基于 W 态的网络中任意两个用户间量子密钥分配方案

陶 原　潘 炜　罗 斌　李 丰
(西南交通大学光通信与光器件研究所　成都　610031)

摘　要：针对实现网络中任意两个用户间密钥分配的问题，该文将 W 态变换为系数全部相同的对称形式，提出一种利用 W 态实现网络量子密钥分配的方案，即可信赖中心(CA)与网络中要求通信的任意两个用户分别拥有 W 态的 3 个粒子，CA 对手中的粒子进行测量并公开测量结果，两个用户按照 CA 的不同测量结果采取相应的措施以生成密钥。继而，分别对存在窃听者(Eve)的情况以及 CA 不可信的情况进行安全性分析。结果表明，该方案能够有效抵御攻击，且可以实现平均消耗 3 个 W 态得到两比特密钥的理论效率。

关键词：量子通信；量子密钥分配；W 态；密钥分配效率
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2008)11-2588-04

A Scheme for Quantum Key Distribution Between Any Two Users in a Network via W State

Tao Yuan　Pan Wei　Luo Bin　Li Feng
(*Optical Communication and Devices Research Laboratory*, *Southwest Jiaotong University*, *Chengdu* 610031, *China*)

Abstract: Considering the problem of key distribute between any two users in a network, we transform the coefficients of W state to be uniform in symmetrical form. A scheme for quantum key distribution in a network via W state is proposed. Certificate Authority (CA) and the two users who want to communicate with each other share the three particles of W state. CA performs a measurement on his own particle and promulgates the result of his measurement, two users create their key in corresponding ways according to the measurement result of CA. Then the security of the situation that exists an eavesdropper (Eve) or CA is unauthentic is discussed respectively. It is proved that this scheme can withstand the attack effectively, and carry out the academic efficiency that three W states can be used to gain two bits key.

Key words: Quantum communication; Quantum key distribution; W state; Efficiency of key distribution

1　引言

基于物理原理的量子密钥分配已被证明是保密通信中密钥安全分配的有效手段。近年来，人们提出了许多量子密钥分配协议，其中多数属于直接连接的两个通信者间的密钥分配。此类协议以没有第三方参与为特点，被称为点对点量子密钥分配，主要包括 BB84 协议[1]，B92 协议[2]，E91 协议[3] 以及最近提出的一些其他方案[4, 5]。然而，实际应用要求在网络中任意用户间实现密钥分配，最早提出的网络量子密钥分配方案是基于量子比特调制原理的文献[6]。此后，文献[7]提出了基于量子纠缠交换原理的方案。文献[8]则提出了一种基于 GHZ 三重态的方案，密钥分配效率为 100%即平均消耗 1 个 GHZ 态得到 1 比特密钥，所采用的密钥生成及保密方式可简单概括为：随机使用两种不同的测量基，以此生成网络中任意两个用户间的密钥，并保证方案的安全性。

虽然 GHZ 态属于三粒子最大纠缠态，但当其中 1 个量子比特退出纠缠时，剩下的量子态将不再处于纠缠状态。所以在有粒子损失的情况下，GHZ 态的纠缠特性是非常脆弱的。W 态虽然不像 GHZ 态那样属于最大纠缠态，但它比 GHZ 态更强健，在有粒子损失的情况下 W 态能够更好地保持纠缠特性。鉴于其以上优点，W 态受到了人们的重视。文献[9]提出一种利用 W 态实现三方间量子密钥分配的方案，理论效率为 25%。

本文将分析利用三粒子纠缠 W 态来实现网络中任意两个用户间密钥分配的可行性。首先将 W 态变换为一种系数相同的对称形式，使之适用于网络环境下的密钥分配，然后提出一种借助可信赖中心 CA，利用 W 态本身特点实现网络量子密钥分配的方案，最后通过理论分析证明其安全性。方案的检测步骤设置了两类不等式(CHSH 型 Bell 不等式[10]和三粒子 W 态的 Bell 不等式[11])用来判断量子态所处状态，以此保证方案的安全性，密钥分配的理论效率可以达到 66.7%。

2　三粒子 W 态的变换

通过分析三粒子纠缠态的性质，Dür 等发现如果态的转化只通过随机性局域操作和经典通信(SLOCC)来进行，但不

2007-04-23收到，2008-01-04改回
国家自然科学基金(10174057，90201011)，教育部科学技术研究重点项目(105148)和四川省应用基础科学研究计划(03J Y029204821)资助课题

