits appears at the first output.*

Proof. The two basis states of the basis $|+\rangle$ are $|0\rangle$ and $|1\rangle$, corresponding to two logical values 0 and 1, respectively. Similarly, the two basis states of the basis $|\times\rangle$ are $|\tilde{0}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\tilde{1}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, corresponding to two logical values 0 and 1, respectively.

We have directly the statement of Proposition 10.1 from the definition of the C-NOT gate (see Fig. 10.1).

We now observe the case in which two input qubits are prepared in basis $|\times\rangle$,

$$
\begin{aligned}
CNOT|\tilde{0}\rangle|\tilde{0}\rangle &= CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
&= \frac{1}{2}(|0\rangle(|0\rangle+|1\rangle)+|1\rangle(|1\rangle+|0\rangle)) \\
&= |\tilde{0}\rangle|\tilde{0}\rangle \\
CNOT|\tilde{1}\rangle|\tilde{0}\rangle &= CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
&= \frac{1}{2}(|0\rangle(|0\rangle+|1\rangle)-|1\rangle(|1\rangle+|0\rangle)) \\
&= |\tilde{1}\rangle|\tilde{0}\rangle \\
CNOT|\tilde{0}\rangle|\tilde{1}\rangle &= CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{1}{2}(|0\rangle(|0\rangle-|1\rangle)+|1\rangle(|1\rangle-|0\rangle)) \\
&= |\tilde{1}\rangle|\tilde{1}\rangle \\
CNOT|\tilde{1}\rangle|\tilde{1}\rangle &= CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{1}{2}(|0\rangle(|0\rangle-|1\rangle)-|1\rangle(|1\rangle-|0\rangle)) \\
&= |\tilde{0}\rangle|\tilde{1}\rangle.
\end{aligned}
$$

We realize that the C-NOT gate now changes the roles of two input qubits. If the second qubit is $|\tilde{1}\rangle$ then it flips the first qubit. Otherwise, it does nothing. The XOR (in basis $|\times\rangle$) is at the first output, not as described in Fig. 10.1. □

Proposition 10.2. *If the two input qubits of the C-NOT gate are prepared in the two different bases, one in $|+\rangle$ and other in $|\times\rangle$, then*

1. *If the first and second qubits are prepared in $|\times\rangle$ and $|+\rangle$, respectively, then the output is an entanglement.*
2. *If the first and second qubits are prepared in $|+\rangle$ and $|\times\rangle$, respectively, then the C-NOT gate does not change the values but can change the global phase of input qubits.*

Proof. If the first and second qubits are prepared in $|\times\rangle$ and $|+\rangle$, respectively, then we have:

$$CNOT|\tilde{0}\rangle|0\rangle = CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$
$$CNOT|\tilde{1}\rangle|0\rangle = CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$$
$$CNOT|\tilde{0}\rangle|1\rangle = CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$$
$$CNOT|\tilde{1}\rangle|1\rangle = CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

Obviously, the output is an entanglement (Bell's states).

If the first and second qubits are prepared in $|+\rangle$ and $|\times\rangle$, respectively, then:

$$CNOT|0\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |0\rangle|1\rangle) = |0\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$CNOT|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |0\rangle|1\rangle) = |0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$
$$CNOT|1\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|1\rangle|1\rangle + |1\rangle|0\rangle) = |1\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$CNOT|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|1\rangle|1\rangle - |1\rangle|0\rangle) = -|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Obviously, the C-NOT gate does not change the values of input qubits. It changes only the global phase if the first and second input qubits are $|1\rangle$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, respectively. □

10.2.2 A simple quantum circuit

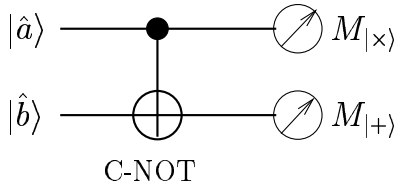


Figure 10.2: The CNOT-M circuit: the pair $(|\hat{a}\rangle, |\hat{b}\rangle)$, where $\hat{a} = \{a, \tilde{a}\}$ and $\hat{b} = \{b, \tilde{b}\}$, goes through a C-NOT gate before being measured independently in two bases $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ and $\{|0\rangle, |1\rangle\}$.

We use the C-NOT gate to build the quantum circuit CNOT-M as described in Fig. 10.2. It has two inputs and two outputs. The two input qubits first go through a C-NOT gate,

and then are measured independently in two different bases $|\times\rangle$ and $|+\rangle$. The final outcome is two classical bits. From Proposition 10.1, we directly derive the following proposition.

Proposition 10.3. *If two input qubits $|\hat{a}\rangle$ and $|\hat{b}\rangle$ are prepared in one common basis ($|\hat{a}\hat{b}\rangle = |ab\rangle$ or $|\tilde{a}\tilde{b}\rangle$), then the CNOT-M circuit reveals no information other than the XOR $a \oplus b$.*

1. *If $|\hat{a}\hat{b}\rangle = |ab\rangle$ (in the common basis $|+\rangle$) then the second output is $(a \oplus b)$ and the first output is either 0 or 1 with equal probabilities, where $a = \{0, 1\}$ and $b = \{0, 1\}$.*
2. *If $|\hat{a}\hat{b}\rangle = |\tilde{a}\tilde{b}\rangle$ (in the common basis $|\times\rangle$) then the first output is $(a \oplus b)$ and the second output is either 0 or 1 with equal probabilities, where $a = \{0, 1\}$ and $b = \{0, 1\}$.*

10.2.3 Quantum Quasi-Trusted (QQT) Relays

Let us observe a three-party communication scenario as follows. The origin Alice wants to establish a secret key with the destination Bob. They want to achieve the unconditional security. However, the distance between them exceeds the limited range of QKD. Carol is an intermediate node that can share QKD links with Alice and Bob. It seems reasonable that Alice and Bob can choose a node Carol who is honest enough to correctly follow a given three-party communication protocol. Vulnerability is Carol can be eavesdropped by the malicious person Eve. In such a scenario, we call Carol a *quasi-trusted* relay.

Definition 10.4 (QQT relay). *A Quantum Quasi-Trusted (QQT) relay is a person or a station that can perform simple quantum operations as measurement, C-NOT, etc., and holds the following conditions :*

1. *Finite-Time Trust: The relay is honest enough to correctly follow a given finite-time communication protocol. After the given protocol has been finished, the relay can be corrupted.*
2. *Under Eavesdropping: The relay can always be under the monitoring of eavesdroppers.*

10.3 Quantum Quasi-Trusted Bridge (QQTB) model

10.3.1 Description

Definition 10.5 (QQTB model). *The QQT-bridge (QQTB) model is a three-party communication model in which the QQT relay Carol acts as a bridge that helps two long-distance*

nodes Alice and Bob to securely establish a shared key. Fig. 10.3 roughly describes the QQTB model.

The QQTB model uses an implicit assumption that Eve cannot eavesdrop the origin Alice and the destination Bob. Such an assumption is trivial since if Alice (or Bob) is eavesdropped then there is no solution. Our definition of the QQTB model also implies that Eve is allowed to perform classical and quantum attacks over channels Alice-Carol and Carol-Bob, even over Carol's site. At the first glance, we realize that the most dangerous vulnerability is from Carol's site. Indeed, although two channels Alice-Carol and Carol-Bob are secured by QKD (see Fig. 10.3), if information appears clearly at Carol's site then Eve can easily read it (see the Under-Eavesdropping condition of Definition 10.4).

Figure 10.3: QKD bridge: Alice and Bob are out of the QKD range; they want to use Carol as a bridge to communicate securely the session key.

The challenge is how we can design secure three-party communication protocols that hold the conditions of the QQT relay (see Definition 10.4). We develop a simple idea that is based on the one-time pad unbreakable encryption scheme. The idea is described as follows. We try to create the situation in which Alice, Carol and Bob own three pads A, C, B, respectively. These pads hold $C = A \oplus B$ (a bit-wise XOR operation). Note that Carol owns C and knows no more than $C = A \oplus B$. When Alice wants to send to Bob a secret key K, she sends $K \oplus A$ to Carol. Carol receives $K \oplus A$, computes $K \oplus A \oplus C = K \oplus B$, and sends the result to Bob. Bob receives $K \oplus B$, computes $K \oplus B \oplus B$ to obtain K. In such a situation, even though Carol owns $C = A \oplus B$, she cannot reveal K. Besides, the key K is unconditionally secured over channel since we use the one-time pad scheme. Obviously, Carol holds the Under Eavesdropping condition (see Definition 10.4). We try to use the Finite-Time Trust condition of Carol to go to such a situation.

We will begin with a simple classical protocol that is insecure. Then we will turn into the quantum world to see how quantum mechanics can help.

10.3.2 A Classical Quasi-Trusted Bridge (CQTB) protocol

The protocol consists of the following steps:

1. Alice securely send to Carol a random m-bit string A by a QKD link.

2. Bob securely send to Carol a random m-bit string B by a QKD link.
3. Carol receives A and B, computes $C = A \oplus B$ (XOR operation).
4. *Carol deletes A and B in her memory device.*
5. Transmitting the secret key:
   - Alice randomly creates the m-bit key K, sends $K \oplus A$ to Carol.
   - Carol receives $K \oplus A$, compute $K \oplus A \oplus C = K \oplus B$, then sends the result to Bob.
   - Bob receives $K \oplus B$, computes $K \oplus B \oplus B$ to obtain K.

What is insecure in this protocol? The step 4 seems helpful in face with the *Finite-Time Trust* condition of the quasi-trusted bridge. After having terminated the protocol, even though Carol is corrupted, the key K is not compromised. But this is not so! Nobody can be sure that in one hand Carol still does correctly the protocol but in the other hand, she makes copies of A and B, maybe only for her curiousness purpose. And then, after the protocol has been completed, she could sell these copies to Eve. Consequently, the key K is compromised. More seriously, the protocol cannot deal with the *Under Eavesdropping* condition of the quasi-trusted bridge (see Definition 10.4). Indeed, if Eve could monitor Carol's memory device, then she can make herself copies of A and B. If A or B is compromised then the key K is compromised.

10.3.3 The QQTB protocol

The Quantum Quasi-Trusted Bridge (QQTB) protocol consists of 4 steps.

Step 1: Preparing, exchanging, and measuring qubits.

