·安全技术· 文章编号：1000-3428(2017)04-0122-04 文献标志码：A 中图分类号：TP309

# 星地量子密钥分发中的数据协调方法

钟先锋，汤 煜，金 标，吴 腾，李凤芝，刘尉悦

（宁波大学 信息科学与工程学院，浙江 宁波 315211）

**摘 要：**量子密钥分发是基于量子物理基本定律来确保通信双方的安全性。低交互次数的数据协调是星地量子密钥分发数据后处理阶段的关键，依据星地量子密钥分发中数据协调的特性和要求，提出一种基于 Turbo 码的星地量子密钥分发数据协调模型。该模型重新修改和设计 Turbo 码的编解码模型及其译码算法，可解决星地量子密钥分发的数据协调过程需多次信息交互的问题。仿真结果表明，经过一定的迭代次数后，Turbo 码可完成不同误码率下密钥的数据协调。

**关键词：**量子保密通信；星地量子密钥分发；数据协调；Turbo 码；模型仿真

**中文引用格式：**钟先锋，汤 煜，金 标，等. 星地量子密钥分发中的数据协调方法[J]. 计算机工程，2017，43(4)：122-125.

**英文引用格式：**Zhong Xianfeng，Tang Yu，Jin Biao，et al. Data Reconciliation Method in Satellite Quantum Key Distribution[J]. Computer Engineering，2017，43(4)：122-125.

# Data Reconciliation Method in Satellite Quantum Key Distribution

ZHONG Xianfeng，TANG Yu，JIN Biao，WU Teng，LI Fengzhi，LIU Weiyue

（College of Information Science and Engineering，Ningbo University，Ningbo，Zhejiang 315211，China）

**【Abstract】**Quantum key distribution applies fundamental laws of quantum physics to guarantee secure communication. Few number of information exchanges is the key of satellite-based quantum key distribution. According to the characteristics and requirements of data reconciliation in satellite quantum key distribution，this paper presents a kind of new data reconciliation model of satellite-based quantum key distribution based on the Turbo codes. The coding and decoding models of Turbo codes are modified and designed，and this model solves the numbers of information exchanges. Simulation result shows that through a number of iterations，Turbo codes can complete the reconciliation of the key in different bit error rate.

**【Key words】**quantum cryptography communication；satellite quantum key distribution；data reconciliation；Turbo codes；model simulation

**DOI：**10.3969/j.issn.1000-3428.2017.04.021

## 0 概述

量子保密通信是经典通信和量子力学相结合的产物，其无条件安全的特点使它成为一种全新的安全通信技术[1-4]，而量子密钥分发作为其中最先获得应用的分支，近年来受到广泛关注[5]。量子密钥分发使用单光子作为信息载体，利用单光子的不可分割、不可克隆原理确保在通信双方建立相同且安全的密钥。然而在实际的密钥分发中，由于地面光纤信号和自由空间量子密钥分发的距离限制，难以实现全球量子密钥分发，因此以卫星为中继，可以有效地解决这个问题。通过最近的一些理论和实验进展可知，星地量子密钥分发实验已经成熟并且成为当前的研究热点[6-8]。

在量子密钥分发中，2 个合法用户 Alice 和 Bob 在密钥分发后会拥有不一致的密钥 $X$ 和 $Y$，双方通过理想公共授权信道传送部分信息从 $X$ 和 $Y$ 中得到一致的密钥，这一过程称为数据协调。在星地量子密钥分发中，卫星和地面站之间通过链路窗口完成数据协调，需要很高的实时性，即在数据协调中需要

**基金项目：**浙江省自然科学基金(LY13F050007，LY17F050004)。

**作者简介：**钟先锋(1992—)，男，硕士研究生，主研方向为量子通信；汤 煜、金 标、吴 腾、李凤芝，硕士研究生；刘尉悦(通信作者)，副教授、博士。

**收稿日期：**2016-03-10 **修回日期：**2016-05-05 **E-mail：**18645043633@163.com

一个低交互次数的算法。然而现有的数据协调模型需要通信双方多次交互信息,不能很好地应用在星地量子密钥分发中。Turbo 码有着优异的纠错性能,且只需要一次信息交互[9-13],故考虑将其应用到星地量子密钥分发。依据星地量子密钥分发中数据协调的特性和要求,本文提出一种基于 Turbo 码的数据协调的模型。

