文章编号:1001-2486(2011)05-0167-04

基于极化单光子和量子计算的量子秘密共享*

王 伟,李宏欣
(解放军外国语学院 基础部,河南 洛阳 471003)

摘 要:结合量子计算算子提出一种基于极化单光子的量子秘密共享协议。该方案可以将全部量子态用于密钥共享,借助量子置换算子和量子纠缠特性证明了方案能够有效抵抗中间人攻击,利用辅助量子态进行监视,方案能够以高概率检测特洛伊木马攻击。通过对置换算子进行高维推广,证明了方案推广到(n, n)的可行性和实用性。

关键词:量子秘密共享;置换算子;极化单光子;中间人攻击;特洛伊木马攻击
中图分类号:TP309 **文献标识码**:A

A Quantum Secret Sharing Scheme Based on Polarized Single Photons and Quantum Computation

WANG Wei, LI Hong-xin
(Department of Basis, PLA University of Foreign Languages, Luoyang 471003, China)

Abstract: With the help of quantum computation operator, a quantum secret sharing scheme based on polarized single photons is proposed. Efficiency analysis indicates that all qubits can be used in the secret sharing. With the permutation operator and quantum entanglement, the protocol can resist the middleman attack effectively. By using the auxiliary qubit, the protocol can detect the Trojan horse attack with high probability. The extension of the permutation operator shows the scheme which contains n pairs is feasible and applicable.

Key words: quantum secret sharing; permutation operator; polarized single photons; middleman attack; Trojan horse attack

量子秘密共享(Quantum Secret Sharing, 简称QSS)是量子密码研究中的一个重要方面,比经典秘密共享更容易实现无条件安全。1998年,Hillery等利用GHZ三重态的量子关联性提出第一个QSS体制[1],此后,量子秘密共享逐渐引起了人们的广泛兴趣,利用极化单光子、多粒子纠缠、量子纠错码、量子计算和连续变量量子比特的性质,人们提出了一系列量子秘密共享方案[1-7]。最初的QSS体制通常使用纠缠态以及随机选择两组测量基实现,在纠错过程中需要进行对基等操作来去掉部分无用的量子比特,因而这些协议的效率通常只有50%[1]。随后,一些提高效率的方法和技术被不断引入QSS体制,比如提前通知测量基[2]、超密编码和量子安全直接通信[8-9]等,改进后的方案除去用于检错的量子比特,理论效率达到100%,不足的是,这些协议仍然需要去掉用于检错的量子比特。我们所提出的方案从根本上解决了这一问题,通过借助量子置换算子对量子态进行变换,使得方案可以将全部量子比特用于生成共享密钥,从真正意义上实现了效率达到100%。此外,通过引入辅助量子态,可以以高概率检测特洛伊木马攻击,从而提高了方案的安全性。

1 预备知识

设m,n是正整数,且$m<n$。将秘密S在一组参与者P中进行分配,如果n个参与者按如下方式共享秘密信息S:任意m个参与者可以协同恢复S,但任意少于m个参与者都不能恢复该消息。这种密码系统称为秘密共享体制,秘密共享体制亦称为(m,n)门限方案[10]。秘密共享体制可以采用不同的方式实现,以量子物理为基础的秘密共享体制称为QSS体制,QSS借助量子物理规律保证无条件安全性[10]。QSS体制的设计思想与经典方案类似,将秘密以适当方式拆分,拆分后的每一个份额由不同的参与者管理,单个参与

* 收稿日期:2010-11-25
基金项目:国家自然科学基金资助项目(60403004)
作者简介:王伟(1963—),男,教授,硕士生导师。

者无法恢复秘密消息,只有若干个参与者一同协作,才能恢复秘密消息。

二维量子置换算子在二维量子比特上的定义为四维希尔伯特空间 H_4 上的一个线性变换,作用在基 $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ 下的矩阵设为 U,容易验证该置换算子满足 $U^4=I$。

