中国科学: 信息科学 2011 年 第 41 卷 第 7 期: 813–819
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

无纠缠量子秘密共享中酉操作的选择

许娟[①], 陈汉武[①*], 刘文杰[②①], 刘志昊[①]

① 东南大学计算机科学与工程学院, 南京 210096
② 南京信息工程大学计算机与软件学院, 南京 210044
* 通信作者. E-mail: hw_chen@seu.edu.cn

收稿日期: 2010–06–24; 接受日期: 2010–08–22
国家自然科学基金 (批准号: 60873101) 和江苏省自然科学基金 (批准号: BK2007104, BK2008209) 资助项目

摘要 文中针对不使用纠缠态的量子秘密共享方案, 提出了一种 Bell 态替换攻击策略, 并定量分析了当量子秘密共享方案采用常见的几种酉操作组合时, 这种攻击的最小失败概率, 从而得到酉操作的选择和 Bell 态替换攻击效果之间的若干关系. 对于量子秘密共享方案的设计和实施中, 如何选择酉操作以保证通信安全的问题, 文中的工作具有重要的指导作用.

关键词 量子秘密共享 Bell 态替换攻击 酉操作 最小失败概率

1 引言

由于量子加密的无条件安全性和窃听的可检测性, 在过去的 20 多年里, 量子加密引起了国内外科学界和工业界的研究热潮 [1−35], 并已成为计算机科学和物理中的一个重要研究方向. 量子加密将量子力学和经典密码学相结合, 利用量子物理的客观规律来保证通信的安全.

量子秘密共享是量子密码中的重要分支之一, 主要研究如何借助量子资源, 将一个秘密分拆给 n 个接收方, 并使得只有 m 个接收方 ($m \leqslant n$) 合作时才能重建这个秘密. 近 10 年来, 量子秘密共享受到了广泛的关注 [1−30]. 按目的, 量子秘密共享可分为共享经典信息 [1−12,25] 和共享量子信息 [13−18,26−28] 两种. 共享量子信息的秘密共享 (secret sharing of quantum information), 也称为量子信息拆分 (quantum information splitting), 一般采用类似于量子纠错码 [19] 或受控隐形传态 [15,16,18] 的思想, 所以必然要用到纠缠态. 而共享经典信息的量子秘密共享 (quantum secret sharing of classical information, QSSCI) 按使用的量子资源, 可分为使用纠缠态和不使用纠缠态两种. 最初的量子秘密共享方案是基于纠缠态的特性来实现秘密共享的 [20,21]. 就目前而言, 纠缠态的制备还比较困难 [22], 因此基于单粒子或乘积态的量子秘密共享方案被提了出来 [4,10,11,23,25].

在本文中, 主要关注基于单粒子来实现经典信息共享的量子秘密共享方案, 即 QSSCI 方案. 在这些方案中, 一般都使用了酉操作, 酉操作的作用是将信息编码到量子上, 或/和打乱量子态使得窃听者无法通过测量有效区分. 带有酉操作的关键步骤描述如下: Bob i 将 N 个单粒子 $|\Psi^i\rangle = \bigotimes_{k=1}^{N} |\psi_k^i\rangle$ 发送给 Bob $i+1$; Bob $i+1$ 对每个粒子执行酉操作, 然后将这些粒子 $|\Psi^{i+1}\rangle$ 发送给 Bob $i+2$. 在这个过程中, 假设 Bob i 是不诚实的, 它可以实施这样一种攻击: (1) 保留 Bob $i-1$ 发送给它的含 N 个单粒

引用格式: 许娟, 陈汉武, 刘文杰, 等. 无纠缠量子秘密共享中酉操作的选择. 中国科学: 信息科学, 2011, 41: 813–819

子的序列 $|\Psi^{i-1}\rangle$, 自己不对 $|\Psi^{i-1}\rangle$ 作任何酉操作; 同时制备 N 个 Bell 态 $|\Phi\rangle_{12}=\bigotimes_{k=1}^{N}|\phi_k\rangle_{12},|\phi_k\rangle_{12}$ 为以下 4 个 Bell 态之一:

