基于可重用基序列的量子安全通信方案

孙 莹[1,2],温巧燕[1],朱甫臣[3]
(1.北京邮电大学网络与交换技术国家重点实验室,北京 100876;
2.西安电子科技大学综合业务网国家重点实验室,陕西西安 710071;
3.现代通信国家重点实验室,四川成都 610041)

摘 要: 本文利用两粒子最大纠缠态作为经典信息的载体,根据通信双方事先共享的基序列之间的相互关系制备和测量量子态,结合纠缠纯化和密性增强技术,提出了一种量子安全通信方案,并且分析了它的安全性.由于方案中测量基的选择是确定性而非随机性的,所以避免了密钥分发过程中的粒子浪费.若不考虑窃听检测所消耗的粒子,平均 1 个纠缠粒子对能够建立 1 qubit 量子密钥或者 1 bit 经典密钥.

关键词: 量子密码; 两粒子最大纠缠态; 可重用基序列
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2010) 01-0111-06

Quantum Secure Communication Based on the Reusable Bases Sequences

SUN Ying[1,2], WEN Qiao-yan[1], ZHU Fu-chen[3]
(1. *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;
2. *State Key Laboratory of Integrated Service Network, Xidian University, Xi'an, Shaanxi* 710071, *China*;
3. *State Key Laboratory of Modern Communication Technology, P O Box* 810, *Chengdu, Sichuan* 610041, *China*)

Abstract: A quantum secure communication scheme based on the deterministic measurement was proposed and discussed. The scheme is implemented by using two-particle maximum quantum entanglement, which is the carrier of the classical information, and the techniques such as entanglement purify and privacy amplification. In this scheme, the correspondents generate and measure the quantum states according to two bases sequences shared in advance. There are no discarded data in the ideal case as a result of the deterministic bases. One entangled state can be used to share 1 qubit or 1 bit on average if the particles for eavesdropping detection are not concerned.

Key words: quantum cryptography; two-particle maximum entangled state; reusable bases sequence

1 引言

密码技术在信息安全领域中有着举足轻重的地位,是实现数据加密、访问控制、数字签名等技术的关键.然而大部分经典密码的安全性都是基于某个数学难题,虽然在目前的计算资源和能力下是暂时安全的,但随着计算机技术的飞速发展,特别是对量子计算的研究表明,基于量子力学原理的量子算法具有强大的计算能力,经典密码体制的安全性在量子计算环境下将受到严重威胁.

基于量子力学基本原理的量子密码的出现解决了上述问题.1969 年 S.Wiesner 首先提出利用量子物理性质对信息进行保密[1].十年后 C.H.Bennett 和 G.Brassard 在此基础上提出了量子密码的概念[2,3],并于 1984 年提出了第一个量子密钥分发(QKD)协议—BB84 协议[4].到目前为止,只有一次一密便签密码(one-time-pad scheme)[5]被证明在随机密钥不被重复利用且与明文等长的条件下是绝对安全的,而一次一密便签密码方案中最重要的就是如何实现密钥的安全分发,所以,对于利用量子物理特性来保证密钥分发安全性的 QKD 协议的研究引起了人们极大的关注[6~12].各种分析量子密码安全问题的研究成果也纷纷涌现[13~15].

虽然 BB84 协议的无条件安全性已经得到证明[16~18],并且由于其简单易行一直深受推崇,但是协议最后却只有一半的数据能用于提取密钥,显然,对于昂贵的量子通信来说,这样的效率并不令人满意.如何既

收稿日期:2008-07-11;修回日期:2009-02-06
基金项目:国家 863 高技术研究发展计划(No.2006AA01Z419);国家自然科学基金重大研究计划(No.90604023,60873191,60821001);现代通信国家重点实验室基金(No.9140C11010601);北京市自然科学基金(No.4072020);ISN 开放基金

保证协议可靠的安全性又能提高协议的效率引起了人们的研究兴趣.1998 年,Hwang 等人提出了第一个不需要在建立密钥时公开粒子编码所用基的 QKD 协议[19],该协议利用一个预先共享的较短的可重用二进制随机序列(即基序列)来控制通信双方传输粒子的编码基,在保证协议安全性的基础上使密钥分发的理论效率达到了 100%.随后,出现了不少采用类似技术提高 QKD 效率的研究成果[20~23].

在本文中,我们在前人工作的基础上设计了一种通过预先共享二进制随机序列作为可重用基序列的量子安全通信方案.一方面,该方案继承了这一类协议的优点,利用通信双方共享的秘密基序列来控制测量基,避免了在密钥分发阶段由于双方随机选择测量基造成的粒子浪费,在理想条件下使量子密钥分发效率达到 100%;另一方面,该方案要求双方分别拥有一个秘密基序列,并且在密钥分发前彼此共享,该基序列用于控制发送者对量子态的制备,而不是接收者的测量基,双方不必使用对称的测量基,测量结果对于窃听者 Eve 来说是完全不相关的,在保持密钥分发高效率的同时也增强了基序列和密钥分发过程的安全性.

