吉首大学学报自然科学版 » 2012, Vol. 33 » Issue (3): 27-31 DOI: 10.3969/j.issn.1007-2985.2012.03.008

椭圆曲线密码体制应用及脆弱性量子分析

（海军工程大学信息安全系，湖北 武汉 430033）

Quantum Analysis on Vulnerability of Elliptic Curve Cryptosystem

（College of Electronic Engineering,Naval Engineering University,Wuhan 430033,China）

摘要 首先简要介绍椭圆曲线相关知识及其密码学应用，然后进行椭圆曲线加密体制（ECC）脆弱性分析，包括ECC的一般曲线分析、特殊曲线分析.重点提出了椭圆曲线上的离散对数脆弱性的量子分析方法.

关键词: 椭圆曲线密码 公钥密码体制 离散对数 脆弱性分析 量子分析

Abstract: The article introduces elliptic curve public-key cryptosystem and its related knowledge.It also analyzes security of elliptic curve public-key cryptosystem,which includes general analysis,special analysis and quantum analysis for vulnerability.

Key words: elliptic curve cryptosystem public-key cryptosystem discrete logarithm vulnerability analysis quantum analysis

作者简介: 周学广（1966-），男，江苏高邮人，海军工程大学电子工程学院教授，博士，博士生导师，中国计算机学会（CCF）高级会员，主要从事密码学与信息安全研究.

引用本文:

周学广. 椭圆曲线密码体制应用及脆弱性量子分析[J]. 吉首大学学报自然科学版, 2012, 33(3): 27-31.

ZHOU Xue-Guang. Quantum Analysis on Vulnerability of Elliptic Curve Cryptosystem[J]. Journal of Jishou University(Natural Sciences Edit, 2012, 33(3): 27-31.

[1] RIVEST R L,SHAMIR A,ADLEMAN L.A Method for Obtaining Digital Signatures and Public Key Cryptosystems [J].Communications of the ACM,1978,21(2):120-126.

[2] ELGAMAL L.A Public Key Cryptosystem and a Signature Scheme Base on Discrete Logarithm [J].IEEE Trans. Info. Theory,1985,31:469-472.

[3] KOBLITZ NEAL.Elliptic Curve Cryptosystems [J].Mathematics of Computation,1987,48:203-209.

[4] MILLER V.Uses of Elliptic Curves in Cryptography [C]//Advances in Cryptology CRYPTO' 85,Lecture Notes in Computer Science.Berling:Springer-Verlag,1986,218:417-426.

[5] 金晨辉，郑浩然，张少武，等.密码学 [M].北京：高等教育出版社，2009.

[6] MENEZES A J,OKAMOTO T,VANSTONE S A.Reducing Elliptic Curve Logarithms to a Finite Field [J].IEEE Trans. Info. Theory,1993,9:1 639-1 646.

[7] XU Guang-wu.Short Vectors,the GLV Method and Discrete Logarithms [J].Journal of Lanzhou University:Natural Sciences,2009,45(1)：73-77.

[8] 陈智华. 基于DNA计算自组装的Diffie-Hellman算法破译 [J]. 计算机学报,2008,31(12)：2 116-2 122.

[9] 司光东，董庆宽，李艳平，等. 一种基于离散对数群签名方案的分析 [J]. 哈尔滨工程大学学报,2007,28(10)：1 131-1 134.

[10] 吕欣，冯登国.密码体制的量子算法分析 [J].计算机科学,2005,32(2):166-168.

[11] SHOR PETER W.Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [J].SIAM J. on

Computing,1997,26(5):1 484-1 509.

[1] 游新娥. **RSA算法中安全大素数生成方法及其改进**[J]. 吉首大学学报自然科学版, 2007, 28(5): 34-37.