## 1　基于 Turbo 码的数据协调

### 1.1　传统的 Turbo 码系统

图 1 是传统 Turbo 码系统的框图,编码端由 2 个并行级联的系统卷积编码器(Recursive System Coder,RSC)、交织器、删余器组成。常见的分量码有:(7,5),(13,15),(37,21)。交织器可以选择伪随机交织,也可以选择块交织,但块交织不如伪随机交织的性能好,通过交织改变密钥序列的位置,使 2 个系统卷积编码器输出的校验位相关性减弱。在编码端,将编码后的校验比特和信息比特一起送入删余器,删余器的作用是从总体上改善 Turbo 码的码率。最后将删余后的比特经过信道传输给译码端。

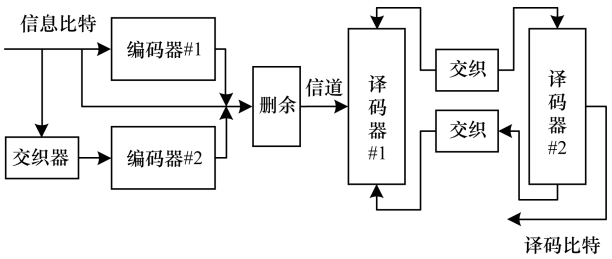


**图 1　Turbo 码系统框图**

译码端主要是由 2 个独立的软输入、软输出译码器并行级联而成,译码器基于 Log-map 算法。译码端采用循环迭代译码,在首次迭代中,译码器#1 输入信息符号概率即先验信息初始化为零,译码后的输出信息符号概率即外信息在交织后用作译码器#2 的先验信息,然后译码器#2 生成的信息符号概率经过解交织后反馈到译码器#1 作为下一轮译码的先验信息。重复上述过程直到达到一定迭代次数为止,最后对译码器#2 的输出信息符号概率进行硬判决得到译码比特。

### 1.2　基于 Turbo 码的数据协调模型

在星地量子密钥分发中,密钥是通过量子信道传输的。在密钥分发后,卫星和地面站会分别拥有密钥序列 $X$ 和 $Y$。在理想情况下,密钥序列应该是一致的,然而在实际量子密钥分发中,由于信道固有损耗及地球曲率、水平大气衰减等因素的影响,卫星和地面站拥有的密钥序列 $X$ 和 $Y$ 会存在一定的误码率。通过 Turbo 码对密钥序列进行数据协调,使得其拥有一致的密钥序列。

在传统的 Turbo 码编解码的模型中,对信息位和编码后的校验位一起传输给译码端。译码端利用校验位对传输中信息的误码进行纠正。而在基于 Turbo 码的数据协调模型中,只将编码后的校验位通过可靠的经典信道传输给译码端,译码端利用此校验位对量子密钥分发后的密钥序列 $Y$ 进行迭代译码,最后译码的输出为 $X'$。如果数据协调成功,那么 $X$ 和 $X'$将会完全一致。

### 1.3　仿真模型的建立

Turbo 码的译码是基于最大后验概率(Maximum A Posterior Probability,MAP)算法,MAP 算法的软输出译码信息用如下似然比定义[14-16]:

$$L_{\mathrm{MAP}}(x_k)=\frac{\sum\limits_{(s',s)\in S^+}\alpha_{k-1}(s')\cdot\gamma_k(s',s)\cdot\beta_k(s)}{\sum\limits_{(s',s)\in S^-}\alpha_{k-1}(s')\cdot\gamma_k(s',s)\cdot\beta_k(s)} \tag{1}$$

其中,$\alpha_{k-1}(s')$表示在码字格图中从初始状态到$k-1$时刻状态的前项递推值;$\beta_k(s)$表示在码字格图中从 $k$ 时刻状态到编码结束时编码器状态的后项递推值;$\gamma_k(s',s)$表示在码字格图中从 $k-1$ 时刻状态到 $k$ 时刻状态的 $s$ 分支度量值。

