利用正交直积态的量子密钥分配协议

赵秋宇[1]，张德喜[1]，李晓宇[2]

(1. 许昌学院电气信息工程学院 河南 许昌 461000; 2. 郑州大学信息工程学院 郑州 450052)

【摘要】基于量子密钥分配协议是目前实现密钥分配最安全的方法，两个三态量子位组成的复合系统中存在一组正交直积态，它可以表现出非定域性。该文提出了一个建立在该系统的非定域性基础上的量子密钥分配协议，协议双方通过交换量子位和集体测量建立起共享的密钥。量子力学的基本原理保证了该协议是无条件安全的，没有第三方可以窃取密钥而不被发现。该协议不需要纠缠态，也不需要做任何量子操作。因此，它更容易在实践中实现，同时具有更高的可靠性与健壮性。

关 键 词 集体测量; 非定域性; 正交直积态; 量子密码学; 量子密钥分配

中图分类号 TN 918; TP 309.7 **文献标识码** A

Quantum Key Distribution Protocol Using Orthogonal Product Quantum States

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

(1. College of Electric and Information Engineering, Xuchang University Xuchang Henan 461000;

2. College of Information Engineering, Zhengzhou University Zhengzhou 450052)

Abstract Quantum key distribution is the most secure technology to distribute a secret key. There is a set of orthogonal product states in a two-qubit three-state quantum system which can show nonlocality. This paper provides a quantum key distribution protocol based otn the nonlocality of such system. The two parties establish the key by exchanging quantum qubits and performing the collective measurement on them. The laws of quantum mechanics guarantee that this protocol is unconditionally secure. No other people can get the key without being found. There are no entangled states and quantum operations needed in the protocol. So it is easier to carry out in practice. And it can gain high reliability and robustness.

Key words collective measurement; nonlocality; orthogonal product states; quantum cryptography; quantum key distribution

密码学的任务是在不安全的信道上传输秘密信息，这就需要预先分配密钥。在经典密码学里，密钥分配是最困难、最复杂的问题。量子密钥分配协议是借助量子系统作为分配密钥的载体，在远离的用户之间建立起密钥。量子力学的基本原理保证了它的绝对安全性，因此，量子密钥分配协议是解决密钥分配问题的理想方法。文献[1]提出了第一个量子密钥分配协议。随后，人们提出利用EPR关联方案，以及B92协议等[2-10]。目前，量子密钥分配技术的实验已经成功实现，在距离超过150 km的两个用户之间成功建立起了密钥[11]。2006年，美国一家公司已经生产出实用的量子密钥分配器。

已有的很多量子密钥分配协议需要使用纠缠态或者需要对作为载体的粒子做各种复杂的量子逻辑门操作。然而，在目前的实验条件下，由于环境噪声的影响，纠缠态很容易丧失相干性导致协议无法执行；而量子逻辑门的操作则技术难度很大，目前只有很少几种能够在实验室实现，且不能保证量子密钥分配协议的顺利完成。为了克服上述困难，本文提出一种使用正交直积量子态的量子密钥分配方案。通信的双方通过交换量子位和集体测量建立起密钥。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。因为不需要使用纠缠态，不需要做复杂的量子门操作，更容易在实验室和工程实践中实现。

1 基本思想

文献[12]提出在两个三状态的量子位组成的复合系统中，一组特殊的直积态也具有某种非定域性。设某组直积态可表示为：

收稿日期：2007 – 12 – 19; 修回日期：2008 – 03 – 20
基金项目：国家自然科学基金(60603002); 河南省自然科学基金(0611052800)
作者简介：赵秋宇(1964 –)，女，副教授，主要从事量子理论与通信工程方面的研究.

$$\begin{cases} |\varphi_1>=|1>|1> \\ |\varphi_2>=|0>\frac{1}{\sqrt{2}}(|0>+|1>) \\ |\varphi_3>=|0>\frac{1}{\sqrt{2}}(|0>-|1>) \\ |\varphi_4>=|2>\frac{1}{\sqrt{2}}(|1>+|2>) \\ |\varphi_5>=|2>\frac{1}{\sqrt{2}}(|1>-|2>) \\ |\varphi_6>=\frac{1}{\sqrt{2}}(|1>+|2>)|0> \\ |\varphi_7>=\frac{1}{\sqrt{2}}(|1>-|2>)|0> \\ |\varphi_8>=\frac{1}{\sqrt{2}}(|0>+|1>)|2> \\ |\varphi_9>=\frac{1}{\sqrt{2}}(|0>-|1>)|2> \end{cases} \tag{1}$$

