中国科学: 物理学 力学 天文学 2010 年 第 40 卷 第 1 期: 26 ~ 32
www.scichina.com phys.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

论 文

基于对称密钥的量子公钥密码

高飞[①*], 温巧燕[①], 秦素娟[①], 朱甫臣[②]

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 现代通信国家重点实验室, 四川成都 810 信箱 610041
* E-mail: gaofei_bupt@hotmail.com

收稿日期: 2009-05-31; 接受日期: 2009-08-19
国家自然科学基金(批准号: 60873191, 60821001 和 60903152)、高等学校博士学科点专项科研基金(编号: 200800131016)、北京市科技新星计划(编号: 2008B51)、教育部科学技术研究重点项目(编号: 109014)、北京市自然科学基金(编号: 4072020)、现代通信国家重点实验室基金(编号: 9140C1101010601)和中国博士后科学基金(编号: 20090450018)资助项目

摘要 提出了一种基于量子加密的量子公钥密码(Quantum Public-key Cryptography, QPKC)方案, 构造了一个 QPKC 系统的完整理论框架, 并分析了该方案的安全性和特点. 分析表明, 量子力学特性使得基于对称密钥构建QPKC成为可能, 这与经典公钥密码体制中的情况大相径庭. 此外, 对之前的 QPKC 方案提出了一种态估计攻击方法.

关键词
量子密码
公钥密码
纠缠

公钥密码(public-key cryptography, PKC)又称为非对称密码, 出现于 20 世纪 70 年代[1,2]. 其思想与之前的密码学体系大不相同, 引领了信息安全领域的技术变革. Rivest, Shamir 和 Adleman[2]在提出著名的 RSA 方案时指出, 一个 PKC 系统通常满足以下四个条件: (ⅰ) 用公钥 e 加密的消息可用私钥正确解密; (ⅱ) 加解密操作在计算上都是容易的; (ⅲ) 从公钥 e 求解私钥 d 在计算上是困难的; (ⅳ) 用私钥 d 加密的消息也可用公钥 e 正确解密. 由于能满足这些条件, PKC 可以很方便地用于分发密钥和数字签名[3].

我们知道, 大多数 PKC 方案对未来的量子计算机来说都是不安全的[4,5]. 因此人们希望找到能够像其它量子密码协议[6~8]那样可以对抗量子计算的公钥密码, 即所谓的量子公钥密码(Quantum Public-key Cryptography, QPKC)[9]. 目前相关研究可以分为两类. 一种是寻找量子计算下的难解问题, 并以此来设计 PKC[10~13]. 这类方案中密钥仍然由经典比特构成, 因此保持了 PKC 的灵活性. 但它们的安全性仍建立在计算复杂性假设之上. 为了简单我们称这类密码系统为第 I 类 QPKC. 另一种则类似于量子密钥分发(Quantum Key Distribution, QKD), 通过引入量子力学元素来追求具有完美安全性的 PKC[14,15]. 这类方案的安全性由物理原理保证, 但密钥通常由较难控制的量子比特组成, 因此 PKC 的灵活性往往会明显降低. 我们称这类密码系统为第 II 类 QPKC. 本文我们研究后者.

最近 Nikolopoulos[14]提出了一种基于单量子比特旋转的 QPKC 方案(GMN 方案), 其基本思想与 Gottesman[15]的方案相似. 本文我们将对 GMN 方案提出一种攻击方法, 并基于量子加密[16,17]给出一种新的QPKC理论框架. 我们的方案将Bell态中的两个粒子分别作为公钥和私钥. 由于这两个粒子都处于最大混合态, 本方案实际上是基于对称密钥构造了 QPKC 系统, 这一点对经典密码学来说是不可思议的. 分析表明, 正是量子力学特性使得这一有趣现象成为可能.

