广义圆锥曲线的多方签名的安全分析与设计

丁 丽[1,2]，周 渊[1,2]，钱海峰[2]
（1. 国家计算机网络与信息安全管理中心，北京 100029；2. 华东师范大学 计算机系，上海 200241）

摘 要：针对一个广义圆锥曲线的多方签名协议（Lin-Wang-Li 协议）进行安全性分析，指出该方案存在着严重的伪造问题，方案的安全性没有基于广义圆锥曲线的离散对数问题和整数分解等任何数学难题，攻击者可以不用解决任何数学难题便可以伪造签名. 同时，对广义的圆锥曲线的多方签名协议安全设计问题提出了解决方案.

关键词：多方签名协议；广义圆锥曲线；离散对数；伪造攻击；数字签名
中图分类号：TP 309.7 **文献标志码**：A **文章编号**：0254－0037(2010)05－0646－05

多方数字签名方案允许多个签名人共同认证1个电子文件，产生固定长度的签名协议. 多方签名必须能证明签名的产生是由持有对应私钥的人员共同签署的文件. 同时，多方数字签名的验证能在一个逻辑步骤内完成，验证者只需将签名人的公钥带入1个等式即可，无需用每个参与签名人的公钥进行逐步验证. 目前，多方(数字)签名协议被广泛应用于组播通信的认证，P2P 的文件共享及移动 Ad Hoc 网络等认证问题. 作为一种特殊的数字签名，该协议被广泛用于共同签署电子文件，认证中心 CA 对数字证书的分发等密码协议.

1 研究背景及本文的贡献

Itakura 等[1]提出了多方数字签名的概念，目前，很多学者提出了各种不同的方案[2-3]. 这些方案都不能抵抗流氓密钥攻击(rogue key attack)，即攻击者可以任意选择其公钥. 针对这样的攻击，人们对公钥基础设施(PKI)中的认证中心(CA)提出了不同的要求，如果 CA 在发布数字签名的公钥证书时需要用户提供私钥或者相应的零知识证明，称这样的公钥注册模型为知道私钥的证明模型(KOSK model)；如果只是要求用户提供对应公钥签名，称之为证明拥有模型(POP model)；如果仅要求用户给出相应的公钥便可注册，则称为朴素公钥模型(PPK model). 这些模型规范了多方数字签名的安全模型，同时也对签名以外的 CA 提出了一定的信任机制和要求. 多方数字签名属于离散对数或整数分解等难题之上的方案[4-6]，基于2个数学难题的多方签名协议，Lin 等[7]提出了基于广义的圆锥曲线方案. 该方案声称其安全性同时基于离散对数和整数分解2个难题之上. 而文献[7]提出的多方数字签名的安全性存在缺陷，既使采用任意一种公钥注册模型，1个注册用户仍然可以从1个已知的多方消息签名对，伪造任意消息的多方签名. 如果没有采用任何的公钥注册模型，则攻击者可以注册1个新的公钥，从而能伪造任意组的任意消息的签名.

2 广义圆锥曲线的基础知识

设 Z_n 是一个模 n 的剩余类环，环 Z_n 上的广义圆锥曲线是同余方程 $y^2 \equiv ax^2 - bx - cxy$ 在 Z_n 上的解 (x,y) 的集，记为 $R_n(a,b,c)$，这里 $n=pq$，p,q 为2个不同的奇素数，且 $p+1=2r$，$q+1=2s$，其中 r 和 s 均为

收稿日期：2009-12-10.
基金项目：国家自然科学基金项目资助(60703004，60873217)、教育部博士点基金项目资助(20070269005)
作者简介：丁 丽(1978—)，女，安徽濉溪人，高级工程师.