特洛伊木马[10]是指一个预先嵌入在合法用户系统中的智能系统(装置或程序),用来摧毁特洛伊木马所寄存的系统,或者用来窃取信息并反馈给远方的分析者,分析者根据反馈的信息获取合法用户的有用信息。根据特洛伊木马的物理特性,人们将其分为经典特洛伊木马、量子特洛伊木马和混合特洛伊木马。量子密码中特洛伊木马典型的攻击方式为:攻击者利用量子信道向合法用户的系统中发送探测量子光信号,通过探测光在合法用户的装置中反射回来的信号,攻击者分析并攻击量子密码系统。

2 协议设计

结合量子置换算子和 Hadamard 变换,基于直积态,我们提出一个(2,2)门限方案。该方案要求参与者使用同一组测量基;发送方 Alice 与接收方 Bob 和 Charlie 共同确定置换算子 U,以及 2 比特串对应变换 U,U^2,U^3 和 $U^4=I$ 的选取方式,即共同确定一一映射 f: $\{00,01,10,11\}\rightarrow\{U,U^2,U^3,I\}$;协议参与者 Bob 知道发送方给自己确定的 Hadamard 变换确定方式 g_B: $\{00,01,10,11\}\rightarrow\{H,I\}$,而不知道发送方给参与者 Charlie 确定的 Hadamard 变换确定方式 g_C: $\{00,01,10,11\}\rightarrow\{H,I\}$,同样参与者 Charlie 知道发送方给自己确定的 Hadamard 变换确定方式 g_C,而不知道其发送方给 Bob 确定的 Hadamard 变换确定方式 g_B,这里 H 是指 Hadamard 变换,为了安全,映射 g 不取常值映射;而这一些对于协议以外的人员是未知的。该方案具体如下:

第 1 步:发送方 Alice 随机制备两个 $2n$ – bit 串 L 和 A(n 是任意取定的正整数)。Alice 向接收方 Bob 和 Charlie 公布比特串 L(通过经典信道公布)。

第 2 步:Alice 采用⊕基(即($|0\rangle,|1\rangle$)基)制备一个两粒子直积态 $|b_ic_i\rangle$ $(1\leqslant i\leqslant n)$,其中:以 A 中两个比特为一组,b_i,c_i 为 A 中任一组对应比特值。

第 3 步: Alice 根据 L 中与该组在 A 中相同位置的比特值对 $|b_ic_i\rangle$ 依次进行变换:首先,根据 2 比特串确定对应的变换,具体如下:00,01,10,11 分别对应变换 $U,U^2,U^3,U^4=I$(U 为前面提到的置换算子),将确定的变换作用在 $|b_ic_i\rangle$ 上得到量子态 $|b_ic_i\rangle_1$;其次再根据 L 中对应 2 比特串在映射 g_B 和 g_C 的值分别对 $|b_ic_i\rangle_1$ 的第一个和第二个量子比特做相应的 Hadamard 变换,即如果 L 中对应 2 比特串在映射 g_B 下对应 H,则对 $|b_ic_i\rangle_1$ 的第 1 个量子比特做 Hadamard 变换,具体如下:如果 L 中对应 2 比特串在映射 g_B 下对应 I,则 $|b_ic_i\rangle_1$ 的第 1 个量子比特不变;同样对 $|b_ic_i\rangle_1$ 的第 2 个量子比特的变换是根据映射 g_C 来进行的;经过对 $|b_ic_i\rangle_1$ 的两个量子比特进行选择性的 Hadamard 变换,从而得到态 $|b_ic_i\rangle_2$。

