单向量子密钥纠错协议的纠错性能仿真分析*

赵峰†

(陕西理工学院物理与电信工程学院, 汉中 723000)

(2013年5月26日收到; 2013年7月6日收到修改稿)

高效误码纠错是量子密钥分配后续数据处理的关键技术之一. 基于汉明码校验子级联单向一次通信纠错方案, 分别对三种校验子级联纠错能力进行了理论和仿真分析. 根据分析结果提出了一种基于混合校验子级联纠错协议, 通过优化纠错流程相关参数提高密钥生成效率. 随后对该协议的纠错能力及其密钥生成效率进行了仿真分析, 最后根据误码率后验分布参数, 对密钥最终误码率及其置信区间进行了估计. 单一校验子级联纠错仿真结果显示: 在相同的纠错能力的条件下, 初始误码率为 $3\% < p \leqslant 11\%$ 时, (7, 4) 汉明码纠错的密钥生成效率最高; 初始误码率为 $1.5\% < p \leqslant 3.0\%$ 时, (15, 11) 汉明码纠错的密钥生成效率最高; 初始误码率为 $p \leqslant 1.5\%$ 时, (31, 26) 汉明码纠错的密钥生成效率最高. 混合校验子级联纠错方案的仿真结果显示: 对于初始误码率为 9.50%, 经过 8 轮次混合校验子级联纠错, 密钥生成效率为 9.94%, 误码率期望值为 5.21×10^{-12}, 置信度为 90%的上限值为 2.85×10^{-11}, 相比用单一 (7, 4) 校验子级联纠错的密钥生成效率提高了约 3 倍.

关键词: 量子密钥分配, 保密纠错, 效率分析

PACS: 03.67.Dd, 03.67.Pp, 02.60.Cb **DOI:** 10.7498/aps.62.200303

1 引 言

量子密钥分配可以为异地的合法通信方提供安全的密钥, 其分配过程基于量子力学测不准原理和未知量子态不可克隆定理, 巧妙地将需要分配的密钥隐藏在不确定的量子通信过程中, 从而实现利用公开、不安全信道传送密钥的目的 [1]. 由于量子比特在制备、传输、检测过程中不可避免地会引入误码, 加之窃听者 Eve 的攻击行为也可能会引入误码 [2−5]. 密钥中的误码不仅会降低共享密钥的一致性, 而且直接导致密钥的安全性降低. 根据量子密钥分配协议的安全误码阈限要求, 当原始密钥中的误码率低于某一阈限值时, 通信双方可以通过后续数据处理获得一定量的密钥. 因此, 为了保证双方共享密钥的一致性, 在后续数据处理过程中首先需要进行误码纠错.

误码纠错是后续数据处理的关键技术之一. 1992 年, Bennett 等 [6] 提出了二元纠错协议, 该方法简单易操作, 但需要在公开信道上进行频繁的信息交换, 且不能发现字段中的偶数个错误比特. 1993 年, Brassard 和 Salvail[7] 提出了一种级联纠错协议, 这种协议能够纠正字段中的两个错误比特. 虽然它的纠错能力强于二元纠错协议, 但是它的通信次数和计算复杂度更大. 2003 年, Butter 等 [8] 基于汉明码的校验子提出了一种误码纠错协议, 这种协议的纠错次数少于二元纠错协议和级联纠错协议, 但单次纠错能力有限, 而且都是多轮次协议, 交互式通信消耗大量的时间.

后来, Biham 等 [9] 和 Mayers[10] 分别提出了一种基于交换校验子纠错方案, Liu 等 [11] 建议了一种用于信息协调的密钥重新分配方案, 这三种纠错方案都是非交互式的. 非交互式纠错协议通过单向通信即可实现误码纠错, 但无法通过一次通信将误码率降至预先设定的水平. 2012 年 Li 和 Zhao[12] 在前人基础上提出了一种基于汉明码的校验子级联纠错协议, 理论上该协议通过一次单向通信即可将误码率降至预先设定的水平, 由于仅使用单一的码型

* 教育部科学技术研究重点项目 (批准号: 212177)、陕西省自然科学基金 (批准号: 2011JQ1003) 和陕西省教育厅科研基金 (批准号: 12JK0973) 资助的课题.

† 通讯作者. E-mail: hfengzhao@126.com

纠错, 未能实现密钥生成效率最大化. 我们在此基础上提出了利用多种码型校验子进行混合级联纠错协议, 然后利用 MATLAB 开展数据仿真分析误码纠错能力及其密钥生成效率, 并对纠错后的误码率进行置信度估计. 实验结果表明, 改进后的协议通过优化参数, 进一步提高了密钥生成效率.

