基于 $\alpha\eta$ 协议的量子数据流加密系统实际安全与性能分析*

陆鸢† 黄鹏 朱俊 代文超 曾贵华

(上海交通大学区域光纤通信网与新型光通信系统国家重点实验室, 上海 200240)

(2011 年 7 月 4 日收到; 2011 年 11 月 3 日收到修改稿)

$\alpha\eta$ 协议是一种利用量子噪声隐藏信息的随机加密协议. 通过求解高斯噪声信道中窃听者获取信息量的计算公式, 推导了该协议实际安全判据. 结果表明, 协议是否安全主要取决于信源量子态的平均光子数和密文符号数. 基于此, 计算了在光束分离攻击下两者的安全取值区间以及协议的有效通信距离.

关键词: $\alpha\eta$ 协议, 安全性分析, 光束分离攻击

PACS: 03.67.Dd, 03.67.Hk

1 引 言

随着光通信技术的发展和量子信息理论的完备, 量子安全通信开始走向实用化 [1]. 现在达到实用条件的量子安全通信方法有两类, 一类是将量子密钥分发协议与经典加密算法相结合, 另一类是将量子加密算法与经典密钥分发相结合. 前者的代表性方案有 BB84 协议 [2] 和 B92 协议 [3], 后者的代表性方案有 $\alpha\eta$ 协议 [4]. 前一类方案利用量子密钥分发技术在通信双方共享一串随机密钥, 并通过信道监测、误码统计等方法判断是否存在窃听, 如果不存在窃听, 则认为分发的密钥是安全的. 结合经典加密算法 (如一次一密算法), 使用分发的密钥加密明文. 为了保证信息安全, 实现此类协议时要求系统分发的随机数必须是真随机数, 且密钥分发速率需要高于系统数据传输速率. 虽然从理论上有一些方法可以产生真随机数 [5−7], 但是由于非理想的实验条件 (如检测器的带宽受限、激光器输出功率抖动、采样系统的噪声、带外噪声串扰等), 实际生成的随机数无法达到无偏真随机的要求. 而且量子密钥分发效率较低, 生成的密钥速率也远低于数据传输需要的速率. 因此, 真正意义的一次一密无法实现. 一种可行的替代方案是将量子密钥分发所生成的安全密钥作为种子, 通过对称数学加密算法 (如美国数据加密标准或高级加密标准)[8−10] 加密信息. 显然, 这会降低原方案的实际安全性.

为了避免上述问题, 美国西北大学的 Yuen 提出了 $\alpha\eta$ 协议. 该协议采用宏观量子态作为信源, 利用量子态的相位噪声隐藏明文信息, 使窃听者无法提取信息, 合法用户能够通过预共享私钥, 在高信噪比条件下还原信息 [11]. 该协议适合高速数据加密, 其理论安全性已被证明 [12−15], 但在证明过程中并没有给出安全判据的定量表达式, 也没有考虑实际传输损耗和环境因素对系统安全性的影响. 本文将考虑高斯有损有噪信道条件下 $\alpha\eta$ 协议密钥与明文的实际安全性. 与基于最佳检测理论的安全分析模型 [11] 和基于辛变换的量子信息等价安全分析模型 [16] 不同, 本文通过计算多元高斯信道容量上界来得到窃听者可获取信息量的定量表达式, 推导出使窃听者获取零信息量的条件作为协议安全的判据. 针对光束分离攻击模型, 进一步求解满足安全判据的协议参数 (如量子态平均光子数、密文符号数) 取值区域. 为了评估协议的可用性, 将实验系统实测参数值代入到安全模型中, 计算满足安全条

* 国家自然科学基金 (批准号: 60970109, 60801051) 和国家高技术研究发展计划 (批准号: 2009AA01Z257) 资助的课题.

† E-mail: hawkfly_lu@hotmail.com

件时协议通信误码率, 并讨论通信距离对误码率的影响.

2 协议介绍

$\alpha\eta$ 协议工作原理如图 1 所示, 包括数据加密与解密两个过程. 协议利用相空间中非正交的量子信号集合表示明文信息. 发送方 Alice 利用预分发的密钥通过共轭算法将明文比特编码在量子态上, 接收方 Bob 使用相同密钥通过投影测量提取信息, 而窃听者 Eve 不知道密钥, 无法获取信息.

下面给出加解密的实现步骤.

步骤Ⅰ Alice 与 Bob 通过安全技术分发一串较短的主密钥 $K_{\rm m}$. 加密时, Alice 利用 Hash 算法, 由主密钥生成会话密钥 $K_{\rm s}$.

步骤Ⅱ Alice 将会话密钥划分为多个子串, 每个子串长为 $l_{\rm bit}$, 并生成加密密钥 $K.K = 2^l \bmod M$, 其中 M 是密文符号数, 为奇数.

步骤Ⅲ Alice 持续发送光脉冲序列, 通过光分束器后每个脉冲分为信号脉冲与参考脉冲. 信号光与参考光的相位差表示明文. 设明文比特为 s, $s \in \{0,\ 1\}$, 则相干态可表示为 $|(-1)^{1\oplus s}X_{\rm A}\rangle$.

