第 51 卷 第 7 期 2002 年 7 月
1000-3290/2002/51(07)/1439-09

物 理 学 报
ACTA PHYSICA SINICA

Vol.51,No.7,July,2002

B92 量子密钥分配协议的变形及其无条件安全性证明

张 权† 唐朝京 张森强

(国防科技大学电子科学与工程学院,长沙 410073)

(2001 年 4 月 28 日收到;2001 年 12 月 19 日收到修改稿)

分析了 Shor 和 Preskill 证明 BB84 量子密钥分配协议无条件安全性的方法,指出不能用 Shor-Preskill 方法直接证明 B92 量子密钥分配协议的无条件安全性。同时借鉴 Shor-Preskill 方法,引入一种将 B92 协议转化为 BB84 协议的变换,通过证明该变换过程不会泄漏密钥信息给窃听者,以此证明 B92 协议的无条件安全性.也解决了 Lo 等人提出的关于用 Shor-Preskill 方法证明 B92 协议的困难.

关键词:B92 协议,CSS 码,量子密钥分配,量子信息

PACC:0365,4230

1. 引 言

通信双方,Alice 和 Bob,为了交换秘密信息,往往需要共享一个秘密的随机数串(密钥)来对信息加密与解密,从而防止窃听者 Eve 从公共信道上截获的信号中提取秘密信息.显然,信息的保密性取决于密钥的保密性,因此密钥分发技术成为密码学研究的关键之一.随着密码学理论的发展,对信息加密的要求越来越高.为此出现了各种密码方案,包括对称钥密码体系和公钥密码体系等.然而,除了一次一密便笺式密码本方案,所有其他密码方案的安全性都没有严格的证明.就连在许多关键领域被广泛应用的 RSA 密码,其安全性也只是基于"大数不可分解"这一数学假设.从复杂度理论而言,RSA 密码算法的安全性基础是一个未经证明的经典 NP 问题.

然而,量子信息与量子计算理论的出现彻底动摇了经典密码方案的安全性基础.Shor[1] 的算法可以在多项式时间内实现大数的素因子分解,从而推翻了 RSA 密码赖以维系的安全性基础.另一方面,量子信息与量子计算理论的发展也促成了以量子密钥分配(QKD)技术为代表的量子密码术的诞生[2—5].由于量子密码术具有重要战略意义,对于 QKD 的实验研究进展非常迅速.目前已经在商用光纤上实现了约 50km[6] 的 BB84[2] 量子密钥分配实验.

与经典密码方案不同的是,QKD 的安全性由量子力学的基本原理,特别是不确定性原理所保证,因此量子密码术可以真正实现无条件的安全性.所谓 QKD 的无条件安全性是指对 Eve 采取的任何符合量子力学约束的窃听策略,QKD 都能够有效地保证密钥的安全性.与 QKD 的实验进展相比,对其无条件安全性的理论证明相对滞后.尽管对于常规手段的窃听策略,各种 QKD 协议的安全性已经得到证明,可是如果 Eve 掌握了类似量子计算机的强大工具,则现有 QKD 协议能否有效防止 Eve 的窃听行为呢?

迄今为止,对于 BB84 协议无条件安全性的讨论已经比较充分.首先,Lo 和 Chau[7] 利用纠缠提纯和量子纠错实现并证明了无条件安全的 BB84 协议,在该方案中他们采用量子计算机作为中继器.之后 Mayers 等人[8] 又证明了无量子中继器的 BB84 协议的安全性.最近,Shor 和 Preskill[9] 综合了上述两种方法的优点,以非常简洁的方法证明了 BB84 协议的无条件安全性.可是,对于另一种非常著名的 QKD 方案——B92 协议[3] 的安全性证明目前还是空白,虽然在实验中它和 BB84 协议一样取得了巨大成功.因此,本文将借鉴 Shor 和 Preskill 证明 BB84 协

† E-mail:meva@cmmail.com

议的方法来证明 B92 协议的无条件安全性.虽然 B92 协议被认为是简化了的 BB84 协议,但是由于 B92 协议采用了非正交的基矢作为编码量子位,所以 Shor-Preskill 方法不能直接应用到 B92 协议的证明中来.本文首先将对 B92 协议作适当变形,以便在不丧失其特色的情况下,利用 Shor-Preskill 方法证明变形 B92 协议的无条件安全性.

本文填补了 B92 协议无条件安全性证明的空白,进一步分析了 Shor-Preskill 方法中运用对称性进行证明的特点,为 QKD 方案的安全性证明设计一种可能的一般思路.

2. BB84 协议的安全性证明

在标准 BB84 协议无条件安全性的证明中,Shor 和 Preskill 采取了以下策略.首先,他们证明了基于纠缠提纯的 BB84 协议的安全性;然后将基于纠缠提纯的 BB84 协议转化为基于 CSS 码的 BB84 协议,并进一步证明基于 CSS 码的 BB84 协议的安全性;最后,通过简化这种基于 CSS 码的 BB84 协议,说明标准 BB84 协议是其特例,从而证明标准 BB84 协议的无条件安全性.

