论 文

基于高维纠缠交换的无酉操作确定性安全量子通信

刘志昊^{①*}, 陈汉武^{①*}, 刘文杰^②, 许娟^①, 李志强^③

① 东南大学计算机科学与工程学院, 南京 211189

② 南京信息工程大学计算机与软件学院, 南京 210044

③ 扬州大学信息工程学院, 扬州 225009

* 通信作者. E-mail: liuzhtopic@163.com, hw_chen@seu.edu.cn

收稿日期: 2010-09-17; 接受日期: 2010-11-25

国家自然科学基金 (批准号: 60873101, 61070240)、江苏省高校自然科学基金 (批准号: 10KJB520021)、东南大学优秀博士论文基金 (批准号: YBJJ1101) 和江苏省高校研究生科研创新计划 (批准号: CXZZ.0157) 资助项目

摘要 在分析高维 Bell 态纠缠交换基本性质的基础上, 提出不需要任何酉操作、具有通用性和一般性的高维确定性安全量子通信方案. 利用高维 Bell 测量的结果, 发送方和接收方分别进行模加、减运算即可编码、解码信息. 构造了两组互补的基, 并根据其互补性质, 提出了检测高维量子信道是否安全的方法. 详细分析了几种常用攻击策略, 并计算了这些攻击所引起的错误率, 进而推导出通信双方需设定的错误率阈值的上界.

关键词 确定性安全量子通信 高维 Bell 态 纠缠交换 高维 Bell 测量

1 引言

以微观粒子作为信息载体, 凭借量子力学特有的一些性质, 如不确定性、相干性和纠缠等, 量子安全通信能实现理论上无条件安全的通信. 它的一个重要的研究方向是量子密钥分配 (quantum key distribution, QKD), 其任务是借助量子特性来完成密钥的分配. 自从 1984 年, Bennett 和 Brassard^[1] 提出第一个量子密钥分配协议即 BB84 协议之后, 量子密钥分配的研究迅速发展, 研究者们提出了许多具有代表性的量子密钥分配协议^[2–4]. 近年来, 量子直接通信 (quantum direct communication, QDC) 作为量子安全通信的另一研究方向也被提出并受到研究者的青睐. 量子直接通信要求通信双方在事先没有共享密钥的条件下即可完成信息的安全传输, 是一种全新的安全通信模式. 量子直接通信包括量子安全直接通信 (quantum secure direct communication, QSDC) 和确定性安全量子通信 (deterministic secure quantum communication, DSQC)^[5]. 两者的区别在于: 前者在解码秘密信息中, 不需要额外的经典信息; 而后者需要额外的经典信息辅助信息解码. 在量子安全直接通信方面, Long 和 Liu^[3] 于 2002 年提出了基于量子数据块的高效量子密钥分配方案, 同样该方案亦是一个可用于量子安全直接通信的模型. 此后不久, Boström 和 Felbinger^[6] 提出了准安全的量子安全直接通信协议, 即 “Ping-pong” 协议. 但是该协议在信道传输效率低于 60% 时信息能被窃听者完全获取^[7,8], 并且不能防御拒绝服务

引用格式: 刘志昊, 陈汉武, 刘文杰, 等. 基于高维纠缠交换的无酉操作确定性安全量子通信. 中国科学: 信息科学, 2011, 41: 1474–1482

攻击^[9]、不可见光子攻击^[10]及在量子噪声信道情况下不安全^[11]. 2003 年, Deng 等^[12]提出了第一个真正安全的量子安全直接通信协议, 即“二步”协议. 此后, 许多量子安全直接通信方案不断被提出^[13–25]. 特别地, 2005 年 Wang 等^[26]提出了基于超密度编码思想利用高维 Bell 态的量子安全直接通信方案, 使得量子安全直接通信的研究推向高维情形. 在确定性安全量子通信方面, Shimizu 和 Imoto^[27]于 1999 年提出了第一个确定性安全量子通信方案. 2002 年 Beige 等^[28]亦提出了基于单光子两量子比特态的确定性安全量子通信方案. 此后, 确定性安全量子通信得到迅速发展^[25,29–36]. 2006 年 Li 等^[37]提出了基于高维单粒子态和高维单粒子酉算子的确定性安全量子通信方案. 由于纠缠交换 (entanglement swapping)^[38,39]具有优越的性质, 在量子信息中起着非常重要的作用. 一些研究者基于纠缠交换的性质提出了确定性安全量子通信协议^[40–44], 然而, 在以上所有协议中, 酉操作是必不可少的.

