doi:10.3969/j.issn.1000-436x.2014.z2.002

基于单粒子的量子公钥加密协议

罗文俊，刘冠丽
（重庆邮电大学 计算机科学与技术学院，重庆 400065）

摘 要：提出一种基于单粒子的量子公钥加密协议。利用随机序列的映射关系对私钥实施量子操作，生成用于消息加密的量子公钥。根据量子不可克隆和密文不可分辨定理，引入新的量子源作为通信传输的载体，设计了易操作的加密编码和解密规则；采用分块的方法，优化了窃听检测方法，降低了对发送方存储能力的要求；结合一次一密的加密方案，保证了在量子通信信道中传送密钥和消息的安全性。基于纠缠态的量子加密算法和基于单粒子的量子公钥加密方案相比较，所提出的协议易于实现，具有良好的使用价值。分析表明，本协议是安全的。
关键词：公钥；量子加密；单粒子；量子选择明文攻击
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0009-05

Quantum public-key encryption protocol based on single-photon

LUO Wen-jun, LIU Guan-li
（College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China）

Abstract: A quantum public-key encryption protocol based on single-photon was provided. Pseudo random sequence mapping to private keys to implement corresponding quantum operations and then obtaining quantum public-key to encode the plaintext was used. Employ the method of block classification to lower the requirement for storage capacity of the sender. A new quantum source as transmission carrier was introduced and simply encoding and decoding rules were designed based on the laws of quantum non-cloning and ciphertext indistinguishability. On the other hand, classical one-time pad technique is used to ensure the security of quantum key and plaintext in the transmission channel. At the same time, select different updating strategy of quantum public-key according to the results of error detection which can significantly reduce key consumption. Compared with the previous quantum public-key encryption based on entangled states and single-photon, there are no entangled states and decoyed particles are needed, so it is not only efficient to reduce the overhead of communication traffic between legitimate users, but also easier to carry out in practice. The analysis shows that the proposed scheme is secure.
Key words: public-key; quantum cryptography; single-photon; quantum chosen plaintext attack

1 引言

量子密码是以经典密码学和量子力学为基础的一种新型的密码体制。随着量子密码学、量子计算和量子信息论研究的不断发展，特别是著名的量子算法——Shor 算法和 Grover 算法的提出，对基于数学难题的传统密码体制的安全性提出了严峻的挑战。为了寻找一种能够抗量子计算能力和具有可证明的无条件安全密码体制，IBM 公司的 Bennett 和 Brassard 于 1984 年共同提出了量子密钥分发(QKD, quantum key distribution)协议，即 BB84 协议[1]，为量子密码学的研究奠定了基础。随后，各种相应

收稿日期：2014-10-24
基金项目：重庆市高校创新团队建设计划基金资助项目（KJTD201310）；国家社会科学基金资助项目（14CTQ026）；重庆市基础与前沿技术研究基金资助项目（cstc2014jcyjA40028）
Foundation Items: The Program for Innovation Team Building at Institutions of Higher Education in Chongqing (KJTD201310); The National Social Science Foundation of China (14CTQ026); The Chongqing Research Program of Application Foundation and Advanced Technology(cstc2014jcyjA40028)

的 QKD 协议相继提出[2~7]。由量子力学的测不准原理，QKD 能够提供可证明的安全性和对窃听者的检测性。大多数 QKD 主要是采用对称加密算法来实现密钥分发，操作简单，效率高。但当需要多个用户进行通信时，密钥管理便成了难题。