1. Alice creates $2n$ random bits $ra_1, .., ra_{2n}$ and chooses a random $2n$-bit string b_A. For each bit ra_i, she creates a corresponding quantum state $|\widehat{ra_i}\rangle = |ra_i\rangle$ (in basis $\{|0\rangle, |1\rangle\}$) if $b_A[i] = 0$, or $|\widehat{ra_i}\rangle = |\widetilde{ra_i}\rangle$ (in basis $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$) if $b_A[i] = 1$. Alice sends $|\widehat{ra_1}, \widehat{ra_2}, .., \widehat{ra_{2n}}\rangle$ to Carol.
2. Similarly, Bob creates $2n$ random bits $rb_1, .., rb_{2n}$, a $2n$-bit strings b_B, then generates and sends $|\widehat{rb_1}, \widehat{rb_2}, .., \widehat{rb_{2n}}\rangle$ to Carol.
3. Carol receives two $2n$-qubit strings from Alice and Bob in a synchronous manner. It means that she receives one by one all the $2n$ pairs $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. To receive a pair

$(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$, Carol randomly turns into either Check-Mode (CM) or Message-Mode (MM).

- In the CM, Carol measures independently $|\widehat{ra_i}\rangle$ and $\widehat{|rb_i\rangle}$ in random bases $|+\rangle$ or $|\times\rangle$. She gathers two classical bits and keeps track of their corresponding bases.
- In the MM, Carol uses the CNOT-M circuit (see Fig. 10.2) to measure the pair $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. She gathers both the output values.

After the receiving finished, CM's and MM's choices roughly result in two n-position strings: the check-position string $CP = cp_1, .., cp_n$ and the message-position string $MP = mp_1, .., mp_n$.

Step 2: Checking for the presence of Eve.

1. For the channel between Alice and Carol: Alice and Carol communicate their bases used in the check-positions CP and the corresponding values. They discard positions where their bases are different. They compare values at remaining positions. If some of these values disagree, then the channel was compromised. In this case, they inform Bob to abort the whole transaction.
2. For the channel between Bob and Carol: Bob and Carol do similarly as Alice and Bob in the checking process above.

Step 3: Creating the pads for Alice, Carol and Bob.

1. Alice and Bob announce their bases in positions $MP = mp_1, .., mp_n$. If their bases are different at mp_i, then they inform Carol to discard this position together.
2. At each remaining position, Carol discards the first output (of the CNOT-M circuit) if the common basis of Alice and Bob is $|+\rangle$. Otherwise, she discards the second output.
3. The remaining values of Alice, Carol and Bob result in three pads $A = A_1, .., A_m; C = C_1, .., C_m; B = B_1, .., B_m$ for Alice, Carol and Bob, respectively. These pads hold $C_i = A_i \oplus B_i, i \in [1, .., m], m \sim \frac{n}{2}$.

Step 4: Transmitting the key K.

1. Carol announces publicly $C = C_1, .., C_m$.
2. Alice creates the random m-bit key K. She sends $K \oplus A \oplus C = K \oplus B$ to Bob.

3. Bob receives $K \oplus B$, computes $K = K \oplus B \oplus B$.

We show why our protocol is secure. At the step 1, when a pair $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$ synchronously arrives to Carol, she randomly turns into either the Check-Mode (CM) or the Message-Mode (MM). Since Eve does not know in advance the choices of Carol, she cannot treat differently the pairs $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. Thus, the error-rate on the check bits must behave like that on the message bits. In the other hand, the error-check procedures in the channels (Alice, Carol) and (Carol, Bob) work exactly as that of the BB84 protocol. By that, QQTB protocol's security is exactly that of the BB84 protocol. This implies that the QQTB protocol is unconditionally secure. Readers interested in security proof of BB84 are invited to read [11, 88, 66, 25, 71].

10.3.4 Discussion

Compared with the trusted model, the QQTB model seems stronger in realistic scenarios. The trusted model implicitly requires nodes being secured in an infinite time. The QQTB model only requires that the nodes are trusted in a finite time. Besides, if nodes in trusted model are eavesdropped then the security is compromised. In contrast, the QQTB model allows to defeat eavesdropping operations on intermediate nodes, provided that these nodes correctly follow the protocol.

The QQTB model is weaker than entanglement-based relaying models since it can extend up to two times the QKD range. Besides, entanglement-based relaying models are the untrusted model while the QQTB model cannot be considered as untrusted one. Indeed, since the bridge Carol participates in the check for the presence of Eve, she can cheat the protocol. Such a situation can be considered as *man-in-middle attack*. Fortunately, we can defeat such an attack by using the Wegman-Carter authentication [93].

Our QQTB protocol does not need entangled photon pairs. This helps to avoid difficulties arising from the decoherence of entangled-photons in practice. However, our protocol must deal with the synchronization problem that may be not simple in practice. Besides, using a CNOT gate can also be considered as a practical disadvantage compared with the original BB84 protocols.

10.4 Quantum Quasi-Trusted Relay (QQTR) model

In QQTB model, we implicitly address single-photon based models to avoid difficulties arising from entangled photon pairs. The question is whether we can extend this model

based only on single-photon up to arbitrarily long distances? We observe the scenario in which there is Dave in the right of Bob. Bob plays the role of untrusted relay as Carol. The goal now is that Alice can convey a secret to Dave, not to Bob. Assume that the distances between Alice, Carol, Bob and Dave are the critical distance of single-photon transmission on that arrival qubits are correctly detected. This means that Alice cannot send directly single photons to Bob or Dave, and Dave cannot send directly single photons to Carol or Alice. Thus, Alice and Dave cannot make together a quantum contact at one sole intermediate location as in the QUB model. Besides, no classical contact can help unless Alice and Dave pre-possess a secret key that has the length at least equal to that of the transmitting secret [84]. As a result, we can conclude that the single-photon based QUB model cannot extend more than two times of the limited single photon based QKD range. This makes sense of the word "bridge" in the QQTB model: two bridges cannot be built successively.

10.4.1 Description

The QQTR model is roughly described as Fig. 10.4. The QQTR model needs entangled-photon sources. Between the origin Alice and the destination Bob we arrange N Carols $C_1, .., C_N$ and $N+1$ Bells $B_1, .., B_{N+1}$ (see Fig. 10.4). $C_1, .., C_N$, $B_1, .., B_{N+1}$ are quasi-trusted nodes. This creates $2N+2$ segments. The concrete value of N depends on the distance between Alice and Bob. Without loss of generality, we assume that the lengths of $2N$ segments are the same and the common length allows quantum devices working correctly and effectively.

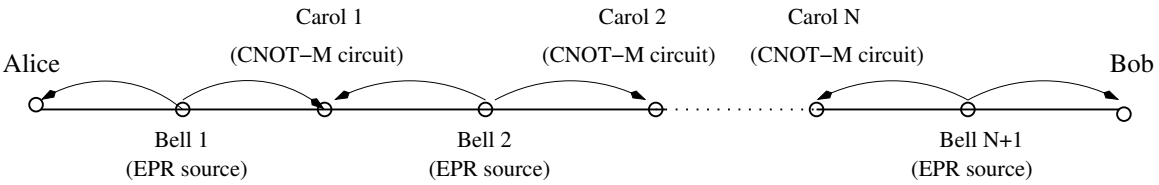


Figure 10.4: Bell 1,.., Bell N are EPR-pair sources. Carol 1, .., Carol N act similarly as Carol in the QQTB protocol.

10.4.2 The QQTR protocol

For convenience, we also use C_0 and C_{N+1} to denote Alice and Bob, respectively. The QQTR protocol consists of 5 steps:

Step 1: Preparing, exchanging, and measuring qubits.

1. Each B_i, $i \in [1, N+1]$, prepares n Bell states $(|\Phi^+\rangle)^n$.

2. Each B_i, $i \in [1, N+1]$, sends the first half of each Bell state to C_{i-1} (the previous site), the second half to C_i (the next site).

3. Alice (or C_0) and Bob (or C_{N+1}), each one receives n qubits. They randomly and independently choose bases to measure their qubits.

4. Each $C_i, i \in [1, N]$, receives $2n$ qubits from B_i and B_{i+1} in a synchronous manner. This means that she receives n times, and for each time she receives a qubit pair: one qubit from B_i and another one from B_{i+1}. She uses the CNOT-M circuit (see Fig. 10.2) to measure each incoming qubit pair. She keeps the measured values and the corresponding bases. Briefly, C_i acts exactly as Carol in the Message-Mode of the QQTB protocol.

Step 2: Sifting.

1. Alice and Bob announce their bases.

2. If the bases are different at the position i, then Alice, Bob, $C_1, .., C_N$ discard this position.

3. For each remaining position i, $C_1, .., C_N$ discard the first or the second output (of the CNOT-M circuit) if the common basis of Alice and Bob is $|+\rangle$ or $|\times\rangle$, respectively.

4. The remaining values result in $N+2$ $2m$-bit strings $a = a_1, .., a_{2m}$; $c(i) = c(i)_1, .., c(i)_{2m}, i = 1..N$; $b = b_1, .., b_{2m}$ for Alice, $C_1, .., C_N$, and Bob, respectively. These $N+2$ strings hold $\oplus_{i=1}^{N} c(i)_j = a_j \oplus b_j, j \in [1, 2m], 2m \sim \frac{n}{2}$.

Step 3: Checking for the presence of Eve.

1. Alice, Bob, and $C_1, .., C_N$ randomly agree m out of $2m$ positions to check the presence of Eve. This results in two m-position strings: the check-position string $CP = cp_1, .., cp_m$ and the message-position string $MP = mp_1, .., mp_m$.

2. Alice, Bob, $C_1, .., C_N$ announce values at check positions CP: $a = a_{cp_1}, .., a_{cp_m}$; $b = b_{cp_1}, .., b_{cp_m}$; $c(i) = c(i)_{cp_1}, .., c(i)_{cp_m}, i \in [1, N]$, respectively. They check if $\oplus_{i=1}^{N} c(i)_{cp_j} = a_{cp_j} \oplus b_{cp_j}$ or not. If some of negative checks, they abort the protocol.

Step 4: Creating the pads for Alice, $C_1, .., C_N$, Bob.

