计算机应用 2012, 32(03) 699-704 DOI: 10.3724/SP.J.1087.2012.00699 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

具有分布式打开权威的隐藏身份签名方案

柳欣[1,2]

1.山东青年政治学院 信息工程学院, 济南 250014;
2.山东大学 计算机科学与技术学院, 济南 250101

摘要: 基于双线性映射的隐藏身份签名方案不满足可开脱性和选择密文攻击(CCA)匿名性,而在RSA群上构造的隐藏身份签名方案具有较高的通信和运算耗费。为此,利用块消息签名技术实现了可开脱性,提出一个允许设置分布式打开权威的改进方案。改进方案通过将分布式密钥提取和可同时执行的知识证明技术应用于底层门限加密方案,有效地实现了对打开权威的权利分发。此外, 为了克服传统串行注册方式无法抵抗拒绝服务攻击的不足,利用承诺的知识证明技术将注册过程增强为满足并发安全性的协议。在随机预言模型下,改进方案可证满足所要求的所有安全性质。对比实验结果表明:改进方案的签名长度更短, 签名与验证算法开销更小,由可信服务器执行的门限解密过程是并发安全的且在自适应攻击者模型下满足可证安全性。

关键词: 数字签名 群签名 基于身份的签名 知识证明 门限加密 自适应安全性

Hidden identity-based signature scheme with distributed open authorities

LIU Xin[1,2]

1.School of Information Engineering, Shandong Youth University of Political Science, Jinan Shandong 250014, China;
2.School of Computer Science and Technology, Shandong University, Jinan Shandong 250101, China

Abstract: Hidden identity-based signature schemes from bilinear maps do not achieve exculpability and Chosen-Ciphertext Attack (CCA) anonymity, while schemes of this type built on RSA groups suffer from significant communication and computation overheads. Concerning this situation, an improved scheme with distributed open authorities was put forward, which satisfied exculpability by making use of the block messages signature. It achieved efficient distribution of the open authority by applying distributed key extraction and simultaneous proof of knowledge to the underlying threshold encryption scheme. Furthermore, to cope with the shortcomings of traditional serial registration, i.e., being vulnerable to the denial-of-service attack, its registration protocol was enhanced to be concurrent-secure by using the method of committed proof of knowledge. In the random oracle model, the proposed scheme could be proved to fulfill all the required properties. Performance comparison shows that the resultant signature is shorter and the algorithms (i.e., Sign and Verify) are more efficient. Moreover, the process of threshold decryption by trusted servers is proved to be concurrently-secure and it is also immune to adaptive adversaries.

Keywords: digital signature group signature identity-based signature knowledge proof threshold encryption adaptive security

收稿日期 2011-08-23 **修回日期** 2011-11-09 **网络版发布日期** 2012-03-01

DOI: 10.3724/SP.J.1087.2012.00699

基金项目:

山东省高等学校科技计划项目(J11LG29)。

通讯作者: 柳欣

作者简介: 柳欣(1978-),男,山东广饶人,讲师,博士研究生,CCF会员,主要研究方向:信息安全、密码学。

作者Email: lxonne@163.com

参考文献:

[1]ZHOU S, LIN D. An interesting member ID-based group signature [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2007/126.

[2]BOYEN X, WATERS B. Compact group signatures without random oracles [C]// EUROCRYPT 2006: Proceedings of the 25th Annual International Cryptology Conference, LNCS 4004. Berlin: Springer-

Verlag, 2006: 427-444.

[3]袁艳,蔡光兴. 新的无随机预言的短群签名方案 [J]. 计算机应用,2011,31(3): 790-792.

[4]KIAYIAS A, ZHOU H S. Hidden identity-based signatures [C]// FC 2007: Proceedings of the 11th International Conference on Financial Cryptography and Data Security, LNCS 4886. Berlin: Springer-Verlag, 2007: 134-147.

[5]KIAYIAS A, ZHOU H S. Hidden identity-based signatures [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2007/140.

[6]HAZAY C, KATZ J, KOO C Y, et al. Concurrently-secure blind signatures without random oracles or setup assumptions [C]// TCC 2007: Proceedings of the 4th IACR Theory of Cryptography Conference, LNCS 4392. Berlin: Springer-Verlag, 2007: 323-341.

[7]AU M H. Contribution to privacy-preserving cryptographic tech-niques [D]. Wollongong, Australia: University of Wollongong, 2009.

[8]BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups [J]. Journal of Cryptology, 2008, 21(2): 149-177.

[9]SHOUP V, GENNARO R. Securing threshold cryptosystems against chosen ciphertext attack [J]. Journal of Cryptology, 2002, 15(2): 75-96.

[10]KIAYIAS A, XU S, YUNG M. Privacy preserving data mining within anonymous credential systems [C]// SCN 2008: Proceedings of the 6th Conference on Security and Cryptography for Networks, LNCS 5229. Berlin: Springer-Verlag, 2008: 57-76.

