第 58 卷 第 1 期 2009 年 1 月
1000-3290/2009/58(01)/0073-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.1,January,2009

量子密码协议的错误序列模型分析*

张 盛† 王 剑 张 权 唐朝京

(国防科学技术大学电子科学与工程学院,长沙 410073)

(2008 年 4 月 2 日收到;2008 年 6 月 19 日收到修改稿)

量子密码协议具有无条件安全特性,其安全性通过窃听检测来保证.为了提高信息序列错误率的估计值精确度,提出了一种错误序列模型分析方法,通过构造法得到错误序列的二阶统计特性,从而通过经典方法对信息序列中错误序列进行预测,最后得到信息序列的错误率.在单次运行协议情况下,提高了窃听检测的精度,适用于其他量子密码协议.

关键词:量子密码,最佳预测,窃听检测,序列重构

PACC:0367,4250

1. 引 言

经典密码协议是基于某个数学难题或计算复杂度来保证信息的安全,而量子密码协议则是在物理本质上实现了真正意义上的信息安全.任何对量子信道进行窃听的行为都会留下痕迹,因而可以通过量子手段检测到窃听者的存在.量子密码协议的窃听可检测性使得其具有无条件安全特性[1—5].其中随机检测在量子密码协议的窃听检测中具有重要的作用.目前,窃听检测主要是通过比较错误率来确定有无窃听行为,如果检测序列的错误率小于最大错误容忍率,则认为信道是安全的.文献[4]利用随机检测的统计特性对窃听检测的可靠性给予了理论上的证明.但是,在单次运行 QKD 协议[6—8]情况下,检测序列的错误率可能与信息序列的错误率不一致.而且检测序列的选取及其长度都会使得单次信息序列的错误率偏离检测序列的错误率.为了提高单次信息序列的错误率估计精度,提出一种错误序列的模型分析方法,增强单次窃听检测的可靠性.

2. 量子密码协议的错误序列模型分析

2.1. QKD 协议的随机平稳性

信号在量子信道的传输过程中,由于攻击者的窃听行为以及信道噪声的影响,导致了 Alice 和 Bob 最后建立的密钥不一致.同时,Alice 的制备基 $b(n)$ 和 Bob 的测量基 $b'(n)$ 的随机性,最终密钥在协议运行前是完全随机的.因此可以将量子密钥的分配过程看成一个随机过程.

设 $K(m)$ 和 $V(m)$ 分别表示最终密钥以及窃听者 Eve 通过窃听得到的密钥,定义随机过程

$$\begin{aligned} &p(k_0,k_1,\cdots,k_m;v_0,v_1,\cdots,v_m,m)\\ &=p(K(0)=k_0,K(1)=k_1,\cdots,K(m)=k_m;\\ &\quad V(0)=v_0,V(1)=v_1,\cdots,V(m)=v_m), \end{aligned} \tag{1}$$

其中 k_i 和 v_i 的取值为 0 或 1.

为了便于分析,定义序列 $c(n)$,其中 $c(i)=b(i)\oplus b'(i)$.

根据密钥定义,容易得到 k_i 的概率分布函数 $p(K(i)=k_i)=\sum_{K(i)=k_i}p(K)$,于是可以得到 $K(i)$ 的数学期望 $m_{K(i)}=E[K(i)]=\sum_{k_i=0,1}k_ip(K(i)=k_i)=\sum_{k_i=0,1}k_i\sum_{K(i)=k_i}p(K)$,显然 $m_{K(i)}$ 与时间 i 无关.另外,Alice 拥有的比特串 $b(n)$ 是随机的,任意两个不同的比特位 $b(i)$ 与 $b(j)$ 两两相互独立.假设 Eve 采用最简单的截取重发攻击,截获一个量子比特 $A(i)$ 后便执行测量,由于 Eve 不知道 $A(i)$ 的制备基,他以 50% 的概率猜对 $A(i)$ 的制备基,此时 Eve 可以通过对 $A(i)$ 的测量获得经典比特 $a(i)$ 值,如

* 国家自然科学基金(批准号:60472032)资助的课题.