1. The values at m positions MP result in $N+2$ m-bit pads: $P^A = P_1^A, .., P_m^A$; $P^{C(i)} = P_1^{C(i)}, .., P_m^{C(i)}, i \in [1, N]$; and $P^B = P_1^B, .., P_m^B$ for Alice, $C_1, .., C_N$, and Bob, respectively. These pads hold $\oplus_{i=1}^N P^{C(i)} = P^A \oplus P^B$.

Step 5: Transmitting the key K.

1. Each $C_i, i \in [1, N]$ announces publicly $P^{C(i)}$.
2. Alice creates the random m-bit key K, $m \sim \frac{n}{4}$. She sends $K \oplus P^A \oplus_{i=1}^N P^{C(i)} = K \oplus P^B$ to Bob.
3. Bob receives $K \oplus P^B$, retrieves $K = K \oplus P^B \oplus P^B$.

10.4.3 Correctness, security and discussion

Correctness. One could claim that is it true that $\oplus_{i=1}^N c(i)_j = a_j \oplus b_j, j \in [1, 2m], 2m \sim \frac{n}{2}$ in the step 2 (sifting)? We will observe the process that creates a common bit (at position j) for Alice and Bob. The input are $N+1$ EPR pairs from $N+1$ Bell's sites. Besides, Alice and Bob must measure the received qubits in one common basis. The Bell state at the site Bell i (B_i) can be represented as (up to $\frac{1}{\sqrt{2}}$)

$$|\Phi^+\rangle_{B_i^{(1)} B_i^{(2)}} = \sum_{n=0}^{1} |n, n\rangle_{B_i^{(1)} B_i^{(2)}} = \sum_{n=0}^{1} |\tilde{n}, \tilde{n}\rangle_{B_i^{(1)} B_i^{(2)}} \tag{10.1}$$

where $B_i^{(1)}(B_i^{(2)})$ is the first (second) qubit of Bell i; $\{|0\rangle, |1\rangle\}$ and $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ denote the bases $|+\rangle$ and $|\times\rangle$, respectively. Note that (also up to $\frac{1}{\sqrt{2}}$)

$$|n\rangle = \sum_{m=0}^{1} (-1)^{nm} |\tilde{m}\rangle, \quad |\tilde{n}\rangle = \sum_{m=0}^{1} (-1)^{nm} |m\rangle \tag{10.2}$$

Initially, the global state is

$$|\Psi_0\rangle = \otimes_{i=1}^{N+1} |\Phi^+\rangle_{B_i^{(1)} B_i^{(2)}} \tag{10.3}$$

where $\otimes$ denotes the tensor product.

Using (10.1) we can re-write (10.3) in basis $|+\rangle$ as

$$|\Psi_0\rangle = \sum_{\{n_i\}=\mathbf{0}}^{\mathbf{1}} \otimes_{i=1}^{N+1} |n_i, n_i\rangle_{B_i^{(1)} B_i^{(2)}} \tag{10.4}$$

or in basis $|\times\rangle$ as

$$|\Psi_0\rangle = \sum_{\{n_i\}=\mathbf{0}}^{\mathbf{1}} \otimes_{i=1}^{N+1} |\widetilde{n_i}, \widetilde{n_i}\rangle_{B_i^{(1)} B_i^{(2)}} \tag{10.5}$$

After distributing the qubits: $B_1^{(1)} \to C_0(A)$, $B_i^{(2)} \to C_i$, $B_{i+1}^{(1)} \to C_i$ (for $i = 1, .., N$), $B_{N+1}^{(2)} \to C_{N+1}(B)$, we have

$$|\Psi_0\rangle = \sum_{\substack{\{n_i\}=\mathbf{0}, \\ n_{N+1}=0}}^{\mathbf{1},1} |n_1\rangle_A \Big(\otimes_{i=1}^{N} |n_i, n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |n_{N+1}\rangle_B \tag{10.6}$$

in basis $|+\rangle$ or

$$|\Psi_0\rangle = \sum_{\substack{\{n_i\}=\mathbf{0}, \\ n_{N+1}=0}}^{\mathbf{1},1} |\widetilde{n_1}\rangle_A \Big(\otimes_{i=1}^{N} |\widetilde{n_i}, \widetilde{n_{i+1}}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |\widetilde{n_{N+1}}\rangle_B \tag{10.7}$$

in basis $|\times\rangle$.

After all the C_i perform the CNOT on their qubit pairs, (10.6) and (10.7) become

$$\begin{aligned} |\Psi_1\rangle &= \sum_{\substack{\{n_i\}=\mathbf{0}, \\ n_{N+1}=0}}^{\mathbf{1},1} |n_1\rangle_A \otimes \Big(\otimes_{i=1}^{N} |n_i, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |n_{N+1}\rangle_B \\ &\equiv \sum_{\{n_i, n_{N+1}, m_i\}=\mathbf{0}}^{\mathbf{1}} |n_1\rangle_A \otimes \Big(\otimes_{i=1}^{N} (-1)^{n_i m_i} |\widetilde{m_i}, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |n_{N+1}\rangle_B \end{aligned} \tag{10.8}$$

or

$$|\Psi_1\rangle = \sum_{\substack{\{n_i\}=\mathbf{0},\\ n_{N+1}=0}}^{\mathbf{1},1} |\widetilde{n_1}\rangle_A \otimes \Big(\otimes_{i=1}^N |\widetilde{n_i \oplus n_{i+1}}, \widetilde{n_{i+1}}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |\widetilde{n_{N+1}}\rangle_B$$
$$\equiv \sum_{\{n_i, n_{N+1}, m_{i+1}\}=\mathbf{0}}^{\mathbf{1}} |\widetilde{n_1}\rangle_A \otimes \Big(\otimes_{i=1}^N (-1)^{n_{i+1} m_{i+1}} |\widetilde{n_i \oplus n_{i+1}}, m_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |\widetilde{n_{N+1}}\rangle_B \tag{10.9}$$

In the case where both Alice and Bob measure their qubits in basis $|+\rangle$ while each C_i measures her qubits $C_i^{(1)}$ and $C_i^{(2)}$ in $|\times\rangle$ and $|+\rangle$ respectively, Eq. (10.8) collapses into (up to a global phase factor)

$$\psi_1 = |n_1\rangle_A \Big(\otimes_{i=1}^N |\widetilde{m_i}, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |n_{N+1}\rangle_B \tag{10.10}$$

where n_1, m_i, n_i, n_{i+1} and n_{N+1} randomly take on either 0 or 1. Obviously, the outcome of $C_i^{(2)}$ yields

$$\begin{aligned} \oplus_{i=1}^N (n_i \oplus n_{i+1}) &= n_1 \oplus n_2 \oplus n_2 \oplus .. \oplus n_N \oplus n_N \oplus n_{N+1} \\ &= n_1 \oplus n_{N+1} \end{aligned}$$

In the case where both Alice and Bob measure their qubits in basis $|\times\rangle$ while each C_i always does as before, Eq. (10.9) collapses into (up to a global phase factor)

$$\psi_1 = |\widetilde{n_1}\rangle_A \Big(\otimes_{i=1}^N |\widetilde{n_i + n_{i+1}}, m_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |\widetilde{n_{N+1}}\rangle_B \tag{10.11}$$

where n_1, m_i, n_i, n_{i+1} and n_{N+1} randomly take on either 0 or 1. Obviously, the outcome of $C_i^{(1)}$ yields again $\oplus_{i=1}^N (n_i \oplus n_{i+1}) = n_1 \oplus n_{N+1}$.

Note that $n_1, n_{N+1}, n_i \oplus n_{i+1}$ are outcomes of Alice, Bob, and Carol C_i, respectively. Thus, the equation stated at the end of Step 2 is proven.

Security. We distinguish possible attack types of Eve.

1. Type 1: Quantum attack on sites Bell 1,.., Bell N+1 $(B_1, .., B_{N+1})$.
2. Type 2: Quantum attack on sites Carol 1, .., Carol N $(C_1, .., C_N)$.

3. Type 3: Quantum attack on channel. Eve could do quantum attacks on $2n + 2$ segments between Alice and Bob.

4. Type 4: Classical attack, eavesdropping on sites $C_1, .., C_N$.

The attack Type 1 implies imperfect EPR sources: the qubit pairs could be entangled with Eve's probes. In [67], fortunately, Lo and Chau have proven that we can effectively check perfect EPR sources by executing random-hashing verification schemes. As a result, we could conclude that our QQTR protocol is secure to this attack type.

Note that $C_1, .., C_N$ reveal no information than the XOR results. Indeed, their output choices (the first or second one) depend on the random coincidence of the basis choices of Alice and Bob. This implies that all the single states (qubits) in the channels (attack type 3) and the $C_1, .., C_N$ (attack type 2) are unknown to Eve. By the no-cloning theorem, Eve will make additional disturbances if she tries to get information from these states [11]. In the step 3 of the QQTR protocol, we check the presence of Eve by evaluating disturbances as in the BB84 protocol. Thus, we conclude that our QQTR protocol is secure to the attack types 2 and 3.

Our protocol also is secure to the attack type 4 since the classical values a, b were not revealed outside Alice and Bob's sites. The knowledge on $c(1), .., c(N)$ cannot derive with certainty the values of a, b. Here, we can say that the principle of the QQTR protocol is exactly that of the single-photon QQTB protocol. This is the spirit of our "quasi-trusted" concept.

Discussion. Our QQTR protocol uses the C-NOT gate and EPR pairs. At the first glance, one can say that it is the idea of quantum repeater based on entanglement swapping and entanglement purification. But this is not so. In our protocol, EPR pairs are collapsed into single photons immediately after having traversed a segment. At the end of the phase exchanging qubits, Alice and Bob do not keep any EPR pair. Instead of using quantum entanglement to conserve the coherence between qubits, we use the global classical information (XOR value) from that one cannot derive exactly partial informations.

Theoretically, our QQTR model is weaker than entanglement-based relaying models. These models allow to check the presence of Eve regardless of the security of intermediate nodes. Our QQTR model requires the intermediate nodes (relays) to be trusted in a finite-time in order to collaborate together to check the presence of Eve (at EPR sources, or on the channels) and protect the partial secrets owned by Alice and Bob. If intermediate nodes are corrupted and do not correctly follow our QQTR protocol then the security can be corrupted. However, if all the intermediate nodes correctly follow the QQTR protocol

then Alice and Bob obtain unconditionally secure keys.