引用格式: 高飞, 温巧燕, 秦素娟, 等. 基于对称密钥的量子公钥密码. 中国科学: 物理学 力学 天文学, 2010, 40: 26 ~ 32

1　对 GMN 方案的安全性分析

我们首先来看 GMN 方案中是怎样制备密钥的. 用户(假设为 Bob)随机选择一个整数 n, 并从 Z_{2^n} 中独立选取 N 个整数 $s_1, s_2, \cdots, s_N$, 得到整数串 $\boldsymbol{s} = (s_1, s_2, \cdots, s_N)$. 然后 Bob 制备 N 个处于状态 $\{\hat{R}^{(j)}(s_j\theta_n)|0\rangle\}$ 的单粒子量子比特, 这里 $1 \leqslant j \leqslant N$, $\theta_n = \pi/2^{n-1}$, $\hat{R}$ 为旋转操作. 显然这些量子比特与 $\boldsymbol{s}$ 中的每个整数一一对应. 私钥即为 $d = \{n, \boldsymbol{s}\}$, $e = \{N, |\Psi_s^{(PK)}(\theta_n)\rangle\}$ 为公钥, 其中 $|\Psi_s^{(PK)}(\theta_n)\rangle$ 表示以上量子比特序列(状态).

正如文献[14]中分析的那样, 当 $n \gg 1$ 时私钥的熵很大, 并随着 n 的增大而递增. 相反, 攻击者 Eve 通过测量公钥只能得到有限的私钥信息, 其上界为 Holevo 量[18], 由所测量量子比特的个数所决定. 因此, 看起来只要 n 足够大, Bob 就可以发布很多份公钥, 同时保证私钥的保密性. 然而, 多份公钥的发布将给 Eve 带来成功窃听的机会. 通过直接对公钥进行测量, Eve 可以在一定程度上估计私钥的值, 并借此从密文中获得明文信息.

利用态估计的相关研究成果[19~21], 可以很方便地计算出 Eve 估计私钥时所能达到的精度. 在 GMN 方案中所有单粒子态都在 Bloch 球的 x-z 平面, 这种情况下通过最优联合测量可使估计结果与目标状态之间的保真度达到[20,21]

$$F = \frac{1}{2} + \frac{1}{2^{M+1}} \sum_{i=0}^{M-1} \sqrt{\binom{M}{i}\binom{M}{i+1}} \approx 1 - \frac{1}{4M}, \tag{1}$$

其中 M 代表目标态粒子的份数. 也就是说, 如果 Eve 有 M 份相同的未知 x-z 平面量子态 $|\psi\rangle$, 她可以通过态估计方法得到一个已知量子态 $|\psi'\rangle$ 使得 $|\langle\psi|\psi'\rangle|^2 = F$. 假设在 GMN 方案中 Eve 可以得到 K 份公钥, 我们以其中一个量子态 $|\psi_{s_j}\rangle$ 为例来展开分析. 这种情况下 Eve 可以通过最优联合测量得到一个估计态 $|\psi'_{s_j}\rangle$, 使得 $|\langle\psi_{s_j}|\psi'_{s_j}\rangle|^2 \approx 1 - 1/(4K)$. 这样 Eve 就可以构造出测量基 $B_{s_j} = \{|\psi'_{s_j}\rangle, |\psi'^{\perp}_{s_j}\rangle\}$, 并能用它测量任何单粒子量子态($|\psi'^{\perp}_{s_j}\rangle$ 表示与 $|\psi'_{s_j}\rangle$ 正交的量子态).

在 GMN 方案中, 密文 $|\psi_{s_j}\rangle$ 和 $|\psi^{\perp}_{s_j}\rangle$ 分别对应于明文比特 $m_j = 0$ 和 1. 因此, Eve 可以截获发送者 Alice 发出的密文量子比特, 并用 B_{s_j} 基测量, 这样就可以判断出相应的明文比特. 因为 $|\psi'_{s_j}\rangle$ 和 $|\psi_{s_j}\rangle$ 在 Bloch 球上很接近, Eve 将以很大的概率 $P_c = F$ 获得正确的明文比特 m_j. 于是 Eve 获得的关于 m_j 的信息量为

$$\begin{aligned} I(A,E) &= H(A) - H(A|E) \\ &= 1 - 2[F\log F + (1-F)\log(1-F)], \end{aligned} \tag{2}$$

其中 A 和 E 分别表示 Alice 和 Eve.

