国 防 科 技 大 学 学 报
第 23 卷 第 6 期 JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY Vol.23 No.6 2001

文章编号：1001-2486（2001）06-0063-07

Shor-Preskill 方法不能直接证明 B92 量子密钥分配协议*

张权，谢晓霞

（国防科技大学电子科学与工程学院，湖南 长沙 410073）

摘 要：密钥分配协议安全性的证明是确保密钥分配绝对安全的要求，经典密码方案的安全性大多难以证明，而利用量子力学的基本原理，可以证明量子密码方案是无条件安全的。介绍了 Shor-Preskill 对 BB84 量子密钥分配协议无条件安全性的证明方法，归纳了其技巧和特点，揭示了对称化方法和量子纠缠提纯技术在该方法中的作用。证明了 Shor-Preskill 方法不能直接用来证明 B92 协议的无条件安全性。提出了利用 Shor-Preskill 方法间接证明 B92 的可能途径。

关键词：B92 协议；BB84 协议；量子密钥分配；量子信息

中图分类号：TN918.4 **文献标识码**：A

The Shor-Preskill Method Is Inapplicable to B92 Protocol

ZHANG Quan, XIE Xiao-xia

(College of Electronical Science and Technology, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: To ensure absolute security of key distribution, each key distribution scheme must be proved. While the security of most classical cipher schemes cannot be proved, the security of quantum cipher schemes is guaranteed by quantum mechanics and can be strictly proved. Shor-Preskill's method with which the unconditional security of BB84 quantum key distribution scheme is proved is introduced first. Its techniques and features are summarized and the subtleties of using symmetrization and quantum entanglement purification (QEP) to reduce a QEP based BB84 to a CSS based BB84, and of using the property of CSS code to reduce the CSS based BB84 to standard BB84 protocol are revealed. Then it is proved that Shor-preskill's method cannot be applied to B92 protocol directly. A possible solution to prove the unconditional security of B92 using Shor-Preskill's method indirectly is proposed.

Key words: B92 protocol; BB84 protocol; quantum key distribution; quantum information

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，以防止窃听者（Eve）从截获的信号中提取秘密信息。信息的保密性取决于密钥的安全性，因此密钥分发技术成为密码学研究的关键。除了一次一密便笺式密码本方案，所有其它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。量子信息理论的出现严重动摇了经典密码方案的安全性基础。Shor[1] 设计的量子算法可以在多项式时间内实现大数的素因子分解。另一方面，量子信息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[3~6]。

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和量子不可克隆定理[2] 所保证，因此量子密码术可以实现真正无条件的安全。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。由于量子密码术所具有的重要战略意义，QKD 的实验研究进展非常迅速[7]。

Shor-Preskill 成功地证明了 BB84 协议的无条件安全性[10]，在量子密码理论界引起了广泛的关注。由于 Shor-Preskill 的方法概念明确，思路简洁，因此被认为是量子密码术研究的一个里程碑。许多研究者开始尝试用 Shor-Preskill 方法证明其它 QKD 方案的无条件安全性。Lo 等就利用该方法成功

* 收稿日期：2001-04-23
作者简介：张权（1974-），男，博士生。

地证明了一种六状态 QKD 方案[12]。

可是，另一种非常著名的 QKD 方案—B92 协议[4]的安全性证明目前还是空白。虽然 B92 协议被认为是简化了的 BB84 协议，但是由于 B92 采用了非正交的基态作为编码量子位，Shor-Preskill 方法所要求的一些关键条件无法得到满足，因而限制了 Shor-Preskill 方法在 B92 协议证明中的应用。

1 BB84 协议的无条件安全性

证明一种量子密钥分配方案的无条件安全性，可以采取下述两种方法。

直接利用量子力学的基本原理：考虑各种可能的窃听策略，证明若窃听成功的概率大于指定门限，则必然违背量子力学的基本原理。例如在证明 BB84 协议防止非透明攻击时，就采用了这种方法。此方法要求的条件比较苛刻，同时要对各种可能的窃听策略进行分析，使得此方法的应用受到很大限制。

