量子密钥分配及其无条件的安全证据 [1]

刘传才

(福州大学计算机系 福州 350002)

摘 要 量子密码学因密钥分配而众所周知，然而早先提出的量子密钥分配的安全证据包含许多技术困难．该文提出了一个概念更为简明的量子密钥分配的安全证据．此外，研究中还发现，在隐形传输下，因为改变了非平凡误差的模型序列，所以隐形传输信道的误差率与正被传输的信号无关．为此，将这一事实与最近提出的量子到经典的约简定理相结合．在讨论中，假定通信双方 Alice 和 Bob 有容错的量子计算机，结果表明：在任意长的距离上，即使面临各种窃听攻击及各种噪声存在的情况下，量子密钥分配依然具有无条件的安全特征．

关键词 量子密码学，量子密钥分配，隐形传输信道，窃听

中图号 TN918.1

1 引 言

1994 年，Shor 提出了一种能将 NP(Non Polynomial-time) 问题转化为 P(Polynomial-time) 问题的量子算法 [1]，矛头直指 RSA[2] 方法，从而在全球掀起了量子计算的研究热潮．就在这期间，量子密钥分配 (QKD, Quantum Key Distribution) 方法应运而生 [2,3]．量子不可克隆定理指出，任何人 (包括窃听者) 不可能为未知的量子态作一个完善的拷贝 [4,5]．因此，在一个量子信道上的窃听将几乎肯定会产生可察觉的扰动．

可以毫不夸张地说，量子计算机面世之日就是 DES 和 RSA 土崩瓦解之日．在这种情形下，虽然一次一密方法仍能保持完好的不可破的密码，但却存在着严重的密钥分配欺诈问题．一般来说，只要消息保密，Alice 和 Bob 就共享一个密钥，但实际上无法确保．从另一个角度来说，经典物理学原则上无法阻止窃听密钥分配信道的事件发生．

为克服上述缺陷，人们一直努力探索新的加密方法来解决这些问题．令人激动的是利用量子力学的特征可实现两个陌生人之间通信的完美保密．如同量子力学方法破译像 RSA 那样用传统方法构造的密码系统一样，量子力学也可帮助编码 [2]．Heisenberg 测不准原理指出，对于微观粒子，由于具有波动性，其坐标和动量不能同时取确定值．由量子力学施加的这个表观限制可成为一个强有力的捕获窃听者的工具，其基本思想是使用非正交的量子状态来为信息编码．更具体地说可用 4 个可能的极化状态 ($\rightarrow,\uparrow,\nearrow$ 或 $\nwarrow$) 之一来描述单个光子，人们是否能确定它的极化状态呢？答案是否定的．

2 安全要求和安全证据的思想

定义 对于任何由 Alice 和 Bob 选择的安全参数 $k, l > 0$，如果这些安全参数遵循量子密钥分配协议，以及如果能构造一个校验标准，使得对于由 Eve 实施的任何窃听攻击能以一个不可忽略的概率值 (即大于 e^{-l}) 通过检测，并满足两个条件：(1) 可忽略拥有最终密钥而小于 e^{-L} 的 Eve 的互信息；(2) 实际上最终密钥本质上是随机的，则就可说这个 QKD 方案是无条件安全的．

在此，首先讨论 QKD 安全证据的简明思想．Alice 准备 r 个量子信号，并将它们的状态编码为一个长度为 n 的量子纠错码 (QECC, Quantum Error Correcting Code)[6]，QECC 能纠

[1] 2001-09-18 收到，2002-06-13 改回
973 资助项目 (编号：G1998030600)，福建省自然科学基金资助项目 (编号：F00013)

[2] RSA 是一种公钥密码体制，根据它的发明者 Rivest, Shamir 和 Adleman 命名．

正 t 个错误. 此外, Alice 也准备了 m 个其它的量子信号, 并将其用作测试信号. 然后 Alice 随机地置换 $N=n+m$ 个信号, 并通过一个由窃听者控制的噪声信道将它们发送给 Bob . Bob 公布他接收到的由 Alice 发送的所有 N 个信号. 依据 Bob 的接收确认, Alice 公布 m 个测试信号的位置和它们的特定状态. Bob 测量 m 个测试信号和计算它们的误差率 e_1 . 利用 e_1 和统计学中经典的随机采样理论, Alice 和 Bob 为 n 个未测试的信号建立置信水平. 因此, 对窃听者窃听的 r 个量子编码信号的信息量施加一个随机约束 (在 QECC 中, 除非发生错误的数量大于 t , 否则 Eve 绝对不会知道有关编码的状态) . 如果 Alice 和 Bob 对安全等级表示满意, 他们就测量 r 个量子信号来生成 r-bit 的密钥.

要使上述思想凑效, 需满足 3 个要求: (1) 每个误差模型可用一个经典的概率来确定; (2) 信号的误差率与被传输的实际信号无关 (即 Eve 不能以某种方式将一个非平凡模式变为一个依赖于所传输信号的平凡模式) ; (3) 可容错地实现量子纠错和密钥生成.