现在来考虑 Eve 攻击时所引入的干扰, 这一点在文献[14]中并没有提到. 为了避免在上述攻击中被发现, Eve 可以在测量结束后将所得的量子态 $|\psi'_{s_j}\rangle$ 或 $|\psi'^{\perp}_{s_j}\rangle$ 重发给 Bob. 这样出现错误的概率为

$$P_e = 2F(1-F). \tag{3}$$

由(2)和(3)式可见, 当 K 较大时, Eve 能够得到几乎全部明文, 同时仅引入很小的错误率, 见表 1 和图 1.

表 1　不同 K 值对应的 $I(A,E)$ 和 P_e

	K=10	K=20	K=50	K=100	K=1000
$I(A,E)$	0.6627	0.8061	0.9092	0.9496	0.9933
P_e	0.0488	0.0247	0.0100	0.0050	0.0005

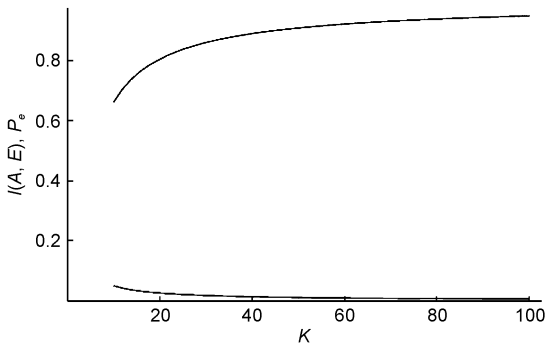

图 1　$I(A,E)$ 和 P_e 的函数图

横轴为 K 值, 上下两条曲线分别为 $I(A,E)$ 和 P_e

最后, 文献[14]及最近的勘误[22]中提到, 每个明文比特可加密到多个量子比特中以抵抗交换测试攻击(SWAP-test attack). 这种情形下, 上述攻击方法的攻击效率将会下降. 然而作为对 QPKC 的一种特殊攻击方法, 态估计攻击看起来更加直接和现实, 因此值得在今后的研究中予以关注.

2 基于量子加密的 QPKC

以上分析表明, 之前的 QPKC 方案容易受到态估计攻击的威胁. 具体来说, 虽然 Eve 不能通过对多份公钥的测量来得到确切的私钥, 但她可以估计私钥的值并据此从密文中提取明文信息. 因此我们需要为 QPKC 寻找一种新的密钥生成方式. 这里我们给出一种使用 Bell 态粒子做密钥的方案, 同时像其它大多数量子密码协议中那样, 引入窃听检测步骤来保证此方案的安全性.

在描述具体方案之前, 我们需要先做以下三点假设: (ⅰ) 在 QPKC 系统中有一个可信中心 Trent; (ⅱ) Trent 可以在通信中认证每个用户的身份, 这一点可以用量子认证协议来完成[23,24]; (iii) 经典信道中传输的消息可以被窃听, 但不能被修改. 这三点都是 PKC(如ⅰ和ⅱ)和量子密码(如iii)中已被广泛接受的基本假设.

此方案具体步骤如下:

阶段 1 密钥制备. Trent 为每个用户产生一对密钥, 即公钥 e 和私钥 d. 这里以 Bob 为例来介绍, 具体过程如下:

(ⅰ) Trent 制备一系列量子比特对 $\boldsymbol{S}_1=\{(p_1,q_1),(p_2,q_2),\cdots,(p_n,q_n)\}$, 每一对都处于 Bell 态

$$\left|\Phi^+\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right) \tag{4}$$

这些粒子构成两个量子比特串 $\boldsymbol{S}_p=\{p_1,p_2,\cdots,p_n\}$ 和 $\boldsymbol{S}_q=\{q_1,q_2,\cdots,q_n\}$, 将分别被用作 Bob 的公钥和私钥.

(ⅱ) 为把 $\boldsymbol{S}_q$ 安全地传输给 Bob, Trent 制备一定数量的诱骗态(decoy state) $\boldsymbol{S}_d=\{d_1,d_2,\cdots,d_k\}$, 其中每个粒子随机处于 $\{\left|0\right\rangle,\left|1\right\rangle$, $\left|+\right\rangle=1/\sqrt{2}(\left|0\right\rangle+\left|1\right\rangle)$, $\left|-\right\rangle=1/\sqrt{2}(\left|0\right\rangle-\left|1\right\rangle)\}$ 四种状态之一.

