中国科学 : 物理学 力学 天文学 2012 年 第 42 卷 第 11 期 : 1237 – 1255
SCIENTIA SINICA Physica, Mechanica & Astronomica phys.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

中国科学技术大学物理学院专刊 · 论文

量子密码安全性研究

李宏伟[①②③], 陈巍[①*], 黄靖正[①], 姚尧[①], 刘东[①], 李芳毅[①], 王双[①*], 银振强[①*], 何德勇[①], 周政[①], 李玉虎[①②], 俞能海[②], 韩正甫[①*]

① 中国科学技术大学中科院量子信息重点实验室, 合肥 230026;
② 中国科学技术大学电子工程与信息科学系, 合肥 230026;
③ 信息工程大学电子技术学院, 郑州 450004
* 联系人: 陈巍, E-mail: kooky@mail.ustc.edu.cn; 王双, E-mail: wshuang@ustc.edu.cn; 银振强, E-mail: yinzheqi@mail.ustc.edu.cn; 韩正甫, E-mail: zfhan@ustc.edu.cn

收稿日期: 2012-09-04; 接受日期: 2012-09-20; 网络出版日期: 2012-10-25
国家自然科学基金资助项目 (批准号: 61101137, 61201239, 61205118)

摘要 本文介绍了量子密码协议安全性证明的三种模型, 并据此针对光源、有源光学调制器件、无源光学调制器件和探测器的非理想特性, 分别度量了实际量子密钥分配系统和理想量子密钥分配协议之间的差异, 并针对各种实际器件的非理想性, 分析了实际量子密钥分配系统安全性存在的问题以及可能存在的攻击方案. 在综合介绍国内外量子密钥分配安全性相关工作进展的同时, 着重对当前的主流设备无关及半设备无关量子密码方案进行了分析阐述.

关键词 量子密码, 协议安全性, 非理想器件, 系统安全性

PACS: 03.67.Dd, 03.67.Hk, 03.65.Ud, 89.70.+c

doi: 10.1360/132012-761

1 引言

保密通信的安全性关系到国家安全, 是任何国家、政府、部门、行业以及个人都高度重视的核心问题. 密码技术是信息安全的核心保障, 现用的经典密码体制主要基于对称密钥密码和公钥密码. 20 世纪 80 年代以来量子计算机和量子算法概念的提出和研究的迅速深化, 对经典密码体制的安全性提出了巨大的挑战. Shannon[1] 证明了 “一次一密 (One-time Pad)” 密码体制在理论上可以达到无条件安全, 前提是合法通信双方可以通过安全的信道, 共享与明文等长、且只使用一次的真随机密钥. 量子密码狭义上也被称为量子密钥分配, 可以为远程通信双方提供无条件安全的密钥协商手段. 其安全性基于量子力学的基本原理 (未知量子态的不可克隆、量子态测量塌缩、量子不确定原理等), 不依赖第三方窃听者的计算能力和存储能力, 因而可以达到密码学意义上的无条件安全. 量子密码技术是量子信息领域发展最为成熟的技术, 结合量子密码技术和 “一次一密” 密码体制可以实现无条件安全的保密通信体制. 经过大量研究者近 30 年的不懈努力, 目前国内外已有多款量子密码商业产品问世

引用格式: 李宏伟, 陈巍, 黄靖正, 等. 量子密码安全性研究. 中国科学: 物理学 力学 天文学, 2012, 42: 1237–1255
Li H W, Chen W, Huang J Z, et al. Security of quantum key distribution (in Chinese). Sci Sin-Phys Mech Astron, 2012, 42: 1237–1255, doi: 10.1360/132012-761

(http://www.idquantique.com/,http://www.qasky.com/), 量子密码技术已经初步走上了产业化之路. 目前, 商用的量子密码产品大多基于 BB84 [2] 类量子密钥分配协议, 此类协议的安全性研究也是最为广泛和深入的. 本文将重点对 BB84 类协议和实际系统的安全性分析进行探讨和阐述.

本文首先介绍了用于分析 BB84 类协议理论安全性的三种基础模型: 即基于纠缠提纯、量子信息论和不确定关系的模型. 随后考虑光源、有源和无源光学器件、以及单光子探测器等部件的非理想特性, 分析了实际量子密钥分配系统的安全性, 并对国内外学者基于器件的非理想特性构造的攻击模型进行了总结. 最后, 对设备无关量子密码方案 (DI-QKD) 和半设备无关量子密码方案 (Semi DI-QKD) 的原理、特点和研究进展进行了介绍.

2 BB84 类协议

首个量子密钥分配 (QKD) 协议是由 Bennett 和 Brassard [2] 在 1984 年提出的 BB84 协议, 该协议与六态协议 [3] 等基于单量子比特的密钥分配协议一起被称为 BB84 类协议. 虽然这些方案量子态编解码的具体物理实现方式有所差异, 但对此类协议的安全性证明均可等效于基于纠缠协议的安全性证明. 本文进行协议描述时, 以 Alice 代表合法通信双方的发送方, Bob 代表接收方, Eve 是通信信道中的窃听者. 进行安全性分析的前提是假设 Eve 拥有无穷的计算能力和存储能力, 甚至拥有量子计算机和量子存储器.

量子密钥分配的步骤可以分为量子部分和经典部分.

量子部分:

初始密钥的生成:

利用量子信道, Alice 随机选择经典二进制比特串 $x_1,x_2,\cdots,x_n$ $(x_i\in\{0,1\},i=1,\cdots,n)$ 并发送与之对应的编码量子态 $(|\varphi_{j_1}^{x_1}\rangle,\cdots,|\varphi_{j_n}^{x_n}\rangle)$ 给 Bob, 其中 $j_1,j_2,\cdots,j_n$ 是 Alice 选择的基矢. Bob 随机的选取测量基 $(k_i\in\{0,1\},i=1,\cdots,n)$ 对其收到的量子态进行测量, 得到一组经典二进制比特 $y_1,y_2,\cdots,y_n$.

经典部分:

(1) 初始密钥的筛选

Alice 和 Bob 分别公布本次通信选取的 j_i 和 k_i, 双方约定仅保留相同基下的测量结果, 而丢弃其余测量结果, 此时 Alice 和 Bob 保留下的对应比特分别记为 $x_1,x_2,\cdots,x_{n'}$ 和 $y_1,y_2,\cdots,y_{n'}$, 其中 $(n'<n)$.

(2) 参数估计

Alice 和 Bob 随机选择一部分筛选后的密钥公布出来, 若比对得到的比特误码率高于设定的安全界限, 则放弃本次 QKD 过程产生的密钥. 若低于设定的安全界限, 则 Alice 和 Bob 保留剩余的比特, 分别记为 $x_1,x_2,\cdots,x_l$ 和 $y_1,y_2,\cdots,y_l$, 其中 $(l<n')$.

(3) 纠错

Alice 发送纠错信息 w 给 Bob, Bob 利用 w 对 $y_1,y_2,\cdots,y_l$ 纠错, 并得到与 Alice 相同的比特串 $x_1,x_2,\cdots,x_l$.

(4) 保密放大

为了使窃听者得到的信息可以达到指数任意小量, Alice 和 Bob 随机共同选择一个普适的 (Universal) 哈希函数 F, 分别计算各自的哈希函数值 $F(x_1,x_2,\cdots,x_l)$, 并将其作为最终的安全密钥.

本文采用 Renner 等人给出的量子密钥分配的无条件安全性定义, 其核心内容如下:

QKD 的安全性定义 [4–6] 经过上述 QKD 过程后, Alice, Bob 和 Eve 的状态可以由下述密度矩阵描述:

$$\rho_{XYE}=\sum_{x,y}P_{XY}(x,y)P_{|x\rangle}\otimes P_{|y\rangle}\otimes\rho_E^{x,y}, \tag{1}$$

其中 $|x\rangle$ 和 $|y\rangle$ 分别为一组正交向量, 用来表征 Alice 和 Bob 的经典密钥比特, P 是投影测量算子, $\rho_E^{x,y}$ 为 Eve 的量子态, Alice 和 Bob 的经典原始密钥比特分别为 x 和 y. 当 Alice 和 Bob 的最终安全密钥比特 (S_A,S_B) 满足以下条件, 则称 (S_A,S_B) 是 ε 安全的,

$$\delta(\rho_{S_AS_BE},\rho_{SS}\otimes\rho_E)\leqslant\varepsilon, \tag{2}$$

其中 $\rho_{SS}=\sum_{s\in S}\frac{1}{|S|}P_S\otimes P_S$ 是理想密钥 (理想密钥是指 Alice 和 Bob 的经典信息与 Eve 的量子态之间没有任何关联, 即 Eve 不能获得密钥的任何信息), δ 为两个态间的迹距离. 在上述定义中密钥 (S_A,S_B) 和理想密钥相同的概率至少为 $1-\varepsilon$, 也就是说, 可以至少以 $1-\varepsilon$ 的概率来确保密钥 (S_A,S_B) 与理想密钥相同, 相应的密钥的安全强度定义为 $1-\varepsilon$.

但是这里需要强调的是无条件安全性的定义并不等价于绝对安全性的定义, 事实上绝对安全性的密码体制也是不存在的. 无条件安全的 QKD 存在着以下特定的限制条件:

1) 可信任的物理位置, 对外界没有不必要的信息泄露. 窃听者 Eve 不能侵入 Alice 和 Bob 的设备, 从而直接获得密钥信息或者测量基的选择. 但是, 这在实际系统中是很难实现的, 在下一节的实际系统安全性分析中会具体的讨论.

2) Alice 和 Bob 必须拥有理想的随机数发生器 (可能是量子随机数发生器), 因此双方可以随机的选择量子态的制备和测量基的选择.

3) 可信任的量子设备 (量子态制备和测量设备)、经典设备 (例如存器和计算设备)、存储和处理量子仪器所产生的经典数据.

4) 经典信道必须是可信认证的, 可以利用经典无条件安全的认证方案来保证.

5) 窃听者的攻击能力限制在量子力学的范围内.

上述安全性的定义最主要的性质是其满足可组合性, 该性质满足了量子密钥在实际应用中的安全性. 具体来说如果量子密钥的安全性为 ε, 而实际应用过程的安全性为 ε'(在理想密钥下), 那么该应用结合量子密钥后的整体安全性为 $\varepsilon+\varepsilon'$.

值得注意的是, 在 Renner 等人的上述定义以及其它安全性分析的文献中, 普遍都认为经典信道的身份认证是无条件安全的. 事实上, 经典信道只有经过无条件安全的明文和身份认证才可以被认为是安全的. 即, 在上述量子密钥分配过程的经典部分, 还必须增加认证这一步骤.

(5) 认证 [7]

上述步骤 (1)–(4) 均需发送经典信息, 由于 Eve 可以窃听信道中传输的所有信息, Alice 和 Bob 需要确认发送的经典信息没有被 Eve 欺骗或篡改. 为此, Alice 需发送经典信息 m 和其认证码 $h_s(m)$ 给 Bob(其中密钥 s 是合法通信双方事先共享的), Bob 根据共享密钥 s 对应的哈希函数对接收到的明文 m' 进行处理, 产生认证码 $h_s(m')$, 若与接收到的认证码相同则认证成功, 否则认证失败. 认证完成后密钥即被丢弃, 不再重复使用. 若 Alice 和 Bob 对交互的所有经典信息认证成功则此次 QKD 成功, 否则重新进行以上步骤.