等效变换法：根据一种已经证明为无条件安全的 QKD 方案，经过若干步安全等效变换转化为需证明的 QKD，则此 QKD 也是无条件安全的。所谓安全等效变换，必须满足：(i) 经过变换，窃听必然导致量子信道发生变化，并且这种变换是可检测或可验证的；(ii) 安全等效变换不会使任何窃听引起的量子信道的变化程度减轻，例如，若窃听会导致量子位错误的话，那么经过变换，可检测错误的概率至少不小于变换前；(iii) 经过变换，密钥分配双方不需要透露更多的经典信息来实现纠错或安全增强。Shor-Preskill 在证明标准 BB84 无条件安全性的时候就采用了这种方法。

在标准 BB84 协议无条件安全性的证明中，Shor-Preskill 的证明思路是：首先证明基于纠缠提纯的 BB84 方案的无条件安全性；然后由纠缠提纯的 BB84 转化为基于 CSS 码的 BB84 方案，同时证明其安全性；最后由基于 CSS 码的 BB84 转化为标准 BB84，并证明转化过程于安全无损，从而证明标准 BB84 协议的安全性。由此可见，证明 BB84 协议安全性的关键是证明基于纠缠提纯的 BB84 方案的无条件安全性，并保证各步之间的转化是可行并且安全的。

1.1 纠缠提纯与 CSS 码

1.1.1 相关记号

在介绍 Shor 等的方法之前，首先介绍一些记号，如下矩阵称为 Pauli 矩阵：

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

其中 I 表示单位矩阵，这里把它作为 Pauli 矩阵是为了叙述的方便。显然，σ_x 作用在量子位上会造成比特翻转（bit-flip）错误，而 σ_z 会导致位相翻转（phase-flip）错误。取 n 位量子序列 R 并记第 k 个量子位为 R_k，对 $a\in\{x,y,z\}$，把 σ_a 作用在 R_k 上记为 $\sigma_{a(k)}$。对于二进制串 s，定义 $\sigma_a^{[s]}$：

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

其中 $s_i=0,1,\sigma_a^0=I$。取 σ_z 的本征态作为 2 维 Hilbert 空间 H_2 的一组正交基，并记作$|0\rangle$ 和$|1\rangle$。显然$|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$和$|+\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$为 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：

$$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix} \tag{3}$$

该变换被称为 Hadamard 变换。四个具有最大纠缠的二体量子系统 $\Phi^{\pm}=(|01\rangle\pm|10\rangle)/\sqrt{2}$ 和 $\Psi^{\pm}=(|00\rangle\pm|11\rangle)/\sqrt{2}$ 构成 H_4 的一组正交基，它们被称为 Bell 基。此外，记 $(\Phi^+)^n$ 为 n 重最大纠缠 Bell 态，简称为 n-Bell 态。

1.1.2 CSS 码

对于经典纠错码 C_1,C_2，若满足

$$\{0\}\subset C_2\subset C_1\subset F_2^n \tag{4}$$

其中 F_2^n 表示 n 维二进制向量空间，C_1 和 $C_2^{\perp}$（$C_2^{\perp}$ 是 C_2 的对偶码，即 $C_2^{\perp}$ 的校验矩阵为 C_2 的生成矩阵）

至多可以纠正 t(其中 $t = \lfloor (d-1)/2 \rfloor$，$d$ 是 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，其码字可以表示为：

$$\mu \mapsto \frac{1}{|C_2|^{1/2}} \sum_{\mu \in C_2} |\mu + \omega\rangle \tag{5}$$

其中 $\mu \in C_1$。当 $\mu_1, \mu_2 \in C_1$ 且 $\mu_1 - \mu_2 \in C_2$ 时，μ_1 和 μ_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，还用 $\boldsymbol{H}_1, \boldsymbol{H}_2$ 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 $\mu \in C_1$，相应的码字为：

$$\mu \mapsto \frac{1}{|C_2|^{1/2}} \sum_{\omega \in C_2} (-1)^{z \cdot w} |x + \mu + \omega\rangle, \tag{6}$$

其中 $z \cdot \omega = z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n$。可见，$Q$ 是 $Q_{x,z}$ 在 $x = z = \tilde{0}$ 时的特例。