(iii) Trent 将 $\boldsymbol{S}_d$ 中的每个粒子穿插进序列 $\boldsymbol{S}_q$ 中的随机位置, 得到一个新序列 $\boldsymbol{S}_{qd}$. 然后通过量子信道将 $\boldsymbol{S}_{qd}$ 发送给 Bob.

(ⅳ) Bob 收到这些粒子以后, Trent 将每个诱骗态的位置和所在的基(即 $B_z=\{\left|0\right\rangle,\left|1\right\rangle\}$ 或 $B_x=\{\left|+\right\rangle,\left|-\right\rangle\}$)告诉 Bob.

(ⅴ) Bob 用相应的基测量所有诱骗态粒子, 并公开测量结果给 Trent. 这样 Trent 就可以通过比较这些粒子的初态和测量结果来判断这个序列在传输过程中是否被窃听过.

(ⅵ) 如果没有发现窃听, Bob 就顺利得到了他的私钥 d, 即序列 S_q. 与此同时, Trent 保存 Bob 的公钥 e, 即 S_p. 否则将退出这次通信.

在后续步骤中我们会看到, 用这些密钥来加密消息可能不够长, 而且它们会被逐渐消耗掉. 然而一旦需要, Trent 随时可以再制备 Bell 态来补充密钥.

阶段 2 加密. 假设用户 Alice 想发送 r 比特消息 $\boldsymbol{m}=\{m_1,m_2,\cdots,m_r\}$ 给 Bob, 其中 $m_i=0$ 或 1, 且 $r\leqslant n$. 那么 Alice 可以通过以下步骤来加密消息:

(ⅰ) Alice 请求 Trent 将 Bob 公钥中的 r 个量子比特发送给她.

(ⅱ) Trent 将序列 $\boldsymbol{S}_p$ 中的前 r 个粒子发送给 Alice. 这里我们用 $\boldsymbol{S}_p^r$ 来表示这部分粒子序列, 即 $\boldsymbol{S}_p^r=\{p_1,p_2,\cdots,p_r\}$. 与阶段 1 中类似, Trent 也使用诱骗态来确保粒子传输过程中的安全性.

(iii) Alice 制备 r 粒子序列 $\boldsymbol{L}=\{l_1,l_2,\cdots,l_r\}$, 粒子状态分别为 $\{\left|m_1\right\rangle,\left|m_2\right\rangle,\cdots,\left|m_r\right\rangle\}$, 与要加密的消息比特一一对应.

(ⅳ) Alice 用公钥 $\boldsymbol{S}_p^r$ 加密消息序列 $\boldsymbol{L}$. 具体地, Alice 通过 CNOT 操作用 $\boldsymbol{S}_p^r$ 中的粒子来加密每个对应的消息粒子. 举例来说, Alice 通过对粒子 p_i 和 l_i 执行 CNOT 操作 $C_{p_il_i}$ (前一个下标 p_i 代表控制粒子, 后一个下标代表目标粒子)来加密 l_i, 即

$$C_{p_il_i}\left|\Phi^+\right\rangle_{p_iq_i}\left|m_i\right\rangle_{l_i}=\frac{1}{\sqrt{2}}\left(\left|00m_i\right\rangle+\left|11\overline{m}_i\right\rangle\right)_{p_iq_il_i}. \tag{5}$$

其中 $\overline{m}_i=1-m_i$.

(ⅴ) 加密完所有的消息粒子后, Alice 将序列 L(密文)发送给 Bob.

阶段 3 解密. Bob 收到粒子序列以后, 可以执行以下步骤来解密出消息 m:

(ⅰ) 对密文 L 中的每一个粒子, Bob 执行 CNOT 操作 $C_{q_i l_i}$ 来解密. 操作后系统状态变为

$$C_{q_i l_i}\frac{1}{\sqrt{2}}\left(\left|00m_i\right\rangle+\left|11\overline{m_i}\right\rangle\right)_{p_i q_i l_i}=\left|\Phi^+\right\rangle_{p_i q_i}\left|m_i\right\rangle_{l_i}. \quad (6)$$

(ⅱ) Bob 用 B_z 测量中 L 的每个粒子. 从式(6)可知, 所有测量结果恰好就是明文消息 m. 至此 Bob 得到 Alice 发来的消息, 解密过程结束.