本文安排如下: 第 2 节介绍纠错过程涉及的相关算法; 第 3 节开展仿真研究, 根据结果提出改进后的纠错协议; 第 4 节对仿真结果进行分析, 给出相关的结论.

2 相关算法分析

2.1 密钥序列随机变换

量子密钥分配过程中的编解码器、量子信道、探测器等引入误码的噪声通常可用高斯白噪声模型来描述. 然而, 窃听者 Eve 引入的误码具有一定的突发性. 通常, 原始量子密钥在纠错前需要进行“随机变换”, 以期将误码均匀地分布在原始密钥中. 线连接置换是一种简单、快速数字比特排列技术 [12], 其置换原理如 (1) 和 (2) 式所示, $\boldsymbol{A}^{(i)}$ 表示第 i 次线性置换前的数组, $\boldsymbol{A}'^{(i)}$ 表示线性置换后的数组:

$$\boldsymbol{A}^{(i)}=\begin{bmatrix} a_{11}^{(i)} & a_{12}^{(i)} & \cdots & a_{1n}^{(i)} \\ a_{21}^{(i)} & a_{22}^{(i)} & \cdots & a_{2n}^{(i)} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1}^{(i)} & a_{m2}^{(i)} & \cdots & a_{mn}^{(i)} \end{bmatrix}, \tag{1}$$

$$\boldsymbol{A}'^{(i)}=\begin{bmatrix} a_{11}^{(i)} & a_{21}^{(i)} & \cdots & a_{m1}^{(i)} \\ a_{12}^{(i)} & a_{22}^{(i)} & \cdots & a_{m2}^{(i)} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1n}^{(i)} & a_{2n}^{(i)} & \cdots & a_{mn}^{(i)} \end{bmatrix}. \tag{2}$$

可以看出, 经过对数组 $\boldsymbol{A}^{(i)}$ 变换后, 第一个字段 $(a_{11},a_{12},\cdots,a_{1n})$ 的第一个比特放置在了新的一轮字段中的第一个位置; 第二个字段 $(a_{21},a_{22},\cdots,a_{2n})$ 的第一个比特放在了新一轮字段中的第二个位置; 以此类推, 直到最后一个字段, 即第 m 个字段的第一个比特放在了新的一轮字段中第 m 个位置.

2.2 汉明码纠错效率分析

二元汉明 $[n,n-k]$ 码, $n=2^k-1$, 其结构特殊, 具有快速纠错能力. 校验的比特分别插入在第 2^l 个位置, 其中 $0\leqslant l<k$. 剩余的位置为信息比特位. 其生成矩阵 $\boldsymbol{G}$ 通过交换对应系统码的第 2^l 列与第 $n-l$ 列. 解码方法是接收的比特串与监督矩阵 H 相乘得到校验子 $s=(s_1,\cdots,s_k)$, 二进制数校验子 $(s_1,\cdots,s_k)$ 指示每一个错误比特的位置.

假设使用长度为 n 的汉明码, 原始密钥初始误码概率为 p, 每个字段中误码的期望值为 np.

1) 假设字段中有一个错误比特, 经过纠错后误码个数为零.

2) 假设字段中有 k 个错误比特 $2\leqslant k\leqslant n-1$, 当进行误码纠错时会出现两种情况:

①经过纠错后仍然存在 k 个误码, 对于任意的汉明码字 $\boldsymbol{c}$, 距离为 k 的码字数为 A_k (码重分布); 因此, 这种情况下纠错后的误码概率为 $A_kp^k(1-p)^{n-k}$;

②经过纠错后将误码个数降至 $k-1$ 或上升至 $k+1$, 对于任何码字 $\boldsymbol{c}$, 码字距离分别为 $k-1$ 或 $k+1$ 的码字数为 A_{k-1},A_{k+1}; 经过纠错后, 可以得到 $A_{k-1}+A_{k+1}$ 个码字中的其中一个; 假设每个码字在纠错过程中具有相同的概率, 经过纠错后误码个数下降至 $k-1$ 的概率为 $\dfrac{A_{k-1}}{A_{k-1}+A_{k+1}}$, 误码个数增加至 $k+1$ 的概率为 $\dfrac{A_{k+1}}{A_{k-1}+A_{k+1}}$.

因此, 有 k 个误码的码字 $\boldsymbol{c}$ 的误码个数变化的概率为 $(C_n^k-A_k)p^k(1-p)^{n-k}$, 其中误码降至 $k-1$ 的概率为 $(C_n^k-A_k)\dfrac{A_{k-1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k}$, 误码增加至 $k+1$ 的概率为 $(C_n^k-A_k)\dfrac{A_{k+1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k}$.