2.1. 纠缠提纯与 CSS 码

2.1.1. 相关记号

在介绍 Shor 等人的方法之前,首先介绍他们用到的一些记号,本文将在 B92 协议的证明中沿用这些记号.如下矩阵称为 Pauli 矩阵:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

其中 σ_x 作用在量子位上会造成比特(bit-flip)错误,而 σ_z 会导致位相(phase-flip)错误.对于 n 位量子序列,把 σ_a($a \in \{x, y, z\}$)作用在第 k 个量子位上,记作 $\sigma_a(k)$.对于二进制串 s,定义 $\sigma_x^{[s]}$ 为

$$\sigma_a^{[s]} = \sigma_{a(1)}^{[s_1]} \otimes \sigma_{a(2)}^{[s_2]} \otimes \cdots \otimes \sigma_{a(n)}^{[s_n]},$$

其中 s_i 的值为 0 或 1,$\sigma_a^0 = I_2$.取 σ_z 的本征态作为二维 Hilbert 空间 $\mathscr{H}_2$ 的一组正交基,并记作 $|0\rangle$ 和 $|1\rangle$.显然 $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 和 $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 构成 $\mathscr{H}_2$ 上的另一组正交基,这两组基的变换关系用基 $\{|0\rangle, |1\rangle\}$ 上的矩阵可以表示为

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

该变换称为 Hadamard 变换,简称 H 变换.4 个具有最大纠缠的二体量子系统为

$$\Psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{1}$$

$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{2}$$

构成 $\mathscr{H}_4$ 的一组正交基,称为 Bell 基.此外,我们称 $(\Phi^+)^{\otimes n}$ 为 n 重最大纠缠 Bell 态,简称 n-Bell 态.

2.1.2. CSS 码

对于经典纠错码 C_1, C_2,若满足

$$\{0\} \subset C_2 \subset C_1 \subset F_2^n,$$

其中 F_2^n 为 n 维二进制向量空间,C_1 和 $C_2^{\perp}$($C_2^{\perp}$ 为 C_2 的对偶码,即 $C_2^{\perp}$ 的校验矩阵 H_2 为 C_2 的生成矩阵)至多可以纠正 t(其中 $t = \left[\frac{d-1}{2}\right]$,$d$ 为 C_1 和 $C_2^{\perp}$ 的 Hamming 距离)个错误,则由 C_1,C_2 可以构造 CSS 码 Q,其码字表示为

$$v \to \frac{1}{|C_2|^{1/2}} \sum_{\omega \in C_2} |v + \omega\rangle, \tag{3}$$

其中 $v \in C_1$.当 $v_1, v_2 \in C_1$,且 $v_1 - v_2 \in C_2$ 时,v_1 和 v_2 给定相同的码字,因此 Q 的码字相当于 C_2 在 C_1 中陪集的等概率叠加.另外,本文用 H_1,H_2 分别表示 C_1,$C_2^{\perp}$ 的校验矩阵.

由 Q 可以推广得到一族类似的量子纠错码 $Q_{x,z}$,其中 $x, z \in F_2^n$,对 $v \in C_1$,相应的码字为

$$v \to \frac{1}{|C_2|^{1/2}} \sum_{\omega \in C_2} (-1)^{z\omega} |x + v + \omega\rangle, \tag{4}$$

其中 $z\omega = z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n$,CSS 码 Q 为 $Q_{x,z}$ 在 $x = z = \tilde{0}$ 时的特例.

2.1.3. 纠缠提纯与 CSS 码

如果 Alice 和 Bob 已经共享了一个 n-Bell 态,则他们可以在共同的基上对这个态各自进行测量,从而获得一个秘密的二进制串,量子不可克隆定理(QNC)保证了该二进制串作为密钥的安全性.可见 QKD 的最终目标可以通过让 Alice 和 Bob 共享 n-Bell 态来实现.然而,由于噪声(信道情况不理想和窃听者 Eve 的干扰均表现为噪声)的存在,Alice 和 Bob 通过量子信道获得的共享 EPR 对往往没有达到最大纠缠.Bennett 等人指出,当拥有 n 个未达到最大纠缠的 EPR 对时,可以利用纠缠提纯获得 m($m < n$)个最大纠缠的 EPR 对[10].

纠缠提纯与 CSS 码存在密不可分的联系.设 Alice 和 Bob 开始就共享一个 n-Bell 态,然后他们对

H_1 中的每一行[r]，各自测量 $\sigma_z^{[r]}$，对 H_2 中的每一行[r']，各自测量 $\sigma_x^{[r']}$．其结果是将他们的量子系统编码为 $Q_{x,z}$，其中 x，z 的取值使 $H_1 x$ 和 $H_2 z$ 分别与 $\sigma_z^{[r]}$ 和 $\sigma_x^{[r']}$ 的测量值相符合，显然 x，z 的值惟一．另一方面，若 Alice 和 Bob 开始时共享了 n 个 EPR 对，其中大部分为 Φ^+，但存在 $k(k \leqslant t)$个比特翻转(即 Ψ^+ 或 Ψ^-)，或者 k 个位相翻转(即 Φ^- 或 Ψ^-)．当 Alice 和 Bob 完成上述测量且比较其结果时，他们可以发现并纠正上述错误，从而得到 $Q_{x,z}$，由 $Q_{x,z}$ 可以解码得到 $m(m < n)$个 Φ^+ 态．

2.2. 标准 BB84 协议无条件安全性证明

2.2.1. 基于纠缠提纯的 BB84 协议及其安全性

基于纠缠提纯的 BB84 协议是 Lo 和 Chau 首先提出的一种改进协议，由于最大纠缠 EPR 对在密钥分配中的安全性已经证明[7]，同时量子纠错技术与纠缠提纯的关系也已说明，因此证明基于纠缠提纯 BB84 协议的安全性等价于证明纠缠提纯过程的可靠性．基于纠缠提纯的 BB84 协议的操作过程如下：

