利用贝尔测量的高效量子密钥分配协议

张德喜[1]，赵秋宇[1]，李晓宇[2]

(1. 许昌学院计算机科学与技术学院 河南 许昌 461000; 2. 郑州大学信息工程学院 郑州 450052)

【摘要】提出了一个建立在EPR关联之上的量子密钥分配协议。通信双方通过交换量子位和贝尔测量建立起共享的密钥，没有第三方可以窃取密钥而不被发现，因此该协议是安全的；该协议也是高效的，除了少数用作检错的量子位之外，所有的量子位都对密钥有贡献。

关 键 词 量子密码学; 量子密钥分配; EPR对; 贝尔测量
中图分类号 TP 309.7 文献标识码 A

Efficient Quantum Key Distribution Scheme Using the Bell State Measurement

ZHANG De-xi[1]，ZHAO Qiu-yu[1]，LI Xiao-yu[2]

(1. College of Computer Science and Technology, Xuchang University Xuchang Henan 461000;
2. College of Information Engineering, Zhengzhou University Zhengzhou 450052)

Abstract This paper provides a quantum key distribution protocol based on the correlations of Einstein-Podolsky-Rosen (EPR) pairs. The two parties establish the key by exchanging qubits and performing the Bell state measurement. This protocol is proved to be secure because that no other people can get the key without being found. All qubits distribute to the key except those for error-checking. So the protocol is efficient.

Key words quantum cryptography; quantum key distribution; EPR pair; the Bell state measurement

在经典密码学里，如何将密钥安全地分给各个合法的用户即密钥分配是一个关键的问题。假如密钥分配过程不能保证绝对安全，随后的加密过程就完全失去了意义。密钥分配是最困难、最复杂的问题。量子密钥分配协议是解决密钥分配问题的理想方法。在量子密钥分配协议中，通信双方利用量子系统作为信息载体来建立密钥，量子力学的基本原理保证了密钥是安全的，不会被任何非法的用户所获得。文献[1]提出了第一个量子密钥分配协议(简称BB84协议)。此后，很多协议被提出来，例如利用EPR关联的方案[2-3]，B92协议[4]，等等[5-9]。目前，量子密钥分配在技术上也已经得到实现，在距离超过150 km两个用户之间成功建立起密钥[10]。最近，美国一家公司已经生产出量子密钥分配器投入市场。

本文提出一种建立在纠缠态系统内部关联基础上的量子密钥分配方案。通信双方通过交换量子位和贝尔测量建立起密钥。没有第三方可以获取密钥而不被发现，因此，该协议是安全的。除了少数用于检错的量子位以外，所有的量子位都对密钥有贡献，所以该协议是高效的。

1 基本思想

EPR对是处在最大纠缠态的双量子系统，它可以处于以下四种状态中的任一种，四种状态分别为：

$$|\Phi^+>=\frac{1}{\sqrt{2}}(|00>+|11>)$$

$$|\Phi^->=\frac{1}{\sqrt{2}}(|00>-|11>)$$

$$|\Psi^+>=\frac{1}{\sqrt{2}}(|01>+|10>)$$

收稿日期：2006 - 07 - 05
基金项目：国家自然科学基金资助项目(90612010)；河南省自然科学基金资助项目(0611052800)
作者简介：张德喜(1965 –)，男，硕士，副教授，主要从事量子密码学和人工智能方面的研究.

$$|\Psi^- >=\frac{1}{\sqrt{2}}(|01>-|10>)$$

这四个状态又叫做贝尔态。容易证明$\{|\Phi^+>,|\Phi^->,|\Psi^+>,|\Psi^->\}$构成了双量子位系统的一个正交完备基矢组。以它为基来测量双量子位系统的状态称为贝尔测量。目前，实验中已经成功地实现了完全的贝尔测量[11-12]。另一方面，如果分别以{|0>,|1>}为基测量贝尔态系统的每一个量子位，则测量结果之间存在确定的关联，即对于$|\Phi^+>$和$|\Psi^+>$，量子位1和量子位2的测量结果相同；对于$|\Phi^->$和$|\Psi^->$，测量结果相反，如表1所示。

