Software Engineering and Applications 软件工程与应用, 2012, 1, 43-46
http://dx.doi.org/10.12677/sea.2012.12008 Published Online December 2012 (http://www.hanspub.org/journal/sea.html)

Analysis and Improvement of a Digital Signature Based on Conic Curve over Z_n *

Junxia Liu[1], Xianwen Yang[2]

[1]Automatic Command Station, Henan Provincial Military Command, Zhengzhou
[2]Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou
Email: yxw200420042004@163.com

Received: Oct. 10th, 2012; revised: Oct. 17th, 2012; accepted: Oct. 28th, 2012

Abstract: Under the analyses of an ElGamal digital signature scheme based on conic curve over Z_n proposed by Yang Hui et al., this paper reveals that the secret key can be gained by the public key and the signature, so Yang et al.'s scheme is not security. An improved digital signature scheme is given, and it can resist the secret key gaining attack. Moreover, a multi-signature digital scheme is supplied based on the improved digital signature scheme. The multi-signature digital scheme has the advantage not to exchange many times among singers to get the same parameter, and therefore reduces the communication traffic.

Keywords: Conic Curve; Discrete Logarithm; Digital Signature; Multiple Digital Signatures; Communication

对一个环 Z_n 上圆锥曲线数字签名的分析与改进*

刘军霞[1]，杨先文[2]

[1]河南省军区指挥自动化工作站，郑州
[2]解放军信息工程大学电子技术学院，郑州
Email: yxw200420042004@163.com

收稿日期：2012 年 10 月 10 日；修回日期：2012 年 10 月 17 日；录用日期：2012 年 10 月 28 日

摘　要：杨慧等人基于环 Z_n 上的圆锥曲线构造了一个 ElGamal 型数字签名方案，文章分析指出，该方案的私钥可以从公钥和签名中恢复出来，因而该签名方案是不安全的。对杨慧等人的签名方案进行了改进，通过分析可知改进方案能够抵抗密钥恢复攻击。基于改进数字签名方案构造了一个多重数字签名方案，该多重数字签名方案无需进行多次交换数据以获得同一个参数，减少了通信量。

关键词：圆锥曲线；离散对数；数字签名；多重数字签名；通信

1. 引言

离散对数问题是公钥密码和数字签名中常用数学难题之一，上世纪 90 年代提出的圆锥曲线应用于公钥密码中，可以视其为有限域上离散对数问题的一个推广。针对有限域GF(p)上的圆锥曲线 $C_p(a, b)$，1996 年张明志[1]首先引进 $C_p(a, b)$上加法运算 $\oplus$，并证明了 $\left(C_p(a,b), \oplus\right)$ 是一个有限加群。1998 年，曹珍富[2]提出了基于 GF(p)上的圆锥曲线公钥密码体制。2005 年，孙琦等人[3]将有限域 GF(p)上的圆锥曲线的研究拓展到环 Z_n 上，并在其上模拟了数字签名方案。

2007 年，杨慧等人[4]基于环 Z_n 上的圆锥曲线构造了一个 ElGamal 数字签名方案，他们综合利用了大数分解的困难性和有限群上计算离散对数问题的困难性，试图增强该签名方案的安全性。本文分析指出，该方案的私钥可以从一组签名消息对和公钥恢复出来，因此，杨慧等人[4]的数字签名方案没有达到预期

*基金项目：国家自然科学基金项目(61072047)。

的效果。对该签名方案进行了改进，改进后的方案可抵抗本文关注的密钥恢复攻击，并利用改进方案提出了一个多重数字签名方案[5]。与现有的 ElGamal 广播多重数字签名相比，本文方案在签名时无需签名者多次数据交互获得同一参数，因而降低了通信代价。

本文剩下部分如下安排：第 2 节介绍环 Z_n 上圆锥曲线的基础知识；第 3 节对杨慧等人的签名方案进行了分析与改进，改进方案能够抵抗密钥恢复攻击；第 4 节基于改进后签名方案，提出了一个多重数字签名方案，与现有的 ElGamal 多重数字签名方案相比，本文多重签名方案在签名时无需多次交换数据，减少了通信量；第 5 节对改进后签名方案的安全性进行分析；第 6 节结论。

