第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0155—03 文献标识码：A 中图分类号：TP309

基于椭圆曲线的匿名代理签名方案

汪 翔，陈 凯，鲍皖苏
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：Shum-Wei 匿名代理签名方案存在原始人伪造攻击，且由于基于离散对数问题构造，实现效率不高。该文基于椭圆曲线公钥密码体制(ECC)构造了一个新的匿名代理签名方案，对新方案的各项基本性质进行具体分析。结果表明，新方案具有强不可伪造性，安全性高，实现速度快，具有较好的实际应用前景。

关键词：椭圆曲线；匿名代理签名；强不可伪造性

Anonymous Proxy Signature Scheme Based on Elliptic Curve

WANG Xiang, CHEN Kai, BAO Wan-su
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】Because Shum-Wei anonymous proxy signature scheme has weakness of original signers forge attack and low implementation efficiency of the construction of discrete logarithm problem, this paper proposes a new anonymous proxy signature scheme based on ECC, and analyzes the essential security characters it has. It shows that the new scheme has the quality of high security and high efficiency of implementation.

【Key words】elliptic curve; anonymous proxy signature; strong enforceability

1 概述

代理签名是文献[1]提出的一种特殊的数字签名。其主要思想为当原始签名人因为某些原因不能签名时，将他的数字签名权力委托给代理签名人，代理签名人代表原始签名人生成数字签名。这种方案在实际中得到了广泛的应用。2001年，文献[2]提出了强代理签名的概念，其具有以下性质：

(1)可验证性。验证人可从代理签名中相信原始签名人认同了这份签名消息。

(2)强不可伪造性。除了代理签名人，任何人包括原始签名人都不能产生有效的代理签名。

(3)强不可否认性。代理签名人不能向任何人否认他所签过的有效代理签名。

(4)强可识别性。任何人都能从代理签名中确定代理签名人的身份。

(5)防止滥用。确保代理签名密钥对不能被用于其他目的。代理签名者的责任应当被具体确定。

在此基础上，文献[3]提出了LKK方案，成为很多代理签名方案设计的基本模型。但在LKK方案中，任何人都可以从一个代理签名中确定代理签名人的身份，这一点对代理签名人是不公平的，因为有时候代理签名人不希望别人完全了解他签过哪些消息。为了解决这个问题，文献[4]提出了代理签名人身份保密的强代理签名方案，称为Shum-Wei方案。2005年，谷利泽等提出了匿名代理签名的概念，提出将代理签名划分为匿名代理签名和公开代理签名的分类方法。而Shum-Wei方案及其之后的一系列代理签名人身份保密的强代理签名方案都是匿名代理签名方案。

Shum-Wei方案是一个需要可信任方的方案。这类匿名代理签名方案除了代理签名人和可信任方，任何人(包括原始签名人)都不能从代理签名中确定代理签名人的身份。但是该方案存在原始人伪造攻击，且该方案是基于离散对数问题构造的，因此，存在计算量大、密钥长以及实现效率低等缺陷。本文提出一种建立在椭圆曲线上的新匿名代理签名方案，其实现效率高，并可抵抗原方案中所存在的原始人伪造攻击。

2 Shum-Wei方案

Shum-Wei方案包括6个阶段：初始化，发送别名，授权，代理签名的生成，代理签名的验证过程和代理签名人身份公开，具体内容如下：

(1)初始化

p 和 q 为2个大素数且 $q|p-1$；Z_p^* 为素数域上的乘法群；g 是 Z_p^* 上的 q 阶本原元，$g\in Z_p^*$，且 $g^q\equiv 1 \bmod p$；A 为原始签名人，B 为代理签名人，V 为签名验证人，T 为可信的别名发送权威；A 的身份标识为 m_w，B 的身份标识为 ID_B；原始签名人私钥为 x_A，$x_A\in Z_p^*$，公钥为 y_A，$y_A=g^{x_A} \bmod p$；代理签名人私钥为 x_B，$x_B\in Z_p^*$，公钥为 y_B，$y_B=g^{x_B} \bmod p$；可信任方 T 的私钥为 x_T，$x_T\in Z_p^*$，公钥为 R_A，$y_T=g^{x_T} \bmod p$；$h()$ 为安全的单向hash函数；m_w 为 A 给 B 的授权书；m 为要签名的消息；$sign()$ 为签名算法；$verify()$ 为验证算法。