因为运用经典论据可能靠不住, 所以在没有精确数学证明的情况下, 人们将概率分布分配给误差模型的集合是自然朴素的观点. 事实上, 大多数通用的量子信道不满足 (1) 和 (2) 的要求.

对于二分纠缠对 (EPR, halves of Einstein-Podolsky-Rose pairs) 传输的特定情况, 文献 [7] 已证实了要满足要求 (1) . 此外, 在量子信息理论中, 借助隐形传输 (quantum teleportation)[3] 过程, 任何通用的量子状态可约化为标准态的传输和经典通信 [8] . 对于一个量子隐形传输信道, 不变性的结果确保一个单纯的窃听者不能改变它的根本错误率, 而使它依赖于传输的量子信号的同一性. 后面的命题 2 将讨论量子隐形传输信道错误率的不变性. 如果 Alice 和 Bob 两人共享 R 个 EPR 对, 通过沿某些通用的轴测量每个成员, 就能获得一个通用的随机数串 (一个 R-bit 的密钥) . 假定 R 对几乎完全保真, 量子力学定律确保生成的密钥将几乎完全是随机的, 而且 Eve 获得的有关密钥的信息量是可忽略的. 事实上, 存在如下引理 [7] :

引理 1 对于一个足够大的 k , 如果 Alice 和 Bob 共享 R 个保真的 EPR 对, 并且至少为 $1-2^{-k}$. 通过沿任何通用的轴测量这些对, Alice 和 Bob 就生成一个 R-bit 的密钥, 那么 Eve 关于最终密钥的互信息受 $2^{-c}+2^{O(-2k)}$ 的约束 (其中 $c=k-\log_2[2R+k+(1/\log_e 2)]$) .

因此, 即使在有噪声和 Eve 的情况下, 利用解决安全 QKD 的 Holy Grail 第二方法可构造分配 R 个几乎完美的 EPR 对的方案.

3 量子到经典的约简定理

如果能将经典的概率理论和统计理论中强有力的技术应用于约简问题, 就可大大简化 QKD 的安全证明. 因此, 本文证明的一个关键所在是量子到经典的约简定理 (文献 [7] 已证明了该定理) , 该定理解释经典论据的使用是正确的. 在数学上, 可将这种量子到经典的约简定理表述为定理 1[7] .

定理 1 考虑一个由 ρ 描述的混合量子状态和一个作用在它上面的一维非对易投影算子 Q_j 的集合. 假设存在一个 Q_j 的粗粒可观测量 O_i 的完备集, 以致使所有 O_i 相互间对易 (粗粒化意味可将每个 O_i 写为一个正交投影 Q_j 集合的和, 以及通过完备实现 $\sum_i O_i=I$) . 让我们考虑一个完备的 von Neumann 测量 M , 它与所有 O_i 对易 (因为 O_i 元素的可互换性, 所以必存在这样的 M) . 令 $|v_k>$ 为 M 的基矢. 因此, $\forall i$, 存在

$$\mathrm{Tr}(O_i\rho)=\mathrm{Tr}(O_i\sum_k |v_k><v_k|\rho|v_k><v_k|) \tag{1}$$

[3] 又称 "量子态的远程传输", 它是一种描述量子态传输的概念. 目前国内还无统一叫法.

依据文献 [9] 的证明，$\forall O_i$，存在一个系数 λ_i 和一个集合 K_i 使得 $O_i = \lambda_i \sum_{l\in K_i} |v_l><v_l|$，以及依据迹 $\mathrm{Tr}A$ 的定义 $\sum_m < v_m|A|v_m >$，可将 (1) 式写为

$$\mathrm{Tr}(O_i\rho) = \sum_m < v_m|\lambda_i \sum_{l\in K_i} |v_l><v_l| \sum_k |v_k><v_k|\rho \sum_{k'} v_{k'}><v_{k'}|v_m>$$

$$= \lambda_i \sum_{l\in K_i} < v_l|\rho|v_l >$$

因为 $|v_l>$ 是 M 的第 l 个本征态 (基矢)，v_l 是本征值，以及 $< v_l|\rho|v_l >$ 是系统处于第 l 个本征态的几率，所以 $\sum_{l\in K_i} < v_l|\rho|v_l >$ 是系统在集合 K_i 内的几率和．因此 (1) 式的意义是系统在集合 K_i 内的几率和的 λ_i 倍．(1) 式表明：一个先前完备的 von Neumann 测量 M 不改变所有粗粒输出 O_i 的概率．命题 1 将进一步阐述定理 1．

在此，引用文献 [7] 中第 2054 页的例子 (i)．假定两个独立的观测者 Alice 和 Bob 共享一个大数，比如说 N，成对的量子比特 [4] 可能由 Eve 准备．而这些对可能以任意方式相互纠缠 (entanglement)，而且也与外部世界纠缠． Alice 和 Bob 怎样才能估计出这 N 对中的单态数呢？解决方法是利用下面的随机采样过程和命题．