身份认证是密码学重要的一方面, 其主要目的是防止窃听者的中间人攻击 (Man-in-the-middle Attack). 量子密钥分配协议认证的出发点是利用经典无条件安全的身份认证协议来认证经典信道的安全性, 其中无条件安全的身份认证协议是指即使窃听者拥有无穷的计算和存储能力, 其仍然得不到认证码中密钥的任何信息. 无条件安全的身份认证常常采用 Wegman-Carter 协议 [7], 该协议的基础是 p-almost Strongly Universal 2 哈希函数.

结合上述描述, 图 1 中给出了量子密钥分配过程中的流程图.

3 理想 BB84 类协议安全性

理想 BB84 类协议是指量子态的制备、测量和

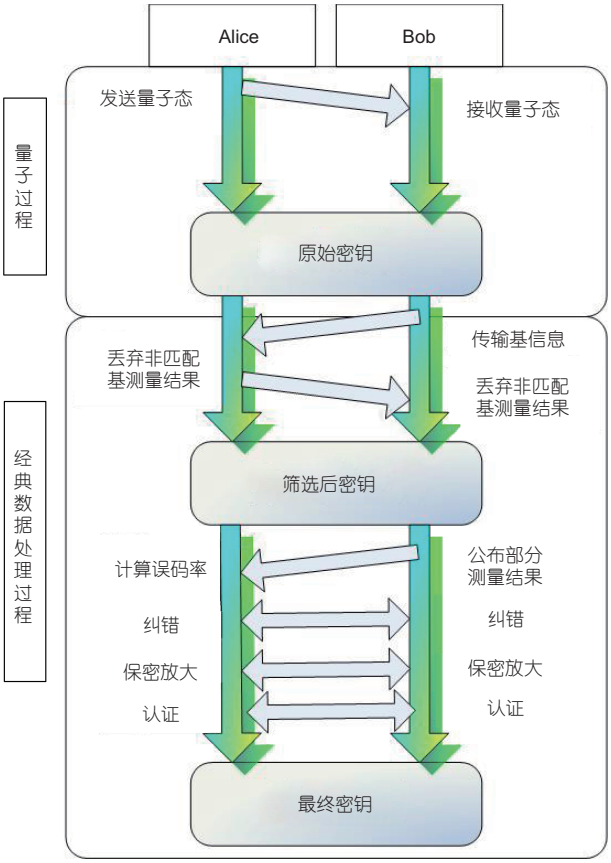

图 1 (网络版彩图) 量子密钥分配协议流程图

Figure 1 (Color online) Quantum key distribution protocol.

探测过程完全符合协议要求, 是理想无误差的, 并且合法通信双方的安全区不泄露额外的态制备和态测量信息. QKD 协议的理论无条件安全性证明最初由 Lo 和 Chau [8] 给出的. 其分析过程要求合法通信双方拥有量子计算机, 与 QKD 的实际应用条件仍有很大的距离. 随后 Shor 和 Preskill [9] 证明了基于态制备和态测量的量子密钥分配协议的安全性等价于基于纠缠提纯协议的安全性. 结合 CSS 纠错码和纠缠提纯技术 (Entanglement Distillation and Purification Technology), 基于现有的纠错技术便可以证明量子密钥分配协议的安全性. 但是, 纠缠提纯技术并不是证明量子密钥分配协议无条件安全的充分必要条件. Renner 等人 [4–6] 利用信息论的方法证明了量子密钥分配协议的无条件安全性, 在其分析过程中没有用到纠缠提纯, 而是直接从信息论的角度出发, 给出窃听者所能获得信息量的上界. 这一过程还证明了对量子密钥分配协议产生的密钥比特以特定概率进行增加噪声的后处理, 可以得到更高的密钥比特. Horodecki 等人 [10] 证明了基于私密纠缠 (Private-entanglement) 的量子密钥分配协议在没有纠缠提纯的情况下依然可以产生安全的密钥比特. Renes 和 Smith [11] 证明了在一些量子密钥分配协议中增加经典噪声可以提高密钥率是因为噪声会增加纠缠提纯协议中的比特误码率, 而相对于窃听者来说, 则使其失去了对部分相位误码率的控制, 即合法通信双方和窃听者获得的信息量都会减小, 但是窃听者的信息量减小的更快.

上述所有的安全性分析的基础是理想的量子密钥分配协议, 并没有考虑到实际系统的非理想性. 实现实际系统所使用的各种器件, 可能存在不符合协议要求的非理想因素. 最早对实际系统安全性进行系统性分析的结果由 Gottesman 等人 [12] 给出, 即著名的 GLLP 公式. 其核心思想是量子密钥分配系统中只有单光子的计数结果才可以生成最终安全的量子密钥比特. 应用 GLLP 公式和诱骗态思想 [13], Lo 等人 [14] 和 Wang [15] 分别给出了实际系统中应用弱相干态光源的安全密钥率计算公式, 使实际量子密钥分配的最大安全距离得到显著的提高.

如果量子密钥分配系统的非理想性是基相关的 (Basis-dependent), 即同一组基下的态制备和测量具有相同的非理想特性, 则可以认为该非理想性是由窃听者 Eve 引入的, 也就是相当于窃听者在量子信道中附加了新的酉变换, 该酉变换可以表征基相关的非理想性. 但是大部分的非理想性并不是基相关的 [16,17], 因此在安全性分析中不能简单的认为是由窃听者 Eve 引入的. 例如在偏振量子密钥分配系统中应用的波片可能是不准确的, 相位量子密钥分配系统中的调相电压是非精确的等. 事实上, 如果这些非理想性不能表征为窃听者的酉变换或操作, 则现有的密钥生成率公式 (GLLP 等) 是不适用的.

3.1 基于纠缠提纯思想的 BB84 类协议安全性 [9,17]

在研究理想量子密钥分配协议的安全性时, 以偏振编码量子密钥分配系统作为研究对象可以不失一般性, 首先对态制备和态测量协议进行介绍. Alice 将经典比特 0 随机编码为量子态 $|0^{\rm o}\rangle$ 或 $|45^{\rm o}\rangle$, 将经典比特 1 随机编码为量子态 $|90^{\rm o}\rangle$ 或 $|-45^{\rm o}\rangle$. Bob 则随机选择水平垂直基 $\{|0^{\rm o}\rangle,|90^{\rm o}\rangle\}$ 或对角基 $\{|45^{\rm o}\rangle,|-45^{\rm o}\rangle\}$ 对接收到的量子态进行测量.

依据 Shor 和 Preskill [9] 的安全性证明思想, 基于态制备和态测量的量子密钥分配协议与基于纠缠提纯协议的在安全性上等价, 协议过程如图 2 所示.

Alice 首先制备最大纠缠态 $|\phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, Alice 随机的对第二个粒子进行 Hadamard 操作, 然后将该粒子发送给 Bob. 若 Bob 接收到了相应

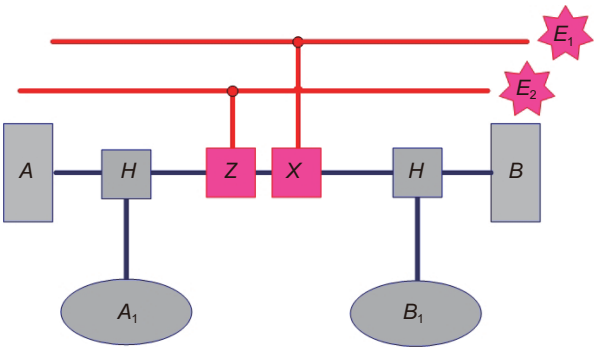

图 2 (网络版彩图) 基于纠缠提纯的量子密钥分配协议

模型考虑的是 Pauli 信道, Z 是窃听者引入相位错误的操作, X 是窃听者引入比特错误的操作, A_1 是 Alice 端的辅助粒子, B_1 是 Bob 端的辅助粒子

Figure 2 (Color online) Entanglement-based protocol with Pauli channel and eavesdropper Eve. Z is Eve's phase error operation, X is Eve's bit error operation. A_1 is part of Alice's system, B_1 is part of Bob's system.

的量子态则予以公布, 并随机的对该量子态进行Hadamard操作. 安全性分析中一般认为最普适的信道是Pauli信道, 这是因为Alice制备了2维的量子态, 所有的错误可以归结为比特错误矩阵 X, 相位错误矩阵 Z 和比特相位错误矩阵 Y, 他们构造了2维希尔伯特空间的一组基. 考虑到窃听者在Pauli信道中的攻击, Alice, Bob 和 Eve 的量子态可以描述为下述形式:

$$\sum_{u,v,i,j}\sqrt{P_{uv}Q_{ij}}(I_A\bigotimes H^i_{B_1}X^u_{E_1}Z^v_{E_2}H^j_{A_1}|\phi_1\rangle|u\rangle_{E_1}|v\rangle_{E_2}\\ |i\rangle_{B_1}|j\rangle_{A_1}), \tag{3}$$

其中 $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ 是理想的 Hadamard 算子, 在量子密钥分配协议中可以表征不同基之间的转换, 例如: 若开始制备的是水平垂直基下的态, 经过 Hadmard 操作后则变为对角基下的态. $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 是 X 算子, 其表征窃听者 Eve 引入的比特误码, $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ 是 Z 算子, 用于表征窃听者引入的相位误码. 相应的 XZ 表征窃听者在Pauli信道中引入的相位比特误码. P_{uv}, $u,v\in\{0,1\}$ 是窃听者引入 X^uZ^v 算子的概率, 满足以下的要求:

$$\sum_{u,v}P_{uv}=1. \tag{4}$$

Q_{ij}, $i,j\in\{0,1\}$ 意味着 Alice 引入 H^i 矩阵, 同时 Bob 引入 H^j 矩阵的概率. 因为在理想协议中合法通信双方随机的选择测量基, 则上述概率应满足 $Q_{ij}=\frac{1}{4}$.