步骤Ⅳ Alice 使用共轭编码生成密文态. 编码算法由下式给出:

$$\begin{aligned}|\alpha_{\rm c}\rangle &= \hat{U}(\phi_{\rm c})|(-1)^{1\oplus s}X_{\rm A}\rangle \\ &= |X_{\rm c} + {\rm j}P_{\rm c}\rangle,\end{aligned} \tag{1}$$

式中, $\hat{U}$ 是相移算符,

$$\phi_{\rm c} = K\frac{\pi}{M} - \pi(K \bmod 2).$$

所以密文态正则分量 $X_{\rm c}, P_{\rm c}$ 的均值可写为

$$\begin{aligned}\langle X_{\rm c}\rangle &= (-1)^{1\oplus s}\cos(\phi_{\rm c})\langle X_{\rm A}\rangle, \\ \langle P_{\rm c}\rangle &= (-1)^{1\oplus s}\sin(\phi_{\rm c})\langle X_{\rm A}\rangle.\end{aligned} \tag{2}$$

步骤Ⅴ Bob 使用分发的主密钥 $K_{\rm m}$ 生成解密密钥 K 对接收的量子密文态进行解密. 解密算法为

$$\begin{aligned}|\alpha_{\rm d}\rangle &= U(\phi_{\rm d})|\alpha_{\rm c}\rangle, \\ \phi_{\rm d} &= -K\frac{\pi}{M} + \pi(K \bmod 2).\end{aligned} \tag{3}$$

步骤Ⅵ 解密后, 量子态为 $|(-1)^{1\oplus s}X_{\rm B}\rangle$, 对于明文比特 $s \in \{0,1\}$, 其对应的相干态为 $|-X_{\rm B}\rangle, |X_{\rm B}\rangle$, 这两个态的内积为 ${\rm e}^{-2|X_{\rm B}|^2}$, 当 $X_{\rm B} \gg 1$ 时, 可以认为两者正交, 经投影测量还原明文.

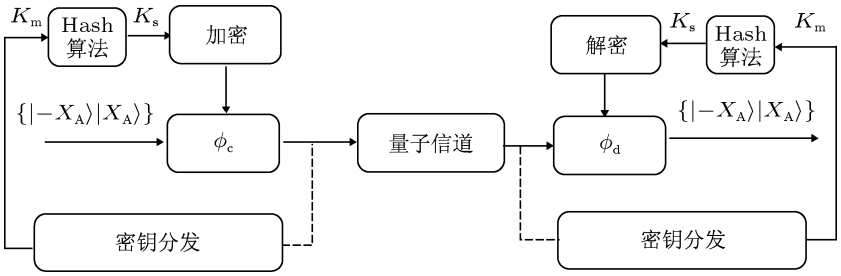

图 1 量子数据加解密原理框图

3 安全性分析

对于经典对称加密算法而言, 密文符号定义为 $\mathbb{C} = f(\mathbb{M}, \mathbb{K})$. 明文 $\mathbb{M}$ 和密钥 $\mathbb{K}$ 决定了密文 $\mathbb{C}$ 的值. Bob 和 Eve 能收到相同的密文. $\alpha\eta$ 加密协议使用非正交的量子态序列表示密文信息, 在不同测量基下观测量子态, 将得到不同的测量值, 且噪声也将影响测量结果. 所以, 此时密文符号应定义为 $\mathbb{C} = f(\mathbb{M}, \mathbb{K}, \mathbb{R}, \mathbb{N})$, 其中 $\mathbb{R}$ 表示不同的测量基, $\mathbb{N}$ 表示信道噪声. 由于 Eve 不知道合法通信方使用的测量基 $\mathbb{R}_{\rm B}$, 只能猜测不同的测量基 $\mathbb{R}_{\rm E}$, 所以 Eve 获得的密文 $\mathbb{C}_{\rm E}$ 不同于 Bob 方所测得的密文 $\mathbb{C}_{\rm B}$. 同时信道噪声 $\mathbb{N}$ 也会影响测量结果, 最终 $\mathbb{C}_{\rm E}$ 呈现随机分布. 因此, $\alpha\eta$ 协议属于随机加密协议 [17]. 文献 [17] 指出, 由于 Eve 不能获得正确的密文, 条件熵

$$H(\mathbb{M}|\mathbb{C}_{\rm E}, \mathbb{K}) > H(\mathbb{M}|\mathbb{C}_{\rm B}, \mathbb{K}). \tag{4}$$

这说明在通信结束后即使 Eve 从第三方得到了此次会话密钥, 也无法正确还原信息. 因此协议可以抵抗密文统计攻击, 达到信息论安全. 但是 (4) 式只

能说明 Eve 无法有效获取信息, 不能说明 Eve 获取的信息量为零, 也不能说明协议 100% 安全.

3.1 安全判据

量子保密通信系统安全可以从两方面考虑. 一方面, 要求系统发送密文序列时窃听者无法从中猜到密钥 K, 即 Alice 与 Eve 之间的密钥互信息量 $I(A,E)_{\rm key}=0$. 另一方面, 要求系统发送密文序列时窃听者无法从中还原明文比特 s, 即 Alice 与 Eve 之间明文互信息量 $I(A,E)_{\rm bit}=0$. 满足这两个方面可以看作是协议实际安全的判据. 下面给出 $I(A,E)_{\rm key}$ 和 $I(A,E)_{\rm bit}$ 的计算表达式, 并讨论协议密钥与明文的安全性.

首先, 讨论密钥安全性问题. 在协议中, 密文符号为 M 元非正交量子态. Alice 与 Eve 之间的信道可视为 M 元输入输出无记忆信道 [18]. 设 Alice 输入符号 m, Eve 输出符号 n 的概率为 $p(n|m)$, 则 Alice 和 Eve 两者互信息量上界为

$$\begin{aligned} I(A,E)_{key} =& H(E)-H(A|E) \\ \leqslant& \sum_{m=0}^{M-1}\sum_{n=0}^{M-1}\Big[\frac{1}{M}p(n|m)\Big(\log p(n|m) \\ &-\log\sum_{i=0}^{M-1}p(n|i)+\log M\Big)\Big]. \end{aligned} \tag{5}$$

