四维 Hilbert 空间上的量子密钥分配协议*)

李恕海　王育民

(西安电子科技大学综合业务网络国家重点实验室　西安 710071)

摘　要　文中抽出了在 4 维 Hibert 空间上的量子密钥分配算法，构造了三种测量基来应对能在两个量子比特上出现的所有错误，保证了窃听检测过程的有效性，从而提供了无条件安全性的根本依据，该协议的最大优势在于显著节省上了量子和经典信息的通信量。

关键词　量子密码学，错误检测，Bell 基测量，无条件安全性

A Novel Quantum Key Distribution Protocol on 4-dimensional Hilbert Space

LI Shu-Hai　WANG Yu-Min

(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract　A novel quantum key distribution protocol is proposed in this paper, by constructing three different types of measurement bases. Such unusual construction guarantees that all possible errors occurred on two qubits can be detected, and provides the unconditional security proof. The most distinguishable advantage of the QKD protocol is saving a great amount of quantum and classical communications.

Keywords　Quantum cryptology, Error detection, Bell-state measurement, Unconditional security

1　引言

自从第一个量子密码协议 BB84[1] 提出以来，大量的量子密码协议相继出现，但大多数的量子密钥分配协议是建立在二维的 Hilbert 空间上，即协议执行的双方每次随机使用两种测量基中的一种测量一个量子比特(可以看成是二维 Hilbert 空间上的一个向量)。本文提出了一个新型的量子密钥分配协议，构造了三种测量基，每次测量两个量子比特(qubit)。这么做的最大优势在于不损害无条件安全性的前提下，节省了经典和量子比特的通信量。

2　协议描述

符号记法：四个 Bell 量子态：$|\Phi^{\pm}\rangle=(|0_A0_B\rangle\pm|1_A1_B\rangle)/\sqrt{2}$，$|\Psi^{\pm}\rangle=(|0_A1_B\rangle\pm|1_A0_B\rangle)/\sqrt{2}$。四个 Pauli 矩阵：$I=\begin{bmatrix}1&0\\0&1\end{bmatrix}$，$X=\begin{bmatrix}0&1\\1&0\end{bmatrix}$，$Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$，$Y=iXZ=\begin{bmatrix}0&-i\\i&0\end{bmatrix}$。Hadamard 变换 $H=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$。$|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$，$|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$。纠缠转移：假设有两个 EPR(Enistein-Podolsky-Rosen)对 $A_1B_1=|\Phi_1^+\rangle=(|0_{A1}0_{B1}\rangle+|1_{A1}1_{B1}\rangle)/\sqrt{2}$ $A_1B_1=|\Phi_2^+\rangle=(|0_{A2}0_{B2}\rangle+|1_{A2}1_{B2}\rangle)/\sqrt{2}$，$A_1A_2$ 被发送给 Alice，B_1B_2 被发送给 Bob，它们使用 Bell 测量基测量，结果可表示如下：

$$|\Phi_1^+\Phi_2^+\rangle=\frac{1}{2}(|\Phi_A^+\Phi_B^+\rangle+|\Phi_A^-\Phi_B^-\rangle+|\Psi_A^+\Psi_B^+\rangle+|\Psi_A^-\Psi_B^-\rangle) \quad (1)$$

下标 A 表示 A_1A_2 所处的量子状态，下标 B 表示 B_1B_2 所处的量子状态。当 A_1B_1 和 A_2B_2 处于其他的 Bell 态时，Alice 和 Bob 使用 Bell 基的测量结果如表 1[6] 所示，显然只有当这两个 EPR 对处于同样的状态，它们的测量结果才相同。

表 1　纠缠交换的结果

A_1B_1 \ A_2B_2	$\|\Phi_2^+\rangle$	$\|\Phi_2^-\rangle$	$\|\Psi_2^+\rangle$	$\|\Psi_2^-\rangle$
$\|\Phi_1^+\rangle$	a	b	c	d
$\|\Phi_1^-\rangle$	b	a	d	c
$\|\Psi_1^+\rangle$	c	d	a	b
$\|\Psi_1^-\rangle$	d	c	b	a

a,b,c,d 中的四种状态 Alice 和 Bob 是等概获得的。

$a=\{|\Phi_A^+\Phi_B^+\rangle+|\Phi_A^-\Phi_B^-\rangle+|\Psi_A^+\Psi_B^+\rangle+|\Psi_A^-\Psi_B^-\rangle\}$