† E-mail:huoxingren112@163.com

果 Eve 采用的是相反的基对 $A(i)$ 进行测量,便会引入错误,此时的误码率达到 25%.根据以上的分析,可以知道在截取重发攻击下,每一位密钥的误码率为 25%,并且跟位置 i 是无关的.

同时,由于在随机检测中关心的是检测序列的错误率,它直接反映了信息序列的错误率,对信息序列中哪位出错并不关心,正因为这种与位置无关的特性,所以可以把错误序列看做是随机平稳过程来考虑.

2.2. 错误序列 $e(n)$ 的预测模型及序列 $e(n)$ 的统计特性

假设 $\{e(n)\}$ 表示 n 位量子比特串总的错误序列,$e(i)=1$ 表示对应的量子位出错(根据后面将介绍的序列重构法可知,$e(i)=1$ 并不一定表示第 i 量子比特位出错).Alice 随机选择 m 位量子比特组成检测序列,通过比较测试结果得到检测序列的错误序列 $\{e(m)\}$,然后根据已知的 $\{e(m)\}$ 对余下的信息序列中的错误序列 $\{e(n-m)\}$ 进行预测,从而得到完整的错误序列 $\{e(n)\}$.其原理图 1.

从图 1 可以看出,在预测器前,需要进行序列重构,然后预测器输出序列 $E(n-m)$,这个序列不是二进制比特串,需要进行波形重整后,才能得到二进制错误序列 $e(n-m)$.关于序列重构和波形重整将在后面介绍.

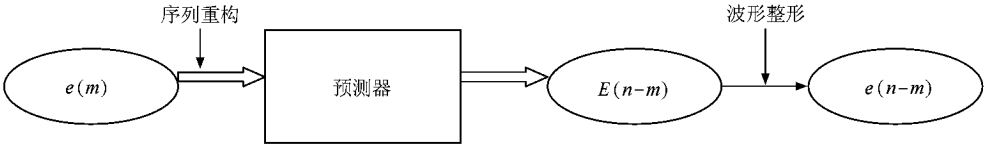

图 1 错误序列预测原理图

为了获得量子信道的错误序列的统计规律,利用了文献[4]中的数学工具,即 QKD 协议的 POVM 模型.根据这个模型,利用类比的方法,得到一种新的经典通信信道模型.经比较得到结论,量子信道虽然不同于经典信道,但是其统计特性与经典信道相似.因此,可以将经典信道的信号处理方法应用到量子信道的分析中.

已知 $\hat{v}=(\hat{c},\hat{q})$ 为协议的最后输出结果,定义 $v=(c,q)$ 为 Eve 的观测量,包括经典部分 c 和量子部分 q.可以认为 $v=V(\hat{v})$,即 Eve 观测量是结果 $\hat{v}$ 的函数.设 H^Q 为寄存器的态空间,于是定义 $E_{\hat{q}|\hat{c}}$ 是作用在 $H^Q\times\hat{C}$ 上的 POVM 算子,相应的结果为 $\hat{v}=(\hat{c},\hat{q})$,于是可以得到 $\hat{v}=(\hat{c},\hat{q})$ 的概率为

$$p_{\hat{v}}(\hat{c},\hat{q})=p_{\hat{c}}(\hat{c})\,Tr_Q(E_{\hat{q}|\hat{c}}\,|\,\Psi(\hat{c})\rangle\langle\Psi(\hat{c})\,|). \tag{2}$$