在式(1)的译码输出似然比的计算中,分子表示译码器输入的比特信息为 1 时的所有可能的状态转移,分母表示译码器输入的比特信息为 0 时的所有可能的状态转移。$\alpha_{k-1}(s')$和 $\beta_k(s)$的计算方法与原始的 Turbo 译码中的计算方法一样,而 $\Pr(p'_k|p_k)=1$ 表示状态的转移,依据信道的不同会有不同的计算方法。一般地,计算公式如下:

$$\begin{aligned}\gamma_k(s',s)&=\Pr(s_k=s,y_k|s_{k-1}=s')\\&=\Pr(y_k|x_k)\cdot\Pr(x_k)\end{aligned} \tag{2}$$

式(2)可以作如下分解:

$$\Pr(x_k)=\frac{\exp\left(\frac{1}{2}L_a(x_k)\right)}{1+\exp\left(\frac{1}{2}L_a(x_k)\right)}\cdot\exp\left(\frac{1}{2}x_kL_a(x_k)\right)$$

$$\Pr(y_k|x_k)=\Pr(x_k|x_k)\cdot\Pr(p'_k|p_k) \tag{3}$$

其中:

$$L_a(x_k)=\ln\left[\frac{\Pr(x_k=+1)}{\Pr(x_k=-1)}\right] \tag{4}$$

在量子密钥分发中,密钥首先是经过量子信道传输,在其数据协调阶段,Alice 和 Bob 双方共享的密钥存在量子比特误码率 $Q$。在数据协调中,Alice 对其密钥编码后产生一串校验位,并通过可靠的经典信道将其传输给 Bob,即 $\Pr(p'_k|p_k)=1$。故式(3)可以表示如下:

$$\begin{aligned}\Pr(y_k|x_k)&=\Pr(x'_k|x_k)\cdot\Pr(p'_k|p_k)\\&=1-Q\end{aligned} \tag{5}$$

综上,在 Turbo 码中式(2)可以表示如下:

$$\gamma_k(s',s)=(1-Q)\frac{\exp\left(\frac{1}{2}L_a(x_k)\right)}{1+\exp\left(\frac{1}{2}L_a(x_k)\right)}\cdot\exp\left(\frac{1}{2}x_kL_a(x_k)\right) \tag{6}$$

在完成迭代译码后,可进行如下译码的硬判决:

$$y_k=\begin{cases}1, L_{\text{MAP}}\geqslant 0\\ 0, L_{\text{MAP}}\leqslant 0\end{cases} \tag{7}$$

在 Turbo 码仿真中,一般把 MAP 算法中的变量都转换为对数的形式,此时译码器的输出可以用对数似然比表示如下:

$$LnL_{\text{MAP}}=\text{In}\sum_{(s',s)\in S^+}\alpha_{k-1}(s')\cdot\gamma_k(s',s)\cdot\beta_k(s)-\text{In}\sum_{(s',s)\in S^-}\alpha_{k-1}(s')\cdot\gamma_k(s',s)\cdot\beta_k(s) \tag{8}$$

这样可以把乘法运算转换为加法运算,大大降低译码复杂度,降低纠错耗时。

## 2 模型的参数设计及仿真

为了进一步分析 Turbo 码的性能,根据仿真模型,编写了 Turbo 码的仿真程序,仿真中对编码后传输的校验比特位随机翻转,用以模拟卫星和地面站在量子密钥分发中产生的误码率,其仿真流程如图 2 所示。

