一种高效的量子秘密共享方案

郭奋卓[1,2], 高 飞[1], 温巧燕[1], 朱甫臣[3]
(1. 北京邮电大学理学院, 北京 100876; 2. 西安电子科技大学综合业务网国家重点实验室, 陕西西安 710071;
3. 现代通信国家重点实验室, 四川成都 610041)

摘 要: 利用量子安全直接通信和量子密集编码的思想, 本文提出一个新的基于 GHZ三重态的高效量子秘密共享 (QSS)方案. 利用量子相干性和一个公开的比特串 K, Alice直接让 Bob和 Charlie共享其秘密消息, 而不是首先与 Bob和 Charlie建立共享的联合密钥, 再用联合密钥传输消息. 该方案中平均消耗一个 GHZ态可以共享两比特的经典信息. 我们分别给出了无噪声信道和有噪声信道情形的安全性分析, 并重点就量子直接秘密共享和量子安全直接通信之间的区别说明了协议中使用公开的 K的必要性.

关键词: 量子秘密共享; 量子安全直接通信; 密集编码; 量子直接秘密共享
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2006) 05-0883-04

A Quantum Secret Sharing Scheme with High Efficiency

GUO Fen-zhuo[1,2], GAO Fei[1], WEN Qiao-yan[1], ZHU Fu-chen[3]
(1. *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;
2. *State Key Laboratory of Integrated Services Network, Xidian University, Xi'an, Shaanxi* 710071, *China*;
3. *National Laboratory for Modern Communications, P. O. Box* 810, *Chengdu, Sichuan* 610041, *China*)

Abstract Drawing idea from the quantum secure direct communication (QSDC) and the dense coding, we propose a novel quantum secret sharing (QSS) scheme with high efficiency based on the GHZ states. Alice shares her secret message with Bob and Charlie directly using quantum correlations and a public string K, rather than shares a joint key with them and uses the joint key to transmit her message. In our scheme, a GHZ state can be used to share two bits message. We analyze the security of our scheme in the realistic and lossy channel respectively, and show it is necessary to use a public K due to the difference between quantum direct secret sharing and QSDC.

Key words quantum secret sharing; quantum secure direct communication; dense coding; quantum direct secret sharing

1 引言

假设 Alice在中国, 有一个重要任务需要在纽约执行, 在那里她有两个代理人 Bob和 Charlie, 他们可以帮助她执行此任务. 他们中至少有一人是可信的, 但 Alice不知道是谁. 经典秘密共享提供了许多处理此问题的思路. 其中最简单的办法是 Alice产生一个随机比特串 R, 计算 $M \oplus R$, 其中 M 为其消息 (任务), 单独从 R 或 $M \oplus R$ 中都得不到任何有关 M 的信息. 然后将 R 与 $M \oplus R$ 分别发给 Bob和 Charlie, 只有他们两人把各自的比特串结合在一起才能获得 Alice的消息 M. 但要想绝对安全地将 R 与 $M \oplus R$ 发给 Bob和 Charlie, Alice必须借助经典一次一密算法, 也即 Alice必须首先与 Bob和 Charlie建立安全的与消息等长的密钥. 量子密钥分发 (QKD)提供了获得无条件安全密钥的方法[1~3]. 将 QKD与上述简单的经典秘密共享相结合可以实现无条件安全的量子秘密共享 (QSS). 但正如文献 [4]所说, 这样直接结合效率很低.

为了简化上述混合方案, 近年来陆续出现了许多 QSS协议. 其中最早提出正式协议的是文献 [4], 假设 Alice, Bob和 Charlie共享一个 GHZ三重态序列, 三人都随机选用一对共轭基中的一个 (X 基或 Y 基)测量自己的粒子, 在公布测量基以后, 只要三人选用的基相同就能建立共享联合密钥. 这一方案无疑是很大的进步, 但理论效率只有 50%, 即平均消耗两个 GHZ态才能得到 1比特的密钥. 此

收稿日期: 2004-06-15; 修回日期: 2005-10-19
基金项目: 国家自然科学基金 (No. 60373059); 博士点基金 (No. 20040013007); 国家自然科学基金重大研究计划 (No. 90604023); 现代通信国家重点实验室基金; ISN开放基金; 北京邮电大学研究生创新基金

后,文献[7]又提出一种基于非正交纠缠态的 QSS方案,其理论效率也为 50%.对于一般的量子门限方案,文献[8~10]给出了其构造方法和条件方面的一些基本结果.此外,还有一些其他的协议,如基于多粒子纠缠态的文献[5],基于 Grover算法的文献[6]和基于纠缠交换的文献[11,12]等.最近 Guo Guo-Ping等提出一个基于直积态的 QSS方案[13],易于实现,且理论效率达到了 100%.