2 量子信道和秘密基序列的建立

本文提出的 QKD 方案用到了 4 个两粒子最大纠缠态作为密钥分发的载体(见式(1)~(4)).

$$|\varphi^+\rangle_{AB}=\frac{1}{\sqrt{2}}(|+z\rangle_A|+z\rangle_B+|-z\rangle_A|-z\rangle_B)$$
$$=\frac{1}{\sqrt{2}}(|+x\rangle_A|+x\rangle_B+|-x\rangle_A|-x\rangle_B) \quad (1)$$

$$|\psi^-\rangle_{AB}=\frac{1}{\sqrt{2}}(|+z\rangle_A|-z\rangle_B-|-z\rangle_A|+z\rangle_B)$$
$$=\frac{1}{\sqrt{2}}(|-x\rangle_A|+x\rangle_B-|+x\rangle_A|-x\rangle_B) \quad (2)$$

$$|\Phi^+\rangle_{AB}\equiv\frac{1}{\sqrt{2}}(|\varphi^+\rangle_{AB}+|\psi^-\rangle_{AB})$$
$$=\frac{1}{\sqrt{2}}(|-x\rangle_A|+z\rangle_B+|+x\rangle_A|-z\rangle_B)$$
$$=\frac{1}{\sqrt{2}}(|+z\rangle_A|+x\rangle_B-|-z\rangle_A|-x\rangle_B) \quad (3)$$

$$|\Psi^-\rangle_{AB}\equiv\frac{1}{\sqrt{2}}(|\varphi^+\rangle_{AB}-|\psi^-\rangle_{AB})$$
$$=\frac{1}{\sqrt{2}}(|+x\rangle_A|+z\rangle_B-|-x\rangle_A|-z\rangle_B)$$
$$=\frac{1}{\sqrt{2}}(|+z\rangle_A|-x\rangle_B+|-z\rangle_A|+x\rangle_B) \quad (4)$$

其中,式(1)、(2)和式(3)、(4)所表示的量子纠缠态分别来自于两组不同的双量子系统完备正交基$\{|\varphi^\pm\rangle,|\psi^\pm\rangle\}$和$\{|\Phi^\pm\rangle,|\Psi^\pm\rangle\}$.下标 A 和 B 分别代表量子态中相互纠缠的两个粒子.

在该 QKD 方案中,网络中通信双方分别拥有一个长为 m 的秘密基序列,建立通信密钥前需要事先共享彼此的基序列,基序列对于任意第三方保密.首轮密钥分发前需共享的信息可以用经典的 BB84 协议实现,或者选用其他安全性已得到证明的 QKD 方案实现.

3 基于可重用基序列的量子安全通信方案

假设 Alice 与 Bob 已经安全地共享了彼此的秘密基序列,现在他们想要进行保密通信,则建立通信密钥的过程可由如下步骤详细描述:

第 1 步 Alice 制备 $m(N+n)$个两粒子最大纠缠态,制备原则如下:

(1)若 Alice 与 Bob 的基序列第 i 位相同且为 0,则 Alice 制备一个处于态$|\phi^+\rangle_{AB}$的 EPR 对,否则转向下一步;

(2)若 Alice 与 Bob 的基序列第 i 位相同且为 1,则 Alice 制备一个处于态$|\psi^-\rangle_{AB}$的 EPR 对,否则转向下一步;

(3)若 Alice 与 Bob 的基序列第 i 位相异且 Alice 的为 0,则 Alice 制备一个处于态$|\Phi^+\rangle_{AB}$的纠缠粒子对,否则转向下一步;

(4)若 Alice 与 Bob 的基序列第 i 位相异且 Bob 的为 0,则 Alice 随机制备一个处于态$|\Psi^-\rangle_{AB}$的纠缠粒子对;

(5)重复步骤(1)~(4) $(N+n)$次,直到 $m(N+n)$ 个两粒子最大纠缠态制备完毕.

然后,Alice 将自己制备的每一纠缠对中的两个粒子分别形成的序列 S_A^d 和 S_B^d 依次划分为$(N+n)$块,分别记为 $S_A^d=[S_{A1},S_{A2},\cdots,S_{A(N+n)}]$和 $S_B^d=[S_{B1},S_{B2},\cdots,S_{B(N+n)}]$,每块 m 个粒子,并通过量子信道将序列 S_B^d 发送给 Bob.

第 2 步 Bob 随机选择 X 基或 Z 基,对收到的粒子依次测量,记录测量结果.

第 3 步 窃听检测:Bob 通过经典信道告诉 Alice 自己已经收到粒子并完成测量.Alice 从 S_B^d 中随机选出 mn 个粒子(称为样本粒子)公布它们在 S_B^d 中所处的位置,让 Bob 公布这 mn 个粒子的测量所用测量基和测量结果.Alice 选择恰当的测量基测量序列 S_A^d 中与样本粒子纠缠的粒子,比较 Bob 公布的测量结果和自己得到的测量结果,若错误率 R_e 高于事先确定的门限值 t(t 是对量子信道噪声造成的粒子传输的差错率的估计),则 Bob 通知 Alice 取消该次协议,由 Alice 决定是否进行新一轮会话,若选择重新开始,则转向步骤 3';否则终止协议.若 R_e 低于 t,Bob 认为信道是安全的,转向步骤 4.