随机采样过程　首先令 k 为随机采样过程中获得的逆平行结果的数目，假定 Alice 和 Bob 随机选择 N 对中的 m 对．对于每一对，随机选择 3 个轴 $(x, y$ 和 $z)$ 中的某个轴，接着沿它测量两个成员，并公布他们的结果．

命题 1[7]　在 N 对中，可把单态部分的 f_s 估计为 $(3k-m)/(2m)$．此外，对于有 N 个目标的有限总体，可由经典的统计理论推断出置信水平．

命题 1 的证明可参考文献 [9] 的详细论述

4 安全的 QKD 方法

对一个由 Alice 和 Bob 共享的量子通信信道，命题 1 中的单态部分 f_s 具有可靠的量子比特份额．假定 Alice 局部地准备了 N 个 EPR 对，之后，通过一个由 Eve 控制的噪声信道， Alice 将每对的一个成员发送给 Bob．由于噪声信道和窃听攻击的结果，这 N 个 EPR 对中的某些可能受到污损．在实际传输中，基于少数传输信号的随机采样，命题 1 给出了一个可靠的量子比特的数学估计．

因为有 QECCs，首先通过使用随机采样过程来估计传输的误差，并试着去构造一个安全的 QKD 方法．其次使用 QECC 来纠正适当的错误数，人们渴望能构造一个安全的 QKD 方法．为确保采样过程真正随机，在实际 QECC 中， Alice 应随机成对地混合测试对．

对于每个被传输的量子信号，需要考虑 4 个误差算子 I, σ_x, σ_y 和 σ_z．这实际上隐含地承认了下面假设的正确性．

假设 1　一个量子通信信道的错误率与被传输的信息无关．更确切地讲，在当前的情形下及在分析 QKD 方法的安全性问题中，人们可安全地为每个错误模式分配一个概率．

尽管此假设直观上似乎是合理的，但是人们仍不知道任何有关通用量子信道的精确证明．为阐述此问题，本文证明一个相关的、或许更弱的涉及一个隐形传输信道的结果．在此，使用一个众所周知的事实：即通过隐形传输可将任何量子信息传输到一个量子通信信道中去．

4.1 隐形传输

在隐形传输 [8] 中，通过同时使用先验的“纠缠” (即由发送方 Alice 和接收方 Bob 共享的标准 EPR 对) 和一个经典的通信信道来实施量子信号的传输． Alice 手中的量子信号因她实

[4] 在量子信息论中，信息的载体不再是经典比特，而是一个一般的二态量子体系，这个二态量子体系可以是一个二能级的原子或离子，也可以是一自旋为 1/2 的粒子或具有两个偏振方向的光子，所有这些体系，均称为量子比特．

施局部测量而被破坏，从而生成一个经典的消息．那么这种消息通过一个经典的通信信道传送给 Bob．由于依赖这种消息的内容，那么通过将 I,σ_x,σ_y 和 σ_z 的某个幺正变换应用到原来与 Alice 共享的 EPR 对的每个成员，从而 Bob 就可重构损坏的量子信号．

有两点值得注意．首先，在隐形传输中，Alice 和 Bob 共享同样的先验纠缠，而这样的纠缠与将被传输的实际量子信号无关．在隐形传输过程的先验共享部分持续的期间内，既然 Alice 总是发送同样的标准量子信号给 Bob，那么在第 3 节中，可直接使用经典的随机采样理论．其次，如果采用可靠的量子计算机来实施，则在隐形传输中，重构步骤不会将新的错误引入到量子系统中．实际上，如果 Alice 和 Bob 把他们共享的噪声量子态用于隐形传输，那么对于每个被传输的信号来说，在重构过程期间，仅仅相互置换了三类错误 σ_x,σ_y 和 σ_z．即使一个误差模式的量子叠加和具有表观限制的纠缠 (由 Alice 和 Bob 共享的初始噪声量子态指定)，这种思想也是正确的．

从数学角度出发，可用公式来表示这种结果．从 Alice 到具有最通用混合态 ρ_u 的 Bob，考虑一个由 N 个量子比特组成的系统 S 的隐形传输．不失一般性，一个由混合态描述的系统可等同地用一个大系统的纯态来描述，而此大系统由一个初始系统和一个辅助系统组成 (对于这种简单有用的观测，John Smolin 称之为 " the Church of the larger Hilbert space "，最近推广使用了这种方法 [10−13]．例如，位承诺 [11−12] 和有关二中取一的隐形传态 [13] 的不可能性的最新证明推广采纳了该思想)．将此思想应用到本文的通用情形，就可将最初系统 S(加上与之有牵连的辅助系统 R) 的态写为

$$|v>_{RS}=\sum_m c_m|w_m>_R|v_m>_S \tag{2}$$

上式中的 c_m 为复数系数，$|w_m>_R$ 和 $|v_m>_S$ 分别为两个系统 R 和 S 的某些基向量．在 " the Church of the larger Hilbert space " 中，也可将 Alice 和 Bob 共享的 N 对初态 ρ_u 纯化为

$$|u>=\sum_{i_1,i_2,\cdots,i_N}\sum_j \alpha_{i_1,i_2,\cdots,i_N,j}|i_1,i_2,\cdots,i_N>\otimes|j> \tag{3}$$