2. 环 Z_n 上的圆锥曲线

设 Z_n 是模 n 的剩余类环，定义 Z_n 上的圆锥曲线 $C_n(a, b)$为同余方程

$$y^2 = ax^2 - bx \pmod{n} \tag{1}$$

在 Z_n 上所有解(x, y)构成的集合，其中 $n = pq$, p, q 为两个不同的大素数，$(a, n) = (b, n) = 1$，a 是模 p 的二次非剩余，b 是模 q 的二次非剩余，且 $p + 1 = 2r$，$q + 1 = 2s$，其中 r，s 是素数，曲线的阶 $N_n = 2rs$。可以对圆锥曲线 $C_n(a, b)$上的点定义一个加法运算 $\oplus$，圆锥曲线上点的集合在该加法作用构成一个有限交换群，在此圆锥曲线上阶为 $N_n = 2rs$ 的点 G 称为基点。圆锥曲线上的离散对数问题定义为：由基点 G 生成的群 $S = \{O, G, 2G, \cdots, (N_n - 1)G\}$，给定 $M, N \in S$ 满足 $M = eN$，则求出正整数 e 是非常困难的[4]。该问题被普遍认为是一个数学困难问题。

3. 杨慧等方案的分析与改进

3.1. 杨慧等签名方案

原方案由参数选取、签名过程和验证过程三部分构成。

参数选取：

1) 设 $G = (x_G, y_G)$ 为曲线 $C_n(a,b)$ 上一点，其阶为 $N_n = 2rs$，称 G 为 $C_n(a, b)$的一个基点；

2) 设 $d \in Z_{N_n}^*$ 为签名私钥，$Q = dG \pmod{n}$ 为签名验证公钥；

3) $H(m)$是对消息 m 的一种安全 Hash 映射；

4) 随机选取一个整数 $k \in Z_{N_n}^*$，且 $(k, N_n) = 1$；

5) 公开 n, N_n, a, b, G, Q, k 作为公钥，私钥为 d。

签名过程：

1) 计算 l，使得 $kl = 1 \pmod{N_n}$；

2) 计算 $kG = (x_1, y_1)$，$\gamma = x_1 \pmod{N_n}$；

3) 计算 $\delta = (H(m) - d\gamma) l \pmod{N_n}$，如果 $\delta = 0$，则重新选择 k 并返回步骤(1)，否则将(γ, δ)作为对消息 m 的签名发送给收方 B。

验证过程：

B 收到签名(γ, δ)后作如下验证

1) 取 $u_1 = \gamma$，$u_2 = \delta k \pmod{N_n}$；

2) 计算 $U = u_1 Q \oplus u_2 G \pmod{n}$。如果 $U = (0, 0)$则拒绝这个签名，否则计算 $V = H(m) G \pmod{n}$。当且仅当 $U = V$ 时，接受这个签名。

其签名验证证明请参考文献[4]。

3.2. 对杨慧等签名方案的分析

若攻击者能够截获一组消息签名对(m, γ, δ)，则攻击者可以运用 Fermat 小定理求逆法[6]计算出 γ 模 N_n 的逆元 γ^{-1}。根据签名过程 $\delta = (H(m) - d\gamma) l \pmod{N_n}$ 可得

$$d = (H(m) - k\delta) \gamma^{-1} \pmod{N_n} \tag{2}$$

因为明文 m 的 Hash 值 $H(m)$和公钥 k 已知，所以通过式(2)可恢复私钥 d。因此，杨慧等人[4]提出的数字签名方案是不安全的。

3.3. 对杨慧等签名方案的改进

原方案安全隐患的根源在于签名过程步骤(1)中 l 的不合理选取。事实上，任何一种与公钥有关又未基于数学难题的选取，都不能保证计算复杂度足够大，从而也就不能保证方案的安全性。为避免攻击者对私钥进行恢复，本文对原方案改进如下。