要求每次得到确定的结果，则可将任意三粒子纠缠态转化为两种基本形式——纠缠 GHZ 态或纠缠 W 态。由于 W 态在量子比特损耗方面具有比 GHZ 态更强的健壮性，受到了越来越多的关注。

文献[12]给出了三粒子 W 态的标准形式：

$$\phi_W = \sqrt{a}|001\rangle + \sqrt{b}|010\rangle + \sqrt{c}|100\rangle + \sqrt{d}|000\rangle \quad (1)$$

其中 $a, b, c > 0$； $d = 1-(a+b+c) \geq 0$。

推广文献[13]的方法，将式(1)按后两个粒子在 Bell 基下展开得：

$$\phi_W = \frac{1}{\sqrt{2}}\left[\left(\sqrt{c}|1\rangle + \sqrt{d}|0\rangle\right)\left(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle\right) + (\sqrt{a}+\sqrt{b})|0\rangle\left|\Psi^+\right\rangle + (\sqrt{a}-\sqrt{b})|0\rangle\left|\Psi^-\right\rangle\right] \quad (2)$$

式(2)中的 $\left|\Phi^+\right\rangle$， $\left|\Phi^-\right\rangle$， $\left|\Psi^+\right\rangle$， $\left|\Psi^-\right\rangle$ 为二粒子最大纠缠空间中的 4 个 Bell 态：

$$\left|\Phi^\pm\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad (3)$$

$$\left|\Psi^\pm\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \quad (4)$$

分析式(2)，并不是所有的测量结果都有用。例如，当第 1 个粒子的测量结果为 $|0\rangle$ 时，其他两方的联合 Bell 基测量结果不确定，4 种 Bell 基测量结果都可能存在，显然不能直接用于量子密钥分配。选取适当的系数， $\sqrt{a} = \sqrt{b} = \sqrt{c} = 1/\sqrt{3}$， $\sqrt{d} = 0$ 这样可使另两方的测量结果在一定程度上处于相关状态，式(2)被转化为

$$\phi_W = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{3}}|1\rangle\left(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle\right) + \frac{2}{\sqrt{3}}|0\rangle\left|\Psi^+\right\rangle\right] \quad (5)$$

这样，W 态的形式只能为

$$\phi_W = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \quad (6)$$

分析式(5)可以发现当第 1 个粒子处于状态 $|1\rangle$ 时，如果对另两个粒子进行 Bell 基测量，结果将等概率地处于状态 $\left|\Phi^+\right\rangle$ 或 $\left|\Phi^-\right\rangle$；如果进行两次单粒子 Von-Neumann 测量，结果将相同并处于状态 $|0\rangle$。当式(5)的第 1 个粒子处于状态 $|0\rangle$ 时，如果对另两个粒子进行两次单粒子 Von-Neumann 测量，结果保持反相关；如果进行 Bell 基测量，结果只可能处于状态 $\left|\Psi^+\right\rangle$。

3　三粒子 W 态的 Bell 定理

文献[11]提出了一个基于三粒子 W 态的 Bell 定理，将 Clauser-Horne(CH)-Bell 不等式[14]应用于 W 态可得：

$$-1 \leq P(z_i=-1, z_j=-1) - P(z_i=-1, x_j \neq x_k) - P(x_i \neq x_k, z_j=-1) - P(x_i = x_j = x_k) \leq 0 \quad (7)$$

其中 z_q 和 x_q $(q = i, j, k)$ 分别表示对量子比特 q 进行观测算子 σ_z 和 σ_x 测量的测量结果(-1 或 1)。$P(z_i=-1, z_j=-1)$ 表示对所有 3 个量子比特进行观测算子 σ_z 测量，其中有两个量子比特的测量结果为-1 的概率。对于文献[11]中的 W 态，通过计算可得 $P(z_i=-1, z_j=-1)=1$， $P(z_i=-1, x_j \neq x_k)=0$， $P(x_i \neq x_k, z_j=-1)=0$， $P(x_i=x_j=x_k)=3/4$，所以正常情况下该三粒子 W 态的测量结果将违反 CH-Bell 不等式。然而，在存在窃听的情况下，测量结果却满足 CH-Bell 不等式。因此可以利用该不等式来检测窃听，以确保量子密钥分配的安全性。