第 3'步 Alice 与 Bob 根据窃听检测获得的错误率 R_e 对彼此的基序列进行蒸馏,然后转向第 1 步.

第 4 步　建立密钥:记检测窃听完毕后,S_A^d 和 S_B^d 中剩下的粒子组成的序列分别为 S_A 和 S_B. Bob 依次公布自己对于 S_B 中的粒子所选择的测量基,Alice 根据 Bob 公开的信息和自己制备的纠缠粒子对初态来决定自己选择何种测量基来测量序列 S_A 中对应的粒子. 由彼此基序列的对应关系,Bob 可以推断出 Alice 制备的两粒子最大纠缠态的初态. 这样,通信双方利用所掌握的纠缠粒子对的初态信息,再结合自己的测量结果就能推断出对方的测量结果.

例如,对于第 $m(i-1)+j(1\leqslant i\leqslant N,1\leqslant j\leqslant m)$ 个两粒子最大纠缠态,假设 Alice 和 Bob 的基序列的第 j 位都是 1,则 Bob 能推断出 Alice 制备的第 $m(i-1)+j(1\leqslant i\leqslant N,1\leqslant j\leqslant m)$ 个纠缠粒子对的初态为 $|\psi^-\rangle_{AB}$. 如果 Bob 随机选择了 Z 基来测量该纠缠态的第二个粒子,则 Alice 根据 Bob 公布的测量基和自己制备的第 $m(i-1)+j(1\leqslant i\leqslant N,1\leqslant j\leqslant m)$ 个纠缠粒子对的初态将选择 Z 基来测量序列 S_{Ai} 中的第 j 个粒子. 如果 Bob 的测量结果是 $|+z\rangle$,由于 $|\psi^-\rangle_{AB}=(|+z\rangle_A|-z\rangle_B-|-|-z\rangle_A+|+z\rangle_B)/\sqrt{2}$,所以 Bob 可以推导得到 Alice 的测量结果 $|-z\rangle$. 最后,两人将 Alice 的测量结果组成的序列作为原始的量子密钥(如上述,$|-z\rangle$ 是 Alice 制备的第 $m(i-1)+j$ 个纠缠粒子对生成的密钥 qubit). 也可以将该 qubit 如下转化为经典密钥 bit:

$$|+z\rangle,|+x\rangle\rightarrow 0;\ |-z\rangle,|-x\rangle\rightarrow 1.$$

这样在上面的例子中,由 Alice 制备的第 $m(i-1)+j$ 个纠缠粒子对生成的经典密钥是 1. 在非理想量子信道条件下,该方案所建立的原始密钥还需要结合纠错和密性增强等步骤,以获得保真度较高的密钥.

第 5 步　新的基序列生成:在进行保密通信前,Alice 和 Bob 协商新的基序列的长度,若长为 m',则从已建立的保真度较高的密钥中两次取出 m' bit,分别作为 Alice 和 Bob 的基序列,为将来重新发起会话时服务.

为了更直观地描述,我们用如下量子线路图来模拟整个方案的实现过程.

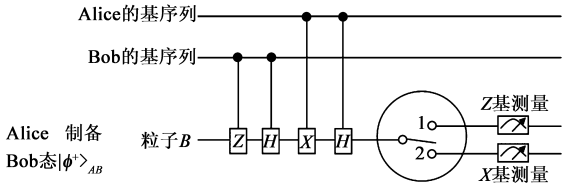

图1　基于可重用基序列的高效QKD模拟线路图

4　安全性分析

假设存在窃听者 Eve,她的目的就是企图通过各种窃听手段获得 Alice 和 Bob 建立的通信密钥,分析得到 Alice 和 Bob 的秘密基序列,并且不被检测到. 实际上,Eve 根据 Alice 和 Bob 公开的信息无法获得关于密钥和基序列的任何信息. 在该方案中,Bob 对所收到的粒子也是随机选择 X 基或 Z 基进行测量的,所以无论是 Alice 和 Bob 在第 3 步还是第 4 步中公开的信息对于 Eve 来说都是随机的,即对于 Eve 来说,这些公开的数据中关于秘密基序列和所要建立的密钥的信息量为 0. 下面我们证明本文所提出的方案对于 Eve 的任意攻击都是安全的.

首先,在理想信道条件下,Eve 企图不引入错误而窃听到关于密钥的任何信息是不可能的,即使 Eve 掌握了 Alice 与 Bob 的秘密基序列.

