计算机工程 2012, 38(04) 126-128 DOI: 10.3969/j.issn.1000-3428.2012.04.041 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于双方交集计算的指纹认证方案

张淑苗 [1a]，**张书晔** [2]，**冯 全** [1b]，**杨 梅** [1b]

(1. 甘肃农业大学 a. 信息科学技术学院；b. 工学院，兰州 730070；2. 兰州理工大学科技处，兰州 730050)

摘要： 针对开放网络中指纹认证的隐私保护问题，利用智能卡设计通用可组合安全的隐秘双方交集计算协议。该协议使用对称加密算法实现双方交集计算，具有较高的计算和通信效率。在此基础上，提出一种隐私保护型身份认证方案，使服务器能安全地比较现场指纹细节点集合与注册模板集合的匹配程度，确认用户身份。分析结果表明，该方案在认证过程中可保证双方私有数据的保密性。

关键词： 双方交集计算 指纹 身份认证 智能卡 隐私保护

Fingerprint Authentication Scheme Based on Two-party Intersection Computation

ZHANG Shu-miao [1a], ZHANG Shu-ye [2], FENG Quan [1b], YANG Mei [1b]

(1a. College of Information Sciences and Technology; 1b. College of Engineering, Gansu Agricultural University, Lanzhou 730070, China; 2. Scientific and Technical Department, Lanzhou University of Technology, Lanzhou 730050, China)

Abstract: In order to protect privacy of biometric data in remote authentication, a protocol is presented for private two-party set intersection problem with Universally Composable(UC) security by using smart cart. The proposed protocol uses only a linear number of symmetric-key computations and thus achieves high efficiency on computation and communication. A remote authentication scheme is furtherly designed based on the proposed protocol, which allows a server securely matching the query fingerprint of a user against the stored template to verify his identity, without leaking these private data.

Keywords: two-party intersection computation fingerprint identity authentication smart card privacy protection

收稿日期 2011-10-11 **修回日期** **网络版发布日期** 2012-02-20

DOI: 10.3969/j.issn.1000-3428.2012.04.041

基金项目:

国家自然科学基金资助项目(61062012)

通讯作者:

作者简介: 张淑苗(1979－)，女，助理研究员、硕士研究生，主研方向：信息安全；张书晔，工程师；冯 全(通讯作者)，教授、博士；杨 梅，讲师

通讯作者E-mail: fquan@gsau.edu.cn

参考文献：

[1] 冯 全, 苏 菲, 蔡安妮. 生物加密综述[J].计算机工程.2008, 34(10):141-143 浏览

[3] Erkin Z.[J].Franz M, Guajardo J, et al. Privacy-preserving Face Recognition[C]//Proc. of PETS'09. Berlin, Germany: Springer- Verlag.2009,:-

[4] Sadeghi A R.[J].Schneider T, Wehrenberg I. Efficient Privacy- preserving Face Recognition [C]//Proc. of ICISC'09. Seoul, Korea: Springer.2009,:-

[7] Freedman M.[J].Nissim K, Pinkas B. Efficient Private Matching and Set Intersection [C]//Proc. of Eurocrypt'04. Interlaken, Switzerland: [s. n..2004,:-

[8] Kissner L.[J].Song D. Privacy-preserving Set Operations[C]//Proc. of CRYPTO'05. Santa Barbara, California, USA: [s. n..2005,:-

[9] Hazay C.[J].Lindell Y. Constructions of Truly Practical Secure Protocols Using Standard Smartcards[C]//Proc. of CCS'08. Alexandria, USA: ACM Press.2008,:-

[10] Fischlin M.[J].Pinkas B, Sadeghi A R. Secure Set Intersection with Untrusted Hardware Tokens[C]//Proc. of CT-RSA'11. Berlin, Germany: Springer.2011,:-

[12] Pankanti S, Prabhakar S, Jain A K. On the Individuality of Fingerprints[J].IEEE Trans. on PAMI.2002, 24(8):1010-1025

[13] Janson P, Tsudik G. Secure and Minimal Protocols for Authen- ticated Key Distribution [J].Computer Communications.1995, 18(9):645-653

本刊中的类似文章

1. 傅鹤岗, 曾凯.多维敏感k-匿名隐私保护模型[J]. 计算机工程, 2012,38(3): 145-147,162
2. 张韶远, 卢建朱.基于生物特征的鲁棒远程用户认证方案[J]. 计算机工程, 2012,38(3): 137-138
3. 丁清, 朱敏, 闫二辉.一种安全高效的WAPI改进策略[J]. 计算机工程, 2012,38(3): 153-155
4. 胡吉旦, 卢建朱.无线网络中一种基于智能卡的匿名认证方案[J]. 计算机工程, 2012,38(01): 122-124
5. 戚世杰, 卢建朱, 胡吉旦.增强型相互认证密钥协商方案[J]. 计算机工程, 2012,38(01): 108-110
6. 麻浩, 王晓明.外包数据库的安全访问控制机制[J]. 计算机工程, 2011,37(9): 173-175
7. 刘雪艳, 张强.基于生物特征的可变角色用户认证机制[J]. 计算机工程, 2011,37(9): 168-170
8. 刘莲花, 谭台哲.多指标融合的指纹图像质量评测方法[J]. 计算机工程, 2011,37(9): 226-228
9. 杨磊, 魏磊, 叶剑, 史红周.一种连续LBS请求下的位置匿名方法[J]. 计算机工程, 2011,37(9): 266-269,272
10. 刘兴川, 林孝康.基于聚类的快速Wi-Fi定位算法[J]. 计算机工程, 2011,37(8): 285-287

文章评论

反馈人		邮箱地址	
反馈标题		验证码	0682