ECC算法在软件保护中的应用及安全性分析

王红珍[1,2],李竹林[1,2]

(1.延安大学 计算机学院,陕西 延安 716000;
2.延安大学 软件研究与开发中心,陕西 延安 716000)

摘 要:椭圆曲线密码体制基于其长度小、安全性高等特点在公钥密码系统中得到广泛应用,其安全性是基于椭圆曲线上的离散对数的难解性,它还依赖于椭圆曲线的选择。建立椭圆曲线密码体制的首要问题之一就是产生能够抵抗已有算法攻击的安全的椭圆曲线。文中主要将ECC加密技术应用于注册码软件加密保护方案中,对其进行了抗密码分析能力的讨论,最后对ECC算法的安全性进行研究及分析。因此,基于其极强的安全性ECC加密技术将会广泛地被应用。

关键词:椭圆曲线密码体制;安全性;注册码;离散对数

中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)08-0155-04

Application and Security Analysis of ECC Algorithm in Software Protection

WANG Hong-zhen[1,2], LI Zhu-lin[1,2]

(1. Department of Computer Science, Yan'an University, Yan'an 716000, China;
2. Software R&D Center, Yan'an University, Yan'an 716000, China)

Abstract: Elliptic curve cryptosystem based on its shorter length, high security features in the public key cipher system is widely used, its security is based on the elliptic curve discrete logarithm abstruse, it also depends on the selection of elliptic curve. Establishment of elliptic curve cryptography is one of the most important problems is to produce secure elliptic curve can resist the attack of existing algorithms. The ECC encryption technology is applied to the register code software encryption and protection scheme, the cryptanalysis-resisting capacity is discussed, finally the ECC algorithm security is researched and analysed. Therefore, based on its strong security ECC encryption technology will be widely applied.

Key words: elliptic curve cryptography; security; license; discrete logarithm

0 引 言

椭圆曲线理论是建立在代数几何、数论等多个数学分支方面的一个交叉点,一直被认为是纯理论学科[1]。1985年,数学家Neal Koblitz和Victor Miller各自独立地提出了椭圆曲线密码算法(ECC),其安全性是建立在椭圆曲线上点的离散对数问题。目前,椭圆曲线密码体制已被公认为是公钥密码体制当中加密强度最高的一种体制,并且基于其极强的安全性ECC加密技术将会广泛地被应用[2]。文中主要将ECC加密技术应用于注册码软件加密保护方案中,并对ECC算法的安全性进行研究和分析。

收稿日期:2011-12-19;**修回日期**:2012-03-21

基金项目:陕西省教育科技项目(2010JK904)

作者简介:王红珍(1973-),女,陕西子长人,实验师,硕士,研究方向为软件体系结构及应用、计算机实验教学、实验室管理工作;李竹林,副教授,博士,研究方向为数字图像处理。

1 ECC应用于注册码软件加密保护方案

1.1 注册码的申请

注册码的申请也就是用户要提交给软件开发技术员的用户信息,由于是"一机一码"制所以必须提供计算机的唯一性信息。通过这种方法能够将软件与用户使用该软件的计算机进行绑定,每次使用软件时都会去自动检查当前计算机的"注册码",进行合法性验证,这样软件即可防止了非法注册码。在这里采用的是提取CPU序列号和计算机的硬盘序列号,通过一定的方式将两者糅合成申请码。图1描述了用户利用注册码软件的注册模块获得注册申请码,并且将开发人员反馈的注册码写入注册表来完成注册的整个过程。在这里,不同的用户信息对应数据库中不同的私钥,因此当软件开发技术员计算注册码所使用的私钥与用户软件验证中使用的公钥是"一对"时,才能构成一个完整的ECC算法[3]。

申请注册码的具体步骤如下[4]:

(1)选择一条合法的椭圆曲线 $E_p(a,b)$ 和有效基点 $G(x,y)$.;

(2)选择适当的私有密钥 $k(k < n, n$ 为 G 的阶 $)$,并利用基点 $G(x,y)$ 来计算公开密钥 $K = kG$;