$b=\{|\Phi_A^+\Phi_B^-\rangle+|\Phi_A^-\Phi_B^+\rangle+|\Psi_A^+\Psi_B^-\rangle+|\Psi_A^-\Psi_B^+\rangle\}$

$c=\{|\Phi_A^+\Psi_B^+\rangle+|\Phi_A^-\Psi_B^-\rangle+|\Psi_A^+\Phi_B^+\rangle+|\Phi_A^-\Psi_B^-\rangle\}$

$d=\{|\Phi_A^+\Psi_A^-\rangle+|\Phi_A^-\Psi_B^+\rangle+|\Psi_A^+\Phi_B^-\rangle+|\Psi_A^-\Phi_B^+\rangle\}$

协议描述：

1. 假设 Alice 有两个 EPR 源 $A_1B_1=|\Phi_1^+\rangle$ 和 $A_2B_2=|\Phi_2^+\rangle$，Alice 保留 A_1A_2，把 B_1B_2 发送给 Bob。

2. Alice 和 Bob 对 A_1A_2 和 B_1B_2 随机做下述三种测量之一：测量基 I：$\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$，测量基 II：$\{|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle\}$，测量基 III：$\{|+0\rangle,|+1\rangle,|-0\rangle,|-1\rangle\}$，所得的测量结果分别对应两个经典比特{00,01,10,11}。

3. Alice 和 Bob 重复 1 和 2 步$(18/5)n$ 次，如果 n 充分大，Alice 和 Bob 得到$(6/5)n$ 个相同测量基的结果，将其中的 n 个测量结果用作窃听检测，如果结果有太多不同，那么 Alice 和 Bob 放弃协议，否则进入下一步。

4. Alice 和 Bob 进一步按如下方法回收不同测量基的测量结果。

5. Alice 和 Bob 对相同基的测量结果和回收后的测量结

*)基金项目：National Natural Science Foundation of China(No. 60672119)。李恕海　博士研究生。

果做信息调和以及保密增强最后得到安全的密钥比特。

回收不同测量基测量结果的策略：

假设 $A_1B_1=A_2B_2=|\Phi^+\rangle$，那么

1)当 Alice 使用 I 型测量基测量 A_1A_2，而 Bob 使用 II 型测量基测量 B_1B_2。注意如下关系，$|\Phi_1^+\Phi_2^+\rangle=\frac{1}{2}(|00_A00_B\rangle+|01_A01_B\rangle+|10_A10_B\rangle+11_A11_B\rangle)$ (2)

当 Alice 得到 $|00\rangle$ 或 $|11\rangle$ 时，相应的测量结果 $a_1a_2=00$ 或 11；在 Bob 没有测量前，显然 $B_1B_2=|00\rangle$ 或 $|11\rangle$，然后使用 Bell 基测量处于 $|00\rangle=(|\Phi^+\rangle+|\Phi^-\rangle)/\sqrt{2}$ 或 $|11\rangle=(|\Phi^+\rangle-|\Phi^-\rangle)/\sqrt{2}$ 的 B_1B_2，测量结果 b_1b_2 要么是 00，要么是 01，而不可能是 10 或 11，所以 Alice 可以判断如果 $a_1a_2=00$ 或 11，同时 Bob 一定得到 $b_1b_2=00$ 或 01，那么这时他们认为可回收的结果为 $r=a_1\oplus a_2=b_1=0$。同样当 Alice 得到 $|01\rangle$ 或 $|10\rangle$ 时，在 Bob 没有测量前 B_1B_2 $|01\rangle$ 或 $|10\rangle$，而 $|01\rangle=(|\Psi^+\rangle+|\Psi^-\rangle)/\sqrt{2}$，$|10\rangle=(|\Psi^+\rangle-|\Psi^-\rangle)/\sqrt{2}$，Alice 可以判断如果 $a_1a_2=01$ 或 10，Bob 一定得到 $b_1b_2=10$ 或 11，那么这时可回收的结果同样可表示为 $r=a_1\oplus a_2=b_1=1$。这样 Alice 和 Bob 可以回收一半的测量结果。