上式中的 i_k 表示第 k 对的状态，它适用 $\tilde{0}\tilde{0}$ 到 $\tilde{1}\tilde{1}$ 的范围，$|j>$ 的量子态为环境 (或由 Eve 制备的一个附属物) 构成了一个正交基，而 $\alpha_{i_1,i_2,\cdots,i_N,j}$ 为某些复数系数．每个状态 $|u>$ 表示一个特定的混合状态．注意到，$|u>$ 可作为一个不同误差模式的线性叠加的纠缠和

$$|u>=\sum_{i_1,i_2,\cdots,i_N}\sum_j \alpha_{i_1,i_2,\cdots,i_N,j}\left(\prod_k \sigma_{i_k}^{(k)}\right)|\psi^->^N\otimes|j> \tag{4}$$

由于不论是 I,σ_x,σ_y，还是 σ_x 都依赖 i_k 的值，所以 (4) 式中的 $\sigma_{i_k}^{(k)}$ 影响到第 k 对的 Bob 成员，而 $|\psi^->$ 表示一个 EPR 对．借助这样的符号表示法，可证明本文的主要命题．

命题 2 在隐形传输之下，误差率保持不变．在上面的符号表示法中，假定采用 Alice 和 Bob 共享的 N 对 (在 (4) 式中，由 N 对组合系统的态 $|u>$ 和 (4) 式中 Eve 的附属物 (ancilla) 来描述) 来实现系统 S(在 (2) 式中，通过组合系统 R 和 S 的 $|v>_{RS}=\sum_m c_m|w_m>_R|v_m>_S$ 来描述) 的隐形传输．进一步假定 Alice 测量的经典输出量为 $\{j_k\}$，即 Alice 通知 Bob 在重构过程中使用算子 $\prod_k \sigma_{j_k}^{(k)}$．因此，可将组合系统 R, S 和 ε 的 Bob 重构态描述为

$$\sum_m c_m|w_m>_R\sum_{i_1,i_2,\cdots,i_N}\sum_j \alpha_{i_1,i_2,\cdots,i_N,j}\left[\prod_k(\sigma_{j_k}^{(k)}\sigma_{i_k}^{(k)}\sigma_{j_k}^{(k)})\right]|v_m>_S\otimes|j> \tag{5}$$

在隐形传输下，复数系数 $c_m\alpha_{i_1,i_2,\cdots,i_N,j}$ 集保持完全不变. 对于每个由 $\{j_k\}$ 标记的隐形传输结果，在作用于子系统的误差算子中，唯一可能的变化取决于耦合行动，即 $\forall k$ ， $\exists\sigma_{i_k}^{(k)}\to\sigma_{j_k}^{(k)}\sigma_{i_k}^{(k)}\sigma_{j_k}^{(k)}$（$\sigma_{j_k}^{(k)}$ 总是它自己的逆），唯一有效的变化是共轭级合操作. 因为在这样的耦合下，平凡的误差算子 (即恒等式 I) 是不变式，并且可以相互交换 3 个非平凡误差算子 σ_x,σ_y 和 σ_z 的位置，所以隐形传输信号的误差率完全与初始的 N 个 EPR 对的相同.

在量子信息理论 [8] 中，这是一个简明的运用. 有关命题 2 的证明，在此不做赘述.

4.2 安全 QKD 方法的过程

在命题 2 的基础上，给出安全 QKD 方法的过程.

(1) Alice 准备 N 个 EPR 对，并通过一个噪声信道把每对的一个成员发送给 Bob (理论上，量子转播器 [14] 和用于所谓纠缠净化法 (量子纠错码的一种推广) 的双向方案可用在此步中. 因此，这里的错误率可以减到很小，而且对任意长的距离方案也有效).

(2) Bob 公开地宣布他所接收到的 N 个量子信号.

(3) Alice 随机地选取 N 个 EPR 对中的 m 对用于测试，并公开地向 Bob 通告她的选择. 对于每一对， Alice 和 Bob 随机地选取三个轴 (x,y 和 z) 中某个轴，并沿选择的轴对两个成员做一次测量.

(4) Alice 和 Bob 公开地发布他们的测量结果，并使用经典的采样理论来估计传输中的错误率.

命题 1 允许 Alice 和 Bob 将经典的采样理论应用于量子问题来估计未测试粒子的错误率. 然后， Alice 和 Bob 在下一步中继续实施量子纠错.

(5) Alice 准备估计 R 个 EPR 对，并通过 QECC 将 R 个半对 (即每对的一个成员) 编码为 $N-m$ 的量子比特.