(3)在这里,产生一个随机整数 $r(r < n)$,并计算点 $R = rG$;

(4)将用户名和点 R 的坐标值(x,y)作为参数,并计算 SHA(安全散列算法)值,即 Hash = SHA(deviceID, x,y) ;

(5)计算 $SN \equiv r - \text{Hash} * k(\text{mod}n)$;

(6)将 SN 和 Hash 作为用户名 username 的序列号,在数据库中 username 与 deviceID 一一对应。

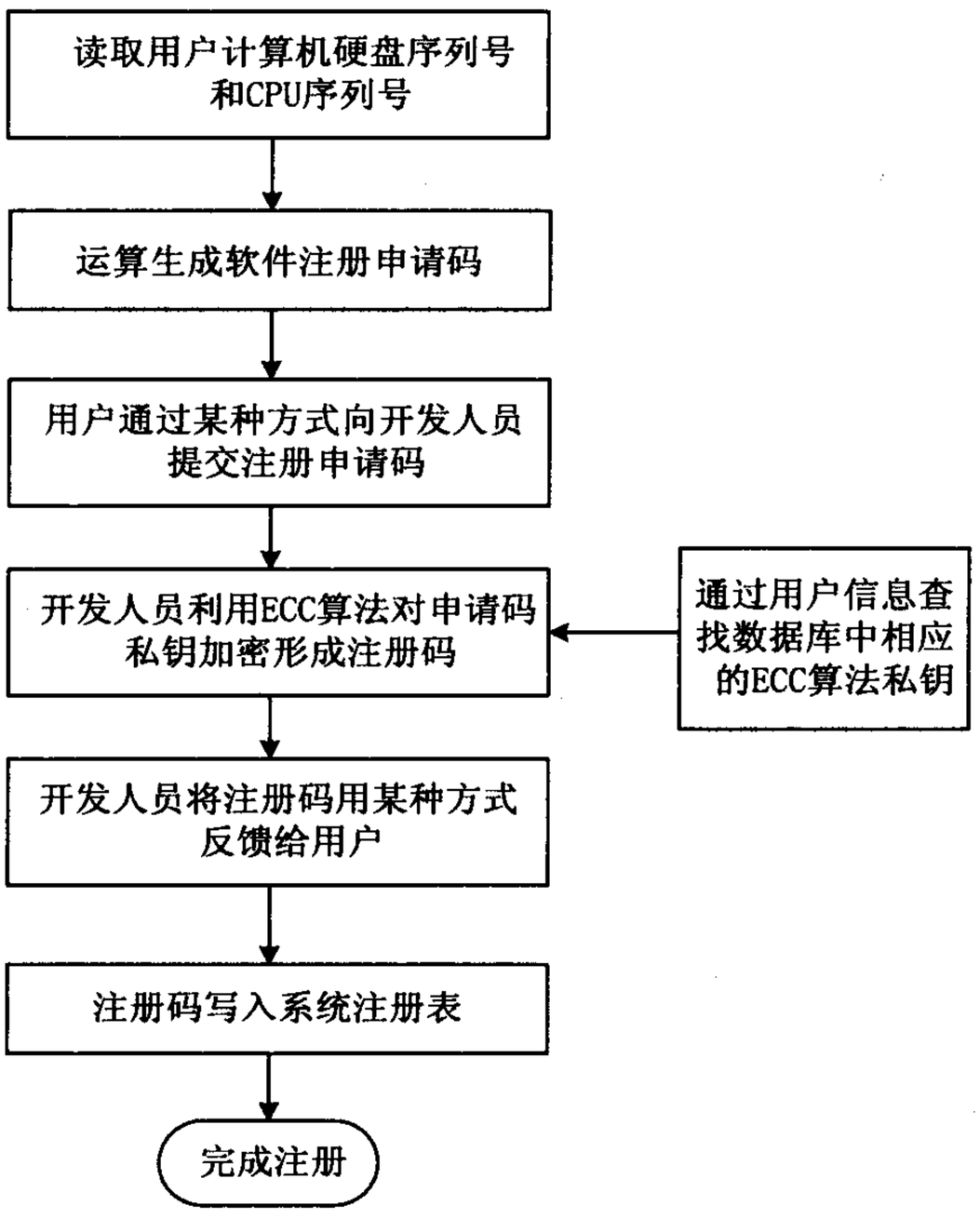

图 1 ECC 注册流程图

1.2 验证注册码

图 2 描述了注册码软件进行用户注册信息合法性验证的过程,在验证时注册码软件再次获取当前计算机的硬件信息并形成一个申请码,然后与解密后的明文(即软件所申请的那台计算机对应的申请码)作比较,这样即保证了注册过后的软件只能在固定的计算机上使用[3]。

验证注册码的具体步骤如下[5]:

(1)从用户输入的序列号中,提取 SN 以及 Hash;

(2)计算点 $R \equiv SN * G + \text{Hash} * K(\text{mod}p)$,如果 SN 、Hash 正确,其值等于申请过程中点 $R(x,y)$ 的坐标,因为 $SN \equiv r - \text{Hash} * k(\text{mod}n)$,所以:

$$SN * G + \text{Hash} * K$$

$$= (r - \text{Hash} * k) * G + \text{Hash} * K$$

$$= rG - \text{Hash} * kG + \text{Hash} * K$$

$$= rG - \text{Hash} * K + \text{Hash} * K$$

$$= rG$$

(3)将 username 对应的 deviceID 和点 R 的坐标值 x,y 作为参数,计算 $H = \text{SHA}(\text{deviceID}, x, y)$;

(4)如果 $H = \text{Hash}$ 则注册。如果 $H \neq \text{Hash}$,则注册失败。