与所有这些协议不同,本文受量子安全直接通信(QSDC)[14,15]和密集编码[16]的启发,提出一种高效的 QSS方案,一个 GHZ态可用于共享 2比特经典信息.并且 Alice和 Bob,Charlie之间不再需要建立联合密钥,Alice直接让他们共享其秘密消息.

2 基于 GHZ三重态的高效量子秘密共享

设三粒子 GHZ态为 $G_0=1/\sqrt{2}(|0_A0_B0_C\rangle+|1_A1_B1_C\rangle)$,若对其第二个粒子做幺正变换 $U_0=I$ 或 $U_1=\sigma_x=|1\rangle\langle 0|+|0\rangle\langle 1|$,则 G_0 保持不变或变为 $G_1=1/\sqrt{2}\cdot(|0_A1_B0_C\rangle+|1_A0_B1_C\rangle)$.将 G_0 和 G_1 按后两个粒子在 Bell基下展开得:

$$G_0=1/\sqrt{2}(|x+\rangle_A|\Phi^+_{BC}\rangle+|x-\rangle_A|\Phi^-_{BC}\rangle)$$

$$G_1=1/\sqrt{2}(|x+\rangle_A|\Psi^+_{BC}\rangle-|x-\rangle_A|\Psi^-_{BC}\rangle)\quad(*)$$

其中:$|x\pm\rangle_A\equiv 1/\sqrt{2}(|0\rangle_A\pm|1\rangle_A)$,四个 Bell态为:

$|\Phi^\pm_{BC}\rangle=1/\sqrt{2}(|0\rangle_B|0\rangle_C\pm|1\rangle_B|1\rangle_C)$,

$|\Psi^\pm_{BC}\rangle=1/\sqrt{2}(|0\rangle_B|1\rangle_C\pm|1\rangle_B|0\rangle_C)$.

在文献[14]中 Deng Fu-Guo等介绍了一个基于 EPR态的 QSDC方案,该协议中分两步发送校验序列和消息序列保证了整个通信的安全,因为解码必须要同时拥有一个 EPR对中的两个粒子.基于上面(*)式中 GHZ态和 Bell态的关系,受文献[14]的启发,设计 QSS方案如下:

(1)Alice产生与消息 M 等长的随机比特串 R,并计算 $S=M\oplus R$,即 S 由 M 和 R 逐位异或得来.

(2)Alice准备一列形式为 G_0 的 GHZ三重态.并将其分为三个部分序列:留在自己手中的 A 序列,发送给 Bob的 B 序列和发送给 Charlie的 C 序列.

(3)Alice将 C 序列中的粒子发送给 Charlie并检测窃听.当 Charlie收到所有的粒子后,Alice随机选取 A 序列的一些粒子和 B 序列中相对应的粒子用于窃听检测,对这些粒子对中的两粒子进行 Bell基测量,并告知 Charlie她所选的粒子位置,Charlie沿 X 方向测量自己对应的粒子,并告知 Alice他的测量结果.Alice比较两人的测量结果.如果没有窃听,两人的结果有如下所示完全确定的相关性:

$$G'=1/\sqrt{2}(|\Phi^+_{AB}\rangle|x+\rangle+|\Phi^-_{AB}\rangle|x-\rangle),$$

即如果 Alice测量得到 $|\Phi^+\rangle$,则 Charlie得到 $|x+\rangle$,Alice得到 $|\Phi^-\rangle$,则 Charlie得到 $|x-\rangle$.如果错误比特率小于某个固定的阈值,协议继续.

(4)Alice将 B 序列中剩余的粒子编码后发送给 Bob,同时将上一步中用于检测窃听的 B 序列中的粒子随机穿插在编码的粒子中发送给 Bob,用于在下一步检测窃听.Alice将 S 依次分为若干单元,每单元 2比特.根据 S,Alice决定对要编码的粒子做 U_0 还是 U_1 变换,然后发送给 Bob.若 S 中的单元为 00或者 01,则做 U_0 变换;若为 10或者 11,则做 U_1 变换.也就是说 U_0 对应 0,U_1 对应 1,它们所对应的都是 S 中每个单元的第一比特.这里 Alice必须记住穿插的用于下一步检测窃听的粒子位置.