设 Eve 观测量 $v=(c,q)$ 满足条件 $C1$[4] 和 $C2$[4],可以得到概率 $p(v)$ 的表达式

$$p(v)=p(c:q)\mathrm{Tr}(E_{q|c}\rho_{c|q}), \tag{3}$$

其中

$$\rho_{c|q}\overset{\mathrm{def}}{=}p^{-1}(c:q)\sum_{\hat{c}|c(\hat{c},q)=c}p(\hat{c})\,|\,\Psi(\hat{c})\rangle\langle\Psi(\hat{c})\,|,$$

$$p(c:q)\overset{\mathrm{def}}{=}\sum_{\hat{c}|c(\hat{c},q)=c}p(\hat{c}).$$

Eve 获得信息 v 的同时也引入了错误,设此时的错误序列为 $\{e(n)\}$,显然 $\{e(n)\}$ 是观测量 v 的函数,因此 $\{e(n)\}$ 的概率

$$p(\{e(n)\})=p(v)=p(c:q)\mathrm{Tr}(E_{q|c}\rho_{c|q}). \tag{4}$$

从(4)式看出,$\{e(n)\}$ 的概率是完全随机的,与位置 n 以及测量基 $b(n)$ 无关.

在经典通信中,信道经常收到噪声的影响,因此信息序列也受到污染,接收端的序列是信息序列与错误序列之和,其简化模型如图 2.

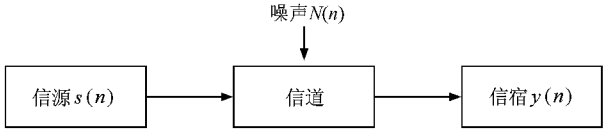

图 2 经典通信模型

图 2 中的 $y(n)=s(n)+z(n)$.如果将经典比特看作是非相干叠加态,则经典通信可以看作是量子通信的特例,设 $|\alpha\rangle=a|0\rangle+b|1\rangle$,($|a|^2+|b|^2=1$),当 $a=0$ 或 $b=0$ 时,$|\alpha\rangle$ 便是经典比特.为了方便比较,定义 $|s(n)\rangle^{C}{}^{C}\langle s(n)+N(n)|$ 为经典的相互正交态,H^C 为相应的希尔伯特空间,F_y 为 H^C 中的正交投影测量算子,根据以上定义,可以得到噪声序列(或错误序列)的概率

$$P(\{e(n)\})=p(\{s(n)\})\mathrm{Tr}(F_y|s(n)+N(n)\rangle^{CC}\langle s(n)+N(n)|). \tag{5}$$

比较(4)和(5)式,可以看出量子信道中的错误

序列与经典信道中的错误序列具有相似的统计特性.通常,经典信道中的噪声是窄带高斯白噪声,可以通过信号处理的方法去除噪声的影响,得到信息序列.量子信道虽然也具有类似高斯白噪声信道的统计特性,但是其错误序列的获得过程又完全不同于经典的错误序列产生过程,经典通信中,要经过解调,判决等步骤,才能得到最终的错误序列,而 QKD 协议中,错误序列的产生是因为量子态受到 Eve 的扰动,从纯态转变成混合态,即使 Bob 采用了和 Alice 的制备基一致的测量基,也可能得到不一致的结果.所以,不能简单地采用经典信号处理模型分析 QKD 协议中的错误序列,因此提出序列重构和波形整形,使得经典的信号处理方法可用于量子密码协议.

2.3. 序列重构

图 1 中的预测器可以采用最佳单步预测器.为了得到单步预测器的系数矢量 $H = (h(0), h(1), \cdots, h(M))^{\mathrm{T}}$,需要已知输入信号 $\{x(n)\}$ 的二阶统计特性,即自相关序列 $\{r(m)\}$,然后通过求解正则方程,求得预测器的滤波系数矢量 H.假设 $\{x(n)\}$ 是实序列,则

$$r(m) = E[x(n)x(n+m)]. \tag{6}$$

量子密钥分配协议中的错误序列是与位置无关的,不同位置的比特值相互独立,即

$$p(e(i), e(j)) = p(e(i))p(e(j)) \quad (i \neq j). \tag{7}$$

根据(6)和(7)式可以得到 QKD 协议的错误序列 $\{e(n)\}$ 的自相关函数

$$\begin{aligned} r(m) &= \sum_{e(i)=0,1} \sum_{e(i+m)=0,1} e(i)e(i+m) \\ &\quad \times p(e(i), e(i+m)) \\ &= \sum_{e(i)=0,1} \sum_{e(i+m)=0,1} e(i)e(i+m) \\ &\quad \times p(e(i))p(e(i+m)). \end{aligned} \tag{8}$$

