第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

基于椭圆曲线和因子分解双难题的数字签名方案

周克元
(宿迁学院二系 宿迁 223800)

摘 要 对沈群等提出的同时基于椭圆曲线和因子分解双难题的数字签名方案给出了攻击分析,本文证明椭圆曲线或因子分解难题有一个可求解,则沈群方案可被攻破。同时给出了一个新的基于椭圆曲线和因子分解双难题的方案,证明了其正确性、安全性和不可伪造性。另外还给出了一个基于椭圆曲线和因子分解双难题的消息恢复数字签名方案,证明了其正确性、安全性和不可伪造性。

关键词 椭圆曲线,因子分解,数字签名,消息恢复,伪造攻击
中图法分类号 TP309.7 **文献标识码** A

Digital Signature Scheme Based on Elliptic Curve and Factoring

ZHOU Ke-yuan
(Department 2, Suqian College, Suqian 223800, China)

Abstract The digital signature algorithm proposed by SHEN Qun et al. gives analytical attack, which is based on elliptic curve and factoring problems. If the difficulties of elliptic curve or factoring can be solved, SHEN Qun digital signature schemes can be attacked. A new digital signature algorithm was proposed, which is based on elliptic curve and factoring problems. The correctness, security and unforgeability were proved. Another, a new digital signature algorithm with message recovery was proposed, which is based on elliptic curve and factoring problems. The correctness, security and unforgeability were proved.

Keywords Elliptic curve, Factoring, Digital signature, Message recovery, Forgery attack

1 引言

针对离散对数和因子分解双难题设计数字签名的研究较多,提出了多种方案[1-5]。椭圆曲线密码系统是离散对数密码系统在椭圆曲线上的移植,椭圆曲线比离散对数具有更高的安全性。针对椭圆曲线和因子分解双难题设计签名方案的研究较少,目前只有沈群等提出的方案[5],但沈群方案并不真正基于双难题,本文证明只要一个难题被攻破,则沈群方案可被攻破。进一步,给出了一个新的双难题签名方案,来防止各类攻击。另外还给出了一个基于椭圆曲线离散对数和因子分解双难题的消息恢复数字签名方案。

基于双难题设计的签名方案基于如下相关理论。

引理1[2] 大素数 $p, n=p_1q_1, n|(p-1)$,其中 p_1, q_1 为大素数。$g\in GF(p)$,且 g 的阶为 n,设 G 为由元素 g 生成的乘法群。对 $\forall y\in G$,求解方程 $y=g^{x^2} \bmod p$ 等价于求解离散对数 $y=g^u \bmod p$ 和求解二次同余方程 $x^2=u \bmod n$,而求解 $x^2=u \bmod n$ 等价于对数 n 进行因子分解。

引理2[6] E 是定义在 F_q 上的一个椭圆曲线。设 $n=p_1q_1, n|\sharp E(F_q)$,其中 p_1, q_1 为大素数。$G\in E(F_q)$,且 G 的阶为 n,D^* 为由元素 G 生成的循环加法群。对 $\forall Y\in D^*$,求解方程 $Y=x^2G$ 等价于在 D^* 上求解椭圆曲线上的离散对数问题 $Y=uG$ 和求解二次同余方程 $x^2=u \bmod n$,而求解 $x^2=u \bmod n$ 等价于对数 n 进行因子分解。

2 沈群方案及相关攻击

2.1 沈群方案

(1)参数选取

设 p 是大素数,且 $p=6p_1q_1-1$,其中 p_1, q_1 为大素数。E 是由 Weierstrass 方程 $Y^2=X^3+1$ 定义在 F_p 上的超奇异椭圆曲线。E 在 F_p 上的点的集合 $E(F_q)$ 形成一个阶为 $p+1$ 的 Abel 群,而 $p=3p_1q_1-1$,所以 $E(F_q)$ 中存在 $n=p_1q_1$ 阶的循环子群 D^*,取一生成元 G,其阶为 n。参数 (p, n, G) 公开,(p_1, q_1) 保密。用户选取私钥 $x\in\{1, 2, \cdots, n-1\}$,计算公钥 $Y=x^2G$。待签名消息 $m(<n)$。

(2)签名过程

对于任意消息 m,签名者进行如下计算:

①随机选择一整数 $t(1<t<n)$,计算 $R=t^2G=(r_x, r_y)$,且 $r_x\in F_p, r_y\in F_p$。

②求解签名方程 $s=t^{-1}(m-xr_x) \bmod n, c=xt \bmod n$。则消息 m 的签名为 (R, s, c)。

(3)验证过程

验证者接收到消息组 $(m; (R, s, c))$ 后,进行如下验证 $(m^2-2csr_x)G=r_x^2Y+s^2R$,如果验证方程成立,签名有效;否则签名无效。