以上9个状态组成了1个双量子位系统的正交归一基矢组 $\{|\varphi_1>,|\varphi_2>,\cdots,|\varphi_9>\}$。显然，如果允许做集体操作，那么基测量就可以把这9个态区分开。文献[12]证明了只在每个量子位能做定域操作和交换经典信息的情况下，没有办法区分这9个态。本文将这9个态按照如下的规则编码：

$$\begin{cases} |\varphi_1>\rightarrow \text{空码字} \\ |\varphi_2>\rightarrow 000 \\ |\varphi_3>\rightarrow 001 \\ |\varphi_4>\rightarrow 010 \\ |\varphi_5>\rightarrow 011 \\ |\varphi_6>\rightarrow 100 \\ |\varphi_7>\rightarrow 101 \\ |\varphi_8>\rightarrow 110 \\ |\varphi_9>\rightarrow 111 \end{cases} \tag{2}$$

假定想要建立密钥的双方是Alice和Bob。首先，Alice和Bob分别随机生成一个量子位，它们可以处于式(3)中的状态集合中的任意一个状态：

$$|0>,|1>,|2>,\frac{1}{\sqrt{2}}(|0>+|1>),\frac{1}{\sqrt{2}}(|0>-|1>),\frac{1}{\sqrt{2}}(|1>+|2>),\frac{1}{\sqrt{2}}(|1>-|2>) \tag{3}$$

把随机生成的这2个量子位分别标记量子位1和量子位2；然后，Bob把自身的量子位2发给Alice，Alice收到之后，以 $\{|\varphi_1>,|\varphi_2>,\cdots,|\varphi_9>\}$ 为基对量子位1和量子位2组成的复合系统做集体测量。可以看到，如果Alice和Bob各自生成的量子位的状态恰好使复合系统系统处于 $\{|\varphi_1>,|\varphi_2>,\cdots,|\varphi_9>\}$ 中一个态，则Alice所做集体测量的结果是唯一确定的。此时，Alice可以公布量子位1的初始状态，则Bob根据它和已知的量子位2的状态，就可以准确地推断出Alice的集体测量的结果。这就是双方所共享的信息，可以用来生成密钥。本文将会证明没有第三者能够获取密钥而不被Alice和Bob发现，可以利用这个结果来设计一个量子密钥分配协议。

2 利用正交直积态的高效量子密钥分配协议

为了建立起共享的密钥，Alice和Bob需要通过两个信道联系：(1) 量子信道，双方可以通过它互相传送量子位；(2) 辅助的经典信道，双方可以交换经典信息。前者是开放的，任何人都可以监听和控制它；后者是认证的，双方之外的第三者可以监听，但不能控制它。Alice和Bob执行步骤如下：

(1) Alice和Bob分别随机生成n个量子位，它可以处于式(1)中任意一个状态；双方都记录下自己生成的所有量子位的状态序列，分别记作k_1和k_2。

(2) Bob将自己生成的量子位依次发送给Alice。

(3) 当Alice收到这些量子位以后，她把自己手中的量子位与收到的量子位按照次序合在一起，得到n个双量子位系统；随后，她公开自己生成的所有量子位的状态序列k_1。

(4) Bob将k_1与自己的k_2比较，将其中刚好使两个量子位组成的双量子位系统的状态处于 $\{|\varphi_1>,|\varphi_2>,\cdots,|\varphi_9>\}$ 中一个态的那些项保留下来，而丢弃其他的。假定有m项保留下来，最后他得到两个新的m项的序列 k_1' 和 k_2'。

(5) Bob将 k_1' 通过经典信道通知给Alice，Alice根据她选出保留下来的那些项对应的双量子位系统，而丢弃所有其他的双量子位系统。

(6) Alice对余下的双量子位系统以 $\{|\varphi_1>,|\varphi_2>,\cdots,|\varphi_9>\}$ 为基做集体测量；同时Bob根据 k_1' 和 k_2' 可以准确地预知Alice的测量结果。所以，双方最后各自得到一个测量结果的n-m项序列K_a和K_b，且如果没有传输错误和攻击者，应当有K_a=K_b。

(7) Alice和Bob分别从K_a和K_b中选出对应的i个项进行比较。如果有太多的不一致，那么双方放弃协议，转到步骤(1)，重新开始；否则，继续下一个

步骤。

(8) 双方把剩下的*n*-*m*-*i*项的序列根据式(2)进行编码，可以得到一个二进制串，它就是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 协议的效率和安全性分析