量子公钥密码(QPKE, quantum public-key encryption)是解决密钥管理问题的好方法。相对于传统的公钥密码，由于其安全性不在依赖数学难题，而是基于量子力学原理。因此，QPKE 不但可以实现具有可计算安全的密钥分配协议，而且能够设计并实现无条件安全的公钥加密算法。Okamoto 等[8]首先提出了基于背包难题的子集和的 QPKE 方案。尽管该方案的公私钥、明文和密文都是经典形式，但是其密钥生成是由量子算法构成的。Gottesman 和 Chuang[9]首次采用量子态作为公钥，构建量子和经典相结合的量子公钥加密体制雏形。Nikolopoulost[10]首次提出了一种基于单粒子比特旋转的量子公钥密码体制，通过随机旋转特定的量子态作为量子公钥来加密传递的消息。Seyfarth 等[11]在 Nikolopoulost 方案的基础上，分析并证明了量子单向函数的量子公钥方案能够更有效地解决密钥泄露的问题。Yang 等[12]引入量子单向陷门函数的概念，构建了融入 RSA、ELGamal、McEliece、Niederreiter 等算法的 QPKE 协议。随后 Yang[13]构建了基于经典困难问题的 QPKE。Min 和 Yang[14]构建了经典和量子环境下的 QPKE 模型，并给出了详细的分析证明。Pan 和 Yang[15]提出了基于共轭编码的单比特和多比特的 QPKE 方案，并证明所设计方案是无条件安全的。之后，众多 QPKE 方案被相继提出[16~20]。其中，Liang 等[17]提出了量子单向函数和量子单向陷门函数的概念，给出了构建量子单向陷门函数的理论模型。相对 QKD 而言，基于经典算法的 QPKE 的安全核心是单向陷门函数的构建，但量子单向陷门函数的计算复杂度较高，使加解密效率不高。为了既能很好地解决密钥管理问题，又能保证安全性和提高加解密效率，Li 等[19]提出了基于非正交态单粒子的量子公钥密码，其原理是引入密钥管理中心(KMC, key management center)对非正交的单粒子密钥进行管理和分发，采用简单的加密解密操作，具有较好的实用价值。

利用量子的特性，提出了一种基于单粒子的量子公钥加密协议。该协议采用新的量子源作为私钥和公钥，通过随机序列对私钥实施相应的量子幺正变换生成公钥。根据量子不可克隆性和密文不可分辨性原理，结合传统的一次一密方法，保证通信过程中密文和私钥的安全。由于本方案不需要制备纠缠态和 Bell 测量，操作简单，易于实现，采用了分块的思想，优化了诱骗粒子窃听检测方法，降低了对用户双方的存储能力，确保合法用户间的通信；通过错误检测的结果选择不同的密钥更新策略，使密钥可以重复利用，提高了密钥的利用率。

2 理论知识

2.1 不可克隆性

Wootters 和 Zurek[21]于 1982 年首次提出了著名的量子不可克隆定理，其定义如下。

定理 1 在量子力学中，不存在这样的一个物理过程：实现对一个未知量子态的精确复制，使每个复制态与初始量子态完全相同[21]。

假设对任意的量子比特$|\psi\rangle$进行克隆，引入量子比特初始态$|s\rangle$作为克隆的载体，其目的是通过利用任意的幺正操作 U 将克隆量子比特从$|s\rangle$态变为$|\psi\rangle$态，并且保证不破坏被克隆的量子比特。具体推算过程如下

$$|\psi\rangle\otimes|s\rangle\to U\left(|\psi\rangle\otimes|s\rangle\right)=|\psi\rangle\otimes|\psi\rangle \tag{1}$$

因为未知量子比特不可能精确复制，使每个复制比特与初始量子比特不可能完全相同。如果克隆的过程可以表示成一个幺正演化过程，那么根据幺正性的要求，2 个量子态能够被相同的物理过程克隆的前提条件是当且仅当它们相互正交。如果 2 个量子态是非正交态，则不可克隆。所以式(1)的推算过程不可能成立。

2.2 无条件安全

定义 1 当 n 足够大时，对于任意量子线路集合$\{C_n\}$和正多项式 $poly(\cdot)$，对于任意 2 个经典比特信息 x 和 y，其相同的概率 $\Pr(\cdot)$ 满足式(2)，则证明 QPKE 方案具有抵抗适应性的选择明文攻击(QCPA, quantum chosen plaintext attack)，即密文不可区分性。

$$\left|\Pr\left[C_n(F(1^n),E_{F(1^n)}(x))=1\right]-\Pr\left[C_n(F(1^n),E_{F(1^n)}(y))=1\right]\right|<\frac{1}{poly(n)} \tag{2}$$