阶段 4 密钥回收. 上面的通信过程具有一个优点, 即加解密步骤完成后 Bob 的密钥状态没有改变. 因此这些密钥可以按照以下步骤进行回收:

(ⅰ) Alice 将 Bob 的公钥(即粒子序列 $\boldsymbol{S}_p^r$)发回给 Trent.

(ⅱ) 为了确保这些回收密钥的安全性, Trent 从 $\boldsymbol{S}_p^r$ 中随机选择一定数量的粒子作为检测粒子, 并随机用 B_z 或 B_x 基测量每个检测粒子以检测窃听.

(ⅲ) Trent 将每个检测粒子的位置和测量基告诉 Bob.

(ⅳ) Bob 用相同的基测量其私钥中相应位置的粒子, 并公开测量结果. 因为每两个对应粒子都应该处于 Bell 态 $\left|\Phi^+\right\rangle$, 测量结果将呈现确定的关联关系.

(ⅴ) 通过比较这些测量结果, Trent 能够判断出回收的公钥是否被攻击过. 如果没有, Trent 和 Bob 就留下其余的粒子以备下次使用. 否则他们抛弃这些回收的密钥.

以上就是基于量子加密的 QPKC 方案. 从中可以看出, 公钥和私钥粒子都来自于 Bell 态 $\left|\Phi^+\right\rangle$, 且处于相同的状态, 即最大混合态 $\rho=1/2(|0\rangle\langle 0|+|1\rangle\langle 1|)$. 因此, 一个有趣的现象发生了, 即在这个 QPKC 方案中实际上实用了对称密钥, 其基本思想类似于量子 Vernam 密码[25]. 我们知道, 经典密码中的 Vernam 算法(即一次一密乱码本)[26]不能用于 PKC, 因为它的加解密密钥相同, 可以被任意复制. 但在量子密码中情况完全不同. 具体来说, 即使公钥和私钥处于相同状态, 人们也不能通过复制加密密钥(即公钥)来得到解密密钥(即私钥), 这一点由量子不可克隆定理来保证[27].

最后, 关于以上 QPKC 方案, 还有几点需要说明. (ⅰ) 实际上 Alice 得到的公钥是 $\boldsymbol{S}_p$ 的一个子串. 在 Alice 收到这些粒子以后, Trent 需要告诉 Bob 他把 $\boldsymbol{S}_p$ 的哪个子串发给了 Alice, 这样 Bob 就可以用对应的私钥粒子来解密 Alice 发来的密文. (ⅱ) 此方案中, Alice 和 Bob 可以使用消息认证码来对抗拒绝服务(Denial-of-Service, DoS)攻击[28,29]. (ⅲ) 当考虑信道噪声的时候, 可以利用纠缠纯化[30,31]和量子保密放大[32]技术来提高传输后 Bell 态的质量.

3 安全性分析

对一个 QPKC 系统来说, 必须保证 Eve 不能获得 Bob 的私钥或者 Alice 的明文消息. 在上述方案中利用了一些常见且可靠的方法来保证安全性. 例如使用 BB84 类粒子作诱骗态来保证量子序列传输的安全, 用共轭基测量的方法来确定回收密钥粒子的状态. 下面我们针对不同阶段来简要分析此方案的安全性.

密钥制备. 在这一阶段 Trent 制备一定量的 EPR 对 $\left|\Phi^+\right\rangle$ 并将每对中的一个粒子(即序列 $\boldsymbol{S}_q$)发送给 Bob 作为他的私钥. 因为 Trent 是可信的, 我们只需要考虑外部窃听者 Eve 的攻击. 在这一阶段, Eve 有机会获得 Bob 的私钥, 并可能利用它正确解密发给 Bob 的密文. 然而由于诱骗态的使用, Eve 的目的将不能达到. 原因如下:

首先, 量子不可克隆定理[27]保证了 Eve 不能复制私钥中的量子比特. 这一点与经典 PKC 截然不同. 后者中私钥是不能公开传输的, 因为它由经典比特组成, 很容易被复制.