本文在分析高维 Bell 态纠缠交换特性的基础上, 提出不需要任何酉操作、编码和解码规则简单、具有通用性和一般性的高维确定性安全量子通信方案. 利用高维 Bell 测量的结果, 发送方进行模加运算, 接收方进行模减运算就可分别编码、解码信息. 基于一组高维单粒子测量基利用量子 Fourier 变换^[45]构造了另一组与之互补的测量基. 根据这两组基的互补性质, 提出检测高维 Bell 态安全性的方法. 文中将详细计算几种常用窃听方法对所提协议进行攻击引起的错误率, 并进一步分析得出为检测量子信道安全需设定的错误率阈值的上界. 与其他量子直接通信协议不同, 本文所提确定性安全量子通信协议不需要任何酉操作, 简化了协议实现的复杂度.

2 高维单粒子测量基及高维 Bell 态纠缠交换

在提出具体的量子通信协议之前, 先研究有关高维单粒子测量基及高维 Bell 态纠缠交换的基本性质, 这些性质是本文所提协议的理论基础.

2.1 两组高维单粒子测量基的构造及其性质

类似于二维量子系统, 在 d ($d \geq 2$) 维量子系统中, 存在一组常用的基 $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$, 称为 Z 基. 根据量子 Fourier 变换^[45], 可以构造另一组基 $\{|X_0\rangle, |X_1\rangle, |X_2\rangle, \dots, |X_{d-1}\rangle\}$, 称为 X 基, 其中, 对于 $0 \leq k \leq d-1$ 有

$$|X_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{2\pi i j k / d} |j\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \varpi^{jk} |j\rangle, \quad (1)$$

其中 $\varpi = e^{2\pi i / d}$. 显然, 当 $d=2$ 时, $\varpi = -1$.

Z 基中任一基向量 (量子状态) 和 X 基中任一基向量 (量子状态) 内积的模的平方为 $1/d$, 即有

$$|\langle i | X_j \rangle|^2 = \frac{1}{d}. \quad (2)$$

说明高维 Z 基和 X 基是互补的 (mutually complementary). 如果量子系统处在 $Z(X)$ 基中的某一基态, 此时利用互补的 $X(Z)$ 基来测量, 所得结果是完全随机的. 事实上, Z 基中任一基向量都可以用 X 基中基向量的线性组合来表示

$$|k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \varpi^{-jk} |X_j\rangle. \quad (3)$$

2.2 高维 Bell 态纠缠交换

在 $d \times d$ 维双量子系统中, d 维 Bell 态是处于最大纠缠的量子对, 表示为

$$|\psi_{nm}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jn} |j\rangle |(j+m) \bmod d\rangle, \quad (4)$$

其中, $d \geq 2, 0 \leq n, m \leq d-1$. 很显然在 $d \times d$ 维双量子系统中共有 d^2 个 d 维 Bell 态, 它们构成一组正交基, 称为 d 维 Bell 基.

当 $n=0$ 和 $m=0$ 时, 可以得到

$$|\psi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle |j\rangle. \quad (5)$$

同样可以将高维 Bell 态 $|\psi_{00}\rangle$ 表示成高维 X 基的形式, 即

$$|\psi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |X_i\rangle |X_{(d-i) \bmod d}\rangle. \quad (6)$$

公式 (5) 和 (6) 说明, 如果对高维 Bell 态中两个粒子都选择 Z 基 (或 X 基) 进行测量, 则测量结果是相关的, 否则, 对一个粒子选择 Z 基, 另一个粒子选择 X 基进行测量, 则测量结果是无关的.

