基于三粒子W态蜜罐的受控量子安全直接通信协议

昌 燕，张仕斌，闫丽丽，盛志伟

(成都信息工程学院信息安全工程学院 成都 610225)

【摘要】三粒子W态作为蜜罐粒子应用于受控量子安全直接通信中，以提高窃听检测率和防止double-CNOT攻击。三粒子W态的每个粒子被随机插入到发送序列中探测窃听，每量子位的窃听探测率达到64%。随机插入的蜜罐粒子可以防止接收者在未经控制者同意获取发送者编码前GHZ态粒子1和粒子2的正确关系，即没有控制者同意接受者无法得到任何秘密信息。在安全性分析中，通过引入熵理论得出了每量子位所能包含的最大信息量，对两种蜜罐策略进行了量化比较。如果窃听者试图窃听秘密信息，用扩展的三粒子GHZ态作为诱惑粒子可以得到每量子位58%的窃听探测率，而用三粒子W态作为诱饵可以得到每量子位64%的窃听探测率。

关 键 词 受控的量子安全直接通信； 蜜罐； 窃听检测； 安全性； W态
中图分类号 TN918.8 文献标志码 A doi:10.3969/j.issn.1001-0548.2015.01.006

Controlled Quantum Secure Direct Communication Protocol Based on Three-Particle W State Decoy

CHANG Yan, ZHANG Shi-bin, YAN Li-li, and SHENG Zhi-wei

(College of Information Security Engineering, Chengdu University of Information Technology Chengdu 610225)

Abstract Three-particle W state decoy is introduced in controlled quantum secure direct communication to improve the eavesdropping detection probability and prevent the double-CNOT attack. Each particle of three-particle W state decoy is inserted into sending particles to detect eavesdroppers. The decoy particles inserted randomly can prevent the receiver from obtaining the correct correlation between particle 1 and particle 2 before sender coding on them, so that he can not get any secret information without controller's permission. In the security analysis, the maximum amount of information in a qubit is obtained by introducing the entropy theory method, and two decoy strategies are compared quantitatively. If eavesdroppers intend to eavesdrop on secret information, the per qubit detection rate can reach 64% by using three-particle W state as decoy, but 58% by using extended three-particle GHZ state as decoy.

Key words CQSDC; decoy; eavesdropping detection; security; W state

安全性是量子通信的最大优点之一，根据量子力学原理，合法的通信双方可以有效探测到窃听者的存在，从而保证了通信的安全性[1]。量子安全直接通信(QSDC)作为量子通信中的一个分支，近年来引起了很多学者的关注[1-15]。量子安全直接通信的最大特点是利用量子不可克隆原理、量子测不准原理以及纠缠粒子的关联性和非定域等，在量子信道中直接传递秘密信息[1]。“ 高效两步量子安全直接通信协议 ”是第一个量子安全直接通信协议[2]。文献[3]提出了基于密集编码的两步量子安全直接通信方案, 并对量子安全直接通信方案的标准进行了讨论。文献[4]提出了利用量子远程传态进行量子直接通信的方案。文献[5]提出了多方控制的量子安全直接通信协议(CQSDC)，在该协议中，发送方利用单光子通过量子信道向接收方发送秘密信息，而接收方只有经过控制方的同意后才能恢复秘密信息。文献[6]对文献[5]的“ 多方控制的量子安全直接通信协议 ”进行了安全性分析，并基于隐形传态思想提出了一种伪信号替换攻击方法，指出利用该攻击方法，接受者可以不经过控制方的同意就能获得秘密消息。文献[7]提出了一种新的基于GHZ态的CQSDC协议，该协议取得了较高的编码容量。文献[8]对文献[7]的基于GHZ态的CQSDC协议进行了安全性分析，提出在double-CNOT攻击下，接受者无需控制者的同意就可非法获得33.3%的秘密信息。文献[9]将蜜罐思想引入量子安全直接通信，提出了用三粒子GHZ扩

收稿日期： 2013 – 02 – 04；修回日期： 2014 – 11 – 04
基金项目：国家自然科学基金(61402058)；四川省科技支撑项目(13ZC2138)
作者简介：昌燕(1979 –)，女，博士生，主要从事信息安全、信息处理、量子密码等方面的研究.