$$|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle). \tag{1}$$

不失一般性, 这里设 $|\phi_k\rangle$ 为 $(1/\sqrt{2})(|00\rangle+|11\rangle)$. (2) 保留 Bell 态的第 1 个粒子 $|\Phi\rangle_1$, 将第 2 个粒子 $|\Phi\rangle_2$ 发送给 Bob $i+1$. (3) 在 Bob $i+1$ 发送单粒子序列给 Bob $i+2$ 的过程中, 将 $|\Psi^{i+1}\rangle$ 截获, 然后将 $|\Psi^{i-1}\rangle$ 发送给 Bob $i+2$. (4) 将 $|\Phi\rangle_{12}$ 的第 1 个粒子和 $|\Psi^{i+1}\rangle$ 结合成 N 个新的 Bell 态 $|\Phi'\rangle_{12}=\bigotimes_{k=1}^{N}|\phi'_k\rangle_{12}$, 并通过对此刻 $|\Phi'\rangle_{12}$ 的测量, (试图) 获知 Bob $i+1$ 所作的酉操作, 即编码信息. (5) 在抽样检测时, 公开宣称与 Bob $i+1$ 完全一样的操作, 以避免窃听被发现. 在本文中, 将这样的攻击称为 Bell 态替换攻击，该攻击的过程如图 1 所示. Bell 态替换攻击受到了文献 [11,24] 的启发, 但攻击方法和两者有所不同, 且更加通用. 需要补充的两点是: Bob i 可以在 Bob j 发送给 Bob $j+1(j>i+1)$ 的过程中将 $|\Psi^{j-1}\rangle$ 截获, 并将 $|\Psi^{i-1}\rangle$ 发送给 Bob $j+1$, 这样, Bob i 获得了 Bob $i+1$ 至 Bob j 所编码的全部信息; 窃听者是非法的另一方 Eve 时, 也可以进行类似的攻击. 另外, 如果每对通信者之间都进行身份验证或信息验证, 则可以起到检测是否存在类似攻击的作用. 但若验证不完全有效或不够完美, 则存在攻击不被发现的可能. 在此不再展开讨论这一点, 本文主要研究酉操作的选择和 Bell 态替换攻击效果之间的关系.

2 酉操作和 Bell 态替换攻击的关系

一个单粒子的态可能是二能级 (qubit), 三能级 (qutrit) 或多能级 (qudit) 的. 本文仅考虑量子态是二能级的情况. 对于一个二能级的量子比特来说, 对它进行的酉操作可以用一个 2×2 的矩阵 U 表示. 矩阵 U 满足酉性, 即 $U^{\dagger}U=I$. 最常用的酉操作有以下几种:

$$\begin{aligned}
I&=\begin{bmatrix}1&0\\0&1\end{bmatrix}=|0\rangle\langle0|+|1\rangle\langle1|,\\
X&=\begin{bmatrix}0&1\\1&0\end{bmatrix}=|0\rangle\langle1|+|1\rangle\langle0|,\\
Y&=\begin{bmatrix}0&1\\-1&0\end{bmatrix}=|0\rangle\langle1|-|1\rangle\langle0|,\\
Z&=\begin{bmatrix}1&0\\0&-1\end{bmatrix}=|0\rangle\langle0|-|1\rangle\langle1|,\\
H&=\frac{1}{\sqrt{2}}\begin{bmatrix}0&1\\1&0\end{bmatrix}=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\langle0|+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\langle1|.
\end{aligned} \tag{2}$$

在现有的 QSSCI 方案中, 特别是使用二能级量子态的方案中, 一般仅使用这几种酉操作, 其他酉操作很少涉及.

另外, 当 Bob i 截获到 $|\Psi^{i+1}\rangle$ 后, 将 $|\Psi^{i+1}\rangle$ 和手中 Bell 态的第一个粒子 $|\Phi\rangle_1$ 结合, 就获得了 N 个新的 Bell 态 $|\Phi'\rangle_{12}$. 如果 Bob i 能通过测量明确区分 $|\Phi'\rangle_{12}$ 的各个态, 则可成功获得 Bob $i+1$ 所编

