中国科学 G辑: 物理学 力学 天文学 2008 年 第 38 卷 第 5 期: 477 ~ 484
www.scichina.com phys.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

重新审视量子对话和双向量子安全直接通信的安全性

高飞[①②*], 郭奋卓[①②], 温巧燕[①②], 朱甫臣[③]

① 北京邮电大学网络与交换技术国家重点实验室, 北京 100876;
② 北京邮电大学理学院, 北京 100876;
③ 现代通信国家重点实验室, 成都 610041
* E-mail: hzpe@sohu.com

收稿日期: 2007-10-19; 接受日期: 2007-12-11
国家高技术研究发展计划(编号: 2006AA01Z419)、国家自然科学基金(编号: 90604023, 60373059)、教育部高等学校博士点基金(编号: 20040013007)、现代通信国家重点实验室基金(编号: 9140C1101010601)、北京市自然科学基金(编号: 4072020)和 ISN 开放基金资助项目

摘要 从信息论和密码学的角度分析了两个量子对话协议和一个双向量子安全直接通信协议的安全性, 指出这些协议中传输的信息将会被部分地泄露出去. 也就是说, 任何窃听者都可以从合法通信者的公开声明中提取到部分秘密信息. 而这种现象在量子安全通信中是不该出现的. 事实上, 很多近期提出的类似协议中也存在这个问题. 希望在今后的研究中信息泄露的问题能够得到大家的重视.

关键词
量子安全直接通信
量子对话
量子密码
密码分析

密码学是用来保证秘密消息在两个用户Alice和Bob之间传输时不会被窃听者Eve得到. 经典密码中密码系统的安全性多基于计算复杂性假设. 但也有一种例外情况, 即一次一密乱码本(one-time pad, 简写OTP). 它利用事先共享的安全密钥来加密要在公开信道中传输的消息, 具有理论上的安全性. 然而, 在Alice和Bob之间建立同样安全的密钥对现有的经典密码系统来说都是困难的. 幸运的是, 作为量子密码 [1]的一个重要应用, 量子密钥分发(quantum key distribution, 简写QKD)[2~6]可以巧妙地完成这项任务. 量子密码将量子力学原理引入密码学, 而正是这些基本原理保证了量子密码在理论上具有无条件安全性.

近来, 量子密码的另外一个分支——量子安全直接通信(quantum secure direct communication, 简写QSDC)被提出并引起了广泛关注 [7~14]. 它允许发送者以确定并安全的方式直接发送秘密消息(而不是随机密钥)给接收者. 同时, 一个精心设计的QSDC协议也能够在理论上达到无条件安全性 [15~17]. 最初的QSDC协议完成的都是单向通信, 例如从Alice到Bob[7~14]. 后来,

人们提出了双向的QSDC, 也就是所谓的量子对话(quantum dialogue)[18]. 在这种协议里, 秘密消息可以沿着正反两个方向同时传输, 即Alice到Bob和Bob到Alice.

随着计算能力的飞速提高, 大多数经典密码系统的安全性都受到日益严重的威胁. 量子密码的目的就是要改变这种状况, 寻找能获得高安全性(理论上的无条件安全)的不同方法. 因此, 高安全性既是量子密码的重要优势, 也是量子密码的必备要求. 然而, 并不是人们提出的所有协议都能达到这种要求. 例如一些协议被某种设计时没有考虑到的巧妙策略所攻破 [19~29]. 本文研究一种不同的安全威胁, 即信息泄露. 众所周知, 公开的经典通信在量子密码中是必须的. 我们必须保证传输的秘密信息(不管是密钥还是消息)不会从这些经典通信中泄露出去. 否则我们就得不到所期望达到的安全性. 然而, 正如我们将在下文中阐述的那样, 在一些双向QSDC协议中所传输的秘密消息会被部分泄露出去.

1 对 NBA 和 MZL 协议的分析

2004 年Nguyen[18]基于Bell态提出了一种量子对话协议. 之后Man等人 [30]指出这个协议对截获重发攻击来说是不安全的, 并给出一种改进方案. 为了方便, 我们分别称这两个方案为NBA协议和MZL协议.