在本文的 QKD 方案中,虽然建立密钥所用到的是纠缠粒子对,但双方仅单向传输了每个粒子对中的第二个粒子(记为粒子 B). 所以 Eve 的所有窃听操作都被限制在序列 S_B^d 的传输过程中. 根据 Stinespring 型扩张定理[24],Eve 的窃听操作可以用 Hilbert 空间 $H_{AB}\otimes H_E$ 上的酉算子 $\hat{U}_E$ 表示. 我们可以用如下等式来描述 Eve 的窃听操作对量子系统的影响:

$$\hat{U}_E|+z\rangle|\varepsilon\rangle_E=|+z\rangle|\varepsilon_0\rangle_E+|-z\rangle|\varepsilon_1\rangle_E \tag{5}$$

$$\hat{U}_E|-z\rangle|\varepsilon\rangle_E=|+z\rangle|\varepsilon_0'\rangle_E+|-z\rangle|\varepsilon_1'\rangle_E \tag{6}$$

$$\begin{aligned}&\hat{U}_E|+x\rangle|\varepsilon\rangle_E\\&=\frac{1}{\sqrt{2}}|+z\rangle|\varepsilon_0\rangle_E+|-z\rangle|\varepsilon_1\rangle_E+|+z\rangle|\varepsilon_0'\rangle_E+|-z\rangle|\varepsilon_1'\rangle_E\\&=\frac{1}{2}[|+x\rangle(|\varepsilon_0\rangle_E|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E+|\varepsilon_1'\rangle_E)\\&\quad+|-x\rangle(|\varepsilon_0\rangle_E-|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)]\end{aligned} \tag{7}$$

$$\begin{aligned}&\hat{U}_E|-x\rangle|\varepsilon\rangle_E\\&=\frac{1}{\sqrt{2}}|+z\rangle|\varepsilon_0\rangle_E+|-z\rangle|\varepsilon_1\rangle_E-|+z\rangle|\varepsilon_0'\rangle_E-|-z\rangle|\varepsilon_1'\rangle_E\\&=\frac{1}{2}[|+x\rangle(|\varepsilon_0\rangle_E|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)\\&\quad+|-x\rangle(|\varepsilon_0\rangle_E-|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)]\end{aligned} \tag{8}$$

其中 $|\varepsilon_1\rangle_E$ 表示 Eve 的附加粒子的初态,$\{|\varepsilon_0\rangle,|\varepsilon_1\rangle,|\varepsilon_0'\rangle,|\varepsilon_1'\rangle\}$ 是由幺正操作 $\hat{U}_E$ 决定的纯态. $|\varepsilon_0\rangle,|\varepsilon_1\rangle,|\varepsilon_0'\rangle,|\varepsilon_1'\rangle$ 满足 $\hat{U}_E\hat{U}_E^{\dagger}=I$,因此 $\langle\varepsilon_0|\varepsilon_0\rangle+\langle\varepsilon_1|\varepsilon_1\rangle=1$,$\langle\varepsilon_0'|\varepsilon_0'\rangle+\langle\varepsilon_1'|\varepsilon_1'\rangle=1$,

$$\langle\varepsilon_1|\varepsilon_0\rangle+\langle\varepsilon_1'|\varepsilon_0'\rangle=\langle\varepsilon_0|\varepsilon_1\rangle+\langle\varepsilon_0'|\varepsilon_1'\rangle=0 \tag{9}$$

针对等式(5)~(8)所示的 4 种情况,Eve 的窃听行为在第三步的窃听检测过程中将会引入的错误率分别为

$$P_e^{00}=\langle\varepsilon_1|\varepsilon_1\rangle=1-\langle\varepsilon_0|\varepsilon_0\rangle \tag{10}$$

$$P_e^{01}=\langle\varepsilon_0'|\varepsilon_0'\rangle=1-\langle\varepsilon_1'|\varepsilon_1'\rangle \tag{11}$$

$$P_e^{10}=\frac{1}{2}(1+\langle\varepsilon_0|\varepsilon_0'\rangle+\langle\varepsilon_1|\varepsilon_1'\rangle-\langle\varepsilon_0|\varepsilon_1'\rangle-\langle\varepsilon_1|\varepsilon_0'\rangle) \tag{12}$$

$$P_e^{11}=\frac{1}{2}(1-\langle\varepsilon_0|\varepsilon_0'\rangle-\langle\varepsilon_1|\varepsilon_1'\rangle-\langle\varepsilon_0|\varepsilon_1'\rangle-\langle\varepsilon_1|\varepsilon_0'\rangle) \tag{13}$$

同时我们假设 Eve 足够聪明,不会令 Alice 和 Bob 仅依靠不同量子态之间的错误率的差异就发现她的窃听行为,这就要求窃听操作 $\hat{U}_E$ 对 $|+z\rangle$ 和 $|-z\rangle$, $|+x\rangle$ 和 $|-x\rangle$ 引入的错误率必须分别相等,即

$$\langle\varepsilon_0|\varepsilon_0\rangle=\langle\varepsilon_1'|\varepsilon_1'\rangle,\langle\varepsilon_1|\varepsilon_1\rangle=\langle\varepsilon_0'|\varepsilon_0'\rangle,$$
$$\langle\varepsilon_1|\varepsilon_0'\rangle=\langle\varepsilon_1|\varepsilon_1'\rangle=0 \tag{14}$$