0. Alice 和 Bob 事先选定一个正整数 $n(n \geqslant 1)$，一种 CSS 码和容许的最大错误概率 $e_{\max}$．
1. Alice 制备 $2n$ 个 EPR 对 $(\Phi^+)^{\otimes 2n}$，并把每个 Φ^+ 的一个量子位归入 A 类，另一个归入 B 类．
2. Alice 随机挑选一个 $2n$ 位二进制串 b，b 的每个二进制位与一个 EPR 对相对应，当 b 的某一位为 1 时，对相应 EPR 对中的 B 类量子位施行 H 变换．
3. Alice 通过量子信道把所有 EPR 对中的 B 类量子位发送给 Bob．
4. Bob 收到所有量子位后通过公开的经典信道向 Alice 确认已经完成接收．
5. Alice 随机选择 $2n$ 个 EPR 对中的 n 个来检验 Eve 是否在偷听．
6. Alice 把二进制串 b 和用作校验位的 EPR 对所对应的位置通过公开的经典信道告知 Bob．
7. Bob 对 b 中取值为 1 的位元所对应的量子位施行 H 变换．
8. Alice 和 Bob 分别在基 $\{|0\rangle, |1\rangle\}$ 上测量 n 个校验 EPR 对，并在公开的经典信道上广播他们的结果．如果校验位不一致的概率超过 $e_{\max}$，他们放弃本次密钥分发过程．否则，继续进行下一阶段密钥分配过程．
9. Alice 和 Bob 对 $r \in H_1$ 的每一行测量 $\sigma_z^{[r]}$，对 $r' \in H_2$ 的每一行测量 $\sigma_x^{[r']}$，并且广播他们的结果，利用纠缠提纯，他们可以获得 m 个 EPR 对 $(\Phi^+)^{\otimes m}$．
10. Alice 和 Bob 分别在基 $\{|0\rangle, |1\rangle\}$ 上测量这 m 个 EPR 对，从而获得一个 m 位的共享密钥．

上述协议由两个阶段组成：第一阶段，Alice 和 Bob 通过随机抽查验证错误概率小于 $e_{\max}$，这一方面是检测是否存在 Eve 的干扰，另一方面是为了保证误差概率在纠错码的纠错能力范围之内．第二阶段，Alice 和 Bob 使用 CSS 码进行纠缠提纯，并获得密钥．

纠缠提纯过程的可靠性表现为校验位通过检验而纠缠提纯过程失败的概率，此概率越小，则纠缠提纯的可靠性越高．由于 Eve 事先不知道哪些量子位被用作校验位，因此她不可能有区别地对待窃听到的量子位，亦即校验位在这里充当了随机样本的角色．此外，对于两种 EPR(经过 H 变换和未经变换)在基 $\{|0\rangle, |1\rangle\}$ 上的测量相当于测量算子 $\sigma_x\sigma_x$ 和 $\sigma_z\sigma_z$，由于 σ_x 和 σ_z 互易，故二者的测量结果满足经典概率叠加性．因此可以用经典随机抽样理论来估计错误数目．利用这种经典简化，Shor 和 Preskill 证明了

$$P(\varepsilon_{\text{code}} \geqslant e_{\max} \mid \varepsilon_{\text{check}} \leqslant (e_{\max} - \varepsilon)) < \exp[(-\varepsilon^2 n/4)(e_{\max} - e_{\max}^2)], \quad (5)$$

其中 $\varepsilon_{\text{code}}$ 和 $\varepsilon_{\text{check}}$ 分别为代码位和校验位的错误概率．(5)式表明，通过适当选取 CSS 码和 $e_{\max}$，可以使上述概率随 n 指数地减小．

2.2.2. 基于 CSS 码的 BB84 协议及其安全性

显然，上述纠缠提纯协议仅涉及了从 Alice 到 Bob 的单向量子通信．在文献[10]中已经证明了任何单向提纯协议都可以简化为一种量子纠错码协议，即 Alice 用量子纠错码制备一编码的量子态并发送给 Bob，而不是制备并发送 EPR 对的一半量子位．

考虑到 Alice 可以在 B 类量子位发送给 Bob 之前对自己的校验量子位进行测量，这并不影响纠缠提纯协议的其他测量过程，而其效果相当于 Alice 事先选择了一个 n 位随机二进制串作为校验序列．同样，Alice 也可以在发送 B 类量子位之前测量 $\sigma_z^{[r]}$ 和 $\sigma_z^{[r']}$，相当于选定一个 $Q_{x,z}$ 来编码 $(\Phi^+)^{\otimes m}$，其中 x，z 由 Alice 的测量结果决定．最后，Alice 还可以事先就对编码的 EPR 对进行测量，这等效于 Alice 选定了一个随机密钥 k，并用 $Q_{x,z}$ 来编码 k(即在(4)式中使 $v = k$)．进行上述改动后，基于纠缠提纯的 BB84

协议就等价于如下基于 CSS 码的 BB84 协议：

1. Alice 选择了一个 n 位随机二进制串作为校验序列，一个 m 位随机密钥 k，以及 $2n$ 位随机串 b.
2. Alice 选择 n 位随机串 x 和 z，由此决定 CSS 码 $Q_{x,z}$.
3. Alice 用 $Q_{x,z}$ 对密钥 $|k\rangle$ 进行编码.
4. Alice 在 $2n$ 位串中随机挑选 n 个位置，并把他事先选定的校验序列放在这些位置，同时把 $Q_{x,z}$ 码字放在其余的位置.
5. Alice 对随机串 b 中取值为 1 的位所对应的量子位施行 H 变换.
6. Alice 把经过上述处理的量子位发送给 Bob. Bob 收到这些量子位后在经典信道上宣布这一事实.
7. Alice 在经典信道上公布 b，x，z 和校验位的位置，以及校验序列的值.
8. Bob 对随机串 b 中取值为 1 的位所对应的量子位施行 H 变换.
9. Bob 比较校验序列与自己测量到的校验位取值，若 $\varepsilon_{\text{check}} \geqslant e_{\max}$，则放弃此次 QKD，否则进行下一步.
10. Bob 按照 $Q_{x,z}$ 对代码位译码，从而获得密钥 k.