1.1.3 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）[2] 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（<n）个最大纠缠的 EPR 对[11]。可以利用 CSS 码实现纠缠提纯。设 Alice 和 Bob 开始就共享一个 n-Bell 态，然后他们对 $\boldsymbol{H}_1$ 中的每一行 $[r]$，各自测量 $\sigma_z^{[r]}$，对 $\boldsymbol{H}_2$ 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 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 分别与 $\sigma_z^{[r]}$ 及 $\sigma_x^{[r']}$ 的测量值相吻合，显然 x，z 的值唯一。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^-），以及 k 个位相翻转（即 Φ^- 或 Ψ^-）。当 Alice 和 Bob 完成上述测量，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（$< n$）个 Φ^+。

1.2 标准 BB84 协议无条件安全性证明

1.2.1 基于纠缠提纯 BB84 方案及其安全性

基于纠缠提纯的 BB84 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[8]，同时量子纠错技术与纠缠提纯的关系也已经在前文说明，因此证明改进 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（$\gg 1$），一种 CSS 码和容许的最大错误概率 $e_{\max}$；

[1]：Alice 制备 $2n$ 个 EPR 对 $(\Phi^+)^{2n}$，并把每个 Φ^+ 中一个量子位归入 $\boldsymbol{A}$ 类，另一个归入 $\boldsymbol{B}$ 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 $\boldsymbol{B}$ 类量子位施行 Hadamard 变换；

[3]：Alice 通过量子信道把所有 EPR 对中的 $\boldsymbol{B}$ 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 Hadamard 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。如果超过 $e_{\max}$ 的校验位不一致，则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 $r \in \boldsymbol{H}_1$ 的每一行测量 $\sigma_z^{[r]}$，对 $r' \in \boldsymbol{H}_2$ 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 $(\Phi^+)^m$；

[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。

可见，该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，因此在窃听时她不可能有区别地对待监测到的量子位，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 Hadamard 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。所以此处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

$$P(\xi_{\text{code}} \geqslant e_{\max} \mid \xi_{\text{check}} \leqslant (e_{\max} - \delta)) < \exp\left(-\frac{1}{4}\delta^2 n/(e_{\max} - e_{\max}^2)\right) \tag{7}$$

其中 ξ_{code} 和 ξ_{check} 分别表示代码位和校验位的错误概率。式（7）表明通过适当选取 CSS 码和 $e_{\max}$，可以使检测失败的概率随 n 指数地减小。

1.2.2 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。已经证明[11]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 $\boldsymbol{B}$ 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它测量过程，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 $\boldsymbol{B}$ 类量子位之前测量 $\sigma_z^{[r]}$ 和 $\sigma_x^{[r']}$，相当于选定一个 $Q_{x,z}$ 来编码 $(\Phi^+)^m$，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（即在式(6)中使 $\mu = k$）。进行上述改动后，基于纠缠提纯的 BB84 就等价于如下基于 CSS 码的 BB84：

[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 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 Hadamard 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、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 Hadamard 变换；

[9]：Bob 比较校验序列和自己测量到的校验位取值，若 $\xi_{\text{check}} \geqslant e_{\max}$ 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。

1.2.3 标准 BB84 协议的安全性证明

从量子纠错码协议到 BB84 的简化过程中采用了 CSS 码的特性。在 CSS 码中，比特翻转和相位误差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。更具体地说，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：

$$\frac{1}{2^n(C_2)}\sum_z \sum_{\omega_1,\omega_2 \in C_2} (-1)^{(\omega_1+\omega_2)\cdot z} \mid k + \omega_1 + x\rangle\langle k + \omega_2 + x \mid$$

$$= \frac{1}{\mid C_2 \mid}\sum_{\omega \in C_2} \mid k + \omega + x\rangle\langle k + \omega + x \mid \tag{8}$$