3) 当某个字段中出现 n 个误码时, $A_n=1$, 其概率为 $C_n^n=1$, 纠错后误码个数为 n 个, 出现的概率为 np.

从上面的分析可以计算出每个字段纠错后的误码数学期望值. 设纠错后的比特误码概率为 p_1, 每个字段的误码个数期望值为 np_1.

$$\begin{aligned} np_1=\sum_{k=2}^{n-1}\Bigg[&kA_kp^k(1-p)^{n-k} \\ &+(k-1)(C_n^k-A_k)\frac{A_{k-1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k} \\ &+(k+1)(C_n^k-A_k)\frac{A_{k+1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k}\Bigg] \end{aligned}$$

$$+np. \tag{3}$$

对于长度为 n 的二元汉明码, 码重计数子为

$$A(z,n)=\sum_{i=0}^{n}A_iz^i=\frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}. \tag{4}$$

因此, (7, 4) 汉明码的码重计数子为 $A(z)=z^7+7z^4+7z^3+1$, 经过一次纠错后

$$p_1=-12p^5+30p^4-26p^3+9p^2. \tag{5}$$

(15, 11) 汉明码的码重计数子为

$$A(z)=z^{15}+35z^{12}+105z^{11}+168z^{10}+280z^9 +435z^8+435z^7+280z^6+168z^5+105z^4 +35z^3+1. \tag{6}$$

经过一次纠错后

$$p_1\approx-4p^{15}+28p^{14}-208p^{13}+925p^{12} -2453p^{11}+4260p^{10}-5359p^9+5361p^8 -4535p^7+3154p^6-1657p^5+629p^4 -154p^3+21p^2. \tag{7}$$

根据 (5) 式和 (7) 式, 可以分别计算出 (7, 4) 汉明码和 (15, 11) 汉明码经过一次纠错后的剩余误码率. 两种汉明码的纠错能力曲线如图 1 所示.

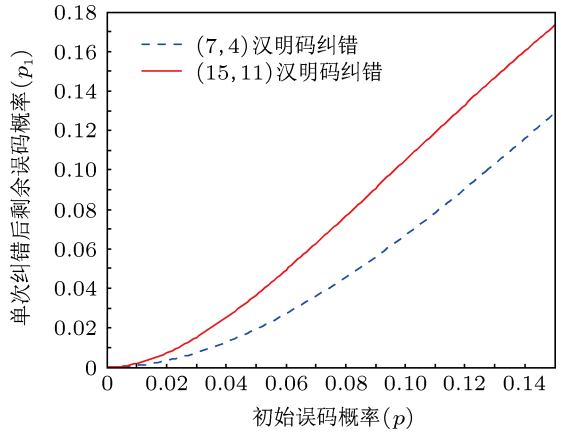

图 1 两种汉明码的纠错能力曲线

图 1 中横向坐标表示纠错前的误码率 p, 纵向坐标表示经一次纠错后的误码率 p_1, 虚线表示 (7, 4) 汉明码的纠错能力曲线, 实线表示 (15, 11) 汉明码的纠错能力曲线. 在相同的初始误码率条件下, 每个字段的误码率期望值随着 n 增大而增大, 相比之下, (7, 4) 汉明码的纠错能力较强. 理论上, 当误码率小于 21%时, 经过多次 (7, 4) 汉明纠错可以将误码率降至任意低的水平. 当误码率小于 9%时, 多次 (15, 11) 汉明纠错可将误码率降至任意低的水平. 因此, 在量子密钥分配允许误码率范围内, 汉明码纠错性能完全能够满足需求.

2.3 误码率置信度分析

设 N 为发送的码字数, n 为码字长度, p 为纠错前原始密钥的误码概率, $n_{\rm w}$ 为汉明纠错后的错误码字数, $n_{\rm b}$ 为错误码字中的错误信息比特数. 则汉明纠错后错误字概率为 $p_{\rm w}=\lim\limits_{N\to\infty}n_{\rm w}/N$, 错误字中的比特错误概率 $p_{\rm b}=\lim\limits_{N\to\infty}n_{\rm b}/n\cdot n_{\rm w}$. 因此, 汉明纠错后待估计的误码比特概率为 $P_{\rm b}=p_{\rm w}\cdot p_{\rm b}$. 设 P 是二维随机变量 $(p_{\rm w},p_{\rm b})$ 的联合先验概率, $P(D|p_{\rm w},p_{\rm b})$ 是实测数据 D 以 $(p_{\rm w},p_{\rm b})$ 为条件的似然概率. 当知道实测数据 D 后, 变量 $(p_{\rm w},p_{\rm b})$ 将具有联合后验概率为

$$P(p_{\rm w},p_{\rm b}|D)\propto P(D|p_{\rm w},p_{\rm b})\cdot P(p_{\rm w},p_{\rm b}), \tag{8}$$