定理 2 当 n 足够大时，对于任一正多项式 $poly(\cdot)$，存在 2 个任意的经典比特信息 x 和 y，满足式(3)成立，则认为该协议是具有无条件安全的。

$$D(E(x),E(y))<\frac{1}{poly(n)} \tag{3}$$

其中，E 是一个量子加密算法，F 是量子密钥生成算法，$E(x)$和 $E(y)$表示为加密密文的量子态。详细的证明过程可参见文献[14]。

3　方案描述

提出一种新的基于单粒子的量子公钥加密协议。假设 Alice 为消息发送者，Bob 为消息接收者。

3.1　密钥生成

步骤 1　Bob 制备私钥序列 $K_{\text{private}}=\{|\varphi_1\rangle,|\varphi_2\rangle,\cdots,|\varphi_n\rangle \,|\, |\varphi_i\rangle\in\{|+\rangle,|-\rangle,|+y\rangle,|-y\rangle\}\ i=1,2,\cdots,n\}$，其中 $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ 和 $|\pm y\rangle=(|0\rangle\pm i|1\rangle)/\sqrt{2}$，并记录值。

步骤 2　Bob 随机选择多项式函数 $f:\{0,1\}^n\to\{0,1\}^n$ 和随机串 $l\in\{0,1\}^n$，计算 $f(l)$ 并将结果记录为 $P=\{P_1,P_2,\cdots,P_n\}$。Bob 根据 P 的元素值对 K_{private} 实施量子幺正变换，形成公钥 $K_{\text{public}}=\{|K_1\rangle,|K_2\rangle,\cdots,|K_n\rangle\}$，即 P 中的第 j 个元素为 1 时，则对私钥 K_{private} 中的第 j 个单粒子实施 S 变换，否则实行 Z 变换，具体过程如式(4)所示。

$$|K_i\rangle=\begin{cases}Z|\varphi_i\rangle, P_i=0\\ S|\varphi_i\rangle, P_i=1\end{cases}\quad i=1,2,\cdots,n \tag{4}$$

其中，$Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$，$S=\begin{pmatrix}1&0\\0&i\end{pmatrix}$。

3.2　加密

假设 Alice 想要发送 $r(r\leqslant n)$ 比特消息 $M=\{m_1,m_2,\cdots,m_r \,|\, m_i\in\{0,1\},i=1,2,\cdots,r\}$ 给 Bob。Alice 可以通过以下步骤加密消息 M。

步骤 1　Alice 请求下载 Bob 公钥 K_{public} 中的 r 量子比特。收到请求后，Bob 随机地在公钥 $K_{\text{public}}=\{|K_1\rangle,|K_2\rangle,\cdots,|K_N\rangle\}$ 中选取 r 量子比特作为此次公钥 $K_{\text{public}}^r=\{|K_1\rangle,|K_2\rangle,\cdots,|K_i\rangle\},i=1,2,\cdots,r$，并记录 K_{public}^r 所对应的 K_{private} 和 P 的值。接着，Bob 从集合 $\{|+\rangle,|-\rangle\}$ 中随机选取 h 量子比特并随机插入到 K_{public}^r 中，形成新序列 K_{public}^{r+h} 发送给 Alice。

步骤 2　Alice 收到 K_{public}^{r+h} 后进行简单的延时。Bob 在确定 Alice 收到公钥后，告知 Alice 随机插入的 h 位置。Alice 通过随机选择 $2/h$ 量子比特进行窃听检测，判断是否正确获取公钥。若检测出错率低于阈值，那么 Alice 告知 Bob 可以发送 K_{public}^r 所对应的测量基序列 $B=\{|B_1\rangle,|B_2\rangle,\cdots,|B_r\rangle\},i=1,2,\cdots,r$；否则重新下载 Bob 公钥。