利用式(5)的特性加上合适的检测方法可以设计一个基于 W 态的网络量子密钥分配方案。

4　基于 W 态的网络量子密钥分配方案

假设 CA 是所属网络的可信赖中心，Eve 为窃听者，现要求在处于同一网络中的两个用户 Alice 和 Bob 间分配密钥。基于系数全部相同的对称 W 态的性质，提出以下量子密钥分配方案：

(1)Alice 提出申请。当 Alice 需要与同一网络中的另一用户 Bob 通信时，Alice 向 CA 提出申请。

(2)CA 验证 Alice 的身份。可以利用文献[15]的方法对 Alice 的身份进行验证。

(3)CA 分发 W 三重态粒子。如果 Alice 的身份正确，CA 制备 W 三重态序列，并将序列中每一个 W 三重态的 3 个粒子分别发送给 Alice, Bob 和自己；如果 Alice 的身份不正确，拒绝请求。

(4)CA，Alice 和 Bob 随机选取一些粒子，根据文献[11]提出的 CH-Bell 不等式检测窃听。当 Alice 和 Bob 收到所有粒子后，确定并公布用于检测窃听的粒子的位置，CA 和 Bob 随机地沿 X 方向或 Z 方向测量这些粒子，通过公开信道公布各自的测量基及测量结果。根据 CA 和 Bob 的测量基，Alice 选择相应的基进行测量，获得测量结果，根据该 CH-Bell 不等式判断是否出错。

(5)计算错误概率，如果高于某一门限值，则放弃该次密钥分配；否则继续第(6)步。

(6)CA 对剩余的粒子进行单粒子 Von-Neumann 测量并公布测量结果，即它的粒子序列的量子比特值序列，每一个量子比特值必是 $\{|0\rangle, |1\rangle\}$ 中的一个。如果测量结果为 $|1\rangle$，三方放弃自己对应的测量结果；如果测量结果为 $|0\rangle$，继续第(7)步。

(7)Alice 和 Bob 检测窃听。CA 测量结果为 $|0\rangle$ 时，Alice 和 Bob 手中的粒子处于状态 $\left|\Psi^+\right\rangle$，Alice 和 Bob 随机选择一些粒子用于检测窃听，双方利用文献[10]提出的 CHSH 型 Bell 不等式判断是否出错。如果错误概率高于某一门限值，则放弃该次密钥分配，否则继续第(8)步。

(8)Alice 和 Bob 对手中剩余的粒子分别进行单粒子 Von-Neumann 测量，测量结果不确定但保持反相关，可以由此生成 Alice 和 Bob 间的密钥。

5　基于W态的网络量子密钥分配方案的安全性分析

下面分别就窃听者(Eve)存在的情况以及CA不可信的情况进行分析，以证明方案的安全性。

5.1 窃听者(Eve)存在情况下的安全性分析

假设窃听者(Eve)可以完全访问网络中的量子信道，最常见的攻击方法是截取-重发攻击。下面针对这种攻击方式对方案的安全性进行分析。

本方案第(3)步需要在量子信道中传输粒子，当Eve截取CA发送给Alice和Bob的两个粒子并进行测量时，该三粒子纠缠对由W态变成经典态。此时，该三粒子态的测量结果不会违反CH-Bell不等式，在第(4)步中CA，Alice，Bob根据CH-Bell不等式，可以判定有窃听者存在。

当然，作为窃听者的Eve可以采用截取-重发攻击的另一种方式，即在截取到CA发送给Alice和Bob的粒子后，重新制备另一三粒子W态，然后把其中的两个粒子分别发送给Alice和Bob，但此时Eve的窃听企图同样会被发现。方案第(4)步要求CA和Bob首先公布自己的测量结果和测量基，由于CA和Bob手中的粒子此时并不处于1个三粒子纠缠W态上，他们公布的测量结果中会出现大量正常情况下不可能存在的情况(例如：双方沿Z方向的测量结果同为-1等)。这样，Eve就会暴露自己的存在，窃听不能成功。