经过对基的步骤后, $i\neq j$ 的情况将会被丢弃, 对 A_1, B_1 和 Eve 的量子系统求迹, 得到 Alice 和 Bob 的密度矩阵为

$$\rho_{AB}=\sum_{u,v}P_{uv}(\tfrac{1}{2}I_A\otimes X^u_{E_1}Z^v_{E_2}|\phi_1\rangle\langle\phi_1|Z^v_{E_2}X^u_{E_1}\otimes I_A\\ +\tfrac{1}{2}I_A\otimes H_{B_1}X^u_{E_1}Z^v_{E_2}H_{A_1}|\phi_1\rangle\langle\phi_1|H_{A_1}Z^v_{E_2}X^u_{E_1}H_{B_1})\otimes I_A. \tag{5}$$

上述分析中提到Pauli信道中存在比特错误和相位错误, 所有的误码均被认为是由窃听者 Eve 引入的, 经过量子信道后, 相应的量子态可以转变为下述 4 种情况:

$$\begin{aligned}|\phi_1\rangle&=\frac{1}{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB}),\\ |\phi_2\rangle&=\frac{1}{\sqrt{2}}(|01\rangle_{AB}+|10\rangle_{AB}),\\ |\phi_3\rangle&=\frac{1}{\sqrt{2}}(|00\rangle_{AB}-|11\rangle_{AB}),\\ |\phi_4\rangle&=\frac{1}{\sqrt{2}}(|01\rangle_{AB}-|10\rangle_{AB}).\end{aligned} \tag{6}$$

如果最初共享的量子态 $|\phi_1\rangle$ 经过量子信道后转变为 Bell 态 $|\phi_1\rangle$ 则量子信道中不存在错误, 但是如果最初共享的量子态 $|\phi_1\rangle$ 经过量子信道后转变为 Bell 态 $|\phi_2\rangle$, $|\phi_3\rangle$ 和 $|\phi_4\rangle$, 则窃听者 Eve 分别在信道中引入了比特错误、相位错误和比特相位错误. 因此最终的比特误码和相位误码可以由下述公式给出:

$$\begin{aligned}e_{\text{bit}}&=\langle\phi_2|\rho_{AB}|\phi_2\rangle+\langle\phi_4|\rho_{AB}|\phi_4\rangle,\\ e_{\text{phase}}&=\langle\phi_3|\rho_{AB}|\phi_3\rangle+\langle\phi_4|\rho_{AB}|\phi_4\rangle.\end{aligned} \tag{7}$$

在量子密钥分配的纠缠提纯过程中, 合法通信双发必须明确量子态由信道扰动引入的比特误码和相位误码, 才能纠正误码并提取最大纠缠态. 在量子密钥分配协议中, 可以通过接收端经典操作中的参数估计得到测量结果的比特误码. QKD 安全性分析最大困难是如何估算协议过程中的相位误码, 结合方程 (5)–(7) 可以得到相位误码的估计结果如下所示:

$$e_{\text{phase}}-e_{\text{bit}}=\langle\phi_2|\rho_{AB}|\phi_2\rangle-\langle\phi_3|\rho_{AB}|\phi_3\rangle=0. \tag{8}$$

因此, 在理想协议中, 可以通过比特误码来精确估计相位误码, 最终的安全密钥率公式为

$$R=1-h(e_{\text{phase}})-h(e_{\text{bit}})=1-2h(e_{\text{bit}}). \tag{9}$$

其中 $h(x)=-x\log_2x-(1-x)\log_2(1-x)$ 是香农熵函数, 而此时允许引入量子信道的最大比特误码率为0.11. 图 3 给出了最终安全密钥率与误码率之间的关系, 需要指出的是此处安全性分析的对象是理想的纠错和保密放大, 但实际系统往往难以满足理想条件, 通信双方可能泄露给窃听者更多的信息量.

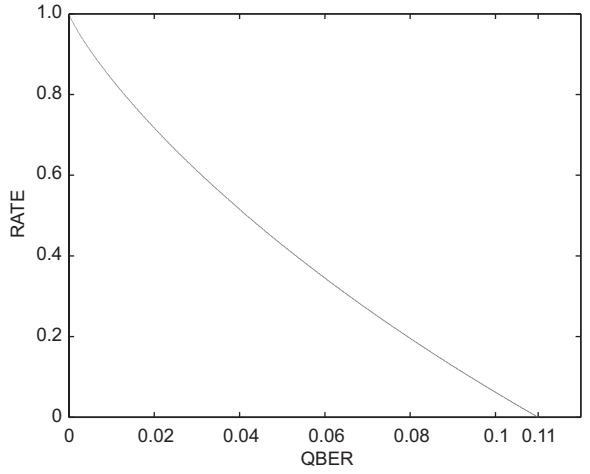

图 3　密钥率 (RATE) 与比特误码率 (QBER) 之间的关系

Figure 3　The relationship between secret key rate and quantum bite error rate.

3.2　基于量子信息论的 BB84 类协议安全性 [4–6]

定理　基于信息论的最终密钥率公式为

$$R = \min_{\sigma_{AB}\in \mathrm{T}} S(X|E) - H(X|Y), \tag{10}$$

其中 T 是所有希尔伯特空间 $H_A \otimes H_B$ 内满足要求的密度算子 σ_{AB} 的合集. $S(X|E)$ 是窃听者的辅助粒子 E 对于 Alice 端测量结果 X 的不确定度, 因为窃听者可以存储其量子态并根据双方的通信结果选取最优的测量, 所以其不确定度需要利用冯诺依曼熵来度量. 而 $H(X|Y)$ 是接收端 Bob 的测量结果 Y 对于 Alice 端测量结果 X 的不确定度, 考虑到双方此时经过测量已经得到了经典二进制比特串, 因此该不确定度只需要经典香农熵来度量.

与基于纠缠提纯协议的安全性分析类似, 假定 Alice 事先制备了最大纠缠态, 并发送其中一个粒子给 Bob, 在 Alice 和 Bob 对量子态进行测量前, 整个系统可以由下述量子态描述:

$$|\psi\rangle_{ABE} = \sum_{i=1}^{4} \sqrt{\lambda_i}|\varphi_i\rangle_{AB} \otimes |v_i\rangle_E, \tag{11}$$

其中 $\sum_{i=1}^{4}\lambda_i = 1$, Alice 和 Bob 的系统经过量子信道中窃听者的干扰后, 可以用 Bell 态公式 (6) 表示演化结果.

窃听者 Eve 对应的量子态可以分别表示为如下形式:

$$\begin{aligned}
|\theta^{00}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_1}|v_1\rangle + \sqrt{\lambda_2}|v_2\rangle),\\
|\theta^{11}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_1}|v_1\rangle - \sqrt{\lambda_2}|v_2\rangle),\\
|\theta^{01}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_3}|v_3\rangle + \sqrt{\lambda_4}|v_4\rangle),\\
|\theta^{10}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_3}|v_3\rangle - \sqrt{\lambda_4}|v_4\rangle),
\end{aligned} \tag{12}$$

其中 $|\theta^{xy}\rangle$ 是当 Alice 和 Bob 的测量结果分别为 x,y 时, 窃听者所能获得的量子态. 进一步考虑到合法通信双方所有的测量结果, 可以给出 Alice 和 Bob 测量后整个系统的密度矩阵形式为

$$\sigma_{XYE} = \textstyle\sum_{x,y}|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes |\theta^{xy}\rangle\langle\theta^{xy}|, \tag{13}$$

对 Bob 的系统求迹, 得到 Alice 和 Eve 系统的密度矩阵形式如下:

$$\begin{aligned}
&\sigma_{XE}\\
&= \mathrm{tr}_B(\sigma_{XYE})\\
&= \sum_{x,y}|x\rangle\langle x| \otimes |\theta^{xy}\rangle\langle\theta^{xy}|\\
&= \frac{1}{2}\begin{pmatrix} \lambda_1 & \sqrt{\lambda_1\lambda_2} & 0 & 0\\ \sqrt{\lambda_1\lambda_2} & \lambda_2 & 0 & 0\\ 0 & 0 & \lambda_3 & \sqrt{\lambda_3\lambda_4}\\ 0 & 0 & \sqrt{\lambda_3\lambda_4} & \lambda_4 \end{pmatrix} \otimes |0\rangle\langle 0|\\
&+ \frac{1}{2}\begin{pmatrix} \lambda_1 & -\sqrt{\lambda_1\lambda_2} & 0 & 0\\ -\sqrt{\lambda_1\lambda_2} & \lambda_2 & 0 & 0\\ 0 & 0 & \lambda_3 & -\sqrt{\lambda_3\lambda_4}\\ 0 & 0 & -\sqrt{\lambda_3\lambda_4} & \lambda_4 \end{pmatrix}\\
&\otimes |1\rangle\langle 1|,
\end{aligned} \tag{14}$$

该密度矩阵对应的冯诺依曼熵为

$$\begin{aligned}
&S(\sigma_{XE})\\
&= -(\lambda_1+\lambda_2)\log_2\left(\frac{\lambda_1+\lambda_2}{2}\right) - (\lambda_3+\lambda_4)\log_2\left(\frac{\lambda_3+\lambda_4}{2}\right)\\
&= 1 + h(\lambda_1+\lambda_2).
\end{aligned} \tag{15}$$

在上述分析的基础上, 对 Alice 和 Bob 的系统求迹得到 Eve 的密度矩阵为

$$\begin{aligned}
&\sigma_E \\
&= \mathrm{tr}_{AB}(\sigma_{XYE}) \\
&= \sum_{x,y} |x\rangle\langle x| \otimes |\theta^{xy}\rangle\langle\theta^{xy}| \\
&= \frac{1}{2}\begin{pmatrix} \lambda_1 & \sqrt{\lambda_1\lambda_2} & 0 & 0 \\ \sqrt{\lambda_1\lambda_2} & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & \sqrt{\lambda_3\lambda_4} \\ 0 & 0 & \sqrt{\lambda_3\lambda_4} & \lambda_4 \end{pmatrix} \\
&+ \frac{1}{2}\begin{pmatrix} \lambda_1 & -\sqrt{\lambda_1\lambda_2} & 0 & 0 \\ -\sqrt{\lambda_1\lambda_2} & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & -\sqrt{\lambda_3\lambda_4} \\ 0 & 0 & -\sqrt{\lambda_3\lambda_4} & \lambda_4 \end{pmatrix},
\end{aligned} \tag{16}$$

该密度矩阵对应的冯诺依曼熵为

$$\begin{aligned}
S(\sigma_E) =& (\lambda_1+\lambda_2)h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right) + (\lambda_3+\lambda_4)h\left(\frac{\lambda_3}{\lambda_3+\lambda_4}\right) \\
&+ h(\lambda_1+\lambda_2).
\end{aligned} \tag{17}$$

不失一般性, 可以假定 Alice 和 Bob 的测量基分别为 $\{|0\rangle|1\rangle\}$, 则 Alice 和 Bob 之间的不确定度可以由经典香农熵来计算得到

$$H(X|Y) = h(\lambda_1+\lambda_2), \tag{18}$$

此时, 最终的密钥率公式为

$$\begin{aligned}
R &\geqslant \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} S(X|E) - H(X|Y) \\
&= \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} S(\sigma_{XE}) - S(\sigma_E) - H(X|Y) \\
&= \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} 1 - (\lambda_1+\lambda_2)h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right) \\
&\quad - (\lambda_3+\lambda_4)h\left(\frac{\lambda_3}{\lambda_3+\lambda_4}\right) - h(\lambda_1+\lambda_2),
\end{aligned} \tag{19}$$

其中, 上述不等式中的相关系数满足下述条件:

$$\begin{aligned}
\lambda_1 &= 1-2Q+\lambda_4, \\
\lambda_2 &= Q-\lambda_4, \\
\lambda_3 &= Q-\lambda_4,
\end{aligned} \tag{20}$$

Q 为比特误码率, 最终密钥率公式为

$$\begin{aligned}
R =& \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} 1 - (1-Q)h\left(\frac{1-2Q+\lambda_4}{1-Q}\right) \\
&- Qh\left(\frac{Q-\lambda_4}{Q}\right) - h(Q),
\end{aligned} \tag{21}$$

其中 $0 \leqslant \lambda_4 \leqslant Q$, 在此基础上对上述密钥率公式求极小值, 可以得到 λ_4 需要满足的条件为 $\lambda_4 = Q^2$, 代入上述密钥率公式可以得到

$$R = 1 - 2h(Q), \tag{22}$$

从而可以得到与纠缠提纯方案相同的密钥率公式.

此安全性分析的过程不依赖于纠缠提纯方案, 估计窃听者的信息量与信道中的相位错误无关. 只是从信息论的角度证明了窃听者能获得的最大信息量. 在此安全性分析的基础上, Renner 等人给出了经典噪声后处理对量子密钥分配安全性的影响, 直观上增加经典比特信息的噪声会引入更多的误码, 相应的合法通信双方会产生更少的密钥比特. 事实上, 随机的增加经典噪声可能会导致合法通信双方最终密钥率的提升, 从纠缠提纯的角度窃听者所能的信息量是由量子态的比特误码和相位误码所引入的, 而增加经典噪声的结果是使得窃听者通过比特误码获得的信息量增加而通过相位误码获得的信息量减小. 这是因为在合法通信双方内部所引入的相位误码是窃听者所不能控制的, 这个观点对于实际量子密钥分配系统的安全性分析有着重要的意义. 而从信息论的角度出发增加经典噪声的后果是在合法通信双方信息量减小的同时, 窃听者的信息量也会减小, 当窃听者减小的信息量更多时合法通信双方可以生成更多的密钥比特.