本文中, 我们并不致力于寻找巧妙的攻击策略, 而主要讨论信息泄露问题, 在这种情况下 Eve 不需要进行任何主动攻击就能得到部分秘密信息(需要注意的是, Eve 仅从公开声明中提取信息, 不会被任何检测窃听过程发现). 因此, 我们不必考虑协议中的检测窃听过程(一般称为控制模式, 简写为 CM), 而把讨论重点放在消息传输过程(一般称为消息模式, 简写为 MM). 从这种意义上来说 NBA 协议和 MZL 协议是相同的, 因为它们之间的不同仅仅在于 CM. 本节以第一个量子对话协议——NBA 协议为例来进行论述.

首先简单介绍 NBA 协议的 MM 部分. Bob 产生一串 EPR 对作为载体, 每对粒子处于状态

$$\left|\Psi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right), \tag{1}$$

Bob可以通过对其中一个粒子做 4 种操作$\{I,\sigma_x,\mathrm{i}\sigma_y,\sigma_z\}$之一在每个EPR对中编码两比特秘密信息. 然后Bob把这个粒子发送给Alice. 类似地, Alice也可以用相同的方式对其进行编码, 并把粒子发回给Bob. 最后, Bob对两个光子进行Bell测量, 同时声明测量结果. 可以看出, 这个通信过程看上去像是一个重复的密集编码(dense coding)[31]. 根据测量结果和他们各自的编码操作, Alice和Bob就能推断出对方所发来的消息比特. 举例来说, 假设测量结果为$\left|\Psi^{-}\right\rangle=1/\sqrt{2}\left(\left|01\right\rangle-\left|10\right\rangle\right)$. 如果Bob的编码操作为$\sigma_z$, 他就能判断出Alice的操作为$I$. 相反, Alice也可以根据她的操作$I$推断出Bob的操作$\sigma_z$. 如果操作$\{I,\sigma_x,\mathrm{i}\sigma_y,\sigma_z\}$分别对应于消息比特{00, 01, 10, 11}, 那么在这个例子中Bob就将“11”发给了Alice, 同时Alice将“00”发给了Bob(见表 1). 类似地, Alice和Bob可以使用更多的EPR对来交换他们的全部秘密消息.

现在来观察 NBA 协议的通信效果. 显然, 在一个 EPR 对的帮助下, Alice 和 Bob 可以传输 4 个消息比特(每人各 2 比特). 那么这里是否真的安全地传输了 4 比特消息呢? 答案是否定的. 为了说明这一点, 可以分析 Eve 能从公开声明中得到什么. 事实上, 任何知道这些公开信息,

表 1 当测量结果为$|\Psi^-\rangle$时 Alice 和 Bob 的可能的编码操作及其对应的消息比特 a)

Alice	I (00)	σ_x (01)	$\mathrm{i}\sigma_y$ (10)	σ_z (11)
Bob	σ_z (11)	$\mathrm{i}\sigma_y$ (10)	σ_x (01)	I (00)

a) 第一行和第二行分别代表 Alice 和 Bob 的操作和消息比特; 如果 Alice 在编码时采用了某一种操作, 她就知道 Bob 肯定采用了同一列中的操作, 这样, Alice 和 Bob 就能交换 2 比特秘密消息

即初态$\left|\Psi^+\right\rangle$和测量结果$\left|\Psi^-\right\rangle$的人都可以得到一个结论, 那就是 Alice 和 Bob 的编码操作一定是下面 4 种可能之一: $\{(I,\sigma_z),\ (\sigma_x,\mathrm{i}\sigma_y),\ (\mathrm{i}\sigma_y,\sigma_x),\ (\sigma_z,I)\}_{\mathrm{AB}}$ (下标 A 和 B 分别表示 Alice 和 Bob 的操作). 因此, Eve 知道 Alice 和 Bob 传输的消息比特必为$\{(00,11),\ (01,10),\ (10,01),\ (11,00)\}_{\mathrm{AB}}$之一, 且出现概率相同. 这对 Eve 来说仅包含$-4\times\frac{1}{4}\log_2\frac{1}{4}=2$比特未知信息. 所以, 4 个消息比特中的 2 比特信息在不知不觉中被泄露出去(举例来说, 当初态为$\left|\Psi^+\right\rangle$而测量结果为$\left|\Psi^-\right\rangle$时, Eve 知道 Alice 和 Bob 发送的消息比特的逐位异或值为“11”, 这意味着 2 比特信息泄露). 换句话说, 在一个 EPR 对所传输的 4 比特秘密信息中, 只有 2 比特被安全地传送. 当初态和测量结果为其他 Bell 态时, 这一结论仍然成立.