其中, $P(p_{\rm w},p_{\rm b})=P(p_{\rm w})\cdot P(p_{\rm b})$. 由于纠错前原始密钥经过随机变换处理, 因此, 我们可假设误字率 $p_{\rm w}$ 具有均匀的先验分布, 其密度函数可以表示为

$$P(p_{\rm w})=1,\quad p_{\rm w}\in(0,1). \tag{9}$$

错误字中比特错误概率 $p_{\rm b}$ 的先验分布既受到汉明纠错性能的影响, 也受到量子传输信道的影响, 可以用 β 分布函数来拟合随机变量 $p_{\rm b}$ 的先验分布, 其密度函数为

$$P(p_{\rm b})=\frac{1}{B(a,\beta)}p_{\rm b}^{\alpha-1}(1-p_{\rm b})^{\beta-1},p_{\rm b}\in(0,1), \tag{10}$$

其中 $B(a,\beta)$ 为 β 函数.

参数为 (a,β) 的 β 分布, 具有数学期望 $\alpha/(\alpha+\beta)$ 和方差 $\alpha\beta/(\alpha+\beta)^2(\alpha+\beta+1)$. 为了使变量 $p_{\rm b}$ 的分布保持与译码器相关的特性 [13], 通常令 $\alpha=2$, 此时 β 函数为 $B(a,\beta)=1/[\beta(\beta+1)]$. 当译码失败时, 最粗糙也是最合理的假设是错误概率 $p_{\rm b}$ 等于当前信噪比下非编码传输的比特错误概率 [14], 在量子密钥分配系统中量子信道的误码率为 p, 因而可设 $\beta=1/p$.

假设各个码字是相互独立的, 错误码字中各个比特也是相互独立的, 以 $(p_{\rm w},p_{\rm b})$ 为条件取得实测数据 D 的似然概率是误字数和误比特数分别服从二项式分布的概率乘积, 可表示为

$$P(D|p_{\rm w},p_{\rm b})$$

$$\propto p_{\mathrm{w}}^{n_{\mathrm{w}}}(1-p_{\mathrm{w}})^{N-n_{\mathrm{w}}}p_{\mathrm{b}}^{n_{\mathrm{b}}}(1-p_{\mathrm{b}})^{n\cdot n_{\mathrm{w}}-n_{\mathrm{b}}}, \quad (11)$$

将 (9)—(11) 式代入 (8) 式可得后验分布密度函数

$$P(p_{\mathrm{w}},p_{\mathrm{b}}|D) \propto p_{\mathrm{w}}^{n_{\mathrm{w}}}(1-p_{\mathrm{w}})^{N-n_{\mathrm{w}}}p_{\mathrm{b}}^{n_{\mathrm{b}}+1}(1-p_{\mathrm{b}})^{n\cdot n_{\mathrm{w}}-n_{\mathrm{b}}+\beta-1}, \quad (12)$$

(12) 式可以看作两个相互独立、参数分别为 $(n_{\mathrm{w}}+1, N-n_{\mathrm{w}}+1)$ 和 $(n_{\mathrm{b}}+2, n\cdot n_{\mathrm{w}}-n_{\mathrm{b}}+\beta)$ 的 β 分布密度函数的乘积. 因此, 错误字和错误比特概率可以通过 β 函数期望值和方差公式计算出来.

设 μ_{w} 和 σ_{w}^2 分别是 $P(p_{\mathrm{w}}|D)$ 的期望和方差, 设 μ_{b} 和 σ_{b}^2 分别是 $P(p_{\mathrm{b}}|D)$ 的期望和方差, 表示如下

$$\mu_{\mathrm{w}} = \frac{n_{\mathrm{w}}+1}{N+2}, \quad (13)$$

$$\mu_{\mathrm{b}} = \frac{n_{\mathrm{b}}+2}{n\cdot n_{\mathrm{w}}+\beta+2}, \quad (14)$$

$$\sigma_{\mathrm{w}}^2 = \frac{(n_{\mathrm{w}}+1)(N-n_{\mathrm{w}}+1)}{(N+2)^2(N+3)}, \quad (15)$$

$$\sigma_{\mathrm{b}}^2 = \frac{(n_{\mathrm{b}}+2)(n\cdot n_{\mathrm{w}}-n_{\mathrm{b}}+\beta)}{(n\cdot n_{\mathrm{w}}+\beta+2)^2(n\cdot n_{\mathrm{w}}+\beta+3)}. \quad (16)$$