假设 Alice 和 Bob 相距很远且他们共享 d 维 Bell 态 $|\psi_{00}\rangle_{1,2}$ 和 $|\psi_{00}\rangle_{3,4}$, 其中 Alice 拥有粒子 1 和 3, Bob 拥有粒子 2 和 4. 通过适当的数学推导, $|\psi_{00}\rangle_{1,2}$ 和 $|\psi_{00}\rangle_{3,4}$ 的张量积态可用如下公式表示:

$$|\psi_{00}\rangle_{1,2} |\psi_{00}\rangle_{3,4} = \frac{1}{d} \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} |\psi_{ij}\rangle_{1,3} |\psi_{(d-i) \bmod d, j}\rangle_{2,4}. \quad (7)$$

如果 Alice 对粒子 1 和 3 进行 Bell 测量, 将有 $1/d^2$ 的概率得到测量结果 $|\psi_{ij}\rangle_{1,3}$, 此时粒子对 2 和 4 将构成 d 维 Bell 态 $|\psi_{(d-i) \bmod d, j}\rangle_{2,4}$, 使得原本纠缠的粒子对 (1,2) 和 (3,4) 的纠缠打破, 而使原本没有关联的两粒子对 (1,3) 和 (2,4) 分别纠缠, 这种现象称为 d 维 Bell 态的纠缠交换.

3 高维确定性安全量子通信

不失一般性, 设 Alice 为发送方, 打算传输一串 d 维秘密信息给接收方 Bob. 为了在逻辑上更清晰, 将协议分成两阶段: 第一阶段为纠缠粒子传送过程, 第二阶段为信息传送过程.

3.1 纠缠粒子传送过程

(1) Alice 制备 $2N$ 对 d 维 Bell 态 $|\psi_{00}\rangle$, 并将这些粒子组成序列 P 和 S , 其中 P 序列中第 j 个粒子 $P(j)$ 与 S 序列中第 j 个粒子 $S(j)$ 来源于同一 Bell 态.

(2) Alice 保留粒子序列 P 并将 S 传送给 Bob, 并将这一事实告知 Bob.

(3) Bob 随机选择 S 序列中 $2M$ ($M \ll N$ 且取 M 足够大以致能够分析出传输序列 S 的错误率) 个粒子作为检测粒子, 并告知 Alice 所选粒子的位置, 然后随机选择 d 维 Z 基 $\{|0\rangle, |1\rangle, |2\rangle, \dots, |d-1\rangle\}$ 或 d 维 X 基 $\{|X_0\rangle, |X_1\rangle, |X_2\rangle, \dots, |X_{d-1}\rangle\}$ 对检测粒子进行测量. 测量完成后, Bob 告知 Alice 对每个检测粒子进行测量所选择的测量基及测量结果.

(4) Alice 采用相同的测量基对序列 P 中相应位置的粒子进行测量, 并公开和 Bob 比较测量结果. 根据公式,

$$|\psi_{00}\rangle_{1,2} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_1 |i\rangle_2 = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |X_i\rangle_1 |X_{(d-i) \bmod d}\rangle_2, \quad (8)$$

可知在不存在信道噪声和窃听的理想情况下: (1) 若 Alice 和 Bob 选择 d 维 Z 基作为测量基, 那么她们的测量结果相同, 即若 Alice 的测量结果为 $|i\rangle$, Bob 的测量结果必然为 $|i\rangle (0 \leq i \leq d-1)$; (2) 若 Alice 和 Bob 选择 d 维 X 基作为测量基, 如果 Alice 的测量结果为 $|X_i\rangle$, 那么 Bob 的测量结果必为 $|X_{(d-i) \bmod d}\rangle (0 \leq i \leq d-1)$. 从而, 若存在信道噪声或窃听, Alice 和 Bob 可以检测出传输粒子序列 S 的错误率: 如果错误率超过某个阈值 ε_{th} , 通信双方放弃本次通信; 否则, 执行后续的信息传送过程.

3.2 信息传送过程

设序列 P 和 S 丢弃检测粒子后组成有序粒子序列分别为 P' 和 S' . 很显然序列 P' 和 S' 中对应位置的两粒子组成高维 Bell 态 $|\psi_{00}\rangle$. Alice 和 Bob 分别将序列 P' 和 S' 相邻位置的两粒子组成一个小组, 即粒子对. 则序列 P' 和 S' 可表示为 $\{[P'(1), P'(2)], \dots, [P'(2N-2M-1), P'(2N-2M)]\}$ 和 $\{[S'(1), S'(2)], \dots, [S'(2N-2M-1), S'(2N-2M)]\}$. 另设 Alice 要传送一串 $2(N-M)$ 位的 d 维信息, 表示为 $\{(k_1, l_1), \dots, (k_{N-M}, l_{N-M})\}$.