改进方案由参数选取、签名过程、验证过程和签名验证证明四部分构成。

参数选取：

1) 设 $G = (x_G, y_G)$ 为曲线 $C_n(a, b)$上一点，其阶为 $N_n = 2rs$，称 G 为 $C_n(a, b)$的一个基点；

2) 设 $d \in Z_{N_n}$ 为签名私钥，

$Q_1 = dG \pmod{n}, Q_2 = dQ_1 \pmod{n}$ 为签名验证公钥；

3) $H(m)$是对消息 m 的一种安全 Hash 映射；

4) 随机选取一个整数 $k \in Z_{N_n}$，且 $(k, N_n)=1$；

5) 公开 $n, N_n, a, b, G, Q_1, Q_2, k$ 作为公钥，私钥为 d。

签名过程：

1) 计算 $kG=(x_1, y_1)$，$\gamma = x_1 (\mathrm{mod} N_n)$；

2) 计算 $\delta = (H(m)-\mathrm{d}\gamma)\mathrm{d} (\mathrm{mod} N_n)$，如果 $\delta=0$，则重新选择 k 并返回步骤(1)，否则将(γ, δ)作为对消息 m 的签名发送给收方 B。

验证过程：

B 收到签名(γ, δ)后作如下验证

1) 取 $u_1=\gamma$，$u_2=\delta$；

2) 计算 $U=u_1Q_2 \otimes u_2G(\mathrm{mod}\, n)$。如果 U = (0, 0) 则拒绝这个签名，否则计算 $V=H(m)Q_1(\mathrm{mod}\, n)$。当且仅当 $U=V$ 时，接受这个签名。

签名验证证明：

$$\begin{aligned} U &= u_1Q_2 \oplus u_2G(\mathrm{mod}\, n) = \gamma Q_2 \oplus \delta G(\mathrm{mod}\, n) \\ &= \gamma \mathrm{d} Q_1 \oplus (H(m)-\mathrm{d}\gamma)\mathrm{d}G(\mathrm{mod}\, n) \\ &= \gamma \mathrm{d}^2 G \oplus (\mathrm{d}H(m)-\mathrm{d}^2\gamma)G(\mathrm{mod}\, n) \\ &= dH(m)G(\mathrm{mod}\, n) = H(m)Q_1(\mathrm{mod}\, n) \\ V &= H(m)Q_1(\mathrm{mod}\, n) \end{aligned}$$

当且仅当 $U=V$ 时，接受这个签名。

4. 基于改进方案的多重签名方案

由于数字签名的完整性、不可否认性等特点，数字签名代替手写签名已经被信息社会逐渐接受。然而，在许多情况下，一份文件需要多个人进行签名。作为第 3 节改进签名方案的应用，本节提出基于环 Z_n 上的圆锥曲线多重数字签名方案，该方案由参数选取、收集人与签名人相互验证[7]、签名过程、验证过程、签名验证证明五部分组成。

参数选取：

选择 Z_n 上的圆锥曲线 $C_n(a, b)$，满足条件同上，设共有 k 个签名人 $U_i (i=1,2,\cdots,k)$，每个签名者拥有一个私钥 $d_i \in Z_{N_n}^*$，满足条件 $Q_{i,1}=d_iG(\mathrm{mod}\, n)$，$Q_{i,2}=d_iQ_{i,1}(\mathrm{mod}\, n)$，其中 $Q_{i,j}\ (j=1,2)$ 为签名公钥，G 为选定圆锥曲线上的基点。U_C 为消息的收集人，U_V 为签名验证人。

收集人与签名人相互验证：

1) 每个 U_i 计算 $T_{i,j}=d_iQ_{C,j}(\mathrm{mod} n) = (x'_{i,j}, y'_{ij})$，$\beta_{i,j}=x'_{i,j}(\mathrm{mod} N_n)$，将 $\beta_{i,j}$ 发给 U_C；