当输入符号服从均匀分布时等号成立. Alice 符号概率 $p(m=i)=1/M$ $(i=0,1,2,\cdots,M-1)$, 服从等概率分布, 代入 (5) 式可得

$$\begin{aligned} I(A,E)_{\rm key} =& \sum_{n=0}^{M-1}p(n|m)\log p(n|m) \\ &-\frac{1}{M}\sum_{m=0}^{M-1}\sum_{n=0}^{M-1}p(n|m)\log\frac{1}{M} \\ =& \log M \\ &+\sum_{n=0}^{M-1}p(n|m)\log p(n|m). \end{aligned} \tag{6}$$

受到量子噪声的影响, 信道中符号错误转移概率随着符号间距离的增加而递减. 假设 Eve 总的接收误符号率为 $P_{\rm e}^{\rm EI}$, 则正确概率为

$$p(m|m)=1-P_{\rm e}^{\rm EI},$$

而平均符号错误转移概率为

$$p(n|m)=\frac{P_{\rm e}^{\rm EI}}{M-1}\quad(n\neq m).$$

(6) 式可化简为

$$\begin{aligned} I(A,E)_{\rm key} =& \log M-H(P_{\rm e}^{\rm EI}) \\ &-P_{\rm e}^{\rm EI}\log(M-1). \end{aligned} \tag{7}$$

由此可知, Eve 可窃取到的信息量由密文符号数 M 及 $P_{\rm e}^{\rm EI}$ 决定.

图 2 给出了 M 取不同值时, $I(A,E)_{\rm key}$ 与 $P_{\rm e}^{\rm EI}$ 之间的变化关系. 从图 2 可以看出, 当 M 给定时, 存在一个确定的误符号率 $P_{\rm e}^{\rm EI}$ 满足方程 $I(A,E)_{\rm key}=0$, 此时对密钥的保护是信息论安全的. 从图 2 还可以看出, 当 $M>20$ 时, 曲线趋向于单调减函数, 此时 $P_{\rm e}^{\rm EI}$ 越大, $I(A,E)_{\rm key}$ 越小, 泄漏的信息也越少.

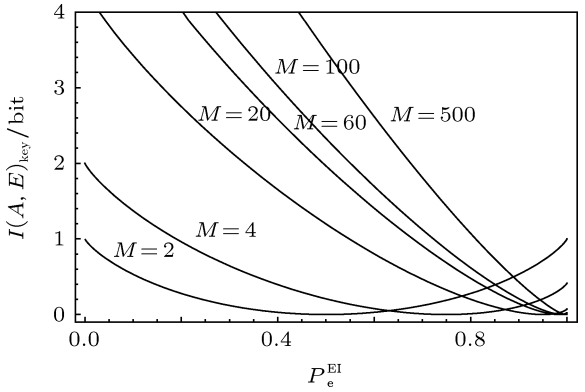

图 2 M 取不同值时, $I(A,E)_{\rm key}$ 与 $P_{\rm e}^{\rm EI}$ 的关系曲线

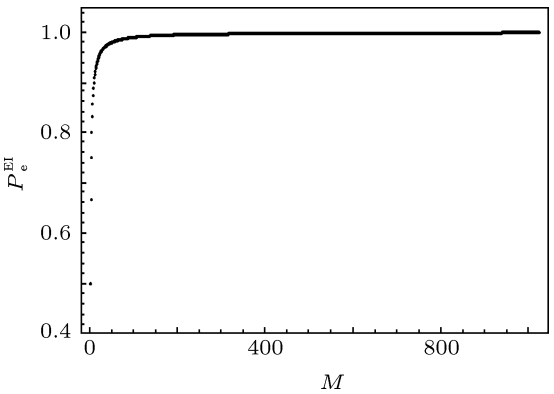

图 3 满足方程 $I(A,E)_{\rm key}=0$ 的 M 和 $P_{\rm e}^{\rm EI}$ 的取值

接着讨论明文的安全性问题. 由于协议中明文信息采用二进制编码, 实际上 Alice 与 Eve 之间的明文互信息量 $I(A,E)_{\rm bit}=1-H_{\rm bin}(P_{\rm e}^{\rm EB})$, $H_{\rm bin}(\cdot)$ 为二元熵, $P_{\rm e}^{\rm EB}$ 是 Eve 窃听明文的误比特率. 当 $P_{\rm e}^{\rm EB}=0.5$, $I(A,E)_{\rm bit}=0$ 时, 明文信息论安全条件得到满足. 因为 Alice 将明文均匀编码在 M 对非正交量子态上, 所以 $P_{\rm e}^{\rm EB}=\frac{1}{2}P_{\rm e}^{\rm EI}$. 我们通

过数值方法, 求解满足方程 $I(A,E)_{\rm key}=0$ 的 M 与 $P_{\rm e}^{\rm EI}$ 的取值, 结果如图 3 所示.

从图 3 可以看出, 随着 M 的增加, 满足方程 $I(A,E)_{\rm key}=0$ 的 $P_{\rm e}^{\rm EI}$ 趋近于 1, 此时 $P_{\rm e}^{\rm EB}$ 趋于 0.5, $I(A,E)_{\rm bit}$ 趋于零. 这说明 $I(A,E)_{\rm bit}=0$ 的条件只能渐近满足, 因此协议对于明文的保护是渐近安全的, 而不是信息论安全的. 这与文献 [11] 中采用基于半正定算子值测量模型的安全性分析结论是一致的.

从以上分析可以看出, $\alpha\eta$ 协议的安全取决于 M 的取值和 Eve 的接收误符号率, 而 Eve 的接收符号的错误率又与所采用窃听攻击策略和拥有的资源有关. 对于 Eve 而言, 一个可实用化的攻击手段是光束分离攻击. 因此我们假设 Eve 拥有理想的设备与无限的计算资源, 进一步分析光束分离攻击下系统参数的安全取值区间. 进行光束分离攻击时, 可采用平衡零差检测或平衡外差检测, 对这两种情况我们分别进行讨论.