(1) Alice 对 P' 中每一小组进行 d 维 Bell 测量, 然后将测量结果与要传输的信息相加 (模 d), 并公开相加后的值. 例如, 假设 Alice 对第 n 个粒子对 $[P'(2n-1), P'(2n)]$ 进行 d 维 Bell 测量的结果为 $|\psi_{i_n j_n}\rangle$ (用 (i_n, j_n) 标识), 则 Alice 公开 x_n 和 y_n , 其中 $x_n = (k_n + i_n) \bmod d$, $y_n = (l_n + j_n) \bmod d$. 由于 Alice 的测量结果 (i_n, j_n) 是完全随机的, (x_n, y_n) 亦是完全随机的.

(2) Bob 对序列 S' 中每一粒子对进行 d 维 Bell 测量, 并根据 Alice 公开的信息解码秘密信息. 例如, 设 Bob 第 n 个粒子对的测量结果为 $|\psi_{p_n q_n}\rangle$, 根据式 (7) 可知, 必有 $p_n = (d - i_n) \bmod d$ 和 $q_n = j_n$. 于是, Bob 可以根据如下规则来解码 Alice 传送的信息 (k_n, l_n) :

$$\begin{cases} k_n = (x_n + p_n) \bmod d, \\ l_n = (y_n - q_n) \bmod d. \end{cases} \quad (9)$$

在无关的第三方看来 x_n 和 y_n 的值是随机的, 而对于 Bob 来说却可以用来解密 Alice 的秘密信息.

4 安全性分析

所提确定性安全量子通信协议分成前后两阶段, 即纠缠粒子传送过程和信息传送过程. 一方面, 只有保证了传送粒子的安全, 才进行后续的信息传送过程. 只要纠缠粒子传送过程不安全, 整个量子通信过程将中止, 不会进行后续的信息传送过程, 且纠缠粒子在传送过程中不携带任何秘密信息, Eve 将毫无所获. 另一方面, 量子传输信道如果是安全的, 即保证了高维纠缠粒子传送过程的安全, 在后续的信息传送过程中, 不再需要在量子信道中传送任何信号, Eve 也就无法从此过程中主动获得信息.

从所提协议可知, Alice 和 Bob 选用两种互补基 (Z 基和 X 基) 对检测粒子进行检测来分析传输粒子的错误率, 从而确定量子信道是否安全. 下面我们将对 3 种常用的攻击类型进行分析, 求出 Eve 引起的错误率, 进而分析错误率阈值 ε_{th} 的上界.

4.1 截获重发 (intercept-and-resend) 攻击

在此种攻击策略中, 窃听者 (Eve) 截获并测量从 Alice 发给 Bob 的粒子, 然后根据测量结果制备一新的状态传给 Bob. 为了便于分析, 假设 Alice 和 Bob 随机选择 d 维 Z 基和 d 维 X 基概率相等. 由于 Eve 测量时并不知道接收方会选择何种测量基, 她将有 $1/2$ 的概率选择正确, 此时 Alice 和 Bob 检测时并不会发现 Eve 的存在. 但当 Eve 选择了错误的测量基时, Alice 和 Bob 的测量结果仅有 $1/d$ 的概率相匹配. 例如, 如果在纠缠粒子传送过程的检测步骤中, Bob 选择 d 维 Z 基进行测量, Eve 也同样选择了 Z 基进行测量, 那么 Alice 和 Bob 测量结果相同, 并不会发现 Eve 的存在; 但是, Eve 如果选择了 X 基进行测量, 由于 Z 基和 X 基是互补的, Alice 和 Bob 仅有 $1/d$ 的概率测量结果相匹配, 即此时 Eve 不被检测出的概率为 $1/d$, 所以对于每个检测粒子而言, Eve 不被发现的概率为 $1/2 + 1/(2d)$. Eve 导致的错误率为