其次, 因为诱骗态粒子与私钥粒子处于相同的状态, 即最大混合态 $\rho=1/2(|0\rangle\langle 0|+|1\rangle\langle 1|)$, 任何人不能通过测量来区分这两类粒子. 这就意味着任何针对私钥粒子的攻击操作也都将会不可避免地作用到诱骗态粒子上. 因此, 这种攻击操作将在诱骗态上留下痕迹, 进而被合法用户所发现. 这里我们将不再详细论证使用这种诱骗态所带来的安全性, 它与 BB84 协议的安全性类似并已经获得广泛认可[33].

加密. 正如上节所述, 在我们的 QPKC 方案中使用了对称密钥, 即公钥与私钥处于相同的量子态. 因此任何拥有公钥的人也可以解密相应的密文. 本阶段中 Eve 有机会在 Trent 发送公钥给 Alice 时截获它.

但是与阶段 1 中类似, 这些量子态不能被复制, 且诱骗态能保证公钥粒子序列的安全. 于是任何对公钥的有效窃听都将被合法用户所发现.

此外, 我们还需要分析当 Alice 传送密文给 Bob 时 Eve 可以从中得到什么. 上述分析已经表明, 如果 Eve 不想被发现, 她从信道中传输的公钥和私钥序列中得不到任何有用信息. 这种情况下 Eve 不能从密文中获得明文的任何信息, 因为不管消息比特是 0 还是 1, 每个密文量子比特都处于相同的态 $\rho=1/2(|0\rangle\langle 0|+|1\rangle\langle 1|)$.

解密. 本阶段由于没有粒子在信道中传输, Eve 没有攻击的机会. 当 Bob 解密出明文后, 他可以利用消息认证码来判断是否存在 DoS 攻击.

密钥回收. 本阶段中 Alice 将公钥发回给 Trent. 从 Eve 的角度来说, 这种情况与阶段 2 初期的传输非常类似. 但这里我们还需要考虑 Alice 的攻击. 因为回收的公钥将被在今后其他人(如 Charlie)与 Bob 通信时重复使用, Alice 也可能会采取一定的手段来进行攻击. 例如 Alice 可以将一个附加粒子纠缠进每个 Bell 态, 并用它解密今后 Charlie 给 Bob 的密文(类似于文献[34,35]中的攻击策略).

考虑到以上威胁, Trent 必须保证 Alice 发回的公钥量子比特的状态没有发生变化(即每个公钥粒子都还与 Bob 手中相应的私钥粒子处于 Bell 态 $|\Phi^+\rangle$). 我们的方案中采用了共轭基测量的方法来检测窃听, 它可以同时抵抗 Eve 和 Alice 的攻击. 这种方法的可靠性已经被证明并广泛应用[36~39], 这里我们将不再做详细分析.

最后, 我们知道在实际 QKD 系统中, Eve 可以只攻击一小部分传输的粒子, 这样引入的干扰就比较小, 可以被信道噪声所掩盖. 这种情况下用户可以对生密钥进行保密放大[40]来获得无条件安全的密钥. 在我们的 QPKC 中也存在类似问题. Eve 可通过攻击小部分密钥粒子, 进而获得部分明文信息. 这种情况下可以使用纠缠纯化[30,31]和量子保密放大[32]的方法, 这些技术可使此方案达到理论上的无条件安全性.

4 讨论与结论

与之前的 QPKC 方案(GMN 方案)相比, 我们的方案具有以下特点:

(ⅰ) 公钥与私钥的作用相同, 满足第 1 节中所述的 PKC 基本条件(ⅳ). 这种情况下用户也可以用私钥来加密消息, 而用公钥正确解密. 这就使得基于本方案设计量子签名协议[41]成为可能;

(ⅱ) 给出了公钥的验证方法, 这一点对 QPKC 系统的安全性至关重要. 一方面利用诱骗态来保护公钥量子比特, 使之不受 Eve 的攻击. 另一方面因为密钥粒子均来自于 Bell 态 $|\Phi^+\rangle$, 对它们进行纠缠纯化和量子保密放大都比较容易(已有相关理论[30~32]). 通过这些技术, 即使在有噪情况下通信双方也能获得高质量的 Bell 态. 也就是说, 本方案中公钥的状态可以得到认证;

(ⅲ) 可以抵抗态估计攻击. 本方案中不同的公钥由来自于不同 EPR 对的粒子组成, 它们之间没有任何关联. 因此拥有多份公钥还是一份公钥对 Eve 来说效果是一样的, 即 Eve 不能从多份公钥中获得更多有用信息;

(ⅳ) 密钥可以重复使用, 并可在必要时随意补充.