在下一小节将讨论 QECC 的必要条件.

(6) 借助他们共享所保留下的 $N-m$ 对， Alice 隐形传输 $N-m$ 个量子比特给 Bob .

命题 2 确保在隐形传输之下错误率的不变性. 因此， Alice 和 Bob 在第 4 步所作的估计是有效的.

(7) 沿一个预先规定的通用轴 (比如说 z 轴)，通过测量 R 个编码的 EPR 对的状态， Alice 和 Bob 执行容错量子计算以生成一个随机的 R-bit 密钥.

4.3 容错量子计算

依据命题 1 和 2 ，若存在可靠的局部量子计算机，很明显本文的方案是很有效的. 然而，因局部量子计算可能不完备，隐形传输和密钥生成期间，亦即在执行第 (6) 步和第 (7) 步期间，可能产生错误. 通过选择拥有强的纠错和容错能力的 QECC ，人们就能容易地考虑那些局部错误. 关键是要考虑一个特定的短计算 (仅沿 z 轴测量，并且不作任何幺正计算) . 任何基于量子计算机的实际误差模型和 QECC 的具体选择，由于不完备的量子计算，人们可给局部误差数一个宽松的上界. 随着容错的实现，在整个过程 (传输、隐形传输和密钥生成) 中，可约束总的误差数. 因此，假定 QECC 有强的纠错和容错能力 (由于量子态非常脆弱，人们通过进一步改进量子纠错码来提高 QECC 的纠错和容错能力：因为使用量子纠错码能改进有噪声的量子计算机的性能，所以操作编码状态引起的误差是受控扩散的. 量子纠错码是量子计算机的一个研究热点之一，但难度不小，目前还未找到一种有效的量子纠错码.)，则安全就能保障 (更准确在第 (5) 步) . 应以编码形式而不是以非编码形式容错地准备 R 个 EPR 对. 由于这里所要求的量子

计算比文献 [7] 中的更简单，因而本文提出的 QKD 方法比文献 [7] 的方法更有效。

5 QKD 的安全分析

就实际的量子密钥分配方案来说，其安全性是未来应用的中心问题。迄今为止，并没有很多适合现有方案和考虑了实际攻击类型的安全分析文献。在本节中，作者将提供一种 QKD 的安全分析。

Nielsen 等 [15] 的研究表明，窃听发生在如下 3 种情况： (1) Eve 仅限于测量单个光子，并且能无误差地做任何这样的测量。 (2) Eve 能测定出一个脉冲中的光子数，并在不干扰其状态的情况下从一个脉冲中分离出一个光子。 (3) Eve 没有量子存储器，并且它的所有测量都在基公布之前完成。 (4) Eve 可用一根更透明的光纤来替换 Alice 和 Bob 间的光纤。为简单起见，假定 Eve 可用一根完好的光纤来替换它。 (5) Eve 不能影响 Alice 或 Bob 设备的物理配置。

(1) 在单光子脉冲波的情况下， Eve 实施单光子的窃听-重发攻击 (SIR, Single Intercept-Resend attack)。 Bennett 等证明 [16]，这种攻击最好是在 Breidbart 基 (即一个 22.5 度取向的基) 下测量该光子。在与受测光子状态相同的情形下， Eve 重发一个脉冲。此时 Eve 推断 Alice 发送位的正确概率为 $\cos^2(\pi/8) \approx 0.85$，为此导致 Bob 的误差率至少为 0.25[15]。

(2) 在脉冲波含有两个光子的情况下，有两种攻击方式可供 Eve 选择： (a) 要么测量 2 个光子； (b) 要么测量 1 个光子。对于前者， Eve 实施一种称之为双光子的窃听-重发攻击 (DIR, Double Intercept-Resend Attack)。在此情况下，即使 Eve 能确切地知道该脉冲的发送位 (bit)，她也不能使 Bob 接收该脉冲波的误差概率比 $\sin^2(\pi/8) \approx 0.15$ 更小。对于后者，实际上是一种 SIR。首先，发送给 Bob 的脉冲波至少含有一个处于正确状态的光子。因此， Eve 知道发送位的概率至多为 0.85。其次， Eve 可能将未受测的光子传送给 Bob，因此 Bob 的误差概率将是正常的 (ε, 因为 Eve 不能影响 Bob 的设备)，但 Eve 冒了光子在设备中损耗的风险。这种攻击也称为分离攻击 (SO, Split-Off attack)。 Alice 传播一束有两个光子的脉冲波的概率小于 $\lambda^2/2$(λ 是 Alice 发送的脉冲波中含有的平均光子数)。即使 Eve 通过一个完好的光纤传输未受测的光子给 Bob 的设备，但是如果光子通过 Bob 的设备接受检测，那么就只对密钥有影响。因此，脉冲波中 $\lambda^2 F_{\text{Bob}}\eta_B/2$ 的份额留给 Eve 去做 SO 攻击 (F_{Bob} 和 η_B 的物理意义见文献 [15])。为增加这种攻击的效应， Eve 可能选择阻塞某些别的脉冲波，一般她不测量单光子的脉冲。在那些 Bob 检测的脉冲波之中，这将增加受攻击脉冲的份额。然而，对 Eve 所阻塞的脉冲波的数量是有限制的：若 Eve 不出现，则 Bob 希望能检测一定数量的脉冲波，更准确地说， Bob 正常地检测发送脉冲的份额为 $\lambda F\eta_B$。 Eve 必须近似地维持受测脉冲波的数量，否则原始密钥 (the raw key) 将比期望的更短。因此，在源于和隶属于脉冲波的原始密钥中，位的份额 f_{SO} 可能至多为