步骤 3　Alice 根据相应的测量基进行测量，获得 K_{public}^r 并用于加密消息 M。然后，Alice 将剩余的 $2/h$ 量子比特随机插入到密文 φ_c 中，通过量子信道发送给 Bob。密文 φ_c 编码规则如下：若发送的消息 m_i=0，则对 $|K_i\rangle$ 实施 Z 变换；若发送的消息 m_i=1，则不做任何操作，即密文为 $\varphi_c=\{|\varphi_{c_1}\rangle,|\varphi_{c_2}\rangle,\cdots,|\varphi_{c_r}\rangle\}$，其中 $|\varphi_{c_i}\rangle=Z^{\bar{m}_i}|K_i\rangle,i=1,2,\cdots,r,\bar{m}=1-m$。

3.3　解密

Bob 接收到密文后，需执行以下步骤进行解密和更新公钥，具体过程如下。

步骤 1　Alice 告知 Bob 密文中插入的 $2/h$ 量子比特对应的位置，Bob 进行测量。如果测量得到的错误率高于阈值，那么 Bob 放弃通信并丢弃此次通信的公钥；如果错误率低于阈值，那么 Bob 随机丢弃 1/2 的量子公钥。

步骤 2　根据 K_{public}^r 所对应的伪随机序列 P_r 中的元素值，Bob 对密文 φ_c 中的每一个单粒子执行相应的操作。若 P_i=0，则 Bob 对密文 $|\varphi_{c_i}\rangle$ 不做任何操作；若 P_i=1，则对密文 $|\varphi_{c_i}\rangle$ 执行 S 变换，即 Bob 对密文 φ_c 执行操作后，密文状态变为

$$|\varphi'_{c_i}\rangle=\begin{cases}|\varphi_{c_i}\rangle, P_i=0\\ S|\varphi_{c_i}\rangle, P_i=1\end{cases},\quad i=1,2,\cdots,r \tag{5}$$

步骤 3　Bob 将记录的 K_{private}^r 值和密文 φ'_c 进行比较。如果 $|\varphi_i\rangle=|\varphi'_{c_i}\rangle$，那么 Alice 发送的消息 m_i 为 0 bit；如果 $|\varphi_i\rangle\neq|\varphi'_{c_i}\rangle$，那么消息 m_i 为 1 bit。最后，Bob 解密得到明文消息 M。

4　安全与有效性分析

4.1　安全性分析

假设存在窃听者 Eve，企图通过截获量子信道上传输的公钥或密文得到 Bob 的私钥或明文消息。下面从量子私钥和密文消息 2 个方面进行安全分析。

首先，对于方案中私钥，每一个 K_{private}，f 和 l 都是随机选取的。根据 $f(l)$计算的值 P，Bob 对 K_{private}

实施幺正变换，生成公钥 K_{public}。假设 Eve 试图通过随机选择测量基来猜测 K_{public} 并获取 K_{private} 的值。那么 Eve 在未知公钥测量基的情况下，要想通过猜测获得正确的私钥的概率为

$$P_{\text{correct}}=\left(\frac{1}{4}\times\left(\frac{1}{2}\times\frac{1}{2}+1\times\frac{1}{2}\right)\times 4\right)\times\frac{1}{2}=\frac{3}{8} \tag{6}$$

如果 r=1 000，根据式(6)可以算得

$$P_{\text{correct}}=\left(\frac{3}{8}\right)^{r}=\left(\frac{3}{8}\right)^{1\,000}\approx 10^{-425} \tag{7}$$

由此可见，Eve 企图从公钥中获取正确的私钥是不可能的。

其次，考虑 Eve 通过截取 Alice 传送的密文和伪造公钥的手段企图获得明文的情况。假设 Eve 根据 Bob 传送给 Alice 的测量基和截获的公钥粒子可以得到此次通信的公钥。接着，Eve 伪造公钥传送给 Alice 进行加密。待 Alice 加密后，Eve 再次截获密文。同样地，由于无法得到 Bob 私钥量子态、随机函数 f 和 n 比特的随机串 l。对于 Eve 而言，2 个任意的经典比特加密后所形成的量子比特密度矩阵呈完全混合态，即对于任意经典比特 x 和 y，其密文的密度矩阵为 $\boldsymbol{\rho}_x=\boldsymbol{\rho}_y=I/2^n$，可以得到 $D(\boldsymbol{\rho}_x,\boldsymbol{\rho}_y)=0$。因此，Eve 无法通过截取密文得到 Alice 传送的明文消息。