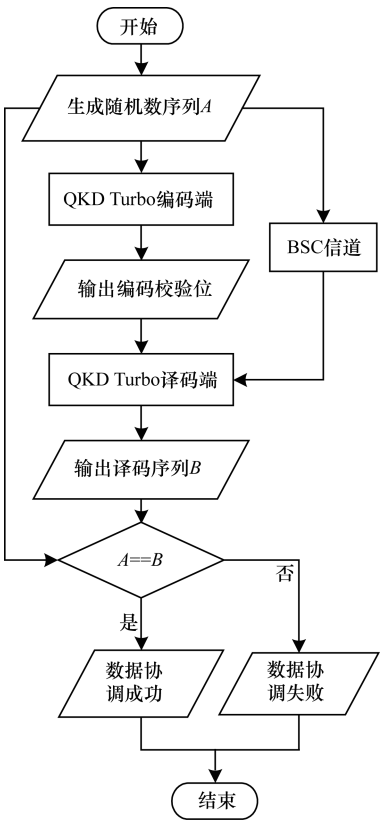


**图 2 Turbo 码仿真流程**

分量码和迭代次数是影响 Turbo 算法数据协调性能的关键因素,在下面的仿真中,帧长设置为 2 048,码率为 0.72。图 3 为不同迭代次数下的 Turbo 码的纠错性能。从图中可以看出,随着迭代次数的增加,QBER 曲线不断降低并趋于收敛;而且随着纠错前误码率的增大,迭代对误码率的影响更加明显。4 次~6 次迭代以后 QBER 性能曲线就已经收敛,继续迭代所带来的增益是非常小的。图 4 给出了不同分量码下 Turbo 码的纠错性能。在仿真中,连续传输 100 帧长度为 2 048 的随机数,迭代译码的次数为 6。从图中可以看出在给定帧长和码率的情况下,随着纠错前误码率的增加,约束长的 Turbo 码的性能优势越来越明显。考虑到量子密钥分发后误码率一般在 3% 左右,而译码复杂度随约束长度的增加呈指数递增,因此从性能和复杂性方面综合考虑,选择约束长度为 4 的分量码来构造 Turbo 算法比较适当。

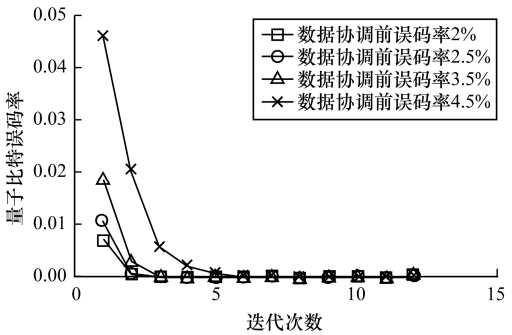


**图 3 迭代次数对 Turbo 码的纠错性能影响**

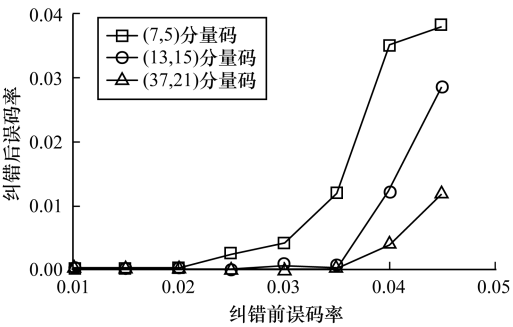


**图 4 分量码对 Turbo 码的纠错性能影响**

以上 2 组的仿真结果便于分析找出合适的参数。综合分析上述结果,将仿真参数做如下设置:迭代次数为 6,采用(13,15)分量码。仿真中每次随机产生 4K 密钥比特并随机翻转部分比特,使其产生 3% 左右的误码率,利用 Turbo 码对密钥进行纠错。对纠错前后误码率进行比对,对比结果如图 5所示,一共给出了 20 次的模拟结果。从图中可以看出,存在误码率的密钥在经过 Turbo 码的数据协调后,得到纠错后的误码率为零,达到了数据协调的目的。

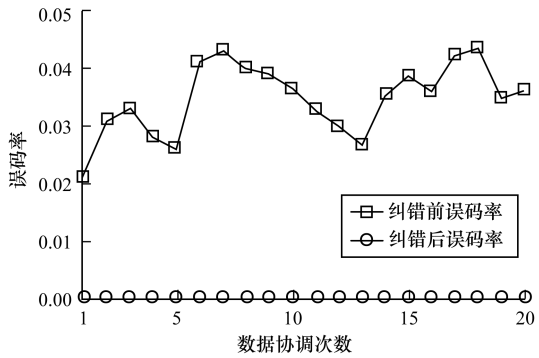


**图 5　纠错前、后误码率对比图**

## 3　结束语

结合密钥分发中数据协调的特性,本文提出一种基于 Turbo 码的星地量子密钥分发数据协调模型,重新修整 Turbo 码的编解码模型以及译码算法,使其能完成数据协调中密钥的纠错。对该模型中的参数进行仿真和研究,可以针对不同误码率情况来调整模型参数,在保证纠错性能的同时提高数据协调的系统性能。采用此模型可以有效地解决现有算法中数据协调需要多次信息交互的问题。仿真结果表明,经过一定次数的迭代后,Turbo 码可完成不同误码率下密钥的数据协调,同时也证明了该模型在未来星地量子密钥分发中应用的可行性。

### 参考文献

[1] Bennett C H, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing[C]//Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. New York, USA: IEEE Press, 1984: 175-179.