(2)发送别名

B 发送身份标识 ID_B 给 T。

T 随机选取 $k_B,k_T\in Z_p^*$，计算

$$h_B=h(k_B,ID_B)$$

$$r_T=g^{k_T} \bmod p$$

$$s_T=x_T h(h_B,r_T)+k_T \bmod q$$

T 发送别名 h_B 给 B，连同对 h_B 的数字签名 (r_T,s_T) 来证明

作者简介：汪 翔(1979－)，男，讲师、在职博士研究生，主研方向：密码理论；陈 凯，硕士研究生；鲍皖苏，教授

收稿日期：2007-09-15 **E-mail：** dixonwx@163.com

别名的有效性，即发送 (h_B, r_T, s_T) 给 B。T 记录所有 3 个一组的 (h_B, k_B, ID_B)，用于以后揭示 B 的身份。

B 验证

$$g^{s_T} = y_T^{h(h_B, r_T)} r_T \bmod p$$

若等式成立，则 B 承认别名有效。

(3)授权

A 随机选择 $k_A \in Z_q^*$，计算

$$r_A = g^{k_A} \bmod p$$

$$s_A = x_A h(m_w, r_A) + k_A \bmod q$$

A 发送 (m_w, r_A, s_A) 给 B。

B 验证

$$g^{s_A} = y_A^{h(m_w, r_A)} r_A \bmod p$$

若等式成立，则 B 承认授权有效。

(4)代理签名的生成

B 计算 $x_p = s_T + s_A \bmod q$ 作为代理签名秘密密钥，对消息 m 生成普通的数字签名 $\sigma = sign(x_p, m)$。则代理签名为 $(m, \sigma, m_w, ID_B, h_B, r_T, r_A)$。

(5)代理签名的验证

V 先验证 m 适合于 m_w，再计算代理签名公开密钥

$$y_P = y_A^{h(m_w, r_A)} r_A y_T^{h(h_B, r_T)} r_T \bmod p$$

验证

$$verify(m, \sigma, y_P) = \text{true}$$

若成立，则签名有效。

(6)代理签名人身份公开

在需要的时候，T 可以公开代理签名人 B 的身份信息，方法如下：

V 发送 h_B 给 T，T 收到后发送对应的 (k_B, ID_B) 给 V，V 验证 $h_B = h(k_B, ID_B)$ 是否成立，若成立，则 ID_B 对应的 B 即为签名的代理签名人。

该匿名代理签名方案一经提出就受到广泛关注，许多学者都对该方案进行了分析。其中，文献[5-6]指出 Shum-Wei 方案不具有强不可伪造性，即原始签名人可以伪造代理签名，并分别给出了对该方案的原始签名人伪造攻击方法。这说明该方案并不完善，并且由于其是利用离散对数问题构造的，因此也存在实现效率不高的缺陷。针对这些缺陷，本文给出了一种基于椭圆曲线的新方案。