$$f_{\text{SO}} \le \lambda^2 F_{\text{Bob}}\eta_B/(2\lambda F\eta_B) = \lambda/(2F_{\text{fiber}}) \tag{6}$$

Eve 自己也可能发射一个或多个光子到脉冲波中。如果 Bob 偶然测量这些光子中的某个光子，而不是测量标准的光子，那么误差概率至少为 0.25(重新考虑上面的窃听-重发攻击)。由于 Eve 不能控制 Bob 测量哪个光子，所以在此情况下 Bob 的总误差概率至少为 $\Pr\cdot 0.25 \ge 0.125$ (Pr 为 Bob 测量 Eve 发射某个光子的概率)。另一方面， Bob 有更多的机会检测该脉冲波，为简单起见，假定 Bob 将总以这样的方式检测受攻击的脉冲波。 Nielsen 等将这种攻击称之为分离重发攻击 (SOR, the Split-Off-Resent attack)[15]。

(3) 在含有 3 个或 3 个以上光子的脉冲波中，原则上至少能以某个非零的概率唯一地确定脉冲波的状态 [17]。在此情况下， Alice 发送这样的脉冲波的概率至多为 $\lambda^3/6$。发送的脉冲波

中受测的份额为 $\lambda F\eta_B$. 因此，依据与 SO 攻击相同的论据可推知，这样的脉冲波至多贡献 f_3 的份额给原始密钥的各位

$$f_3 = \lambda^2/(6F\eta_B) \tag{7}$$

为简单起见，假定在所有情形下 Eve 会实施一种 SIR， DIR 或 SOR 攻击，它不是将脉冲波传送给第 3 方 (BB, Big Brother) . 此外，假定 BB 知道 Alice 的所有选择，并且 BB 将返回脉冲波中发送给 Eve 的位. 如果 Bob 在适当的基下测量，则在一种以这样方式构造的状态中发送一个强的脉冲给 Bob， Bob 的误差概率为 0.125 . 当然，现实生活中不存在这样的第 3 方，设置第 3 方仅仅是为了便于分析和说明. 在实际生活中， Eve 不会比利用 BB 做得更好： Eve 肯定能获得受攻击的脉冲波的位. 在所考虑的 3 种攻击之中，受此因素影响而导致 Bob 的误差最小.

在此，有必要考虑基公布之后和原始密钥计算出之后的情形. 在原始密钥的位之外， Eve 知道的份额为 $f_3 = \lambda^2/(6F\eta_B)$ ，而 Bob 能正确地测量这些位. 此外，位的份额 $f_{\rm SO}$ 源于 SO 攻击的脉冲波，而最终的份额 $f_{\rm BB}$ 源于 Eve 利用 BB 攻击的脉冲波. 这意味 Bob 的观察误差率为 $0.125f_{\rm BB} + (1 - f_{\rm BB} - f_3)\varepsilon$. 为了不被截获， Eve 必须大致地确定 ε . 依据这一点，可容易地导出

$$f_{\rm BB} \le f_3\varepsilon/(0.125 - \varepsilon) \tag{8}$$

注意到，仅当 $\varepsilon < 0.125$ 时，上式才有意义.

其次，考虑 Eve 可获得的信息. 为估计保密增强 (privacy amplification) 效应，对多光子脉冲波和 BB 做假设，假定 Eve 能确切地知道位的份额 $f_3 + f_{\rm BB}$. 此外，对于隶属于 SO 攻击的脉冲波，既然在公布单个基之前， Eve 必须测量单个光子，显然 Eve 确实不知道所有的对应位. 根据文献 [16] ，为了对抗保密增强， Eve 的最佳策略是在 Breidbart 基下测量每个光子，这样它就能以 85% 的概率了解每一位. 因此，基于文献 [18] ，即使 Eve 确切地知道 0.585 份额的位，人们也能计算. 因此，在原始密钥中，假定 Eve 知道的位份额至多为

$$f_3 + f_{\rm BB} + 0.585f_{\rm SO} \le \lambda^2(1 + \varepsilon/(0.125 - \varepsilon))/(6F\eta_B) + 0.585\lambda/(2F_{\rm fiber}) \tag{9}$$

当然，在未受攻击的脉冲波中， Eve 完全不知道位.

