第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·博士论文· 文章编号：1000—3428(2007)12—0022—03 文献标识码：A 中图分类号：TP391

量子密钥分发误码协调算法分析

赵 峰，王发强，郑力明，路轶群，刘颂豪
(华南师范大学信息光电子科技学院光子信息技术广东省高校重点实验室，广州 510006)

摘 要：误码消除是量子密钥分发过程的关键技术之一。分析了奇偶-汉明单向函数纠错算法的原理，给出了对原始量子密钥进行误码协调的步骤及表达式，对这种算法的纠错能力进行了理论和实验分析。结果显示，当原始密钥误码率为11%时，利用该纠错技术能够完全消除误码，且最终密钥生成效率与密钥的原始误码率直接相关。

关键词：误码协调；奇偶比较；汉明码；量子密钥分发

Error Reconciliation Algorithm for Quantum Key Distribution

ZHAO Feng, WANG Faqiang, ZHENG Liming, LU Yiqun, LIU Songhao
(Lab of Photonic Information Technology, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006)

【Abstract】 Error reconciliation is a necessary step for quantum key distribution process. The efficiency and the correction ability of error reconciliation procedures are analyzed and estimated, and it gives some expressions about it. The experiment results indicate that it can easily eliminate all errors when the error rate is at 11%.

【Key words】 Error reconciliation; Parity comparison; Hamming codes; Quantum key distribution

量子密钥分发使得合法通信双方Alice和Bob在异地可以随时建立起秘密的随机序列，通常称为密钥，其安全性由海森堡的不确定性原理和量子不可克隆定理保证。然而，由于实际量子信道存在不可避免的噪声，以及非法窃听者干扰，使得合法双方生成的密钥中存在一定的误码。因此，当密钥分发完成后，若其误码率在一定范围内，则通信双方通常利用保密纠错技术来消除误码[1~4]。量子密钥分发过程一般需要4个步骤：量子传输，数据筛选，保密数据纠错和信息保密增强。经典通信中的误码消除技术常常会伴随通信信息的泄漏。实际量子保密通信误码消除过程需要极少的泄漏密钥的信息，并且泄漏的信息可以通过保密增强技术来消除[5,6]。

数据纠错技术是通信系统中不可缺少的部分，在量子保密通信中通常利用奇偶比较方法来构造各种纠错协议[7,8]，通常双方按照协议将生成的密钥分成段，并计算其奇偶性，然后在经典信道中进行奇偶比较。为了消除窃听者获得的信息，在每次比较结束双方丢掉一位。利用奇偶比较完全消除误码，需要多次在经典信道上进行通信。由于通信的次数会随着密钥长度增加而增加，通常n位的序列需要 $\log_2 n$ 次通信[7]，并且，为了安全起见每次通信前需要身份认证[9]，这样完全消除密钥误码过程需要的时间随着密钥增加而增加。

二元汉明码的纠错能力为 $t=1$，利用汉明码的校验矩阵 h 来构造校验码，Alice和Bob双方通过比较校验码来验证共享密钥的完整性，在文献[10]中用于量子密钥分发误码协调[10]。本文对奇偶-汉明纠错算法在量子密钥分发过程中的应用进行分析。

1 奇偶-汉明纠错算法

奇偶-汉明纠错算法利用了奇偶比较来检误，比较汉明校验码进行纠错。由于二元汉明码的纠错能力为 1，当某段的误码多于一个时利用汉明算法可能会引入误码。因此，汉明算法仅仅当密钥误码率很低，每段含一个误码以上可能很小时是很有效的。Alice, Bob 首先利用奇偶比较方法对误码进行一次比较，若奇偶性一致，则表示该段中没有误码或含有偶数个误码；若奇偶不一致，则表示含有奇数个误码，当误码率较低而且服从二相分布，则存在一个误码的概率远远大于奇数多个。然后利用汉明纠错方法对奇偶性不一致的进行纠错。通常为了减少泄漏的信息，在奇偶比较结束时丢掉最后一位。而利用汉明纠错算法则需丢掉 m 位，其位置为 $\{2^i\}(i\in\{0,...,m-1\})$。

二元汉明校验矩阵 $h^{(m)},(m\geq 3)$ 表述为

$$h_{i,j}^{(m)}=[\frac{j}{2^{i-1}}](\mathrm{mod}2) \tag{1}$$

例如当 $m\equiv 3$ 时，其矩阵表示为

$$h^{(3)}=\begin{bmatrix}1010101\\0110011\\0001111\end{bmatrix} \tag{2}$$

利用校验矩阵构造校验码 $S=\{S_i\}$，$i=1,...,m$，则 S_i 为

$$S_i=\left(\sum_{j=1}^{2^m-1}X_j h_{i,j}^{(m)}\right)(\mathrm{mod}\ 2)\in\{0,1\}^m \tag{3}$$