该状态相当于 $|k+\omega+x\rangle$ 的经典混合态，其中 $\omega \in C_1$。设 Alice 发送给 Bob 的态为 $|k+\omega+x\rangle$，Bob 接收到的码字为 $|k+\omega+x+e\rangle$，他从中减去 x 并译码得到 C_1 中的一个码字 μ，可以证明 $P(\mu = k+\omega) \to 1$。于是他们可以用 $\mu + C_2$ 作为最终的密钥。这一过程就等价于如下标准 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 1 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 1 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 $\mu+\nu$，其中 ν 是 n 个代码位的相应值，μ 是 C_1 中的任意码字；

[9]：Bob 从他的含有错误的代码位 $\nu+e$ 中减去 $\mu+\nu$ 后得到 $\mu+e$，对之纠错后获得 μ；

[10]：Alice 和 Bob 使用 C_2 在 C_1 中的陪集 $\mu+C_2$ 作为最终的密钥。

2 Shor-Preskill 方法的特点

在证明基于纠缠提纯的 BB84 时，一个非常重要的条件是 Alice 和 Bob 正确地估计错误概率。可是在操作中他们只对可观测量 $\Gamma_{01} = |0\rangle\langle 0| + |1\rangle\langle 1|$ 进行测量，没有办法区分比特错误和位相翻转错误，如何保证两种错误总的错误概率小于 $e_{\max}$ 是基于纠缠提纯的 BB84 有效性的关键。利用 Hadamard 变换，在两种错误之间实现对称，就很好地解决了上述问题。

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 中，对于 $b_i = 1$ 的 EPR 对，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：

$$e_{\text{bit-flip}}^{\{01\}} + e_{\text{phase-flip}}^{\{+-\}} = \frac{1}{2}(p_2+p_3) + \frac{1}{2}(p_1+p_2) = \frac{1}{2}(p_1+2p_2+p_3) \tag{9}$$

其中上标表示相应的基，同样位相错误概率为：

$$e_{\text{phase-flip}}^{\{01\}} + e_{\text{bit-flip}}^{\{+-\}} = \frac{1}{2}(p_1+p_2) + \frac{1}{2}(p_2+p_3) = \frac{1}{2}(p_1+2p_2+p_3) \tag{10}$$

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，只要计算比特翻转错误概率就可以了解总的错误概率。

在基于 CSS 码的 BB84 方案中，Alice 将用 CSS 码 $Q_{x,z}$ 编码后的密钥 k 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。这一点非常关键，因为它保证了 CSS 码方案的有效性。为此，Shor 和 Preskill 在基于 CSS 码的 BB84 中使用了量子寄存器，在 Bob 收到所有码字后 Alice 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。

由基于 CSS 码的 BB84 来证明标准 BB84 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 可以转化为标准 BB84。

3 Shor-Preskill方法不能直接证明B92协议

3.1 标准B92协议

标准B92量子密钥分配协议采用任意两个非正交的态对信息进行编码，本文设 $1 = |0\rangle$，$0 = |+\rangle$。B92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 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制备它们的初值是一致的；

[6]：Alice丢弃那些Bob没有检测到量子位初始态。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。

由此可见，从第7步开始，B92和BB84协议一样采用CSS码进行保密增强。当然在BB84中，采用CSS码是为了证明的方便，而在B92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[10]。

3.2 Shor-Preskill方法不能直接证明B92协议

第2节中的特点都是Shor-Preskill证明方法必须满足的基本条件，由于在B92协议中，这些条件大多难以满足，因此限制了我们使用该方法直接证明B92协议的无条件安全性。

首先，B92协议采用两个非正交态矢（注意在BB84中采用了两组正交基，即四个态矢）进行密钥分配，也就是说，在BB84协议中，采用了两组正交基 $\{|0\rangle, |1\rangle\}$ 和 $\{|+\rangle, |-\rangle\}$ 对信息位进行编码，而B92协议则采用两个中非正交的态，例如 $\{|0\rangle, |+\rangle\}$，来编码信息位。在BB84中，由于比特错误和位相翻转错误的概率相同，所以可以采用Hadamard变换使平均错误概率等于比特错误概率。但是在B92协议中，当发生比特错误或位相翻转时，量子位成为两个编码态混合态。此时，即使错误概率事实上是对称的，Alice和Bob也没有办法加以区分。因此在B92中无法进行类似的的对称简化。