最后考虑误差效应和校正问题，即必须校正 ε 的误差份额. 这要求泄露位的份额至少为 $h(\varepsilon)$, 依据 Shannon 约束，这里的 $h(\ )$ 是二进制熵函数 $h(\varepsilon) = \varepsilon\log(1/\varepsilon) + (1-\varepsilon)\log 1/(1-\varepsilon)$. 当 ε 小到和这里所考虑的一样时，相互作用的方法 (Cascade) 非常接近该约束. 因此，就保密增强而言，如果 $f_{\rm Eve} = f_3 + f_{\rm BB} + 0.585f_{\rm SO} + h(\varepsilon)$ 以及 n 为原始密钥中的位数，那么 Eve 就知道误差校正后有关原始密钥确定的位信息 $nf_{\rm Eve}$. 如果使用标准的保密增强方法从最终密钥的 $n(1 - f_{\rm Eve}) - s$ 位蒸馏 [18] ，那么在 s 内有关最终密钥的 Eve 的期望信息呈指数地减小，事实上，至多为 $2^{-s}/\ln 2$ 位. 因此，关于最终密钥及大的 n ，对于一个特定的有关 Eve 信息的期望约束，可蒸馏出的位份额本质上为

$$1 - f_{\rm Eve} \ge 1 - h(\varepsilon) - \lambda^2(1 + \varepsilon/(0.125 - \varepsilon))/(6F\eta_B) - 0.585\lambda/(2F_{\rm fiber}) \tag{10}$$

Nielsen 等做的数次实验 [15] 表明， $F \approx \lambda \approx \eta_B \approx 0.1$, $F_{\rm fiber} \approx 0.25$ 和 $\varepsilon \approx 0.055$. 因此 $1 - f_{\rm Eve}$ 大约为 17% .

很明显，在多种场合下，这种分析对 Eve 非常有利. 无疑人们可借助一个不太宽松而更复杂的分析方法获得一个更好的约束.

Nielsen 等推导出了 ε 的表达式为

$$\varepsilon = \frac{\eta_B F\lambda P_e^{\rm signal} + P_{\rm det}^{\rm dark}}{\eta_B F\lambda + 2P_{\rm det}^{\rm dark}} \tag{11}$$

将 (11) 式代入 (10) 式后，就可将参数 η_B 和 $P_{\text{det}}^{\text{dark}}$ 联系起来：即通过配置检测器使 η_B 更高，但无光计数率 (the dark count rate) 也相应地随之上升．依据 Nielsen 等的实验 [15]，近似有 $P_{\text{det}}^{\text{dark}} = 1.6 \cdot 10^{-3}\eta_B^{3/2}$，并将此式代入 (10) 式，导出 $(1 - f_{\text{Eve}})$ 仅依赖于参数 $\lambda, \eta_B, F, F_{\text{fiber}}$ 和 P_e^{signal} 的下界．在这些参数当中，前两个参数不相关，而且能容易地改变它们，余下的参数或多或少由设备确定，在 Nielsen 等的实验 [15] 中，$F \approx 0.1$, $F_{\text{fiber}} \approx 0.25$, $P_e^{\text{signal}} \approx 0.01$．

因此，研究 η_B 和 λ 的最佳选择是有趣的．对于这种最佳参数的选定，作者选择考虑保密能力 (secrecy capacity)，也就是由发送脉冲波数分配的最终密钥长度．最终密钥的平均长度为 $\lambda F \eta_B (1 - f_{\text{Eve}})/4$（$F$ 为线路的总传输，见文献 [15]）．Nielsen 等的研究表明，λ 的最佳选择近似为 0.1，此时可获得 η_B 的最大值 (电流检测器不允许有大于 0.25 的值出现)，亦即检测器的最大偏差电压．对于这样的选择，可获得大约 0.0002 的保密能力．此外，如果选择检测器的偏差电压，则量子效率大约为 0.1，保密能力会下降 2~3 个指标，而无光记数的减少对效率的减小不会有补偿作用．因为它减少了多个光子脉冲的攻击效应 (Eve 可截留少数一个光子的脉冲波)，所以检测器效率的增加是有用的．另一方面，如果可任意地增加检测器的效率，则会最终降低保密能力，因为无光记录的增加会需要更多的误差纠正，因此会丢失更多的位．然而，就所使用的检测器而言，在 η_B 可实现的范围内，这是不可能实现的．

虽然人们努力使基于上面安全分析的保密能力最优化，但是目前系统的实时速度仅是每秒大约 16 个安全位，这主要受制于相对低的每秒发送的脉冲波数 (平均为 80,000pulse/s)．然而，也需注意量子线速度不是 BB84[5] 方案实施的主要瓶颈，而 Internet 的连接速度 (也就是经典信道的速度) 才是 BB84 方案实施的主要瓶颈．

