中国科学院研究生院学报 2011, 28(2) 262-265 DOI: ISSN: CN:

论文

关于一个数值比较协议的安全性证明

邵秀凤[1], **李荣花**[2]

1. 北京城市学院人工智能研究所, 北京 100083;
2. 中国科学院研究生院信息安全国家重点实验室, 北京 100049

摘要:

Cachin在1990年的ACM计算机和通信安全会议上提出了一个电子竞价和拍卖协议,并给出了协议的安全性证明. 我们分析发现Cachin的协议证明中存在一个错误,并纠正了这个错误.

关键词: 信息安全 安全协议 可证明安全 安全多方计算 百万富翁问题

On the security proof of a protocol for private integer comparison

SHAO Xiu-Feng[1], LI Rong-Hua[2]

1. Artificial Intelligence Institute, Beijing City University, Beijing 100083, China;
2. State Key Lab of Information Security, Graduate University, Chinese Academy of Sciences, Beijing 100049, China

Abstract:

In 1990 ACM Conference on Computer and Communications Security, Cachin proposed a protocol for private bidding and auctions and gave the security proof. We show that there is a mistake in Cachin’s security proof, and we correct the mistake.

Keywords: information security secure protocol provable security secure multiparty computation millionaires&rsquo problem

收稿日期 2009-12-21 **修回日期** 2010-06-25 **网络版发布日期**

DOI:

基金项目:

通讯作者:

作者简介:

作者Email: lirhyh@yahoo.com.cn

参考文献:

[1] Yao A C. Protocls for secure computation //Proceedings of 23rd IEEE Symposium on Foundations of Computer Science.1982:160-164.

[2] Cachin C. Efficient private bidding and auctions with an oblivious third party //6th ACM Conference on Computer and Communications Security. ACM Press, 1990:120-127.

[3] Blake I F, Kolesnikov V. Strong conditional oblivious transfer and computing on intervals //10th International Conference on the Theory and Application of Cryptology and Information Security, Asiacrypt'04, Jeju Island, Korea. Berlin: Springer, LNCS 3329, 2004:515-529.

[4] Qin J, Zhang Z F, Feng D G,et al. A protocol of comparing information without leaking [J]. Journal of Software, 2004, 15(3): 421-427 (in Chinese). 秦静, 张振峰, 冯登国,等. 无信息泄露的比较协议 [J]. 软件学报, 2004, 15(3): 421-427.

[5] Qin J, Zhang Z F, Feng D G, et al. A protocol of specific secure two-party computation
[J]. Journal of China Institute of Communications, 2004, 25(11): 35-42(in Chinese). 秦静, 张振峰, 冯登国,等. 一个特殊的安全双方计算协议
[J]. 通信学报, 2004, 25(11): 35-42.

本刊中的类似文章

1．张志芳.乘性单调张成方案[J]. 中国科学院研究生院学报, 2006,23(6): 827-832

2．王芷玲; 张玉清; 杨 波.公平交换协议设计原则[J]. 中国科学院研究生院学报, 2006,23(4): 555-560

3．荆巍巍，黄刘生，姚亦飞，徐维江.保护私有信息的统计量化规则挖掘[J]. 中国科学院研究生院学报, 2008,26(6): 771-780

4．徐海霞 李 宝.选择解承诺方案[J]. 中国科学院研究生院学报, 2007,24(1): 106-113

5．黄 亮　冯登国　张 敏.一个基于安全模型的测试用例生成工具[J]. 中国科学院研究生院学报, 2007,24(3): 300-306

6．潘嘉昕, 马昌社, 王立斌.基于口令的高效语义安全群密钥交换协议[J]. 中国科学院研究生院学报, 2010,27(4): 547-555

7．史祎诗, 王雅丽, 肖俊, 杨玉花, 张静娟.双位相密钥衍射系统用于旋转抛物面包围三维信息加密的研究[J]. 中国科学院研究生院学报, 2010,27(3): 414-419

8．王鹏.一个关于MAC伪随机性与不可伪造性的注记[J]. 中国科学院研究生院学报, 2010,27(2): 263-266