2.2.3. 标准 BB84 协议的安全性证明

将量子纠错码协议简化为标准 BB84 协议时须借助于 CSS 码的特性. 在 CSS 码中，比特错误和位相错误的纠正过程是可分离的，如果 Alice 和 Bob 放弃相位误差校正过程，其结果实质上就是 BB84 协议. 更具体地，因为 Bob 在提取共享密钥时并不需要 z，因此 Alice 甚至根本不必发送它. 考虑 Alice 选定了密钥 k 且不发送 z 的情况，遍历所有 z 并对其取平均，可以发现 Alice 实际发送的态为

$$\frac{1}{2^n \mid C_2 \mid}\sum_{z}\sum_{\omega_1,\omega_2\in C_2}(-1)^{(\omega_1+\omega_2)z} \times |k+\omega_1+x\rangle\langle k+\omega_2+x| = \frac{1}{\mid C_2 \mid}\sum_{\omega\in C_2}|k+\omega+x\rangle\langle k+\omega+x|. \quad (6)$$

该状态相当于 $|k+\omega+x\rangle$ 的经典混合态，其中 $\omega\in C_2$. 设 Alice 发送给 Bob 的态为 $|k+\omega+x\rangle$，Bob 接收到的码字为 $k+\omega+x+e$，他从中减去 x 并译码，得到 C_1 中的一个码字 u，可以证明 $P(u=k+\omega)\to 1$，于是他们可以用 $u+C_2$ 作为最终的密钥. 这一过程实际上就等价于如下标准 BB84 协议：

1. Alice 选定两个 $(4+\delta)n$ 位长的随机二进制串 b，t.
2. Alice 根据 b 和 t 制备 $(4+\delta)n$ 个量子位，当 b_i 为 0 时，采用基 $\{|0\rangle, |1\rangle\}$ 来制备第 i 个量子位，否则采用基 $\{|+\rangle, |-\rangle\}$ 当 t_i 为 1 时，采用 $|0\rangle$ 或 $|+\rangle$ 来表示第 i 个量子位，否则用 $|1\rangle$ 或 $|-\rangle$ 来表示第 i 个量子位.
3. Alice 将制备好的 $(4+\delta)n$ 个量子位通过量子信道发送给 Bob.
4. Bob 随机选定一个 $(4+\delta)n$ 位长二进制串 p，当 p_i 为 0 时，将第 i 个量子位映射到 $\{|0\rangle, |1\rangle\}$ 上，否则将之映射到 $\{|+\rangle, |-\rangle$ 上. 测量完成后，Bob 通过公开的经典信道通知 Alice.
5. Alice 公布 b.
6. 当 $b_i \neq p_i$ 时，他们丢弃相应量子位及测量结果. 根据经典统计理论，他们获得 $2n$ 个以上测量结果的概率接近于 1，万一获得的测量结果少于 $2n$ 个，他们可以重新进行制备和测量. 然后 Alice 从这些测量结果中随机选取 $2n$ 个留作后续使用，并选择其中的 n 个作为校验位.
7. Alice 和 Bob 公布各自校验位的值，若错误数超过 $ne_{\max}$，则放弃此次密钥分配，否则继续下一步.
8. Alice 公布 n 位二进制串 $u+v$，其中 v 是 n 个代码位的相应值，u 是 C_1 中的任意码字.
9. Bob 从他的含有错误的代码位 $v+e$ 中减去 $u+v$ 后得到 $u+e$，对之纠错后获得 u.
10. Alice 和 Bob 使用 C_2 在 C_1 中的陪集 $u+C_2$，作为最终的密钥.

3. B92 协议的变形及其无条件安全性证明

3.1. Shor-Preskill 方法不能直接证明 B92 协议

Shor 和 Preskill 在证明 BB84 协议时用到了一些非常重要的方法和技巧. 首先，采用对称化方法，使得比特错误和位相错误的概率相等，且等于平均错误概率. 设信道中发生错误 σ_x，σ_y，σ_z 的概率分别为 p_1，p_2，p_3，量子位保持不变的概率为 $1-p_1-p_2-p_3$. 在基于纠缠提纯的 BB84 协议中，对于 $b_i=1$ 的 EPR 对，由于 $HZH=X$，所以 Alice 和 Bob 其实是在基 $\{|+\rangle, |-\rangle\}$ 上进行测量，该组基上的位相错误

等价于 $\{|0\rangle, |1\rangle\}$ 上的比特错误，因此总的比特错误概率为

$$e_{\text{bit-flip}}^{\{0,1\}} + e_{\text{phase-flip}}^{\{+,-\}} = \frac{1}{2}(p_2 + p_3) + \frac{1}{2}(p_1 + p_2) = \frac{1}{2}(p_1 + 2p_2 + p_3),$$

其中上标表示相应的基，同样位相错误概率为

$$e_{\text{phase-flip}}^{\{0,1\}} + e_{\text{bit-flip}}^{\{+,-\}} = \frac{1}{2}(p_1 + p_2) + \frac{1}{2}(p_2 + p_3) = \frac{1}{2}(p_1 + 2p_2 + p_3).$$

可见比特错误和位相错误的概率相等，因此在估计信道错误时，只要计算比特错误.

其次，在 Shor-Preskill 证明中，密钥 k 被编码在 CSS 码 $Q_{x,z}$ 中，并和校验位一起发送给 Bob，因此 Bob 必须正确接收并测量所有码位. 为此 Shor 和 Preskill 在基于 CSS 码的 BB84 协议中使用了量子寄存器，在 Bob 收到所有码字后公布各量子位所使用的基 b. 这样做不仅保证 Bob 正确检测所有量子位，还提高了密钥分配的效率.