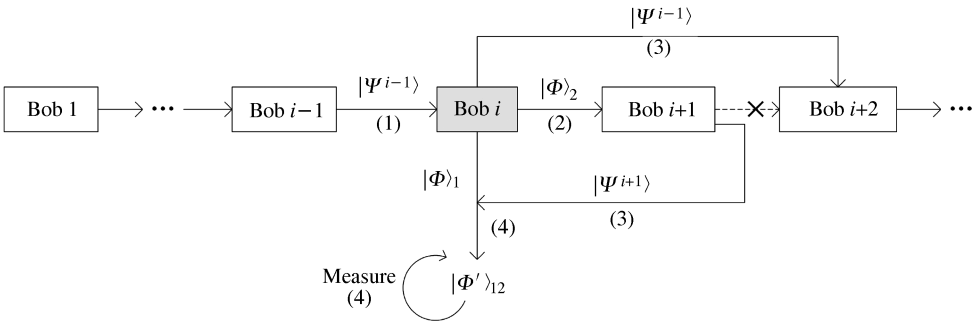

图 1 Bell 态替换攻击示意图

Figure 1 Schematic diagram of substitute-Bell-state attack

码的信息. 显然, 当 $|\Phi'\rangle_{12}$ 中各个粒子的态相互正交时, Bob i 能够成功获得 Bob $i+1$ 全部的编码信息. 此时, Bob i 不需要 Bob $i+1$ 的合作, 即可获得共享秘密. 在文献 [36] 中, 给出了明确区分任意量子态的成功概率的上界, 即

$$D \leqslant 1 - \frac{1}{n-1}\sum_{i\neq j}\sqrt{p_i p_j}|\langle\psi_i|\psi_j\rangle|. \tag{3}$$

上式中, n 表示要区分的量子态个数, ψ 表示要区分的量子态, p 表示量子态出现的先验概率. 为了分析 Bell 态替换攻击的效果, 参照区分任意量子态的成功概率 D, 给出 Bell 态替换攻击的最小失败概率 $F_{\min}$.

定义 1 设窃听者对 QSSCI 方案施行 Bell 态替换攻击. 窃听者截获光子序列后, 获得 N 个两量子态 $|\phi'_k\rangle(1 \leqslant k \leqslant N)$, 每个 $|\phi'_k\rangle$ 的先验概率为 p'_k. 定义 Bell 态替换攻击的最小失败概率 $F_{\min}$ 为

$$F_{\min} = \frac{1}{n-1}\sum_{i\neq j}\sqrt{p'_i p'_j}|\langle\phi'_i|\phi'_j\rangle|. \tag{4}$$

显然, $F_{\min}$ 表示无法明确区分量子态的最小概率, 它的值体现了量子秘密共享方案对 Bell 态替换攻击的安全程度. 因此, $F_{\min}$ 的值越大, Bell 态替换攻击的效果越差, 量子秘密共享方案对该攻击的安全性越高.

通过研究现有的基于单粒子的 QSSCI 方案可以发现, 酉操作可以分为一步 [23] 或两步 [9,12] 执行两种情况, 因此分别按这两种情况进行讨论. 首先, 假设酉操作的选择是等概率的, 且每个单粒子为以下 4 个态之一:

$$|0\rangle, |1\rangle, (1/\sqrt{2})(|0\rangle + |1\rangle) = |+\rangle, (1/\sqrt{2})(|0\rangle - |1\rangle) = |-\rangle. \tag{5}$$

定义 2 (一步酉操作) Bob $i+1$ 在将粒子序列发送给 Bob $i+2$ 之前, 仅对每个粒子执行一次随机的酉操作, 则称为是一步酉操作. Bob $i+1$ 可随机选择的酉操作叫做一个酉操作组合, 用 "{}" 表示.

文献 [23] 中 Charlie 的操作即为一步酉操作. 根据 Bob $i+1$ 所选酉操作的不同, Bob i 能成功执行 Bell 态替换攻击的概率也不同. 根据公式 (2) 中酉操作的几种常见组合, 分别计算 Bell 态替换攻击的最小失败概率 $F_{\min}$, 结果如表 1 所示.

通过表 1 可以看出, 在列出的酉操作组合中, $\{I, Y, H\}$ 组合是不能选择的; $\{I, X, H\}$, $\{I, Z, H\}$ 和 $\{I, X, Z, H\}$ 是最佳酉操作组合, 其次是 $\{I, X, Y, Z, H\}$.