素数，$(a,n)=(b,n)=1$，即 a,b 同 n 互素. 选择一曲线 $R_n(a,b,c)$，满足 $\left(\frac{c^2+4a}{p}\right)=\left(\frac{c^2+4a}{q}\right)=-1$，即满足 x^2+cx-a 在 F_p 和 F_q 上不可约(其实，还可选择其值分别为 ±1 的另外 3 种组合)，因此，有 $|R_n(a,b,c)|=(p+1)(q+1)$. 进一步得

$$N_n=lcm\{|R_p(a,b,c)|,|R_q(a,b,c)|\}=\{p+1,q+1\}=2rs.$$

找到圆锥曲线 $R_n(a,b,c)$ 的 1 个阶为 N_n 的点 G(及生成的 Abel 群)，运算定义及性质见文献[7]. 给定 $G,Q=dG(\mathrm{mod}n)$，求 d 的问题. 必须同时解决整数分解和离散对数 2 种难题[7].

3　Lin-Wang-Li 多方签名方案

3.1　系统参数生成过程

生成圆锥曲线 $R_n(a,b,c)$，这里 $n=pq,p,q$ 为 2 个不同的奇素数，且 $p+1=2r,q+1=2s$，其中 r 和 s 均为素数，$(a,n)=(b,n)=1$，即 a,b 同 n 互素. 则 $|R_n(a,b,c)|=(p+1)(q+1)$. 令 $G=(x,y)$，则

$$N_n=lcm\{|R_p(a,b,c)|,|R_q(a,b,c)|\}=\{p+1,q+1\}=2rs$$

的圆锥曲线上的一点.

$H(m)$ 为抗碰撞的 hash 函数 H 在消息 m 处的函数值.

假设有 k 个用户参与多方签名，每个用户 U_i 有 1 个私钥 d_i 和 1 个公钥 $Q=d_iG(\mathrm{mod}n)$，公开 n,G,Q_i，用户各自私密保存 d_i.

3.2　多方签名的产生过程

选取随机数 $k_i\in Z_{N_n}^*$，计算 $C_i=k_iG=(x_i,y_i)$，并广播 C_i，同时计算 $\delta_i=k_i-d_iH(m)(\mathrm{mod}N_n)$.

收集者收到每个签名人 U_i 的 (C_i,δ_i) 后，计算 $C=\sum_{i=1}^{k}C_i(\mathrm{mod}n)$ 和 $\delta=\sum_{i=1}^{k}\delta_i$，$(C,\delta)$ 即为最终多方签名.

3.3　多方签名的验证过程

计算 $Q=\sum_{i=1}^{k}Q_i(\mathrm{mod}n)$，验证 $C=\delta G\oplus H(m)Q$ 是否成立来确定签名是否有效.

4　Lin-Wang-Li 多方签名的安全分析

4.1　内部成员的攻击

设攻击者为 U_1，当他注册后由签名的产生过程的等式 $\delta_i=k_i-d_iH(m)(\mathrm{mod}N_n)$ 可知 U_1 是知道 N_n 的，否则 δ_i 无法计算. 下面给出分析的结果和攻击的过程.

结论 1　任意签名成员在得到一个消息 m(满足 $H(m)$ 为奇数)的最终多方签名 (C,δ) 后，可以在无需多方参与的条件下，产生任意消息 m' 的多方签名 (C',δ'). U_1 攻击过程为

1) 给定消息 m 的最终多方签名 (C,δ)，则

$$C=\delta G+H(m)Q,$$

$$Q=\sum_{i=1}^{k}Q_i=\sum_{i=1}^{k}d_iG,$$

由此 $\delta=\sum_{i=1}^{k}r_i-H(m)\sum_{i=1}^{k}d_i=l-H(m)\sum_{i=1}^{k}d_i$，其中 r_i 是随机数.

2) 不妨设 $H(m)=f$，这里 f 是奇数. 不是一般性，设 f 与 N_n 互素(如果不互素将导致 n 的分解)，则计

算 g 使得 $f \cdot g = 1 (\mathrm{mod} N_n)$.

3）对任意消息 m'，计算他的 $H(m')$，则 $H(m') = (H(m')g)H(m) = tH(m) (\mathrm{mod} N_n)$. 则 $\delta' = t\delta = tl - tH(m) \sum_{i=1}^{k} d_i = tl - H(m') \sum_{i=1}^{k} d_i$.