其中，$X_j(j=1,...,2^{m-1})$ 为合法通信双方（Alice,Bob）含有误码的一段密钥序列。双方进行纠错过程中在经典信道上发送 $S=\{S_i\}$，而不发送 X_j 本身。

利用奇偶-汉明纠错算法过程如下：Alice 和 Bob 选择相

基金项目：国家“973”计划基金资助项目(G2001039302)
作者简介：赵 峰(1979－)，男，博士生，主研方向：量子信息技术；王发强、郑力明，副教授；路轶群，研究员；刘颂豪，院士
收稿日期：2006-08-10 **E-mail：**qkd@scnu.edu.cn

同的参数 m 将生成的密钥序列分割为数段，每段长为 2^m 位，然后计算出奇偶性进行比较，完成后每段丢掉一位。对奇偶不一致的序列段用汉明校验矩阵构造校验码 $S=\{S_i\}$。然后 Alice 向 Bob 发送其构造校验码 S_a，Bob 收到后与自己的构造校验码 S_b 进行异或运算：

$$S_d = S_a \otimes S_b \tag{4}$$

则由 S_d 中的码组成的二进制数表示双方每段码中存在误码的位置，Bob 根据结果纠正自己的序列，使得与 Alice 一致，双方为了减小信息泄漏丢弃一部分数据。

2 效率分析

利用奇偶-汉明纠错方法进行纠错时通常关注两个方面：(1)完全消除误码需要在经典信道上通信的次数，因为泄漏的信息随着通信的次数增加而增加，所以在一定初始误码率下通信的次数越少越好；(2)码的生成效率，量子密钥生成速率相对较低，远远不能满足当前海量的经典通信加密解密的需要，因此要求码的生成效率越大越好。

若 Alice 和 Bob 从量子密钥分发实验中提取出 M 位原始密钥，其误码率为 p_0，然后将其分成 M/N 段，其中 $N=2^m(m\geq 3)$ 为每段二进制码的个数。通过一次奇偶比较后双方知道奇偶性有 S 段不同。若每段中的误码服从二相分布，则 S 可表示为

$$S \approx \frac{M}{N}\sum_{n=0}^{\frac{N}{2}-1} C_N^{2n+1} p_0^{2n+1}(1-p_0)^{N-2n-1} \tag{5}$$

为了消除窃听者获得的信息，在奇偶比较后每段丢掉一位，共丢掉 M/N 位码，再利用汉明纠错方法对奇偶性不一致的段进行纠错，结束后再丢掉 $S\log_2 N$ 位码。经过一次奇偶-汉明纠错后共丢掉

$$d = \frac{M}{N} + S\log_2 N$$

位码，因此，经过一次纠错后其码的剩余效率为

$$\mu = 1-\frac{1}{N}-\frac{1}{N}\sum_{n=0}^{\frac{N}{2}-1} C_N^{2n+1} p_0^{2n+1}(1-p_0)^{N-2n-1}\cdot\log_2 N \tag{6}$$

其结果如图 1 所示。

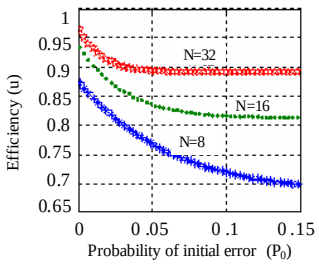

图 1 经过 1 次纠错后码的剩余效率

选择不同的参数 N，分别经过一次纠错后，码的剩余效率随着误码率的增加而减小，并且 N 越大，其效率越高。

经过一次纠错后其剩余码中的误码率可以表示为

$$p_n = \frac{M\cdot p_0 - S.p_1 + S\cdot(1-p_1) - (\frac{M}{N}+S\cdot\log_2 N)p_0}{M-\frac{M}{N}-S\cdot\log_2 N} \tag{7}$$

其中，$S\cdot p_1$ 为经过一次汉明纠错消除的误码个数；$S\cdot(1-p_1)$ 为由于汉明纠错引入的误码个数；

$(\frac{M}{N}+S\cdot\log_2 N)p_0$ 为丢弃码中含有的误码个数；p_1 为在奇偶性不一致的段中含有一个误码的概率，其表示为

$$p_1 = \frac{C_{N-1}^1 p_0(1-p_0)^{N-2}}{\sum_{n=0}^{N/2-1} C_{N-1}^{2n+1} p_0^{2n+1}(1-p_0)^{N-2n-2}} \tag{8}$$

由式(8)、式(7)可以表示为

$$p_n = p_0\frac{N-1-(2p_1-1+p_0\log_2 N)\sum_{n=0}^{\frac{N}{2}-1} C_N^{2n+1} p_0^{2n}(1-p_0)^{N-2n-1}}{N-1-\log_2 N\sum_{n=0}^{\frac{N}{2}-1} C_N^{2n+1} p_0^{2n+1}(1-p_0)^{N-2n-1}} \tag{9}$$