图 2 验证流程

1.3 抗密码分析能力

从技术上来讲,对于本方案的威胁手段,可能的情况有以下 2 种:

(1)破解 ECC 公钥加密算法;

(2)破解本方案所采用的单向散列算法 SHA。

ECC 加密算法的安全性依赖于椭圆曲线离散对数的安全性,安全椭圆曲线的选取是建立椭圆曲线密码体制的基石,所以曲线的安全是保证密码体系安全的重要因素。在过去的十多年里,椭圆曲线离散对数问题受到了数学界的极大关注。目前,还没有发现椭圆曲线离散对数(ECDLP)有什么特别大的弱点[6]。

安全 Hash 算法 SHA 在本方案中起着检验信息是否正确的作用,SHA 是由美国国家标准与技术委员会和国家安全局设计。而且在 2004 年 8 月 17 日召开的国际密码学年会上,来自我国山东大学的王小云教授的关于《破译 MD5、HAVAL-128、MD4 以及 RIPEMD-128 算法》的报告在会议上引起了轰动,随后 NIST 于 2004 年 8 月 24 日发表专门评论针对所破译的以 MD5 为代表的 Hash 函数算法的报告,其评论的主要内容是“在最近的国际密码学会议(Crypto 2004)上,有研究人员宣布他们发现了破解多种 Hash 算法的方法,其中

包括 MD4,MD5,HAVAL-128,RIPEMD 及 SHA-0。经分析表明,于 1994 年替代 SHA-0 的 SHA-1 的减弱条件的变种算法能够被破解;但是完整的 SHA-1 并不能被破解。研究结果说明,SHA-1 的安全性目前没有问题,但是随着技术的发展,技术与标准局计划逐步淘汰 SHA-1,换用其它更长、更安全的算法来替代。"从这里可以看出,SHA-1 暂时在已知的单向散列算法中是安全的[7]。

2　基于 ECC 算法制作的注册方案优点及其特点

2.1　基于 ECC 算法制作的注册方案的优点

基于 ECC 算法制作的注册方案的优点如下:

(1)每台计算机的注册码不同。用户获取一个密码只能在固定的机器上注册使用软件。这不同于目前大多数软件所采用的注册保护方法,即只要知道注册码,则可以在任何计算机上安装注册。

