P.O.Box 8718, Beijing 100080, China	Journal of Software，Mar. 2004,15(3):421-427
E-mail: jos@iscas.ac.cn	ISSN 1000-9825，CODEN RUXUEW，CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2004 by The Editorial Department of Journal of Software

无信息泄漏的比较协议

秦 静, 张振峰, 冯登国, 李 宝

Full-Text PDF Submission Back

秦 静1,2, 张振峰2, 冯登国2, 李 宝2 1(山东大学 数学与系统科学学院,山东 济南 250100)2(信息安全国家重点实验室(中国科学院 研究生院),北京 100039)
作者简介: 秦静(1960－),女,山东济南人,教授,主要研究领域为密码学,安全协议;张振峰(1972－),男,副研究员,主要研究领域为密码学/网络与信息安全;冯登国(1965－),男,研究员,博士生导师,主要研究领域为信息与网络安全;李宝(1962－),男,研究员,博士生导师,主要研究领域为信息安全,安全协议.
联系人: 秦静 Phn: +86-531-6189566, Fax: +86-531-8364652, E-mail: houtui3@263.net
Received 2002-12-19; Accepted 2003-09-09

Abstract
At present, research on secure multi-party computation is of great interest in modern cryptography. It should be acknowledged that if any function can be computed securely, then it results in a very powerful tool. In fact, all natural protocols are, or can be rephrased to be, special cases of the multi-party computation problems. Design and analysis of the special multi-party computation protocols is meaningful and has attracted much interest in this field. Based on the combination of a public-key cryptosystem of the homomorphic encryption and on the theoretic construction relying on the (-hiding assumption, a protocol for comparing information of equality is proposed. The protocol needs only a single round of interaction and ensures fairness, efficiency and security. The protocol is fair, which means that one party knows the sound result of the comparison if and only if the other one knows the result. The protocol is efficient with the help of an oblivious third party for calculating. However, the third party cannot learn any information about the participant's private inputs and even about the comparison result, and cannot collude with any participant. The protocol is secure for the two participants, that is, any information about their secret input will not leak except the final computation result. A precise proof of security of the protocol is presented. Applications of this protocol may include private bidding and auctions, secret ballot elections, commercial business, identification in a number of scenarios and so on. It is believed that the protocol may be of practical significance for electronic transaction.

Qin J, Zhang ZF, Feng DG, Li B. A protocol of comparing information without leaking. *Journal of Software*, 2004,15 (3):421~427.
http://www.jos.org.cn/1000-9825/15/421.htm

摘要
关于安全多方计算的研究是目前国际密码学界的研究热点.如果能够安全地计算任何函数,就掌握了一个很强大的工具,实际上任何一个密码协议都可以化归一个特殊的安全多方计算协议.特殊的安全多方计算协议的设计与分析又是当前人们致力研究的课题.基于(-隐藏假设以及同态公钥加密体制的语义安全性假设,给出了一个特殊的安全双方计算协议--无信息泄漏的比较相等协议.该协议具有公平性:一方知道最后结果的等价条件为另一方也知道这个结果;安全性:除了最后结果以外,不泄露有关双方输入的任何信息;有效性:借助于茫然第三方协助完成计算任务,使协议简单有效,但这个第三方不知道最后结果及参与方的秘密,也不能与参与方串谋作弊;并对协议的正确性与安全性进行了理论证明.该协议在网上投标(拍卖)、网上商业谈判、电子选举等领域中有着广阔的应用前景.

基金项目：Supported by the National Natural Science Foundation of China under Grant No.60373039 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2001AA144040, 2003AA144151 (国家高技术研究发展计划(863)); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the National Outstanding Young Scientists Foundation of China under Grant No.60025205 (国家杰出青年科学基金); the Natural Science Foundation of Shandong Province of China under Grant No.Y2003A03 (山东省自然科学基金)

References:

[1] Goldreich O. Secure multi-party computation, manuscript version 1.3. 2002. htttp://theory.lcs.mit.edu/~oded

[2] Cramer R. Introduction to secure computation. In: Damgaard I, ed. Lectures on Data Security-Modern Cryptology in Theory and Practice. Lecture Notes in Computer Science, Vol 1561. Springer-Verlag, 1999. 16~62.

[3] Yao AC. Protocols for secure computation. In: Proc. of the 23rd IEEE Symp. on Foundation of Computer Science. Chicago: IEEE Computer Society, 1982. 160~164.

[4] Cachin C. Efficient private bidding and auctions with an oblivious third party. In: ACM Conf. on Computer and Communications Security, ed. Proc. of the 6th ACM Conf. on Computer and Communications Security. Assn for Computing Machinery, 1999. 120~127.

[5] Fagin R, Naor M, Winkler P. Comparing information without leaking it. Communications of the ACM, 1996,39(5):77~85.

[6] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed., John Wiley & Sons, Inc., 1996.

[7] Cachin C, Micali S, Stadler M. Computationally private information retrieval with polylogarithmic communication. In: Slern J, ed. Proc. of the Advances in Cryptology-EUROCRYPT'99. Lecture Notes in Computer Science, Vol.1592, Springer-Verlag, 1999. 402~414.

[8] Naccache D, Stern J. A new public-key cryptosystem based on higher residues. In: Association for Computing Machinery, ed. Proc. of the 5th ACM Conf. on Computer and Communications Security. San Francisco: ACM, 1998. 59~66.

[9] Okamoto T, Uchiyama S. A new public key cryptosystem as secure as factoring. In: Nyberg K, ed. Proc. of the Advances in Cryptology-EUROCRYPT'98. Lecture Notes in Computer Science, Vol 1403, Springer-Verlag, 1998. 308~318.

[10] Paillier P. Public-Key cryptosystem based on composite degree residuosity classes. In: Proc. of the Advances in Cryptology-EUROCRYPT'99. Lecture Notes in Computer Science, Vol 1592, Springer-Verlag, 1999. 223~238.

[11] Naor M, Yung M. Universal one-way hash functions and their cryptographic applications. In: Association for Computing Machinery, ed. Proc. of the 21st Annual ACM Symp. on Theory of Computing (STOC). Seattle: ACM, 1989. 33~43.

[12] Bellare M. A note on negligible functions. Journal of Cryptology, 2002,15(4):271~284.