2)当 Alice 使用 I 型测量基测量 A_1A_2，而 Bob 使用 III 型测量基测量 B_1B_2。根据式(2)，如果 Alice 得到 $|00\rangle$ 且测量结果 $a_1a_2=00$，此时 $B_1B_2=|00\rangle=(|+0\rangle+|-0\rangle)/\sqrt{2}$，即 Bob 使用 III 型测量基所得的结果 $b_1b_2=00$ 或 10，因此 Alice 和 Bob 认为测量结果 $r=a_2=b_2=0$。同样 $|01\rangle=(|+1\rangle+|-1\rangle)/\sqrt{2}$，$|10\rangle=(|+0\rangle-|-0\rangle)/\sqrt{2}$，$|11\rangle=(|+1\rangle-|-1\rangle)/\sqrt{2}$，因此其余的情况完全相同，Alice 和 Bob 放弃 a_1 和 b_1，保留 a_2 和 b_2 来回收一半的测量结果。

3)当 Alice 使用 II 型测量基测量 A_1A_2，而 Bob 使用 III 型测量基测量 B_1B_2。由(1)可知，当 Alice 得到 $A_1A_2=|\Phi^+\rangle$，Bob 得到 $B_1B_2=|\Phi^+\rangle=(|+0\rangle+|+1\rangle+|-0\rangle+|-1\rangle)/2$，即 b_1b_2 可能是 00,01,10,11 中的任何一个，因此 Alice 不能判断出任何有关 Bob 测量结果的信息，而 $|\Phi^-\rangle=(|+0\rangle+|+1\rangle-|-0\rangle+|-1\rangle)/2$，$|\Psi^+\rangle=(|+0\rangle-|+1\rangle+|-0\rangle+|-1\rangle)/2$，$|\Psi^-\rangle=(-|+0\rangle+|+1\rangle+|-0\rangle+|-1\rangle)/2$，所以这种情况下 Alice 和 Bob 不能回收任何有用的测量结果。

注意到当 Alice 和 Bob 互换角色时与上面的情况完全一致。综上所述，Alice 和 Bob 不但能将大约 1/3 的相同测量基的测量结果留下，而且还能根据不同的情况回收大约 2/9 的不同测量基的测量结果，即共 5/9 的测量结果可用。

3 安全性证明

证明思路是将我们的协议等价于 Modified Lo-Chau Protocol[5]，首先根据安全性定理[3]：如果 Alice 和 Bob 能够确定没有被用作错误检测的 $\rho=(A_1B_1A_2B_2)^{\otimes n}$ 与 $|\Phi^+\rangle^{\otimes 2n}$ 的保真度 $F(\rho,|\Phi^+\rangle^{\otimes 2n})=\sqrt{\rho^{\frac{1}{2}}(|\Phi^+\rangle\langle\Phi^+|)^{\otimes 2n}\rho^{\frac{1}{2}}}$ 满足：$F(\rho,|\Phi^+\rangle^{\otimes 2n})>1-2^{-s}$，那么

$$S(\rho)<(2n+s+1/\ln 2)2^{-s}+O(2^{-2s}), \quad (3)$$

这里 $S(\rho)=-\mathrm{tr}(\rho\log\rho)$ 是密度矩阵 ρ 的 Von Neumann 熵。如果式(3)成立，那么 Eve 能得到有关 ρ 的信息量为指数无穷小。这里先将 Alice 和 Bob 使用同样测量基的量子比特当作是 Alice 和 Bob 存储的，然后进行错误检测。注意到 B_1B_2 处于 $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle,|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle,|+0\rangle,|+1\rangle,|-0\rangle,|-1\rangle\}$ 的等概混合态，根据不可克隆定理，任何窃听者 Eve 要想获得有关 B_1B_2 的信息，唯一的方法是测量它，但是这种测量会导致错误，如果 Alice 和 Bob 能够确定 ρ 中的错误数目少于量子纠错码的纠错限度，那么它们就能执行一个量子纠错的过程，从而将 Eve 有关 ρ 的信息量减少到指数级无穷小，所以这里应该先考量 Alice 和 Bob 如何确定错误数量。