3.2 采用平衡零差检测时系统参数的安全取值区间

首先计算 Eve 采用平衡零差检测时系统的安全取值区间. 实际光纤信道被假设为高斯有损有噪信道, 定义单位真空噪声 δx_0 服从均值为零方差为 1 的标准高斯分布 $N(0,1)$, 信道中其他噪声源方差以单位真空噪声方差进行归一化, 等效后量子信道模型如图 4 所示.

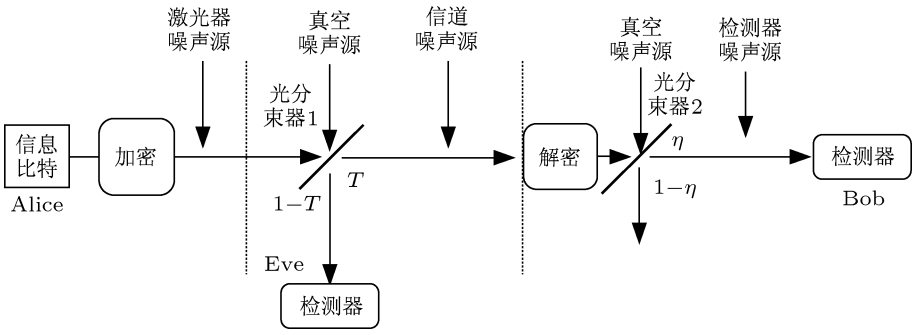

图 4 高斯有损有噪信道的等效模型

Alice 根据明文信息 $\{0,\ 1\}$ 比特生成对应的平移真空态 $\{|-X_{\rm A}\rangle,|X_{\rm A}\rangle\}$, 经过加密算法后生成随机相干态 $|X_{\rm c}\rangle$. 由于存在激光器相位调制噪声, 量子态送入量子信道之前会受到发送端内部分布为 $N(0,V_{\rm in})$ 噪声源 $\delta x_{\rm in}$ 的影响. 量子态经过传输率为 T 的信道, 到达 Bob 方. 光纤损耗等效为分光比为 T:$(1-T)$ 的光分束器 1, 由于能量损耗, 会耦合进真空噪声 δx_0. 量子态在传输的过程中会受到分布为 $N(0,V_{\rm ch})$ 的信道过噪声 $\delta x_{\rm ch}$ 的影响. 当 Bob 收到量子信号后, 根据解密算法还原明文, 信号由量子效率为 η 的平衡零差检测器进行检测. 检测器内部损耗等效为分光比为 $\eta:(1-\eta)$ 的光分束器 2. 检测器电噪声 $\delta x_{\rm el}$ 分布为 $N(0,V_{\rm el})$. 为了不降低 Bob 接收信号的信噪比, 使窃听行为不被合法通信方察觉, Eve 进行窃听时可以使用无损信道代替有损信道, 利用光分束器截取一部分信号能量进行窃听, Bob 接收信号不受影响. 这样, 合法用户将无法发现窃听行为.

当 Eve 采用最优平衡零差检测器检测截取的量子信号时, Eve 得到的密文态可由正则算符 $\hat{X}_{\rm E}$ 和相应的方差 $V_{\rm E}$ 描述 [19], 即

$$\begin{aligned}\hat{X}_{\rm E}&=\sqrt{1-T}(\hat{X}_{\rm c}+\delta x_{\rm in})+\sqrt{T}\delta x_0,\\ V_{\rm E}&=(1-T)(\chi_{\rm A}+\chi_{\rm line}^{\rm Hom}),\end{aligned}\tag{8}$$

式中

$$\chi_{\rm A}=1+V_{\rm in},$$
$$\chi_{\rm line}^{\rm Hom}=\frac{T}{1-T}.$$

Eve 要得到明文和密钥需要同时测量正则分量 $X_{\rm E}$ 和 $P_{\rm E}$. (1) 式说明 Eve 采用平衡零差检测时, 最优的策略是精确测量其中一个值, 同时猜测正确的密文态是处于 $[0,\pi]$ 区间还是 $[\pi,2\pi]$ 区间. 假设

Eve 测量 $X_{\rm E}$, 她有一半的概率猜错区间而误码. 对于猜对的那一半概率, 由于量子噪声的影响其输出量子态的正则分量 $X_{\rm E}$ 服从以 $\langle \hat{X}_{\rm E}\rangle$ 为均值, 以 $V_{\rm E}$ 为方差的高斯随机分布. Eve 的误符号率由下式给出:

$$P_{\rm e}^{\rm EI} = 1-\frac{1}{2}\left(\sum_{k=0}^{M-1} P(X=X_{\rm c})P\left(X_{\rm c}-\frac{\Delta_k}{2} < X_{\rm E} < X_{\rm c}+\frac{\Delta_k}{2}\middle| X=X_{\rm c}\right)\right). \tag{9}$$

这里 Δ_k 为密文相邻符号间距离,

$$\Delta_k = \sqrt{(1-T)\mu}\left[\cos\left(\frac{k\pi}{M}\right) - \cos\left(\frac{(k+1)\pi}{M}\right)\right],$$

其中 μ 为信号脉冲的平均光子数. 经计算可得

$$\begin{aligned} P_{\rm e}^{\rm EI} &= \frac{1}{2}+\frac{1}{2M}\left(\sum_{k=0}^{M-1}\mathrm{erfc}\left[\frac{\Delta_k}{2\sqrt{2V_{\rm E}}}\right] - \frac{1}{2}\mathrm{erfc}\left[\frac{\Delta_0}{2\sqrt{2V_{\rm E}}}\right]\right) \\ &= \frac{1}{2}+\frac{1}{2M}\left(\sum_{k=0}^{M-1}\mathrm{erfc}\left[\sqrt{\frac{R_{\rm E}}{8}} \times\left(\cos\left(\frac{k\pi}{M}\right)-\cos\left(\frac{(k+1)\pi}{M}\right)\right)\right] - \frac{1}{2}\mathrm{erfc}\left[\sqrt{\frac{R_{\rm E}}{8}}\left(1-\cos\left(\frac{\pi}{M}\right)\right)\right]\right), \end{aligned} \tag{10}$$