本文受宿迁市科研项目:数字签名算法的分析与研究,宿迁学院科研项目:离散对数数字签名算法的研究与改进资助。
周克元(1978—),男,硕士,讲师,主要研究方向为密码与编码,E-mail:zhoukeyuan2001@163.com。

2.2 对沈群方案的攻击

(1)若因子分解难题可计算,则沈群方案可被攻破

$sc=x(m-xr_x) \bmod n=(xm-x^2r_x) \bmod n$,若 n 因子分解可攻破,由数论相关理论[7],则可求出私钥 x,进一步由 $c=xt \bmod n$ 可求出随机数 t。

(2)若椭圆曲线难题可计算,则沈群方案可被攻破

若椭圆曲线离散对数问题可攻破,则由 $Y=x^2G$ 可求出 x^2。由 $s^2c^2=x^2(m^2+x^2r_x^2-2mr_xx) \bmod n$ 可求出私钥 x,进一步由 $c=xt \bmod n$ 可求出随机数 t。

根据上述分析,沈群方案并不是真正基于双难题的签名方案,只要因子分解可攻破或椭圆曲线离散对数可攻破,沈群方案则不再安全。

3 新的双难题签名方案

下面给出一个新的方案,方案基于椭圆曲线离散对数和因子分解双难题。

(1)参数选取

在 2.1 节(1)参数选取的基础上,计算 $Z=x^{-2}G$,公钥为 (p,n,G,Y,Z),私钥为 (x,p_1,q_1)。$h()$ 为安全 Hash 函数。

(2)签名阶段

对于任意消息 m,签名者进行如下计算:

①随机选择整数 $t(1<t<n)$,计算 $R=t^2G=(r_x,r_y)$,$r=r_x \bmod n$,计算 $e=h(m)$;

②计算 $s=t^{-1}(x+x^{-1}e) \bmod n$。

则消息 m 的签名为 (R,s)。签名中用到的 x^{-1} 可预求逆,以提高签名速度

(3)验证阶段

B 接收到签名消息组 $(m;(R,s))$ 后,进行如下验证:

①计算 $e=h(m)$;

②计算 $s^2R=Y+e^2Z+2eG$,若正确则接受该签名,否则不接受。

(4)正确性证明

$s^2R=t^{-2}(x^2+x^{-2}e^2+2e)$,$R=(x^2+x^{-2}e^2+2e)$,$G=Y+e^2Z+2eG$

4 安全性及效率分析

4.1 对抗从公钥中求出私钥 x 的攻击

攻击者从方程 $Y=x^2G$ 中求解 x,由引理 2 知其难度相当于因子分解和求解离散对数问题。

4.2 对抗从签名中求出密钥 x 的攻击

签名方程 $s=t^{-1}(x+x^{-1}e) \bmod n$ 中有两个变量 x,t,故无法求出密钥 x。

4.3 对抗伪造签名攻击

攻击者任取消息 m,可计算出 $e=h(m)$。随机选取 t,可计算出 R,r,但由于不知私钥 x,无法从式 $s=t^{-1}(x+x^{-1}e) \bmod n$ 中求出 s,因此不能伪造签名。

4.4 对抗具有计算离散对数问题能力的攻击

假设攻击者具有计算离散对数问题的能力,则可由 $Y=x^2G$ 计算出 x^2,而由 $x^2 \bmod n$ 求解 x 相当于求解 n 的因子分解[6],故无法求出 x,同理无法求出随机数 t,则由方程 $s=t^{-1}(x+x^{-1}e) \bmod n$ 无法求出签名 s。

4.5 对抗具有计算因子分解问题的攻击

假设攻击者具有计算因子分解能力,若想由式 $Y=x^2G$ 计算私钥 x,需要首先解决离散对数问题求出 x^2,然后才能利用因子分解计算 x。另外,攻击者想伪造签名也无法成功,假设攻击者任取消息 m,随机选取 t,可计算出 e,r,t^{-1},但若要计算 $s=t^{-1}(x+x^{-1}e) \bmod n$ 仍需 x。第三,若已知 $s^2=t^{-2}(x^2+x^{-2}e^2+2e) \bmod n$ 亦可求出 s,但求 s^2 需要知道 x^2 和 x^{-2} 的值,而这首先需要具有计算椭圆曲线离散对数的能力,由 $Y=x^2G$、$Z=x^{-2}G$ 计算出 x^2 和 x^{-2}。则即使因子分解问题可计算,s 也无法求出。

4.6 对抗随机数 t 同态攻击

假设签名者使用了 3 个随机数 t_1,t_2,t_3 分别对消息 m_1,m_2,m_3 进行签名,其中随机数 t_1,t_2,t_3 满足 $t_3=(t_1+t_2) \bmod n$,签名分别为 $(m_1;(R_1,s_1))$、$(m_2;(R_2,s_2))$、$(m_3;(R_3,s_3))$,对应签名方程列成方程组为:

$$\begin{cases} s_1t_1=(x+x^{-1}e_1) \bmod n \\ s_2t_2=(x+x^{-1}e_2) \bmod n \\ s_3(t_1+t_2)=(x+x^{-1}e_3) \bmod n \end{cases}$$