在理想信道中,如 Eve 想要逃脱检测窃听,则必须满足

$$P_e^{00}=P_e^{01}=P_e^{10}=P_e^{11}=0 \tag{15}$$

也就是说, $|\varepsilon_0\rangle$, $|\varepsilon_1\rangle$, $|\varepsilon_0'\rangle$, $|\varepsilon_1'\rangle$ 必须满足以下条件:

$$\langle\varepsilon_1|\varepsilon_1\rangle=\langle\varepsilon_0'|\varepsilon_0'\rangle=0,\langle\varepsilon_0|\varepsilon_0\rangle=\langle\varepsilon_1'|\varepsilon_1'\rangle=1,$$
$$\langle\varepsilon_0|\varepsilon_1'\rangle=\langle\varepsilon_1|\varepsilon_0'\rangle=1 \tag{16}$$

由于粒子 B 的单向传输,所以 Eve 只能尝试从附加粒子中提取有意义的信息.

$$\begin{aligned}\hat{U}_E|\varphi^+|\varepsilon\rangle_E&=\frac{1}{\sqrt{2}}[|+z\rangle(|+z\rangle\varepsilon_0\rangle+|-z\rangle|\varepsilon_1\rangle)+|-z\rangle(|+z\rangle\varepsilon_0'\rangle\\&\quad+|-z\rangle|\varepsilon_1'\rangle)]\\&=\frac{1}{\sqrt{2}}|+x\rangle[|+x\rangle(|\varepsilon_0\rangle+|\varepsilon_0'\rangle+|\varepsilon_1\rangle+|\varepsilon_1'\rangle)\\&\quad+|-x\rangle(|\varepsilon_0\rangle+|\varepsilon_0'\rangle-|\varepsilon_1\rangle-|\varepsilon_1'\rangle)]\\&\quad+\frac{1}{\sqrt{2}}|-x\rangle[|+x\rangle(|\varepsilon_0\rangle-|\varepsilon_0'\rangle+|\varepsilon_1\rangle-|\varepsilon_1'\rangle)\\&\quad+|-x\rangle(|\varepsilon_0\rangle-|\varepsilon_0'\rangle-|\varepsilon_1\rangle+|\varepsilon_1'\rangle)]\end{aligned} \tag{17}$$

$$\begin{aligned}\hat{U}_E|\psi^-|\varepsilon\rangle_E&=\frac{1}{\sqrt{2}}[|+z\rangle(|+z\rangle\varepsilon_0'\rangle+|-z\rangle|\varepsilon_1'\rangle)-|-z\rangle(|+z\rangle|\varepsilon_0\rangle\\&\quad+|-z\rangle|\varepsilon_1\rangle)]\\&=\frac{1}{\sqrt{2}}|+x\rangle[|+x\rangle(|\varepsilon_0\rangle-|\varepsilon_0'\rangle+|\varepsilon_1\rangle-|\varepsilon_1'\rangle)\\&\quad+|-x\rangle(|\varepsilon_0\rangle+|\varepsilon_0'\rangle-|\varepsilon_1\rangle-|\varepsilon_1'\rangle)]\\&\quad+\frac{1}{\sqrt{2}}|-x\rangle[|+x\rangle(|\varepsilon_0\rangle+|\varepsilon_0'\rangle+|\varepsilon_1\rangle+|\varepsilon_1'\rangle)\\&\quad+|-x\rangle(|\varepsilon_0\rangle+|\varepsilon_0'\rangle-|\varepsilon_1\rangle-|\varepsilon_1'\rangle)]\end{aligned} \tag{18}$$

$$\begin{aligned}\hat{U}_E|\Phi^+|\varepsilon\rangle_E&=\frac{1}{\sqrt{2}}|+x\rangle(|+z\rangle\varepsilon_0'\rangle_E+|-z\rangle|\varepsilon_1'\rangle_E)\\&\quad+|-x\rangle(|+z\rangle|\varepsilon_0\rangle_E+|-z\rangle|\varepsilon_1\rangle_E)\\&=\frac{1}{2\sqrt{2}}\{|+z\rangle[|+x\rangle(|\varepsilon_0\rangle_E+|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E+|\varepsilon_1'\rangle_E)\\&\quad+|-x\rangle(|\varepsilon_0\rangle_E-|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)]\\&\quad-|-z\rangle[|+x\rangle(|\varepsilon_0\rangle_E+|\varepsilon_1\rangle_E-|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)\\&\quad+|-x\rangle(|\varepsilon_0\rangle_E-|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)]\}\end{aligned} \tag{19}$$

