计算机应用 2012, 32(03) 694-698 DOI: 10.3724/SP.J.1087.2012.00694 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

重新认识背包公钥密码的安全性

丁燕艳,费向东,潘郁

南京工业大学 经济与管理学院,南京 210009

摘要: 针对背包密码屡被破译的局面,分析了其中原因。指出背包公钥序列是由初始序列变换而来的,初始序列由易解背包形成,存在着冗余度,因此背包公钥序列不可能是完全随机的,利用这些冗余度是破译成功的必要条件,目前大多数被破译的背包密码只使用了模乘运算等混乱技术,这不足以隐藏初始序列的冗余度。为此引入了加法扩散技术,以分散初始序列的冗余度,使攻击者在破译过程中难以利用,举实例说明了项内扩散和项间扩散两种扩散技术。分析表明,运用扩散技术后,能抵御目前已知的攻击方法。

关键词: 背包公钥密码 冗余度 模乘运算 混乱 扩散

Security reconsideration of knapsack public-key cryptosystem

DING Yan-yan, FEI Xiang-dong, PAN Yu

School of Economics and Management, Nanjing University of Technology, Nanjing Jiangsu 210009, China

Abstract: Concerning the situation that knapsack public-key cryptosystem has been broken repeatedly, this paper analyzed the cause. It is expounded that a knapsack public-key sequence is generated by transforming an initial sequence composed of an easy knapsack problem with redundancy; hence, a knapsack public-key sequence is unlikely completely random. Currently, most broken knapsack cryptosystems only use confusion, such as modular multiplication, so as not to conceal the redundancy of the initial sequence adequately. It is necessary to utilize the redundancy for breaking a cryptosystem. Therefore, addition diffusion was introduced in this paper to diffuse the redundancy of an initial sequence, so that an adversary can not make use of the redundancy when breaking a cryptosystem. Inner-item diffusion and inter-item diffusion were illustrated. The analysis indicates the cryptosystem is secure against the known attacks with diffusion.

Keywords: knapsack public-key cryptosystem redundancy modular multiplication confusion diffusion

收稿日期 2011-09-26 **修回日期** 2011-12-01 **网络版发布日期** 2012-03-01

DOI: 10.3724/SP.J.1087.2012.00694

基金项目:

江苏省软科学研究计划项目(BR2010080)。

通讯作者: 丁燕艳

作者简介: 丁燕艳(1987-),女,江苏无锡人,硕士研究生,主要研究方向:管理决策、商务智能;费向东(1966-),男,江苏无锡人,高级工程师,硕士,主要研究方向:密码算法、安全协议;潘郁(1955-),男,江苏南通人,教授,博士,主要研究方向:计算管理、商务智能。

作者Email: panyu@njut.edu.cn

参考文献:

[1]MERKLE R C, HELLMAN M H. Hiding information and signatures in trapdoor knapsacks[J]. IEEE Transactions on Information Theory, 1978,24(5):525-530.

[2]COSTER M J, JOUX A, LAMACCHIA B A, et al. Improved low-density subset sum algorithms[J]. Computational Complexity, 1992, 2(2): 111-128.

[3]ODLYZKO A M. The rise and fall of knapsack cryptosystems[EB/OL]. [2010-05-10]. http://www.dtc.umn.edu/~odlyzko/doc/arch/knapsack.survey.pdf.

[4]LAI M K. Knapsack Cryptosystems: The Past and the Future [EB/OL]. [2011-09-15]. http://www.ics.uci.edu/~mingl/knapsack.html.

[5]王保仓,韦永壮,胡予濮. 基于随机背包的公钥密码[J]. 电子与信息学报,2010,32(7):1580-1584.

[6]LENSTRA A K, LENSTRA H W, Jr, LOVASZ L. Factoring polynomials with rational coefficients[J]. Mathematische Annalen,1982,261(4):513-534.

[7]王保仓,巨春飞. 对一个背包公钥密码的格攻击[J].计算机应用研究,2010,27(4):1466-1492.

[8]SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal,1949,28(4):656-715.

[9]SHAMIR A. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem[J]. IEEE Transactions on Information Theory,1984,30(5):699-704.

[10]SCHNEIER B.应用密码学[M]. 吴世忠,祝世雄,张文政,等译.北京:机械工业出版社,2000:185-250.

[11]LAGARIAS J C. Knapsack public key cryptosystems and diophantine approximation[C]// Proceedings of CRYPTO '83. Berlin: Springer-Verlag, 1984:3-23.

[12]王保仓,韦永壮,胡予濮. 基于中国剩余定理的快速公钥加密算法[J].西安电子科技大学学报:自然科学版,2008,35(3):449-454.

[13]章照止.破译一个新的背包公钥密码系统[J]. 系统科学与数学,1991,11(1):91-96.

[14]韩立东,刘明洁,毕经国. 两种背包型的公钥密码算法的安全性分析[J].电子与信息学报,2010,32(6):1485-1488.