有些学者可能会觉得我们的方案看起来不像是一个实际的公钥密码体制(例如 RSA 等常见经典 PKC 方案), 原因有两点: (ⅰ) 本方案中用到了类似 QKD 中那样的方法来检测窃听; (ⅱ) 本方案使用对称密钥. 需要强调的是, 这两点看似不符合公钥密码特征的性质, 都是由 QPKC 的量子本质所决定的. 下面我们分别予以解释:

(ⅰ) 众所周知, 量子力学特性使得合法通信者可以检测到潜在的窃听行为, 这正是量子密码可达到无条件安全的本质原因. 为了实现这一优势, 协议中的窃听检测过程是必要的. 由于 QPKC 中的公钥一般是量子的, 其状态在传输之后需要验证, 所以 QPKC 系统中也同样如此. GMN 方案中之所以没有这些检测步骤, 是因为文献[14]中没有考虑公钥认证的问题;

(ⅱ) 本方案中选择 Bell 态粒子做密钥, 最初的目的是避免态估计攻击的影响. 目前来看, Bell 态非常适合用于 QPKC, 这是因为我们可以用现有技术来对它进行认证(特别是纠缠纯化和量子保密放大). 虽然之前的协议并没有涉及, 但量子密钥的认证对一个 QPKC 系统的安全性来说无疑是非常重要的. 我们知道, 在经典 PKC 系统中绝对不能使用相同的公

钥和私钥, 否则任何人都可以通过对公钥的拷贝来获得私钥, 进而正确解密所有相应的密文. 因此人们的确需要设计出非对称密码体制, 使得 Eve 不能从公钥中得到私钥. 然而在量子情形下, 情况将大不相同. 一方面, 量子不可克隆定理不允许对量子比特的拷贝. 另一方面, QPKC 中必须对(量子)公钥进行认证, 而一旦认证通过, 那就意味着 Eve 没有从公钥中读出任何有用信息(否则 Eve 的窃听必将引入干扰, 进而被用户检测到). 在这种情况下, 我们似乎没有任何必要再特意去设计两个不同的密钥. 也就是说, 在 QPKC 中用相同的密钥就可以了. 实际上我们的方案及相关分析已经表明, 在 QPKC 中使用对称密钥是可行的, 这一有趣现象正是量子力学特性所带来的.

综上所述, 我们提出了一个新的 QPKC 方案, 并初步构建了 QPKC 系统的完整理论框架. 分析表明在 QPKC 中可以使用对称密钥, 这一点与经典 PKC 中的情况完全不同. 同时分析了本方案的安全性及特点. 此外, 我们还给出了一种对 GMN 方案[14]的特殊攻击方法. 自量子密码出现以来, 各国学者一直希望能设计出一种量子公钥密码体制, 它既能像 QKD 那样具有无条件安全性, 又能像经典 PKC 那样灵活易用. 但要设计出真正实用的 QPKC 系统, 或者探索这种系统的可行性, 仍旧是一件很困难的工作, 需要进一步的深入研究.

参考文献

1 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inform Theory, 1976, 22: 644—654[DOI]

2 Rivest R L, Shamir A, Adleman L A. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM, 1978, 21: 120—126[DOI]

3 Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd ed. New York: John Wiley and Sons, 1996. 24—29

4 Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science. Los Alamitos: IEEE, 1994. 124—134

5 Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM, 1996. 212—219

6 高飞, 郭奋卓, 温巧燕, 等. 重新审视量子对话和双向量子安全直接通信的安全性. 中国科学 G 辑: 物理学 力学 天文学, 2008, 38(5): 477—484

7 Chen W, Han Z F, Mo X F, et al. Active phase compensation of quantum key distribution system. Chinese Sci Bull, 2008, 53: 1310—1314[DOI]