再者，由基于 CSS 码的 BB84 协议来证明标准 BB84 协议时，用到了 CSS 码的特性，即对比特错误和位相错误的纠正过程可以分开，同时由于对称化的作用，Bob 并不需要位相错误的纠错信息 z，因此基于 CSS 码的 BB84 协议可以转化为标准 BB84 协议.

上述技巧和特点限制了人们使用该方法直接证明 B92 协议的无条件安全性. 这是因为，首先 B92 协议采用两个非正交态矢进行密钥分配，而在 BB84 协议中采用了两组正交基，即 4 个态矢. 亦即在 BB84 协议中，每个量子位包含了 2 比特编码信息，而在 B92 协议中每个量子位仅包含 1 比特信息，故在 B92 协议中无法使用上述对称化方法. 其次，对于 B92 协议，不可能设计出类似于基于 CSS 码 BB84 协议的改进协议，从而保证 Bob 接收到所有量子位并且正确地测量. 即使 Bob 同样拥有量子寄存器，由于每个量子位的编码信息就是态矢所对应的基，也就是相应的测量方法，所以要让 Bob 正确测量所有量子位，只能告诉他对应的测量方法，这就泄漏了所有的编码信息而无法进行密钥分配（本文附录给出了该结论的证明）. 由此可见，Shor-Preskill 方法不能直接用来证明标准 B92 密钥分配协议的无条件安全性.

由于 B92 和 BB84 协议之间存在非常紧密的联系，通过适当变换，B92 协议可以转化为 BB84 协议. 因此通过研究这些变换对安全性的影响，揭示了可以由 BB84 协议来间接证明 B92 协议的安全性. 本文证明的主要思路是，首先对 Shor-Preskill 已经证明的标准 BB84 协议进行适当的变换，并证明其无条件安全性，然后说明变换后的 BB84 协议等效于我们的变形 B92 协议，最后证明在窃听者看来，变形 B92 协议与标准 B92 协议完全一致，由此说明标准 B92 协议是无条件安全的.

3.2. 标准 B92 协议

标准 B92 协议量子密钥分配协议采用任意两个非正交的态矢对信息进行编码，本文设 $|0\rangle \to 1$，$|+\rangle \to 0$. 标准 B92 协议的执行过程如下：

1. Alice 选定一个 $n' = (8 + \delta)n$ 位长的随机二进制串 b.
2. Alice 根据 t 制备 n' 个量子位，当 $t_i = 1$ 时，$|q\rangle_i = |0\rangle$，当 $t_i = 0$ 时，$|q\rangle_i = |+\rangle$.
3. Alice 将制备好的量子位通过量子信道逐个发送给 Bob.
4. Bob 随机选定一个 n' 位长二进制串 p，在第 i 时间片：当 $p_i = 1$，对 $P_{-,0} = 1 - |0\rangle\langle 0|$ 进行测量，当 $p_i = 0$，对 $P_{-,+} = 1 - |+\rangle\langle +|$ 进行测量.
5. Bob 通过公开的经典信道通知 Alice 他在哪些时间片检测到量子位，如没有噪声干扰，Bob 在这些量子位的测量结果与 Alice 制备它们的初值一致.
6. Alice 丢弃那些 Bob 没有检测到的量子位初始态. 根据经典统计理论，他们获得 $2n$ 个以上测量结果的概率接近于 1，万一获得的测量结果少于 $2n$ 个，他们可以重新进行制备和测量. 然后 Alice 从这些测量结果中随机选取 $2n$ 个留作后续使用，并选择其中的 n 个作为校验位.
7. Alice 和 Bob 公布各自校验位的值，若错误数超过 $ne_{\max}$，则放弃此次密钥分配，否则继续下一步.
8. Alice 公布 n 位二进制串 $u + v$，其中 v 是 n 个代码位的相应值，u 是 C_1 中的任意码字.
9. Bob 从他的含有错误的代码位 $v + e$ 中减去 $u + v$ 后得到 $u + e$，对之纠错后获得 u.
10. Alice 和 Bob 使用 C_2 在 C_1 中的陪集 $u + C_2$ 作为最终的密钥.

可见从第 6 步开始，B92 协议和标准 BB84 协议

基本相同.当然在标准 BB84 协议中,采用 CSS 码是为了证明的方便,我们在 B92 协议中采用 CSS 码是为了在形式上接近 Shor-Preskill 的 BB84 协议,实际上任何量子纠错编码都可以用来实现保密增强[9].

3.3. 修改的标准 BB84 协议

我们观察到在标准 BB84 协议中,Alice 制备初始态的过程可以分成两个阶段:首先由 t 来确定编码信息是 0 还是 1;然后根据 b 来确定使用哪一组基.编码基的选取过程可以等效为按照 b 的取值来决定是否实施 H 变换.如果 t 确定的初始编码位在基 $\{|0\rangle, |1\rangle\}$ 上,当 $b_i = 0$ 时,不对相应量子位执行 H 变换,当 $b_i = 1$ 时,则对之进行变换.例如当 $t_i = 1, b_i = 1$ 时,按照标准 BB84 协议的方法制备得到相应量子位 $|q\rangle_i = |+\rangle$,按照上述方法,由 $t_i = 1$,取初始编码位 $|0\rangle$,又由 $b_i = 1$,对初始编码位执行 H 变换得 $|+\rangle$,可见与标准 BB84 协议的结果相同.现在设初始编码值由两个非正交矢量来表示,即第一阶段按照 B92 协议的方法制备初始态,当 $t_i = 1$ 时,取 $|0\rangle$ 作相应量子位,而当 $t_i = 0$ 时,相应量子位取作 $|+\rangle$.第二阶段,b 仍然用来决定对相应量子位施行对称变换,不过这里不再采用 H 变换,我们所采用的对称变换可以用基 $\{|0\rangle, |1\rangle\}$ 上的矩阵表示为

$$\Xi = \frac{1}{\sqrt{2}}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}. \tag{7}$$

H 变换与 Ξ 变换的关系可以用图 1 来表示.