$$\varepsilon_1 = \frac{1}{2} \left(1 - \frac{1}{d} \right). \quad (10)$$

4.2 中间基 (intermediate-basis) 攻击

在此种攻击策略中, Eve 不是选择高维 Z 基或 X 基对 Alice 发送给 Bob 的高维纠缠粒子进行测量, 而是选择 Z 基和 X 基的中间基 Y ^[46] 对这些粒子进行测量. 其定义为: 对于任意的 i ($0 \leq i \leq d-1$) 都有

$$|\langle Y_i | Z_i \rangle| = |\langle Y_i | X_i \rangle| = \max_value, \quad (11)$$

且对于任意的 j ($0 \leq j \leq d-1$, 且 $j \neq i$) 都有

$$|\langle Y_i | Z_j \rangle| = |\langle Y_i | X_j \rangle| = \min_value, \quad (12)$$

其中 $\max_value$ 和 $\min_value$ 为两个常量. 可得

$$|Y_i\rangle = \frac{1}{\sqrt{C}}(|Z_i\rangle + |X_i\rangle), \quad (13)$$

显然, $\langle Y_i | Y_i \rangle = 1$, 即有 $C = 2(\sqrt{d} + 1)/\sqrt{d}$. 从而可以得到

$$|\langle Y_i | Z_i \rangle| = |\langle Y_i | X_i \rangle| = \frac{\sqrt{d} + 1}{\sqrt{Cd}} \quad (14)$$

和

$$|\langle Y_i | Z_j \rangle| = |\langle Y_i | X_j \rangle| = \frac{1}{\sqrt{Cd}}. \quad (15)$$

不失一般性, 假设 Alice 和 Bob 将对某一高维 Bell 态选择 Z 基进行窃听检测, 而 Alice 将其中一个粒子传送给 Bob 的过程中, Eve 对其选择了 Y 基测量. 此后 Alice 测量留在手中的粒子得到的结果为 $|Z_i\rangle$, 可知 Eve 得到 $|Y_i\rangle$ 的概率为 $P(|Y_i\rangle) = \langle Z_i | Y_i \rangle \times \langle Y_i | Z_i \rangle = (1 + d + 2\sqrt{d})/Cd$, 而得到 $|Y_j\rangle$ ($j \neq i$) 的概率为 $P(|Y_j\rangle) = \langle Z_i | Y_j \rangle \times \langle Y_j | Z_i \rangle = 1/Cd$. 从而可知, Alice 和 Bob 的测量结果相匹配的概率为

$$P_c = [P(|Y_i\rangle)]^2 + \sum_{j=0, j \neq i}^{d-1} [P(|Y_j\rangle)]^2. \quad (16)$$

也就是说, 中间基攻击造成的错误率为

$$\varepsilon_2 = 1 - P_c = \frac{3d + \sqrt{d} - 4}{4d + 4\sqrt{d}}. \quad (17)$$

4.3 通用量子克隆机 (universal quantum cloning machine) 攻击

假设 Eve 有一台如文献 [47] 所述的通用量子克隆机, 能最优克隆 Alice 传送给 Bob 的粒子, 从而对所提确定性安全量子通信协议进行攻击. 攻击过程表示为

$$|\varphi_k\rangle_{\text{Alice}}|0\rangle_{\text{Eve}}|Q\rangle_q \xrightarrow{\text{UQCM}} \alpha|\varphi_k\rangle_{\text{Alice}}|\varphi_k\rangle_{\text{Eve}}|Q_k\rangle_q + \beta \sum_{l \neq k} (|\varphi_k\rangle_{\text{Alice}}|\varphi_l\rangle_{\text{Eve}} + |\varphi_l\rangle_{\text{Alice}}|\varphi_k\rangle_{\text{Eve}})|Q_l\rangle_q, \quad (18)$$