式中, $\mathrm{erfc}(\cdot)$ 为补余误差函数, $R_{\rm E}$ 为 Eve 接收的信号能量与噪声能量之比,

$$R_{\rm E} = \frac{\mu}{\chi_{\rm A}+\chi_{\rm line}^{\rm Hom}}.$$

(10) 式说明 Eve 的误符号率不仅与密文符号数有关, 也与信噪比有关. Alice 增大 M 值可以使得 Eve 的误符号率无限逼近于 100%, 近似满足明文安全条件 $I(A,E)_{\rm bit}=0$. 将 (10) 式代入方程 $I(A,E)_{\rm key}=0$ 可以求解满足密钥安全条件的信号脉冲平均光子数 μ.

为了最大化 Eve 窃听能力, 我们假设 Eve 可以通过信道截断得到所有信号功率 ($T=0$). 在此条件下, 将 (9) 式代入方程 $I(A,E)=0$, 求解不同密文符号 M 值下相应的信号平均光子数 μ.

图 5 给出了密文符号数与信号脉冲平均光子数的安全取值区域. 从图 5 可以看出, 当密文符号数越多时, 所允许的信号发射功率也就越大. 当 $M=101$ 时, 安全平均光子数上限 $\mu=31$. 当 $M=511$ 时, 安全平均光子数上限 $\mu=124$. 当 $M=1023$ 时, 安全平均光子数上限 $\mu=264$. 理论上 M 取值可以趋于无穷大, 但是 M 取值越大, 意味着信号需要调制的符号数也越多, 实现起来也更困难. 考虑到模拟调制电路实用性, 文中 M 取值小于 1024. 在图 5 所示的安全区域内, 对密钥保护是信息论安全的, 明文信息泄漏量 $I(A,E)_{\rm bit}\leqslant 7.2\times10^{-5}$ bit.

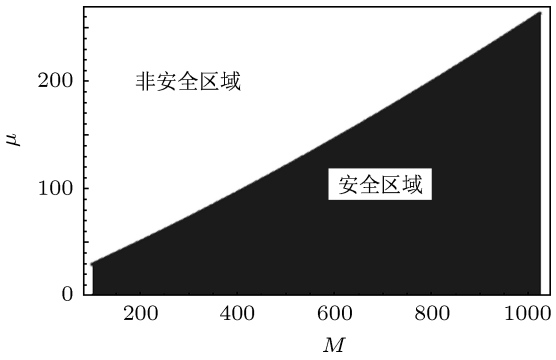

图 5 采用平衡零差检测, $T=0, V_{\rm in}=0$ 时, 满足 $I(A,E)_{\rm key}=0$ 的 M 与 μ 之间的关系

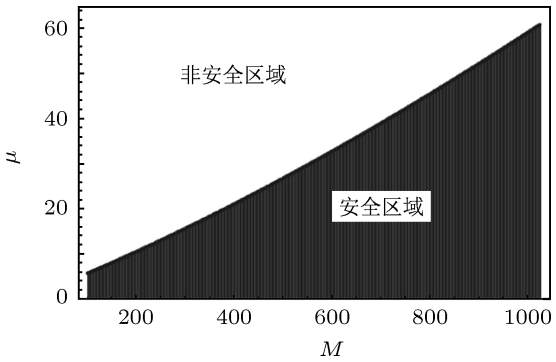

图 6 采用平衡零差检测, $T=0, V_{\rm in}=0$ 时, 已知明文攻击下满足 $I(A,E)_{\rm key}=0$ 的 M 与 μ 之间的关系

如果 Eve 已经知道所截获密文对应的明文以及相应的编码规则, 可以实现已知明文攻击, 即 Eve 知道密文量子态正则分量处于相空间 $[0,\pi]$ 区间还是 $[\pi,2\pi]$ 区间. 因此新的误符号率 $P_{\rm e}^{\rm EI'}=2P_{\rm e}^{\rm EI}-1$. 图 6 给出了相同信道条件下, 已知明文攻击时密文符号数与 Alice 发射脉冲的平均光子数之间的关系. 由图 6 可知, 为抵抗已知明文攻击, Alice 需要能量更弱的相干态. 当 $M=101$ 时, 所需的平均光子数 $\mu=7$. 当 $M=501$ 时, 所需的平均光子

数 $\mu = 34$. 当 $M = 1023$ 时, $\mu = 76$. 由以所述可知, 抵抗已知明文攻击的安全条件要比唯密文攻击更难满足.

3.3 采用平衡外差检测时系统参数的安全取值区间

平衡外差检测原理如图 7 所示, Eve 可同时得到正则分量 $\langle \hat{X}_{\rm E} \rangle$ 和 $\langle \hat{P}_{\rm E} \rangle$ 的值. 由于检测器使用光分束器会引入真空噪声, 因此 Eve 的接收信噪比将下降一半.