如果考虑到 Bob 对其经典比特随机以概率 p 进行随机翻转, 此时对 Bob 的系统求迹, 得到 Alice 和 Eve 的系统如下所示:

$$\begin{aligned}
&\sigma_{UE} \\
&= \frac{1}{2}\begin{pmatrix} \lambda_1 & \sqrt{\lambda_1\lambda_2} & 0 & 0 \\ \sqrt{\lambda_1\lambda_2} & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & \sqrt{\lambda_3\lambda_4} \\ 0 & 0 & \sqrt{\lambda_3\lambda_4} & \lambda_4 \end{pmatrix}
\end{aligned}$$

$$\otimes((1-p)|0\rangle\langle 0|+p|1\rangle\langle 1|)+$$
$$\frac{1}{2}\begin{pmatrix}\lambda_1 & -\sqrt{\lambda_1\lambda_2} & 0 & 0\\ -\sqrt{\lambda_1\lambda_2} & \lambda_2 & 0 & 0\\ 0 & 0 & \lambda_3 & -\sqrt{\lambda_3\lambda_4}\\ 0 & 0 & -\sqrt{\lambda_3\lambda_4} & \lambda_4\end{pmatrix}$$
$$\otimes((1-p)|1\rangle\langle 1|+p|0\rangle\langle 0|), \quad (23)$$

该密度矩阵对应的冯诺依曼熵为

$$S(\sigma_{UE}) = 1+h(\lambda_1+\lambda_2)$$
$$+(\lambda_1+\lambda_2)h\left[\frac{1}{2}+\sqrt{\frac{1}{4}-4p(1-p)\frac{\lambda_1\lambda_2}{(\lambda_1+\lambda_2)^2}}\right]$$
$$+(\lambda_3+\lambda_4)h\left[\frac{1}{2}+\sqrt{\frac{1}{4}-4p(1-p)\frac{\lambda_3\lambda_4}{(\lambda_3+\lambda_4)^2}}\right], \quad (24)$$

若 Bob 不对经典测量结果随机注入噪声, 即 $p=0$. 则上述冯诺依曼熵进一步的退化为

$$S(\sigma_{UE}) \to 1+h(\lambda_1+\lambda_2) = S(\sigma_{XE}). \quad (25)$$

从上述公式可以看出, 若 Bob 随机注入噪声则整个系统的不确定程度增加, 而由下面的推导可以看到窃听者自身的量子态没有变化, 相应的可以分析得到窃听者对随机注入噪声后的经典密钥比特的不确定性增加. 在上述分析的基础上, 对窃听者 Eve 的系统计算相应的冯诺依曼熵为

$$S(\sigma_E) = (\lambda_1+\lambda_2)h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)+(\lambda_3+\lambda_4)h\left(\frac{\lambda_3}{\lambda_3+\lambda_4}\right)$$
$$+h(\lambda_1+\lambda_2). \quad (26)$$

Alice 和 Bob 之间的系统的比特误码率由 $\lambda_1+\lambda_2$ 增加至 $(\lambda_1+\lambda_2)+(1-p)(1-\lambda_1-\lambda_2)$, 相应的系统的不确定度可以有下述香农熵来描述:

$$H(X|Y) = h[p(\lambda_1+\lambda_2)+(1-p)(1-\lambda_1-\lambda_2)]. \quad (27)$$

与无噪声注入的情况进行类似的分析, 最终的密钥率公式为

$$R \geqslant \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} 1+h(\lambda_1+\lambda_2)$$
$$+(\lambda_1+\lambda_2)h\left[\frac{1}{2}+\sqrt{\frac{1}{4}-4p(1-p)\frac{\lambda_1\lambda_2}{(\lambda_1+\lambda_2)^2}}\right]$$
$$+(\lambda_3+\lambda_4)h\left[\frac{1}{2}+\sqrt{\frac{1}{4}-4p(1-p)\frac{\lambda_3\lambda_4}{(\lambda_3+\lambda_4)^2}}\right]$$
$$-\left[(\lambda_1+\lambda_2)h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)+(\lambda_3+\lambda_4)h\left(\frac{\lambda_3}{\lambda_3+\lambda_4}\right)\right.$$
$$\left.+h(\lambda_1+\lambda_2)\right]$$
$$-h[p(\lambda_1+\lambda_2)+(1-p)(1-\lambda_1-\lambda_2)], \quad (28)$$

对上述密钥率公式进行数值计算可以得到最终的密钥率公式, 从下图的密钥率公式与误码率的关系可以看到: Bob 对接收方的经典比特注入噪声可以使最大误码率容限从 0.11 提高至 0.124, 图 4 描述了在注入噪声的情况下误码率与密钥率的关系.

3.3 基于不确定关系的 BB84 类协议安全性

基于不确定关系证明 BB84 类协议安全性的基础是非对易的量子测量不可能准确的预知不同测量基下的测量结果, Tomamichel 和 Renner [18] 利用不确定关系证明了 BB84 协议的安全性. 该安全性分析适用于窃听者拥有量子存储的情况, 其具体过程如下.

考虑量子系统 Alice 和量子系统 Bob, Alice 发送其中一个量子态给 Bob. Alice 有两组 POVM 测量算子, 测量算子 X 对应的测量集合为 $\{M_x\}$, 测量算子 Z

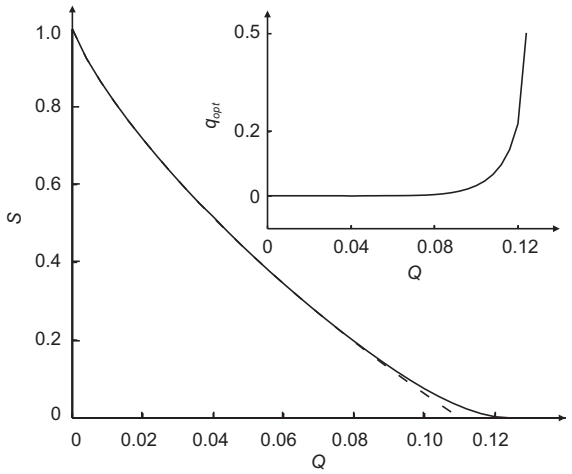

图 4　通过在接收端注入噪声可以提高 BB84 协议所能允许的最大误码率 [5]

Figure 4　The maximal tolerated QBER can be improved by adding classical noise [5].

对应的测量集合为 $\{M_z\}$. Mario 等人 [19] 给出的不确定关系如下所示:

$$H(X|B)+H(Z|B)\geqslant q+H(A|B), \tag{29}$$

其中 $q=\log_2\frac{1}{c}$, $c=\max_{x,z}|\langle x|z\rangle|^2$, 此处 Alice 的测量为秩为 1 的投影测量算子 $M_x=|x\rangle\langle x|, M_z=|z\rangle\langle z|$. 从上述公式可以看出, 若 Alice 和 Bob 之间存在纠缠, 则 $H(A|B)<0$, 相应的 Bob 的不确定性会减小.

当考虑到窃听者的系统时, Alice, Bob 和 Eve 成为三体纯态, 利用上述理论分析可以推导出如下的不确定关系:

$$H(X|B)+H(Z|E)\geqslant q, \tag{30}$$

其中 E 为窃听者 Eve 的量子态, 该不确定关系的推导过程如下:

利用 $H(X|B)+H(Z|B)\geqslant q+H(A|B)$ 可以得到

$$H(XB)+H(ZB)\geqslant q+H(AB)+H(B), \tag{31}$$

由于 Alice, Bob 和 Eve 是三体纯态, 则 $H(XB)=H(XE), H(AB)=H(E)$. 代入上述不确定关系表达式中可以得到

$$\begin{aligned} &H(XE)+H(ZB)\geqslant q+H(E)+H(B)\\ &\Rightarrow H(X|E)+H(Z|B)\geqslant q. \end{aligned} \tag{32}$$

随后, Tomamichel 和 Renner 利用冯诺依曼平滑熵 (Smooth Min-entropy 和 Smooth Max-entropy), 给出了更为普适的不确定关系度量方法:

$$H(X|E)^{\varepsilon}_{\max}+H(Z|B)^{\varepsilon}_{\min}\geqslant q. \tag{33}$$

利用该不确定关系证明量子密钥分配安全性有三条基本假设:

(1) Alice 和 Bob 拥有各自的随机数发生器且不能被窃听者控制.

(2) Alice 确定性的知道量子态的制备状态, 量子态的制备是完美的或者是可检测的非完美制备.

(3) 测量设备可以认为是黑盒子, 即测量设备无关.

基于不确定关系的量子密钥分配协议中, 密钥率的公式为

$$R\geqslant H(X|E)^{\varepsilon}_{\min}-H(Z|B)^{\varepsilon}_{\max}. \tag{34}$$

当 Alice 端的量子态制备完美时可以得到 $c=\frac{1}{2}$, 不妨假定合法通信双方在两组测量基下的比特误码率相同, 即 $H(Z|B)^{\varepsilon}_{\max}=H(X|B)^{\varepsilon}_{\max}=h(Q)$, 其中 Q 是比特误码率. 则最终的密钥率公式为

$$R\geqslant H(X|E)^{\varepsilon}_{\min}-H(Z|B)^{\varepsilon}_{\max}\geqslant 1-2h(Q). \tag{35}$$

4 实际量子密钥分配系统安全性分析

QKD 系统的实际安全性分析一直是一个备受关注的研究方向 [20–22]. 实际安全与理论安全之间存在差别的主要原因是实际 QKD 系统中采用的器件存在多种不满足理论模型要求的非理想特性, 这些非理想性有可能导致器件响应上的误差、边信道 (Side Channel) 信息的泄漏甚至设备被远程操控, 从而使 QKD 系统的安全性出现漏洞. 窃听者利用这些漏洞可以在引入低于理论容限的误码率或不引入误码率的情况下获取部分甚至全部的密钥比特, 因此其攻击行为难以被合法通信双发检测.

本节总结了近期关于 QKD 系统实际安全性的研究工作, 分别讨论了实际 QKD 系统中光源、有源光学器件、无源光学器件以及单光子探测器等实际器件的非完美性对系统安全性带来的影响. 在有损有噪声信道的条件下, 针对实际系统的安全性分析和攻击方案总结如表 1 所示.

4.1 非理想光源

理想的 BB84 协议要求使用单光子源, 否则窃听者可以采取光子数分离攻击 (Photon-number Splitting Attack). 但是由于目前尚无真正可用的单光子光源, 实际 QKD 系统一般会使用弱相干光源, 结合诱骗态 (Decoy State) 方法 [13–15] 来抵御光子数分离攻击. 下面以弱相干光源为重点, 讨论光源非完美性对 QKD 系统安全带来的影响.