有人可能会说, Eve 不能得到任何一个消息比特的具体值, 因此 NBA 协议仍然是安全的. 这种想法是不对的. 在一个密码学协议中, 尤其是追求无条件安全的量子密码协议中, 所有的秘密信息都应该被安全地传输. 当一个协议中只有部分秘密信息在传输中能够保证安全时, 我们不能说它是一个安全协议. 实际上, 正如第 4 节中将要讨论的那样, 这种不安全性相当于在 OTP 中重复使用密钥.

2 对 JZ 协议的分析

Ji和Zhang于近期提出了一个基于单粒子的量子对话协议(JZ协议)[32]. 然而在这个协议中, 也存在信息泄露的问题.

JZ 协议的过程是这样的. Bob 产生 N 组单粒子, 每个粒子随机处于如下 4 个状态之一: $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, 其中

$$|+\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right),\quad |-\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right). \tag{2}$$

在这 N 组粒子中, 只有一组用来传输消息比特, 其他组都用来检测窃听. 与第 1 节类似, 因为 Eve 不采取任何主动攻击, 这里不需要考虑检测窃听的过程. 不失一般性, 我们可以通过只讨论一个用作信息载体的粒子来理解 JZ 协议的思想. 生成这个粒子之后, Bob 可以通过对它实施两个操作$\{I,\mathrm{i}\sigma_y\}$之一将 1 比特秘密消息编码进来(以上两个操作分别对应{0, 1}). 注意上述 4 种量子态在 I 操作下保持不变, 而在$\mathrm{i}\sigma_y$操作下会发生翻转, 即

$$\mathrm{i}\sigma_y|0\rangle=|1\rangle,\ \mathrm{i}\sigma_y|1\rangle=|0\rangle,\ \mathrm{i}\sigma_y|+\rangle=|-\rangle,\ \mathrm{i}\sigma_y|-\rangle=|+\rangle. \tag{3}$$

编码之后 Bob 将这个粒子发送给 Alice. 收到粒子后, Alice 也用同样的方式将她的 1 比特秘密消息编码进去. 此时 Bob 公开告知 Alice 这个粒子的初始状态. 然后 Alice 用一个正确的基, $B_z=\{|0\rangle,|1\rangle\}$ 或 $B_x=\{|+\rangle,|-\rangle\}$, 来测量这个粒子. 这里所谓的正确的基是指粒子初始状态所在的基(注意在操作 I 和 $\mathrm{i}\sigma_y$ 下上述 4 种状态可能不变也可能翻转, 但它们所处的基均不变). 最后 Alice 公开她的测量结果. 通过这个过程, Alice 和 Bob 每人都可以得到对方发来的 1 比特秘密消息. 举例来说, 假设粒子的初始状态为 $|+\rangle$. 如果 Bob 对它作用了 $\mathrm{i}\sigma_y$ (即发送消息比特"1"), 且 Alice 的测量结果为 $|-\rangle$, 则 Bob 知道 Alice 在编码时实施了 I 操作, 因为 $I\left(\mathrm{i}\sigma_y|+\rangle\right)=|-\rangle$. 也就是说, Bob 知道 Alice 发来的消息比特为"0". 与此同时, 根据粒子的初始状态 $|+\rangle$、测量结果 $|-\rangle$ 以及自己的编码操作 I, Alice 可判断出 Bob 的编码操作为 $\mathrm{i}\sigma_y$, 进而得到 Bob 发来的比特"1". 用这种方法, Alice 和 Bob 可以用更多的粒子来交换他们的全部秘密消息.