其结果如图 2 所示。

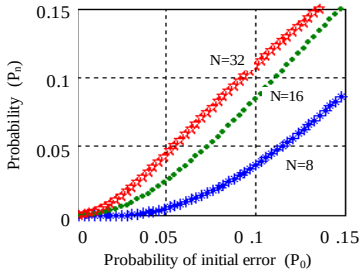

图 2 经过 1 次纠错后剩余码的误码率

图 2 表示利用不同的参数 N，在不同初始误码率下经过一次奇偶-汉明纠错后剩余码的误码率，图中随着 N 增大其纠错能力急剧下降，当 N=8 时其纠错能力最大。

3 实验分析

实验数据为在量子密钥分发实验中(BB84 协议)Alice 和 Bob 获得的 3 部分二进制随机序列。第 1 部分有 3 072 位，误码率为 10.90%；第 2 部分有 3 112 位，误码率为 7.68%；第 3 部分有 3 072 位，误码率为 3.81%。Alice 和 Bob 经过随机打乱后，分别利用不同的 N 对其进行分割，然后在经典信道上进行一次纠错。表 1 为利用不同的 N 进行分割后，用奇偶-汉明纠错算法分别进行一次纠错后的误码率变化情况。

表 1 利用不同的 N 进行分割，然后进行一次纠错后的误码率，从中可以看出随着 N 的增加其纠错能力急剧下降，当用 N＝32 已经很难消除初始误码率为 7.68%序列中的误码。

表 1 分析结果

误码率	N=8	N=16	N=32	N=64
10.90%	6.26%	10.19%	11.57%	11.35%
7.68%	3.62%	6.21%	7.56%	8.06%
3.81%	0.87%	1.74%	2.70%	3.86%
0.80%	0.00%	0.09%	0.18%	0.36%

表 2 为分别选择 N＝8 和 N＝16 利用奇偶-汉明纠错法完全消除误码在经典信道上需要的通信次数和纠正的码数。

表 2 通信次数和纠正的码数

	纠错次数	丢弃个数	纠正个数
N=8	3	1 577	239
N=16	6	1 697	239

从表 2 可以看出，选择不同的参数对同一组随机序列进行误码消除时，虽然用较小的 N 码进行一次纠错其生成效率低，但是较小的 N 具有较强的纠错能力，如表 1 所示，但是

完全消除误码过程所需的通信次数少，因此，最终码的生成效率高。同时也说明了奇偶-汉明纠错算法码的生成效率直接与初始误码率有关，而且利用小的 N 可以大大减少通信次数。在实验中每经过一次纠错，Alice 和 Bob 用相同的协议随机扰乱序列，使连续误码随机分布在序列中。同时，根据奇偶-汉明纠错算法的特点，误码率会随着纠错的次数增加而降低，因此，可以通过每次的奇偶比较结果来判断剩余码中存在的误码率。

4 安全性分析

密码学单向函数在现代密码学中起着重要的作用，它是一种易于计算而难于求逆的函数[11]。奇偶校验码和汉明纠错码都是将一定长度的信息压缩为一固定长度的输出，然而从其校验码却无法直接推出原信息，因此具有单向性[12,13]。在量子密钥分发过程中Alice在经典信道上给Bob只发送纠错信息 $S=\{S_i\}$，而Eve能窃听到他们的全部，然后试图从式(3)恢复出 $X=\{X_j\}$， 这样实际上就是一个未知量多于方程个数的方程组。从式(1)中可以看出，当 $m=3$ 时， $n=7$ 个未知数构成的式(3)的秩为 m，因此无法直接解出 $X=\{X_j\}$。基于线性码构造的单向函数其碰撞强度也随 m 增加而增强[14]。同时在公共信道上交换的信息通过经典加密后进行交换，在误码协调完成后，再利用秘密放大和密钥管理等经典方式来消除泄漏的信息。

5 讨论

应用于量子密钥分发的纠错算法其安全性和纠错效率都很重要，包括两部分：(1)完全消除误码在经典信道上通信的次数，信息泄漏随着通信次数的增加而增加，而每次经典信道上通信需要身份认证等来确认合法身份；(2)完全消除误码后剩余的码数，目前的通信需要海量的密钥来加密信息，而目前的量子密钥分发速率远远不能满足，因此完全消除误码后剩余码数是很重要的。奇偶-汉明纠错算法从理论和实验上显示该算法纠错效率高，其安全性由线性码构造的单向函数性能和经典加密技术保证，因此可以用于量子密钥分发过程的误码协调。

参考文献

1 Zbinden H, Gisin N, Huttner B, et al. Practical Aspects of Quantum Cryptographic Key Distribution[J]. Journal of Cryptology, 2000,13(7): 207-220.