其次，对于B92协议，不可能设计出类似于基于CSS码BB84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。以下就是该结论的证明。

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

$$\begin{aligned}\langle b|P|b\rangle = 0 &\Rightarrow \langle b|b\rangle - \langle b|P|b\rangle = 1\\ &\Rightarrow \langle b|(\mathbf{1}-P)|b\rangle = \langle b|b\rangle\langle b|b\rangle\\ &\Rightarrow p = \mathbf{1} - |b\rangle\langle b| \end{aligned} \tag{11}$$

将 P 代入 $\langle a|P|a\rangle = 1$ 可得：

$$\langle a|(\mathbf{1}-P)|a\rangle = \langle a|a\rangle - \|\langle a|b\rangle\|^2 = 1 - \|\langle a|b\rangle\|^2 = 1 \tag{12}$$

式(12)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　该引理可以用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 比特。

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 $q < 1$，故测量每量子位获得的平均经典信息 $I = q < 1$，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。

上述定理表明，除非 Alice 告知 Bob 关于每个量子位的测量基，Bob 不可能对连续 n 个随机量子位都正确地测量并获得确定的测量结果。而这样做，显然会让 Eve 获得关于密钥的相关信息。因此，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。

4　讨论

Shor-Preskill 方法不能用来直接证明 B92 协议的安全性，但他们所采用的一些技巧，尤其是对称化方法和利用 CSS 码进行纠缠提纯等，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。本文通过分析 Shor-Preskill 方法的特点，说明直接应用他们的方法来证明 B92 协议是不可行的。当然，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 可以转化为 BB84 协议。因此，我们认为可以利用 BB84 来间接地证明 B92 协议的无条件安全性。证明的主要思路是，对 Shor-Preskill 已经证明的 BB84 协议进行适当的变换，说明这种经过变换的 BB84 可以等效于某种改进的 B92 协议，利用改进的 B92 协议证明标准 B92 协议的无条件安全性。此外，在 Shor-Preskill 的证明中仍然引入了一些假设，如 Bob 拥有量子寄存器，量子制备装置是完美的等。这些假设对于实用的量子密钥系统而言并不过分，也没有违背无条件安全性的要求，但是如果在不包含上述假设的情况下证明 BB84 以及其它 QKD 方案的无条件安全性，将更能说明 QKD 无条件安全性的优势。

参考文献：

[1] Shor P. Algorithms for quantum computation：Discrete logarithms and factoring [A], Proc. of 35th Symp. Found. of CS, 1994：124-134.

[2] Wootters W K, etc. A single quantum cannot be cloned [J]. Nature, 299, 1982：802-803.

[3] Bennett C H, etc. Quantum key distribution and coin tossing [A]. Proc. of IEEE Int. Conf. on Comp. Sys. Proces. , IEEE press, 1984：175－179.

[4] Bennett C H. Quantum cryptography using any two nonorthogonal states [J]. Phys. Rev. Lett. 68, 1992：3121－3124.

[5] Ekert A. Quantum cryptography based on Bell ' s theorem [J]. Phys. Rev. Lett. 67, 1991：661－663.

[6] Biham E, etc. Security of quantum cryptography against collective attacks [J]. Phys. Rev. Lett. 78：2256－2259, 1997.

[7] Hughes R J, etc. Quantum key distribution over a 48 km optical fibre network [J]. J. Mod. Opt. 47：533－547, 2000.

[8] Lo H K, etc. Unconditional security of quantum key distribution over arbitrarily long distances [J]. Science 283, pp2050, 1999.

[9] Mayers D, preprint http：//xxx. lanl. gov/abs/quant－ph/9802025, to appear in J. of Assoc. Comp. Mach. A preliminary version in D. Mayers.

[10] Shor P W, etc. Simple proof of security of the BB84 quantum key distribution protocol [J]. Phys. Rev. Lett. 85：441－444, 2000.

[11] Bennett C H, etc. Mixed－state entanglement and quantum error correction [J]. Phys. Rev. A 54：3824－3851, 1996.

[12] Lo H K, etc. Proof of unconditional security of six－state quantum key distribution scheme [EB]. http：//xxx. lanl. gov/abs/quant－ph/0102138.