其中 $|\varphi_k\rangle_{\text{Alice}}$ 和 $|\varphi_k\rangle_{\text{Eve}}$ 为 Alice 所传送的粒子经过量子克隆机后得到两相同的副本, 即 $|\varphi_k\rangle_{\text{Alice}} = |\varphi_k\rangle_{\text{Eve}}$, $\{|Q_k\rangle\}$ 为窃听者 Eve 的量子克隆机 Hilbert 空间的一组正交基, 克隆机的初始状态为 $|Q\rangle_q$. 由量子克隆机作用保持酉性可知, $\alpha^2 + 2(d-1)\beta^2 = 1$. 又根据文献 [47] 可知, 对一个量子态进行量子克隆的两个副本与原态最大保真度为 $F_d = (d+3)/(2d+2)$, 即对应的破坏度为 $D_d = 1 - F_d = (d-1)/(2d+2)$. 即 Eve 采用通用量子克隆机攻击引起的错误率为

$$\varepsilon_3 = D_d = \frac{1}{2} \left(1 - \frac{2}{d+1} \right). \quad (19)$$

显然, 错误率 ε_1 , ε_2 和 ε_3 随着维度 d 的增大而增大. 说明随着维度的增加协议具有更好的安全性.

通过比较知道, 对于任意的 $d \geq 2$, 均有 $\varepsilon_1 \geq \varepsilon_3$ 和 $\varepsilon_2 \geq \varepsilon_3$. 如果窃听者选择对 Alice 发送给 Bob 的粒子进行攻击的概率为 η , 那么 Alice 和 Bob 可以分析出错误率阈值

$$\varepsilon_{\text{th}} \leq \min\{\eta\varepsilon_1, \eta\varepsilon_2, \eta\varepsilon_3\} = \frac{\eta}{2} \left(1 - \frac{2}{d+1} \right). \quad (20)$$

当 $d \rightarrow \infty$ 时, 阈值上界趋向于 $\eta/2$.

以上分析, 仅针对理想量子信道情况. 对于存在噪声的量子信道, 可以调整错误率阈值及通过高维纠缠粒子提纯过程 [48], 保证 Alice 和 Bob 之间分布的是最大纠缠的高维纯 Bell 态, 再进行信息传送过程.

5 讨论和结束语

显然, 和低维量子直接通信协议相比, 本文所提高维确定性安全量子通信协议具有通用性和一般性. 由于利用了高维 Bell 态作为信息载体, 故其容量更大, 是二维 Bell 态容量的 $\log_2 d$ 倍; 同时, 协议的安全性随着维度的增大而增强. 和其他基于低维纠缠交换的量子通信协议一样, 所提高维通信协议的安全性基于纠缠分发的安全性, 使得在秘密信息通信之前就能确保安全; 并且纠缠粒子只需在量子信道中传输一次, 减少了量子信道噪声和信道损失的影响, 这在实际条件下增加了协议的安全性和比特生成效率. 和 Wang 等 [26] 及 Li 等 [37] 分别提出的高维量子直接通信协议相比, 本文所提量子通信模型的一个显著的特点是整个通信过程中不需要酉操作. 由于纠缠粒子在量子信道中只传输一次, 且整个通信过程中不需要酉操作, 故所提高维协议比 Wang 等 [26] 提出的高维协议在实验上更容易实现. 尽管如此, 由于高维 Bell 态的制备、存储、传输和测量, 以及克服消相干都是实际过程中遇到的问题, 实现它仍有一定的难度.

总之, 基于高维 Bell 态纠缠交换特性, 提出一般化的确定性安全量子通信协议, 具有较高的理论价值. 协议中整个通信过程不需要酉操作; 通信双方根据高维 Bell 测量的结果, 通过模加、减运算即可完成信息的编、解码. 为了分析量子信道的安全性, 我们利用了两种互补的测量基对检测粒子进行

测量, 这种方法, 既类似于 BBM92^[49] 采取的方法, 又是它的一般化方法, 从而分析出常用攻击策略所引起的错误率, 并进一步推导出错误率阈值的上界. 由于所提协议在逻辑上将纠缠粒子的传输和信息的传输分开, 这大大降低了信息被窃取的可能. 此外, 本文所提协议稍加改动亦可以用作量子密钥分配方案来分配确定的密钥或本质上完全随机 (不是伪随机) 的密钥.