[2] Gisin N, Ribordy G, Tittle W, et al. Quantum Cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

[3] 薛　鹏,郭光灿. 量子通信[J]. 物理, 2012, 33(6): 385-391.

[4] 印　娟. 自由空间量子通信实验研究[D]. 合肥:中国科学技术大学, 2009.

[5] 吴　光. 长距离量子密钥分发系统[D]. 上海:华东师范大学, 2007.

[6] Perdigues A J M, Furch B, Matos C J, et al. Quantum Communications at ESA: Towards Aspace Experiment on the ISS[J]. ACTA Astronautica, 2008, 63(1-4): 165-178.

[7] Hughes R J, Buttler W T, Kwiat P G, et al. Quantum Cryptography for Secure Satellite Communications[C]//Proceedings of IEEE Aerospace Conference. Washington D. C., USA: IEEE Press, 2000: 191-200.

[8] Stucki D, Gisin N, Guinnard O, et al. Quantum Key Distribution over 67 km with a Plug & Play System[J]. New Journal of Physics, 2002(4): 1-8.

[9] Lo H K, Curty M, Tamaki K. Secure Quantum Key Distribution[J]. Nature Photonics, 2014, 8(3): 595-604.

[10] 赵　峰,王发强,郑力明,等. 量子密钥分发误码协调算法分析[J]. 计算机工程, 2007, 33(12): 22-24.

[11] 刘　洋. 远距离量子密钥分发相关研究[D]. 合肥:中国科学技术大学, 2012.

[12] 刘东华. Turbo 码关键技术及 Turbo 原理的应用研究[D]. 长沙:国防科学技术大学, 2003.

[13] Richard J, Jane E, Charles G. Practical Free Space Quantum Key Distribution over 10 km in Daylight and at Night[J]. New Journal of Physics, 2002(4): 12-16.

[14] 吴　光. 长距离量子密钥分发系统[D]. 上海:华东师范大学, 2007.

[15] 梁福来. Turbo 码译码算法及交织器的研究[D]. 秦皇岛:燕山大学, 2013.

[16] Wang Hanxin, Chen Shaoping, Zhu Cuitao. Optimal Design for Turbo Code's Iterative Decoding [J]. Computer Engineering and Applications, 2007, 43(3): 99-101.

编辑　索书志

(上接第 121 页)

[9] Lochert C, Mauve M, Fussler H, et al. Geographic Routing in City Scenarios [J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2005, 9(1): 69-72.

[10] Gaito S, Maggiorini D, Pagani E, et al. Distance Vector Routing for Public Transportation Vehicular Networks: Performance Evaluation on a Real Topology[C]//Proceedings of IFIP Wireless Days. New York, USA: IEEE Press, 2009: 338-342.

[11] 陶　冰,李德敏,张光林,等. 基于公交车骨干网的区域路由协议研究[J]. 计算机工程, 2016, 42(3): 7-12.

[12] Kwangsun Y. Multiple Attribute Decision Analysis with Imprecise Information [J]. IIE Transactions, 1989, 21(1): 21-26.

[13] Simon H A. The New Science of Management Decision[M]. Newark, USA: Prentice Hal PTR, 1977.

[14] Laarhoven P, Pedrycz W. A Fuzzy Extension of Saaty's Priority Theory [J]. Fuzzy Sets and Systems, 1983, 11(3): 229-241.

[15] Tzeng G H, Huang J J. Multiple Attribute Decision Making, Methods and Applications[J]. Lecture Notes in Economics and Mathematical Systems, 2011, 37(5): 1-531.

[16] Opricovic S, Tzeng G H. Defuzzification with a Fuzzy Multicriteria Decision Model[J]. International Journal of Uncertainty, Fuzziness and Knowledge Based Systems, 2003, 11(5): 635-652.

[17] Opricovic S, Tzeng G H. Fuzzy Multicreteria Model for Post-earthquake Land Use Planning[J]. Natural Hazards Reviews, 2003, 4(2): 59-64.

[18] Soares V, Rodrigues J, Farahmand F. Performance Assessment of a Geographic Routing Protocol for Vehicular Delay-tolerant Networks[C]//Proceedings of IEEE Wireless Communications and Networking Conference. Washington D. C., USA: IEEE Press, 2012: 2526-2531.

编辑　刘　冰