诱骗态技术 (Decoy State Method) 诱骗态思想可以保证实际系统在使用弱相干态光源时也可以生成密钥比特, 其核心思想利用了窃听者无法区分进入信道的光子来自信号态还是是诱骗态. Lo 和 Wang 等人证明了诱骗态量子密钥分配协议在假设密钥无限长条件下的安全性, 其密钥率公式为

表 1　实际系统的安全性分析和攻击方案

Table 1　Practical security analysis and attacking scheme

光源非理想	有源光学器件	无源光学器件	单光子探测器非理想
诱骗态技术	相位重映射	被动法拉第反射镜	探测效率时域不匹配
光强涨落	不完全随机化相位	波长相关分束器	探测器线性工作模式
非可信光源	相位调制器衰减		探测器死时间
多激光器	相位调制器误差		死时间设置下码率
	光强度调制器		

$$R \geqslant \frac{1}{2}[Y_1 P_1(1-h(e_1)) - Q_\mu h(E_\mu)], \tag{36}$$

其中, R 是最终的密钥率, $\frac{1}{2}$ 是对基过程中的筛选效率, Y_1 是单光子态的计数率, P_1 是发送端单光子态的概率, e_1 是单光子态引入的比特误码率, Q_μ 是信号态的计数率, E_μ 是信号态的误码率. 首先给出诱骗态量子密钥分配协议在极限情况下的理论分析, 此时 Y_1, P_1, e_1, Q_μ 和 E_μ 分别由下式给出:

$$\begin{aligned} Y_1 &= Y_0 + \eta, \\ P_1 &= \mu e^{-\mu}, \\ e_1 &= \frac{e_0 Y_0 + e_{\mathrm{Det}}\eta}{Y_1}, \\ Q_\mu &= Y_0 + 1 - \mathrm{e}^{-\eta\mu}, \\ E_\mu &= \frac{\frac{1}{2}Y_0 + e_{\mathrm{Det}}(1-\mathrm{e}^{-\eta\mu})}{Q_\mu}, \\ \eta &= 10^{\frac{-\alpha l}{10}}\eta_D, \end{aligned} \tag{37}$$

其中 μ 是信号态的平均光子数, α 是量子信道的损耗效率参数, l 是光纤长度, η_D 是探测器的探测效率, Y_0 是探测器的暗计数, e_{Det} 是探测器自身引入的误码率值.

不妨假定在实际量子密钥分配系统中, Alice 和 Bob 选择诱骗态的平均光子数为 ν. 实际实验系统中能够观测到计数率 Q_μ 和误码率 E_μ 的测量结果, 则相应的单光子计数率 Y_1 和单光子误码率 e_1 可以由下述公式获得 (更详细的诱骗态的讨论和推导过程可以参考文献 [23]):

$$Y_1 \geqslant \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu \mathrm{e}^{\nu} - Q_\mu \mathrm{e}^{\mu}\frac{\nu^2}{\mu^2} - Q_\mu E_\mu \mathrm{e}^{\mu}\frac{\mu^2-\nu^2}{\frac{1}{2}\mu^2}\right),$$

$$e_1 \leqslant \frac{Q_\mu E_\mu}{Q_1^L}, \tag{38}$$

在密钥无穷长的情况下, 诱骗态协议中的信号态和诱骗态在相同光子数下的计数率和误码率是相同的, 且光子数分布严格服从泊松分布. 但是, 在实际的实验系统中只能得到有限长的密钥比特. 由于密钥长度有限, 光子的计数率和误码率存在着统计涨落, 而窃听者可以通过利用统计涨落来获得更多的信息量. 为了分析诱骗态量子密钥分配协议在密钥有限长时的安全性, 相应计数率和误码率的结果应该服从数理统计的大数定律. Scarani 和 Renner [24] 分析了基于理想单光子源的 BB84 协议在密钥有限长条件下的安全性, 并证明了诱骗态量子密钥分配协议在密钥有限长条件下的安全性 (另见文献 [25, 26]).

光强涨落 (Intensity Fluctuation) [27–30]　在对诱骗态方法生成的密钥率进行理论计算时, 必须假设信号态和诱骗态的振幅值是稳定且可知的. 但在实际实验中, 由于量子波动和调制设备非理想等因素, 光源输出光强存在随机涨落, 引起信号态与诱骗态的振幅与期望值发生不可预知的偏离, 从而导致密钥率的计算出现误差. 若光源的光强涨落超出一定范围, QKD 协议将因密钥率的理论值与实际值有过大偏差而被迫停止运行. 为解决这一问题, 有学者分析了光强涨落对 QKD 系统实际安全性的影响. 他们提出了一个描述光强涨落的方案 [27], 将光强的涨落等效为光强调制误差, 并证明即使调制误差较大, 诱骗态方法仍能保证 QKD 协议的无条件安全并维持较高的密钥生成率, 进而给出了修正后的密钥率计算公式 [28–30]. 此结论之后被证明可以推广至有任意数量诱骗态的 QKD 协议 [31]. 实验证明, 结合诱骗态方

法和主动光强监控能有效降低光强波动造成的不利影响 [32]. 此外, 使用下参量转换光源和标记单光子源的 QKD 协议方案同样存在光强波动的问题 [33,34], 但受到的影响明显比使用弱相干光源的方案要小, 相同的结论也适用于标记配对相干态光源 [35].

非可信光源 (Untrusted Source)[36–39] 在双向 "Plug-and-play" 式 QKD 系统 [36] 的安全性分析中, 光源在调制为单光子态之前要经过信道的传输, 信道中传输的光源被认为可完全由窃听者 Eve 控制, 窃听者可以通过改变光子数的分布来获取更多的密钥信息量. 国内外学者在理论和实验上已经证明, 通过实时主动地监控光源光子数分布, 能够保证使用不可信光源的 QKD 系统维持无条件安全, 且密钥生成率对比可信光源系统无明显降低 [37]. 相比主动监控, 有学者认为被动监控更符合实际应用的需要 [38,39]. 被动监控方法主要有三种: 平均光子数监控、光子数分析和光子数分布监控. 当信道信噪比不太低的时候, 使用被动光子数分析是解决不可信光源问题的一个较易实现且高效的方法.

多激光器 (Multi Sources)[40] 在一些 BB84 协议的实际编码实现方案中, 为了简化调制步骤, Alice 会采用多台激光器来制备四种偏振态. 然而, 即使是相同型号的激光器, 每一台之间总会存在着各种各样微小的差别. 例如, 不同的激光器所产生的激光光谱不能保证完全相同 [40]. 依靠这些细微的差别, 窃听者可以通过分析光频谱来辨别信道中传播的光子由哪一台激光器发出, 从而可能掌握 Alice 的选基信息. 因此与单激光器方案相比, 多激光器方案会给窃听者引入更多的信息量.

4.2 有源光学器件

在实际 QKD 系统中常用的有源光学器件有相位调制器 (Phase Modulator)、光强调制器 (Intensity Modulator)、光纤拉伸器 (Fiber Stretcher) 等等. 其中相位调制器主要被应用在诱骗态方案里对弱相干态进行相位随机化, 以及在相位编码 BB84 协议方案里进行相位编解码调制; 光强控制器则主要被应用于制备信号态, 或是将激光器输出的连续光调制成光脉冲. 以下讨论实际相位调制器以及光强调制器的非完美性对 QKD 系统安全造成的影响.

相位重映射攻击 (Phase Remapping Attack)[41,42] 相位调制器通过控制加载电压的大小调制出相应的相位. 文献 [41] 指出, 窃听者可以通过控制延时, 使脉冲到达相位调制器的时间刚好处在调制电压的上升沿或下降沿区间, 从而使实际调制的相位值小于 Alice 预期值. 利用这一漏洞, 窃听者可以对 Plug-and-play 和 Sagnac 系统 [43] 实施相位重映射攻击, 在引入 19.7% 的误码率 (低于阈值 25%) 情况下, 获取到全部的密钥信息 [42].

不完全随机化相位攻击 (Partially Random Phase Attack)[44] 对于使用弱相干光源的 BB84 协议 QKD 系统而言, 相位随机化是实现诱骗态方法的一个重要假设 [45]. 相位随机化要求对每个弱相干态加载的随机相位在 $[0,2\pi]$ 范围内选取. 若选取范围小于 $[0,2\pi]$(即不完全随机化), 窃听者有可能窃取到密钥信息. 文献 [44] 对无法做到完全相位随机化的双向 Plug-and-play 系统提出了一种可行的截取重发攻击方案 (不完全随机化相位攻击). 在这个攻击方案里, 窃听者制备伪造态 (Fake State) 发送给 Alice, 再通过零拍测量 (Homodyne Detection) 来获取 Alice 的相位调制信息, 最后依据该信息对 Bob 发送的光脉冲做相位调制. 在中短传输距离情况下, 不完全随机化相位攻击引入的误码率低于阈值, 因此可以免于被通信双方被发现. 这一方案被证明对单诱骗态的 BB84 协议也同样适用.

相位调制器衰减 (Phase Modulator Attenuation)[46] 现有的光纤量子密钥分配实验系统大多基于相位编码, 这是由于光纤信道存在固有的双折射效应. 相位编码系统中常用不等臂干涉环作为编解码器件. 干涉环分为长短臂, 其中一个臂上利用相位调制器对量子态进行调相编解码. 在安全性分析中不等臂干涉环的一个重要假设是长臂和短臂有相同的衰减, 其中发射端的衰减对于量子密钥分配系统的整体安全性没有影响, 而接收端的衰减可以作为信道衰减的一部分, 原则上也不会影响量子密钥分配系统的密钥率公式. 然而任何实际的调相器是存在衰减的, 所以调相器衰减引入的最直接问题是量子态制备的非平衡性. 而之前的安全密钥率公式 GLLP 不再适用于非平衡干涉环的量子密钥分配系统. 解

决这一问题的一个直接办法是人为补偿不等臂衰减的非平衡性, 从而使 GLLP 公式可以适用于该系统. 但是这种安全性证明方法牺牲了一部分多余的密钥比特, 因此并不是最优的. 我们给出了一种新的安全性证明方法, 通过将一种构造的虚拟光源替代实际应用的光源, 可以得到较优的密钥率公式. 该协议如图 5 所示.

可以证明实际系统中的光子态产生密钥比特的安全性和虚拟光源经过虚拟酉变换后的光子态生成的密钥比特在安全性上是等价的. 此安全性证明中构造的酉变换的详细描述形式如下:

$$\begin{aligned} U|0\rangle_l|0\rangle_s|0\rangle_A &= |0\rangle_l|0\rangle_s|0\rangle_A, \\ U|0\rangle_l|1\rangle_s|0\rangle_A &= |0\rangle_l|1\rangle_s|0\rangle_A, \\ U|1\rangle_l|0\rangle_s|0\rangle_A &= \frac{\sqrt{\nu}}{\sqrt{\mu}}|1\rangle_l|0\rangle_s|0\rangle_A \\ &\quad + \frac{\sqrt{\mu-\nu}}{\sqrt{\mu}}|0\rangle_l|0\rangle_s|1\rangle_A, \\ U|n\rangle_l|m\rangle_s|0\rangle_A &= |n\rangle_l|m\rangle_s|0\rangle_A, \quad m+n\geqslant 2, \end{aligned} \tag{39}$$

其中 $|0\rangle_A$ 和 $|1\rangle_A$ 是 Alice 相互正交的量子态, 但 Alice 不知道每个量子态是属于单光子态、真空态或多光子态.