参考文献

- 1 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing. Bangalore, 1984. 175–179
- 2 Gisin N, Ribordy G G, Tittel W, et al. Quantum cryptography. *Rev Mod Phys*, 2002, 74: 145–195
- 3 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*, 2002, 65: 032302
- 4 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. *Phys Rev A*, 2003, 68: 042315
- 5 Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication. *Front Phys China*, 2007, 2: 251–272
- 6 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. *Phys Rev Lett*, 2002, 89: 187902
- 7 Wójcik A. Eavesdropping on the “ping-pong” quantum communication protocol. *Phys Rev Lett*, 2003, 90: 157901
- 8 Zhang Z J, Li Y, Man Z X. Improved Wójcik’s eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. *Phys Lett A*, 2005, 341: 385–389
- 9 Cai Q Y. The “ping-pong” protocol can be attacked without eavesdropping. *Phys Rev Lett*, 2003, 91: 109801
- 10 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A*, 2006, 351: 23–25
- 11 Deng F G, Li X H, Li C Y, et al. Eavesdropping on the ‘ping-pong’ quantum communication protocol freely in a noise channel. *Chin Phys*, 2007, 16: 277–281
- 12 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A*, 2003, 68: 042317
- 13 Cai Q Y, Li B W. Improving the capacity of the Boström-Felbinger protocol. *Phys Rev A*, 2004, 69: 054301
- 14 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. *Phys Rev A*, 2004, 69: 052319
- 15 Lucamarini M, Mancini S. Secure deterministic communication without entanglement. *Phys Rev Lett*, 2005, 94: 140501
- 16 Wang C, Deng F. G, Long G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. *Opt Commun*, 2005, 253: 15–20
- 17 Li X H, Li C Y, Deng F G, et al. Quantum secure direct communication with quantum encryption based on pure entangled states. *Chin Phys*, 2007, 16: 2149–2153
- 18 Lin S, Wen Q Y, Gao F, et al. Quantum secure direct communication with χ -type entangled states. *Phys Rev A*, 2008, 78: 064304
- 19 Yi X J, Nie Y Y, Zhou N R, et al. Secure direct communication based on non-orthogonal entangled pairs and local measurement. *Int J Theor Phys*, 2008, 47: 3401–3407
- 20 Chamoli A, Bhandari C M. Secure direct communication based on ping-pong protocol. *Quantum Inf Process*, 2009, 8: 347–356
- 21 Dong L, Dong H K, Xiu X M, et al. Quantum secure direct communication using a six-qubit maximally entangled state with dense coding. *Int J Quantum Inf*, 2009, 7: 645–651
- 22 Qin S J, Wen Q Y, Meng L M, et al. Quantum secure direct communication over the collective amplitude damping channel. *Sci China Ser G-Phys Mech Astron*, 2009, 52: 1208–1212
- 23 Zhang X L, Zhang Y X, Wei H. Quantum secure direct communication with Greenberger-Horne-Zeilinger-type state (GHZ state) over noisy channels. *Chin Phys B*, 2009, 18: 435–439
- 24 Cao W F, Yang Y G, Wen Q Y. Quantum secure direct communication with cluster states. *Sci China Phys Mech Astron*, 2010, 53: 1271–1275