第 4 步:Alice 将变换后的量子态 $|b_ic_i\rangle_2$ 的第 1 个比特 $|b_i\rangle_2$ 发送给 Bob,第 2 个比特 $|c_i\rangle_2$ 发送给 Charlie,Bob 和 Charlie 对接收到的量子态,根据 L 对应位置的 2 比特串在映射 g_B 和 g_C 的像,做相应的 Hadamard 变换。具体办法为:如果 L 中对应位置的 2 比特串在映射 g_B 下的像是 I,则 Bob 对接收到的量子态 $|b_i\rangle_2$ 不做变换,如果像是 H,则 Bob 对接收到的量子态 $|b_i\rangle_2$ 做 Hadamard 变换;Charlie 对接收到的量子态 $|c_i\rangle_2$ 也做相应的变换,依据是 L 中对应位置的 2 比特串在映射 g_C 下的像,具体方法与 Bob 类似。最后进行⊕基检测,并保存检测值。接收结束时, Bob 和 Charlie 分别拥有比特串 $B=\{|b_1\rangle_1,|b_2\rangle_1\cdots|b_n\rangle_1\}$ 和 $C=\{|c_1\rangle_1,|c_2\rangle_1\cdots|c_n\rangle_1\}$的检测值。

第 5 步:Alice 公布纠错检测位置,Bob 和 Charlie 把纠错检测位置的检查值发回给 Alice,Alice 根据 L 对应位置的两比特值进行一定规则的变换,满足:00,01,10,11 分别对应 U^3,U^2,U,I 变换,从而得到初始态 $|b_ic_i\rangle$。Alice 根据测量结果进行纠错,如果发现出错概率大于一定阈值,则通知 Bob 和 Charlie 放弃这轮操作,再返回第 1 步;如果出错概率小于一定阈值,则通知 Bob 和 Charlie 通信成功。

第 6 步:联合共享。Bob 和 Charlie 根据比特串 L、U 变换的选择和自己拥有的比特串 $B=\{|b_1\rangle_1,|b_2\rangle_1\cdots|b_n\rangle_1\}$和 $C=\{|c_1\rangle_1,|c_2\rangle_1\cdots|c_n\rangle_1\}$的检测值,联合对方手中的检测值进行变换,方法同第 5 步,得到联合密钥 A。

3 效率和安全性

该方案最大的特点就是收发双方都采取同一种测量基,降低了应用上的成本。检错时用的量子比特可以继续用于密钥的共享,从而使量子比特利用率达到 100%,方便协议各方更好地建立

和管理联合密钥。

由于设计方案采用同步检测,有效地抵抗了内存攻击,下面只针对中间人攻击和特洛伊木马攻击进行研究。

3.1　针对中间人攻击的安全性

假定第三方 Eve 截获了 Alice 公布的比特串 L、纠错检测位置、联合测量方式,也截获了 Alice 分别发送给 Bob 和 Charlie 的量子比特,同时分别制备量子态发送给 Bob 和 Charlie,但 Eve 不知道置换算子 U,更不清楚 2 比特串对应变换 $U,U^2,U^3,U^4=I$ 的选取方式,以及 Hadamard 变换的确定方式。应该注意到置换算子 U 是 4 阶置换的一个 4 阶元,于是,4 阶置换的任何一个 4 阶元都可以作为该方案中的置换算子,根据近世代数知识,可供使用的置换算子有 3 个,Eve 选对置换的概率为$\frac{1}{3}$;在选对置换的情况下,2 比特串到变换的对应关系是{00,01,10,11}到$\{U,U^2,U^3,I\}$的一个一一对应,这种一一对应共有 24 个,于是 Eve 选对 2 比特串变换方式的概率为$\frac{1}{24}$;由于 Hadamard 变换位置的确定是二选一,Eve 选对 Hadamard 变换的概率为$\frac{1}{2}$。综上所述,Eve 成功攻击该方案的概率仅为$\frac{1}{24\times2\times3}=\frac{1}{144}$。因此,可以认为该方案能够有效抵抗中间人攻击。