展态作为蜜罐，进行量子信道的安全检测，得到了每量子位58%的窃听探测率。本文将蜜罐思想引入基于GHZ态的受控的量子安全直接通信(DCQSDC)中，用三粒子W态的每个粒子作为蜜罐窃听检测粒子，可以得到每量子位64%的窃听检测率，同时也有效防止了double-CNOT攻击。

1 协议描述

假设Bob是控制者，Alice是发送者，Charlie是接收者。

1.1 制备阶段

Bob和Alice制备用于传送秘密信息的三粒子GHZ态串和用于探测信道安全性的蜜罐三粒子W态串，制备过程有4个步骤。

1) Bob制备一个含有N个三粒子GHZ态$|\psi\rangle=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$的有序序列，用于传送秘密信息。$N$个有序的三粒子GHZ态序列可以表示为：$\{[P_1(1),P_1(2),P_1(3)],\ [P_2(1),P_2(2),P_2(3)],\ [P_n(1),P_n(2),P_n(3)]\}$。其中$P_n(1)$表示第$n$个GHZ态的第1个粒子，$P_n(2)$表示第$n$个GHZ态的第2个粒子，$P_n(3)$表示第$n$个GHZ态的第3个粒子。由$\{P_1(1),P_2(1),\cdots,P_n(1)\}$构成的序列称为$S_1$；$\{P_1(2),P_2(2),\cdots,P_n(2)\}$构成的序列称为$S_2$；$\{P_1(3),P_2(3),\cdots,P_n(3)\}$构成的序列称为$S_3$。

2) Bob制备一个含有M个三粒子W态$|\psi\rangle_{\mathrm{w}}=\frac{1}{\sqrt{3}}(|000\rangle+|110\rangle+|001\rangle)_{123}$的有序序列作为蜜罐粒子序列，探测Bob给Alice发送信息时是否被窃听。其中每个W态的3个粒子称为一组，用D_{BA_i}表示，$i=1,2,\cdots,M$，而组D_{BA_i}中的3个粒子分别用$D_{\mathrm{BA}_{i1}}$，$D_{\mathrm{BA}_{i2}}$，$D_{\mathrm{BA}_{i3}}$表示，由D_{BA_i}构成的序列表示为D_{BA}。

3) 按照2)中的办法，Bob制备探测其给Charlie发送信息时，是否有窃听的蜜罐粒子序列D_{BC}。

4) 按照2)中的办法，Alice制备探测其给Charlie发送信息时，是否有窃听的蜜罐粒子序列D_{AC}。

1.2 发送及窃听探测阶段

1) Bob对S_2序列中的每个粒子随机进行pauli$\{I,\sigma_z,\sigma_x\sigma_{iy}\}$操作，得到$S_2'$，Bob把$D_{\mathrm{BA}}$序列中每个组的粒子随机插入到$S_1$和$S_2'$序列，构成新的序列$S_1'$和$S_2''$。如可以像下面这样插入：

S_1序列$P_1(1),P_2(1),\cdots,P_n(1)$；

S_1'序列$P_1(1),D_{\mathrm{BA}_{11}},P_2(1),D_{\mathrm{BA}_{13}},\cdots,P_n(1)D_{\mathrm{BA}_{1i}}$。

将S_1'和S_2''发送给Alice。Bob通过经典信道告诉Alice蜜罐粒子的插入位置。

2) Alice收到Bob发送的粒子序列后按照Bob告诉的插入位置抽取出蜜罐粒子，并组装成D_{BA_i}组，对每个D_{BA_i}组进行W态$|\psi\rangle_{\mathrm{w}}=\frac{1}{\sqrt{3}}(|100\rangle+|010\rangle+|001\rangle)_{123}$检测，若测量结果是该W态，则表示没有窃听，否则有窃听。若无窃听，Alice丢弃蜜罐粒子，恢复S_1和S_2'序列，进入下一步。

3) Bob把D_{BC}序列中每个组的粒子随机插入到S_3序列，构成新的序列S_3'，发送给Charlie。其中插入蜜罐粒子的方式与1)中类似，Charlie通过与2)中类似的方法检测是否有窃听。若无窃听Alice丢弃蜜罐粒子，恢复S_3序列，进入下一步。

4) Alice把其要传送给Charlie的信息，通过对S_1序列和S_2'序列进行8个pauli-pairs操作：

$$\{U_1=\sigma_z\otimes\sigma_z,U_2=I\otimes\sigma_z,U_3=i\sigma_y\otimes\sigma_z,$$
$$U_4=\sigma_x\otimes\sigma_z,$$
$$\{U_5=I\otimes\sigma_x,U_6=\sigma_x\otimes\sigma_z,U_7=\sigma_x\otimes\sigma_x,$$
$$U_4=i\sigma_y\otimes\sigma_x\}$$

进行编码，形成编码序列C_1和C_2'。假设U_1: 000，U_2: 001，U_3: 010，U_4: 011，U_5: 100，U_6: 101，U_7: 110，U_8: 111。Alice把D_{AC}序列中每个组的粒子随机插入到C_1和C_2'序列，发送给Charlie。其中插入蜜罐粒子的方式与1)中类似，Charlie通过与2)中类似的方法检测是否有窃听，若无窃听，Charlie丢弃蜜罐粒子，恢复C_1和C_2'进入下一步。