We realize that in the QQTR protocol the number of secure bits m does not depend on the number of segments $2N + 2$: $m \sim \frac{n}{4}$ where n is the number of EPR states transmitted from each EPR source (see the step 5 of the QQTR protocol).

10.5 Conclusion

We proposed quasi-trusted QKD relaying models. The quasi-trusted property is characterized by: (i) being honest enough to correctly follow a given multi-party finite-time communication protocol; (ii) however, being under the monitoring of eavesdroppers. The heart of our works is the CNOT-M circuit (see Fig. 10.2 and Proposition 10.3 in Section 10.2.2).

We distinguished single-photon and entanglement based models. We showed that our single-photon based model is only capable of extending up to two times the limited range of the original QKD schemes. Our entanglement based model is capable of extending up to an infinite length of QKD. Both models guarantee the perfect security of the final key provided that intermediate nodes correctly follow the communication protocol. Our quasi-trusted assumption seem quite reasonable in practice. Besides, the proposed models do not need to store quantum states for a long time as required in the standard quantum repeater model. Indeed, if the synchronization can be well done then the proposed models do not need to use quantum memory devices. This can bring significant advantages in scenarios where there is no quantum memory devices as today.

Chapter 11

Quantum Untrusted relaying models

11.1 Introduction

Let us re-call a simple QKD relaying problem. This is a three-party communication where the origin, Alice, wants to share a secret key with the destination Bob. They want that the key is unconditionally secure. However, the distance between them is out of range of QKD which is the sole technique that allows them to obtain their goal so far. Carol is an intermediate node that can share QKD links with Alice and Bob. However, Alice and Bob do not want to trust Carol. They suppose that Carol is *untrusted* and the malicious Eve can have full control over Carol. The question of interest is how Alice and Bob can still gain the availability of Carol to establish their secret key without reducing the security of the original QKD schemes?

The idea of our approach is simple. We remark that if Alice, Carol and Bob own respectively three classical random pads A, C, B, where $C = A \oplus B$ (bit-wise XOR operation) then the final key can go through Carol without reducing the confidentiality of key. *Notice that Carol owns C and knows no more other than $C = A \oplus B$.* Indeed, when Alice wants to send to Bob a secret key K, she sends $K \oplus A$ to Carol. Carol receives $K \oplus A$, computes $K \oplus A \oplus C = K \oplus B$, and sends the result to Bob. Bob receives $K \oplus B$, computes $K \oplus B \oplus B$ to obtain K. Since Alice and Bob use the one-time pad unbreakable scheme [84], Carol will be "blind" to the final key K even though she has $C = A \oplus B$.

If we can create the situation as described above then the three-party QKD relaying problem will be solved. Let us try to do a quick analysis. Since Alice (respectively Bob)

and Carol can share a QKD link, this implies that Alice (resp. Bob) can successfully send to Carol unknown quantum states (unknown to Eve also to Carol) in order to implement a QKD protocol. In such cases, instead of transmitting the classical information A (resp. B), Alice (resp. Bob) sends to Carol an unknown quantum state $|A\rangle$ (resp. $|B\rangle$) that encodes A (resp. B). Now, if Alice (resp. Bob) agrees to perform a QKD protocol with Carol, then Carol can get the classical information A (resp. B) from the unknown state $|A\rangle$ (resp. $|B\rangle$). Once Carol has both A and B, she can compute $C = A \oplus B$. This seems that we has created the intended goal. But this is not so! Carol now has not only C where $C = A \oplus B$, but also A and B. This does not satisfy Alice and Bob because they suppose that Eve can have full control over Carol, hence, Eve can read A and B (as well as Carol) and consequently, the final key K is compromised.

The essential point here is that the *unknown quantum state* $|A\rangle$ (resp. $|B\rangle$) should *NOT* be collapsed to reveal the *classical* information A (resp. B) in any case. However, Carol must derive the classical value C, where $C = A \oplus B$, from two unknown states $|A\rangle$ and $|B\rangle$. Hence, the question of interest is whether it exists a manner that produces $|C\rangle$, where $C = A \oplus B$, that is an unknown quantum state to Carol and of course unknown to Eve, too? If Yes, then Alice and Bob afterward can cooperate to perform with Carol a QKD protocol on the state $|C\rangle$ to distill C without revealing A (resp. B).

Since the quantum Controlled-NOT (CNOT) gate can produce a qubit $|c\rangle = |a \oplus b\rangle$, where $|a\rangle$ and $|b\rangle$ are two input qubits, we can immediately think of this gate. However, producing $|c\rangle = |a \oplus b\rangle$ is only a particular case of using the CNOT gate. The XOR operation is not true for two arbitrary input qubits. Besides, in the quantum world, since all the unitary transformations are *reversible*, is it possible that the CNOT gate will reveal some information about a (resp. b) once Carol has got $c = a \oplus b$? We will show that we can build secure QKD relaying models by using the CNOT gate in the next sections. Indeed, we will re-use Propositions 10.1, 10.2, 10.3, stated in Section 10.2. Note that using the CNOT gate is only an implementation way of our approach.

11.2 Quantum Untrusted Bridge (QUB) Model

11.2.1 Model description

The QUB model is roughly described in Fig. 11.1. There, "QKD link" implies the critical range inside which transmitted photons do not vanish and can still be correctly detected. As in the original QKD schemes, we must assume that there is an authenticated classical channel between Alice and Bob to defeat "man-in-middle" attacks. Roughly speaking,

the context of the QUB model is similar to that of the three-party QKD relaying problem mentioned in the beginning of this paper. Our task is to design a three-party communication protocol that allows Alice and Bob to achieve their goal.

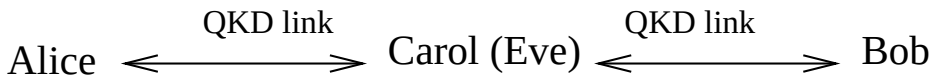


Figure 11.1: Alice and Bob are out of the QKD range. They must securely transmit the shared key through Eve. They must effectively detect and then discard the cases in which Eve reads the transmitting key.

11.2.2 The QUB protocol

The protocol consists of 5 steps.

Step 1: Preparing, exchanging, and measuring qubits.

1. Alice creates $2n$ random bits $ra_1, .., ra_{2n}$ and chooses a random $2n$-bit string b_A. For each bit ra_i, she creates a corresponding quantum state $|\widehat{ra_i}\rangle = |ra_i\rangle$ (in basis $\{|0\rangle, |1\rangle\}$) if $b_A[i] = 0$, or $|\widehat{ra_i}\rangle = |\widetilde{ra_i}\rangle$ (in basis $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$) if $b_A[i] = 1$. Alice sends $|\widehat{ra_1}, \widehat{ra_2}, .., \widehat{ra_{2n}}\rangle$ to Carol.

2. Similarly, Bob creates $2n$ random bits $rb_1, .., rb_{2n}$, a $2n$-bit strings b_B, then generates and sends $|\widehat{rb_1}, \widehat{rb_2}, .., \widehat{rb_{2n}}\rangle$ to Carol.

3. Carol receives $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle), i \in [1, 2n]$ from Alice and Bob. For each pair $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$, Carol uses the CNOT-M circuit (see Fig. 10.2) to get two classical output bits. Note that these two classical bits contain no more information than a classical XOR bit $ra_i \oplus rb_i$ (see Proposition 10.1 and Proposition 10.3).

4. *Carol sends to Alice and Bob $2n$ pairs of two classical output bits. The role of Carol stops here.*

Step 2: Sifting.

1. Alice and Bob communicate their bases b_A and b_B. If their bases are different at position i then they discard this position.

2. At each remaining positions i, they discard one of two corresponding bits received from Carol as follows. They discard the first value or the second value if their common basis (at position i) is $|+\rangle$ or $|\times\rangle$, respectively.

3. Now, all the remaining values result in three $2m$-bit [1] strings $a = a_1, .., a_{2m}$, $c = c_1, .., c_{2m}$, $b = b_1, .., b_{2m}$ where Alice keeps two string a, c and Bob keeps two strings b, c. Note that in the ideal case (perfect apparatus, perfect channels, etc.) these three strings should hold $c_i = a_i \oplus b_i$ where $i \in [1, 2m]$ and $2m \sim \frac{2n}{2}$.

Step 3: Checking for the presence of Eve.

1. Alice, Bob randomly agree m out of $2m$ positions to check the presence of Eve. This results in two m-position strings: the check-position string $CP = cp_1, .., cp_m$ and the message-position string $MP = mp_1, .., mp_m$.

2. Alice, Bob announce their values a_{cp_i}, b_{cp_i} at the check-positions cp_i. They check for $c_{cp_i} = a_{cp_i} \oplus b_{cp_i}$. If the number of negative checks is greater than a pre-calculated threshold then they abort the transaction.

Step 4: Creating the pads for Alice, Bob.

1. The values in m message-positions result in three m-bit pads $A\prime = A\prime_1, .., A\prime_m$, $C\prime = C\prime_1, .., C\prime_m$, $B\prime = B\prime_1, .., B\prime_m$ where Alice holds two strings $A\prime, C\prime$ and Bob holds two strings $B\prime, C\prime$. Note that if the quantum apparatus and channels are ideal then $C\prime_i = A\prime_i \oplus B\prime_i, i \in [1, m], m \sim \frac{n}{2}$.

2. From the three strings $A\prime$,$B\prime$ and $C\prime$, Alice and Bob perform the classical schemes of Error Correction and Privacy Amplification to obtain A, B and C that hold $C = A \oplus B$ and Eve has a negligible quantity of information about A and B.

Step 5: Transmitting the key K.

1. Alice creates the random key K that has the same length of A, B and C. She sends $K \oplus A \oplus C = K \oplus B$ to Bob.

2. Bob receives $K \oplus B$, computes $K \oplus B \oplus B$ to obtain K.

11.2.3 Security

Notice that at Step 3, the error-rate in the check positions must behave like that in the message positions. Indeed, since Eve does not know in advance the choices of check-positions

[1] Alice and Bob must discard one position if the number of remaining positions is odd.

and message-positions that are randomly chosen, she cannot treat the pairs $(|ra_i\rangle, |rb_i\rangle)$ differently .