可以看出在 JZ 协议中, 用户利用 1 个粒子可以传输 2 比特秘密消息(Alice 和 Bob 分别传输 1 比特). 现在来观察 Eve 可以从公开的经典通信(即粒子的初始状态和测量结果)中得到多少信息. 考虑同样的例子, 即初始状态为 $|+\rangle$ 而测量结果为 $|-\rangle$. 这种情况下 Eve 知道 Alice 和 Bob 的编码操作不是 $[I,\mathrm{i}\sigma_y]_{\mathrm{AB}}$ 就是 $[\mathrm{i}\sigma_y,I]_{\mathrm{AB}}$. 对 Eve 来说这种不确定性仅包含 1 比特信息(假设两者发生的概率相同). 因此, 2 比特消息中只有 1 比特信息被安全地传输, 而另外 1 比特被泄露出去. 同理, 当粒子的初始状态和测量结果为其他情况时, 这一结论仍然成立.

3 对 MXN 协议的分析

随着量子对话的不断发展, 人们提出了多方情形下的双向QSDC. 2006 年, Man等人[33]基于GHZ态提出了这样一种协议(MXN协议). 但分析表明, MXN协议中很多所传输的秘密信息将被泄露出去.

这里先简单介绍 MXN 协议. 同样我们不用关心它的检测窃听过程. 在协议的开始, Alice, Bob 和 Charlie 共享有一串 GHZ 三粒子纠缠态, 它们的状态为

$$\left|\mathrm{GHZ}_{000}\right\rangle_{\mathrm{ABC}}=\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)_{\mathrm{ABC}}. \tag{4}$$

他们将每两个这样的 GHZ 态作为一个单元来传输各自的秘密消息. 考虑三者共享的两个 GHZ 态 $\left|\mathrm{GHZ}_{000}\right\rangle_{123}$ 和 $\left|\mathrm{GHZ}_{000}\right\rangle_{456}$, 这里下标 1~6 代表不同的粒子, 其中 1 和 4 属于 Alice, 2 和 5 属于 Bob, 而 3 和 6 属于 Charlie. 此时 Alice 通过对粒子 4 实施 4 个幺正操作 $\{I,\sigma_z,\mathrm{i}\sigma_y,\sigma_x\}$ 之一(分别对应于消息比特{00, 01, 10, 11}), 将 2 比特秘密消息编码进 $\left|\mathrm{GHZ}_{000}\right\rangle_{456}$. 与此同时 Bob (Charlie)也可以对粒子 5(6)作用两个操作 $\{I,\mathrm{i}\sigma_y\}$ 之一(分别对应于消息比特{0, 1})将自己的 1 比特秘密消息编码进同一个 GHZ 态. 编码过后, $\left|\mathrm{GHZ}_{000}\right\rangle_{456}$ 将变成 8 个 GHZ 态之一 $\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}$. 不难看出, 如果一个用户知道了 $\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}$ 的具体状态, 他/她就能知道另外两

个用户在这一 GHZ 态中编码的消息比特. 举例来说, 如果 Bob 在编码阶段对粒子 5 作用了操作 I(即他想发送给 Alice 和 Charlie 的消息比特为“0”), 且粒子 4~6 的终态为

$$\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}=\left|\mathrm{GHZ}_{101}\right\rangle_{456}=\frac{1}{\sqrt{2}}\left(\left|001\right\rangle-\left|110\right\rangle\right)_{456}, \tag{5}$$