表 1　一步酉操作与 Bell 态替换攻击的关系 (省略归一化和 Dirac 符号)

Table 1　Relation between one-step unitary operations and substitute-Bell-state attack (omitting normalization and Dirac symbol)

Select unitary operations	Obtained quantum states	$F_{\min}$
I, X, H	$\phi^+, \psi^+, \phi^- + \psi^+$	$\sqrt{2}/6$
I, Y, H	$\phi^+, \psi^-, \phi^- + \psi^+$	0
I, Z, H	$\phi^+, \phi^-, \phi^- + \psi^+$	$\sqrt{2}/6$
I, X, Y, H	$\phi^+, \psi^+, \psi^-, \phi^- + \psi^+$	$\sqrt{2}/12$
I, X, Z, H	$\phi^+, \phi^-, \psi^+, \phi^- + \psi^+$	$\sqrt{2}/6$
I, Y, Z, H	$\phi^+, \phi^-, \psi^-, \phi^- + \psi^+$	$\sqrt{2}/12$
I, X, Y, Z, H	$\phi^+, \phi^-, \psi^+, \psi^-, \phi^- + \psi^+$	$\sqrt{2}/10$

表 2　两步酉操作与 Bell 态替换攻击的关系 (省略归一化和 Dirac 符号)

Table 2　Relation between two-step unitary operations and substitute-Bell-state attack (omitting normalization and Dirac symbol)

Select unitary operations	Obtained quantum states	$F_{\min}$
$I, X; I, H$	$\phi^+, \psi^+, \phi^- + \psi^+, \phi^+ - \psi^-$	$\sqrt{2}/6$
$I, Y; I, H$	$\phi^+, \psi^-, \phi^- + \psi^+, \phi^- - \psi^+$	0
$I, Z; I, H$	$\phi^+, \phi^-, \phi^- + \psi^+, \phi^+ + \psi^-$	$\sqrt{2}/6$
$I, X, Y; I, H$	$\phi^+, \psi^+, \psi^-, \phi^- + \psi^+, \phi^+ - \psi^-$	$2\sqrt{2}/15$
$I, X, Z; I, H$	$\phi^+, \phi^-, \psi^+, \phi^- + \psi^+, \phi^+ = \psi^-$	$2\sqrt{2}/15$
$I, Y, Z; I, H$	$\phi^+, \phi^-, \psi^-, \phi^- + \psi^+, \phi^+ = \psi^-$	$2\sqrt{2}/15$
$I, X, Y, Z; I, H$	$\phi^+, \phi^-, \psi^+, \psi^-, \phi^- + \psi^+, \phi^+ - \psi^-, \phi^- - \psi^+, \phi^+ + \psi^-$	$\sqrt{2}/7$

定义 3 (两步酉操作)　Bob $i+1$ 在将粒子序列发送给 Bob $i+2$ 之前, 先对每个粒子执行 1 次随机的酉操作, 然后再执行 1 次, 且这次含有与第 1 次不同的酉操作, 则称为是两步酉操作. 两步酉操作的酉操作组合用 "{ ; }" 表示, 分号前面表示第 1 次可选酉操作, 分号后面表示第 2 次可选酉操作.

文献 [9,12] 中 Alice i 的操作即为两步酉操作. 根据 Bob $i+1$ 所选酉操作的不同, Bell 态替换攻击的最小失败概率 $F_{\min}$ 如表 2 所示 (仅列出了常见的几种组合).

由表 2 可知, 在列出的酉操作组合中, $\{I, Y; I, H\}$ 组合是不能选择的; $\{I, X; I, H\}$ 和 $\{I, Z; I, H\}$ 是最佳酉操作组合, 其次是 $\{I, X, Y, Z; I, H\}$.

纵观表 1 和 2, 可以得出以下结论: (1) 表 1 和 2 列出的几种常见酉操作组合中, $\{I, Y, H\}$ 和 $\{I, Y; I, H\}$ 酉操作组合在量子秘密共享方案中是绝对不能采用的. (2) 仅考虑表 1 和 2 中的几种常见酉操作组合, 则 $\{I, X, H\}$, $\{I, Z, H\}$, $\{I, X, Z, H\}$, $\{I, X; I, H\}$ 和 $\{I, Z; I, H\}$ 是最佳酉操作组合, 其次为 $\{I, X, Y, Z; I, H\}$. (3) 在一个酉操作组合中, 并不是种类越多, 对 Bell 态替换攻击的安全性就一定越高. (4) 当酉操作种类相同时, 两步酉操作相对 Bell 态替换攻击的安全程度并不是一定大于或等于一步酉操作. 例如, 选择 $\{I, X, Z; I, H\}$ 时, Bell 态替换攻击的最小失败概率比选择 $\{I, X, Z, H\}$ 时要低. (5) 一般来说, 酉操作种类增加, 编码和解码的复杂度也会相应地增加; 因此, 在对 Bell 态替换攻击安全程度相同的情况下, 应优先考虑种类少的酉操作组合.