首先来看协议的效率。该协议中，Alice和Bob各自独立生成量子位，Bob需要发送量子位给Alice，根据步骤(4)，只有Alice和Bob各自的量子位的状态恰好使复合双量子位系统处于$\{|\varphi_1>,|\varphi_2>,\cdots,|\varphi_9>\}$中一个态时，这两个量子位才保留下来，不符合该条件的都将被丢弃。已知Alice和Bob生成量子位的时候都是随机的，即产生式(3)中每一个态的概率都为1/7，则恰好产生符合条件的概率为：

$$P=\frac{1}{7}\times\left(\frac{1}{7}\times 2+\frac{1}{7}+\frac{1}{7}\times 2+\frac{1}{7}+\frac{1}{7}+\frac{1}{7}+\frac{1}{7}\right)=\frac{9}{49} \quad (4)$$

考虑到如果Alice和Bob均选择|1>，对应的复合系统的状态为$|\varphi_1>=|1>1>$，而根据式(2)，它对应空码字，也就说对于密钥没有贡献，排除$|\varphi_1>$之后，概率降为$P'=\frac{8}{49}$。最后，根据步骤(8)，复合系统每一个态的测量结果产生一个三个位的码字。平均每发送一个量子位，生成密钥的位数为：

$$b=\frac{8}{49}\times 3=\frac{24}{49} \quad (5)$$

因为还有一部分量子位需要用于检错，因此式(5)是本协议效率的上限。

其次可以证明量子力学的基本原理保证了本协议的安全性。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。

在协议的步骤(6)里，如果没有传输错误和攻击者存在，Bob可以根据k_1'和k_2'准确地推导出Alice的测量结果，从而建立双方共享的密钥。而第三者，如Eve，她只能得到公开的k_1'，而无法得到k_2'，因此，所有她能做的事情只能是仅仅根据k_1'来猜测Alice的测量结果。容易证明，对于每一个复合系统，她猜对的概率为：

$$P_{\mathrm{E}}=\frac{1}{7}\times\left(\frac{1}{2}+1+\frac{1}{2}+1+1+1+1\right)=\frac{6}{7} \quad (6)$$

如果序列有*N*项，则Eve猜对所有*N*个项的概率为：

$$P_{\mathrm{E}}=\left(\frac{6}{7}\right)^{N} \quad (7)$$

如果*N*=1 000，则$P_{\mathrm{E}}=\left(\frac{6}{7}\right)^{1\,000}\approx 10^{-66}$。这是一个小得难以想象的概率，Eve是不可能获得密钥的。

再次，Eve可能截获Bob发送给Alice的量子位2，试图通过测量来获取它的状态，从而得到k_2'。因为量子位2处于式(3)中的7个状态之一，而这7个状态并非正交的。因此，无论采用哪一组测量基，Eve都没有办法唯一确定地得到量子位2的状态，而且一旦Eve测量了量子位2，必然会使量子位2的状态坍缩到测量基的本征态。如，如果量子位2的初始态为$\frac{1}{\sqrt{2}}(|1>+|2>)$，Eve选择的测量基为$\{|0>,|1>,|2>\}$，则测量之后，量子位2的状态坍缩为|1>或者|2>，显然，双量子位复合系统的状态也发生了改变。根据协议，当Alice收到Bob发来的所有量子位之后，她要选出*i*个进行检错。这种情况下，Alice得到的测量结果和Bob推断的结果必定不可能完全一致。详细计算表明，对于每一个复合双量子位系统来说，两者一致的概率小于1/2。那么，对于*i*个双量子位系统来说，完全一致的概率，或者说，Eve不被发现的概率为$P_{\mathrm{E}}<\left(\frac{1}{2}\right)^{i}$，如果*i*=100，则$P_{\mathrm{E}}<\left(\frac{1}{2}\right)^{100}\approx 10^{-30}$。Alice和Bob都必然会发现Eve的存在。因此，Eve的这种攻击策略也是不能成功的。

综上，可证明本文的量子密钥分配方案是安全的。

4 讨　论

在本文的协议中，双方只需要产生和发送处于正交直积态的量子位，以及做简单的集体测量，既不需要使用纠缠态，也不需要做任何复杂的操作(如CNOT变换、Hadamard变换等)。众所周知，纠缠态远比直积态更难产生和控制，而且，复杂的量子操作也会给技术实现带来困难和降低协议执行的可靠性。以前的很多协议，或者需要使用纠缠态或者需要做某些复杂量子操作[2,7-9]。因此，本文的协议更容易在实践中实现，同时具有更高的可靠性与健壮性，以及更好的应用价值。

(下转第410页)

子和旋轨耦合参数对α-Al_2O_3中Ru^{3+}晶体g因子的贡献，所得结果与实验符合很好，并较前人工作有所改进。通过讨论杂质Ru^{3+}的局部结构性质，表明该体系具有较明显的共价效应，且三角畸变对g因子(特别是各向异性Δg)有明显的贡献。

参 考 文 献

[1] JIMENEZ DE M. C, SUAREZ-GARCIA A, SERNA R, et al. Optical activation of Er^{3+} in Al_2O_3 during pulsed laser deposition[J]. Optical Materials, 2007, 29(5): 539-542.