2) U_C 计算 $R_{i,j}=d_CQ_{i,j}(\mathrm{mod} n)=(x''_{i,j}, y''_{ij})$，$\alpha_{i,j}=x''_{i,j}(\mathrm{mod} N_n)$，若 $\alpha_{i,j}=\beta_{i,j}$，则 U_i 合法，否则不合法；

3) U_C 计算 $D_i=d_CQ_{i,j}(\mathrm{mod} n)=(x^*_{i,j}, y^*_{i,j})$，$\eta_{i,j}=x^*_{i,j}(\mathrm{mod} N_n)$，将 $\eta_{i,j}$ 发给 U_i；

4) U_i 计算 $E_{i,j}=d_iQ_{C,j}(\mathrm{mod} n)=(x^{**}_{i,j}, y^{**}_{i,j})$，$\varepsilon_{i,j}=x^{**}_{i,j}(\mathrm{mod} N_n)$，若 $\varepsilon_{i,j}=\eta_{i,j}$，则 U_C 合法，否则不合法。

签名过程：

1) 消息发起人 U_I 将消息 m 发给每个签名人 U_i 和消息收集人 U_C；

2) U_i 选择随机数 $k_i\ (1 \le k_i \le N_n-1)$，利用 3.3 小节签名过程生成签名$(\gamma_i, \delta_i)$，并将其发送给消息收集人 U_C；

3) U_C 利用 3.3 小节验证过程验证每个(γ_i, δ_i)，当都正确时，计算 $\delta=\delta_1+\delta_2+\cdots\delta_k(\mathrm{mod} N_n)$。若 δ = 0 则要求每个签名人重签，否则将 $(\gamma_1, \gamma_2, \cdots \gamma_k, \delta)$ 作为对消息 m 的签名发给验证人 U_V。

验证过程：

U_V 首先计算 $Q_1=Q_{1,1}\oplus Q_{2,1}\oplus\cdots\oplus Q_{k,1}(\mathrm{mod} n)$，进而计算：

$$U=H(m)Q_1(\mathrm{mod} n),$$
$$V=\gamma_1Q_{1,2}\oplus\gamma_2Q_{2,2}\oplus\cdots\oplus\gamma_kQ_{k,2}(\mathrm{mod} n),$$
$$W=\delta G(\mathrm{mod} n),$$

若三者有为(0, 0)，则拒绝该签名；若 $W\oplus V(\mathrm{mod} n)=U$ 成立，则接受该签名，否则拒绝。

签名验证证明：

$$\begin{aligned} W\oplus V(\mathrm{mod} n) &= \delta G \oplus (\gamma_1Q_{1,2}\oplus\gamma_2Q_{2,2}\oplus\cdots\oplus\gamma_kQ_{k,2})(\mathrm{mod} n) \\ &= \sum_{i=1}^{k}(d_iH(m)-\gamma_id_i^2)G \oplus (\gamma_1Q_{1,2}\oplus\gamma_2Q_{2,2}\oplus\cdots\oplus\gamma_kQ_{k,2})(\mathrm{mod} n) \\ &= \sum_{i=1}^{k}(d_iH(m)-\gamma_id_i^2)G \oplus \sum_{i=1}^{k}\gamma_id_i^2G(\mathrm{mod} n) = \sum_{i=1}^{k}d_iH(m)G(\mathrm{mod} n) \\ &= H(m)Q_{1,1}\oplus H(m)Q_{2,1}\oplus\cdots\oplus H(m)Q_{k,1}(\mathrm{mod} n) = H(m)Q_1(\mathrm{mod} n) = U \end{aligned}$$

所以若 $W \oplus V \left(\mathrm{mod}n\right) = U$ 成立，则接受该签名。

由签名过程知，签名人把签名直接发给消息收集人就已完成签名，而同类 ElGamal 型签名方案需要签名人两次发给消息收集人才能完成签名[7,8]。因此，该签名方案减少了通信量。