5) Bob通过经典信道把对S_2进行的pauli操作告诉Charlie，Charlie用相应的pauli操作对C_2'进行操作得到C_2。Charlie对C_1、C_2、S_3进行GHZ测量，通过与原始状态比较，得到Alice对S_1和S_2'所做的操作，从而得到Alice发送给他的信息。

2 安全性分析

2.1 每个量子位的窃听探测率分析

当Bob把混有蜜罐粒子的粒子序列发送给Alice时，假设窃听者Eve在信道中窃听，由于他并不清楚窃听到的粒子是否蜜罐粒子，因此只能对所有粒子进行相同的攻击操作，假设Eve施与粒子的攻击操作为E，经过Eve的攻击操作后原来状态为$|0\rangle$的粒子变为$|0'\rangle=E\otimes|0x\rangle=\alpha|0x_0\rangle+\beta|1x_1\rangle$；原来状态为$|1\rangle$的粒子变为$|1'\rangle=E\otimes|1x\rangle=\ m|0y_0\rangle+n|1y_1\rangle$；其中$|\alpha|^2+|\beta|^2=1$，$|m|^2+|n|^2=1$。被Eve攻击后，联合系统的状态变为：

$$|\psi\rangle_{\text{Eve}} = E\otimes E\otimes E\left[\frac{1}{\sqrt{3}}(|1x0x0x\rangle+|0x1x0x\rangle+|0x0x1x\rangle)\right]=\frac{1}{\sqrt{3}}[(m|0y_0\rangle+n|1y_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)+(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)+(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)]=\frac{1}{\sqrt{3}}(\alpha^2m|0y_00x_00x_0\rangle+m\alpha\beta|0y_00x_01x_1\rangle+m\beta\alpha|0y_01x_10x_0\rangle+m\beta^2|1y_11x_11x_1\rangle+n\alpha^2|1y_10x_00x_0\rangle+\beta n\alpha|1y_10x_01x_1\rangle+m\beta\alpha|1y_11x_10x_0\rangle+n\beta^2|1y_11x_11x_1\rangle+m\alpha^2|0x_00y_00x_0\rangle+\alpha^2n|0x_01y_10x_0\rangle+\beta m\alpha|1x_10y_00x_0\rangle+n\alpha\beta|1x_11y_10x_0\rangle+\alpha m\beta|0x_00y_01x_1\rangle+\alpha n\beta|0x_01y_11x_1\rangle+\beta^2m|1x_10y_01x_1\rangle+\beta^2n|1x_11y_11x_1\rangle+\alpha^2m|0x_00x_00y_0\rangle+\alpha\beta m|0x_01x_10y_0\rangle+\alpha\beta m|1x_10x_00y_0\rangle+\beta^2m|1x_11x_10y_0\rangle+\alpha^2n|0x_00x_01y_1\rangle+\alpha\beta n|0x_01x_11y_1\rangle+\alpha\beta n|1x_10x_01y_1\rangle+\beta^2n|1x_11x_11y_1\rangle)$$

Alice正确测量每一位蜜罐粒子的概率即每一位没有窃听的概率为：

$$p(|\psi_E\rangle)=\frac{1}{3}(3|n\alpha^2|^2+6|\alpha\beta m|^2)$$

令 $|\alpha|^2=a$，$|\beta|^2=b$，$|m|^2=s$，$|n|^2=t$，则，$p(|\psi_E\rangle)=\frac{1}{3}(3ta^2+6abs)$。由于 $a+b=1$，$s+t=1$，$p(|\psi_E\rangle)=\frac{1}{3}(3ta^2+6a-6at-6a^2-6a^2t)$。

每一位被Eve窃听且被探测到的概率的下界为：

$$d_{\text{low}}=1-p(|\psi_E\rangle)=1-\frac{1}{3}(3ta^2+6a-6at-6a^2-6a^2t)$$

可以认为二进制信道的香农熵即为一位量子位所表示的二进制信息所包含的最大信息量。若Bob发送给Alice的粒子处于$|0\rangle$态，则该$|0\rangle$态量子态所包含的最大信息量为：

$$I_{|0\rangle}=-a\log_2 a-(1-a)\log_2(1-a)=H(a)$$

若Bob发送给Alice的粒子处于$|1\rangle$态，则该$|1\rangle$态量子态所包含的最大信息量为：

$$I_{|1\rangle}=-n\log_2 n-(1-n)\log_2(1-n)=H(n)$$

由于Bob发送给Alice的粒子被检测处于$|0\rangle$态和$|1\rangle$态的概率相同，都为0.5，因此可取 $a=h$。则对于一个量子位，Eve可以窃听到的总信息量为：

$$I=I_{|0\rangle}+I_{|1\rangle}=\frac{1}{2}[H(a)+H(h)]=H(a)$$

此时：

$$p(|\psi_E\rangle)=2a-2a^2-a^3$$

$$d_{\text{low}}=1-2a-2a^2-a^3$$

由此可以求得，当 $I=1$ 时，$d_{\text{low}}=0.64$。即当Eve想要窃听一位量子位上所携带的全部信息时，被探测到的概率至少为64%。

文献[9]中利用扩展三粒子GHZ态作为蜜罐进行窃听探测，得到的每位量子位上全部信息被窃听且被探测到的概率至少为58%，而本文中利用三粒子W态得到的每位量子位上全部信息被窃听且被探测到的概率至少为64%。

