量子电子学报 2012, 29(1) 69-73 DOI: ISSN: 1007-5461 CN: 34-1163/TN

量子光学

基于量子特性的多人签名方案

赵龙[1],曹正文[1],罗锐[2],徐萍[1],康维宏[1]

1 西北大学信息科学与技术学院, 陕西 西安, 710127;
2 中国电子科技集团公司第二十研究所, 陕西 西安 710068

摘要:

针对多人参与签名的情况，提出了一种量子签名方案。发送方利用Hash函数得到任意位经典消息的摘要信息，并将该摘要信息转化为量子比特。签名各方用自己的私钥与经典消息的摘要信息进行异或运算，运用所得序列依次对该量子比特做幺正变换，将变换后的量子比特作为签名信息。签名的验证工作由一个可信赖的仲裁执行，验证过程引入了奇偶校验原理。分析表明，该方案所产生的签名信息不会因为签名人数的增多而变长，具有较高的通信效率，并且验证过程简单。

关键词: 量子密码 多人签名 幺正变换 量子密钥分配

Multi-signature scheme based on quantum properties

ZHAO Long[1], CAO Zhengwen[1], LUO Rui[2], Xu ping[1], KANG Weihong[1]

1 College of Information Science and Technology, Northwest University, Xi’an 710127, China;
2 20th Research Institute of China Electronics Technology Group Corporation, Xi’an 710068, China

Abstract:

A quantum signature scheme is proposed for multiple people signature situation. The digest of the classical message of any length is got via Hash function and transformed into quantum bits in the sender. Each signatory uses his private key XOR the digest and gets a sequence. The quantum bits is performed a controlled unitary transformation according to the sequence by the signatory in turn, and signature information is state of the quantum bits. A trusted arbitrator is presented to verify the signature. The progress of verification uses idea of classical parity. Analysis shows that the length of the signature doesn’t get longer with the number of signatory increased in the scheme. The communication efficiency is high, and the progress of verification is simple.

Keywords: quantum cryptography multi-signature unitary transformation quantum key distribution

收稿日期 2011-02-15 **修回日期** 2011-06-14 **网络版发布日期** 2012-01-28

DOI:

基金项目:

陕西省教育厅自然科学专项基金资助项目（08JK444），省教育厅产业化示范项目（2010JC24）

通讯作者: 曹正文（1969-），女，湖南人，硕士生导师，从事通信、导航技术方面的研究。

作者简介: 赵龙 （1987-）陕西人，硕士生，从事量子保密通信理论的研究。Email：zhaolong1029@163.com

作者Email: caozhw@nwu.edu.cn

参考文献:

[1]曾贵华，马文平，王新梅，等.基于量子密码的签名方案[J].电子学报，2001，29(8)：1098-1100.
[2]Gottesman D, Chuang I. Quantum digital signatures[EB/OL]. http://arxiv.org/abs/quant-ph/0105032, 2001.

[3]Hwayean Lee, Changho Hong, Hyunsang Kim, et al. Arbitrated quantumn signature scheme with message recovery[J]. Physics Letters A 2004, 321: 295-300.
[4] LU X, FENG D G. An arbitrated quantum message signature scheme[A]. In: J. Zhang, J. －H. He, and Y. Fu. Lecture Notes in Computer Science[C]. Berlin Heidelberg: Springer-Verlag, 2004:1054-1060
[5]王剑，张全，唐朝京. 针对经典消息的高效量子签名协议[J]. 通信学报，2007，28(1)：64-68.
[6]温晓军. 安全量子身份认证与信息签名协议的研究[D]. 北京：北京交通大学2007.
[7]Nielsen M. Chuang I量子计算和量子信息（二）[M]. 郑大钟，赵千川 译.北京:清华大学出版社,2004.
[8]曾贵华,王新梅,量子密码协议的改进[J]. 通信学报，2000，21（2）：60-63.
[9]邓富国，周萍，李熙涵，等. 量子安全直接通信研究进展[J]. 原子核物理评论，2005，22(4)：382-385.
[10]Bandyopadhyay S. Teleportation and secret sharing with pure entangled states[J]. Physical Review A, 2000, 62: 012308-1-5.
[11]Buhrman H, Cleve R, Watrous J, et al. Quantum Fingerprinting[J]. Physical Review Letters, 87: 167902.
[12]Peter W.Shor, John Preskill. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical review letters 2000 85(2): 441-444.

本刊中的类似文章

1．吕洪君 郭俊旺 彭斐 吴天昊 解光军.用基本两位量子逻辑门实现N位量子逻辑门的研究[J]. 量子电子学报, 2010,27(1): 26-30
2．周媛媛 李晓强 周学军.基于预报单光子源的BB84诱惑态量子密钥分配研究[J]. 量子电子学报, 2010,27(5): 565-572
3．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
4．王东 查新未.基于Cluster态的量子通信[J]. 量子电子学报, 2011,28(6): 687-692
5．曹东 宋耀良.基于量子隐写术的计算安全比特承诺协议[J]. 量子电子学报, 2012,29(1): 63-68