由于量子密钥协议是无条件安全的,对于 Eve 的任何攻击策略,存在一个误码率上限 P_m,假设 $p(e(i)) = P_m$,可以推出,QKD 协议的错误序列 $\{e(n)\}$ 的自相关函数为一常数 c,此时单步预测器的正则方程将退化为一元一次方程,即 $h(1) = 1$.因此,不能直接利用数字信号处理的方法对 QKD 协议的错误序列 $\{e(n)\}$ 进行分析,序列重构可以解决这个问题.

已知序列 $\{d(n)\}$,定义位置算子 $\hat{p}_{ij}$,表示交换序列第 i 位和第 j 位的值,得到新序列 $\{d'(n)\}$.因此,通过位置互换可以构建新的序列

$$\{d'(n)\} = \prod_{0 \leqslant i,j \leqslant n} \hat{p}_{ij} \{d(n)\}. \tag{9}$$

(9)式表示对原序列经过若干次位置交换后,得到的新序列为 $\{d'(n)\}$.

序列重构利用了相似构造法,设 Alice 向 Bob 发送了 N 量子位,记为 $\{A(N)\}$,假设 Bob 能够全部接收到,将错误序列的总长度 N 表示为 $N = m \times n$,Alice 随机的选择 n 位构成新的子序列,重复 m 次,于是可以得到 m 个随机组合的新子序列 $\{A_i(n)\}, i = 0,1,\cdots,m$.每一个子序列对应了一个错误序列 $\{e_i(n)\}, i = 0,1,\cdots,m$.根据虚拟测试定理[4]可以知道,序列 $\{A_i(n)\}$ 中的错误数依概率 $1 - \mu(\beta, N)$ 与检测序列一致,其中

$$\begin{aligned} \mu(\beta, N) &= \exp\Bigg(\frac{-\beta^2 \min\{P_1^2, P_2^2, \cdots, P_m^2\}}{2\delta + \beta} N \\ &\quad + \frac{2\beta^2 P_i^2}{(2\delta + \beta)^2} \Bigg), \end{aligned} \tag{10}$$

P_i 表示序列 $\{A(N)\}$ 中某一位属于子序列 $\{A_i(n)\}$ 的概率.

只要选取适当的 n 和 m,则可以使 m 个子序列的错误数近似相等,即其错误序列的重量近似相等.由于任意两个重量相等的二进制序列,总可以通过位置交换,使得二者相等.

设二进制序列 $\{x_1(n)\}$ 和 $\{x_2(n)\}$ 的重量相等,则根据(9)式,可以得到

$$\{x_1(n)\} = \prod_{0 \leqslant i,j \leqslant n} \hat{p}_{ij} \{x_2(n)\}. \tag{11}$$

对于错误序列 $\{e_i(n)\}, i = 0,1,\cdots,m$,不妨以 $\{e_0(n)\}$ 为模板,根据最小距离原则,对其余的序列 $\{e_i(n)\}(i = 1,\cdots,m)$ 进行重构,使得新序列 $\{e_1'(n)\}(i = 1,2,\cdots,m)$ 与 $\{e_i(n)\}$ 的汉明距离最小.若某一子序列与 $\{e_i(n)\}$ 的重量相等,则经过位置交换后,新序列与 $\{e_i(n)\}$ 的距离为 0.