(2)这种保护方案不需要任何硬件(如加密狗)或软盘。

(3)该方案可以选择控制软件运行在哪些机器上、运行的时间或者运行次数等。

(4)该方案还可让软件在不注册的情况下使用(作为演示软件),但只能运行一段时间或部分功能。注册成功后则可变为正式软件来使用。

(5)该方案采用特别技术,使解密者或黑客很难找到产生注册码的规律。

(6)该方案在使用注册码产生软件(注册机)时可采用密码、总次数限制、密钥盘等方法。

(7)该方案方便易用,价格低廉。

2.2　基于 ECC 算法制作的注册方案的特点

基于 ECC 算法制作的注册方案的特点如下:

(1)该注册加密的软件,只能在一台计算机上安装使用。把软件拷贝或复制到其它计算机上不能正常运行。

(2)若用户想在另一台计算机上安装运行,必须把软件在这一计算机上运行时的序列号,交给软件开发人员获取注册密码。当然还要再交一份软件费用。

(3)此加密方法特别适应在网络上发布的软件或者用光盘发布的软件(需要取得网卡的地址)。

3　ECC 的安全性分析

ECC 加密算法的安全性依赖于椭圆曲线离散对数的安全性,安全椭圆曲线的选取是建立椭圆曲线密码体制的基石,所以曲线的安全是保证密码体系安全的重要因素。在过去的十多年里,椭圆曲线离散对数问题受到了数学界的极大关注。目前,还没有发现椭圆曲线离散对数(ECDLP)有什么特别大的弱点。目前,椭圆曲线密码算法是最流行的公钥密码算法之一,所以对 ECC 的攻击也是当前密码学研究的热点之一。根据文献[8 ~ 12]中的介绍,文中总结出以下几种对椭圆曲线密码体制问题的攻击方法,并作简要的分析。

3.1　对所有曲线攻击

(1)穷搜索法(Exhaustive Search Algorithm)。

穷搜索法是一种最直观的方法,即遍历 1 到 k 计算 P 的点乘,得到 Q 为结束遍历。该方法最坏的情况是计算 n 步。这种方法的复杂度为 $O(n)$,只有理论意义,而无现实意义。

(2)小步大步法(Baby-Step Giant-Step Algorithm)。

设 P 为椭圆曲线 E 上的点,P 的阶为 n,已知点 $R \in \langle P\rangle$(P 生成的循环群),求正整数 l,使得 $R = lP(0 \leqslant l \leqslant n)$,将 l 表示为 $l = c\lceil n^{1/2}\rceil + d$,令 $S_d = R - dP$,存储关于 S_d 的表,对于 $c = 0,1,\cdots,\lceil n^{1/2}\rceil - 1$,依次计算 $S_c = c\lceil n^{1/2}\rceil P$,将 S_c 与 S_d 表中的点比较,如果某个 S_c' 与 S_d' 相同,就有 $l' = c'\lceil n^{1/2}\rceil + d'$。

小步大步法的复杂度为 $O(n^{1/2})$,这是已知计算 ECDLP 的最好的复杂度,但是该算法需要存储大约 $n^{1/2}$ 个点,这是一种以空间换时间的方法,最坏需要计算 $n^{1/2}$ 步。

(3)Pollard ρ 算法(Pollard's rho Algorithm)。

Pollard ρ 算法是对小步大步法的随机变形,这种方法的时间复杂度为 $O((\pi n)^{1/2})$,其空间复杂度可以忽略。因此它比小步大步法优越之处就在于它的空间复杂度可忽略。

(4)分布式 Pollard ρ 算法。

分布式 Pollard ρ 算法是由 Van Oorschot 和 Wiener 提出的 Pollard ρ 的并行算法,该方法是将 Pollard ρ 算法分为 m 个过程,在不同的处理器上并行处理,其时间复杂度约为 $O((\pi n)^{1/2}/2m)$。分布式 Pollard ρ 算法是目前已知的对 ECDLP 求解的最好方法之一,也是对一般椭圆曲线离散对数问题最好的攻击方法之一。