2.2 double-CNOT攻击

文献[8]中基于GHZ态的受控量子安全直接通信协议中存在double-CNOT攻击，即Charlie利用自己是合法通信者的身份窃听到Alice在对粒子1和粒子2编码前粒子1和粒子2的关系，因此Charlie可以在没有经过控制者Bob的同意下得到33.3%的秘密信息。本文的方案中，Bob在给Alice发送粒子序列之前分别对粒子序列 S_1 和 S_2 进行了随机插入蜜罐粒子和随机pauli操作，因此如果Charlie能够窃听到发送前的粒子对状态，但由于发送前的粒子中插入了蜜罐序列，Charlie得到的发送前的粒子位与Alice接收后并去除蜜罐粒子后剩余的粒子位不是一一对应。因此，在没有Bob同意的情况下Charlie无法得到秘密信息。本文方案中每一次粒子序列发送时都伴随有蜜罐粒子，而且每一量子位被探测到的概率至少为64%，因此Charlie如要窃听，很容易被发现。

3 结　论

DCQSDC协议中利用三粒子W态中的每个粒子作为蜜罐粒子来探测窃听者，达到了每量子位64%的探测率，通过将这种蜜罐粒子引入到基于GHZ态的CQSDC协议中，有效防止了double-CNOT攻击。同时与文献[9]协议相比，DCQSDC协议中用三粒子W态蜜罐达到了比三粒子扩展GHZ态高8%的窃听检测率。

参　考　文　献

[1] LONG G L, WANG C, LI Y S , et al. Quantum secure direct communication[J]. Scientia Sinica Phys, Mech & Astron, 2011, 41(4): 332-342.

[2] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme[J]. Phys Rev A, 2002, 65:

032302.
[3] DENG F G, LONG G L, LIU X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. Phys Rev A, 2003, 68(4): 042317.
[4] YAN F L, ZHANG X Q. A scheme for secure direct communication using EPR pairs and teleportation[J]. Eur Phys J B, 2004, 41: 75-78.
[5] WANG J, CHEN H Q, ZHANG Q, et al. Multiparty controlled quantum secure direct communication protocol[J]. Acta Physica Sinica, 2007, 56(2): 673-676.
[6] WANG T Y, QIN S J, WEN Q Y, et al. Analysis and improvement of multiparty controlled quantum secure direct communication protocol[J]. Acta Physica Sinica, 2008, 57(12): 7452-7457.
[7] WANG J, ZHANG Q, TANG C J. Multiparty controlled guantum secure direct communication using Greenberger-Home-Zeilinger state[J]. Optics Communications, 2006, 266(2): 732-737.
[8] FEI G, QIN S J, WEN Q Y, et al. Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state[J]. Optics Communications, 2010, 283(1): 192-195.
[9] LI J, GUO X J, SONG D J, et al. Improved quantum "ping-pong"protocol based on extended three－particle GHZ state[J]. China Communications, 2012(1): 111-115.
[10] LONG G L, WANG C, DENG F G, et al. From guantum key distribution to guantum secure direct communication [C]//Pacific Rim Conference on Lasers and Electro-Optics. Seoul, Korea: [s.n.], 2007, 1-4: 943-944.
[11] LONG G L, DENG F G, WANG C, et al. Quantum secure direct communication and deterministic secure quantum communication[J]. Front Phys China, 2007, 2(3): 251-272.
[12] GU B, PEI S X, SONG B, et al. Deterministic secure quantum communication over a collective-noise channel[J]. Sci China Ser G-Phys Mech Astron, 2009, 52(12): 1913-1918.
[13] YANG Y G, WEN Q Y, ZHU F C. An efficient quantum secure direct communication scheme with authentication[J]. Chin Phys, 2007, 16(7): 1838-1842.
[14] GAO F, WEN Q Y, ZHU F C. Teleportation attack on the QSDC protocol with a random basis and order[J]. Chin Phys B, 2008, 17(9): 3189-3193.
[15] LI J, SONG D J, GUO X J, et al. A quantum secure direct communication protocol based on a five-particle cluster state and classical XOR operation[J]. Chinese Physics C, 2012, 36(1): 31-36.

编 辑 漆 蓉