[11]LYSYANSKAYA A. Threshold cryptography secure against the adaptive adversary, concurrently [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2000/019.

[12]CANETTI R, GENNARO R, JARECHI S, et al. Adaptive security for threshold cryptosystems [C]// CRYPTO 1999: Proceedings of the 19th Annual International Cryptology Conference, LNCS 1666. Berlin: Springer-Verlag, 1999: 98-116.

[13]JARECHI S. Efficient threshold cryptosystems [D]. Cambridge, USA: Massachusetts Institute of Technology, 2001.

[14]FISCHLIN M, ONETE C. Relaxed security notions for signatures of knowledge [C]// ACNS 2011: Proceedings of the 9th International Conference on Applied Cryptography and Network Security, LNCS 6715. Berlin: Springer-Verlag, 2011: 309-326.

[15]GENNARO R, JARECHI S, KRAWCZYK H, et al. Secure distributed key generation for discrete-log based cryptosystems [J]. Journal of Cryptology, 2007, 20(1): 51-83.

[16]AU M H, SUSILO W, MU Y. Constant-size dynamic k-TAA [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2008/136.

[17]ROSEN A, SHELAT A. Optimistic concurrent zero knowledge [C]// ASIACRYPT 2010: Proceedings of the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security, LNCS 6477. Berlin: Springer-Verlag, 2010: 359-376.

[18]NGUYEN L, SAFAVI-NAINI R. Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings [C]// ASIACRYPT 2004: Proceedings of the 10th Annual International Conference on the Theory and Application of Cryptology and Information Security, LNCS 3329. Berlin: Springer-Verlag, 2004: 372-386.

[19]OHTAKE G, FUJII A, HANAOKA G, et al. On the theoretical gap between group signatures with and without unlinkability [C]// AFRICACRYPT 2009: Proceedings of the 2nd African International Conference on Cryptology, LNCS 5580. Berlin: Springer-Verlag, 2009: 149-166.

[20]FISCHLIN M. Communication-efficient non-interactive proofs of knowledge with online extractor [C]// CRYPTO 2005: Proceedings of the 25th Annual International Cryptology Conference, LNCS 3621. Berlin: Springer-Verlag, 2005: 152-168.

[21]FERRARA A L, GREEN M, HOHENBERGER S, et al. Practical short signature batch verification [C]// CT-RSA 2009: Proceedings of the Cryptographers' Track at the RSA Conference 2009, LNCS 5473. Berlin: Springer-Verlag, 2009: 309-324.

[22]WASEF A, SHEN X. Efficient group signature scheme supporting batch verification for securing vehicular networks [C]// IEEE ICC 2010: Proceedings of the 2010 IEEE International Conference on Communications. Piscataway, NJ: IEEE Press,2010: 1-5.