由于内部的不诚实方攻击威胁要比来自外部的破坏更强,这里再对来自 Bob 或 Charlie 的窃听进行安全性分析。

不妨假设参与协议的共享者之一 Charlie 不诚实,他截获了 Alice 发给 Bob 的粒子,由于 Charlie 不知道 Bob 的粒子$|b_i\rangle_2$Hadamard 变换方式(映射 g_B),即不知道$|b_i\rangle_2$是否是$|b_i\rangle_1$经过 Hadamard 变换而得到,在恢复出$|b_i\rangle_1$时有$\frac{1}{2}$的概率会出错。因此,在检错阶段,Alice 会以高概率发现错误,从而终止操作。

3.2　针对特洛伊木马攻击的安全性

量子密码中的特洛伊木马攻击同经典密码中一样,具有很强的破坏性和隐蔽性,其攻击范围十分广泛,可以对单光子源、弱激光脉冲和连续变量量子比特等光源进行攻击,严重威胁着量子密钥分配的安全。特洛伊木马的攻击原理主要是利用显示系统的不完备,借助系统漏洞潜入系统进行探测,区分正交态是特洛伊木马最基本的能力,而且木马可以进入发送方的探测系统窃取 Bell 态的探测结果。特洛伊木马最显著的特点就是需要发送探测光信号来进行反馈,我们可以从这一点出发,利用辅助量子态来检测特洛伊木马的存在。

Alice 可以选定一个待检测的量子比特$|b_ic_i\rangle$,针对量子比特$|b_i\rangle$和$|c_i\rangle$,Alice 构造辅助量子比特$|a_b\rangle=|0\rangle$或$|a_b\rangle=|1\rangle$(等概率$\frac{1}{2}$),及$|a_c\rangle=|0\rangle$或$|a_c\rangle=|1\rangle$(等概率$\frac{1}{2}$),然后对$|a_b\rangle$和$|a_c\rangle$进行 Hadmard 变换,再对$|a_bb_i\rangle$和$|a_cc_i\rangle$进行受控非运算,最后进行幺正变换 T,即作 $T\cdot CNOT\cdot(H\otimes I)$变换,其中

$$T=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&1\\0&1&1&0\\1&0&0&-1\\0&1&-1&0\end{pmatrix}$$

分别对变换后的第 1 个量子态进行测量,根据文献[6]的结果,有 $T\cdot CNOT\cdot(H\otimes I)|a_bb_i\rangle=|a_bb_i\rangle$,$T\cdot CNOT\cdot(H\otimes I)|a_cc_i\rangle=|a_cc_i\rangle$,据此可以检测整个通信系统是否存在特洛伊木马。

综上所述,由于采用了量子置换算子、同步检测,根据需要,可以利用辅助量子监测手段,使得协议可以有效抵抗中间人攻击、内存攻击和特洛伊木马攻击。

4　协议的推广

通过对量子置换算子在 n 维量子比特空间上进一步推广定义,可以将方案由(2,2)推广到(n,n)方案。(n,n)方案同样要求参与者使用同一组测量基,参与者共同确定了置换算子 U_{2^n},n 比特串对应变换 $U_{2^n},U_{2^n}{}^2,U_{2^n}{}^3,\cdots,U_{2^n}{}^{2^n}=I$ 的选取方式,以及协议参与者本人的 Hadamard 变换确定方式 $g:\{0,1\}^n\to\{H,I\}$,不知道其他参与人员的 Hadamard 变换确定方式,而这一些对于协议以外的人员是未知的。

将 n 维量子比特空间上的量子置换算子定义为 U_{2^n},在基$|00\cdots0\rangle,|00\cdots1\rangle,\cdots,|11\cdots1\rangle$上的表示是一个 $2^n\times2^n$ 矩阵。

U_{2^n}具有方案(2,2)中 U 对基态相同的变换功能,具体操作比方案(2,2)要更复杂一些,Alice 在⊕基(($|0\rangle,|1\rangle$)基)下制备一个 n 量子比特直积态$|b_1b_2\cdots b_n\rangle$,$b_1,b_2,\cdots,b_n$ 为 A 序列中对应比特值(此时 A 和 L 比特序列长度可以适当增大到 n 的某个整数倍,同时以 n 比特长度为单位进行分析)。然后根据 L 中的比特值对$|b_1b_2\cdots b_n\rangle$