Our proof is inspired by the BB84 security proof of Bennett *et al.* presented in [11]. We will prove that all the quantum attacks of Eve that can avoid detection are the ones that give no information. We transform the QUB model to a two-party communication model as follows. This is a communication between Boris and Anne. Boris plays the roles of Alice and Bob. Anne plays the role of Carol. Boris and Anne perform Steps 1, 2 and 3 of the QUB protocol. Obviously, the eavesdropping detection of Boris is equivalent to that of Alice and Bob in the QUB protocol.

After Step 2 (sifting) has been finished, Boris (Alice and Bob) and Anne (Carol) work only on the qubit pairs (one qubit from Alice, another qubit from Bob) that have component qubits prepared in a common basis. Such a pair is one of eight states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, $|\widetilde{00}\rangle$, $|\widetilde{01}\rangle$, $|\widetilde{10}\rangle$, $|\widetilde{11}\rangle$. Assume that $|xy\rangle$ is one of these pairs which is sent from Boris in Step 1. Anne receives $|xy\rangle$, uses the quantum circuit (see Fig. 10.2) to obtain two classical values that contain no more than one classical bit $x \oplus y$. When Anne sends both of these values to Boris, this is equivalent to the case in which, although Anne does not know the basis, she successfully prepares and sends the qubit $|x \oplus y\rangle$ to Boris. Boris receives $|x \oplus y\rangle$ at the end of Step 1. He measures this qubit in the appropriate basis to get $x \oplus y$ and uses $x \oplus y$ to check the presence of Eve at Step 3.

Eve could have full control over Anne's site. Assume that Eve also has a quantum computer. We denote all Eve's quantum transformations (not only on channels but also on Anne's site) by the unitary operator U. Denote by $|E\rangle$ the probing quantum state of Eve. Assume that $|uv\rangle$ is another pair sent by Boris such that $|xy\rangle$ and $|uv\rangle$ are non-orthogonal, e.g. $|xy\rangle = |00\rangle$ and $|uv\rangle = |\widetilde{00}\rangle$. In order to avoid the detection of Boris, the transformations U and the probe $|E\rangle$ must leave the returning states $|x \oplus y\rangle$ and $|u \oplus v\rangle$ undisturbed. That means,

$$U\big(|xy\rangle|E\rangle\big) \mapsto |x \oplus y\rangle|E_1\rangle \text{ and } U\big(|uv\rangle|E\rangle\big) \mapsto |u \oplus v\rangle|E_2\rangle$$

where $|E_1\rangle$, $|E_2\rangle$ are two normalized quantum states of Eve. Since U is unitary, we have:

$$\langle x \oplus y|u \oplus v\rangle = \langle E_1|\langle x \oplus y|u \oplus v\rangle|E_2\rangle = \langle x \oplus y|u \oplus v\rangle\langle E_1|E_2\rangle$$

Since $|xy\rangle$ and $|uv\rangle$ are prepared in two non-orthogonal bases $|+\rangle$ and $|\times\rangle$, $|x \oplus y\rangle$ and $|u \oplus v\rangle$ are non-orthogonal. That means $\langle x \oplus y|u \oplus v\rangle \neq 0$. Thus, $\langle E_1|E_2\rangle$ must be 1. On

the other hand, $|E_1\rangle$ and $|E_2\rangle$ are normalized. Hence, $|E_1\rangle = |E_2\rangle$. That means that Eve cannot distinguish $|xy\rangle$ from $|uv\rangle$ by her probe. In other words, all the quantum attacks by Eve that can avoid detection are the ones that give no information. This is what we have to prove.

Besides quantum attacks, Eve could also attack classical information. However, the sole information that she could get is the classical value $x \oplus y$ revealed at Carol's site. Fortunately, Eve cannot derive the two pieces of information x and y from the global information $x \oplus y$. The key transmission at Step 5 is unconditionally secured since we use the one-time pad unbreakable scheme. Therefore, our protocol is as unconditionally secure as the original QKD protocols.

11.3 Quantum Untrusted Relay (QUR) Model

11.3.1 Model description

The QUR model needs entangled-photon sources. Between the origin Alice and the destination Bob we arrange N Carols $(C_1, .., C_N)$ and $N + 1$ Bells $(B_1, .., B_{N+1})$ as described in Fig. 11.2. This creates $2N + 2$ segments. The concrete value of N depends on the distance between Alice and Bob. Without loss of generality, we assume that the lengths of $2N$ segments are the same and the common length allows quantum devices to work correctly and effectively.

Carols, $C_1, .., C_N$, have the same role as the untrusted bridge Carol in the QUB model. This means that Eve could have full control of these sites. As in the original QKD schemes, we must assume that there is an authenticated classical between Alice and Bob to defeat "man-in-middle" attacks. As in the QUB model, the task is how to design a protocol that allows, in the one hand, to effectively detect malicious operations over key transmissions from Alice to Bob, and on the other hand, to keep in secret the proper partial values of Alice and Bob. We will follow the idea of the QUB model: (i) using unknown quantum states to protect information, (ii) the sole information that is revealed outside Alice and Bob is the global information (XOR value) from which Eve cannot correctly deduce the partial pieces of information.

11.3.2 The QUR protocol

For convenience, we also use C_0 and C_{N+1} to denote Alice and Bob, respectively. The QUR protocol consists of 5 steps:

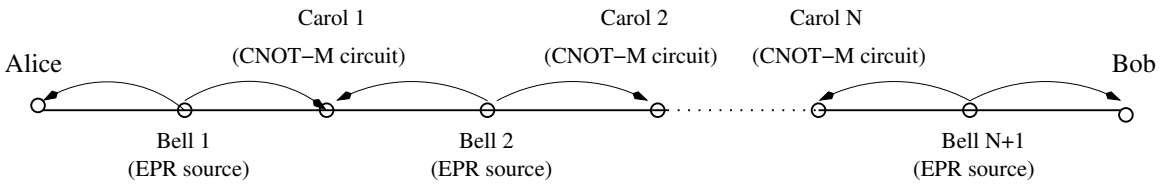


Figure 11.2: Bell 1,.., Bell N are EPR-pair sources. Carol 1, .., Carol N act as Carol in the QUB protocol.

Step 1: Preparing, exchanging, and measuring qubits.

1. Each B_i, $i \in [1, N+1]$, prepares n Bell states $(|\Phi^+\rangle)^n$.
2. Each B_i, $i \in [1, N+1]$, sends the first half of each Bell state to C_{i-1} (the previous), the second half to C_i (the next).
3. Alice (or C_0) and Bob (or C_{N+1}), each one receives n qubits. They randomly and independently choose bases to measure their qubits.
4. Each C_i, $i \in [1, N]$, receives $2n$ qubits from B_i and B_{i+1} in a synchronous manner. That means that she receives n times, and for each time she leads the qubit from B_i and the qubit from B_{i+1} to the first and second inputs of the CNOT-M circuit (see Fig. 10.2). *Then, she sends the pair of two classical output values to Alice and Bob.*
5. *The roles of $B_1, .., B_{N+1}, C_1, .., C_N$ stop here.*

Step 2: Sifting.

1. Alice and Bob announce their bases.
2. If their bases are different at the position i then Alice and Bob discard this position.
3. For each remaining position i, Alice and Bob do on N pairs received from $C_1, .., C_N$ as follows. For each of N pairs, they keep only either the first value or the second value if their common basis is $|\times\rangle$ or $|+\rangle$, respectively.
4. The values of the remaining positions result in $N+2$ $2m$-bit [2] strings $a = a_1, .., a_{2m}$; $c(i) = c(i)_1, .., c(i)_{2m}$ where $i \in [1, N]$; $b = b_1, .., b_{2m}$. Alice holds $N+1$ string $a, c(1), .., c(N)$ and Bob holds $N+1$ string $b, c(1), .., c(N)$. These $N+2$ strings should hold $\oplus_{i=1}^{N} c(i)_j = a_j \oplus b_j, j \in [1, 2m], 2m \sim \frac{n}{2}$.

[2] Alice and Bob must discard one position if the number of remaining positions is odd.

Step 3: Checking for the presence of Eve.

1. Alice and Bob randomly agree m out of $2m$ positions to check the presence of Eve. This results in two m-position strings: the check-position string $CP = cp_1, .., cp_m$ and the message-position string $MP = mp_1, .., mp_m$.

2. Alice and Bob announce values in check-position $a = a_{cp_1}, .., a_{cp_m}$; $b = b_{cp_1}, .., b_{cp_m}$; $c(i) = c(i)_{cp_1}, .., c(i)_{cp_m}$ where $i \in [1, N]$. They check for $\oplus_{i=1}^{N} c(i)_{cp_j} = a_{cp_j} \oplus b_{cp_j}$. If the number of negative checks is greater than a pre-calculated threshold then they abort the protocol.

Step 4: Creating the pads for Alice and Bob.

1. The values in m message-positions result in $N + 2$ m-bit pads $Q^A = Q_1^A, .., Q_m^A$; $Q^{C(i)} = Q_1^{C(i)}, .., Q_m^{C(i)}$ where $i \in [1, N]$; and $Q^B = Q_1^B, .., Q_m^B$ where Alice keeps $N+1$ pads $Q^A, Q^{C(1)}, .., Q^{C(N)}$ and Bob keeps $N + 1$ pads $Q^B, Q^{C(1)}, .., Q^{C(N)}$. Note that if the quantum apparatus and channels are ideal then these pads hold $\oplus_{i=1}^{N} Q^{C(i)} = Q^A \oplus Q^B$.

2. Alice and Bob compute $Q^C = \oplus_{i=1}^{N} Q^{C(i)}$. From the 3 strings Q^A, Q^B, Q^C, Alice and Bob perform the classical schemes of Error Correction and Privacy Amplification to obtain P^A, P^B and P^C that hold $P^C = P^A \oplus P^B$ and Eve has a negligible quantity of information about P^A and P^B.

Step 5: Transmitting the key K.

1. Alice creates the random key K that has the same length of P^A, P^B and P^C. She sends $K \oplus P^A \oplus P^C$ to Bob.

2. Bob receives $K \oplus P^A \oplus P^C$, computes $K \oplus P^A \oplus P^B \oplus P^C = K$.

11.3.3 Correctness

One can claim that it is true that $\bigoplus_{i=1}^{N} c(i)_j = a_j \oplus b_j, j \in [1, 2m], 2m \sim \frac{n}{2}$ at the end of Step 2 (sifting). We will show that this statement is true.