因此经过汉明纠错后, 误比特率的期望 μ 和方差 σ^2 为

$$\mu = \mu_{\mathrm{w}}\cdot\mu_b, \quad (17)$$

$$\sigma^2 = \sigma_{\mathrm{w}}^2\sigma_{\mathrm{b}}^2 + \mu_{\mathrm{b}}^2\sigma_{\mathrm{w}}^2 + \mu_{\mathrm{w}}^2\sigma_{\mathrm{b}}^2. \quad (18)$$

任意给定 $\theta\in(0,1)$, 若 $\varepsilon=\sigma/\sqrt{\theta}$, 由契比雪夫不等式知概率 $P(\mu-\varepsilon\leqslant P_b\leqslant\mu+\varepsilon)$ 的置信度不小于 $1-\theta$. $\mu+\varepsilon$ 为 $1-\theta$ 的置信区间误码率的上限.

3 单向一次通信纠错性能仿真分析

3.1 汉明码校验子级联纠错算法

基于校验子级联编码纠错算法如下 [12].

1) Alice 将原始密钥分成长为 n 比特的字段, 然后对密钥进行比特随机线性置换, 以期将误码均匀分布在密钥序列中. Alice 计算出每个字段的校验子 $s_{\mathrm{A}_i}^{(j)}$, 然后丢弃每个字段的检验比特, 这里 i 表示每个字段的序号, j 表示序号的轮次. Alice 重复上述操作, 从 $j=1$ 到 $j=l$, 得到校验子 $s_{\mathrm{A}_i}^{(1)}, s_{\mathrm{A}_i}^{(2)}, \cdots, s_{\mathrm{A}_i}^{(l)}$, 其中 l 表示预先设定的纠错轮次.

2) Alice 将他的校验子 $s_{\mathrm{A}_i}^{(1)}, s_{\mathrm{A}_i}^{(2)}, \cdots, s_{\mathrm{A}_i}^{(l)}$ 作为发送信息, 为了防止第三方篡改, 她需要进行数字签名, 然后将信息和认证值发送给 Bob.

3) 当 Bob 接收到序列 $s_{\mathrm{A}_i}^{(1)}, s_{\mathrm{A}_i}^{(2)}, \cdots, s_{\mathrm{A}_i}^{(l)}$ 时, Bob 首先检测信息是否未被篡改. 如果认证通过, Bob 用相同的方法对自己的密钥进行线性置换, 然后计算出每个字段的校验子 $s_{\mathrm{B}_i}^{(1)}$. 根据校验子 $s_{\mathrm{A}_i}^{(1)}$ 和 $s_{\mathrm{B}_i}^{(1)}$, 他计算出第 1 轮中的第 i 个字段的校验子 $s_i^{(1)} = s_{\mathrm{A}_i}^{(1)} \otimes s_{\mathrm{B}_i}^{(1)}$, 然后纠正第 i 个字段的误码. 纠错后, 他丢弃所有的校验比特. Bob 重复上述操作, 得到校验子 $s_i^{(j)}$, 然后进行误码纠错, 直到 $j=l$. 经过 l 轮次的纠错后, 他得到最终的密钥.

3.2 纠错性能仿真分析

在数据仿真中, Alice 和 Bob 的原始密钥利用伪随机二进制序列 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 代替, 误码呈均匀分布, $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的初始误码率记为 p. 基于 (7, 4) 汉明码校验子级联纠错性能如表 1 所示, 初始误码率为 9.50%, 原始密钥长度为 282475249. 基于 (15, 11) 汉明码校验子级联纠错性能如表 2 所示, 初始误码率为 5.50%, 原始密钥长度为 170859375. 基于 (31, 26) 汉明码校验子级联纠错性能如表 3 所示, 初始误码率为 2.61%, 原始密钥长度为 887503681.

当初始误码率 $3\% < p \leqslant 11\%$, 适合用 (7, 4) 码纠错. 例如, (7, 4) 码将误码率从 6.13%降至 2.82%时只需要一次纠错, 密钥生成效率为 57.14%; (15, 11) 码将误码率从 5.50%降至 2.82%时则需要两次纠错, 密钥生成效率为 53.78%; (31, 26) 码则无法纠错. 因此, 密钥初始误码率大于 3%时, 使用 (7, 4) 汉明码纠错在保证纠错能力的条件下, 密钥生成效率最高.