进行同(2,2)方案中规则相同的变换,后面的步骤同(2,2)方案是相同的。

假定第三方 Eve 截获了 Alice 公布的比特串 L、纠错检测位置、联合测量方式,也截获了 Alice 分别发送给各方的量子比特,同时分别制备量子态发送给对应方,但 Eve 不知道置换算子 U_{2^n},更不清楚 n 比特串对应变换的选取方式,以及 Hadamard 变换的确定方式。应该注意到置换算子 U_{2^n}是 2^n 阶置换的一个 2^n 阶元,类似于(2,2)方案的证明过程,可以认为该方案能够有效抵抗中间人攻击。同样,我们可以利用辅助量子态的检测,来抵抗特洛伊木马的攻击。

5 结论

QSS 是量子密码研究的一个重要分支,本文基于极化单光子,结合量子置换算子,提出了一种新的 QSS 协议。由于该协议采用量子置换算子、Hadmard 变换和同步检测的手段,使得方案可以有效抵抗中间人攻击和内存攻击;同时,可以借用辅助量子态检测手段,检测特洛伊木马攻击。与以往的 QSS 体制相比,该协议具有 3 个方面的优点:方案可以将全部量子比特(包括用于检错部分)用于生成共享密钥,这是很多方案没有实现的;发收方只需采取一种测量基,从而大大降低了实验和应用成本;该方案可以有效地推广到 (n,n)门限方案。

根据 QSS 方案的发展及应用趋势,在以上研究的基础上,几个方面的问题值得人们进一步研究。(1)更新量子秘密共享方案的参数问题和方案的多次使用带来的安全性问题。(2)QSS 方案在辅助量子态的共享、联合量子钞票的共享以及多方安全计算方面的进一步应用。(3)研究特殊情况下合适的共享方案,如无仲裁的秘密共享、可验证的秘密共享、带预防的秘密共享和带除名的秘密共享等。

参考文献:

[1] Hillery M, Buzek V, Berthiaume A. Quantum Secret Sharing[J]. Phys. Rev. A, 1999,59: 1829 – 1834.

[2] Guo G P, Guo G C. Quantum Secret Sharing without Entanglement[J]. Phys. Lett. A, 2003, 310: 247.

[3] Wang T Y, Wen Q Y, Chen X B, et al. An Efficient and Secure Multiparty Quantum Secret Sharing Scheme Based on Single Photons[J]. Optics Communications, 2008, 281:6130 – 6134.

[4] Deng F G, Long G L, Zhou H Y. An Efficient Quantum Secret Sharing Scheme with Einstein-Podolsky-Rosen Pairs [J]. Physics Letters A, 2005, 340: 43 – 50.

[5] Crépeau C, Gottesman D, Smith A. Approximate Quantum Error-correcting Codes and Secret Sharing Schemes [J]. Eurocrypt 2005, LNCS 3494: 285 – 301.

[6] Du J Z, Qin S J, Wen Q Y. Threshold Quantum Cryptograph Based on Grover's Algorithm[J]. Phys. Rev. A, 2007, 363: 361 – 368.

[7] Xia Y, Song J, Song H S. Quantum State Sharing Using Linear Optical Elements[J]. Optics Communications, 2008, 281: 4946 – 4950.

[8] Wang J, Zhang Q, Tang C J. Multiparty Controlled Quantum Secure Direct Commnication Using Greenberger-Horne-Zeilinger State[J]. Optics Communications, 2006, 266: 732 – 737.

[9] Deng F G. Two-step Quantum Direct Communication Protocol Using the EPR Pair Block[J]. Phys. Rev. A, 2003, 68: 042317.

[10] 曾贵华,量子密码学[M]. 北京:科学出版社,2006:195 – 196,241 – 242.