8 高飞, 郭奋卓, 温巧燕, 等. ping-pong 协议中不同检测策略的效率比较. 中国科学 G 辑: 物理学 力学 天文学, 2009, 39(2): 161—166

9 曾贵华. 量子密码学. 北京: 科学出版社, 2006. 147—153

10 Okamoto T, Tanaka K, Uchiyama S. Quantum public-key cryptosystems. In: Advances in Cryptology: Crypto 2000 Proceedings. Berlin: Springer, 2000. 1880: 147—165

11 Kawachi A, Koshiba T, Nishimura H, et al. Computational indistinguishability between quantum states and its cryptographic application. In: Advances in Cryptology: Eurocrypt 2005 Proceedings. Berlin: Springer, 2005. 3494: 268—284

12 Yang L. Quantum public-key cryptosystem based on classical NP-complete problem. arXiv: quant-ph /0310076

13 Koshiba T. Security notions for quantum public-key cryptography. arXiv: quant-ph/0702183

14 Nikolopoulos G M. Applications of single-qubit rotations in quantum public-key cryptography. Phys Rev A, 2008, 77: 032348[DOI]

15 Gottesman D, Chuang I L. Quantum digital signatures. arXiv: quant-ph/0105032

16 Zhang Y S, Li C F, Guo G C. Quantum key distribution via quantum encryption. Phys Rev A, 2001, 64: 024302[DOI]

17 Zeng G H. Encrypting binary bits via quantum cryptography. Chinese J Electron, 2004, 13: 651—653

18 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 531—533[DOI]

19 Massar S, Popescu S. Optimal extraction of information from finite quantum ensembles. Phys Rev Lett, 1995, 74: 1259—1263[DOI]

20 Derka R, Buzek V, Ekert A. K. Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement. Phys Rev Lett, 1998, 80: 1571—1575[DOI]

21 Bagan E, Baig M, Munoz-Tapia R. Optimal scheme for estimating a pure qubit state via local measurements. Phys Rev Lett, 2002, 89:

277904[DOI]
22 Nikolopoulos G M. Erratum: Applications of single-qubit rotations in quantum public-key cryptography. Phys Rev A, 2008, 78: 019903[DOI]
23 Dusek M, Haderka O, Hendrych M, et al. Quantum identification system. Phys Rev A, 1999, 60: 149—156[DOI]
24 Zeng G H, Zhang W P. Identity verification in quantum key distribution. Phys Rev A, 2000, 61: 022303[DOI]
25 Leung D W. Quantum Vernam cipher. Quantum Inf Comput, 2002, 2: 14—34
26 Vernam G S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. J Am Inst Elect Eng, 1926, 55: 109—115
27 Wootters W K, Zurek W H. A single quantum cannot be cloned. Nature (London), 1982, 299: 802—803[DOI]
28 Cai Q Y. The "Ping-Pong" protocol can be attacked without eavesdropping. Phys Rev Lett, 2003, 91: 109801[DOI]
29 Gao F, Guo F Z, Wen Q Y, et al. Consistency of shared reference frames should be reexamined. Phys Rev A, 2008, 77: 014302[DOI]
30 Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett, 1996, 76: 722—725[DOI]
31 Pan J W, Gasparoni S, Ursin R, et al. Experimental entanglement purification of arbitrary unknown states. Nature (London), 2003, 423: 417—422[DOI]
32 Deutsch D, Ekert A, Jozsa R, et al. Quantum privacy amplification and the security of quantum cryptography over noisy channels. Phys Rev Lett, 1996, 77: 2818—2821[DOI]
33 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050—2056[DOI]
34 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]
35 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]
36 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell theorem. Phys Rev Lett, 1992, 68: 557—559[DOI]
37 Waks E, Zeevi A, Yamamoto Y. Security of quantum key distribution with entangled photons against individual attacks. Phys Rev A, 2002, 65: 052310[DOI]
38 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319[DOI]
39 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]
40 Bennett C H, Brassard G, Robert J. Privacy amplification by public discussion. SIAM J Comput, 1988, 17: 210—229[DOI]
41 Zeng G H, Keitel C H. Arbitrated quantum-signature scheme. Phys Rev A, 2002, 65: 042312[DOI]