$$\begin{aligned}\hat{U}_E|\Psi^-|\varepsilon\rangle_E&=\frac{1}{\sqrt{2}}|+x\rangle(|+z\rangle\varepsilon_0\rangle_E+|-z\rangle|\varepsilon_1\rangle_E)\\&\quad-|-x\rangle(|+z\rangle|\varepsilon_0'\rangle_E+|-z\rangle|\varepsilon_1'\rangle_E)\\&=\frac{1}{2\sqrt{2}}\{|+z\rangle[|+x\rangle(|\varepsilon_0\rangle_E+|\varepsilon_1\rangle_E-|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)\\&\quad+|-x\rangle(|\varepsilon_0\rangle_E-|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)]\\&\quad+|-z\rangle[|+x\rangle(|\varepsilon_0\rangle_E+|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E+|\varepsilon_1'\rangle_E)\\&\quad+|-x\rangle(|\varepsilon_0\rangle_E-|\varepsilon_1\rangle_E+|\varepsilon_0'\rangle_E-|\varepsilon_1'\rangle_E)]\}\end{aligned} \tag{20}$$

观察 Eve 窃听前后 Alice 与 Bob 的量子系统的状态,比较等式(1)~(4)与式(17)~(20),如果 Eve 想在窃听检测中不引入错误,则必须满足

$$\left.\begin{aligned}&|\varepsilon_1\rangle=|\varepsilon_1'\rangle=0\\&|\varepsilon_0\rangle-|\varepsilon_0'\rangle+|\varepsilon_1\rangle-|\varepsilon_1'\rangle=|\varepsilon_0\rangle+|\varepsilon_0'\rangle-|\varepsilon_1\rangle-|\varepsilon_1'\rangle=0\end{aligned}\right\}$$
$$\Rightarrow|\varepsilon_0\rangle=|\varepsilon_1'\rangle \tag{21}$$

将式(21)代入到等式(17)~(20)中,可以推出,对于量子态 $\varphi=|\varphi^+\rangle,|\psi^-\rangle,|\Phi^+\rangle,|\Psi^-\rangle$,均有 $\hat{U}_E\varphi|\varepsilon\rangle_E=\varphi\otimes|\varepsilon_0\rangle$ 成立.综上所述,Eve 若企图在窃听检测中不引入错误,则必然不能从窃听中获得任何信息.换句话说,Eve 如果要从窃听中获得信息必然会引入错误.

因为样本粒子的初态处于 $\{|+z\rangle,|-z\rangle,|+x\rangle,|-x\rangle\}$ 的概率 $P^{00},P^{01},P^{10},P^{11}$ 是相等的,且 $P^{00}+P^{01}+P^{10}+P^{11}=1$,则 Eve 的窃听行为在方案的检测过程中将会引入错误的概率计算如下:

$$\begin{aligned}P_e&=1-[1-(P^{00}P_e^{00}+P^{01}P_e^{01}+P^{10}P_e^{10}+P^{11}P_e^{11})]^{mn}\\&=1-\{1-[\frac{1}{4}\langle\varepsilon_1|\varepsilon_1\rangle+\frac{1}{4}\langle\varepsilon'_0|\varepsilon'_0\rangle\\&\quad+\frac{1}{4}\times\frac{1}{2}(1+\langle\varepsilon_0|\varepsilon'_0\rangle+\langle\varepsilon_1|\varepsilon'_1\rangle-\langle\varepsilon_0|\varepsilon'_1\rangle-\langle\varepsilon_1|\varepsilon'_0\rangle)\\&\quad+\frac{1}{4}\times\frac{1}{2}(1-\langle\varepsilon_0|\varepsilon'_0\rangle-\langle\varepsilon_1|\varepsilon'_1\rangle-\langle\varepsilon_0|\varepsilon'_1\rangle-\langle\varepsilon_1|\varepsilon'_0\rangle)]\}^{mn}\\&=1-[\frac{3}{4}+\frac{1}{4}(\langle\varepsilon_0|\varepsilon'_1\rangle+\langle\varepsilon_1|\varepsilon'_0\rangle-2\langle\varepsilon_1|\varepsilon_1\rangle)]^{mn}\end{aligned} \tag{22}$$

可见如果不满足等式(16),则 Eve 被检测到的概率 $P_e>0$.

其次,在噪声信道条件下,Eve 企图不引入错误而窃听到关于密钥的任何信息是不可能的,除非她同时掌握 Alice 与 Bob 的秘密基序列中某一(或某些)对应位置的 2 bit.

