量子电子学报 2012, 29(1) 63-68 DOI: ISSN: 1007-5461 CN: 34-1163/TN

本期目录 | 下期目录 | 过刊浏览 | 高级检索　　[打印本页]　[关闭]

量子光学

基于量子隐写术的计算安全比特承诺协议

曹东[1], **宋耀良**[1,2]

1 南京理工大学电子工程与光电技术学院， 江苏 南京 210094；
2 南京邮电大学通信与信息工程学院， 江苏 南京 210003

摘要：

在量子比特承诺协议中，目前流行的方案没有很好地解决信道噪声的影响，实用性不强。根据量子隐写术对信息的隐藏性，提出一种新的量子比特承诺协议。提出了利用量子信道噪声结合遮盖比特隐藏敏感信息，同时采用量子纠错码的方法克服信道噪声，有效地抵抗了第三方窃听攻击和噪声对信息的影响和破坏。通过理论分析与仿真证明该协议的绑定性和完善隐蔽性；理论证明了方案的有效性，为量子密码协议的推广应用提供了理论基础。

关键词： 量子信息　量子密码　比特承诺　量子隐写术

Computationally secure bit commitment protocol based on quantum steganography

Cao Dong[1]，Song Yaoliang[1,2]

1 School of Electronic Engineering & Optoelectronic Technology, Nanjing University of Science & Technology, Nanjing 210094 , China;
2 College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 21003, China

Abstract:

In quantum bit commitment (QBC), most existed proposals of them analyze little of communicating an innocent message over noisy quantum channels. These methods are not practical. Based on the information hiding characteristics of quantum steganography, we propose a novel QBC. An elegantly scheme is presented for disguising secret information as quantum noise, and embedding it in stego qubits which encode into a codeword of quantum error-correcting code. The method is proved secure and effectiveness in the presence of noisy quantum channel and a potential eavesdropper. The results of theoretical analysis and numerical simulation show that the proposed scheme has perfect concealing and binding properties. Theoretical analysis proved the validity. The method forms a theoretical basis for the promotion and application of quantum cryptographic protocols.

Keywords: quantum information　quantum cryptography　bit commitment　quantum steganography

收稿日期 2011-05-16 **修回日期** 2011-06-27 **网络版发布日期** 2012-01-28

DOI:

基金项目:

国家自然科学基金(61071145, 41074090),教育部博士点专项基金(200802880014)资助

通讯作者: 男，1960年生，教授，博士生导师，研究方向为自适应信号处理，量子信息，通信系统理论与设计。

作者简介: 曹东(1974-)，博士生，讲师，主要研究方向为信号处理，量子信息安全。E-mail:caodongcn@gmail.com
作者Email: ylsong@mail.njust.edu.cn

扩展功能

本文信息

- Supporting info
- PDF(802KB)
- [HTML全文]
- 参考文献[PDF]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 引用本文
- Email Alert
- 文章反馈
- 浏览反馈信息

本文关键词相关文章

- 量子信息
- 量子密码
- 比特承诺
- 量子隐写术

本文作者相关文章

- 曹东
- 宋耀良

PubMed

- Article by Cao,d
- Article by Song,Y.L

参考文献：

[1] Blun M. Coin flipping by telephone[C]. Proc IEEE Sprint COMPCOM, Las Vegas, 1982:133-137.
[2] Naor M. Bit commitment using pseudorandomness[J]. Journal of Cryptology, 1991, 2(2): 151-158.
[3] Damgard I and Fujisaki E. An integer commitment scheme based on groups with hidden order[C]. Advances in Cryptology －ASIACRYPT, New Zealand, 2002: 125-142.
[4] Brassard G, Crepeau C, Jozsa R and Langlois D. A quantum bit commitment scheme provably unbreakable by both parties[C]. Proceedings of 34th Annual IEEE Symposium on the Foundations of

Computer Science. Palo Alto, California, USA, 1993: 362-371.

[5] Andrew C C Yao. Security of quantum protocols against coherent measurements[C]. Proceedings of 26th Annual ACM Symposium on the Theory of Computing. Las Vegas, Nevada, USA, 1995:67-75.

[6] Mayers D. Unconditional secure quantum bit commitment is impossible[J]. Phys. Rev. Lett, 1997, 78: 3414-3417.