则Bob知道Charlie对粒子6实施了$\mathrm{i}\sigma_y$操作而Alice对粒子4实施了I操作. 进而得到Alice的消息比特“00”以及Charlie的消息比特“1”. 因此, 为了实现这种通信, 三个用户只需找到一种方法来弄清楚他们共享的$\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}$处于哪一个GHZ态. 在MXN协议中, 他们可以在另外一个纠缠态$\left|\mathrm{GHZ}_{000}\right\rangle_{123}$的帮助下达到这个目的. 具体地, Alice, Bob和Charlie分别对自己手中的粒子对(1, 4), (2, 5)及(3, 6)做Bell测量, 并公开声明测量结果. 这种情况下, 将会发生下面的纠缠交换(ES)[34]:

$$\left|\mathrm{GHZ}_{000}\right\rangle_{123}\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}\Rightarrow\left|\varphi^1\right\rangle_{14}\left|\varphi^2\right\rangle_{25}\left|\varphi^3\right\rangle_{36}, \tag{6}$$

其中$\left|\varphi^1\right\rangle_{14}$, $\left|\varphi^2\right\rangle_{25}$和$\left|\varphi^3\right\rangle_{36}$分别表示 Alice, Bob 和 Charlie 的测量结果. 根据 ES 的规律, 任何知道这三个测量结果的人都可以推断出$\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}$(详见文献[33]). 于是三者都可以得到另外两用户发来的消息比特. 这样, 利用更多的 GHZ 态, 三个用户可以用同样方法交换他们所有的秘密消息.

如上协议中, 用户可以利用两个 GHZ 态来传输 4 比特秘密消息(Alice 2 比特, Bob 和 Charlie 各 1 比特). 现在来分析是否所有这些比特都被安全地传输. 如上所述, 当测量结果$\left|\varphi^1\right\rangle_{14}$, $\left|\varphi^2\right\rangle_{25}$和$\left|\varphi^3\right\rangle_{36}$被声明以后, 任何人都可以判断出$\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}$的具体状态, 包括 Eve. 这就意味着这些消息比特的部分信息将被泄露出去. 为了说明这一点, 可以再次考虑上面的例子, 即编码操作后粒子 4~6 处于状态$\left|\mathrm{GHZ}_{101}\right\rangle_{456}$(见(5)式). 这种情况下 Eve 可以推断 Alice, Bob 和 Charlie 的编码操作必为$[I,I,\mathrm{i}\sigma_y]_{\mathrm{ABC}}$和$[\sigma_x,\mathrm{i}\sigma_y,I]_{\mathrm{ABC}}$之一. 于是她知道传输的消息比特为$[00,0,1]_{\mathrm{ABC}}$或$[11,1,0]_{\mathrm{ABC}}$. 对 Eve 来说这种不确定性仅包含$-2\times\frac{1}{2}\log_2\frac{1}{2}=1$比特信息(假设两者发生的概率相同). 因此, 实际上 4 个消息比特中只有 1 比特信息被安全地传输, 而有 3 比特信息被泄露出去. 同理, 当$\left|\mathrm{GHZ}_{xyz}\right\rangle_{456}$为其他 GHZ 态时我们可以得到同样的结论.

上面的分析都是基于三方 MXN 协议, 在这些协议中 75%的信息将被泄露. 事实上, 这一问题在推广的 N 方协议中更加严重. 这种情况下 N 个用户可以利用一对 N 粒子 GHZ 态来传输 N+1 个消息比特(Alice 2 比特, 其他 $N-1$ 方各 1 比特). 通过类似的分析我们得到以下结论, 即在传输的 N+1 个消息比特中, 只有 1 比特信息安全送达, 而 N 比特信息被泄露出去.

4 结果和讨论

分析了 3 种双向QSDC协议的安全性, 指出所传输的秘密消息的部分信息将会在无意中被泄露出去. 由于信息泄露的问题与以往那些可以使Eve成功获得确切秘密的攻击策略有很大不

同, 这种威胁很容易被忽略. 因此, 这个问题还没有引起广泛注意. 例如除了上面分析的协议[18,30,32,34]以外, 还有不少协议[35~39]中存在这种风险.