(5)Alice和 Bob检测窃听.当 Bob收到所有的粒子后,Alice告诉他用于检测窃听的粒子位置.Alice和 Bob都沿 Z 方向测量这些粒子,Bob告诉 Alice自己的测量结果.Alice比较两人的测量结果是否满足既定的相关性.在第(3)步测量完后,Alice和 Bob的对应粒子处于 Bell态 $|\Phi^+\rangle$或 $|\Phi^-\rangle$,所以可重新用于检测窃听.如果错误比特率小于一定的阈值,说明没有窃听.

上述步骤(3)~(5)也可以变为 Alice将 C 序列发送给 Charlie,将 B 序列按上述第(4)步编码后发送给 Bob,然后三人按文献[4]中的方法检测窃听.若错误比特率小于某个特定的阈值,则协议继续.

(6)Bob和 Charlie一起用 Bell基测量他们剩余的(即 Alice编码过消息 S 的)对应于同一 GHZ态的粒子,对应的结果 $|\Phi^+\rangle$,$|\Phi^-\rangle$,$|\Psi^+\rangle$和 $|\Psi^-\rangle$分别解码为 00,01,10和 11,得到比特串 S_1.

(7)当 Bob和 Charlie全部测量完毕后,Alice沿 X 方向测量自己剩余的粒子,并随机选取一些位置让他们公布测量结果.根据自己所作的变换和测量结果,Alice能够检测到 Bob和 Charlie测量的是否是来自于同一 GHZ态的粒子.为了保证消息的绝对安全,这里用于检测的粒子应该是前面没有编码 S 的粒子,也就是说 Alice最好在前面编码的时候留出一些粒子在这里检测窃听.

根据(*)式,Alice知道 Bob和 Charlie的解码比特串 S_1,例如,如果她对相应的 B 序列中的粒子做了 U_1 变换,且测量结果为 $|x+\rangle$,则对应 S_1 中比特为 10;若结果为 $|x-\rangle$,则对应 S_1 中比特为 11.

(8)Alice计算并公布一个公开的比特串 K.她仍然以两比特为单元对 S 与 S_1 进行划分,并根据每个单元是否相同计算得到比特串 K'.具体如下:若对应单元相同,则得到 K'中对应比特为 00;若对应单元不同,则 K'中比特为 01.(这里利用了 S 与 S_1 中每单元第一比特一定相同的性质).例如:S=00,01,11,10,01,11,S_1=00,00,10,10,01,10,则 K'=00,01,01,00,00,01.于是有 $K'=S\oplus S_1$ 和 $S=K'\oplus S_1$ 成立.又因为 $S=M\oplus R$,所以 $M=K'\oplus S_1\oplus R$.记 $K=K'\oplus R$,Alice公布 K.

(9)Bob和 Charlie通过计算 $M=K\oplus S_1$ 恢复 Alice的消息 M.

(10)Alice,Bob和 Charlie三人对 M 进行纠错.在这里

为了保持 M 的完整性, 可以采用保留校验比特的纠错码, 比如 CASCADE 码[17].

3 安全性分析

在理想情况下, 即我们假设量子信道几乎是无噪声的, 由 (*)式可知, 传输过程中的 B, C 序列中的两粒子, 在 Alice未测量自己的粒子之前, 处于两个 EPR 态的最大混合态. 在文献[18]中给出了基于 EPR 对的量子密码协议的安全性分析, 详细给出了 Eve所获得的互信息与她所引入的错误率之间的 trade-off 在本协议中, 由于传输中的两粒子处于两 EPR 对的最大混合态, 所以就一般的攻击来说比文献[18]中的情况具有更高的安全性.

其实, 信道损失较大主要是给了 Eve截获重传的的机会. Eve可以截获在第(3)步中发给 Charlie的粒子, 自己保留部分粒子, 而将其余的粒子以损失较小的信道发送给 Charlie, 只要保证 Charlie接收到的粒子符合原来的信道效率即可. 这样在 Alice给 Bob发送 B 序列粒子的时候, Eve 可以截获其中与她第一次截获的粒子相应的粒子, 而对它们进行 Bell基测量, 从而可推知 S 的部分信息, 然后在 Alice公布 K 的时候得到 M 的部分信息, 这是直接通信所不允许的. 在文献[14]中提出一个利用纠缠交换技术解决这类问题的方法, 可以避免上面提到的攻击.