We observe the process that creates a common bit (at position j) for Alice and Bob. The input are $N + 1$ EPR pairs from $N + 1$ Bell's sites. Besides, Alice and Bob must

measure the received qubits in one common basis. The Bell state at the site Bell i (B_i) can be represented as (up to $\frac{1}{\sqrt{2}}$)

$$|\Phi^+\rangle_{B_i^{(1)}B_i^{(2)}} = \sum_{n=0}^{1} |n,n\rangle_{B_i^{(1)}B_i^{(2)}} = \sum_{n=0}^{1} |\tilde{n},\tilde{n}\rangle_{B_i^{(1)}B_i^{(2)}} \tag{11.1}$$

where $B_i^{(1)}(B_i^{(2)})$ is the first (second) qubit of Bell i, $\{|0\rangle,|1\rangle\}$ and $\{|\tilde{0}\rangle,|\tilde{1}\rangle\}$ denote the bases $|+\rangle$ and $|\times\rangle$, respectively. Note that (also up to $\frac{1}{\sqrt{2}}$)

$$|n\rangle = \sum_{m=0}^{1} (-1)^{nm}|\tilde{m}\rangle, \quad |\tilde{n}\rangle = \sum_{m=0}^{1} (-1)^{nm}|m\rangle \tag{11.2}$$

Initially, the global state is

$$|\Psi_0\rangle = \otimes_{i=1}^{N+1} |\Phi^+\rangle_{B_i^{(1)}B_i^{(2)}} \tag{11.3}$$

where $\otimes$ denotes the tensor product.

Using (11.1) we can re-write (11.3) in basis $|+\rangle$ as

$$|\Psi_0\rangle = \sum_{\{n_i\}=\mathbf{0}}^{\mathbf{1}} \otimes_{i=1}^{N+1} |n_i,n_i\rangle_{B_i^{(1)}B_i^{(2)}} \tag{11.4}$$

or in basis $|\times\rangle$ as

$$|\Psi_0\rangle = \sum_{\{n_i\}=\mathbf{0}}^{\mathbf{1}} \otimes_{i=1}^{N+1} |\widetilde{n_i},\widetilde{n_i}\rangle_{B_i^{(1)}B_i^{(2)}} \tag{11.5}$$

After distributing the qubits: $B_1^{(1)} \to C_0(A)$, $B_i^{(2)} \to C_i$, $B_{i+1}^{(1)} \to C_i$ (for $i = 1,..,N$), $B_{N+1}^{(2)} \to C_{N+1}(B)$, we have

$$|\Psi_0\rangle = \sum_{\substack{\{n_i\}=\mathbf{0},\\ n_{N+1}=0}}^{\mathbf{1},1} |n_1\rangle_A \Big(\otimes_{i=1}^{N} |n_i,n_{i+1}\rangle_{C_i^{(1)}C_i^{(2)}} \Big) |n_{N+1}\rangle_B \tag{11.6}$$

in basis $|+\rangle$ or

$$|\Psi_0\rangle = \sum_{\substack{\{n_i\}=\mathbf{0},\\ n_{N+1}=0}}^{\mathbf{1},1} |\widetilde{n_1}\rangle_A \Big(\otimes_{i=1}^{N} |\widetilde{n_i}, \widetilde{n_{i+1}}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |\widetilde{n_{N+1}}\rangle_B \tag{11.7}$$

in basis $|\times\rangle$.

After all the C_i perform the CNOT on their qubit pairs, (11.6) and (11.7) become

$$\begin{aligned} |\Psi_1\rangle &= \sum_{\substack{\{n_i\}=\mathbf{0},\\ n_{N+1}=0}}^{\mathbf{1},1} |n_1\rangle_A \Big(\otimes_{i=1}^{N} |n_i, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |n_{N+1}\rangle_B \\ &\equiv \sum_{\{n_i, n_{N+1}, m_i\}=\mathbf{0}}^{\mathbf{1}} |n_1\rangle_A \otimes \Big(\otimes_{i=1}^{N} (-1)^{n_i m_i} |\widetilde{m_i}, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |n_{N+1}\rangle_B \end{aligned} \tag{11.8}$$

or

$$\begin{aligned} |\Psi_1\rangle &= \sum_{\substack{\{n_i\}=\mathbf{0},\\ n_{N+1}=0}}^{\mathbf{1},1} |\widetilde{n_1}\rangle_A \Big(\otimes_{i=1}^{N} |\widetilde{n_i \oplus n_{i+1}}, \widetilde{n_{i+1}}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |\widetilde{n_{N+1}}\rangle_B \\ &\equiv \sum_{\{n_i, n_{N+1}, m_{i+1}\}=\mathbf{0}}^{\mathbf{1}} |\widetilde{n_1}\rangle_A \otimes \Big(\otimes_{i=1}^{N} (-1)^{n_{i+1} m_{i+1}} |\widetilde{n_i \oplus n_{i+1}}, m_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |\widetilde{n_{N+1}}\rangle_B \end{aligned} \tag{11.9}$$

In case both of Alice and Bob measure their qubits in basis $|+\rangle$, while each C_i measures her qubits $C_i^{(1)}$ and $C_i^{(2)}$ in $|\times\rangle$ and $|+\rangle$ respectively, Eq. (11.8) collapses into (up to a global phase factor)

$$\psi_1 = |n_1\rangle_A \Big(\otimes_{i=1}^{N} |\widetilde{m_i}, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |n_{N+1}\rangle_B \tag{11.10}$$

where n_1, m_i, n_i, n_{i+1} and n_{N+1} randomly take on either 0 or 1. Obviously, the outcome of $C_i^{(2)}$ yields $\oplus_{i=1}^{N}(n_i \oplus n_{i+1}) = n_1 \oplus n_2 \oplus n_2 \oplus .. \oplus n_N \oplus n_N \oplus n_{N+1} = n_1 \oplus n_{N+1}$.

In case both of Alice and Bob measure their qubits in basis $|\times\rangle$, while each C_i always

does as before, Eq. (11.9) collapses into (up to a global phase factor)

$$\psi_1 = |\widetilde{n_1}\rangle_A \Big(\otimes_{i=1}^{N} |n_i \widetilde{+ n_{i+1}}, m_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |\widetilde{n_{N+1}}\rangle_B \tag{11.11}$$

where n_1, m_i, n_i, n_{i+1} and n_{N+1} randomly take on either 0 or 1. Obviously, the outcome of $C_i^{(1)}$ yields again $\oplus_{i=1}^{N}(n_i \oplus n_{i+1}) = n_1 \oplus n_{N+1}$.

Note that $n_1, n_{N+1}, n_i \oplus n_{i+1}$ are outcomes of Alice, Bob, and Carol C_i, respectively. Thus, the equation stated at the end of Step 2 is true.

11.3.4 Security

We now prove that the QUR protocol is secure. We observe the process that creates a common classical bit for Alice and Bob. The inputs of this process are: (i) $N+1$ EPR pairs from $B_1, .., B_{N+1}$, (ii) the measuring basis choices of Alice and Bob are coincident. Assume that Eve takes full control over all the sites $C_1, .., C_N$, $B_1, .., B_{N+1}$. As in Ref. [67], initially, we can describe the pure state prepared by Eve:

$$|u\rangle = |i_1, i_2, .., i_{N+1}\rangle |j\rangle$$

where $|i_k\rangle$ denotes the EPR pair of the B_k, $|j\rangle$ denotes an ancilla quantum state that is used as the probe of Eve.

After all the measurements have been done at the end of the step 1, Alice owns the classical a, Bob owns the classical b and $C_1, .., C_N$ produce N classical bits $c_1, .., c_N$, respectively. These classical bits hold $a \oplus b = \oplus_{h=1}^{N} c_h = c$. In the other word, Eve must present the value $c = a \oplus b$ regardless of the common basis of Alice and Bob is $|+\rangle$ or $|\times\rangle$. Thus, we have the following transformation

$$U|u\rangle = U|i_1, i_2, .., i_{N+1}\rangle|j\rangle = |\hat{a}\rangle_A |\hat{b}\rangle_B |\widehat{a \oplus b}\rangle |E\rangle \tag{11.12}$$

where the subscripts $_A$ and $_B$ stand for the qubit owners Alice and Bob, respectively. Eve owns the state $|E\rangle$ and must present to Alice and Bob the state $|\widehat{a \oplus b}\rangle$ regardless of $\hat{a}(\hat{b}) = a(b)$ or $\tilde{a}(\tilde{b})$. This implies that

$$U|u\rangle = U|i_1, i_2, .., i_{N+1}\rangle|j\rangle = |a\rangle_A |b\rangle_B |a \oplus b\rangle |E_1\rangle \tag{11.13}$$

and

$$U|u\rangle = U|i_1, i_2, .., i_{N+1}\rangle|j\rangle = |\tilde{a}\rangle_A|\tilde{b}\rangle_B|\widetilde{a \oplus b}\rangle|E_2\rangle \tag{11.14}$$

In order to avoid the detection, Eve must present to Alice and Bob the qubits $|a \oplus b\rangle$ and $|\widetilde{a \oplus b}\rangle$. From (11.13) and (11.14), we have: $\langle a \oplus b|\langle b|\langle a||\tilde{a}\rangle|\tilde{b}\rangle|\widetilde{a \oplus b}\rangle = \langle a|\tilde{a}\rangle\langle b|\tilde{b}\rangle\langle a \oplus b|\widetilde{a \oplus b}\rangle$ $= \langle E_1|\langle a \oplus b|\langle b|\langle a||\tilde{a}\rangle|\tilde{b}\rangle|\widetilde{a \oplus b}\rangle|E_2\rangle = \langle a|\tilde{a}\rangle\langle b|\tilde{b}\rangle\langle a \oplus b|\widetilde{a \oplus b}\rangle\langle E_1|E_2\rangle$.

Since $\langle a|\tilde{a}\rangle\langle b|\tilde{b}\rangle\langle a \oplus b|\widetilde{a \oplus b}\rangle \neq 0$, $\langle E_1|E_2\rangle$ must be one. In other words, the probe of Eve gives no information unless Eve makes detectable disturbances. The QUR protocol is capable of preventing quantum attacks like original QKD protocols.