检错模式：任何发生在单个比特 $|\varphi\rangle$ 上的错误 E 可以表示为

$$E=e_0I+e_1X+e_2Z+e_3XZ, \quad (4)$$

因此，只需检测到 X,Z,XZ 三种错误。

拓展到 2 个量子比特的情况下错误就表示为 $E^{\otimes 2}$，即需要检测到 $\{I_1X_2,I_1Z_2,I_1X_2Z_2,X_1I_2,X_1X_2,X_1Z_2,X_1X_2Z_2,Z_1I_2,Z_1X_2,Z_1Z_2,Z_1X_2Z_2,X_1Z_1I_2,X_1Z_1X_2,X_1Z_1Z_2,X_1Z_1X_2Z_2\}$ 这 15 种错误症状，下标 1,2 分别表示 Pauli 矩阵作用在 B_1 和 B_2 的位置。这些错误都能被这三种基测到，具体检测细节如下：

由式(2)，显然出现在 B_1B_2 上的任何包含 X 的错误症状，Alice 和 Bob 使用 I 型测量基的测量结果一定不同，因此 I 型测量基检测到 $I_1X_2,I_1X_2Z_2,X_1I_2,X_1X_2,X_1Z_2,X_1X_2Z_2,Z_1X_2,Z_1X_2Z_2,X_1Z_1I_2,X_1Z_1X_2,X_1Z_1Z_2,X_1Z_1X_2Z_2$。

II 型测量基检测到 $I_1X_2,I_1Z_2,I_1X_2Z_2,X_1I_2,X_1Z_2,X_1X_2Z_2,Z_1I_2,Z_1X_2,Z_1X_2Z_2,X_1Z_1I_2,X_1Z_1X_2,X_1Z_1Z_2$ 这是因为，当 Alice 和 Bob 都使用 Bell 基测量时，根据表 1 和表 2 可以看出只要出现在 B_1B_2 上的错误类型不相同，那么它们所得到的结果就不相同，因此它们可以在窃听检测的过程中发现。

表 2 有错误发生时 $|\Phi_1^+\Phi_2^+\rangle$ 的状态转换

	I_{B2}	X_{B2}	Z_{B2}	$X_{B2}Z_{B2}$
I_{B1}	$\|\Phi_1^+\Phi_2^+\rangle$	$\|\Phi_1^+\Psi_2^+\rangle$	$\|\Phi_1^+\Phi_2^-\rangle$	$\Phi_1^+\Psi_2^-\rangle$
X_{B1}	$\|\Psi_1^+\Phi_2^+\rangle$	$\|\Psi_1^+\Psi_2^+\rangle$	$\|\Psi_1^+\Phi_2^-\rangle$	$\Psi_1^+\Psi_2^-\rangle$
Z_{B1}	$\|\Phi_1^-\Phi_2^+\rangle$	$\|\Phi_1^-\Psi_2^+\rangle$	$\|\Phi_1^-\Phi_2^-\rangle$	$\Phi_1^-\Psi_2^-\rangle$
$X_{B2}Z_{B2}$	$\|\Psi_1^-\Phi_2^+\rangle$	$\|\Psi_1^-\Psi_2^+\rangle$	$\|\Psi_1^-\Phi_2^-\rangle$	$\Psi_1^-\Psi_2^-\rangle$

根据共轭关系 $X=HZH$，$Z=HXH$，$XZ=-HXZH$，因此 III 型测量基检测到的错误症状相当于，将 I 型测量基检测到在 B_1 上的错误做关于 H 的共轭变换，得到如下可检的错误症状：$I_1X_2,I_1X_2Z_2,Z_1I_2,Z_1X_2,Z_1Z_2,Z_1X_2Z_2,X_1X_2,X_1X_2Z_2,X_1Z_1I_2,X_1Z_1X_2,X_1Z_1Z_2,X_1Z_1X_2Z_2$。