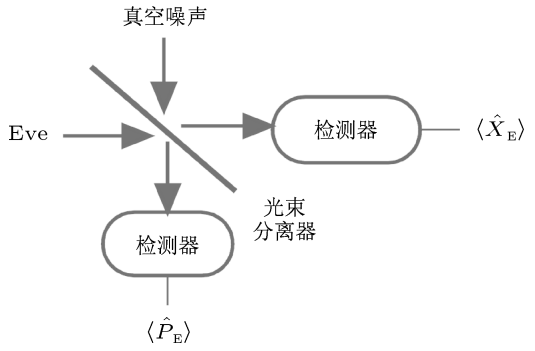

图 7 平衡外差检测原理图

Eve 输出的密文量子态的算符 $\hat{X}_{\rm E}$ 和 $\hat{P}_{\rm E}$ 为

$$\begin{aligned}\hat{X}_{\rm E} =& \frac{1}{\sqrt{2}}\Big(\sqrt{1-T}(\hat{X}_{\rm c}+\delta x_{\rm in})+\sqrt{T}\delta x_0\Big)\\ &+\frac{1}{\sqrt{2}}\delta x_0,\\ \hat{P}_{\rm E} =& \frac{1}{\sqrt{2}}\Big(\sqrt{1-T}(\hat{P}_{\rm c}+\delta x_{\rm in})+\sqrt{T}\delta x_0\Big)\\ &+\frac{1}{\sqrt{2}}\delta x_0.\end{aligned} \tag{11}$$

两者具有相同的方差

$$V_{\rm E} = \frac{1-T}{2}(\chi_{\rm A}+\chi_{\rm line}^{\rm Het}),$$

其中

$$\chi_{\rm line}^{\rm Het} = \frac{T+1}{1-T}.$$

从 (11) 式可知, Eve 的信噪比下降为原来的一半. 此时 Eve 的误符号率

$$\begin{aligned}P_{\rm e}^{\rm EI} =& 1-\Bigg(\sum_{k=0}^{M-1}P(X=X_{\rm c};P=P_{\rm c})\\ &\times P\Big(X_{\rm c}-\frac{\Delta_k}{2}<X_{\rm E}<X_{\rm c}\\ &+\frac{\Delta_k}{2}\Big|X=X_{\rm c};P_{\rm E}>0|P=P_{\rm c}\Big)\\ &+\sum_{k=M}^{2M-1}P(X=X_{\rm c};P=-P_{\rm c})P\Big(X_{\rm c}-\frac{\Delta_k}{2}\\ &<X_{\rm E}<X_{\rm c}+\frac{\Delta_k}{2}\Big|X=X_{\rm c};\\ &P_{\rm E}<0|P=-P_{\rm c}\Big)\Bigg)\\ =& 1-\frac{1}{M}\Bigg(\sum_{k=1}^{M-1}\delta(P_{\rm c})\delta(|\Delta_k|)+\frac{1}{2}\\ &+\frac{1}{2}{\rm erf}\big[\delta(|\Delta_0|)\big]\Bigg),\end{aligned} \tag{12}$$

式中,

$$\begin{aligned}\delta(P_{\rm c}) =& \frac{1}{2}+\frac{1}{2}{\rm erf}\left[\sqrt{\frac{(1-T)\mu}{V_{\rm E}}}\sin\left(\frac{k\pi}{M}\right)\right],\\ \delta(|\Delta_k|) =& \left|{\rm erf}\left[\frac{|\Delta_k|}{2\sqrt{2V_{\rm E}}}\right]\right|,\\ \Delta_k =& \sqrt{\frac{(1-T)\mu}{2}}\\ &\times\left(\cos\left(\frac{k\pi}{M}\right)-\cos\left(\frac{(k+1)\pi}{M}\right)\right).\end{aligned}$$

将 (12) 式代入方程 $I(A,E)_{\rm key} = 0$ 得到 M 与 μ 的关系, 结果如图 8 所示. 图 8 表明, 对于窃听者而言, 使用平衡外差检测要优于平衡零差检测. 当 Eve 采用平衡外差检测时, 虽然会引入额外的真空噪声, 但是 Eve 的检测结果也将更加精确, 因此合法用户需要使用更严格的参数来保证系统安全.

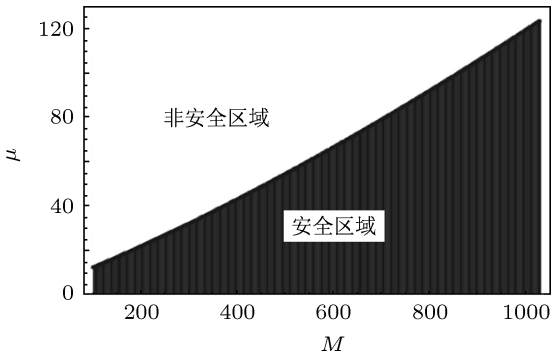

图 8 采用平衡外差检测, $T = 0$, $V_{\rm in} = 0$ 时, 满足 $I(A,E)_{\rm key} = 0$ 的 M 与 μ 之间的关系

结合图 5、图 6 和图 8 的仿真结果可知, 相同信道条件下, Eve 采用已知明文攻击时满足系统安全条件最困难. 图 6 给出了抵抗光束分离攻击系统参数最安全的取值区间.

4 $\alpha\eta$ 协议在光纤通信系统中的应用

为了评估 $\alpha\eta$ 协议在实际光通信系统中运行安全性, 我们在实验室环境下搭建了相应的实验光路. 利用实验光路测量了单模光纤信道中相关的信道参数值. 根据这些参数, 进一步分析协议在实际应用环境下的安全性, 并讨论了通信距离对通信误码率的影响.