相位调制器误差 (Imperfect Modulator)[17] 在实际调制器误码安全性方面以偏振方案为例来分析, Alice 态相关安全性分析的基础是发送端的量子态与理想协议相比有角度偏转. 具体来说, Alice 的经典比特 0 被随机编码为偏振量子态 $|\alpha_1{}^{\rm o}\rangle$ 或 $|45+\alpha_2{}^{\rm o}\rangle$, 而经典比特 1 被编码为偏振量子态 $|90+\alpha_3{}^{\rm o}\rangle$ 或 $|-45+\alpha_4{}^{\rm o}\rangle$, 其中 α_1, α_2, α_3 和 α_4 是描述 Alice 角度偏转的安全参数. Bob 随机的选择非理想水平垂直基 $\{|\beta_1{}^{\rm o}\rangle, |90+\beta_3{}^{\rm o}\rangle\}$ 或非理想对角基 $\{|45+\beta_2{}^{\rm o}\rangle, |-45+\beta_4{}^{\rm o}\rangle\}$ 测量其接收到的量子态, 其中 β_1, β_2, β_3 和 β_4 是描述接收端非理想性的安全参数. 因为编解码的随机选择性, 所有的非理想性都不应该被窃听者 Eve 控制. 文献 [17] 分析了调制误差参数对最终密钥率的影响, 由于窃听者不能控制合法通信双方的安全区, 在安全性分析中可以发现调制误差在降低合法通信双方信息量的同时也会降低窃听者的信息量.

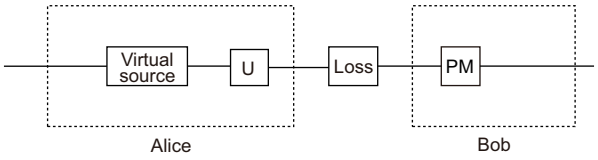

图 5 构造虚拟酉变换和虚拟光源的相位编码量子密钥分配系统

经过此虚拟酉变换, 虚拟光源发送的单光子衰减为真空态或仍然是单光子态. 在量子信道中只有单光子态才可以最终产生安全的密钥比特

Figure 5 UMZI method QKD with an imaginary unitary transformation and virtual source. After the unitary transformation, the single photon state emitted by the virtual source can be transformed into single photon state and vacuum state respectively. In the quantum channel, only the single photon state can be used for generating the final secret key.

光强度调制器 (Intensity Modulator)[47] 通过在光强调制器上加载不同的电压可以控制输入光强的透过率. 光强调制器能提供的最大透过率与最小透过率之比称为它的消光比 (Extinction Ratio), 实际光强调制器消光比一般在 25 dB 左右. 在一些 QKD 系统中为了提高效率, Alice 会同时制备 BB84 协议里所需的四种态 (0, 1, +, −), 然后通过光强调制器消去其中三种, 剩下一种作为被选中的信号态发送给 Bob. 由于光强调制器消光比有限, 本应被消去的三种态会存留有一定的光强叠加在信号态中, 形成本底噪声 (Back Ground Noise), 从而增加了 QKD 系统的误码. 注意到这种本底噪声无法被控制或根除, 因而窃听者并不能通过它来获取到有用的信息. 因此在计算保密放大过程损失的信息量时, 可以将这部分由本底噪声造成的误码率剔除, 从而使实际成码率有所提高.

4.3 无源光学器件

在全光纤 QKD 系统中, 常用的无源光学器件有光纤分束器、光纤偏振分束器、法拉第镜、环行器、波分复用器等等. 以下讨论法拉第反射镜和光纤分束器的非完美性对 QKD 系统安全造成的影响.

被动法拉第反射镜攻击 (Passive Faraday-mirror Attack)[48] 在 Plug-and-play 系统中, 法拉第反射镜能够起到补偿信道对信号态偏振干扰的作用, 是让系统能够稳定工作的一个重要部件. 理想的法拉第反射镜使反射出来的线偏振光相对入射时偏振旋转

90°, 而非理想的法拉第反射镜在这个旋转角度上可能存在着偏差. 文献 [48] 的研究指出, 这一偏差将导致从 Alice 返回给 Bob 的信号态在所处希尔伯特空间中的维度从 2 维变成 3 维. 这一额外维度使窃听者能更好地估计 Alice 的调制信息, 从而在截取重发攻击中引入的误码率小于 25%. 结合上一节提到的相位重映射攻击方法, 窃听者引入的误码率能进一步减小到低于 11%, 低于 BB84 协议在联合攻击下的误码率容限. 因此在对实际系统安全性进行分析时, 必须考虑到法拉第反射镜的非完美性, 对密钥率公式做出相应的修正.

分束器波长相关攻击 (Wavelength-dependent Beam Splitter Attack) [49] 几乎所有 QKD 系统的设计都会用到光分束器 (Beam Splitter). 熔融拉锥光纤分束器因其工艺成熟、价格低廉等优点而被广泛应用于全光纤 QKD 系统. 在对 QKD 系统的实际安全性分析中, 光纤分束器的分束比 (Coupling Ratio) 一般被假定是固定不变且不能被窃听者更改的. 但是通过理论计算 [50,51] 和测试验证可以发现, 熔融拉锥光纤分束器的分束比会随输入光波长的改变产生周期性的变化. 以 QKD 系统中常用的 50:50 分束器为例, 虽然在设定的工作波长 (1550 nm) 处分束比特性理想, 但是当输入光波长偏离工作波长时, 分束比也随之发生变化.

熔融拉锥光纤分束器这一波长相关特性成为实际 QKD 系统的一个安全漏洞, 文献 [49] 研究了这一漏洞对被动偏振编码的 BB84 协议系统所造成的影响, 并提出了一种波长攻击方案. 在被动偏振编码方案中, Bob 对测量基的选择依赖于分束器以相同的概率随机地让单光子到达输出口 PORT1(对应水平垂直基测量) 或是 PORT2 (对应对角基测量). 利用光纤分束器的波长相关特性, 窃听可以通过发送不同波长的伪造态来控制 Bob 的测量基选择, 从而迫使 Bob 每次都得到与窃听者相同的选基和响应. 验证实验表明, 窃听者能够在只增加极少量额外噪声 (约 0.1%) 的情况下获取到几乎全部的密钥信息.

4.4 探测器不完美

为了实现长距离密钥分配, 光纤 QKD 系统通常工作在 1550 nm 波段, 在此波段下, 通常使用超导纳米线探测器或者基于 InGaAs/InP 雪崩管的红外单光子探测器. 后者具有量子效率较高、结构简单、使用方便等特点, 因此在实际 QKD 系统中被广泛使用. 为了减少暗计数, 基于 InGaAs/InP 雪崩管的探测器通常工作在门模式 (Gated Mode) 和 $-30^{\circ}\mathrm{C}-50^{\circ}\mathrm{C}$ 的条件下. 门控模式探测器只有在门信号期间才能进行有效探测, 其探测效率会随光子到达时间发生改变. 这种效率变化在特定条件下会成为攻击漏洞. 在正常工作条件下, 有单个光子到达探测器, 探测器就会输出一次雪崩信号. 然而, 单光子探测器也会对强光信号进行响应. 攻击者使用强光信号也可以使得单光子探测器产生特定的输出, 从而进行攻击. 由于 InGaAs/InP 雪崩管固有的半导体结构缺陷会捕获载流子并在没有光子到来时释放, 进而产生雪崩信号, 因此该器件在正常的探测信号之容易产生虚假的探测脉冲输出, 这被称为后脉冲效应. 为了减小后脉冲效应, 在一次有效探测之后, 需要设置一定的死时间, 以减小虚假探测脉冲发生的概率. 攻击者可以利用死时间作为漏洞进行攻击.

利用探测效率时域不匹配 [52–55] 实际系统中, 探测器效率是时间的函数, 图 6 给出了双探测器在时间上探测效率不匹配的示意图.

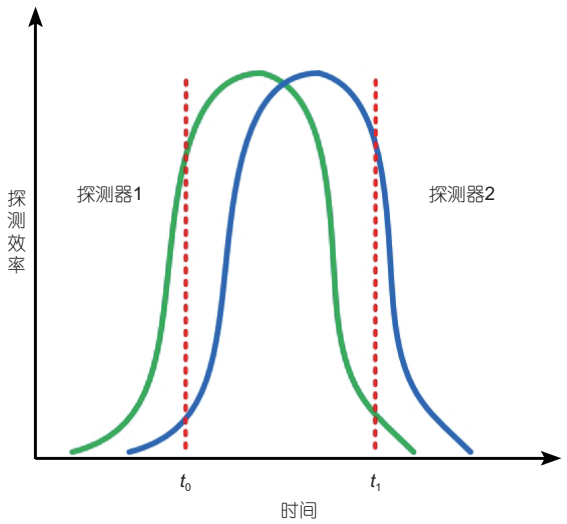

图 6 (网络版彩图) 双探测器基于时间的探测效率不匹配的示意图

Figure 6 (Color online) Dual detector has different detection efficiency.

t_0 时刻 SPD0 的探测效率明显高于 SPD1, 而在 t_1 时刻则刚好相反. 利用此漏洞, Makarov 等人 [52,53] 提出了 Faked States 攻击. 这是一种截取重发攻击, Eve 截取 Alice 发送的量子态, 随机选择基测量. 根据测量结果, Eve 选用与测量时相反的测量基和测量结果, 重新制备一个量子态. 例如 Eve 用 Z 基测量得到 0, 那么他在 X 基下制备 1. Eve 将重做的量子态发给 Bob, 控制其到达时间在 t_0 (测量结果为 0) 或者 t_1 (测量结果为 1). 这种攻击将引入 25% 的误码. 并且受条件的限制, 该攻击无法具体实验. 此后, Qi 等人 [54] 于 2007 年利用相同的漏洞, 提出了 Time-shift 攻击. 在这种攻击中, Eve 不需要测量制备量子态, 只需随机改变 Alice 发出的量子态到达 Bob 端的时间, 使其在 t_0 或者 t_1 到达即可. 理论上该攻击不会引入误码, 但在效率部分不匹配情况下无法获得全部的密钥信息. 2008 年他们给出了此攻击的实验方案 [55], 使用 ID500 型商用 QKD 系统 (http://www.idquantique.com/), Eve 能够以 4% 的概率成功获取部分密钥.

利用探测器线性工作模式 [56–59] QKD 系统所用单光子探测器处于线性模式时不会响应单光子信号, 但能响应一定功率的强光信号. 2010 年, Lydersen 等人在实验上证明可以利用连续的强光致盲探测器, 使其一直工作在线性模式. 在此基础上, Eve 截取 Alice 发送的量子态, 重新制备经典脉冲叠加在强光之上可实现强光致盲攻击 (Light Blinding Attack) [56]. 使用强光致盲探测器的好处在于能消除后脉冲等噪声对误码的影响, 然而 Yuan 等人 [57] 指出强光致盲攻击能够成功的原因在于 APD 电路中包含了偏置电阻. 他们指出在正确使用 APD 时, 强光致盲攻击对多数 APD 都是无效的. Lydersen 等人 [58] 对此的解释是移除偏置电阻后也有多种方法可以致盲探测器; 即使能够避免致盲, 也不能避免攻击. 因为工作于门模式的探测器在门之间就处于线性模式, 触发脉冲完全可以直接在探测器开门之后应用, 而这正是 After-gate 攻击 [59] 的做法. 实际系统中通常将开门时间前后区域发生的计数也作为正常计数, 这使得可以在紧邻门之后输入强光脉冲实施攻击, 当然这会引入很强的后脉冲效应. 如果系统在死时间内仍然接收计数并重设死时间, 那么 Eve 就可以利用此漏洞使 Bob 的探测器在大部分时间内处于死时间状态, 这样实施的攻击也可以减小后脉冲的影响.