Alice 和 Bob 回收后的共大约 $2n$ 比特可用测量结果，根据随机抽样定理[5]，Alice 从中随机抽取 n 个比特作为测试比特，然后告诉 Bob 所选位置，Alice 和 Bob 比较测试比特；对任何 $\delta>0$，在测试比特中少于 δn 个错误，而在剩余的没有测试的比特中多于 $(\delta+\varepsilon)n$ 个错误的概率渐进地小于 $\exp[-O(\varepsilon^2n)]$。因此在协议中第 3 步认证成功后，剩余的测量结果中的错误数量也没有超过量子纠缠限度的概率以指数级趋近于 1。然后进行量子纠错纠正 ρ 中的错误得到保真度为 1 的 EPR 对，从而导致 Eve 得到的信息为指数无穷小，这个过程等价于协议中第 5 步对测量结果进行信息调和与保密放大[5,6]，得到最终的安全密钥比特；如果错误数量超过了量子纠错限度，就认为 Eve 窃听引入的错误数量不能被纠正，Alice 和 Bob 放弃该协议。因此我们的协议是无条件安全的。

结论 文中提出的 4 维的量子密钥分配协议，与其它协

(下转第 86 页)

证明:我们需要证明任意与 $f(x)$ 相互独立的函数 $g(x)$ 都可以通过算法 2 来生成。设 $f(x)$ 与 $g(x)$ 相互独立,为书写方便,我们记 $d=\gcd(2^n,W_H(f))$。根据定理 2,我们有

$$W_H(fg)=\frac{W_H(f)W_H(g)}{2^n}=\frac{W_H(f)}{d}\cdot\frac{dW_H(g)}{2^n}$$

令 $k=\frac{dW_H(g)}{2^n}$,则 k 必为整数(否则可以推出 $W_H(fg)$ 不为整数,这显然不可能)。因此上式表明,$supp(f)$ 中有 $k\cdot\frac{W_H(f)}{d}$ 个元素包含在 $supp(g)$ 中,或者可以等价地理解为,当将 $supp(f)$ 中的元素分成大小为 $\frac{W_H(f)}{d}$ 的组时,在 $supp(g)$ 中有 k 个这样的组。更精确地,$supp(f)\cap supp(g)$ 的大小为 $k\cdot\frac{W_H(f)}{d}$(否则很容易导出矛盾结论)。如果能证明 $supp(g)$ 中另有 $supp(\bar{f})$ 中的 $k\cdot\frac{W_H(\bar{f})}{d}$ 个元素,则 $g(x)$ 就是按照算法 2 生成的。容易验证,

$$k\cdot\frac{W_H(f)}{d}+k\cdot\frac{W_H(\bar{f})}{d}=k\cdot\frac{2^n}{d}=\frac{dW_H(g)}{2^n}\cdot\frac{2^n}{d}=W_H(g)$$

这就证明了 $supp(f)$ 中的 $k\cdot\frac{W_H(f)}{d}$ 个元素和 $supp(\bar{f})$ 中的 $k\cdot\frac{W_H(\bar{f})}{d}$ 个元素构成了 $supp(g)$ 中的全部元素。故定理结论得证。

下面给出一个例子说明这种构造方法的工作原理。

例 1 4 个变元的布尔函数 $f(x)=x_1\oplus x_2x_3\oplus x_1x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_1x_2x_4$ 的支撑为 $supp(f)=\{0001,0011,0110,0111,1000,1001,1010,1011,1100,1101,1110,1111\}$,并且 $supp(\bar{f})=\{0000,0010,0100,0101\}$。将 $supp(f)$ 和 $supp(\bar{f})$ 分别分成 $\gcd(2^n,W_H(f))=4$ 组,对 $supp(f)$ 有多种不同的分法,这里随便选一种,不妨按照上述排列次序每三个一组。然后分别从 $supp(f)$ 和 $supp(\bar{f})$ 中取整数 k 组作为 $supp(g)$。当 $k=1$ 时,我们可以得到不同的 $g(x)$:

$g_1(x)=1\oplus x\oplus x_2\oplus x_1x_2\oplus x_3\oplus x_1x_3\oplus x_3x_4\oplus x_1x_3x_4$

$g_2(x)=x_3\oplus x_1x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4$

$g_3(x)=x_2\oplus x_1x_3\oplus x_4\oplus x_1x_4$

$g_4(x)=x_2x_3\oplus x_1x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_2x_3x_4$

$g_5(x)=1\oplus x_2\oplus x_3\oplus x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4$

$g_6(x)=x_1\oplus x_1x_2\oplus x_3\oplus x_2x_3\oplus x_3x_4\oplus x_1x_3x_4$

$g_7(x)=x_1\oplus x_2\oplus x_1x_3\oplus x_2x_3\oplus x_2x_4\oplus x_1x_2x_4$

$g_8(x)=x_1\oplus x_1x_2\oplus x_1x_3\oplus x_1x_2x_3\oplus x_2x_4\oplus x_1x_2x_4$