[15]何敬民,卢开澄.背包公钥系统的安全性与设计[J]. 清华大学学报:自然科学版,1988,28(1):89-97.

本刊中的类似文章

1．柯丹丹 蔡光程 曹倩倩.基于图像特征的各向异性扩散去噪方法[J]. 计算机应用, 2012,32(03): 742-745

2．郭红伟.基于频谱边缘检测的运动模糊方向精确估计[J]. 计算机应用, 2012,32(03): 770-772

3．梁敏 朱虹 欧阳光振 刘薇.模糊图像点扩散函数的亚像素精度离散化方法[J]. 计算机应用, 2012,32(02): 496-498

4．张燕芳 熊海灵.基于Bass与元胞自动机混合模型的快速消费品产品扩散研究[J]. 计算机应用, 2011,31(12): 3305-3308

5．葛君伟 李志强 方义秋.云存储环境下基于分散式服务器的Erasure Code算法[J]. 计算机应用, 2011,31(11): 2940-2942

6．侯文滨 吴成茂.基于Arnold变换的图像分存加密方法[J]. 计算机应用, 2011,31(10): 2682-2686

7．刘奎 苏本跃 赵晓静.基于结构张量的图像修复方法[J]. 计算机应用, 2011,31(10): 2711-2713

8．贾娴 刘培玉 公伟.应用于入侵取证的改进信息增益算法[J]. 计算机应用, 2011,31(08): 2156-2158

9．王蕾 冯晓毅 万小娜.基于改进卡尔曼滤波的盲图像恢复[J]. 计算机应用, 2011,31(03): 711-714

10．郭茂银 田有先.改进的LIP偏微分方程图像去噪方法[J]. 计算机应用, 2011,31(02): 383-385

11．吴小天 孙伟.基于误差扩散的图像分存方案[J]. 计算机应用, 2011,31(01): 74-77

12．张寒冰 袁昕.数字半色调技术中的误差扩散算法的研究[J]. 计算机应用, 2010,30(4): 925-928

13．任小波 杨忠秀.一种动态扩散粒子群算法[J]. 计算机应用, 2010,30(1): 159-161

14．李振恒 孙丰荣 刘芬 王庆浩 耿俊卿 秦晓红.基于改进的各向异性扩散方程的医学超声图像降噪方法[J]. 计算机应用, 2009,29(12): 3369-3371

15．舒玉强 杨红雨.基于人类视觉特性的两步去噪模型[J]. 计算机应用, 2009,29(12): 3372-3374

16．韩涛 杨金民 张大方 李寅.基于扩散激活模型的无线自组网分簇方法[J]. 计算机应用, 2009,29(1): 155-157

17．朱景福 黄凤岗.一种高阶各向异性扩散小波收缩图像降噪算法[J]. 计算机应用, 2009,29(08): 2068-2070

18．郭静 田有先.基于像素预判的各向异性扩散并行图像恢复[J]. 计算机应用, 2009,29(05): 1353-1358

19. 刘瑞华 鲍政.基于Gibbs分布的盲图像修复[J]. 计算机应用, 2008,28(9): 2281-2284

20. 张洁 檀结庆.基于各向异性扩散方程的Canny边缘检测算法[J]. 计算机应用, 2008,28(8): 2049-2051

21. 李征.基于ESS均衡的电子商务信任模型[J]. 计算机应用, 2008,28(8): 2173-2176

22. 丛维 郭定辉.用于图像去噪的改进型非线性扩散方程[J]. 计算机应用, 2008,28(7): 1764-1765

23. 王金龙 耿雪玉.基于研究者发文序列的研究领域扩散[J]. 计算机应用, 2008,28(6): 1424-1426

24. 陈家新 吴颖 黎蔚.基于各向异性扩散的医学图像分水岭分割算法[J]. 计算机应用, 2008,28(6): 1527-1529

25. 杜胜永 郭强.被动分簇策略在定向扩散路由算法中的应用[J]. 计算机应用, 2008,28(2): 402-405

26. 董颖 陈辉 赵彬.一种基于线性亮度变化模型的鲁棒的光流算法[J]. 计算机应用, 2008,28(1): 216-219

27. 洪联系 李传目 卢明玺.扩散映射置乱与超混沌系统组合图像加密算法[J]. 计算机应用, 2007,27(8): 1891-1894

28. 蒋先刚 .基于各向异性扩散的图像平滑及在三维重构预处理中的应用[J]. 计算机应用, 2007,27(1): 249-251

29. 黄世国 耿国华 .一种非线性逆扩散图像增强算法[J]. 计算机应用, 2006,26(8): 1842-1844

30. 谢美华，王正明.基于最小相关系数的扩散去噪的最优停止时间选取[J]. 计算机应用, 2005,25(05): 1078-1080

31. 谢美华，王正明.基于图像分解的多核非线性扩散去噪方法[J]. 计算机应用, 2005,25(04): 757-759

32. 崔灵果，曹元大.SPN分组密码中最优扩散层的构造与验证[J]. 计算机应用, 2005,25(04): 856-858