下面说明 Alice为什么不能直接编码其消息 M, 其根本原因是秘密共享不同于一般的双方通信. 在秘密共享协议中, 合法通信者 Bob或 Charlie可能有一人是不诚实的, 即攻击者可能是他们两人中的一个. 不妨假设 Bob是不诚实的, 他试图自己获得消息 M 的全部或部分信息, 而使 Charlie得不到任何信息. 从上面的分析可知在第(3)步结束后, 就可以确定 C 序列的粒子安全到达了 Charlie; 在第(5)步结束后就可以确定 B 序列的粒子安全到达了 Bob, 所以对于一般的 Eve(不诚实的 Bob除外), 此协议与文献[14]具有相同的安全性. 但不诚实的 Bob此时可以执行如下攻击: 在第(6)步, 他自己准备一列处于 $|\phi^+\rangle = 1/\sqrt{2}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)$ 的 Bell态. 用每个 $|\phi^+\rangle$ 中的第一个粒子与自己从 Alice处得到的 B 序列中的粒子作 Bell基测量, 而用其中的第二个粒子与 Charlie的 C 序列中相应的粒子作 Bell基测量. 从下面四个式子所示的纠缠交换过程我们可以看到, 不管 B 序列和 C 序列的粒子本身处于哪个 Bell态, Bob通过这一纠缠交换过程都可以准确判断出来, 因为他可以得到每一次纠缠交换后的两个结果. 从而 Bob能够得到 S_1, 即得到 Alice发送的 S 的每单元的第一比特. 也就是说, 如果此时 Alice是直接对 M 编码(即假设 $M = S$), 则 Bob得到了 M 的部分信息, 而此时 Charlie得到的是四个 Bell态的随机分布, 即一串随机比特. 所以 Alice不能直接编码其消息 M. 在本协议中, 在确信他们共同测量的是来自自己的粒子后, Alice才公布 K, 他们才能得到 M, 而在此之前, 他们所能得到的是随机的 S_1.

$$|\Psi^+_{BC}\rangle\otimes|\Psi^+_{12}\rangle = 1/2(|\phi^+_{B1}\rangle\otimes|\phi^+_{C2}\rangle - |\phi^-_{B1}\rangle\otimes|\phi^-_{C2}\rangle + |\Psi^+_{B1}\rangle\otimes|\Psi^+_{C2}\rangle - |\Psi^-_{B1}\rangle\otimes|\Psi^-_{C2}\rangle)$$

$$|\Psi^-_{BC}\rangle\otimes|\Psi^+_{12}\rangle = 1/2(-|\phi^+_{B1}\rangle\otimes|\phi^-_{C2}\rangle + |\phi^-_{B1}\rangle\otimes|\phi^+_{C2}\rangle - |\Psi^+_{B1}\rangle\otimes|\Psi^-_{C2}\rangle + |\Psi^-_{B1}\rangle\otimes|\Psi^+_{C2}\rangle)$$

$$|\phi^+_{BC}\rangle\otimes|\Psi^+_{12}\rangle = 1/2(|\phi^+_{B1}\rangle\otimes|\Psi^+_{C2}\rangle + |\phi^-_{B1}\rangle\otimes|\Psi^-_{C2}\rangle + |\Psi^+_{B1}\rangle\otimes|\phi^+_{C2}\rangle + |\Psi^-_{B1}\rangle\otimes|\phi^-_{C2}\rangle)$$

$$|\phi^-_{BC}\rangle\otimes|\Psi^+_{12}\rangle = 1/2(|\phi^+_{B1}\rangle\otimes|\Psi^-_{C2}\rangle + |\phi^-_{B1}\rangle\otimes|\Psi^+_{C2}\rangle + |\Psi^+_{B1}\rangle\otimes|\phi^-_{C2}\rangle + |\Psi^-_{B1}\rangle\otimes|\phi^+_{C2}\rangle)$$

我们知道, 许多量子安全直接通信协议都是来源于量子密钥分发协议的思想, 例如文献[14]中的安全通信协议是受文献[19]的启发而提出的. 基于上述攻击, 作者发现现有的所有在通信者之间共享联合密钥的秘密共享协议都不能转化为量子直接秘密共享协议, 这说明量子直接秘密共享要比两方量子直接通信更难实现. 避开这一难点, 我们借助经典的方法实现量子"直接"秘密共享, 比较实际可行. 协议中第(7)步的检测窃听防止了不诚实 Bob的上述攻击, 即使他采用上述攻击, 只能得到随机的比特串 S_1, 而同时 Alice就能发现这种欺骗. Alice最后公布 K, 相当于公开了一次一密加密算法的密钥, 不会影响协议的无条件安全性.