6 结束语

本文为量子密钥分配的无条件安全给出了一个简单的证据，这种无条件安全是指抵御最通常的窃听攻击和最常见的噪声类型的临界安全．本文的方法在任意长的距离上提供了安全的 QKD，但要求 Alice 和 Bob 要有可靠的量子计算机，这显然远远超出了现有的技术条件．然而，在展望量子加密的未来中，人们提出的所有 QKD 的安全证明所涉及到的假设都超出了现有的技术水平．令人感到欣慰的是本文所研究的技术有广阔的应用．例如，隐形传输是一种能抵御量子特洛伊马攻击的强有力的技术：因为隐形传输只是量子态的传送，由量子不可克隆定理可知，量子特洛伊马不可能复制或篡改量子态 (如窃取口令和拷贝文件)．事实上，某些结果甚至适用 Alice 和 Bob 没有量子计算机的情形．在后继的工作中，我们将研究在有窃听者的情况下，如何使用随机采样和随机隐形传输来证明一种通用的对讲 (two-party) 容错量子计算的可行性．

参 考 文 献

[1] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Los Alamitos, IEEE Computer Society Press, 1994, 124–133.

[2] C. H. Bennett, Quantum information and computation, Physics Today, 1995, 48(10), 24–30.

[3] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett., 1991, 67(6), 661–663.

[4] D. Dieks, Communication by EPR devices, Phys. Lett., 1982, 92A(6), 271–272.

[5] W. K. Wootters, W. Zurek, A single quantum cannot be done, Nature, 1982, 299(28), 802–803.

[6] 赵志，冯芒，詹明生，量子算法与量子计算实验，物理学进展，2001, 21(2), 183–215.

[5] 这是一种基于两种光轭基的四态方案.

[7] Lo H. -K., H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science, 1999, 283(5410), 2050–2056.

[8] C.H. Bennett, G. Brassard, C. Crepeau, *et al.*, Teleporting an unknown quantum state via dual classical and Einstein-Podoloky-Rosen channel, Phys. Rev. Lett., 1993, 70(13), 1895–1899.

[9] Lo H. -K., A simple proof of the unconditional security of quantum key distribution, Extended Enterprise Laboratory, HP Laboratories Bristol: Techinical Report HPL-1999-63, May, 1999.

[10] D. Deutsch, A. Ekert, R. Jozsa, C. Mauhiavello, *et al.*, Erratum: Quantum privacy amplification and the security of quantum cryptography over noise channels, Phys. Rev. Lett., 1998, 80(9), 2022–2022.

[11] Lo H. -K., H. F. Chau, Is quantum bit commitment really possible, Phys. Rev. Lett., 1997, 78(17), 3410–3413.

[12] D. Mayers, Unconditionally secure quantum bit commitment is impossible, Phys. Rev. Lett., 1997, 78(17), 3414–3417.

[13] Lo H. -K., Insecurity of quantum secure computations, Phys. Rev., 1997, 56A(2), 1154–1162.

[14] W. Dür, H. -J. Briegel, J. I. Cirac, P. Zoller, Quantum repeaters based on entanglement purification, Phys. Rev., 1999, 59A(1), 169–181.

[15] P. M. Nielsen, C. Schori, J. L. Srensen, *et al.*, Experimental quantum key distribution with proven security against realistic attacks, J. of Modern Optics, 2001, 48(8), 1491–1518(http://www.arxiv.org/pdf/quant-ph/0203118).

[16] C. H. Bennett, F. Bessette, G. Brassard, *et al.*, Experimental quantum cryptography, J. of Cryptology, 1992, 5(1), 3–28.

[17] M. Dušek, M. Jahma, N. Lütkenhaus, Unambiguous state discrimination in quantum cryptography with weak coherent states, Los Alamos preprint archive quant-ph/9910106 v2, 1999.

[18] C. H. Bennett, G. Brassard, C. Crépeau, *et al.*, Generalized privacy amplification, IEEE Trans. on Information Theory, 1995, IT-41(6), 1915–1923.

QUANTUM KEY DISTRIBUTION AND ITS UNCONDITIONAL SECURITY PROOF

Liu Chuancai

(*Department of Computer, Fuzhou University, Fuzhou* 350002, *China*)

Abstract Quantum cryptography is best known for key distribution. However, previous proposed proofs of security of Quantum Key Distribution (QKD) contain various technical subtleties. In this paper, a conceptually simpler proof of security of QKD is proposed. Also, the error rate of a teleportation channel has no concern with the signal being transmitted. This is because the non-trivial error patterns are permuted under teleportation. This inherent fact is combined with the recently proposed quantum to classical reduction theorem. In the argument, supposed Alice and Bob to have fault-tolerant quantum computer, the result shows that QKD can be made unconditionally secure over arbitrarily long distances even against the most general type of eavesdropping attacks and in the presence of all types of noises.

Key words Quantum cryptography, Quantum key distribution, Teleportation channel, Eavesdropping

刘传才： 男，1963 年生，副教授，主要研究方向为模式识别与智能系统、网络信息安全.