(5)Pohlig-Hellman 算法。

这个算法是由 Pohlig 和 Hellman 提出的[7]。

设椭圆曲线的基点是 P,它的阶是 n,$Q = lP$。$n = \prod p^{c_i}$ 为标准因子分解,首先,分解 $n = p^{c_1}p^{c_2}\cdots p^{c_i}$;其次,对每个 p^{c_i} 能计算 $l \bmod p^{c_i}$,也就是将找 l 的问题归结到寻找 $l \bmod p^{c_i}$ 上;最后,由中国剩余定理解同余方程组得到 l。当 n 不含有大素数因子时,该方法很有效,所以,为了抗击该攻击,n 必须是大素数因子。

3.2　对特殊曲线攻击

(1)MOV 攻击。

这个方法是 Menezes、Okamoto 和 Vanstone 在 1991 年提出的将 ECDLP 归约到有限域上离散对数的有效解法,称为 MOV 归约。这一方法主要用于对超奇异椭圆曲线的攻击,对其它的椭圆曲线不适应。

(2)Smart 方法。

1997 年 Smart、Satoh 和 Araki 同时分别独立地提出了对素域上某一类非正规椭圆曲线的攻击方法,即 SSAS 攻击或 Smart 方法。所谓非正规椭圆曲线为有限域 F_q 上的一条椭圆曲线的阶恰好是 q 的椭圆曲线。Smart 方法对于其它类型的椭圆曲线是无效的。

4 结束语

ECC 密码体制是建立在椭圆曲线密码理论基础上的先进公钥密码体制。该系统所具有的安全性已经被全世界所承认。基于其极强的安全性 ECC 加密技术将会广泛地被应用,因此文中基于 ECC 算法的注册码软件加密保护设计方案具有一定的理论参考价值和实际应用价值。

参考文献:

[1] 于 彬,许占文. 椭圆曲线密码体制的研究[J]. 沈阳工业大学学报,2004(5):551-554.

[2] 徐秋亮,李大兴. 椭圆曲线密码体制[J]. 计算机研究与发展,1999(11):1282-1288.

[3] 黄 俊,许 娟,左洪福. 基于 RSA 算法的注册码软件加密保护[J]. 计算机应用,2005(9):2080-2085.

[4] 张晓丰,樊启华,程红斌. 密码算法研究[J]. 计算机技术与发展,2006,16(2):179-180.

[5] 张 雁,林 英,郝 林. 构建安全椭圆曲线密码体制的关键问题[J]. 计算机应用,2004(12):82-84.

[6] IEEE P1363/D6(Drafe Version 6). Standard Specification for Public Key Cryptography [EB/OL]. 2004. http://grouper.ieee.org/groups/1361/P1363/draft.html.

[7] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) [S]. 1998.

[8] 户军茹,韩益亮. 椭圆曲线密码体制相关问题[J]. 通信技术,2003(12):151-152.

[9] 王张宜,杨寒涛,张焕国. 椭圆曲线密码的安全性分析[J]. 计算机工程,2002(5):161-163.

[10] Saeki M. Elliptic curve cryptosystems[EB/OL]. 2003-09-03. http://cnscenter.future.co.kr/crypto/algorithm/ecc.html.

[11] Pohlig S, Hellman M. An Improved Algorithm of Computing Logarithms Over GF(p) and Its Cryptographic Significance [J]. IEEE Trans on Information Theory, 1978(1):106-110.

[12] 于雪燕,胡金初,柴春轶. 椭圆曲线密码体制及其参数生成的研究[J]. 计算机技术与发展,2006,16(11):160-161.

(上接第 154 页)

[C]//Military Communications Conference. San Diego, CA: [s. n.], 2008:1-7.

[2] He W, Liu X, Nguyen H, et al. A cluster-based protocol to enforce integrity and preserve privacy in data aggregation[C]// 29th IEEE International Conference on Distributed Computing Systems Workshops. Montreal, QC: [s. n.], 2009:14-19.