4 结论

吸取 QSDC和量子密集编码的思想, 我们提出一个基于 GHZ三重态的高效量子秘密共享方案. 将一列 GHZ三重态分为三个部分序列. 利用分批传输粒子序列 B 和 C, 并三次检测窃听, 保证了协议的无条件安全性. 第一次检测窃听用过的粒子由于仍保持最大相关性, 可用于第二次检测窃听, 大大节约了资源. 在安全性分析中, 本文利用了已有量子密码协议的安全性, 并着重就量子直接秘密共享不同于量子安全直接通信的安全性做了分析. 除去用于窃听检测的粒子, 一个 GHZ三重态可以用于共享 2比特的经典消息, 如果用于在三者之间建立联合密钥, 则一个 GHZ态可以分发 2比特的密钥, 所以按引言中提到的, 也即在文献[13]中描述的理论效率, 本文方案中的效率是文献[4]中的 4倍(那里两个 GHZ态可以分发 1比特的经典密钥), 文献[13]的 2倍. 再者, 该协议不需要在通信三方之间首先建立联合密钥, 而是通过最后公开一个比特串 K, 直接让 Bob和 Charlie共享 Alice的经典消息比特, 大大简化了原来的量子秘密共享方案.

参考文献:

[1] G Brassard, et al An update on quantum cryptography [A]. Advances in Cryptology-CRYPT'84 [C]. Berlin Springer Verlag 1984, 475-480

[2] Charles H Bennett Quantum cryptography using any two non-orthogonal states[J]. Physical Review Letters, 1992

68: 3121-3124.
[3] Artur K Ekert. Quantum cryptography based on Bell's theorem [J]. Physical Review Letters, 1991, 67: 661-663.
[4] M Hillery, et al. Quantum secret sharing[J]. Physical Review A, 1999, 59: 1829-1834.
[5] GUO Fen-zhuo, WEN Qiao-yan, et al. Quantum secret sharing based on multi-particle entanglement[J]. The Journal of China Universities of Posts and Telecommunications, 2005, 12(1): 15-19.
[6] Li-Yi Hsu. Quantum secret-sharing protocol based on Grover's algorithm[J]. Physical Review A, 2003, 68: 022306.
[7] A Karlsson, et al. Quantum entanglement for secret sharing and secret splitting[J]. Physical Review A, 1999, 59: 162-168.
[8] D Gottesman. On the theory of quantum secret sharing [J]. Physical Review A, 2000, 61: 042311.
[9] Anderson C A Nascimento, et al. Improving quantum secret-sharing schemes[J]. Physical Review A, 2001, 64: 042311.
[10] R Cleve, et al. How to share a quantum secret[J]. Physical Review Letters, 1999, 83: 648-651.
[11] V Karimipour, et al. Entanglement swapping of generalized cat states and secret sharing[J]. Physical Review A, 2002, 65: 042320.
[12] 秦素娟, 刘太琳, 温巧燕. 基于纠缠交换和局域操作的量子秘密共享[J]. 北京邮电大学学报, 2005, 28(4): 74-77.
QIN Su-juan, LIU Tai-lin, WEN Qiao-yan. Quantum secret sharing based on entanglement swaping and local operation [J]. Journal of Beijing University of posts and Telecommunications, 2005, 28(4): 74-77. (in Chinese)
[13] Guo-Ping Guo, et al. Quantum secret sharing without entanglement[J]. Physics Letters A, 2003, 310: 247-251.
[14] Fu-Guo Deng, et al. Two-step quantum direct communication protocol using the EPR pair block[J]. Physical Review A, 2003, 68: 042317.
[15] Kim Boström, et al. Deterministic secure direct communication using entanglement [J]. Physical Review Letters, 2002, 89: 187902.
[16] C H Bennet, et al. Communication via one- and two-particle operators on EPR states [J]. Physical Review Letters, 1992, 69: 2881-2884.
[17] G Brassard, L Salrail. Secret-key reconciliation by public discussion[A]. Advances in Cryptology-EUROCRYPT'93 [C]. Berlin: Springer Verlag, 1993, 410-423.
[18] H Inamori, et al. Security of EPR-based quantum cryptography against incoherent symmetric attacks[J]. Journal of Physics A: Mathematical and General, 2001, 34: 6913-6918.
[19] G L Long, X S Liu. Theoretically efficient high-capacity quantum-key-distribution scheme[J]. Physical Review A, 2002, 65: 032302.

作者简介:

郭奋卓 女, 1977年生于山西省, 现为北京邮电大学博士生, 主要研究方向是密码学、量子信息、量子密码. E-mail: gfenzhuo@163.com

温巧燕 女, 1959年生于陕西省, 北京邮电大学教授, 博士生导师, 主要研究方向是密码学与信息安全.