西安电子科技大学学报 2009, 36(3) 428-432 DOI: ISSN: ISSN 1001-2400 CN: 61-1076/TN

本期目录 | 下期目录 | 过刊浏览 | 高级检索 [打印本页] [关闭]

论文

MQ公钥密码体制等价密钥分析

王鑫[1];孙晨[2];王新梅[1]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071;
2. 空军工程大学 导弹学院，陕西 三原 713800)

摘要：

MQ公钥密码体制存在多个私钥对应同一个公钥的问题．应用高斯不变算子对私钥空间进行等价分类，给出了任一私钥的等价类中所含元素的个数与明密文分量之间的关系式.该式表明，对任一公钥有指数级个私钥与之对应，从而使私钥(进而公钥)空间大量减少．同时，还给出了私钥的仿射结构的标准形，该形式具有稀疏性，从而能够有效地减少计算量，提高存储效率．最后，以R-SE(2)签名体制为例，分析了分层结构对体制安全性的影响.

关键词： 多变量公钥密码 代数分析 等价密钥 高斯不变算子 R-SE(2)

Equivalent keys of multivariate quadratic public key cryptosystem

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China;
2. Missile Inst. of Airforce Eng. Univ., Sanyuan 713800, China)

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China;
2. Missile Inst. of Airforce Eng. Univ., Sanyuan 713800, China)

Abstract:

The multivariate quandratic cryptosystem has the problem that many superflous private keys correspond to the same public key. By applying the Gauss Sustainer, the private key space is partitioned into equivalence classes. And then, a relationship between the number of elements in any equivalence private key class and plaintext (ciphertext) is established. This formula shows the number of private keys corresponding to any given public key is exponential. Hence, the private (further the public) key space is reduced greatly. Moreover, the normal form of affine transformations of the private key is derived. It has the sparse characteristic, which will reduce computing complexity and improve the storage efficiency. Finally, the R-SE(2) public key signature scheme is taken for an example, and the security performance of this scheme affected by the step-structure is analyzed.

Keywords: multivariate public key cryptosystem algebraic cryptanalysis equivalent keys Gauss sustainer R-SE(2)

收稿日期 2008-04-16 修回日期 2008-06-02 网络版发布日期 2009-05-25

DOI:

基金项目:

国家自然科学基金(90604009;60503010);省级.省部级基金

通讯作者: 王鑫

作者简介:

参考文献：

［1］Shor P. Polynomial-time Algorithms for Pime Factorization and Discrete Logarithms on A Quantum Computer ［J］. SIAM Journal on Computing, 1997, 26(5): 1484-1509.
［2］Garay M, Johnson D. Computers and Intractability —a Guide to the Theory of NP-Completeness ［M］. San Francisco: W H Freeman and Company, 1979: 250-251.
［3］Patarin J, Goubin L. Trapdoor One-way Permutations and Multivariate Polynomials ［C］//International Conference on Information Security and Cryptology 1997, LNCS: 1334. Berlin: Springer, 1999: 356-368.

扩展功能
本文信息
Supporting info
PDF(514KB)
[HTML全文](1KB)
参考文献[PDF]
参考文献
服务与反馈
把本文推荐给朋友
加入我的书架
加入引用管理器
引用本文
Email Alert
文章反馈
浏览反馈信息
本文关键词相关文章
多变量公钥密码
代数分析
等价密钥
高斯不变算子
R-SE(2)
本文作者相关文章
王鑫
王新梅
PubMed
Article by Yu,x
Article by Yu,X.M

[4] European IST. NESSIE Project [EB/OL]. [2000-12-12]. http://www.cryptonessie.org.

[5] Akkar M, Courtois N T, Duteuil R, et al. A Fast and Secure Implementation of Sflash [C] //PKC 2003, LNCS: 2567. Berlin: Springer, 2003: 267-278.

[6] 韦宝典, 刘景伟, 王新梅. NESSIE分组密码及其安全性分析 [J]. 西安电子科技大学学报, 2004, 31(3): 377-382.
Wei Baodian, Liu Jingwei, Wang Xinmei. The NESSIE Block Ciphers and Their Security [J]. Journal of Xidian University, 2004, 31(3): 377-382.

[7] Kipnis A, Shamir A. Cryptanalysis of the Oil and Vinegar Signature Scheme [C] //Advances in Cryptology—CRYPTO 1998, LNCS: 1462. Berlin: Springer, 1998: 257-267.

[8] Wolf C, Preneel B. Equivalent Keys in HFE, C*, and Variations [C] //Proceedings of Mycrypt 2005, LNCS: 3725. Berlin: Springer, 2005: 33-49.

[9] Wolf C, Preneel B. Superfluous Keys in Multivariate Quadratic Asymmetric Systems [C] //PKC 2005, LNCS 3386. Berlin: Springer, 2005: 275-287.

[10] Kasahara M, Sakai R. A Construction of Public Key Cryptosystem for Realizing Ciphertext of Size 100 Bit and Digital Signature Scheme [J]. IEICE Trans on Fundamentals, 2004: E87-A(1): 102-109.

本刊中的类似文章

文章评论

序号	时间	反馈人	邮箱	标题	内容
1	2009-10-21	caragon	caragon@googlemail.com		????????????????????????????????£????????????????f???ugg ukugg saleugg bootsUGG Bailey Buttonsupra shoesnike dunkMBT Shoes discountugg sale ugg shoes ugg