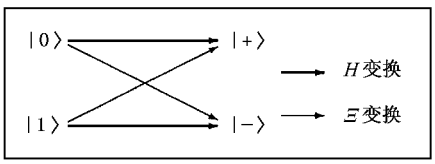

图 1 H 变换与 Ξ 变换

显然 Ξ 满足幺正性,其作用也是对两组基进行对换,不过 $\Xi|0\rangle = -|-\rangle$ 以及 $\Xi|+\rangle = |1\rangle$.经过上述改变后,Alice 制备的初始态在统计特性和对称性方面与按照标准 BB84 协议制备的量子态完全相同[11],如图 2 所示.

当 Bob 收到所有量子位后按任意基测量,Alice 公布 $m = b \oplus t$,即 b 和 t 的按位异或.根据上述分析,可以推出 $m_i = 1$ 所对应的量子位的编码基为 $\{|+\rangle, |-\rangle\}$,而 $m_i = 0$ 所对应的编码基为 $\{|0\rangle, |1\rangle\}$,Bob 可以据此判断自己是否采用了正确的测量基.若 Bob 所采用的测量基与 m 指示的不同,他们就丢弃相应的测量结果.最后经过修改的 BB84 协议相应的操作步骤变为

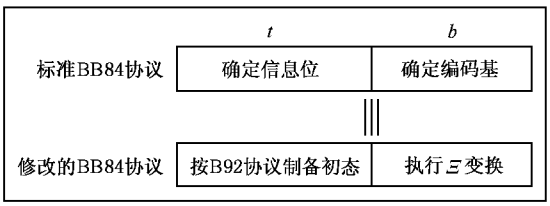

图 2 利用 Ξ 变换制备 BB84 协议的初始态

2'. Alice 根据 b 和 t 制备 $(4+\delta)n$ 个量子位,当 $t_i = 1$ 时,$|q\rangle_i = |0\rangle$,$t_i = 0$ 时,$|q\rangle_i = |+\rangle$;当 $b_i = 1$ 时,对第 i 个量子位实施 Ξ 变换,否则该量子位不变.

5'. Alice 公布 $m = b \oplus t$.

6'. 当 $m_i \neq p_i$ 时,他们丢弃相应量子位及测量结果.根据经典统计理论,他们获得 $2n$ 个以上测量结果的概率接近于 1,万一获得的测量结果少于 $2n$ 个,他们可以重新进行制备和测量.然后 Alice 从这些测量结果中随机选取 $2n$ 个留作后续使用,并选择其中的 n 个作为校验位.

显然,这种修改的 BB84 协议与标准 BB84 协议完全等效,因此在安全性方面也与标准 BB84 协议相同.

通过对称变换 Ξ,可以在不作较大改动的情况下将 B92 协议与标准 BB84 协议联系起来.由于量子密钥分配过程包括初态制备、测量及保密增强几个阶段,B92 协议与 BB84 协议最大的区别在于编码基不同,在实现过程中就表现为初态制备的不同.将标准 BB84 协议的初态制备过程分解为 B92 协议初态制备和实施 Ξ 变换两个互相独立的阶段,有助于我们利用已经证明为安全的 BB84 协议来验证 B92 协议的安全性.在基于 CSS 码的 BB84 协议中,H 变换的作用是使比特错误和位相错误的概率相同,Bob 接收到量子位后必须根据 Alice 提供的信息对相应量子位实施 H 变换.而我们的 Ξ 变换则是为了实现 B92 协议与 BB84 协议之间的转化,同时 Ξ 变换在密钥分配过程中只执行一次.另一方面我们也发现,这种修改的 BB84 协议不能直接转化为基于 CSS 码的方案.虽然各种状态矢量是对称的(出现的概率相同),但由于引入了 Ξ 变换,各种错误出现的概率是否相同难以证明,因此 CSS 码方案所要求的错误

对称性条件也难以保证.

3.4. 变形 B92 协议

由上述修改的 BB84 协议，发现 Ξ 变换可以由 Alice 在发送量子位前实施，也可以由 Bob 在测量前进行.这样修改的 BB84 协议就转化为我们的变形 B92 协议，如图 3 所示.图 3 中“$\rightarrow$”表示发送量子位，所以“$\rightarrow$”左边的操作由 Alice 执行，“$\rightarrow$”右边的操作由 Bob 执行.这一改变不会帮助 Eve 获得更多关于量子态的信息，因此也无益于她来窃取密钥.若 Ξ 变换由 Bob 在测量前实施，则对于 Alice 而言，她的操作与标准 B92 方案完全相同；对于 Bob，他的测量方法有了一些改动，首先他要对量子位实施随机 Ξ 变换，其次他将随机地选择对可观测量 $\Gamma_{01}=|0\rangle\langle 0|+|1\rangle\langle 1|$ 或 $\Gamma_{+-}=|+\rangle\langle +|+|-\rangle\langle -|$ 进行测量.对于 B92 协议，Bob 的检测方法并不影响协议的安全性，事实上，Bob 可以采用任何对获取信息最为有利的测量方法.然而应该看到，从统计学分析，上述方法并没有提高 Bob 获取信息的能力，他所能获得的信息也没有增加.