所有基于可重用秘密基序列的量子密钥分发协议[19~23]的理想条件都是基于基序列的严格保密.从等式(17)~(20)可以看出,本文的方案在 Alice 与 Bob 的秘密基序列严格保密的理想条件下,即使 Eve 能够将窃听引发的错误隐藏在 Alice 与 Bob 之间的信道噪声中,却完全无法区分 Alice 的四种测量结果 $\{|+z\rangle,|-z\rangle,|+x\rangle,|-x\rangle\}$.另外,该方案在 Alice 与 Bob 只有一方泄露秘密基序列的情况下也同样是安全的.因为 Eve 在仅掌握一方秘密基序列的情况下只能依据协议第 4 步中 Bob 公开的测量基推断 Alice 的测量结果是 $\{|+z\rangle,|-z\rangle\}$ 或 $\{|+x\rangle,|-x\rangle\}$,但仍然不能确定最终建立的

密钥比特是 0 或 1.也就是说,在 Alice 与 Bob 的秘密基序列中某一(或某些)对应位置的 2bit 不是同时泄露的情况下,即使逃脱了窃听检测,Eve 也不能获取最终密钥的任何信息.这一点与其他类似协议[19~23]必须基于基序列的严格保密不同.

5　结论

本文提出了一种基于可重用基序列的量子安全通信方案,本质上,这是一个集量子制备与存储技术于一身的 Alice 与一个仅具备量子测量技术的 Bob 之间的密钥分发方案.该方案继承了这一类协议拥有较高的密钥生成效率的优点,避免了通信双方由于随机选择测量基造成的粒子浪费,所有 qubit 只进行了单向传输,并且除去用于检测窃听的 qubit 外,其他均用于有效传输密钥,所以该方案的 qubit 效率 $\eta_q = \frac{q_u}{q_t}$(q_u 表示最终有效的 qubit 数目,q_t 表示通过量子信道传输的 qubit 总数)在理想条件下能够达到 100%.若忽略窃听检测过程所需的经典通信,只考虑第 4 步 Bob 公布测量基所需要的经典通信,平均每传输 1 qubit 最终可以建立 1 qubit 的量子密钥或者 1 bit 的经典密钥.与其他基于可重用基序列的密钥分发协议[19~23]相比,该方案利用来自两组不同的双量子系统完备正交基$\{|\varphi^{\pm}\rangle, |\psi^{\pm}\rangle\}$和$\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$中的纠缠粒子对,并且要求 Bob 收到来自 Alice 的粒子后随机选择测量基测量,因此它还具有以下优点:

(1)前者由于 Bob 选择的测量基是根据秘密基序列确定性地选择测量基,所以假如 Eve 采取截获-测量-重发攻击,则在检测窃听阶段,如果对于某一位粒子,Bob 公布的测量结果与 Eve 的测量结果不同,Eve 就能获知自己在该位置选错了测量基,也就知道了该位置正确的测量基,从而获得对应的秘密基序列的比特值.因此,若想利用同一秘密基序列进行该协议多次或者检测发现窃听需要重新开始协议,则每次均需要对秘密基序列进行密性增强才能保证协议的安全性,但同时秘密基序列的长度不断减短,也就是说同一串基序列能建立的安全密钥的长度是有限的.

而在本文所提出的方案中,由于 Bob 的测量基是随机的,Eve 根据 Bob 的随机测量及结果无法判断任何信息,所以基序列可以完全重复利用.

(2)对于前者,若 Eve 掌握了秘密基序列的部分信息,她可以利用这些信息窃取部分密钥,而不被检测到.而对于本文所提出的方案,由于 Bob 的测量基是随机的,与秘密基序列无关,对比等式(1)~(4)与(17)~(20),即使在 Eve 掌握了全部秘密基序列的情况下,窃听检测仍然可以有效检测到 Eve 的窃听行为,从而取消该次协议.

参考文献:

[1] S Wiesner. Conjugate coding[J]. SIGACT News, 1983, 15(1): 78 – 88.

[2] C H Bennett, G Brassard, et al. Quantum cryptography, or unforgeable subway tokens[A]. Advances in Cryptography: Proceedings of CRYPTO 82[C]. New York: Plenum Press, 1983. 267 – 275.

[3] C H Bennett, G Brassard. Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing[A]. IEEE International Symposium on Information Theory[C]. St-Jovite: Qebec Press, 1983. 91 – 95.

[4] C H Bennett, G Brassard. Quantum cryptography: public-key distribution and coin tossing[A]. Proceedings of the International Conference on Computers, Systems and Signal Processing [C]. India: Bangalore Press, 1984. 175 – 179.

[5] G S Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications[J]. Journal of the American Institute of Electrical Engineers, 1926, 55(1): 109 – 115.

[6] A K Ekert. Quantum cryptography based on Bell theorem[J]. Physical Review Letters, 1991, 67(6): 661 – 663.

[7] C H Bennett. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121 – 3124.

[8] C H Bennett, Brassard G, et al. Quantum cryptography without Bell theorem[J]. Physical Review Letters, 1992, 68(5): 557 – 559.

[9] D Bruss. Optimal eavesdropping in quantum cryptography with six states[J]. Physical Review Letters, 1998, 81(14): 3018 – 3021.

[10] A Cabello. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635 – 5638.

[11] G P Guo, C F Li, et al. Quantum key distribution scheme with orthogonal product states[J]. Physical Review A, 2001, 64(4): 042301.