利用探测器死时间 [60] 探测器的死时间效应使得 Eve 能够操纵探测器的探测效率实施 Dead time 攻击 [60]. 此攻击不需要截取量子态, 只需在信号脉冲前面注入一个衰减的攻击脉冲 (脉冲强度满足除了需要的探测器外, 其他的探测器都被能致盲), 利用探测器的死时间效应就能获取全部的密钥信息. 该攻击方案对几乎所有的 QKD 系统都有效. 以 BB84 偏振编码为例, 具体方法为: Eve 将衰减的光脉冲调制在协议所使用的四个偏振态之一, 先于 Alice 发送的信号态到达 Bob 端的探测器, 根据脉冲的强度和偏振, Bob 有一定概率探测到 Eve 发送的脉冲, 这样 Eve 就部分致盲了 Bob 的探测器. 随后而至的量子态只能在没有被致盲的探测器上有响应. 例如在偏振编码的系统中, 如果 Eve 随机选择的偏振调制为 $|-\rangle$, Bob 被动选基测量系统中探测 $|H\rangle$, $|V\rangle$ 和 $|-\rangle$ 的探测器以一定的概率被致盲, 只有探测 $|+\rangle$ 的探测器是有效的, 窃听者由此控制了接收端探测器的响应. 值得注意的是, 致盲脉冲的强度比较低的时候, Eve 成功的概率也比较低, 可以通过控制脉冲的强度来提高获取密钥信息的概率. 实验用的是自由空间偏振编码系统, 结果显示 Eve 的致盲脉冲平均光子数达到 16.52 时, 他与 Alice 和 Bob 的 sifted key 有 98.83% 的重叠, 即 Eve 与 Bob 之间的信息量达到了 0.908.

死时间设置下码率的估计 [61] 在 QKD 实验调试时, 密钥率的估计是一个很重要的方面. 在考虑后脉冲效应时, 系统需要设定死时间来减少误码, 我们采用蒙特卡洛法数值模拟了 QKD 的过程, 可以快速得出不同参数配置下的密钥率, 从而能够方便的设定最优死时间参数, 使密钥生成率达到最大值, 对实验具有很好的指导意义.

5 设备无关及半设备无关量子密钥分配

检测所有 QKD 器件的非理想性在技术上是非常困难的事情, 有学者提出了设备无关量子密钥分配 (DIQKD) 用来抵抗各种器件非理想所引入的攻击手段, 其安全性证明过程无需对量子设备的内部机

制做出任何假设. 在 DIQKD 中, QKD 的态制备和态测量设备被视为以经典输入产生经典输出的黑盒子. 这些设备被认为实现了一个量子过程, 但是这个过程没有对 Hilbert 空间的维度、以及实际量子过程中的量子操作或者量子态做出任何假定. 需要指出的是 Cai 和 Lv [62] 在 2007 年就已经证明使用量子隐形传态 (Quantum Teleportation) 也可以避免边信道攻击 (Side-channel Attacks).

与设备可信任 QKD 协议的安全性假设相比, DIQKD 协议弱化了第三个条件, 其描述修改为 3′) Alice 和 Bob 信任他们的经典设备以及存储和处理量子仪器所产生的经典数据.

全设备无关 (Full Device Independent) 设备无关量子密钥分配协议的分析基于量子纠缠, Alice 和 Bob 不仅不信任纠缠粒子源, 同时也不信任他们的测量仪器. 例如, 由于仪器的缺陷, 测量取向可能随着时间而不断漂移, 或者整个测量装置都不可信, 因为它们有可能由窃听者制作, 因此 Alice 和 Bob 并不能保证实际测量基就是理想协议所要求. 事实上, 他们甚至不能对他们定义的 Hilbert 空间的维度做出假设. 在 DIQKD 中, Alice 和 Bob 因此需要根据观测到的经典输入 - 输出关系遍历所有与之相符的量子态和测量基 (在任意维度的 Hilbert 空间中), 并估计窃听者所能获得的最大信息量. 相比之下, 在通常的 QKD 协议中, Alice 和 Bob 对执行的测量和 Hilbert 空间的维度都有明确地限定. 这些限定对 QKD 的安全性是非常重要的. 例如, 在 Alice 和 Bob 共享四维系统的情况下, BB84 协议的安全性就会被完全的破坏.

QKD 方案的安全性可以基于 Bell 不等式的违反, 这一直觉认识最早起源于著名的 Ekert1991 协议 [63], 随后 Barrett 等人 [64] 在定量描述方面取得了开创性的进展. 他们证明了在窃听者仅被不可超光速 (No-signaling) 原理 (而不是整个量子体系) 限制的情况下, QKD 系统仍然是安全的. 2007 年 Acin 等人 [65] 在 Ekert1991 协议基础上给出了 DIQKD 在最优联合攻击 (Collective Attack) 下的安全性, 在证明中并未对量子密钥分发设备的运作和所操纵的量子系统做出任何假设. 在假设窃听者 Eve 遵循量子力学的前提下, 给出了 Bob 和 Eve 之间 Holevo 信息的一个紧的上界, 且这个上界是关于 Bell 不等式违反量的一个函数.

单边设备无关 QKD (One-sided Device-independent Quantum Key Distribution) 由于 DI-QKD 方案的实验实现面临着纠缠态制备效率低和探测器漏洞 (Detection Loophole) 等问题, 2012 年 Branciard 等人 [66] 提出了单边设备无关量子密钥分配协议 (One-side DI-QKD). 在该协议中, Alice 和 Bob 只有一方 (比如 Bob) 信任他的测量装置. 这一方案介于标准的 QKD(两方都信任他们的测量装置) 和 DIQKD(两方都不信任他们的测量装置) 之间, 在某些现实情况下这可能是更实际的假设. Branciard 等人表明相对于 DIQKD 来说, 单边 DIQKD 更容易满足获得最终密钥的条件, 并且指出 One-side DIQKD 和 Quantum Steering 之间的关系, 正如 DIQKD 和 Bell 不等式违反之间的关系, 从而为实验的可行性开辟了道路.

半设备无关 QKD (Semi-device-independent Quantum Key Distribution) 2011 年 Pawlowski 等人 [67] 提出将设备无关安全性的概念应用于单向 (量子态制备和测量)QKD 之中, 他们证明了半设备无关 (Semi device-independent) 单向 QKD 协议在个体攻击 (Individual Attack) 下是安全的. 在半设备无关的情况下, 可信的各方所使用的设备是未经刻画的, 但所使用的量子系统的维度是假设受限的. 证明中 Pawlowski 等人主要利用了维度目击 (Dimension Witnesses) [68] 和随机存取码 (Random-access Codes) [69] 来度量合法通信双方之间的非经典关联.

基于类似的思想, 我们提出了基于 2 维量子维度目击不等式的单向无纠缠随机数扩展方案 [70,71], 该随机数扩展方案可以应用现有的量子密钥分配系统平台来实现, 方案的实现不依赖于纠缠资源, 对于其随机性我们可以通过数值计算测量结果的冯诺依曼小熵得到. 该方案不需要假设任何的态制备和态测量模型, 但需假设量子系统的维度限制在 2 维的希尔伯特空间、攻击模式采用联合攻击. 需要指出的是, 随机数扩展方案中量子态制备和量子态测量在同一个安全区域, 同时任何经典比特的测量结果不会泄露给第三方. 该方案在同一个安全区有两个黑盒子分别描述量子态制备和量子态测量, 具体的方案如图 7 所示, 基于量子随机存取码的维度目击值和输出结果小熵之间的关系如图 8 所示.

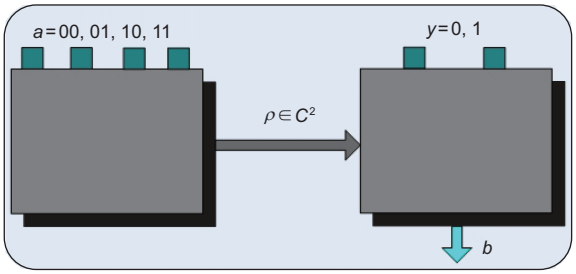

图 7　(网络版彩图) 双半设备无关随机数扩展方案

该方案左边的黑盒子为量子态制备的黑盒子, 右边的黑盒子为量子态测量黑盒子. 在方案的随机性分析中我们基于量子随机存取码 (Quantum Random Access Code) 构造了维度目击不等式 (Dimension Witness Inequality)

Figure 7　(Color online) Semi-device independent random number expansion protocol, the state preparation and measurement can be regarded as the black box, randomness of the measurement outcomes are based on the quantum dimension witness inequality.

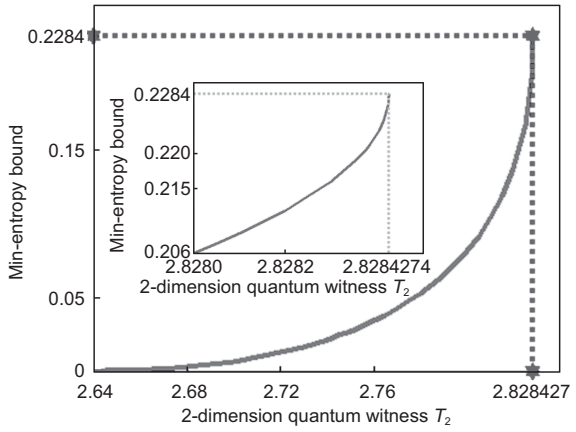

图 8　基于随机存取码的维度目击值与测量结果小熵之间的关系

Figure 8　The relationship between the average efficiency of $2 \to 1$ QRAC measured by T_2 and the min-entropy bound.

测量仪器无关 QKD (或者边信道无关 QKD, Measurement-device-independent QKD or Side-channel-free QKD)　众所周知, 在量子密码术中如何消除探测器的边信道攻击是一个棘手的问题. Lo 等人 [72] 提出了一个简单的解决方案, 即测量端仪器无关量子密钥分配 (Measurement-device-independent QKD). 它不仅消除了探测器所有的边信道, 而且可利用传统激光器使安全距离加倍.　相较于之前的 DIQKD 解决方案, MDIQKD 不要求探测器拥有接近于 100% 的探测效率, 而且不需要结合 (基于隐形传态的) 量子比特放大器或者脉冲光子数的量子非破坏测量, 因此可以在使用低探测效率的光学元件和高损耗信道的条件下得以实现.

同样为了解决边信道攻击的问题, Braunstein 等人 [73] 提出了边信道无关量子密钥分配协议 (Side-channel-free QKD). 在通常的 QKD 协议中, 一般假设 Alice 和 Bob 的安全区域 (Private Spaces) 完全无法从外部进入. 尽管如此, 在实际情况下安全区域的任何通信端口都有可能引入一个探测安全区内部的边信道. 为了防止和克服这种攻击, 安全区不能直接参与任何的态制备或响应外部信号的探测. Braunstein 等人利用两体纠缠态的坍缩来进行态制备, 并以一种类似于隐形传态 (Teleportation) 的方式, 将所有真实信道替换为虚拟信道. 该协议最简单的设置即对应于一个纠缠交换 (Entanglement Swapping) 实验, 其中双隐形传输通道起到了 Hilbert 空间过滤器 (Filters) 的作用, 进而消除了边信道攻击. 最后, 由一个外部不可信的中继执行一个适当的局域操作和经典通信 (LOCC) 来创建 Alice 和 Bob 之间的关联, 从而产生密钥.