化简后可得关于 x 的一元二次方同余方程,求解 x 相当于对 n 因子分解。故可防止随机数 t 同态攻击。

4.7 效率分析

利用椭圆曲线因子分解设计签名方案最新的有崔哲方案,将本文算法复杂度与其比较,复杂度相同,签名长度较短,结果见表 1。

表 1 两种方案比较

	崔哲方案[8]		本文方案	
	签名	验证	签名	验证
模乘	1	3	1	3
模逆	1	0	1	0
点积	5	8	3	3
Hash 函数	1	1	1	1
签名长度	4|n|		3|n|	
数学难题	椭圆曲线、因子分解		椭圆曲线、因子分解	

5 基于椭圆曲线因子分解的消息恢复数字签名方案

利用椭圆曲线因子分解设计消息恢复数字签名方案的相关研究较少,本文给出一个方案。

(1)参数选取

参数选取同 2.1 节(1)。另增加 $h()$ 为安全 Hash 函数。

(2)签名阶段

对于任意消息 m,签名者进行如下计算:

①随机选择整数 $t(1<t<n)$,计算 $R=t^2G=(r_x,r_y)$,$r_1=r_x \bmod n$;

②计算 $e=h(r_1,m) \bmod n$;

③串接 $m'=m \| e$,计算 $r=(m'-r_1) \bmod n$。若 $m'>n$,则将 m' 分解为 $m_1'm_2'\cdots m_k'$ 使得每一个 $m_i'<n$,再进行操作;

④计算 $s=(tx^{-1}-h(r)) \bmod n$。

则消息 m 的签名为 (r,s)。签名中用到的 x^{-1} 可预求逆,以提高签名速度。

(3)验证阶段

验证者接收到签名消息组 $(m;(r,s))$ 后,进行如下验证:

①计算 $(s+h(r))^2Y=(x_2,y_2)$,$r_2=x_2 \bmod n$;

②消息恢复 $M'=(r_2+r) \bmod n$,设 $M'=M \| e'$;

③验证 $e'=h((M'-r) \bmod n,M) \bmod n$,若正确则接受该签名且 $M=m$,否则不接受。

(4) 正确性证明

因为 $(s+h(r))^2Y=t^2x^{-2}Y=t^2G$，所以 $r_2=r_1$，$M'=(r_2+r) \bmod n=m'$，$M=m$，$e'=e$，因此 $e'=h((M'-r) \bmod n, M) \bmod n=h(r_1,m) \bmod n=e$。

6 安全性及效率分析

6.1 对抗从公钥中求出私钥 x 的攻击

攻击者从方程 $Y=x^2G$ 中求解 x，由引理 2 知其难度相当于因子分解和求解离散对数问题。

6.2 对抗从签名中求出密钥 x 的攻击

签名方程 $s=(tx^{-1}-h(r)) \bmod n$ 中有两个变量 x，t，故无法求出密钥 x。

6.3 对抗伪造签名攻击

任取整数 $t(1<t<n)$，虽可计算出 $R=t^2G$，r_1，e，m'，r，但因不知私钥 x，不能计算出 s，攻击不成功。

6.4 对抗具有计算椭圆曲线离散对数问题能力的攻击

假设攻击者具有计算离散对数问题的能力，则可由 $Y=x^2G$ 计算出 x^2，而由 $x^2 \bmod n$ 求解 x 相当于求解 n 的因子分解[7]，故无法求出 x，同理无法求出随机数 t，则由方程 $s=(tx^{-1}-h(r)) \bmod n$ 无法求出签名 s。

6.5 对抗具有计算因子分解问题的攻击

假设攻击者具有计算因子分解的能力，若想由式 $Y=x^2G$ 计算私钥 x，需要首先解决离散对数问题求出 x^2，然后才能利用因子分解计算 x；另外，攻击者想伪造签名也无法成功，假设攻击者任取消息 m，随机选取 t，可计算出 $R=t^2G$，r_1，e，m'，r，但若要计算 $s=(tx^{-1}-h(r)) \bmod n$，仍需 x。

6.6 随机数 t 同态攻击分析

假设签名者使用了 3 个随机数 t_1,t_2,t_3 分别对消息 m_1，m_2,m_3 进行签名，其中随机数 t_1,t_2,t_3 满足 $t_3=(t_1+t_2) \bmod n$，签名分别为 (r_1,s_1)、(r_2,s_2)、(r_3,s_3)，对应签名方程列成方程组为：

$$\begin{cases} s_1=(t_1x^{-1}-h(r_1)) \bmod n \\ s_2=(t_2x^{-1}-h(r_2)) \bmod n \\ s_3=((t_1+t_2)x^{-1}-h(r_3)) \bmod n \end{cases}$$