当初始误码率 $1.5\% < p \leqslant 3.0\%$ 时, 适合用 (15, 11) 码纠错. 例如, (7, 4) 码将误码率从 2.82%降至 3.80×10^{-4} 时需要两次纠错, 密钥生成效率为 32.65%; (15, 11) 码将误码率从 2.82%降至 2.59×10^{-4} 时需要三次纠错, 密钥生成效率为 39.44%; (15, 11) 码将误码率从 2.82%降至 1.36%时需要一次纠错, 密钥生成效率为 73.33%; (31, 26) 码将误码率从 2.61%降至 1.36%时需要两次纠错, 密钥生成效率为 70.34%. 因此, 当误码率 $1.5\% < p \leqslant 3.0\%$ 时, 使用 (15, 11) 汉明码纠错, 在保证纠错能力的条件下, 密钥生成效率最高.

当初始误码率 $p \leqslant 1.5\%$ 时, 适合用 (31, 26) 码纠错. 例如, (7, 4) 码将误码率从 1.36%降至 3.13×10^{-5} 时需要两次纠错, 密钥生成效率为 32.65%; (15, 11) 码将误码率从 1.36%降至 1.84×10^{-6} 时需要三次纠错, 密钥生成效率为 39.44%; (31, 26) 码将误码率从 1.36%降至 1.13×10^{-6} 时需要四次纠错, 密钥生成效率为 49.48%. 因此, 当误码率 $p \leqslant 1.5\%$ 时, 使用 (31, 26) 汉明码纠错, 在保证纠错能力的条件下, 密钥生成效率最高.

表 1 基于 (7, 4) 汉明码校验子级联纠错性能 ($p = 9.50\%$)

纠错轮次	1	2	3	4	5	6
剩余误码率p_1	6.13%	2.82%	0.66%	3.80×10^{-4}	1.05×10^{-6}	0
密钥生成效率	57.14%	32.65%	18.66%	10.66%	6.09%	3.48%

表 2 基于 (15, 11) 汉明码校验子级联纠错性能 ($p = 5.50\%$)

纠错轮次	1	2	3	4	5	6
剩余误码率p_1	4.27%	2.82%	1.36%	0.35%	2.59×10^{-4}	1.84×10^{-6}
密钥生成效率	73.33%	53.78%	39.44%	28.29%	21.21%	15.55%

表 3 基于 (31, 26) 汉明码校验子级联纠错性能 (p=2.61%)

纠错轮次	1	2	3	4	5	6
剩余误码率p_1	2.04%	1.36%	0.66%	0.18%	1.34×10^{-4}	1.13×10^{-6}
密钥生成效率	83.87%	70.34%	59.00%	49.48%	41.50%	34.81%

3.3 纠错协议改进

混合校验子级联纠错协议如下.

1) 当量子密钥筛选完毕后, Alice 和 Bob 进行误码率估计 (抽样估计或诱饵态估计).

2) 根据原始密钥误码率估计值及纠错后的误码率要求, Alice 和 Bob 分别设定纠错轮次 l 及其每个轮次需要用的纠错码型. 例如, 当初始误码率为 9.50%时, 要求纠错后的误码率小于 10^{-10} 数量级, 考虑三个纠错码型在不同误码率区间的纠错能力和密钥生成效率, 确定出每个轮次需要的纠错码型.

3)—5) 步骤对应原纠错协议的 1)—3) 步骤, 需要变化的是每个轮次使用了不同的纠错码型.

3.4 混合级联纠错能力仿真分析

混合级联纠错方案的纠错能力仿真数据如表 4 所示. 其中仿真数据长度为 119559244, 初始误码率为 9.50%, 经过混合 8 轮次纠错. 根据纠错码在不同的纠错区间的纠错能力特点, 我们在第 1, 2 轮次使用了 (7, 4) 码纠错, 第 3 轮次使用了 (15, 11) 码纠错, 第 4—8 轮次使用了 (31, 26) 码纠错, 最终密钥的误码率实测值为 0, 密钥生成效率为 9.94%.