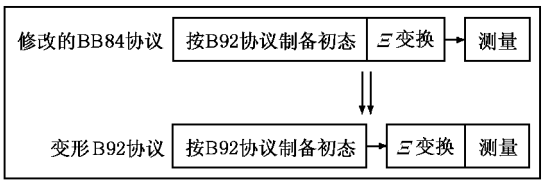

图 3　修改的 BB84 协议等效为变形 B92 协议

根据上面的分析，变形 B92 协议的操作过程为

1. Alice 选定一个 $n'=(8+\delta)n$ 位长的随机二进制串 b.
2. Alice 根据 b 制备 n' 个量子位，当 $b_i=1$ 时，$|q\rangle_i=|0\rangle$，当 $b_i=0$ 时，$|q\rangle_i=|+\rangle$.
3. Alice 将制备好的量子位通过量子信道逐个发送给 Bob.
4. Bob 随机选定两个 n' 位长二进制串 p，t，在第 i 时间片：当 $p_i=1$，对 i 量子位实施变换 Ξ，当 $p_i=0$，i 量子位不变.当 $t_i=1$，对 $\Gamma_{+-}=|+\rangle\langle +|+|-\rangle\langle -|$ 进行测量，每次测量结果编码为 $|+\rangle\rightarrow 0$，$|-\rangle\rightarrow 1$；当 $t_i=0$，对 $\Gamma_{01}=|0\rangle\langle 0|+|1\rangle\langle 1|$ 进行测量，每次测量结果编码为 $|0\rangle\rightarrow 1$，$|1\rangle\rightarrow 0$.全部的测量结果编码表示为二进制串 m.
5. Bob 通过公开的经典信道，通知 Alice 测量已经完成，并把序列 $k=p\oplus t\oplus m$ 广播出去，同样“$\oplus$”表示按位异或.
6. Alice 和 Bob 丢弃那些与 $k_i=1$ 所对应的位，根据经典统计理论，他们获得 $2n$ 个以上测量结果的概率接近于 1，万一获得的测量结果少于 $2n$ 个，他们可以重新进行制备和测量.然后 Alice 从这些测量结果中随机选取 $2n$ 个留作后续使用，并选择其中的 n 个作为校验位.

此后的操作过程与标准 BB84 协议中相应的步骤相同.

在变形 B92 协议中，第 5 步是因为不考虑信道噪声的情况下，只有当 $k_i=0$ 时，Bob 才能根据其测量结果完全确定 Alice 制备的初态，从而获得相应的编码信息.如图 4 所示.

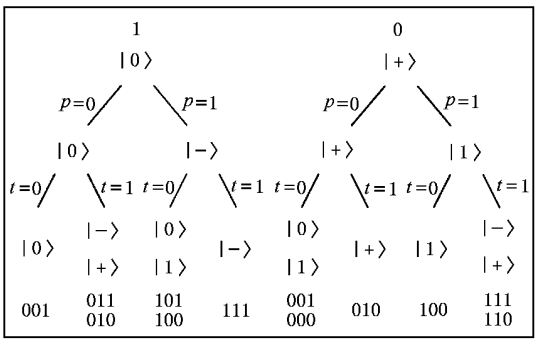

图 4　Bob 测量过程及过程代码

不考虑信道错误，Bob 对接收到的量子位进行测量.当量子位为 $|0\rangle$（编码信息为 1），若 $p_i=0$，则该量子位保持不变.当 Bob 测量 Γ_{01} 时，结果为 $|0\rangle$ 的概率为 1，该过程用代码表示为 001，三个码位分别表示 p，t 和译码信息；当 Bob 测量 Γ_{+-} 时，结果为 $|-\rangle$，$|+\rangle$ 的概率各为 50%，分别用 011，010 表示.同样可以对其他情况进行分析，并用代码表示，图 4 中最后一行即为相应的过程代码.显然 001，010，100，111 都分别出现两次，所以测量过程给出的信息是不确定的，而 000，011，101，110 则只出现一次，因此测量过程可以给出确定的编码信息.例如若 Bob 的测量过程代码为 011，那么他可以确信 Alice 发送给他的是 $|0\rangle$.此外这些给出确定结果的过程代码都具有校验值为 0 的特点，因此 Bob 只要公布 $p\oplus t\oplus m$，Alice 就知道了 Bob 已经正确提取了那些量子位的编码信息.

从以上分析可以发现，如果把执行 Ξ 变换作为

Bob 进行广义测量的一部分，那么变形 B92 协议对于 Eve 而言，与标准 B92 协议没有任何区别，所以二者的安全性完全等价. 另外，该协议与我们修改的 BB84 协议区别仅在于进行 Ξ 变换的时机，如果把 Ξ 变换也看作信道对量子位的作用，那么发送前还是发送后执行 Ξ 变换相当于交换 Ξ 和 σ_a 的位置，这只改变信道错误类型，而错误的数量以及信息的保密性都不会受到影响. 当然，如果由 Alice 执行 Ξ 变换，由于 Alice 事先知道了编码信息和编码基，所以可以公布其中之一来提高 Bob 的检测效率，这也正是标准 BB84 协议中情况. 图 5 总结了标准 BB84、修改的 BB84、变形 B92 以及标准 B92 协议之间的关系，从图 5 可以清楚地看到，经过一系列变换，标准 BB84 协议的安全性等价于标准 B92 协议.