在实际的密钥分配过程中,Alice 从 N 位量子比特中随机选择一部分用于错误检测,余下的部分为信息序列用来建立密钥.为了便于分析,假设 Alice 选择了其中的 $N/3$ 位比特作为检测序列,余下的 $2N/3$ 位比特为信息序列,可以得到 $n = N/3, m = 3$.经过序列重构后,信息序列中的错误序列与检测序列中的错误序列具有相似的结构,具有了一定的相关特性.

预测器的输出是经过重构的错误序列估计值.因此,即使得到预测值 $\tilde{e}(i) = 1$,并不能说明信息序

列的第 i 位出错.然而,大家关心的并不是到底哪些位出错,而是到底有多少位出错.由于信息序列和测试序列的错误率具有相似的统计特性,因此,总存在这样的算子 $\prod_{0\leqslant i,j\leqslant N}\hat{p}_{ij}$,使得信息错误序列的结构与测试错误序列相似,从而表现出较强的相干性,其自相关函数也不再是常数.

正是因为存在这样的算子,才可以认为预测器的输入序列是经过重构后的序列,并且重构是自发进行的,序列在进入预测器之前本身就已经具有了重构的特性.因此,序列重构并不是人为加入到 QKD 协议中的步骤.

2.4. 参数估计

前面讨论的最佳单步预测器满足以下的正则方程:

$$\begin{bmatrix} r_x(0) & r_x(1) & \cdots & r_x(M-1) \\ r_x(1) & r_x(0) & \cdots & r_x(M-2) \\ & & & \\ r_x(M-1) & r_x(M-2) & \cdots & r_x(0) \end{bmatrix}\begin{bmatrix} h(1) \\ h(2) \\ \\ h(M) \end{bmatrix} = \begin{bmatrix} r_x(1) \\ r_x(2) \\ \\ r_x(M) \end{bmatrix}. \tag{12}$$

通过随机检测,可以得到 m 位长的错误序列 $\{e(m)\}$,以 $\{e(m)\}$ 作为已知的数据,对 $\{e(N)\}$ 的自相关函数 $r_x(l)$ 进行参数估计,参数提取的方法有很多种:自相关法,协方差法,修正的协方差法等.

由于自相关法相当于对数据加窗,因而偏差比较大;修正的协方差法又过于苛刻的要求信号在正反两个方向上呈现相同的特性,而序列重构使得信号在正反两个方向上会有所差异,因而选用协方差法比较合适.

可以得到错误序列 $\{e(N)\}$ 的估计值如下所示:

$$\tilde{r}_x(l,k) = \begin{cases} \dfrac{1}{m-M}\sum_{n=M}^{m-1} e(n-l)e(n-k), \\ \tilde{r}_x(k,l), \end{cases}$$
$$l,k = 1,2,\cdots,M. \tag{13}$$

于是得到下面的估值方程组:

$$\begin{bmatrix} \tilde{r}_x(1,1) & \tilde{r}_x(1,2) & \cdots & \tilde{r}_x(1,M) \\ \tilde{r}_x(2,1) & \tilde{r}_x(2,2) & \cdots & \tilde{r}_x(2,M) \\ & & & \\ \tilde{r}_x(M,1) & \tilde{r}_x(M,2) & \cdots & \tilde{r}_x(M,M) \end{bmatrix}\begin{bmatrix} \tilde{h}(1) \\ \tilde{h}(2) \\ \\ \tilde{h}(M) \end{bmatrix} = \begin{bmatrix} \tilde{r}_x(1,0) \\ \tilde{r}_x(2,0) \\ \\ \tilde{r}_x(M,0) \end{bmatrix}. \tag{14}$$

根据以上的方程组,可以求解出最佳预测器的参数.设滤波器的输出结果为 $\{\tilde{E}(n-m)\}$,显然 $\{\tilde{E}(n-m)\}$ 不是二进制序列,所以还需要对波形进行重整,以得到真正的错误序列.