表 4 混合校验子级联纠错能力分析 ($p = 9.50\%$)

纠错轮次	纠错码型	初始误码率	剩余误码率	密钥生成效率l/%
1	(7, 4)	9.50%	6.13%	57.14
2	(7, 4)	6.13%	2.82%	32.65
3	(15, 11)	2.82%	1.37%	23.94
4	(31, 26)	1.37%	0.68%	20.08
5	(31, 26)	0.68%	0.19%	16.84
6	(31, 26)	0.19%	1.54×10^{-4}	14.13
7	(31, 26)	1.54×10^{-4}	1.42×10^{-6}	11.85
8	(31, 26)	1.42×10^{-6}	0	9.94

比较表 4 与表 1 所示数据, 在相同的初始误码率条件下, 利用单一 (7, 4) 码校验子级联纠错, 经过 6 轮次级联纠错后, 最终密钥的误码率实测值为 0, 密钥生成效率为 3.48%. 若用混合校验子纠错后的密钥生成效率为 9.94%, 提高了约 3 倍.

若将误码率从 6.13%降至 10^{-6} 数量级, 单一 (7, 4) 码校验子级联纠错的密钥生成效率为 6.09%, 单一 (15, 11) 码校验子级联纠错的密钥生成效率为 15.55%, 混合码型纠错的密钥生成效率为 20.74%. 因此, 混合校验子级联纠错在保证纠错能力条件下,

有效地提高了密钥生成效率.

基于有限长度仿真数据, 当误码率为 0 时, 需要对误码率的期望值, 以及误码率置信度及其置信区间进行估计. 接下来, 我们估计第 8 次纠错后的误码率及其置信度. 如表 4 所示, 经过 7 轮次纠错后的误码率为 1.42×10^{-6}, 剩余的密钥数量 16890536, 每个码字长度为 31, 因此共有 544856 个码字. 利用 (13)—(18) 式可以得出表 5 所列出的数据. 因此, 最终误码率的实测值与估计值如表 5 所示.

如表 5 所示, 当最终误码率实测值为 0 时, 误码率期望值为 5.21×10^{-12}. 表 6 给出了误码率期望值的置信区间与置信度的关系, 列出了该估计值在 10 种置信度下的置信区间. 当误码率期望值为 5.21×10^{-12} 时, 置信度为 90% 的上限值为 2.85×10^{-11}.

表 5 混合校验子级联纠错仿真参数、实测数据和误码率估计

实测数据	$N=544856\ n=31\ n_{\rm w}=0\ n_{\rm b}=0\ \beta=704225$		
估计参数	实测值	期望	方差
$p_{\rm w}$	0	1.84×10^{-6}	3.37×10^{-12}
$P_{\rm b}$	0	2.84×10^{-6}	4.03×10^{-12}
$P_{\rm b}$	0	5.21×10^{-12}	5.43×10^{-23}

表 6 混合汉明校验子 6 次级联纠错后误码率估计的置信区间与置信度的关系

置信度	0.90	0.91	0.92	0.93	0.94	0.95	0.96	0.97	0.98	0.99
$\varepsilon(\times10^{-11})$	2.33	2.46	2.61	2.79	3.01	3.29	3.68	4.25	5.21	7.37
置信上限 ($\times10^{-11}$)	2.85	2.98	3.13	3.31	3.53	3.82	4.21	4.78	5.73	7.89
置信下限 ($\times10^{-11}$)	0	0	0	0	0	0	0	0	0	0

4 结 论

汉明码校验子级联纠错算法具有单向通信的特点, 当初始误码率小于量子密钥安全阈限值时, 理论上一次通信即可实现任意低的误码率, 但利用单一码型纠错的密钥生成效率较低. 我们根据数据仿真结果, 提出了在考虑初始误码率条件下, 利用多种码型进行混合级联纠错方法, 并利用 MATLAB 仿真分析误码纠错能力及密钥生成效率, 对纠错后密钥的误码率及其置信度进行了估计. 实验结果表明, 改进后的方案其密钥生成效率得到了进一步的提高, 尤其是当初始误码率超过 9.50%时, 密钥生成效率提高近 3 倍.

仿真结果表明: 当初始误码率 $3\%<p$ 时, 利用 (7, 4) 码纠错具有纠错能力和密钥生成效率上的优势; 当初始误码率 $1.5\%<p\leqslant3.0\%$ 时, (15, 11) 码纠错具有纠错能力和密钥生成效率上的优势; 当误码率 $p\leqslant1.5\%$ 时, (31, 26) 码纠错具有纠错能力和密钥生成效率上的优势. 因此, 在纠错前, 需要对原始密钥的误码率进行估计, 然后设定纠错轮次 (级联深度) 及其相应的纠错码型, 从而有效提高密钥的生成效率. 对于典型的 BB84 量子密钥分配来说, 其安全误码上限为 11%, 基于汉明码校验子级联纠错协议完全可以满足保密纠错需求. 此外, 原始量子密钥的初始误码率估计, 通常利用随机抽样实现, 但估计值会受到抽样方式及其样本数量的影响而存在偏差. 对于使用诱饵态方法的量子密钥分配过程来说, 通过对初始误码率的准确估计, 有利于设定恰当的纠错轮次及其纠错码型, 从而使得密钥生成效率最大化.