5.2 CA不可信情况下的安全性分析

正常情况下，由于Alice和Bob间的密钥是随机产生的，CA无法获得关于密钥的任何信息。在CA不可信的情况下，它可以制备状态$|\phi\rangle=(|011\rangle+|100\rangle)_{ABC}/\sqrt{2}$,然后分别发送$A$, B粒子给Alice和Bob，自己保留C粒子。在方案第(6)步中故意公布自己的测量结果为$|0\rangle$，然后在方案第(8)步中对自己手中的粒子C进行单粒子Von-Neumann测量，根据测量结果，推断出Alice和Bob间的密钥。

通过下面的分析可以发现方案第(4)步能够有效阻止该攻击策略。分析状态$|\phi\rangle$可以发现，在该状态中量子比特$|0\rangle$与$|1\rangle$所处的位置是对称的，直接利用文献[11]中给出的三粒子W态的Bell不等式计算可得$P(z_i=-1,z_j=-1)=1/2$，$P(z_i=-1,x_j\neq x_k)=P(x_i\neq x_k,z_j=-1)=1/2$，$P(x_i=x_j=x_k)=1/4$，将数据代入式(7)，发现该状态满足CH-Bell不等式，所以正常情况下方案第(4)步可以发现CA的窃听企图。作为不诚实中心，CA可以在第(4)步中谎报测量结果即提高概率$P(z_i=-1,z_j=-1)$，降低概率$P(z_i=-1,x_j\neq x_k)$，$P(x_i\neq x_k,z_j=-1)$和$P(x_i=x_j=x_k)$以躲避方案第(4)步的检测。

要想提高概率$P(z_i=-1,z_j=-1)$，CA必须将自己沿Z方向的测量结果更多地谎报为-1，但是这样就会大量出现Alice与CA沿Z方向测量结果同为-1的情况。计算可得$P(z_A=z_C=-1)=0$，即这种情况在正常情况下是不会出现的，Alice和Bob由此可以发现CA的窃听企图。

通过计算可得$P(z_C=-1,x_A\neq x_B)=P(z_C=1,x_A\neq x_B)=1/2$，所以当CA沿$Z$方向测得结果为-1时，无论CA公布结果1还是-1，Alice和Bob沿X方向测量，结果不相同的概率都为1/2。又通过计算可得$P(z_B=-1,x_A=1,x_C=-1)=P(z_B=-1,x_A=-1,x_C=1)=p(z_B=-1,x_A=x_C=1)=P(z_B=-1,x_A=x_C=-1)=1/4$，所以当Bob沿$Z$方向的测量结果为-1时，CA无论是否谎报自己沿$X$方向的测量结果，最终概率都不会发生改变。

经过计算可得$P(x_i=x_j=x_k=1)=1/4$，$P(x_i=x_j=x_k=-1)=0$，所以CA要想降低概率$P(x_i=x_j=x_k)$必须将自己沿X方向的测量结果更多地谎报为-1。又有$P(x_A=x_B=-1,x_C=1)=1/4$，所以实际上当CA采取该方式通报结果时，$P(x_i=x_j=x_k)$的概率并不会降低，而且还会大量出现三方沿X方向的测量结果同为-1的情况，由$P(x_i=x_j=x_k=-1)=0$可得，这种情况在正常情况下是不会出现的，CA的窃听企图也因此会被发现。

CA还可以采取不测量就直接谎报测量结果或者在测量后同时谎报测量基与测量结果等方式来躲避检测。通过理论计算可得，不诚实中心CA的这些窃听策略都不能成功。因为按照本方案的步骤，CA在公布结果时不知道Alice和Bob的测量基与测量结果，它无法通过谎报结果来躲避CH-Bell不等式的检测即如果它分发的不是三粒子W态，就会被方案第(4)步发现。

CA可能采取的另一种策略是分发三粒子W态序列后，在方案第(6)步中公布一个与实际情况相反的单粒子Von-Neumann测量结果。这样，CA也可以获得Alice和Bob间的密钥，但此时Alice和Bob手中的粒子将退出纠缠，在方案第(7)步中Alice和Bob根据Bell理论可以发现CA的窃听企图。所以，设置方案第(7)步的目的是为了确保CA不可信情况下密钥分配的安全性。