2.5. 波形整形

对预测值 $\{\tilde{E}(n-m)\}$ 进行波形重整可以通过最佳判决器实现,其判决原理如图 3 所示.从图中可以看出,经过判决器后,实数序列 $\{\tilde{E}(n-m)\}$ 变成了二进制序列 $\{\tilde{e}(n-m)\}$,判决器的判决准则不一样,得到的二进制序列也不同,可采用的判决准则有最小均方误差准则,最大似然准则等.最后根据判决器输出的二进制序列,计算出信息序列的错误率 p_e.从而完成了协议单次运行下信息序列错误率的估计.

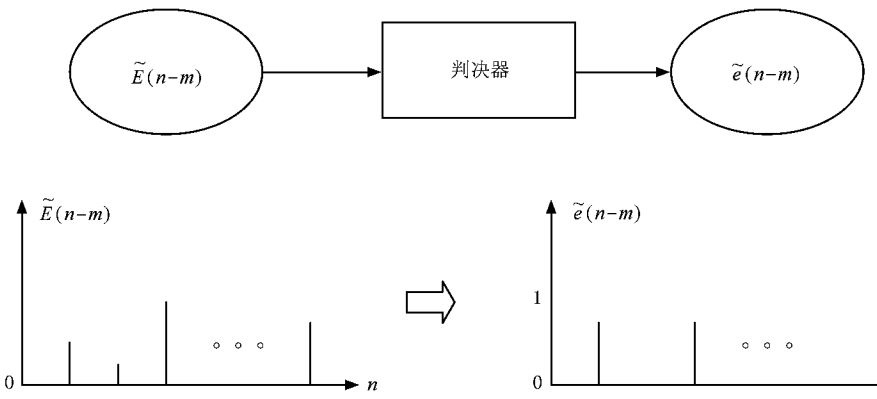

图 3 波形整形

3. 结　论

本文提出了一种信息序列的错误序列模型分析方法，根据量子密钥分配协议的特点，利用序列重构构造出检测序列的错误序列二阶统计特性，对信息序列的错误率进行估计. 这种方法提高了单次信息序列错误率估计的精度，增强了单次窃听检测的可靠性.

[1] Lo H, Chau H F 1999 *Science* **283** 2050

[2] Lo H K 2001 *Quantum Information and Computation* **1**(2) 81

[3] Gottesman Daniel, Lo H K 2003 *IEEE Transactions on Information Theory* **49** 457

[4] Mayers Dominic 2001 *Journal of the ACM* **48** 351

[5] Biham Eli, Boyer Michel, Boykin P Oscar, Mor Tal, Roychowdhury Vwani 2006 *Journal of Cryptology* **19** 381

[6] Bennett C H, Brassard G 1984 *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing* (IEEE, New York press) p175

[7] Feng F Y, Zhang Q 2007 *Acta Phys. Sin.* **56** 1924 (inChinese) [冯发勇、张　强 2007 物理学报 **56** 1924]

[8] Jiao R Z, Feng C X 2008 *Acta Phys. Sin.* **57** 685 (in Chinese) [焦荣珍、冯晨旭 2008 物理学报 **57** 685]

An analysis of the model of the error bits of quantum cryptography protocol*

Zhang Sheng†　Wang Jian　Zhang Quan　Tang Chao-Jing

(*College of Electronic Science and Engineering, National University of Defense Technology, Changsha* 410073, *China*)

(Received 2 April 2008; revised manuscript received 19 June 2008)

Abstract

Quantum cryptography protocols have the feature of unconditional security, which is ensured by attack-detection. A new method is introduced to improve the precision of the estimation of the error rate in the information bits. With the new technique, more information about the error bits can be obtained, then the value of error rate of the information bits can be obtained by classical signal estimation. This method can improve the precision of attack-detection within a single running of all quantum cryptography protocols.

Keywords: quantum cryptography, best estimation, attack-detection, bits rebuilding

PACC: 0367, 4250

* Project supported by the National Natural Science Foundation of China (Grant No. 60472032).

† E-mail: huoxingren112@163.com