From the point of view of classical attacks, the information that Eve can get is the classical value $a \oplus b$. However, Eve cannot derive two partial secrets a and b from the global information $a \oplus b$. The key transmission at the step 5 is unconditionally secure since we use the one-time pad unbreakable scheme. Therefore, our protocol is unconditionally secure as original QKD protocols.

11.4 Conclusion

We presented two novel untrusted models that relay QKD keys without reducing the security of the original QKD protocols. This can say that we improved the QKD relaying models presented in Part II: we have successfully released the "quasi-trusted" constraint on intermediate nodes. The core idea always is to combine two facts, (i) to reveal only the global classical information (XOR value) at relaying nodes, (ii) to use unknown quantum states to prevent classical secret information from malicious quantum transformations of Eve.

In order to compare the performance of the proposed QKD relaying models with previous models in the realistic condition (e.g. noisy channels, imperfect devices, etc.), we need further studies and practical experimentations. In a glance, however, we could make some following comments. We first talk about the QUB model. The originality of the QUB model is the capacity of extending the QKD range up to two times without invoking entangled photons. Although the entangled-state sources has a very important role in the quantum communication, the non-local correlation of the entanglement state is very fragile, and hard to be manipulated with today's technology. The single-state based QKD relaying model can avoid this complication, hence, it seems to very interesting to develop such relaying models. Our proposed QUB is a first step in such a development, that has a significant meaning: relaying QKD keys without entangled-state sources is feasible. ***There is no counterpart***

of our QUB model in the QKD literature.

Our QUR model allows the distribution of the secret key over long distances without invoking entanglement swapping. Although there are some common required special quantum resources (precisely, entanglement sources and the CNOT gate), ***our QUR model and the standard entanglement swapping (ES)-based quantum repeater model are distinguished.*** First, they are different from the point of view of the core idea. Indeed, while the idea of the standard ES-based model is creating *entangled-state pairs* over the entire length of key distribution, our idea is simply to combine two well-known facts:

1. Enemies cannot gain information without disturbing *unknown quantum single-states*. This is the idea of the original QKD schemes.

2. Enemies cannot infer two partial pieces of *classical* information a and b from the global *classical* information $c = a$ XOR b. This is the idea of the classical unbreakable one-time pad scheme.

From the point of view of the implementation and performance, they are different, too. Indeed,

1. Although, our CNOT-M circuit is also capable of distinguishing Bell's states, i.e. making a Bell measurement, our QUR model *does not* perform any entanglement swapping (ES) operation. As is well-known, ES will not be accomplished until one applies an appropriate Pauli rotation according to two result bits of the Bell measurement. Our QUR does not use Pauli's rotations.

2. Since the Pauli rotation is applied *after* receiving two classical bits of the Bell measurement (that costs a classical transmission), the ES-based model requires to store quantum states in a *significant time*. This is one of reasons to which the ES-based model requires quantum memory devices. In the case of our QUR model, one only needs to solve the problem of synchronization of two input quibts of the CNOT gate. Such a synchronization can be done with the lack of quantum memory devices.

3. Instead of maintaining the fragile nonlocal quantum entanglement in the entire length of key distribution, our QUR model uses classical parity to keep the correlation of a qubit pair. Obviously, our QUR model has avoided a hard requirement of the standard ES-based model since keeping classical information is trivial.

4. Our QUR protocol needs to use only *one* classical bit of the Bell measurement instead

of *two* as is the case of the standard ES-based model. This implies an important improvement of performance.

Our QUR introduces also some drawbacks compared to the standard ES-based model. Indeed, since the standard ES-based model, after each ES operation, applies the entanglement purification (EP) phase that can distill some higher-fidelity entangled ones from many lower-fidelity entangled pairs, it can theoretically achieve an arbitrary long distance in the practical noisy and lossy situations. As for our QUR model, this seems still difficult to achieve an arbitrarily long distance due to noises, losses, imperfect device and the synchronization problem at the CNOT gate. However, we can still hope that our QUR model will help to obtain longer QKD reaches compared to the capacity of the original QKD schemes. Besides, we can think also of applying quantum error correction schemes to improve the QUR's performance.

Part IV

Conclusion

Chapter 12

Conclusion

12.1 Summary of Results

The central object of study of this Dissertation is the limitation of QKD's range. We have attacked the problem from the indirect and direct approaches: on the one hand, we have investigated the possibility of building the large-scale QKD network; and on the other hand, we have directly studied new methods relaying the QKD keys without reducing the unconditional security of the original QKD protocols. Indeed, extending the range of QKD and building large-scale networks have a tight correlation: if one can solve the former then one can use it to solve the latter, and vice-versa.

In order to build the large-scale QKD networks, we have proposed a dense QKD network model that allows two arbitrary network's nodes establishing shared extremely secret keys. We have showed that the proposed QKD network is capable of keeping the unconditional security over key transmission of the original QKD schemes provided that each network's node must guarantee itself a calculable security level that makes appear the "safety percolation" phenomenon in which all the safe nodes are almost-certainly connected. Once the "safety percolation" phenomenon appears, we have proposed stochastic routing algorithms and given the formulas measuring the number of the sub-keys that need to be sent in order to obtain the final secret key.

In order to directly extend the QKD range, we have proposed the new models that allow relaying QKD keys without reducing the security of the original QKD schemes. The Quantum Quasi-Trusted Bridge (QQTB) and Quantum Quasi-Trusted Relay (QQTR) models require the intermediate nodes following honestly the key-relay protocol. In such a case, even though the malicious Eve eavesdrops the intermediate nodes, she cannot get any in-

formation about the final key. Our QQTB and QQTR models introduced some significant and interesting features compared to the previous QKD relaying models (see our partial discussions and conclusion in Sections 10.3.4, 10.4.3 and 10.5).

Our Quantum Untrusted Bridge (QUB) and Quantum Untrusted Relay (QUR) models can be considered as enhanced versions of the QQTB and QQTR models. In these models, Eve is permitted to have full control over the intermediate nodes. However, if, in order to steal information of the final key, Eve does not follow the key-relay protocol then she is detected. Otherwise, she cannot have any information about the final key. Such a situation is totally similar to that in the original QKD protocols. Our QUB and QUR models introduced some significant and interesting features compared to the previous QKD relaying models (see our partial conclusion in Section 11.4).

12.2 Suggestions for Further Exploration

Our researches have been the first steps to go toward the new potential solutions for the problem of QKD's range. Hence, many things need to done in the future.

For our proposed QKD large-scale model, the topology, effective special-purposed routing algorithms, attack strategies of Eve and application scenarios can be the new interesting subjects of study.

For our proposed QKD relaying models, an estimation of required resources in the practical case of imperfect quantum devices is of interest. A comparative study about the performance of the proposed models with that of the standard quantum repeaters based on entanglement swapping is also one of our goals. Besides, we are also interested in the evolution of our QUB model, i.e. searching for the new QKD relaying models that do not require entanglement sources.

Bibliography

[1] S. Amor, D. H. Tran, and M. Bui. A percolation based model for ATC simulation. In *Proc. of the 4th Int. Conf. on Computer Sciences, Research Innovation and Vision for the Futur (RIVF)*, pages 17–22, Vietnam, 2006.

[2] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52:3457–3467, 1995.

[3] V. Beffara and V. Sidoravius. Percolation theory. *Encyclopedia of Mathematical Physics*, pages 21–28, 2006.

[4] J. S. Bell. On the einstein podolsky rosen paradox. *Physics*, 1:195–200, November 1964.

[5] P. Bellot and M.-D. Dang. Bb84 implementation and computer reality. In *Proc. of the 2009 IEEE-RIVF Int. Conf. on Computing and Communication Technologies (IEEE-RIVF)*, Danang, Vietnam, July 2009.

[6] P. Bellot, P. Gallion, S. Guilley, and J-L. Danger. The hqnet project. `http://hqnet.enst.fr`.

[7] P. Bellot, P. Gallion, S. Guilley, and J-L. Danger. The visq project. `http://visq.enst.fr`.

[8] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[9] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physics Review Letters*, 70:1895–1899, Mars 1993.

[10] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 41:1915–1923, November 1995.

[11] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without bell's theorem. *Physics Review Letters*, 68:557–559, February 1992.

[12] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W.K. Wooters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physics Review Letters*, 76:722–725, 1996.

[13] C.H. Bennett, D.V. DiVincenzo, J.A. Smolin, and W.K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996.

[14] C.H. Bennett and S.J. Wiesner. Communication via one-and-two-particle operators on Einstein-Podolsky-Rosen states. *Physics Review Letters*, 69:2881–2884, 1992.

[15] H. Bennett, F. Bessette, G. Brassard, and L. Salvail andJ. Smolin. Experimental quantum cryptography. *Jounal of Cryptology*, 5:3–28, 1992.

[16] H. Bennett and D. DiVincenzo. Quantum computing: Towards an engineering era? *Nature*, 377:389–390, 1995.

[17] S. Bohacek, J. P. Hespanha, J. Lee, C. Lim, and K. Obraczka. Game theoretic stochastic routing for fault tolerance on computer networks. *IEEE Transaction on Parallel and Distributed Systems*, 18:1227–1240, 2007.

[18] S. Bohacek, J. P. Hespanha, and K. Obraczka. Saddle policies for secure routing in communication networks. In *Proc. of the 41st IEEE Conf. on Decision and Control*, pages 1416– 1421, Las Vegas, Nevada, USA, 2002.

[19] S. Bohacek, J. P. Hespanha, K. Obraczka, J. Lee, and C. Lim. Enhancing security via stochastic routing. In *Proc. 11th Int. Conf. on Computer Communication and Networks*, pages 58– 62, Miami, Florida, USA, 2002.

[20] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. *Lecture Note of Computer Science (LNCS)*, 765:410–423, 1994.

[21] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Physics Review Letters*, 81:5932–5935, December 1998.

[22] W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Lutherand, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons. Practical free-space quantum key distribution over 1 km. *Physics Review Letters*, 81:3283–3286, 1998.

[23] W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson. Daylight quantum key distribution over 1.6 km. *Physics Review Letters*, 84:5652–5655, 2000.