- 25 Wang C, Hao L, Song S Y, et al. Quantum direct communication based on quantum search algorithm. *Int J Quantum Inf*, 2010, 8: 443–450
- 26 Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. *Phys Rev A*, 2005, 71: 044305
- 27 Shimizu K, Imoto N. Communication channels secured from eavesdropping via transmission of photonic Bell states. *Phys Rev A*, 1999, 60: 157–166
- 28 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key. *Acta Phys Pol A*, 2002, 101: 357–368
- 29 Yan F L, Zhang X Q. A scheme for secure direct communication using EPR pairs and teleportation. *Eur Phys J B*, 2004, 41: 75–78
- 30 Wang J, Zhang Q, Tang C J. Quantum secure direct communication based on order rearrangement of single photons. *Phys Lett A*, 2006, 358: 256–258
- 31 Zhu A D, Xia Y, Fan Q B, et al. Secure direct communication based on secret transmitting order of particles. *Phys Rev A*, 2006, 73: 022338
- 32 Yuan H, Song J, He Q, et al. Robust quantum secure direct communication and deterministic secure quantum communication over collective dephasing noisy channel. *Commun Theor Phys*, 2008, 50: 627–632
- 33 Gao G. Efficient quantum secure communication protocol by rearranging particle orders. *Commun Theor Phys*, 2009, 52: 845–847
- 34 Gu B, Pei S X, Song B, et al. Deterministic secure quantum communication over a collective-noise channel. *Sci China Ser G-Phys Mech Astron*, 2009, 52: 1913–1918
- 35 Yuan H, Song J, Hu X Y, et al. An efficient deterministic secure quantum communication scheme with cluster state. *Int J Quantum Inf*, 2009, 7: 689–696
- 36 Liu W J, Chen H W, Ma T H, et al. An efficient deterministic secure quantum communication scheme based on cluster states and identity authentication. *Chin Phys B*, 2009, 18: 4105–4109
- 37 Li X H, Deng F G, Li C Y, et al. Deterministic secure quantum communication without maximally entangled states. *J Korean Phys Soc*, 2006, 49: 1354–1359
- 38 Żukowski M, Zeilinger A, Horne M A, et al. “Event-ready-detectors” Bell experiment via entanglement swapping. *Phys Rev Lett*, 1993, 71: 4287–4290
- 39 Pan J W, Bouwmeester D, Weinfurter H, et al. Experimental entanglement swapping: Entangling photons that never interacted. *Phys Rev Lett*, 1998, 80: 3891–3894
- 40 Gao T, Yan F L, Wang Z X. Deterministic secure direct communication using GHZ states and swapping quantum entanglement. *J Phys A: Math Gen*, 2005, 38: 5761–5770
- 41 Man Z X, Zhang Z J, Li Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. *Chin Phys Lett*, 2005, 22: 18–21
- 42 Xiu X M, Dong H K, Dong L, et al. Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping. *Opt Commun*, 2009, 282: 2457–2459
- 43 Zhan Y B, Zhang L L, Zhang Q Y. Quantum secure direct communication by entangled qutrits and entanglement swapping. *Opt Commun*, 2009, 282: 4633–4636
- 44 Qin S J, Gao F, Wen Q Y, et al. Improving the quantum secure direct communication by entangled qutrits and entanglement swapping against intercept-and-resend attack. *Opt Commun*, 2010, 283: 1566–1568
- 45 Nielsen M A, Chuang I L. Quantum computation and quantum information. Photocopy ed. Beijing: Higher Education Press, 2003. 216–247
- 46 Bechmann-Pasquinucci H, Tittel W. Quantum cryptography using larger alphabets. *Phys Rev A*, 2000, 6106: 062308
- 47 Bužek V, Hillery M. Universal optimal cloning of arbitrary quantum states: From qubits to quantum registers. *Phys Rev Lett*, 1998, 81: 5003–5006
- 48 Alber G, Delgado A, Gisin N, et al. Efficient bipartite quantum state purification in arbitrary dimensional Hilbert spaces. *J Phys A: Math Gen*, 2001, 34: 8821–8833
- 49 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell’s theorem. *Phys Rev Lett*, 1992, 68: 557–559

Deterministic secure quantum communication without unitary operation based on high-dimensional entanglement swapping

LIU ZhiHao^{1*}, CHEN HanWu^{1*}, LIU WenJie², XU Juan¹ & LI ZhiQiang³

1 School of Computer Science and Engineering, Southeast University, Nanjing 211189, China;

2 School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China;

3 College of Information Engineering, Yangzhou University, Yangzhou 225009, China

*E-mail: liuzhtopic@163.com; hw_chen@seu.edu.cn

Abstract By analysis of the basic properties of entanglement swapping of high-dimensional Bell states, a universal and general deterministic secure quantum communication (DSQC) protocol is proposed, in which unitary operation is not required. By making use of the results of high-dimensional Bell measurement, the sender and the receiver can encode and decode the message respectively by performing the modular addition and subtraction. Two mutually complementary bases are constructed; and according to the property of mutual complement, a method for checking security of the high-dimensional quantum channel is put forward. Some common attack strategies are analyzed, and the corresponding error rates are calculated. Then the upper bound of the threshold of error rate is deduced.

Keywords deterministic secure quantum communication, high-dimensional Bell state, entanglement swapping, high-dimensional Bell measurement