6　结论及展望

量子密码技术是一种物理密码, 它使用信息携带载体的内禀物理量及其量子力学属性对加载的密钥信息进行保护. 这一技术可以有效的解决 One-time Pad 密码体制所需的密钥分发信道问题, 两者结合可以实现无条件安全的保密通信. 此外, 量子密码具有按需动态实时分发的特性, 有利于解决密钥管理和存储的问题, 这些特点使得量子密码学的研究受到密码学界的高度重视.

由于量子密钥系统安全性分析是一个长期的系统工程, 理想协议下的安全性并不等价于实际系统的安全性, 国内外的学者日益关注如何有效的给出所有实际器件非理想性的度量方式和其对安全性的影响, 同时探索这些器件的非理想性可能引入的攻击漏洞和安全性可以采取的预防措施. 与此同时, 研

究基于黑盒子器件量子密码安全性可以有效的抵御器件不完美攻击, 但是这些新型的协议在实验实现上往往存在着探测器漏洞 (Detection Loophole) 等实验困难. 在这两种安全模式研究的基础上, 整个量子密码系统的安全性度量架构是值得进一步深入探讨的课题.

参考文献

1 Shannon C E. Communication theory of secrecy systems. Bell Sys Tech J, 1949, 28(4): 656–715
2 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. New York: IEEE, 1984. 175–179
3 Dagmar B. Optimal eavesdropping in quantum cryptography with six states. Phys Rev Lett, 1998, 81: 3018–3021
4 Renner R. Security of quantum key distribution. arXiv:quant-ph/0512258
5 Kraus B, Gisin N, Renner R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. Phys Rev Lett, 2005, 95: 080501
6 Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. Phys Rev A, 2005, 72: 012332
7 Wegman M N, Carter J L. New hash functions and their use in authentication and set equality. J Comput Sys Sci, 1981, 22: 265–279
8 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050–2056
9 Shor P, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444
10 Horodecki K, Horodecki M, Horodecki P, et al. Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity. IEEE Transact Inf Theor, 2008, 54(6): 2604–2620
11 Renes J M, Smith G. Noisy preprocessing and the distillation of private states. Phys Rev Lett, 2007, 98: 020502
12 Gottesman D, Lo H K, Lukenhaus N, et al. Security of quantum key distribution with imperfect devices. Quantum Inf Comput, 2004, 4: 325–360
13 Hwang W Y. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901
14 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504
15 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett, 2005, 94: 230503
16 Marøy ø, Lydersen L, Skaar J. Security of quantum key distribution with arbitrary individual imperfections. Phys Rev A, 2010, 82: 032337
17 Li H W, Yin Z Q, Wang S, et al. Security of quantum key distribution with state-dependent imperfections. Quantum Inf Comput, 2011, 11(11-12): 0937–0947
18 Tomamichel M, Renner R. Uncertainty relation for smooth entropies. Phys Rev Lett, 2011, 106: 110506
19 Mario B, Matthias C, Roger C, et al. The uncertainty principle in the presence of quantum memory. Nat Phys, 2010, 6: 659–662
20 Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography. Phys Rev Lett, 2000, 85(6): 1330–1333
21 Williamson M, Vlatkovedral. Eavesdropping on practical quantum cryptography. J Mod Opt, 2003, 50(13): 1989–2011
22 Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution. Rev mod phys, 2009, 81(3): 1301–1350
23 Ma X, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution. Phys Rev A, 2005, 72: 012326
24 Scarani V, Renner R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. Phys Rev Lett, 2008, 100: 200501
25 Li H W, Zhao Y B, Yin Z Q, et al. Security of decoy states QKD with finite resources against collective attacks. Opt Commun, 2009, 282(4162-4166): 012329
26 Tan Y G, Cai Q Y. Practical decoy state quantum key distribution with finite resource. Eur Phys J D, 2010, 56: 449–455
27 Wang X B, Peng C Z, Pan J W. Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source. Appl Phys Lett, 2007, 90(3): 031110
28 Wang X B. Decoy-state quantum key distribution with large random errors of light intensity. Phys Rev A, 2007, 75(5): 052301
29 Wang X B, Peng C Z, Zhang J, et al. General theory of decoy-state quantum cryptography with source errors. Phys Rev A, 2008, 77(4): 042311
30 Wang X B, Yang L, Peng C Z, et al. Decoy-state quantum key distribution with both source errors and statistical fluctuations. New J Phys, 2009, 11: 075006
31 Hayashi M. General theory for decoy-state quantum key distribution with an arbitrary number of intensities. New J Phys, 2007, 9: 284
32 Xu F, Zhang Y, Zhou Z, et al. Experimental demonstration of counteracting imperfect sources in a practical one-way quantum-key-distribution system. Phys Rev A, 2009, 80(6): 062309
33 Wang S, Zhang S L, Li H W, et al. Decoy-state theory for the heralded single-photon source with intensity fluctuations. Phys Rev A, 2009, 79(6):

062309
34 Hu J Z, Wang X B. Reexamination of the decoy-state quantum key distribution with an unstable source. Phys Rev A, 2010, 82(1): 012331
35 Zhou C, Bao W S, Fu X Q. Decoy-state quantum key distribution for the heralded pair coherent state photon source with intensity fluctuations. Sci China-Inf Sci, 2010, 012: 2485–2494
36 Muller A, Herzog T, Huttner B, et al. “Plug and play” systems for quantum cryptography. Appl Phys Lett, 1997, 70: 793–795
37 Zhao Y, Qi B, Lo H K. Quantum key distribution with an unknown and untrusted source. Phys Rev A, 2008, 77(5): 052327
38 Peng X, Jiang H, Xu B J, et al. Experimental quantum-key distribution with an untrusted source. Opt lett, 2008, 33(18): 2077–2079
39 Zhao Y, Qi B, Lo H K, et al. Security analysis of an untrusted source for quantum key distribution: Passive approach. New J Phys, 2010, 12: 023024
40 Nauerth S, Fürst M, Schmitt-Manderbach T, et al. Information leakage via side channels in freespace BB84 quantum cryptography. New J Phys, 2009, 11: 065001
41 Fung C H F, Qi B, Kiyoshi T, et al. Phase-remapping attack in practical quantum-key-distribution systems. Phys Rev A, 2007, 75(3): 032314
42 Xu F, Qi B, Lo H K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New J Phys, 2010, 12: 113026
43 Qi B, Huang L L, Lo H K, et al. Quantum key distribution based on a Sagnac loop interferometer and polarization-insensitive phase modulators. In: Proceedings of the 2006 IEEE International Symposium on Information Theory. Seattle: IEEE, 2006. 2090–2093
44 Sun S H, Gao M, Jiang M S, et al. Partially random phase attack to the practical two-way quantum-key-distribution system. Phys Rev A, 2012, 85(3): 032304
45 Lo H K, Preskill J. Phase randomization improves the security of quantum key distribution. arXiv:quant-ph/0504209
46 Li H W, Yin Z Q, Han Z F, et al. Security of practical phase-coding quantum key distribution. Quantum Inf Comput, 2010, 10(9-10): 0771–0779
47 Huang J Z, Yin Z Q, Han Z F, et al. Effect of intensity modulator extinction on practical quantum key distribution system. Eur Phys J D, 2012, 66: 159
48 Sun S H, Jiang M S, Liang L M. Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system. Phys Rev A, 2011, 83(6): 062331
49 Li H W, Wang S, Huang J Z, et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multi-wavelength sources. Phys Rev A, 2011, 84(6): 062308
50 Ankiewicz A, Snyder A, Zheng X H. Coupling between parallel optical fiber cores—Critical examination. Lightw Technol J, 1986, 4(9): 1317–1323
51 Tekippe V. Passive fiber-optic components made by the fused biconical taper process. Fiber Int Opt, 1990, 9(2): 97–123
52 Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys Rev A, 2006, 74: 022313
53 Makarov V, Hjelme D R. Faked states attack on quantum cryptosystems. J Mod Opt, 2005, 52(5): 691–705
54 Qi B, Fung C H F, Lo H K, et al. Time-shift attack in practical quantum cryptosystems. Quantum Inf Comput, 2007, 7: 73–82
55 Zhao Y, Fung C H F, Qi B, et al. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys Rev A, 2008, 78: 042333
56 Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat Photonics, 2010, 4: 686–689
57 Yuan Z L, Dynes J F, Shields A J. Avoiding the blinding attack in QKD. Nat Photonics, 2010, 4: 800–801
58 Lydersen L, Wiechers C, Wittmann C, et al. Avoiding the blinding attack in QKD. Nat Photonics, 2010, 4: 800–801
59 Wiechers C, Lydersen L, Wittmann C, et al. After-gate attack on a quantum cryptosystem. New J Phys, 2011, 13: 013043
60 Henning W, Harald K, Markus R, et al. Quantum eavesdropping without interception an attack exploiting the dead time of single photon detectors. New J Phys, 2011, 13: 073024
61 Liu D, Yin Z Q, Wang S, et al. Estimation of key rate after setting dead time. Chin Phys B, 2012, 21: 6060202
62 Cai Q Y, Lv H. Quantum key distribution against Trojan horse attacks. Chin Phys Lett, 2007, 24(5): 1154–1157
63 Ekert A K. Quantum cryptography based on Bell’s theorem. Phys Rev Lett, 1991, 67: 661–663
64 Barrett J, Hardy L, Kent A. No signaling and quantum key distribution. Phys Rev Lett, 2005, 95: 010503
65 Acin A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks. Phys Rev Lett, 2007, 98: 230501
66 Branciard C, Cavalcanti E G, Walborn S P, et al. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. Phys Rev A, 2012, 85: 010301
67 Pawlowski M, Brunner N. Semi-device-independent security of one-way quantum key distribution. Phys Rev A, 2011, 84: 010302

68 Gallego R, Brunner N, Hadley C, et al. Device-independent tests of classical and quantum dimensions. Phys Rev Lett, 2010, 105: 230501
69 Nayak A. Optimal lower bounds for quantum automata and random access codes. In: Proceedings of the 40th IEEE FOCS. New York: IEEE, 1999. 369–376
70 Li H W, Yin Z Q, Wu Y C, et al. Semi-device-independent random-number expansion without entanglement. Phys Rev A, 2011, 84: 034301
71 Li H W, Marcin P, Yin Z Q, et al. Semi-device independent random number expansion protocol with *n* to 1 quantum random access codes. Phys Rev A, 2012, 85: 052308
72 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503
73 Braunstein S, Pirandola S. Side-channel-free quantum key distribution. Phys Rev Lett, 2012, 108: 130502

Security of quantum key distribution

LI HongWei[1,2,3] , CHEN Wei[1*], HUANG JingZheng[1], YAO Yao[1], LIU Dong[1], LI FangYi[1], WANG Shuang[1*], YIN ZhenQiang[1*], HE DeYong[1], ZHOU Zheng[1], LI YuHu[1,2], YU NengHai[2] & HAN ZhengFu[1*]

[1] *Key Laboratory of Quantum Information,University of Science and Technology of China, Hefei* 230026*, China;*
[2] *Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei* 230026*, China;*
[3] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450004*, China*

In this work, three security models of quantum key distribution are introduced. The practical characters of the light source, the modulator and the single photon detector are analyzed, and the corresponding differences between the perfect and the practical quantum key distribution system are estimated. The details of the attacking methods and measures are described and investigated. We also focus on the device-independent class quantum key distribution protocol, which is a new important aspect of this research area.

quantum key distribution, protocol security, imperfect devices, system security

PACS: 03.67.Dd, 03.67.Hk, 03.65.Ud, 89.70.+c

doi: 10.1360/132012-761