[7] Lo H K. Insecurity of quantum secure computations[J]. Phys. Rev. A, 1997, 56:1154-1162.

[8] Ramos R V, Mendonca F A. Quantum bit commitment protocol without quantum memory. http://arxiv.org/abs/0801.0690v1, 2008.

[9] Magnin L, Magniez F, Leverrier A, Cerf N J. Strong no-go theorem for gaussian quantum bit commitment[J]. Phys. Rev. A, 2010, 81(1):010302

[10] Li Q, Li C, Long D Y, Chan W H, Wu C H. On the impossibility of non-static quantum bit commitment between two parties. http://arxiv.org/abs/1101.5684v1,2011.

[11] Chailloux A, Kerenidis I. Optimal bounds for quantum bit commitment. http://arxiv.org/abs/1102.1678v1 ,2011.

[12] Shaw B A, Brun T A. Quantum Steganography. http://arxiv.org/abs/1006.1934, 2010.

[13] Shaw B A, Brun T A. Hiding Quantum Information in the Perfect Code. http://arxiv.org/abs/1007.0793, 2010.

[14] Ben-Aroya A, Ta-Shma A. On the complexity of approximating the diamond norm. http://arxiv.org/abs/0902.3397v3, 2009.

[15] Watrous J. Semidefinite programs for completely bounded norms. http://arxiv.org/abs/0901.4709v2, 2009.

[16] Benenti G, Strini G. Computing the distance between quantum channels: usefulness of the Fano representation[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2010, 43(21): 215508.

[17] Nielsen M A, Chuang I L. Quantum computation and quantum information. Higher Education Press. 2003, page379.

[18] 张守林, 张盛, 王剑. 基于压缩态的连续变量量子对话协议[J]. 量子电子学报, 2011, 28(3): 335-340 Zhang S L, Zhang S, Wang J. Continuous variable quantum dialogue protocol based on squeezed state[J]. Chinese Journal of Quantum Electronics. 2011, 28(3): 335-340

本刊中的类似文章

1. 朱勋 王干全.一种新的关于两电子纠缠的判据[J]. 量子电子学报, 2009,26(3): 297-300

2. 石市委 易佑民 .使用共振腔实现受控非门及量子隐形传态的方案[J]. 量子电子学报, 2009,26(3): 301-305

3. 李冬梅.利用线性光学器件实现三体纠缠相干态的纠缠交换[J]. 量子电子学报, 2009,26(4): 446-450

4. 唐世清 张登玉 高峰 谢利军 詹孝贵.在双模腔QED系统中用原子-腔共振相互作用实现三量子比特Toffoli门[J]. 量子电子学报, 2009,26(5): 548-554

5. 丁智勇 何娟 吴韬.利用超导量子相干装置一步制备W类纠缠态[J]. 量子电子学报, 2010,27(3): 314-318

6. 潘桂侠.用 GHZ态实现任意两粒子态的量子信息分离方案[J]. 量子电子学报, 2010,27(5): 573-579

7. 王启文 红兰.抛物量子点中的二能级体系[J]. 量子电子学报, 2011,28(1): 110-114

8. 颜伟 倪林.基于量子联合测量的紧框架构造方法研究[J]. 量子电子学报, 2011,28(1): 44-51

9. 万旭 崔珂 高原 张鸿飞 罗春丽 王坚.量子密钥分发系统中高精度同步方案设计[J]. 量子电子学报, 2011,28(3): 324-328

10. 张守林 张盛 王剑.基于压缩态的连续变量量子对话协议[J]. 量子电子学报, 2011,28(3): 335-340

11. 陈永志 刘云 温晓军.一个量子代理弱盲签名方案[J]. 量子电子学报, 2011,28(3): 341-349

12. 李满兰 叶柳.利用GHZ态实现单粒子直积态的量子信息分裂[J]. 量子电子学报, 2011,28(6): 693-698

13. 杨霏 丛爽.量子系统的纠缠探测与纠缠测量[J]. 量子电子学报, 2011,28(4): 391-401

14. 何娟 丁智勇 吴韬 于立志 倪致祥.实现三比特量子控制相位门的离子阱方案[J]. 量子电子学报, 2011,28(4): 429-433

15. 陈新 施钧辉 葛运健 双丰.自旋链中量子信息的完美传输与量子链中态的完美操控[J]. 量子电子学报, 2011,28(5): 564-570