[1] Gisin N, Ribordy G, Wolfgang T, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Zhao F, Li J L 2010 *J. Optoelectronics·Laser* **21** 1383 (in Chinese) [赵峰, 李静玲 2010 光电子 · 激光 **21** 1383]

[3] Li S, Ma H Q, Wu L A, Zhai G J 2013 *Acta Phys. Sin.* **62** 084214 (in Chinese) [李申, 马海强, 吴令安, 翟光杰 2013 物理学报 **62** 084214]

[4] Yue X L, Wang J D, Wei Z J, Guo B H, Liu S H 2012 *Acta Phys. Sin.* **61** 184215 (in Chinese) [岳孝林, 王金东, 魏正军, 郭邦红, 刘颂豪 2012 物理学报 **61** 184215]

[5] Jiao R Z, Tang S J, Zhang C 2012 *Acta Phys. Sin.* **61** 050302 (in Chinese) [焦荣珍, 唐少杰, 张弼 2012 物理学报 **61** 050302]

[6] Bennett C, Bessette F, Brassard G, Salvail L, Smolin J 1992 *J. Cryptol.* **5** 3

[7] Brassard G, Salvail L 1994 *Advances in Cryptology—EUROCRYPT '93* Norway, May 23–27, 1993 p410

[8] Buttler W T, Lamoreaux S K, Torgerson J R, Nickel G H, Donahue C H, Peterson C G 2003 *Phys. Rev.* A **67** 052303

[9] Biham E, Boyer M, Boykin P, Mor T, Roychowdhury V 2006 *J. Cryptol.* **19** 381

[10] Mayers D 2011 *J. ACM* **48** 351

[11] Liu D, Yin Z Q, Wang S, Wang F M, Chen W, Han Z F 2012 *Chin. Phys.* B **21** 060202

[12] Li Y, Zhao L 2012 arXiv:1201.1196v3 [quant-ph]
[13] He Y C, Yang L, Wang X M 2001 *J. China Institute Commun.* **22** 99 (in Chinese) [贺玉成, 杨莉, 王新梅 2001 通信学报 **22** 99]
[14] Frey B J, MacKay D J C 1997 *Proceedings of 35th Allerton Conference on Communication, Control and Computing Champaign* Urbana, USA 29 September–1 October, 1997 p1

Simulation analysis of one-way error reconciliation protocol for quantum key distribution*

Zhao Feng†

(*School of Physics and Telecommunication Engineering, Shaanxi University of Technology, Hanzhong* 723000*, China*)

(Received 26 May 2013; revised manuscript received 6 July 2013)

Abstract

Higher efficiency of error reconciliation technique is for data post-processing for quantum key distribution. Based on the one way error reconciliation scheme of Hamming syndrome concatenation, the error correction performances of there kinds of Hamming codes are demonstrated by data simulation analysis. The simulation results indicate that when the initial error rates are $(-\infty, 1.5\%]$, $(1.5\%, 3\%]$, and $(3\%, 11\%]$, if using Hamming (31, 26), (15, 11), and (7, 4) codes to correct the errors, respectively, the key generation rate is maximized. Base on these outcomes, we propose a kind of modified error reconciliation scheme which is based on the mixed pattern of Hamming syndrome concatenation. The ability to correct the errors and the key generation rate are verified through data simulation. Meanwhile, using the parameters of the posterior distribution based on the tested data, a simple method of estimating bit error rates (BER) with a confidence interval is estimated. The simulation results show that when the initial bit error rate is 9.50%, after correcting error 8 times error, the error bits are eliminated completely and the key generation rate is 9.94%. The BER expectation is 5.21×10^{-12}, when the confidence is 90% the corresponding upper limit of BER is 2.85×10^{-11}. The key generation rate increased by about 3-fold compared with that of original error reconciliation scheme.

Keywords: quantum key distribution, error reconciliation, efficiency analysis

PACS: 03.67.Dd, 03.67.Pp, 02.60.Cb **DOI:** 10.7498/aps.62.200303

* Project supported by the Key Program of Science and Technology Research Foundation of Ministry of Education, China (Grant No. 212177), the Natural Science Foundation of Shaanxi, China (Grant No. 2011JQ1003), and the Scientific Research Fundation of the Education Department of Shaanxi Province, China (Grant No. 12JK0973).

† Corresponding author. E-mail: hfengzhao@126.com