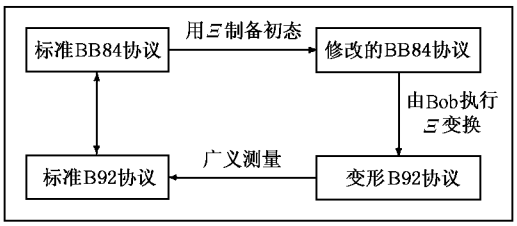

图 5 标准 BB84 协议与标准 B92 协议安全性的关系

4. 讨 论

虽然 Shor-Preskill 方法不能用来直接证明 B92 协议的安全性，但是他们的一些技巧，尤其是对称化方法和利用 CSS 码进行纠缠提纯，对于简化和改进 QKD 方案的安全性证明具有非常深远的影响. 在本文的证明中，通过借鉴他们的对称化方法，我们发现了利用 Ξ 变换在 BB84 和 B92 协议之间进行转换，从而可以利用已经被证明的 BB84 协议来证明 B92 协议. 另一方面，如果把 BB84 协议作为证明变换的一个阶段，那么仍然可以认为本文的证明是采用了 Shor-Preskill 的方法，这或许也解决了 Lo 提出的关于用 Shor-Preskill 方法证明 B92 协议的困难[12].

此外，本文的证明仍然引入了一些假设，包括 Bob 拥有量子寄存器及量子制备装置是完美的等. 事实上，本文所证明的无条件安全的 B92 协议本身并不要求 Bob 拥有最大寄存器，考虑到证明过程中，需要利用 BB84 协议的无条件安全性，而 Shor 等人在证明 BB84 协议的无条件安全时引入了量子寄存器，因此 B92 协议无条件安全性的证明也需要量子寄存器。当然，这些假设对于实用的量子密钥系统而言并不过分，当然在不包含上述假设的情况下证明 BB84 和 B92 协议以及其他 QKD 方案的无条件安全性仍然需要继续探索.

附录 关于命题‘在二状态 QKD 方案中，Bob 在连续 n 次测量中采用正确的检测方法并获得确定测量结果的概率随 n 增大呈指数减小’的证明

引理 1 不存在一种测量 P 可以严格区分非正交态 $|a\rangle$ 和 $|b\rangle$，即 $\langle a|P|a\rangle = 1$，且 $\langle b|P|b\rangle = 0$.

证 设 $\langle a|a\rangle = 1$，$\langle b|b\rangle = 1$，则由

$$\langle b|P|b\rangle = 0 \Rightarrow \langle b|b\rangle - \langle b|P|b\rangle = 1$$
$$\Rightarrow \langle b|(1-P)|b\rangle = \langle b|b\rangle\langle b|b\rangle$$
$$\Rightarrow P = 1 - |b\rangle\langle b|. \tag{A1}$$

将 P 代入 $\langle a|P|a\rangle = 1$，可得

$$\langle a|P|a\rangle = \langle a|a\rangle - \|\langle a|b\rangle\|^2 = 1 - \|\langle a|b\rangle\|^2 = 1. \tag{A2}$$

(A2)式表明 $\langle a|b\rangle = 0$，这显然与 $|a\rangle$，$|b\rangle$ 非正交矛盾.

引理 2 设 Bob 每次测量都可以获得一个确定的结果(0 或 1). 若 Bob 每次都选用了正确的检测方法进行测量，则对于连续 n 次测量(n 充分大)，Bob 通过测量所获得的信息为 0，因此测量本身毫无意义.

证 该引理可以通过经典概率论方法直接证明. 因为每次测量获得平均信息为 1 比特，所以 n 次测量可获得 n 比特信息. 但是 Bob 为了在 2^n 种测量方法中选择一种正确的方法，Bob 需要事先获得 $-\log 2^{-n} = n$ 比特的信息. 因此 Bob 通过测量所能获得的信息为 0.

定理 在二状态 QKD 方案中，Bob 在连续 n 次测量中采用正确的检测方法并获得确定测量结果的概率随 n 增大呈指数减小.

证 由引理 1 可得每次正确测量得到确定结果(0 或 1)的概率 $q < 1$，故每量子位包含的平均经典信息 $I = q < 1$，因此连续 n 次测量均采用正确的检测方法并获得确定测量结果的概率为 q^{-n}，当 n 充分大时，Bob 不可能获得全部的编码信息.

[1] Shor P W 1994 *Proceeding of the 35th Annual Symposium on the Foundations of Computer Science* (New York: IEEE Press) p124

[2] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (New York: IEEE Press) p175

[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[4] Ekert A 1993 *New Scientist* **137** 35
[5] Biham E and Mor T 1997 *Phys. Rev. Lett.* **78** 2256
[6] Hughes R J, Morgan G L and Peterson C G 2000 *J. Mod. Opt.* **47** 533
[7] Lo H K and Chau H F 1999 *Science* **283** 2050
[8] Mayers D 1996 *Advances in Cryptology—Proceedings of Crypto '96* (New York: Springer-Verlag) p343
[9] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[10] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824
[11] Duan L M 1997 *Acta Phys. Sin.* (*Overseas Edition*) **6** 811
[12] Lo H K and Chau H F 2001 *Preprint* quant-ph/0102138

Modification of B92 protocol and the proof of its unconditional security

Zhang Quan† Tang Chao-Jing Zhang Sen-Qiang
(*School of Electronical Science and Technology, National University of Deference Technology, Changsha* 410073, *China*)
(Received 28 April 2001; revised manuscript received 19 December 2001)

Abstract

Shor and Preskill's method with which thy proved the unconditional security of BB84 quantum key distribution protocol was analyzed first. We also indicated that their method could not be applied to prove the unconditional security of B92 scheme directly. In order to take advantage of Shor-Preskill's techniques in their proof of the unconditional security of BB84, we have introduced in this paper a transformation that can exchange between BB84 and B92. By proving that the transformed B92 protocol leaks no more information to eavesdropper, we demonstrate the unconditional security of B92. We also solve the problem how to prove the unconditional security of B92 with Shor-Preskill's method.

Keywords: B92 protocal, CSS code, QKD, quantum information
PACC: 0365, 4230

† E-mail: meva@cmmail.com