本刊中的类似文章

1．刘超凡 张永良 肖刚.基于滚动指纹数字签名的电子商务安全认证[J]. 计算机应用, 2012,32(02): 475-479

2．柳欣.具有直线提取器的匿名指纹方案[J]. 计算机应用, 2011,31(08): 2187-2191

3．王晚 杜伟章.基于离散对数问题的多级代理盲签名方案[J]. 计算机应用, 2011,31(07): 1904-1905

4．范函 张少武.对两个基于离散对数的数字签名方案的攻击分析与改进[J]. 计算机应用, 2011,31(07): 1859-1861

5．袁艳 蔡光兴.新的无随机预言的短群签名方案[J]. 计算机应用, 2011,31(03): 790-792

6．傅德胜 王强.XML数字签名在工作流系统中的应用[J]. 计算机应用, 2011,31(03): 808-811

7．王泽成.基于身份数字签名方案的通用可组合安全性[J]. 计算机应用, 2011,31(01): 118-122

8．李颖 周大水.对一种多重数字签名方案的攻击和改进[J]. 计算机应用, 2010,30(9): 2389-2392

9．王登第 柴乔林 孙翔飞 李涛.新的传感器网络假冒攻击源检测方案[J]. 计算机应用, 2010,30(8): 2125-2129

10．柳菊霞 苏靖枫.基于离散对数的代理盲签名方案[J]. 计算机应用, 2010,30(8): 2167-2169

11．陈宁宇 顾永跟 苏晓萍.数字签名方案的同底构造攻击[J]. 计算机应用, 2010,30(4): 1042-1044

12．杨长海.无证书门限多代理多签名方案[J]. 计算机应用, 2010,30(2): 513-516

13．王泽成 李志斌.通用可组合安全的多重数字签名[J]. 计算机应用, 2010,30(11): 3032-3035

14．张秋余 孙战辉.椭圆曲线数字签名中阈下信道通信研究[J]. 计算机应用, 2010,30(1): 196-197

15．吴晨煌 陈智雄 王海明 沈毅军.一个无证书代理签名方案的安全性分析及改进[J]. 计算机应用, 2009,29(4): 944-946,

16．夏琦 许春香 高建彬.对一种代理签名方案的密码学分析和改进[J]. 计算机应用, 2009,29(2): 353-354

17．樊玫玫 彭长根.一种基于身份的多方公平交换协议[J]. 计算机应用, 2009,29(2): 367-369

18．耿永军 张延红 崔国华.基于身份的结构化重签名方案[J]. 计算机应用, 2009,29(09): 2339-2341

19．朱紫钊 姚国祥.基于离散对数的数字签名方案[J]. 计算机应用, 2009,29(09): 2342-2343

20．马海英 石振国 顾翔.标准模型下的高效短群签名[J]. 计算机应用, 2009,29(08): 2220-2222

21．马春阳 张亚玲.VRML文档的消隐数字签名安全模型[J]. 计算机应用, 2009,29(07): 1793-1795

22．王泽成.基于DDHP的紧安全性归约多重数字签名方案[J]. 计算机应用, 2009,29(07): 1799-1802

23．叶晓彤 彭龚 简清明.基于无可信第三方IBS的XML数字签名[J]. 计算机应用, 2009,29(05): 1297-1300

24．何韦伟 季新生 刘彩霞.基于数字签名认证的IKE协议安全性分析及改进[J]. 计算机应用, 2008,28(7): 1807-1809

25．吴克力 韦相和 张宏 刘凤玉.基于多重线性型的多指定验证人签名[J]. 计算机应用, 2008,28(6): 1369-1371

26．雷治军 刘文化 禹勇.对一种代理盲签名方案的密码学分析[J]. 计算机应用, 2008,28(5): 1144-1145

27．朱建新 李成华 张新访.对一种基于身份的强密钥绝缘签名方案的改进[J]. 计算机应用, 2008,28(5): 1128-1129

28．杨学俊 王灯国 黄徐徐.一个基于ID的可删除群签名方案[J]. 计算机应用, 2008,28(4): 918-920

29．钱可龙 徐秋亮.基于新的群签名的密封式电子拍卖方案[J]. 计算机应用, 2008,28(3): 813-815

30．阿力木江艾沙 刘胜全.一种改进的前向安全数字签名方案[J]. 计算机应用, 2008,28(2): 440-442

31．王泽成 斯桃枝 李志斌.改进的带签名者意向的结构化多重签名方案[J]. 计算机应用, 2008,28(1): 71-73

32．王玲玲 张国印 马春光.一种基于双线性对的可验证无证书环签密方案[J]. 计算机应用, 2007,27(9): 2167-2169

33．徐丽娟 徐秋亮 郑志华.基于身份的指定验证人的门限代理签名方案[J]. 计算机应用, 2007,27(5): 1058-1061

34．夏旭 朱从旭 陈志刚.P2P协同工作环境下的一种多媒体认证系统[J]. 计算机应用, 2007,27(4): 846-848

35．吕波 谢晓尧.移动IPv6安全防火墙系统研究[J]. 计算机应用, 2007,27(3): 608-609

36. 张璐 张璟 井浩 李军怀.网络采购系统中安全机制的研究与实现[J]. 计算机应用, 2007,27(2): 318-320

37. 王标 林宏刚 林松.环Zn上圆锥曲线上的群签名方案及其应用[J]. 计算机应用, 2007,(12): 2942-2944

38. 杜焕强 吴铤 叶春涛.基于身份的代理盲签名[J]. 计算机应用, 2007,27(11): 2715-2717

39. 袁喜凤 孙艳蕊 孙金青 杨迎辉 .基于离散对数和因子分解具有消息恢复的签名方案[J]. 计算机应用, 2007,27(10): 2459-2460

40. 杨春 简丽 何军 .基于BB84与椭圆曲线的数字签名方案[J]. 计算机应用, 2007,27(10): 2475-2477

41. 宋庆 杨天奇 .一个改进的证实数字签名方案[J]. 计算机应用, 2006,26(11): 2605-2606

42. 吴晨煌 黄振杰 .强代理不可否认签名[J]. 计算机应用, 2006,26(11): 2592-2595

43. 娄悦 施荣华 曹龄兮 .基于强认证技术的会话初始协议安全认证模型[J]. 计算机应用, 2006,26(10): 2332-2335

44. 任德玲，韦卫，吕继强.代理可转换认证加密方案[J]. 计算机应用, 2005,25(09): 2086-2088

45. 崔国华，葛平.基于大数域因式分解的签名方案[J]. 计算机应用, 2005,25(04): 842-843

46. 戴华，张林聪，李炳法.基于数字水印和数字签名的电子支票支付系统[J]. 计算机应用, 2005,25(02): 403-406

47. 苏云学，祝跃飞，闫丽萍.一个利用群签名的电子拍卖协议[J]. 计算机应用, 2005,25(01): 157-159