表1 贝尔测量结果之间存在的关联

状态	测量结果			
	量子位1	量子位2	量子位1	量子位2
$\|\Phi^+>$	0	0	1	1
$\|\Phi^->$	0	1	1	0
$\|\Psi^+>$	0	0	1	1
$\|\Psi^->$	0	1	1	0

按照密码学的习惯，假定通信的双方为Alice和Bob，它们想要建立起共享的密钥；第三方Eve想要非法盗取密钥。

1) Alice和Bob均各生成一个EPR，分别处于状态$|\Phi_{12}^+>$和$|\Phi_{34}^+>$，其中：

$$|\Phi_{12}^+>=\frac{1}{\sqrt{2}}(|0>_1|0>_2+|1>_1|1>_2) \tag{1}$$

$$|\Phi_{34}^+>=\frac{1}{\sqrt{2}}(|0>_3|0>_4+|1>_3|1>_4) \tag{2}$$

式中 下标1、2、3、4用来区分不同的量子位。

2) Alice把量子位2发送给Bob。Bob收到量子位2之后，将该量子位与自身的EPR对合在一起，则所有四个量子位组成的总系统的状态可以记作：

$$|S>=\frac{1}{2}(|0>_1|0>_2|0>_3|0>_4+|0>_1|0>_2|1>_3|1>_4+|1>_1|1>_2|0>_3|0>_4+|1>_1|1>_2|1>_3|1>_4) \tag{3}$$

容易看到，式(3)可以改写成：

$$\begin{aligned}|S>=\frac{1}{\sqrt{2}}[&|0>_1(|\Phi_{23}^+>+|\Phi_{23}^->)|0>_4+|0>_1(|\Psi_{23}^+>+|\Psi_{23}^->)|1>_4+\\&|1>_1(|\Psi_{23}^+>-|\Psi_{23}^->)|0>_4+|1>_1(|\Phi_{23}^+>-|\Phi_{23}^->)|1>_4]\end{aligned} \tag{4}$$

3) Bob对量子位2和量子位3组成的复合系统做贝尔测量，则四量子位系统的状态就坍缩成为两个双量子位系统纠缠态的直积，其结果可以总结如下：

(1) 若测量结果为$|\Phi_{23}^+>$，则$|S>=|\Phi_{23}^+>|\Phi_{14}^+>$；

(2) 若测量结果为$|\Phi_{23}^->$，则$|S>=|\Phi_{23}^->|\Phi_{14}^->$；

(3) 若测量结果为$|\Psi_{23}^+>$，则$|S>=|\Psi_{23}^+>|\Psi_{14}^+>$；

(4) 若测量结果为$|\Psi_{23}^->$，则$|S>=|\Psi_{23}^->|\Psi_{14}^->$。

显然，此时Alice自身的量子位1和Bob自身的量子位4就组成了一个EPR对。若它们分别以{|0>,|1>}为基测量量子位1和量子位2，其结果存在确定的关联。因此，Alice和Bob根据自己的测量结果和贝尔测量的结果就可以推断出对方的测量结果，从而按照一定的规则建立起双方共享的密钥。在后续的讨论中，可以证明没有攻击者能够获取密钥而不被Alice和Bob发现。因此，可以利用这一结果设计一个量子密钥分配协议。

2 利用贝尔测量的高效量子密钥分配协议

下面，详细地给出高效量子密钥分配协议。Alice和Bob执行以下步骤：

(1) Alice生成n个EPR对，每一个均处于状态$|\Phi_{12}^+>$；Bob也生成n个EPR对，每一个也均处于状态$|\Phi_{34}^+>$。

(2) Alice将每个EPR对的第二个量子位发送给Bob，自身余下n个量子位。

(3) 当Bob收到量子位以后，把每个量子位和自身的对应的EPR对中的第一个量子位合在一起作贝尔测量。如果得到$|\Phi_{23}^{+}>$或者$|\Phi_{23}^{-}>$，记为0；如果得到$|\Psi_{23}^{+}>$或者$|\Psi_{23}^{-}>$，记为1；最终，Bob将得到一个n位的二进制串，记作b，同时，自身还有原有的EPR对余下的n个量子位。

(4) Bob以{|0>,|1>}为基测量余下的n个量子位，如果得到测量结果|0>，则记为0；如果得到|1>，则记为1。最后，Bob又得到一个n位的二进制串，记作k。