图 9 给出了我们的实验装置示意图, 所用光路基于双不等臂麦克尔逊干涉仪结构. Alice 方使用短脉冲激光器发送的光脉冲序列, 脉冲序列被 1:99 的光分束器分为信号光和本振光两路. 其中信号光走长臂, 参考光走短臂. 信号臂中使用电光强度调制器将信号光衰减到 -80 dBm(此时平均光子数约为 150). 使用电光相位调制器完成协议加密. 加密后的信号脉冲使用三环偏振控制器调整偏振状态, 使信号光偏振与参考光偏振正交, 再通过偏振合束器复用进单模光纤信道. Bob 方通过前置的一个动态偏振控制器调整信号光与本振光脉冲的偏振态, 再使用偏振分束器将偏振正交复用的信号光与本振光分开, 分开后的信号光走短臂, 而本振光走长臂. 本振臂使用电光相位调制器完成信号解密. 收发双方的不等臂干涉仪长短臂的臂长差要求相等, 经过校准实际误差小于 2 mm. 信号光与本振光在光分束器端口发生一阶干涉, 相干检测结果送入计算机完成后续处理. 实验系统中采用的数模转换电路位宽 12 bit, 这里 $M = 1023$.

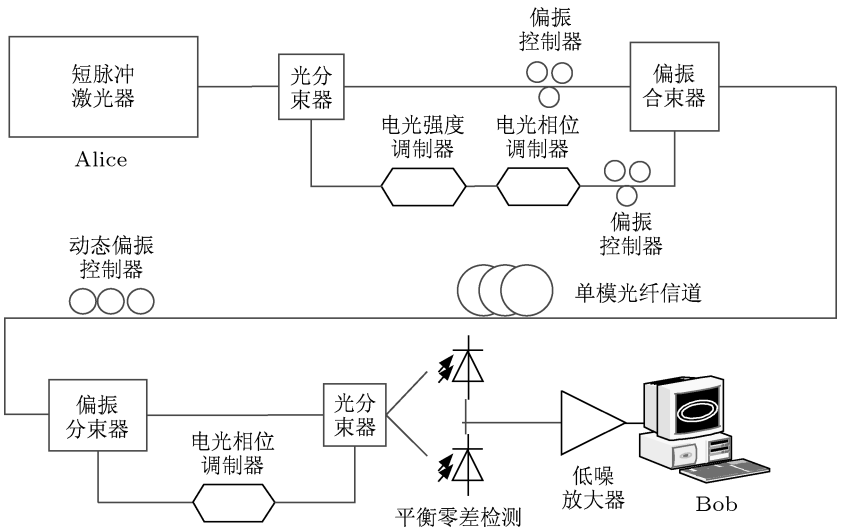

图 9 基于双不等臂麦克尔逊干涉仪结构的 $\alpha\eta$ 量子数据流加密实验装置示意图

Bob 作为合法用户, 能够选择正确的测量基进行测量. 因此连接 Alice 和 Bob 的量子信道可视为二元对称信道. 描述 Bob 方接收量子态的正则算符 $\hat{X}_{\rm B}$ 及相应的方差 $V_{\rm B}$ 分别为

$$\begin{aligned}\hat{X}_{\rm B} =&\sqrt{\eta}\big[\sqrt{T}(\hat{X}_A+\delta x_{\rm in})+\sqrt{1-T}\delta x_0\\&+\delta x_{\rm ch}\big]+\sqrt{1-\eta}\delta x_0^{\rm H}+\delta x_{\rm el},\\ V_{\rm B} =&T\eta\left(\chi_{\rm A}+\chi_{\rm line}+\frac{\chi_{\rm Hom}}{T}\right),\end{aligned}\tag{13}$$

式中,

$$\chi_{\rm line}=\frac{1-T}{T}+V_{\rm ch},$$
$$\chi_{\rm Hom}=\frac{1-\eta+V_{\rm el}}{\eta}.$$

经计算 Bob 的误码率

$$\begin{aligned}P_{\rm e}^{\rm BI} =& P(X_{\rm B}<0|X=X_{\rm A})P(X=X_{\rm A})\\&+P(X_{\rm B}>0|X=-X_{\rm A})P(X=-X_{\rm A})\\=&\frac{1}{2}{\rm erfc}\left[\frac{\sqrt{T\eta\mu}}{\sqrt{2V_{\rm B}}}\right].\end{aligned}\tag{14}$$

(14) 式表明 Bob 采用二元判决时, 其误码率由接收信噪比 $R_{\rm B}=\dfrac{\mu}{V_{\rm B}}$ 决定. 在发射平均光子数给定的前提下, 提高 Bob 的接收信噪比主要靠降低接收噪声总方差 $V_{\rm B}$ 实现. 降低接收噪声总方差有以下两类方法: 一是提高检测器量子效率 η, 等效于降低平衡零差检测器内部噪声方差 $\chi_{\rm Hom}$. 二是降低信道中各部噪声源方差, 如发送方内部噪声 $\delta x_{\rm in}$、信道过噪声 $\delta x_{\rm ch}$ 以及平衡零差检测器内部噪声 $\delta x_{\rm el}$.

根据文献 [20] 的方法, 我们测量了实验系统参数值, 统计了各噪声源方差. 经过测量得到发送方调制引起的内部噪声方差 $V_{\rm in} = 0.023N_0$, 信道过噪声方差 $V_{\rm ch} = 0.018N_0$, 平衡零差检测器的量子效率为 $\eta = 0.526$, 电噪声方差 $V_{\rm el} = 0.04361N_0$. 这里 N_0 是在本振光强度 -28 dBm 的情况下所测得的单位真空噪声方差.