2 Gisin N, Ribordy G, Tittel W, et al. Quantum Cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 150-151.

3 Bennett C H, Bessette F, Brassard G. Experimental Quantum Cryptography[C]//Proceedings of Eurocrypt'99. 1990.

4 Hoi-Kwong L. Method for Decoupling Error Correction from Privacy Amplification[J]. New Journal of Physics, 2003, 5(1): 1-24.

5 Bennett C H, Brassard G, Crepeau C. Generalized Privacy Amplification[J]. IEEE Transactions on Information Theory, 1995, 41(6).

6 Brasard G, Salvail L. Secret Key Reconciliation by Public Discussion[C]//Proc. of Eurocrypt'94. 1994.

7 Kuritsyn K. Modification of Error Reconciliation Scheme for Quantum Cryptography[C]//Proc. of SPIE'03. 2003.

8 Nakassis A, Biefang J, Williams C. Expeditious Reconciliation for Practical Quantum Key Distribution[C]//Proc. of SPIE'04. 2004.

9 LÜtkenhaus N. Estimates for Practical Quantum Cryptography[J]. Phys. Rev. A, 1999, 59(5): 3301-3319.

10 Buttler W T, Lamoreaux S K, Torgerson J R, et al. Fast, Efficient Error Reconciliation for Quantum Cryptography[J]. Physical Review A, 2003, 67(5): 1-8.

11 Goldreich O. 密码学基础[M]. 温巧燕, 杨义先, 译. 北京: 人民邮电出版社, 2003.

12 Menezes A J, Van Oorschot P C, Vantone S A. Hand Book of Applied Cryptography[M]. Boca Raton: CRC Press, 1997.

13 刘跃峰, 马康玉, 刘 超. 基于非二进制纠错码的函数的构造及应用[J]. 计算机工程, 2004, 30(4): 115-116.

14 Knudsen L, Preneel B. Construction of Secure and Fast Hash Functions Using Nonbinary Error-correcting Codes[J]. IEEE Transactions on Information Theory, 2002, 48(9): 2530-2533.

(上接第 21 页)

5 结论

本文提出了一种新的基于局部灰度概率统计和图像方向信息测度的小目标检测方法。局部灰度概率分布统计可有效表征红外图像中的奇异点，抑制平缓背景和弱的边缘，突出目标；图像的方向信息测度统计可有效表征目标点和边缘点的差异，滤除强边缘干扰点。利用局部灰度概率统计和图像方向信息测度统计，对红外图像进行处理，大幅减少了候选目标点的数量，节省了后续多帧决策处理的计算量和存储量，提高了算法的整体效率。实验表明，算法简单有效，对复杂背景下运动小目标的检测取得了很好的效果。进一步优化算法，提高定位精度，并结合有效的目标跟踪方法，进行小目标检测和跟踪系统的工程实现，是下一步的工作方向。

参考文献

1 Adar S, Buganim S, Rotman S R. Analyzing Point Target Detection Algorithms//Proceedings of the SPIE.'05 2005: 249-256.

2 Zhang Wei, Cong Mingyu. Algorithms for Optical Weak Small Targets Detection and Tracking: Review[C]//Proceedings of the 2003 International Conference on Neural Networks and Signal Processing. 2003: 643-647.

3 Desai U B, Shabbir N. Small Object Detection and Tracking: Algorithm, Analysis and Application[C]//International Conference on Pattern Recognition and Machine Intelligence. 2005: 108-117.

4 彭嘉雄, 周文林. 红外背景抑制与小目标分割检测[J]. 电子学报, 1999, 27(12): 47-51.

5 Yang L, Yang J. Adaptive Detection for Infrared Small Target Under Sea-Sky Complex Background[J]. Electronics Letters, 2004, 40(17).

6 王广君, 田金文. 基于局部熵的红外图像小目标检测[J]. 红外与激光工程, 2000, 29(5): 26-29.

7 Samy R A, Jean-Francois B. Robust Estimation of Texture Parameters for Small-target Detection in Clutter, Targets and Backgrounds: Characterization and Representation III[C]//Proceedings of SPIE'97 1997: 2-9.

8 徐 英, 周金鹏. 基于邻域灰度分布的 IR 弱小目标检测[J]. 国防科技大学学报, 2002, 24(5): 84-87.

9 Schwering P. Infrared Cloud Background Clutter[C]//Proceedings of SPIE'92. 1992: 311-322.

10 杨海军, 梁德群. 基于图像方向性信息测度的图像象素分类[J]. 中国图象图形学报, 2001, 6A(5): 429-433.

11 Tzannes A P. Detection of Point Targets in Image Sequences by Hypothesis Testing: a Temporal Test First Approach[C]//IEEE International Conference on Acoustics, Speech, and Signal Processing. 1999: 3377-3380.