另外需要说明的是, 为了避免 Bell 态替换攻击的完全成功, 任何参与者在利用酉操作编码时, 必须要有实现基变换的酉操作存在. 假设在基于二能级单粒子的量子秘密共享方案中, 参与者仅采用像 I,

X, Y 或 Z 这样实现比特翻转、相位翻转或两者兼有的操作, 而不采用如 H 这样使量子态在 $\{|0\rangle, |1\rangle\}$ 和 $\{|+\rangle, |-\rangle\}$ 两个共轭基之间转换的操作, 则窃听者施行 Bell 态替换攻击之后, 最终得到的两量子态必然为 $|\phi^{\pm}\rangle$ 或 $|\psi^{\pm}\rangle$, 即 4 个 Bell 态之一. 容易算出, 4 个 Bell 态是两两正交的, 且是四维 Hilbert 空间上的 1 组基, 所以窃听者使用 Bell 基测量, 即可区分最终的两量子态; 也就是说, 窃听者能够准确地获知被窃听者所作的酉操作. 显然, 这是不被允许的. 当参与者同时也随机使用 H 操作时, 窃听者最终获得的量子态也可能是相互正交的, 如 $\{I, Y, H\}$ 和 $\{I, Y; I, H\}$. 所以, 如果基于单粒子的量子秘密共享方案对 Bell 态替换攻击而言是安全的, 那么存在实现基变换的酉操作是必要条件, 但不是充分条件. 在文献 [23] 中, Alice 通过 I 或 Y 操作, 来将自己的特定信息编码到粒子上. 显然, 如果窃听者施行 Bell 态替换攻击, 将得到 $|\phi^{+}\rangle$ 或 $|\psi^{-}\rangle$, 攻击的最小失败概率 $F_{\min} = 0$, 因此该方案存在安全隐患.

3 结论

本文针对不使用纠缠态的量子秘密共享方案, 提出了一种 Bell 态替换攻击策略. 通过定义该攻击的最小失败概率, 定量分析了几种常见的酉操作组合对该攻击的安全程度, 从而给出了 Bell 态替换攻击的效果和酉操作选择之间的关系. 在量子秘密共享方案的设计和实施中, 对于选择什么样的酉操作, 本文的工作具有重要的参考和指导作用.

另外, 本文仅针对使用二能级量子态两个共轭基的情况, 对几种常见酉操作组合进行了分析, 其他更复杂的情况还有待进一步的研究.

参考文献

1 Gottesman D. Theory of quantum secret sharing. Phys Rev A, 2000, 61: 423111–423118

2 Yang C, Gea-Banacloche J. Teleportation of rotations and receiver-encoded secret sharing. J Opt B-Quant Semiclass Opt, 2001, 3: 407–411

3 Karimipour V, Bahraminasab A, Bagherinezhad S. Entanglement swapping of generalized cat states and secret sharing. Phys Rev A, 2002, 65: 42320

4 Guo G P, Guo G C. Quantum secret sharing without entanglement. Phys Lett A, 2003, 310: 247–251

5 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 52307

6 Deng F G, Long G L, Wang Y, et al. Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin Phys Lett, 2004, 21: 2097–2100

7 Deng F G, Zhou H Y, Long G L. Bidirectional quantum secret sharing and secret splitting with polarized single photons. Phys Lett A, 2005, 337: 329–334

8 Yang Y G, Wen Q Y, Zhu F C. An efficient quantum secret sharing protocol with orthogonal product states. Sci China Ser G-Phys Mech Astron, 2007, 50: 331–338

9 Gao T, Yan F L, Li Y C. Quantum secret sharing between m-party and n-party with six states. Sci China Ser G-Phys Mech Astron, 2009, 52: 1191–1202

10 Xu J, Chen H W, Liu W J, et al. An efficient quantum secret sharing scheme based on orthogonal product states. In: Proceedings of 2010 IEEE Congress on Evolutionary Computation. Barcelona, 2010. 949–952

11 Yan F L, Gao T, Li Y C. Quantum secret sharing between multiparty and multiparty with four states. Sci China Ser G-Phys Mech Astron, 2007, 50: 572–580