4）同时计算 $C' = tC$，则 (C', δ') 为消息 m' 一个有效的多方签名.

4.2 流氓密钥攻击

结论 2 任意攻击者可以注册一个新的公钥后，可以伪造其余人参与的多方签名. 攻击过程为

1）攻击者首先注册公钥 $Q_0 = xG - \sum_{i=1}^{k} Q_i$，则

$$xG = \sum_{i=1}^{k} Q_i \oplus Q_0;$$

2）对任意消息 m 的最终多方签名 (C, δ) 有

$$\delta = l - xH(m),$$

$$C = (l + xH(m))G$$

其中 l 为随机数.

可以验证 (C, δ) 为有效的多方签名，由

$$C = \delta G \oplus xH(m)G = \delta G \oplus H(m)Q = \delta G \oplus \sum_{i=1}^{k} Q_i \oplus Q_0$$

5 广义圆锥曲线多方签名的产生

1）选取随机数 $k_i \in Z_{N_n}^*$，计算 $C_i = k_i G = (x_i, y_i)$，并广播 $H(C_i, 0)$，

2）收到其他人的 $H(C_j, 0) (j \neq i)$ 后，广播 C_i，验证其对应的 hash 函数值.

3）计算 $C = \sum_{i=1}^{k} C_i (\mathrm{mod}\ n)$ 和

$$\delta_i = k_i - d_i H(Q_i \| Q_1, \cdots, Q_k \| C \| m) (\mathrm{mod}\ N_n).$$

4）收到每个签名人 U_i 的 δ_i 后，计算 $\delta = \sum_{i=1}^{k} \delta_i$，发送 (C, δ) 为消息 m 的最终多方签名给签名验证者.

多方签名的验证过程 首先计算 $e_i = H(Q_i \| Q_1, \cdots, Q_k \| C \| m)$，其次验证 $C = \delta G \oplus \sum_{i=1}^{k} e_i Q_i$ 是否成立，以此确定签名是否有效.

6 讨论及应用

6.1 效率分析

在表 1 中，将本文所设计的多方签名与已有的几种多方签名在签名效率、验证效率和签名长度等方面进行比较. 在运算效率方面，exp 表示 1 次指数运算，multi-exp 表示 1 次多指数运算，在进行一些预计算后，多指数运算能与 1 次指数运算具备几乎相同的效率. 方案中的 exp 是圆锥曲线上的数乘运算，与一般的模幂指数运算速度相当. 在签名长度方面，方案的签名 (C, δ) 中，$C = (x, y)$ 为圆锥曲线上的点，可以用 $\frac{y}{x} \in Z_n$ 来表示，长度与 $|N|$ 大致相同. 而 δ 的长度为 $|Nn|$，小于 $|N|$ 的长度.

因此，方案中多方签名的长度为 $1|N| + 1|Nn|$，小于 BN 方案和 HRL 方案的签名长度 $2|N|$.

表 1　几种多方签名方案的比较

Table 1　Comparison of several multi-signature schemes

方案	签名效率	验证效率	签名长度
BN 方案[10]	2 exp	1 multi-exp	$2\|N\|$
HRL 方案[11]	2 exp	1 multi-exp	$2\|N\|$
本文方案	1 exp + 1mul	1 multi-exp	$1\|N\| + 1\|Nn\| < 2\|N\|$

6.2　方案的应用

基于 Lin-Wang-Li 多方签名方案[7]，设计出一种高效的安全的多方签名方案，多方签名的长度与单个普通的签名长度基本相同，不随参与多方签名人数的增加而增加. 可以明显减少通信中的比特数，从而能节约电能，增加电池使用寿命. 该多签名算法可以运用到无线设备如 PDA、手机、RFID 芯片和传感器网络中，同样，该算法也适用于在某些通讯信号不稳定的场合.