可计算出 x^{-1}，故方案不能抵抗随机数 t 同态攻击，参数 t 的选取需保持随机性。

6.7 效率分析

利用椭圆曲线因子分解双难题设计消息恢复数字签名方案的相关研究较少。与最新的利用椭圆曲线单难题设计消息恢复数字签名的方案比较，本文方案的运算效率和签名长度亦达到最优，见表 2。

表 2 3 种方案比较

	阚元平方案[9]		周克元方案[10]		本文方案	
	签名	验证	签名	验证	签名	验证
模乘	1	2	1	1	1	1
模逆	0	0	0	0	0	0
点积	1	0	2	1	2	1
Hash 运算	1	1	1	1	1	1
签名长度	3|n|		5|n|		2|n|	
数学难题	椭圆曲线		椭圆曲线		椭圆曲线、因子分解	

结束语 对沈群提出的基于椭圆曲线离散对数和因子分解双难题的数字签名方案进行了分析，指出了错误，进行了攻击分析。给出了一个新的签名方案，证明了其正确性和安全性，并与已有方案进行了比较。另给出一个基于椭圆曲线离散对数和因子分解双难题的消息恢复数字签名方案，证明了其正确性和安全性，并与已有方案进行了比较。

参 考 文 献

[1] Harn L. Public-key Cryptosystem Design Based on Factoring and Discrete Logarithms[J]. IEEE Proceedings-Computers and Digital Techniques, 1994, 141(3): 193-195

[2] 邵祖华. 基于因数分解和离散对数的数字签名协议[J]. 通信保密, 1998(4): 36-41

[3] 沈忠艳, 于秀源. 一个基于两大难题的数字签名方案[J]. 信息技术, 2004, 28(6): 21-22

[4] Zheng Ming-hui, Cui Guo-hua. New signature scheme based on two cryptographic assumptions[J]. Journal of Southeast University(English Edition), 2007, 23(3): 461-464

[5] Ismail E S, Tahat N M F. The Modified Signature Scheme Based on Factoring and Discrete Logarithms[J]. Information Security Journal: A Global Perspective, 2011, 20: 245-249

[6] 沈群, 陈桢. 同时基于两种数学难题的数字签名方案[J]. 福建电脑, 2008(2): 16, 28

[7] 陈景润. 初等数论(3)[M]. 哈尔滨: 哈尔滨工业大学出版社, 2012: 120-124

[8] 崔哲, 余梅生. 一种改进的 H-K 数字签名方案[J]. 计算机科学, 2005, 32(8): 337-338

[9] 阚元平. 基于椭圆曲线的具有消息恢复特性的签名方案[J]. 计算机工程与科学, 2010, 32(2): 58-59

[10] 周克元. 快速椭圆曲线消息恢复数字签名方案[J]. 西北师范大学学报: 自然科学版, 2013, 49(5): 54-56

(上接第 360 页)

[4] 胡乔林, 孙一品, 苏金树. BAR-BGP: 基于备份通告和恢复转发的可靠域间路由[J]. 计算机研究与发展, 2011, 48(12): 2242-2252

[5] Lad M, Massey D, Pei D, et al. PHAS: a prefix hijack alert system[C]// Proceedings of the 15th USENIX Security Symposium. Vancouver, Canada, 2006: 108-119

[6] Schapira M, Zhu Y, Rexford J. Putting BGP on the right path: A case for next-hop routing[C]// Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. Monterey, CA, USA, 2010: 1-6

[7] RIPE. Ripe's MyASN[EB/OL]. http://www.ris.ripe.net/myasn.html, 2011-05-01/2013-04-22

[8] 刘欣, 王小强, 朱培栋, 等. 互联网域间路由系统安全态势评估[J]. 计算机研究与发展, 2009, 46(10): 1669-1677

[9] 郭毅, 王振兴, 程东年. 基于博弈的域间路由协同监测激励策略[J]. 中国科学, 2012, 42(7): 803-814

[10] Shen Y, Bi J, Wu J P, et al. A two-level source address spoofing prevention based on automatic signature and verification mechanism[C]// Proceedings of the IEEE symposium on computers and communications. Tarrytown, NY, USA, 2008: 392-397

[11] Ning H, Peidong Z, Peng Z. Reputation Mechanism for Inter-domain Routing Security Management[C]// Proceedings of the 9th International Conference on Computer and Information Technology. Xiamen, China, 2009: 98-103

[12] 李峰, 申利民, 司亚利, 等. 一种基于实体上下文和时间戳的信任预测模型[J]. 电子与信息学报, 2011, 33(5): 1217-1223