[2] XIANG X, ZU X T, ZHU S, et al. Optical properties of metallic nanoparticles in Ni-ion-implanted α-Al_2O_3 single crystals[J]. Appl Phys Lett, 2004, 84: 52-54.

[3] LEBEDEV M, KRUMDIECK S. Optically transparent, dense α-Al_2O_3 thick films deposited on glass at room temperature[J]. Current Applied Physics, 2008, 8(3-4): 233-236.

[4] PAN C, CHEN S Y , SHEN P. Photoluminescence and transformation of dense Al_2O_3: Cr^{3+} condensates synthesized by laser-ablation route[J]. Journal of Crystal Growth, 2008, 310(3): 699-705.

[5] WEINSTEIN I A, POPKO E A. The simulation of TL processes in α-Al_2O_3 using different ratios between parameters of trapping and luminescent centers[J]. Journal of Luminescence, 2007, 122/123: 377-380.

[6] GESCHWIND S, REMEIKA J P. Paramagnetic resonance of Gd^{3+} in Al_2O_3[J]. Phys Rev, 1961, 122: 757-761.

[7] 魏 群, 杨子元, 王参军, 等. Al_2O_3: V^{3+}晶体局域结构及其自旋哈密顿参量研究[J]. 物理学报, 2007, 56(4): 2393-2398.

[8] GESCHWIND S, REMEIKA J P. Spin resonance of transition metal ions in corundum[J]. J Appl Phys, 1962, 33: 370-377.

[9] ABRAGAM A, BLEANEY B. Electron paramagnetic resonance of transition ions[M]. London: Oxford University Press, 1970.

[10] WU S Y, FU Q , LIN J Z, et al. Theoretical studies of the local structures and the EPR parameters for Ru^{3+} in the garnets[J]. Optical Materials, 2007, 29: 1014-1018.

[11] HODGES J A. Strongly enhanced superhyperfine interaction on Ru^{3+} in $Tm_3Al_5O_{12}$[J]. J Phys C: Solid State Phys, 1985, 18: 4373-4384.

[12] YU W L, ZHAO M G, LIN Z Q. High-order perturbation formulae for the zero-field splitting of a ^6S ion in C_3 symmetry and its application to Mn(I):$Ca_5(PO_4)_3F$[J]. J Phys C: Solid State Phys, 1985, 18: 1857-1863.

编 辑 张 俊

(上接第403页)

参 考 文 献

[1] BENNET C H, BRASSARD G. Quantum cryptography: Public-key distribution and tossing[C]//Proceedings of IEEE International conference on Computers, Systems and Signal Processing. Bangalore India: IEEE Press, 1984.

[2] EKERT A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67: 661-663.

[3] 张德喜, 赵秋宇, 李晓宇. 利用贝尔测量的高效量子密钥分配协议[J]. 电子科技大学学报, 2006, 35(6): 917-919.

[4] ZHANG De-xi, LI Xiao-yu. A quantum information hiding scheme using orthogonal product states[J]. WSEAS Transactions on Computers, 2007, 6(5): 757-762.

[5] ZHANG De-xi, LI Xiao-yu. Quantum authentication using orthogonal product states[C]//Proceedings of the 3rd International Conference on Natural Computation (ICNC'07). Haikou: IEEE Computer Society, 2007: 608-612.

[6] GOLDENBERG L, VAIDMAN L. Quantum cryptography based on orthogonal states[J]. Physical Review Letters, 1995, 75: 1239-1243.

[7] HUTTNER B, IMOTO N, GISIN N, et al. Quantum cryptography with coherent states[J]. Physical Review A, 1995, 51: 1863-1869.

[8] CABELLO A. Quantum key distribution in the holevo limit [J]. Physical Review Letters, 2000, 85: 5635-5638.

[9] LI Xiao-yu. Quantum key distribution using the Bell state measurement[J]. International Journal of Modern Physics C, 2003, 14(2): 761-763.

[10] LONG G L, LIU L S. General scheme for superdense coding between multiparties[J]. Physical Review A, 2002, 65: 032305.

[11] KIMURA T, NAMBU Y, HATANAKA T, et al. Single-photon interference over 150km transmission using silica-based integrated-optic interferometers for quantum cryptography[J]. Jpn J Appl Phys Part 2, 2004, 43(9A/B): L1217-L1219.

[12] BENNETT C H, DIVICENZO D P, FUCHS C A, et al. Quantum nonlocality without entanglement[J]. Physical Review A, 1999, 59: 1070-1091.

编 辑 税 红