在Eve或不诚实中心CA能够完全控制公开信道即不但能窃听而且能篡改公开信道消息的情况下，他们可以通过强中间人攻击策略获得密钥。为了防止这种攻击，Alice和Bob可采用一个与方案第(2)步类似的量子身份验证协议来验证各自身份，从而避免Eve或不诚实中心CA通过假冒身份实施的中间人攻击。

由以上分析可见，无论处于Eve存在的情况还是CA不可信的情况，本方案都可以确保量子密钥分配的安全性。

6 结束语

以往网络环境下的量子密钥分配方案多采用Bell态或GHZ态来实现，本文提出一种利用系数全部相同的对称三粒子W态实现网络量子密钥分配的方案，可以实现平均消耗3个W态得到两比特密钥的理论效率，并通过理论分析证明了方案的安全性。相对基于GHZ态的网络量子密钥分配方案，本方案使用了不同的密钥生成及保密方式。与利用W态实现三方间量子密钥分配的方案相比(25%)，本方案的理论效率要高出一倍以上。

参 考 文 献

[1] Bennett C H and Brassard G. Quantum cryptography:

public-key distribution and coin tossing, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing[C], Bangalore, India, 1984: 175–179.

[2] Bennett C H. Quantum cryptography using any two non-orthogonal state [J]. *Phys. Rev. Lett.*, 1992, 68(21): 3121–3124.

[3] Ekert A. Quantum cryptography based on Bell's theorem [J]. *Phys. Rev. Lett.*, 1991, 67(6): 661–663.

[4] Lo Hoi-Kwong, Ma Xiong-feng, and Chen Kai. Decoy state quantum key distribution [J]. *Phys. Rev. Lett.*, 2005, 94(23): 230504-1–230504-4.

[5] Ma Xiongfeng, Qi Bing, Zhao Yi, and Lo Hoi-Kwong. Practical decoy state for quantum key distribution [J]. *Phys. Rev. A*, 2005, 72(1): 012326-1–012326-15.

[6] Townsend P D. Secure key distribution based on quantum cryptography [J]. *Electronics Letter*, 1994, 30(10): 809–811.

[7] Biham E, Huttner B, and Mor T. Quantum cryptographic network based on quantum memories [J]. *Phys. Rev. A*, 1996, 54(4): 2651–2658.

[8] 曾贵华. 量子密码学[M]. 北京: 科学出版社, 2006: 107–113.
Zeng Guihua. Quantum Cryptography [M]. Beijing: Sciencep, 2006: 107–113.

[9] 杨宇光, 温巧燕, 朱甫臣. 基于W态的量子密钥分配和秘密共享[J]. 北京邮电大学学报, 2006, 29(3): 40–43.
Yang Yu-guang, Wen Qiao-yan, and Zhu Fu-chen. Quantum key distribution and secret sharing via W states [J]. *Journal of Beijing University of Posts and Telecommunications*, 2006, 29(3): 40–43.

[10] Clauser J F, Shimony M A, and Holt R A. Proposed experiment to test local hidden-variable theories [J]. *Phys. Rav. Lett.*, 1969, 23(15): 880–884.

[11] Cabello A. Bell's theorem with and without inequalities for the three-qubit Greenberger-Horne-Zeilinger and W states [J]. *Phy. Rev. A*, 2002(65): 032108–032112.

[12] Dür W, Vidal G, and Cirac J I. Three qubits can be entangled in two inequivalent ways [J]. *Phys. Rev. A*, 2000, 62(6): 062314–1–062314–12.

[13] 郭奋卓, 高飞, 温巧燕, 朱甫臣. 一种高效的量子秘密共享方案[J]. 电子学报, 2006, 34(5): 883–886.
Guo Fen-zhuo, Gao Fei, Wen Qiao-yan, and Zhu Fu-chen. A quantum secret sharing scheme with high efficiency [J]. *Acta Electronica Sinica*, 2006, 34(5): 883–886.

[14] Hardy L. Nonlocality of a single photon revisited [J]. *Phys. Rev. A*, 1994(73): 2279–2283.

[15] Zeng Gui-hua and Zhang Wei-ping. Identity verification in quantum key distribution[J]. *Phys. Rev. A*, 2000, 61(2): 022303-1–022303-5.

陶　原：　男，1983年生，硕士生，研究方向为量子信息与量子通信.

潘　炜：　男，1959年生，教授，博士生导师，研究方向为光纤通信与全光通信网、量子信息与量子通信.