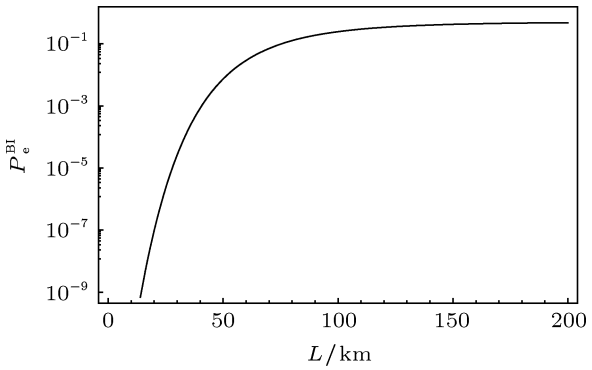

图 10 平均光子数 $\mu = 76$ 时, Bob 的接收误码率 $P_{\rm e}^{\rm BI}$ 与传输距离 L 的关系

将上述参数值代入 (7) 式和 (9) 式, 得到 $T = 0$ 时 Alice 安全发送光子数 $\mu = 76$.

由实测参数, 我们仿真了平均光子数 $\mu = 76$ 时 Bob 的接收信噪比与通信距离之间的关系, 图 10 给出了仿真结果. 从图 10 可以看出, Bob 的接收误码率随着通信距离的增加而增加. 为了保证用户之间的通信质量, Bob 接收误码率应小于 0.1%, 因此系统的有效通信距离约为 40 km.

5 结 论

本文给出了判定高斯有损有噪信道中 $\alpha\eta$ 协议实际安全的方法. 通过计算窃听者获取的信息量, 推导了该协议的安全判据. 结果表明, 协议对密钥的保护是信息论安全, 对明文的保护是渐近安全, 而影响安全性的关键参数是信源平均光子数和密文符号数. 信源通过选择平均光子数较低的弱相干态与较大的密文符号数, 可以满足协议安全条件. 本文进一步计算了光束分离攻击下平均光子数和密文符号数的最优取值区域. 实验表明协议的有效安全通信距离约为 40 km, 合法用户的明文误码率低于 0.1%. 这为设计实用化量子加密系统提供了重要的依据.

[1] Zeng G H 2010 *Quantum Private Communication* (Berlin: Springer-Verlag) pp112—117

[2] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore: IEEE) pp175—179

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

[4] Yuen H P, Kim A M 1998 *Phys. Lett.* A **241** 135

[5] Zhu Y Y, Lu Y, Zhu J, Zeng G H 2011 *Int. J. Quantum Inform.* **9** 1113

[6] Gabriel C, Wittmann C, Sych D, Dong R F, Mauerer W, Andersen U L, Marquardt C, Leuchs G 2010 *Nat. Photon.* **4** 711

[7] Fürst M, Weier H, Nauerth S, Marangon D G, Kurtsiefer C, Weinfurter H 2010 *Opt. Express* **18** 13029

[8] Mayers D 2001 *Assoc. Comput. Mechan.* **48** 351

[9] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K, Yamamoto Y 2007 *Nat. Photon.* **1** 343

[10] Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Miki S, Yamashita T, Wang Z, Tanaka A, Yoshino K, Nambu Y, Takahashi S, Tajima A, Tomita A, Domeki T, Hasegawa T, Sakai Y, Kobayashi H, Asai T, Shimizu K, Tokura T, Tsurumaru T, Matsui M, Honjo T, Tamaki K, Takesue H, Tokura Y, Dynes J F, Dixon A R, Sharpe A W, Yuan Z L, Shields A J, Uchikoga S, Legr M, Robyr S, Trinkler P, Monat L, Page J B, Ribordy G, Poppe A, Allacher A, Maurhart O, Länger T, Peev M, Zeilinger A 2011 *Opt. Express* **19** 10387

[11] Barbosa G A, Corndorf E, Kumar P, Yuen H P 2003 *Phys. Rev. Lett.* **90** 22

[12] Corndorf E, Liang C, Kanter G S, Kumar P, Yuen H P 2005 *Phys. Rev.* A **71** 062326

[13] Yuen H P, Nair R, Corndorf E, Kanter G S, Kumar P 2006 *Quantum Inform. Comput.* **6** 561

[14] Hirota O 2007 *Phys. Rev.* A **76** 032307

[15] Hirota O, Kurosawa K 2007 *Quantum Inform. Process.* **6** 81

[16] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R, Grangier P 2003 *Quantum Inform. Comput.* **3** 535

[17] Nair R, Yuen H P, Corndorf E, Eguchi T, Kumar P 2006 *Phys. Rev.* A **74** 052309

[18] Thomas M C, Joy A T 1991 *Elements of Information Theory* (New York: Wiley) pp183—194

[19] He G Q, Guo H B, Li Y D, Zhu S W, Zeng G H 2008 *Acta Phys. Sin.* **57** 2212 (in Chinese) [何广强, 郭红斌, 李昱丹, 朱思维, 曾贵华 2008 物理学报 **57** 2212]

[20] Lodewyck J, Bloch M, Garcia-Patron R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W, Grangier P 2007 *Phys. Rev.* A **76** 042305

The practical security and performance analysis of the quantum data stream cipher system by the $\alpha\eta$ protocol*

Lu Yuan† Huang Peng Zhu Jun Dai Wen-Chao Zeng Gui-Hua

(*State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiaotong University, Shanghai* 200240*, China*)

(Received 4 July 2011; revised manuscript received 3 November 2011)

Abstract

The $\alpha\eta$ protocol is the random cipher protocol and hides information by the quantum phase noise. In this paper, the security criterion of the protocol is deduced by developing a quantum channel model and calculating the amount of information obtained by the eavesdropper. The results show the security of the protocol depends mainly on the average photon number of the signal quantum states and the number of cipher-text symbols. Considering the above factors, the secure value region of the average photon number and cipher-text symbol number is calculated, which is against the beam splitter attack. Furthermore, the effective communication distance is simulated.

Keywords: $\alpha\eta$ protocol, security analysis, beam splitter attack

PACS: 03.67.Dd, 03.67.Hk

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60970109, 60801051) and the National High Technology Research and Development Program of China (Grant No. 2009AA01Z257).

† E-mail: hawkfly_lu@hotmail. com