5. 改进方案的安全性分析

下面对改进的签名方案进行安全性分析：

1) 若攻击者能够截获一个消息签名对(m, γ, δ)，那么根据签名过程 $\delta = \left(H\left(m\right) - \mathrm{d}\gamma\right)d\left(\mathrm{mod}N_n\right)$ 可得二次同余方程

$$\mathrm{d}^2\gamma - \mathrm{d}H\left(m\right) + \delta = 0\left(\mathrm{mod}N_n\right) \qquad (3)$$

其中 $N_n = 2rs$ 是一个大整数。由数论知识可得，在仅已知 N_n 而未知其分解的情况下，由式(3)求解 d 是一个困难问题[9]。换言之，攻击者“几乎不可能”通过消息签名对(m, γ, δ)恢复出私钥 d。因此，改进方案能够抵抗密钥恢复攻击；

2) 为防止签名重放攻击，可在消息签名过程中设立时间标志，验证过程中对时间标志进行验证，若发现时间标志无效，则拒绝该签名；

3) 就目前而言，如果攻击者欲伪造一个有效的签名(γ, δ)，需要求解的问题难度不低于求解基于环 Z_n 上圆锥曲线上的离散对数的难度。因此，改进签名方案能抵抗此类的伪造攻击；

4) 安全运行的前提是确保私钥 d 不能泄漏，否则攻击者将很容易地伪造签名值，其后果往往是灾难性的。为减少私钥 d 被盗的损失，可在改进签名方案的基础上加入前向安全机制[10]。

此外，圆锥曲线上的多重数字签名方案是在改进签名方案的基础上建立起来的，故与基于改进签名方案具有相同的安全性。

6. 结论

本文根据环 Z_n 上的圆锥曲线公钥密码体制，改进了杨慧的数字签名方案，其安全性基于大数分解的困难性和环 Z_n 上圆锥曲线 $C_n(a, b)$的离散对数问题。作为改进签名方案的应用，提出了一个多重数字签名方案。最后，改进签名方案的安全性分析表明改进方案能抵抗密钥恢复攻击，并对其它安全指标也进行了说明。作为下一步研究工作，我们将在本文研究基础上实现其他数字签名方案(如代理签名、群签名和盲签名)。

参考文献 (References)

[1] 张明志. 用圆锥曲线分解整数[J]. 四川大学学报(自然科学版), 1996, 33(4): 356-359.

[2] 曹珍富. 基于有限域 F_P 上圆锥曲线的公钥密码系统[A]. 密码学新进展——Chinacrypt'98[C]. 北京: 科学出版社, 1998: 45-49.

[3] 孙琦, 朱文余, 王标. 环 Z_n 上圆锥曲线和公钥密码协议[J]. 四川大学学报(自然科学版), 2005, 42(3): 471-478.

[4] 杨慧, 肖国镇. 基于环 Z_n 上圆锥曲线的 ElGamal 数字签名方案[J]. 计算机科学, 2007, 34(6): 98-100.

[5] T. C. Wu, S. L. Chou and T. S. Wu. Two-based multisignature protocols for sequential and broadcasting architectures. Computer Communications, 1996, 19(9): 851-856.

[6] A. J. Menezes, P. C. Oorschot and S. A. Vanstone. 胡磊, 王鹏, 译. 应用密码学手册[M]. 北京: 电子工业出版社, 2005: 56-64.

[7] 王晓明. 一种多重数字签名方案的安全方案[J]. 南开大学学报(自然科学版), 2003, 36(1): 33-38.

[8] 杜海涛, 张青坡, 钮心忻等. 一个新的离散对数有序多重签名方案[J]. 计算机工程与应用, 2007, 43(2): 148-150.

[9] 潘承洞, 潘承彪. 初等数论[M]. 北京: 北京大学出版社, 2001: 157-176.

[10] 杨洁, 钱海峰, 李志斌. 一种具有强前向安全性的代理签名方案[J]. 计算机工程, 2008, 34(17): 162-166.