$g_9(x)=1\oplus x_1\oplus x_2\oplus x_3\oplus x_2x_3\oplus x_1x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{10}(x)=x_1x_2\oplus x_3\oplus x_2x_3\oplus x_1x_2x_3\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{11}(x)=x_2\oplus x_1x_3\oplus x_2x_3\oplus x_1x_2x_3\oplus x_2x_4\oplus x_2x_3x_4$

$g_{12}(x)=x_1x_2\oplus x_1x_3\oplus x_2x_4\oplus x_2x_3x_4$

$g_{13}(x)=1\oplus x_1\oplus x_2\oplus x_1x_2\oplus x_3\oplus x_1x_3\oplus x_2x_3\oplus x_4\oplus x_1x_4\oplus x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{14}(x)=x_3\oplus x_1x_3\oplus x_2x_3\oplus x_1x_2x_4\oplus x_3x_4\oplus x_1x_3x_4\oplus x_2x_3x_4$

$g_{15}(x)=x_2\oplus x_1x_2\oplus x_2x_3\oplus x_2x_4\oplus x_2x_3x_4$

$g_{16}(x)=x_1x_2x_3\oplus x_2x_4\oplus x_2x_3x_4$

例 1 仅仅给出了对 $supp(f)$ 的一种分组的情况,对于每一种分组,同样可以得到另外 16 个函数。对 $k=2,3$ 的情况同样讨论。注意当 $k=2$ 时,所构造的函数是平衡的。

结论 本文研究了布尔函数的统计独立的性质、判定、构造。利用布尔函数的汉明重量,给出了两个布尔函数统计独立的充分必要条件。进一步,对任意给定的布尔函数,如果它存在统计独立的函数的话,本文给出了一种构造所有那些与给定函数统计独立的布尔函数,并证明了其正确性和完备性。本文的结果将有利于文[3]中布尔置换构造算法的实现。

参 考 文 献

1 Shamir A, Rivest R L, Adlemen L. A method for obtaining digital signatures. Comunications of the ACM, 1979,21(2):120~126

2 Wu C K, Veredherejen V. Public Key Cryptosystems Based on Boolean Permutations and Their A lications. International Journal of Computer Mathematics,2000,74(2):167~184

3 何良生,孙红波. 布尔置换的构造,电子学报(已录用,待发表)

4 武传坤. 密码学中的布尔函数:[西安电子科技大学博士学位论文]. 1993

5 邢育森,杨义先. 密码体制中布尔置换的构造和记数. 通信学报,1998(3):74~76

6 温巧燕,等. 密码学中的布尔函数. 科学出版社,2000

(上接第 76 页)

议的不同之处在于,不同测量基的测量结果不是完全相互独立的,因此可以回收。这种构造方法在节省经典通信量和量子比特数上有显著的优势,如表 3 所示。

表 3 通信量的比较

每 n 个量子比特	经典通信量(bits)	丢弃量子数(qubits)
BB84,Ekert'91[2]	$2n$	$(1/2)n$
我们的方案	$(\log_2 3)n\approx 1.6n$	$(4/9)n$

参 考 文 献

1 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proc. IEEE Int. Conf. on Computers, systems, and signal processing, Bangalore, IEEE, New York, 1984. 175~179

2 Ekert A K. Quantum cryptography based on Belll's theorem. Phys Rev Lett, 1991, 67: 661~663

3 Gao Fei, Guo Fenzhuo, Wen Qiaoyan, Zhu Fuchen. Quantum key distribution without alternative measurements and rotations, Physics Letters A, 2006, 349: 53~58

4 Lo H, Chau H F. Unconditional security of quantum key distribution over arbitrary long distance. Science, 1999, 283, 2050~2056; Also available at arXive eprint quant-ph/9803006

5 Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 587~591

6 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. ,2000, 85:441~444; Also available at arXive e-print quant-ph/0003004

7 秦素娟,刘太琳,温巧燕. 基于纠缠交换和局域操作的量子秘密共享. 北京邮电大学学报,2005,28(4):74~77