最后，假设 Eve 可以事先任意选定一定数量的(明文,密文)对，其目的是通过这一过程获得关于加密算法的有用信息，利于在将来更有效地破解由同样加密算法加密的信息。在协议中，各公钥均由 $f(l)$ 和私钥进行相应的量子变换生成的，且每个私钥均随机选自 4 个粒子 $\{|+\rangle,|-\rangle,|+y\rangle,|-y\rangle\}$ 中的一个。根据加密编码规则，每一个密文 $|\varphi_{c_i}\rangle$ 也属于量子态 $\{|+\rangle,|-\rangle,|+y\rangle,|-y\rangle\}$ 中的一个。所以，不管明文消息比特是 0 还是 1，每个密文都处于相同的密度矩阵。此外，由于 Alice 在首次通信之前，通过随机选择 2/h 量子比特进行检测，判断是否为正确获取公钥的方法，可以有效地避免了 Eve 对 Bob 公钥的恶意破坏或篡改。另外，在每次通信中所使用的公钥至少有 1/2 能够实时更新，对不同的公钥加密得到的密文 $|\varphi_{c_i}\rangle$ 也不相同。因此，Eve 无法通过截取多次的公钥的方法获得明文消息，也无法通过一定数量的（明文，密文）对来推导出加密算法的有用信息。因此，提出的协议是无条件安全的。

4.2 有效性分析

本协议主要采用非正交的单粒子作为传输载体，不需要制备纠缠态和 Bell 测量。此外，在每一次密钥传送前，不需要制备大量的诱骗粒子随机地插入到密钥序列中，也不用通过经典信道公布所有诱骗粒子的位置和测量基进行窃听检测。对于 Alice 而言，只需负责接收公钥和测量基，并在加密消息时对所接收的公钥采用错误检测方法来验证公钥的合法性。

另外，本协议主要根据对量子比特进行错误检测结果来选择不同的更新密钥方式，而不是采取对密钥仅一次性使用的方法。当 Bob 发送公钥给 Alice 时，Bob 从集合 $\{|+\rangle,|-\rangle\}$ 中随机选取 h 量子比特附加在 K_{public}^{r} 中，形成新序列 K_{public}^{r+h} 发送给 Alice。由于 Alice 只是用 r 量子比特的公钥进行加密。因此，将剩下的 2/h 量子比特保持不变，随机插入到密文中。待 Alice 加密后，将密文和 2/h 量子比特一并通过量子信道发送给 Bob。在通信阶段，量子比特产生错误的原因主要有信道的噪声和 Eve 的窃听行为。根据量子不可克隆原理，如果信道中存在窃听者进行窃听，那么就必然会引入错误。所以，在加密和解密之前，Alice 和 Bob 需要进行错误检测，即能有效地减少在经典信道上的通信量开销，降低对发送方的存储能力的要求，提高密钥的重复利用率，又能保证公钥和密文信息不被 Eve 篡改。

5 结束语

根据非正交量子的特性，提出了基于单粒子的量子公钥加密协议。由于不需要制备纠缠态和采用 Bell 测量，仅仅对随机产生的单粒子实施简单的量子操作，生成用于加密消息的量子公钥。通过简单的加密编码规则对明文加密。为了有效地避免特定量子源下窃听者的攻击，引入了新的诱骗粒子源作为通信载体和块检测方法，优化了传统的窃听检测方法，降低了对发送方的存储能力的要求。通过采用随机公布窃听检测结果的方法和检测结果选择不同的密钥更新策略，不仅提供了公钥的验证方法，同时保证了协议具有实时分配密钥和提高量子密钥消耗的特点。经安全分析，本协议可以达到无条件安全。

参考文献：

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public-key distribution and tossing[A]. Proceeding of IEEE International Conference on Computers, Systems and Signal Processing[C]. New York, 1984.175-179.