为了更好地理解这种不安全性, 可以将涉及到的方案简化成一个QKD协议, 借此将这种安全性讨论转移到一种大家更熟悉的密码学算法中, 即OTP. 不失一般性, 我们以JZ协议为例, 考虑其中一个作为信息载体的粒子. 在简化方案中, Bob先准备这个粒子, 使它随机地处于四个状态$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$之一(分别对应于{0, 1, 0, 1}), 并将它发送给Alice. 当Alice收到这个粒子以后, Bob告知Alice它所在的基, 即B_z或B_x. 此时Alice用相应的测量基来测量这个粒子, 得到一个密钥比特k(值为 0 或 1). 这个过程与延迟选择(delayed choice)BB84 协议中的情况[40]类似. 然后Alice和Bob用OTP算法来加密他们各自的消息比特(明文) p_A和p_B, 分别得到密文$c_A = p_A \oplus k$和$c_B = p_B \oplus k$ ($\oplus$ 表示模 2 加). 最后, 他们公开声明各自的密文. 由于知道密钥比特k, Alice和Bob都能得到对方所发送的消息比特(即明文). 通过这种方法, Alice和Bob可以分别传送 1 比特秘密消息给对方, 其效果与JZ协议中非常相似. 然而, 众所周知, OTP中的密钥绝对不能重复使用, 否则将会变得不安全[41,42]. 显而易见, 上面的通信过程中密钥被使用了两次, 因此这种通信是不安全的. 事实上, 根据公开声明的密文c_A和c_B, Eve可以推断出传输的消息比特不是$[c_A, c_B]_{AB}$就是$[c_A \oplus 1, c_B \oplus 1]_{AB}$, 而这种不确定性仅包含 1 比特信息, 而不是 2 比特. 因此, JZ协议的通信效果跟上面的QKD&OTP通信是一样的, 但OTP中的密钥被使用了两次. 类似地, 从通信效果上来看, 上述所有存在信息泄露问题的双向QSDC协议都等价于一个重复使用密钥的OTP加密算法(密钥被使用两次或更多). 而两者都不是真正安全的保密通信.

为了避免秘密信息的泄露, 我们首先应该正确估计量子信道的保密容量. 例如在 JZ 协议中, 一个量子比特只能保密传输 1 比特消息, 当要传输的比特数大于 1 的时候就必然会发生信息泄露. 因此, 如果用一个粒子去传输 1 比特消息, 我们就能够保证通信的安全性. 换句话说, 适当降低通信效率是解决上述信息泄露问题的一种可行方法.

自出现至今, 密码学始终包含两个方面的研究内容. 一是各种密码协议的设计, 二是对现有密码系统的分析, 即试图找到它们的漏洞并进行相应的改进. 这两方面的研究对密码学的发展都是不可或缺的. 在量子密码中也是如此. 本文指出了一种经常出现的对 QSDC 安全性的误解, 即在一些双向 QSDC 协议中秘密消息将会被部分地泄露出去. 作为密码学研究中(包括经典密码学和量子密码学)用于分析安全性的一种有效工具, 信息论已经得到各国学者的广泛认可. 因此, 当分析协议的安全性时, 我们需要从信息论和密码学的角度去思考问题. 总之, 希望本文中讨论的信息泄露问题能够在今后的研究中引起大家的关注.

参考文献

1 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145—195[DOI]

2 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore: IEEE, 1984. 175—179

3 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661—663[DOI]