[12] J L Mi, F Q Wang, et al. Practical non-orthogonal decoy state quantum key distribution with heralded single photon source [J]. Chinese Physics, 2008, 17(4): 1178 – 1183.

[13] N Lütkenhaus. Security against eavesdropping in quantum cryptography[J]. Physical Review A, 1996, 54(1): 97 – 111.

[14] N Lütkenhaus. Estimates for practical quantum cryptography [J]. Physical Review A, 1999, 59(5): 3301 – 3319.

[15] G Brassard, N Lütkenhaus, et al. Security aspects of practical quantum cryptography[A]. Advances in Cryptology-Eurocrypt 2000[C]. Berlin/Heidelberg: Springer, 2000. 289 – 299.

[16] D Mayers. Unconditional security in quantum cryptography [J]. Journal of the Association for Computing Machinery, 2001, 48(3): 351 – 406.

[17] E Biham, M Boyer, et al. A proof of the security of quantum key distribution[J]. Journal of Cryptology, 2006, 19(4): 381 – 439.

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

[19] W Y Hwang, I G Koh, et al. Quantum cryptography without public announcement of bases[J]. Physics Letters A, 1998, 244(6): 489 – 494.

[20] W Y Hwang, X B Wang, et al. Shor-Preskill-type security proof for quantum key distribution without public announcement of bases[J]. Physical Review A, 2003, 67(1): 012302.

[21] F G Deng, G L Long. Controlled order rearrangement encryption for quantum key distribution[J]. Physical Review A, 2003, 68(4): 042315.

[22] K Wen, G L Long. Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communication[J]. Physical Review A, 2005, 72(2): 022336.

[23] K Wen, F G Deng, et al. Secure reusable base-string in quantum key distribution[DB/OL]. http://cn.arxiv.org/PScache/arxiv/pdf/0706/0706.3791v1.pdf, 2007 – 6.

[24] W F Stinespring. Positive functions on C * -algebras[J]. Proceedings of the American Mathematical Society, 1955, 6(2): 211 – 216.

作者简介:

孙 莹 女,1982 年生于山东省,北京邮电大学博士研究生,主要研究方向:密码学、量子保密通信.

E-mail: sunshiny2007@yahoo.cn

温巧燕 女,1959 年生于陕西省,北京邮电大学教授,博士生导师,主要研究方向:密码学与信息安全.

(上接第 110 页)

[9] Mitola, J III, et al. Cognitive radio: making software radios more personal[J]. IEEE Personal Comms, 1999, 6(4): 13 – 18.

[10] 刘琪,李承恕.多模可重构终端的无线接入管理[J].电子学报,2007,35(10):1833 – 1837.
LIU Qi, LI Cheng-shu. Radio access management for multimode reconfigurable terminals[J]. Acta Electronica Sinica, 2007, 35(10): 1833 – 1837. (in Chinese)

[11] Liu Qi, LI Chengshu. Framework and access technology for integration between WLAN and B3G[A]. IET ICWMMN Conference[C]. Hangzhou, China: Institution of Engineering and Technology, 2006. 396 – 399.

[12] Wendong Hu, Willkomm D, et al. Dynamic frequency hopping communities for efficient IEEE 802.22 operation [J]. IEEE Comms Magazine, 2007, 45(5): 80 – 87.

[13] 梅文华等.跳频通信[M].北京:国防工业出版社,2005, 51 – 213.
Mei Wen-hua, etal. Frequency Hopping Communications[M]. Beijing: National Defense Industry Publishing House, 2005, P51 – 213(in Chinese).

[14] Qi Liu, Chengshu Li. Adaptive Spectrum sharing scheme based on frequency hopping communications[J]. Journal of Internet Technology (JIT), 2008, 9(3): 273 – 280.

[15] 刘琪,李承恕. WLAN 与 B3G 结合的结构框架和接入技术[J].铁道学报,2006,28(4):60 – 64.
LIU Qi, LI Cheng-shu. Framework & access technology for integration of WLAN & B3G[J]. Journal of the China Railway Society, 2006, 28(4): 60 – 64. (in Chinese)

[16] Xiangpeng Jing, Dipankar Raychaudhuri. Spectrum co-existece of IEEE 802.11b and 802.16a networks using reactive and proactive etiquette policies[J]. Mobile Netw Appls, 2006, 11(4): 539 – 554.

[17] Philip J Vigneron, Colin Brown. Multiband frequency hopping for high data-rate communications with adaptive use of spectrum[A]. New Frontiers in Dynamic Spectrum Access Networks Baltimore[C]. Maryland USA: IEEE, 2005. 251 – 255.

[18] Elvion S Sousa, John A Silvester. Optimum transmission ranges in a direct-sequence spread-spectrum multihop packet radio network [J], IEEE Journal on Selection Areas in Comms, 1900, 8(5): 762 – 771.

[19] C C Chan and S V Hanly. Calculating the outage probability in a CDMA network with spatial Possion traffic[J]. IEEE Trans. Veh. Technol, 2001, 50(1): 183 – 204.