[2] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.

[3] LU H, CAI Q Y. Quantum key distribution with classical Alice[J]. International Journal of Quantum Information, 2008, 6(6): 1195-1202.

[4] LI X H, DENG F G, ZHOU H Y. Efficient quantum key distribution over a collective noise channel[J]. Physical Review A, 2008, 78(2): 022321.

[5] GAO F, LIU B, WEN Q Y, *et al*. Flexible quantum private queries based on quantum key distribution[J]. Optics Express, 2012, 20(16): 17411-17420.

[6] BEAUDRY N, LUCAMARINI M, MANCINI S, *et al*. Security of two-way quantum key distribution[J]. Physical Review A, 2013, 88(6): 062302-12.

[7] SUN Z W, DU R G, LONG D Y. Quantum key distribution with limited classical Bob[J]. International Journal of Quantum Information, 2013, 11(1): 1350005-1-7.

[8] OKAMOTO T, TANAKA K, UCHIYAMA S. Quantum public-key cryptosystems[A]. Cryptology Crypto 2000[C]. Berlin: Springer, 2000. 147-165.

[9] GOTTESMAN D, CHUANG I. Quantum digital signatures[EB/OL]. http://arxiv.org/abs/quant-ph/0105032,2001-03-08.

[10] NIKOLOPOULOS G M. Applications of single-qubit rotations in quantum public-key cryptography[J]. Physical Review A, 2008, 77(3): 032348.

[11] SEYFARTH U, NIKOLOPOULOS G M, ALBER G. Symmetries and security of a quantum public-key encryption based on single-qubit rotations[J]. Physical Review A, 2012, 85: 022342.

[12] YANG L, LIANG M, LI B, *et al*. Quantum public-key cryptosystems based on induced trapdoor one-way transformation[EB/OL]. http://arxiv.org/abs/1012.5249v2, 2011-07-12.

[13] YANG L. Quantum public-key cryptosystem based on classical NP-complete problem[EB/OL]. http://arxiv.org/abs/quant-ph/0310076, 2003-10-12.

[14] LIANG M, YANG L. Public-key encryption and authentication of quantum information[J]. Science China Ser G-Physics, Mechanics& Astronomy, 2012, 55(9): 1618-1629.

[15] PAN J Y, YANG L. Quantum public-key encryption with information theoretic security[EB/OL]. http://arxiv.org/abs/1006.0354v3, 2012-02-20.

[16] LOU M X, CHEN X B, YUN D, *et al*. Quantum public-key cryptosystem[J]. International Journal of Theoretical Physics, 2012, 51(3): 912-924.

[17] LIANG M, YANG L. Quantum-message-oriented public-key encryption scheme beyond computational hypothesis[A]. Proceeding of SPIE Vol 8440: Quantum Optics II[C]. United States: SPIE, 2012. 84400L-1-7.

[18] ZHENG S H, GU L Z, XIAO D. Bit-oriented quantum public key probabilistic encryption schemes[J]. International Journal of Quantum Information, 2014, 53(1): 116-124.

[19] LI X Y, LI L. Quantum public-key cryptosystem using non-orthogonal states[J]. Journal of Software, 2013, 8(8):1906-1913.

[20] YANG L, YANG B Y, PAN J Y. Quantum public-key encryption with information theoretic security[A]. Proceeding of SPIE Vol 8440: Quantum Optics II[C]. United States: SPIE, 2012.84400E-1-6.

[21] WOOTTERS W K, ZUREK W H. A single quantum cannot be cloned[J]. Nature, 1982, 299(28): 802-803.

作者简介：

罗文俊（1966-），男，重庆人，博士，重庆邮电大学教授、硕士生导师，主要研究方向为信息安全、计算机密码学，涉及云计算安全、数字签名、安全多方计算、量子密码、无线网络安全协议等。

刘冠丽（1989-），女，广西南宁人，重庆邮电大学硕士生，主要研究方向为信息安全、量子密码等。