(5) Bob将第一个串b通过经典信道发送给Alice。

(6) Alice收到串b之后，以{|0>,|1>}为基测量自身的n个量子位，并且参照串b按照下面的规则记录，即如果得到测量结果|0>，且串b对应的位是0，则记作0；如果得到测量结果|0>，且串b对应的位是1，则记作1；如果得到测量结果|1>，且串b对应的位是0，则记作1；如果得到测量结果|1>，且串b对应的位是1，则记作0。最终，Alice也得到一个二进制串k_1。容易看出，如果没有传输错误和攻击者，则$k_1=k$。

(7) Alice和Bob从各自的二进制串中选出对应的m个位进行检错比较。如果有太多的不一致，双方放弃协议，转到步骤(1)重新开始。否则，继续步骤(8)。

(8) 最后剩下的$n-m$位的二进制串就是Alice和Bob共享的密钥。

至此，量子密钥分配过程完成。Alice和Bob建立起共享的密钥，双方可以用它来加密信息。

3　协议的安全性分析

量子力学的基本原理保证了本协议是安全的。如果协议顺利执行完毕，Alice和Bob之间就顺利建立密钥。没有任何攻击者能够在不被发现的情况下窃取密钥。下面给出详细的分析。

根据此前的分析，当Alice把量子位2发送给Bob时，为了获取密钥，Eve可以截获它。但是，Eve不可能通过测量量子位2来获取密钥。因为根据高效量子密钥分配协议，Bob接收到量子位2，会将它与自身的量子位3合在一起做贝尔测量。随后，Alice和Bob分别测量自身的量子位1和量子位4，最终才能生成密钥。而在Eve截获量子位2的阶段，密钥根本还不存在，也就谈不上Eve通过测量来获取它。而且，不难看出，一旦Eve对量子位2进行测量，则它必然会被Alice和Bob发现，所以这种攻击策略是行不通的。

现在来看另一种攻击策略。假定Alice截获量子位2之后不去测量它，而是生成伪造的量子位发给Bob，试图通过这种技巧来窃取密钥，可以证明，这种策略也是不可能成功的。对于每一个截获的量子位，Eve生成一个伪造量子位，它的状态的一般形式可以写作：

$$\rho_E=\sum_{i=1}^{2}p_i\,|\varphi_i>_E\,{}_E<\varphi_i| \tag{5}$$

式中　$|\varphi_i>_E=\alpha_i|0>_E+\beta_i|1>_E$，$\sum_i p_i=1$，且$|\alpha_i|^2+|\beta_i|^2=1$。一个混合态是一些纯态的加权组合，那么，当测量这个混合态时，其测量结果应该就是测量这些纯态所得结果的加权平均。因此，对于纯态$|\varphi_1>_E$，当Bob收到这个伪造的量子位之后，整个五量子位系统的状态为：

$$\begin{aligned}F=&|\Phi_{12}^{+}>[\alpha_1(|\Phi_{E3}^{+}>+|\Phi_{E3}^{-}>)|0>_4+\beta_1(|\Psi_{E3}^{+}>-|\Psi_{E3}^{-}>)|0>_4+\\&\alpha_1(|\Psi_{E3}^{+}>+|\Psi_{E3}^{-}>)|1>_4+\beta_1(|\Phi_{E3}^{+}>-|\Phi_{E3}^{-}>)|1>_4]\end{aligned} \tag{6}$$

当Bob收到伪造的量子位之后，根据协议对量子位E和量子位3组成的系统做贝尔测量。然后，Alice和Bob分别测量量子位1和量子位4。从式(6)可以看出，此时量子位4和量子位1是互相独立的，并不存在关联，Alice和Bob的测量结果之间也没有任何关联。因此，双方根据协议得到一个一致的密钥位的最大概率为1/2。同样，对于纯态$|\varphi_2>_E$，结果是一样的。所以，总的来说，双方得到一个一致的密钥位的最大概率为1/2。按照高效量子密钥分配的协议，Alice和Bob要选出m个位进行比较，这m个位完全一致的概率，或者说Eve不被发现的概率为$P_{\text{error}}=(1/2)^m$。如果m=100，则$P_{\text{error}}\approx10^{-30}$，这是个小得难以想象的概率。换句话说，Eve必定会被发现，这种攻击策略是不可能成功的。