[24] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.L.A. Sloane. Quantum error correction via codes over gf(4). *IEEE Transaction on Information Theory*, 44:1369–1387, 1998.

[25] H. Chau. Practical scheme to share a secret key through an up to 27.6% bit error rate quantum channel. *Physical Review A*, 66:060302, December 2002.

[26] I.L. Chuang, R. Laflamme, P.W. Shor, and W.H. Zurek. Quantum computers, factoring, and decoherence. *Science*, 270:1633–1635, 1995.

[27] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London, series A : mathematical and physical sciences*, 454:339–354, 1998.

[28] D. Collins, N. Gisin, and H. De Riedmatten. Quantum relays for long distance quantum cryptography. *Journal of Modern Optics*, 52:735–753, March 2005.

[29] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transaction on Information Theory*, 24:339–348, May 1978.

[30] M.-D. Dang, T.-L.-T. Nguyen, Q.-C. Le, T.-M. Nguyen, and P. Bellot. Usage of secure networks built using quantum technology. In *Proc. of the 3rd Int. Conf. on Computer Sciences, Research Innovation and Vision for the Future (RIVF)*, Cantho, Vietnam, February 2005.

[31] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London, series A : mathematical and physical sciences*, 400:97–117, 1985.

[32] D. Deutsch, A. Ekert, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physics Review Letters*, 77:2818–2821, 1996.

[33] D.Gottesman, H.K-.Lo, N.Lükenhaus, and J.Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 4:325–360, 2004.

[34] E. Diamanti, H. Takesue, K. Inoue, T. Honjo, and Y. Yamamoto. Performance of various quantum key distribution systems using 1.55-mm up-conversion single photon detectors. *Physical Review A*, 72:052311, 2005.

[35] D. Dieks. Communication by epr devices. *Physics Letters A*, 92:271–272, 1982.

[36] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller. Quantum repeaters based on entanglement purification. *Physical Review A*, 59:169–181, January 1999.

[37] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, May 1935.

[38] A. Ekert. Quantum cryptography based on bell's theorem. *Physics Review Letters*, 67:661–663, August 1991.

[39] A. Ekert, P. Hayden, and H. Inamori. Basic concepts in quantum computation, November 2000. `http://arxiv.org/abs/quant-ph/0011013`.

[40] C. Elliott. Building the quantum network. *New Journal of Physics*, 4:46.1–46.12, July 2002.

[41] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J.Schlafer, and H. Yeh. Current status of the DARPA quantum network, March 2005. `http://arxiv.org/abs/quant-ph/0503058v2`.

[42] C. Elliott, D. Pearson, and G. Troxel. Quantum cryptography in practice. In *Proc. of the Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 227–238, Karlsruhe, Germany, August 2003.

[43] K. Furuta, H. Muratani, T. Isogai, and T. Yonemura. Analyzing the effectiveness of the quantum repeater, August 2006. `http://arxiv.org/abs/quant-ph/0608143v1`.

[44] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Physical Review A*, 210:151–156, 1996.

[45] N. Gisin, G. Ribordy, W. Tittle, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, 2002.

[46] C. Gobby, Z.L. Yuan, and A.J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84:3762–3764, 2004.

[47] P.M. Gorman, P.R. Tapster, and J.G. Rarity. Secure free-space key exchange to 1.9 km and beyond. *Journal of Modern Optics*, 48:1887–1901, 2001.

[48] G. Grimmett. *Percolation*. Springer-Verlag, second edition, 1999.

[49] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28th annual ACM Symposium on Theory of Computing (STOC)*, pages 212–219, Philadephia, Pennsylvania, USA, 1996.

[50] Guihua Zeng and Guangcan Guo. "Quantum Authentication Protocol", 2000.

[51] J. Hespanha and S. Bohacek. Preminilary results in routing games. In *Proc. of American Control Conference (ACC)*, pages 1904–1909, Virginia, USA, 2001.

[52] B. D Hughes. *Random walks and random environments*, volume 1. Oxford University Press, 1995.

[53] B. D Hughes. *Random walks and random environments*, volume 2. Oxford University Press, 1995.

[54] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, 4:43.1–43.14, 2002.

[55] K. Inoue and T. Honjo. Robustness of differential-phase-shift quanum key distribution against photon-number splitting attack. *Physical Review A*, 71:042305, 2005.

[56] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura. Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography criterion. *Japanese Journal of Applied Physics*, 43:L1217–L1219, 2004.

[57] E. Knill, R. Laflamme, and W.H. Zurek. Resilient quantum computation. *Science*, 279:342–346, 1998.

[58] C. Kurtsiefer, P. Zarda, M. Halder, P. Gorman, P. Tapster, J. Rarity, and H. Weinfurter. Long distance free-space quantum cryptography. *Proceedings of SPIE*, 4917:25–31, 2002.

[59] Q.-C. Le and P. Bellot. Enhancement of agt telecommunication security using quantum cryptography. In *Proc. of the 4th Int. Conf. on Computer Sciences, Research Innovation and Vision for the Future (RIVF)*, pages 7–16, Ho Chi Minh, Vietnam, February 2006.

[60] Q.-C. Le and P. Bellot. How to use the quantum xor gate as a relay to extend the qkd range. In *Proc. of the 4th Int. Conf. on Boolean Functions: Cryptography and Application*, Copenhagen, Denmark, May 2008.

[61] Q.-C. Le and P. Bellot. A new proposal for qkd relaying models. In *Proc. of the 17th International Conference on Computer Communications and Networks*, St. Thomas, Virgin Island, USA, August 2008.

[62] Q.-C. Le and P. Bellot. How can quasi-trusted nodes help to securely relay qkd keys. *International Journal of Network Security*, 9:233–241, 2009.

[63] Q.-C. Le, P. Bellot, and A. Demaille. On the security of Quantum Networks: a proposal framework and its capacity. In *Proc. of the Int. Conf. on New Technologies, Mobility, and Security (NTMS)*, pages 385–396, Paris, France, May 2007.

[64] Q.-C. Le, P. Bellot, and A. Demaille. Stochastic Routing in Large Grid Shaped Quantum Networks. In *Proc. of the 5th Int. Conf. on Computer Sciences, Research Innovation and Vision for the Future (RIVF)*, pages 166–174, Hanoi, Vietnam, March 2007.

[65] Q.-C. Le, P. Bellot, and A. Demaille. Towards the world-wide quantum network. In *Proc. of the 4th Information Security Practice and Experience Conference (ISPEC, LNCS 4991)*, pages 218–232, Sydney, Australia, April 2008.

[66] H. K. Lo. A simple proof of the unconditional security of quantum key distribution. *Journal of Physics A*, 34:6957–6967, September 2001.

[67] H. K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distance. *Science*, 283:2050–2056, March 1999.

[68] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Physics Review Letters*, 94:230504, 2005.

[69] U. Maurer. Secret key agreement by public discussion from common information. *IEEE Transaction on Information Theory*, 39:733–742, May 1993.

[70] U. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transaction on Information Theory*, 45:499–514, March 1999.

[71] D. Mayer. Unconditional security in quantum cryptography. *Journal of the ACM*, 48:351–406, May 2001.

[72] M.Dianati and R. Alléaume. Architecture of the secoqc quantum key distribution network. In *Proc. of 1st International Conference on Quantum, Nano, and Micro Technologies (ICQNM)*, page 13, Guadeloupe, French Caribbean, January 2007.

[73] M.Dianati and R. Alléaume. Transport layer protocols for the secoqc quantum key distribution (qkd) network. In *Proc. of 32nd Annual IEEE on Local Computer Networks*, pages 1025–1034, Dublin, Ireland, October 2007.

[74] M.Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Physics Review Letters*, 93:120501, 2004.

[75] J. Myers, T. Wu, and D. Pearson. Entropy estimates for individual attacks on the bb84 protocol for quantum key distribution. *Proceedings of SPIE*, 5436:36–47, 2004.

[76] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[77] D. Pearson. High-speed qkd reconciliation using forward error correction. In *Proc. of the 7th Int. Conf. on Quantum Communication, Measurement and Computing (QCMC)*, pages 299–302, Glasgow, UK, 2004.

[78] A. Poppe, M. Peev, and O. Maurhart. Outline of the secoqc quantum key distribution network in viena. *International Journal of Quantum Information*, 6:209–218, April 2008.

[79] Qing Xu., M. B. Costa e Silva, J-L. Danger, S. Guilley, P. Gallion, Patrick Bellot, and F. Mendieta. Towards Quantum key distribution System using Homodyne Detection with Differential Time-multiplexed Reference. In *Proc. of the 5th Int. Conf. on Computer Sciences, Research Innovation and Vision for the Futur (RIVF)*, pages 158–165, Hanoi, Vietnam, 2007.

[80] E.M. Rains. Quantum codes of minimum distance two. *IEEE Transaction on Information Theory*, 45:266–271, 1999.

[81] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physics Review Letters*, 92:057901, 2004.

[82] A. V. Sergienko. *Quantum Communications and Cryptography.* CRC Press, 2006.

[83] C. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 625–656, July,October 1948.

[84] C. Shannon. Communication theory of secrecy of systems. *Bell System Technical Journal*, 28:656–715, October 1949.

[85] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc. of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124–134, Santa Fe, New Mexico, November 1994.

[86] P.W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physics Review A*, 52:2493–2496, 1995.

[87] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997.

[88] P.W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physics Review Letters*, 85:441–444, July 2000.

[89] B. Slutsky, R. Rao, P. Sun, L. Tancevski, and S. Fainman. Defense frontier analysis of quantum cryptographic systems. *Applied Optics*, 37:2869–2878, 1998.

[90] M. van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Transaction on Information Theory*, 43:712–714, March 1997.

[91] G. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers*, 55:109–115, 1926.

[92] W.-Y.Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physics Review Letters*, 91:057901, 2003.

[93] M. Wegman and L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981.

[94] R.F. Wesner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Physical Review A*, 40:4277–4281, 1989.

[95] S. Wiesner. Conjugate coding. *SIGACT News*, 15:78–88, 1983.

[96] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Science*, 299:802–803, 1982.

[97] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54:1355–1387, October 1975.

[98] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian. Experimental quantum key distribution with decoy state. *Physics Review Letters*, 96:070502, 2006.

[99] M. Zukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Physics Review Letters*, 71:4287–4290, 1993.