12 Yan F L, Gao T. Quantum secret sharing between multiparty and multiparty without entanglement. Phys Rev A, 2005, 72: 12304

13 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state Sharing. Phys Rev Lett, 2004, 92: 177901–177903

14 Li Y M, Zhang K S, Peng K C. Multiparty secret sharing of quantum information based on entanglement swapping. Phys Lett A, 2004, 324: 420–424
15 Deng F G, Li C Y, Li Y S, et al. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys Rev A, 2005, 72: 22338
16 Deng F G, Li X H, Li C Y, et al. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys Rev A, 2005, 72: 44301
17 Lance A M, Symul T, Bowen W P, et al. Continuous-variable quantum-state sharing via quantum disentanglement. Phys Rev A, 2005, 71: 33814
18 Li X H, Zhou P, Li C Y, et al. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J Phys B, 2006, 39: 1975–1983
19 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648–651
20 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
21 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59: 162
22 Wagenknecht C, Li C M, Reingruber A, et al. Experimental demonstration of a heralded entanglement source. Nat Photonics, 2010, 4: 549–552
23 Zhang Z J, Li Y, Man Z X. Multiparty quantum secret sharing. Phys Rev A, 2005, 71: 44301
24 Li C, Chang C, Hwang T. Comment on "quantum secret sharing between multiparty and multiparty without entanglement". Phys Rev A, 2006, 73: 16301
25 Yang Y G, Wen Q Y. Threshold quantum secret sharing between multi-party and multi-party. Sci China Ser G-Phys Mech Astron, 2008, 51: 1308–1315
26 Wang Y H, Song H S. Preparation of multi-atom specially entangled W-class state and splitting quantum information. Chinese Sci Bull, 2009, 54: 2599–2605
27 Zhang W, Liu Y M, Yin X F, et al. Partition of arbitrary single-qubit information among n recipients via asymmetric (n+1)-qubit W state. Sci China Ser G-Phys Mech Astron, 2009, 52: 1611–1617
28 Zuo X Q, Liu Y M, Zhang W, et al. Simpler criterion on W state for perfect quantum state splitting and quantum teleportation. Sci China Ser G-Phys Mech Astron, 2009, 52: 1906–1912
29 Hao L, Li J L, Long G L. Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. Sci China Ser Phys Mech Astron, 2010, 53: 491–495
30 Zhang X L, Ji D Y. Analysis of a kind of quantum cryptographic schemes based on secret sharing. Sci China Ser G-Phys Mech Astron, 2009, 52: 1313–1316
31 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chinese Sci Bull, 2009, 54: 2991–2997
32 Li C Z. Real application of quantum communications in China. Chinese Sci Bull, 2009, 54: 2976–2977
33 Wen H, Han Z F, Zhao Y B, et al. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network. Sci China Ser F-Inf Sci, 2009, 52: 18–22
34 Yang Y G, Wen Q Y. Threshold quantum secure direct communication without entanglement. Sci China Ser G-Phys Mech Astron, 2008, 51: 176–183
35 Xu J, Chen H W, Liu W J, et al. Efficient phase-coded quantum key distribution scheme. J Southeast Univ Nat Sci Ed, 2009, 39: 216–219
36 Zhang S Y, Feng Y, Sun X M, et al. Upper bound for the success probability of unambiguous discrimination among quantum states. Phys Rev A, 2001, 64: 62103

Selection of unitary operations in quantum secret sharing without entanglement

XU Juan[1], CHEN HanWu[1*], LIU WenJie[2,1] & LIU ZhiHao[1]

1 *School of Computer Science and Engineering, Southeast University, Nanjing* 210096*, China;*
2 *School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing* 210044*, China*
*E-mail: hw_chen@seu.edu.cn

Abstract We propose a substitute-Bell-state attack strategy for quantum secret sharing schemes without entanglement, as well as a definition of the minimum failure probability of such attack strategy. A quantitative analysis of security degrees corresponding to different unitary operations is also provided, when the secret sharing schemes without entanglement are stricken by substitute-Bell-state attack. As a result, the relation between the selection of unitary operations and the effect of substitute-Bell-state attack is shown, which can serve as an important guidance for the selection of unitary operations in designing and implementing quantum secret sharing schemes.

Keywords quantum secret sharing, substitute-Bell-state attack, unitary operation, minimum failure probability