综上所述，就证明了本文的量子密钥分配方案是安全的。

（下转第923页）

证明了该结构的可行性。

对该JPEG2000行为级模型自动综合和布局布线，并采用TSMC0.25 μm工艺进行了流片，该JPEG2000专用处理芯片的面积为3.7 mm×3.3 mm，最高工作频率为48 MHz。测试结果表明算术解码器能够完成的解码功能，结果与软件仿真和FPGA测试结果一致。验证结果表明该结构在功能上的正确性，可以大幅度提高算术解码器解码速度，能满足JPEG2000系统要求。

参　考　文　献

[1] Shannon C E. A mathematical theory of communication[J]. Bell Syst. Tech. J., 1948, 27: 379-423, 623-656.
[2] Eliasp P. Information theory and coding[M]. New York: McGraw-Hill, 1963.
[3] Rissanen J. Generalized Kraft inequality and arithmetic coding[J]. IBM J. Res. Devel., 1976, 20: 198-203.
[4] Pasco R C. Source coding algorithms for fast data compression[D]. California: Standford Univ., 1976.
[5] Pennebaker W B, Mitchell J L, Langdon G G, et al. An overview of the basic principle of the Q-coder adaptive binary arithmetic coder[J]. IBM J. Res. Devel., 1988, 32(6): 717-726.

编　辑　刘文珍

(上接第919页)

4　讨论与总结

相对于以前的一些量子密钥分配协议，例如BB84协议等，本协议的特点是高效性。在BB84协议里[1]，寻求建立共享的密钥的双方必须各自随机选择测量基$\{|0>,|1>\}$或者$\{\frac{1}{\sqrt{2}}(|0>+|1>),\ \frac{1}{\sqrt{2}}(|0>-|1>)\}$来测量手中的量子位。只有双方恰巧选择了相同的测量基的前提下，它们才能得到相同的测量结果，进而建立起一个共享的密钥位。平均来说，双方选择相同测量基的概率为50%，因此，只有一半的量子位能够对密钥的产生有所贡献。换句话说，BB84协议的效率最大为50%，因此，BB84协议的效率是很低的。而高效量子密钥分配协议中，不存在测量基的随机选择，双方的测量结果都是唯一对应的，除了用来检错的量子位之外，所有其他量子位都对密钥有所贡献。因此，高效量子密钥分配协议是相对高效的。

本文提出了一个建立在纠缠态内部关联基础上的量子密钥分配协议。通信双方通过交换量子位和贝尔测量来建立起共享的密钥。除了用作检错的部分之外，所有的EPR对都对生成密钥有贡献，因此它是高效的。本文还证明了在可能的攻击下，它是安全的。

参　考　文　献

[1] Bennet C H, Brassard G. Quantum cryptography: Public-key distribution and tossing[C]// IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984.
[2] Ekert A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67: 661-663.
[3] Bennttt C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem[J]. Physical Review Letters, 1992, 68: 557-559.
[4] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68: 3121-3124.
[5] Huttner B, Imoto N, Gisin N,et al. Quantum cryptography with coherent states[J]. Physical Review A, 1995，51: 1863-1869.
[6] Goldenberg L, Vaidman L. Quantum cryptography based on orthogonal states[J]. Physical Review Letters, 1995, 75: 1239-1243
[7] Cabello A. Quantum key distribution in the holevo limit[J]. Physical Review Letters, 2000, 85: 5635-5638.
[8] Xue P, Li C F, Guo G C. Conditional efficient multiuser quantum cryptography network[J]. Physical Review A, 2002, 65: 022317.
[9] Long G L, Liu L S. General scheme for superdense coding between multiparties[J]. Physical Review A, 2002, 65: 032305.
[10] Kimura T, Nambu Y. Single-photon interference over 150km transmission using silica-based integrated-optic interferometers for quantum cryptography[J/OL]. http://www. eprints: quant-ph, 2006-06-18.
[11] Kim Y H, Kulik S P, Shih Y. Quantum teleportation of a polarization state with a complete bell state measurement[J]. Physical Review Letters, 2000, 86: 1370-1373.
[12] Cinelli C, Barbieri M, Martini F D, et al. Realization of hyperentangled two-photon states[J]. International Journal of Laser Physics, 2005, 15(1): 124-128.

编　辑　熊思亮