参考文献：

[1] ITAKURA K，NAKAMURA K. A public key cryptosystem suitable for digital multisignatures[J]. NEC Research and Development，1983，71：1-8.

[2] BOYD C. Digital Multisignatures[C]//Cryptography and Coding. Oxford：Oxford University Press，1989：241-246.

[3] OKAMOTO T. A digital multisignature scheme using bijective public-key cryptosystems[J]. ACM Trans Comput Syst，1988，6(4)：432-441.

[4] MICALI S，OHTA K，REYZIN L. Accountable-subgroup multisignatures[C]//Proceedings of the 8th ACM conference on Computer and Communications Security (ACM CCS 2001)，New York：ACM Press，2001：245-254.

[5] RISTENPART T，YILEK S. The power of proofs-of-possession：Securing multiparty signatures against rogue-key attacks[C]//Advances in Cryptology-EUROCRYPT 2007，LNCS 4515，Heidelberg：Springer，2007：228-245.

[6] BELLARE M，NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[C]//Proceedings of the 13th ACM conference on Computer and communications security (ACM CCS 2006)，New York：ACM Press，2006：390-399.

[7] LIN S，WANG B，LI Z J. Digital multisignature on the generalized conic curve over Zn[J]. Computers & Security，2009，28(1-2)：100-104.

[8] 张明志. 用圆锥曲线分解整数[J]. 四川大学：自然科学版，1996，33(4)：356-359.
ZHANG Ming-zhi. Factoring Integers with Conics[J]. Journal of Sichuan University：Natural Science Edition，1996，33(4)：356-359.（in Chinese）

[9] 曹珍富. 基于有限域 F_p 上圆锥曲线的公钥密码系统[C]//密码学进展—Chinacypt'98，北京：科学出版社，1998：45-49.
CAO Zhen-fu. A public key cryptosystem based on a conic over finite fields[C]//Advances in cryptology-CHINACRYPT'98，Beijing：Sci. Press，1998：45-49.（in Chinese）

[10] BELLARE M，NEVEN G. Identity-Based Multi-signatures from RSA[C]//Topics in Cryptology-CT-RSA 2007，LNCS 4377，Heidelberg：Springer，2007：145-162.

[11] HARN L，REN J，LIN C L. Efficient identity-based GQ multisignatures[J]. International Journal of Information Security，2009，8(3)：205-210.

Security Analysis and Improvement of Digital Multi-signature on the Generalized Conic Curve

DING Li[1,2], ZHOU Yuan[1,2], QIAN Hai-feng[2]

(1. National Computer Network Emergency Response technical Team/Coordination Center of China, Beijing 100029, China;
2. Department of Computer, East China Normal University, Department of Computer Science and Technology, Shanghai, 200241, China)

Abstract: In this paper we present the security analysis on a multi-signature scheme based on the generalized conic curve (Lin-Wang-Li protocol) is presented, which exist the severe forgery problems. The security of the scheme is not based on any difficult issues such as the discrete logarithms on the generalized conic curve or the hardness of integer factoring. An adversary can forge the signature without solving any hard problems. In order to solve the existing problems, we improve the scheme is improved and a present our multi-signature scheme on the generalized conic curve is presented.

Key words: multi-signature protocol; generalized conic curve; discrete logarithms; forgery attacks; digital signature

(责任编辑 张士瑛)

(上接第 645 页)

The Fast Implementation of MD6 on GPU

LI Li-xin[1], YE Jian[1], YU Yang[1]

(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract: Secure Hash Algorithm (SHA) is an important tool in practice of cryptography such as digital signature, and it has been widely applied in electronic business etc. the information security fields, etc. MD6 is one of the several candidates for the SHA-3 competition. How to implement MD6 efficiently is an urgent question to be answered. This paper presents a parallel analysis of MD6, and a fast realization on GPU platform, so as to provide an easy way to implementing SHA quickly and efficiently.

Key words: GPU; SHA algorithm; MD6 algorithm; TBB; CUDA

(责任编辑 张士瑛)