4 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121—3124

[DOI]
5 周春源, 吴光, 陈修亮, 等. 50 km 光纤中量子保密通信. 中国科学 G 辑: 物理学 力学 天文学, 2003, 33(6): 538—543
6 王川, 张竞夫, 王平晓. 自由空间中量子密码通讯实验. 中国科学 G 辑: 物理学 力学 天文学, 2005, 35(2): 149—157
7 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902[DOI]
8 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[DOI]
9 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319 [DOI]
10 Lucamarini M, Mancini S. Secure deterministic communication without entanglement. Phys Rev Lett, 2005, 94: 140501[DOI]
11 Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum super-dense coding. Phys Rev A, 2005, 71: 044305
12 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
13 Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys Rev A, 2006, 74: 054302
14 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
15 Hoffmann H, Bostroem K, Felbinger T. Comment on "Secure direct communication with a quantum one-time pad". Phys Rev A, 2005, 72: 016301
16 Deng F G, Long G L. Reply to "Comment on 'Secure direct communication with a quantum one-time pad'". Phys Rev A, 2005, 72: 016302[DOI]
17 Deng F G, Li X H, Li C Y, et al. Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs. Phys Lett A, 2006, 359: 359—365[DOI]
18 Nguyen B A. Quantum dialogue. Phys Lett A, 2004, 328: 6—10[DOI]
19 Zhang Y S, Li C F, Guo G C. Comment on "Quantum key distribution without alternative measurements". Phys Rev A, 2001, 63: 036301
20 Wójcik A. Eavesdropping on the "Ping-Pong" quantum communication protocol. Phys Rev Lett, 2003, 90: 157901[DOI]
21 Wójcik A. Comment on "Quantum dense key distribution". Phys Rev A, 2005, 71: 016301[DOI]
22 Gao F, Guo F Z, Wen Q Y, et al. Comment on "Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers". Phys Rev A, 2005, 72: 036302[DOI]
23 Gao F, Guo F Z, Wen Q Y, et al. Comment on "Quantum key distribution for d-level systems with generalized Bell states". Phys Rev A, 2005, 72: 066301[DOI]
24 Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A, 2005, 72: 044302[DOI]
25 Lo H K, Ko T M. Some attacks on quantum-based cryptographic protocols. Quantum Inf Comput, 2005, 5: 40—47
26 Qin S J, Gao F, Wen Q Y, et al. Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys Lett A, 2006, 357: 101—103
27 Gao F, Wen Q Y, Zhu F C. Comment on: "Quantum exam". Phys Lett A, 2007, 360: 748—750[DOI]
28 Gao F, Qin S J, Wen Q Y, et al. A simple participant attack on the Brádler-Dušek protocol. Quantum Inf Comput, 2007, 7: 329—334
29 Zhang Z J, Liu J, Wang D, et al. Comment on "Quantum direct communication with authentication". Phys Rev A,

2007, 75: 026301[DOI]
30 Man Z X, Zhang Z J, Li Y. Quantum dialogue revisited. Chin Phys Lett, 2005, 22: 22—24[DOI]
31 Bennett C H, Wiesner S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett, 1992, 69: 2881—2884[DOI]
32 Ji X, Zhang S. Secure quantum dialogue based on single-photon. Chin Phys, 2006, 15: 1418—1420[DOI]
33 Man Z X, Xia Y J, Nguyen B A. Quantum secure direct communication by using GHZ states and entanglement swapping. J Phys B-At Mol Opt Phys, 2006, 39: 3855—3863[DOI]
34 Zukowski M, Zeilinger A, Horne M A, et al. "Event-ready-detectors" Bell experiment via entanglement swapping. Phys Rev Lett, 1993, 71: 4287—4290[DOI]
35 Man Z X, Xia Y J. Controlled bidirectional quantum direct communication by using a GHZ state. Chin Phys Lett, 2006, 23: 1680—1682[DOI]
36 Xia Y, Fu C B, Zhang S, et al. Quantum dialogue by using the GHZ state. J Korean Phys Soc, 2006, 48: 24—27
37 Jin X R, Ji X, Zhang Y Q, et al. Three-party quantum secure direct communication based on GHZ states. Phys Lett A, 2006, 354: 67—70[DOI]
38 Man Z X, Xia Y J. Improvement of security of three-party quantum secure direct communication based on GHZ states. Chin Phys Lett, 2007, 24: 15—18[DOI]
39 Chen Y, Man Z X, Xia Y J. Quantum bidirectional secure direct communication via entanglement swapping. Chin Phys Lett, 2007, 24: 19—22[DOI]
40 Gao F, Guo F Z, Wen Q Y, et al. On the information-splitting essence of two types of quantum key distribution protocols. Phys Lett A, 2006, 355: 172—175[DOI]
41 Shannon C E. Communication theory of secrecy system. Bell Syst Tech J, 1949, 28: 656—715
42 Gao F, Qin S J, Wen Q Y, et al. One-time pads cannot be used to improve the efficiency of quantum communication. Phys Lett A, 2007, 365: 386—388[DOI]