[3] Bista R, Yoo H K, Chang J W. A new sensitive data aggregation scheme for protecting integrity in wireless sensor networks [C]//10th IEEE International Conference on Computer and Information Technology. Bradford, UK: [s. n.], 2010:2463-2470.

[4] Bista R, Jo K J, Chang J W. A new approach to secure aggregation of private data in wireless sensor networks[C]//Eighth IEEE International Conference on Dependable Autonomic and Secure Computing. Chengdu, China: [s. n.], 2009:394-399.

[5] Bista R, Kim H D, Chang J W. A new private data aggregation scheme for wireless sensor networks[C]//10th IEEE International Conference on Computer and Information Technology. Bradford, UK: [s. n.], 2010:273-280.

[6] 刘鑫芝. 无线传感器网络安全数据融合算法研究[J]. 计算机与现代化,2010(5):151-155.

[7] 唐 慧,胡向东. 无线传感器网络安全数据融合算法研究[J]. 通信技术,2007(12):290-293.

[8] 罗 蔚,胡向东. 无线传感器网络中一种高效的安全数据融合协议[J]. 重庆邮电大学学报(自然科学版),2009(1):110-114.

[9] 覃志松,黄延磊. Zigbee 无线传感器网络安全研究及改进[J]. 微计算信息,2010(3):54-55.

[10] 邓黎黎,刘才兴. 基于信任的无线传感器网络安全路由研究[J]. 计算机技术与发展,2010,20(6):159-162.

[11] 魏琴芳,张双杰,胡向东,等. 基于同态 MAC 的无线传感器网络安全数据融合[J]. 传感技术学报,2011(12):1750-1755.

[12] Madden S, Franklin M J, Hellerstein J M. TAG: a tiny aggregation service for ad-hoc sensor networks[C]//Proceedings of the 5th symposium on operating systems design and implementation. New York, USA: [s. n.], 2002:131-146.

[13] He W, Liu X, Nguyen H, et al. PDA: privacy-preserving data aggregation in wireless sensor networks[C]//Proceedings of the 26th IEEE International Conference on Computer Communications. Anchorage, AK: [s. n.], 2007:2045-2053.

[14] Levis P, Lee N, Welsh M, et al. TOSSIM: accurate and scalable simulation of entire TinyOS applications[C]//1st international conference on embedded networked sensor systems. Los Angeles, USA: [s. n.], 2003:126-137.

即时通讯实时监测系统的设计与实现

作者：刘庆， 刘颖， 周华春
作者单位：北京交通大学电子信息工程学院,北京100044
刊名：计算机技术与发展
英文刊名：Computer Technology and Development
年，卷(期)：2012(8)

参考文献(12条)

1. 于彬;许占文 椭圆曲线密码体制的研究[期刊论文]-沈阳工业大学学报 2004(05)

2. 徐秋亮;李大兴 椭圆曲线密码体制[期刊论文]-计算机研究与发展 1999(11)

3. 黄俊;许娟;左洪福 基于RSA算法的注册码软件加密保护[期刊论文]-计算机应用 2005(09)

4. 张晓丰;樊启华;程红斌 密码算法研究[期刊论文]-计算机技术与发展 2006(02)

5. 张雁;林英;郝林 构建安全椭圆曲线密码体制的关键问题 2004(12)

6. IEEE P1363/D6(Drafe Version 6).Standard Specification for Public Key Cryptography 2004

7. Public Key Cryptography for the Financial Services Industry:The Elliptic Curve Digital Signature Algorithm(ECDSA) 1998

8. 户军茹;韩益亮 椭圆曲线密码体制相关问题[期刊论文]-通信技术 2003(12)

9. 王张宜;杨寒涛;张焕国 椭圆曲线密码的安全性分析[期刊论文]-计算机工程 2002(05)

10. Saeki M Elliptic curve cryptosystems 2003

11. Pohlig S;Hellman M An Improved Algorithm of Computing Logarithms Over GF(p) and Its Cryptographic Significance 1978(01)

12. 于雪燕;胡金初;柴春轶 椭圆曲线密码体制及其参数生成的研究[期刊论文]-计算机技术与发展 2006(11)