3 基于椭圆曲线的匿名代理签名方案

3.1 具体方案

方案包括 6 个阶段：初始化，发送别名，授权，代理签名的生成，代理签名的验证和代理签名人身份公开，具体内容如下：

(1)初始化

设 F_q 是一 q 元有限域，E 是定义在 F_q 上的一条椭圆曲线，设 $G \in E(F_q)$，G 的阶 n 是一个大素数，则可用加法群 $<G>$ 来构造公钥密码体制。A 为原始签名人，B 为代理签名人，V 为签名验证人，T 为可信的别名发送权威；B 的身份标识为 ID_B；设 A 的私钥为 d_A，$1 \le d_A \le n-1$；公钥为 Q_A，$Q_A = d_A G$；B 的私钥为 d_B，$1 \le d_B \le n-1$；公钥为 Q_B，$Q_B = d_B G$；可信任方 T 的私钥为 d_T，$1 \le d_T \le n-1$；公钥为 Q_T，$Q_T = d_T G$；$h()$ 为安全的单向 hash 函数；m_w 为 A 给 B 的授权书；m 为要签名的消息；$sign()$ 为签名算法(这里的签名算法可用 ECDSA)；$verify()$ 为验证算法。

(2)发送别名

B 发送身份标识 ID_B 给 T。

T 随机选取 $1 \le k_B, k_T \le n-1$，计算

$$h_B = h(k_B, ID_B)$$

$$R_T = k_T G = (x_T, y_T)$$

$$s_T = d_T h(h_B, x_T) + k_T \bmod n$$

T 发送别名 h_B 给 B，连同对 h_B 的数字签名 (R_T, s_T) 来证明别名的有效性，即发送 (h_B, R_T, s_T) 给 B。T 记录所有 3 个一组的 (h_B, k_B, ID_B)，以备以后揭示 B 身份的需要。

B 验证

$$s_T G = h(h_B, x_T) Q_T + R_T$$

若等式成立，则 B 承认别名有效。

(3)授权

A 随机选择 $1 \le k_A \le n-1$，计算

$$R_A = k_A G = (x_A, y_A)$$

$$s_A = d_A h(m_w, x_A) + k_A \bmod n$$

A 发送 (m_w, R_A, s_A) 给 B。

B 验证

$$s_A G = h(m_w, x_A) Q_A + R_A$$

若等式成立，则 B 承认授权有效。

(4)代理签名的生成

B 计算 $d_P = x_A s_T + s_A \bmod n$ 作为代理签名秘密密钥，对消息 m 生成普通的数字签名 $\sigma = sign(d_P, m)$。则代理签名为 $(m, \sigma, m_w, h_B, R_T, R_A)$。

(5)代理签名的验证

V 先验证 m 适合于 m_w，再计算代理签名公开密钥

$$Q_P = x_A h(h_B, x_T) Q_T + x_A R_T + h(m_w, x_A) Q_A + R_A$$

验证 $verify(m, \sigma, Q_P) = \text{true}$ 是否成立。

(6)代理签名人身份公开

需要的时候，T 可以公开代理签名人 B 的身份信息，方法如下：

V 发送 h_B 给 T，T 收到后发送对应的 (k_B, ID_B) 给 V，V 验证 $h_B = h(k_B, ID_B)$ 是否成立。若成立，则 ID_B 对应的 B 即为签名的代理签名人。

3.2 安全性分析

根据匿名代理签名方案，应从 6 个方面满足对该方案进行分析：

(1)可验证性

若被签名消息 m 适合 m_w，则验证人 V 可以确定代理签名是经 A 授权的。

(2)强不可伪造性

伪造攻击是针对代理签名秘密密钥 d_P 的构造进行的。该方案中 d_P 一部分来源于 A，一部分来源于 T 并捆绑了来源于 A 的参数。只有 B 能计算代理签名密钥，即只有 B 可以为 A 生成有效的代理签名，其他人不能生成有效的代理签名。

采用类似文献[3]中的原始签名人伪造攻击方法对该方案进行安全性分析，若该攻击方法成立，原始签名人 A 就可以计算一个新的 $R_A' = (x_A', y_A')$，使得 $d_P' = x_A h(m_w, x_A') \bmod n$ 成为有效的代理签名秘密密钥，而验证方 V 计算代理签名公开密钥应得到

$$Q_P^{'} = x_A^{'}h(h_B, x_T)Q_T + x_A^{'}R_T + h(m_w, x_A^{'})Q_A + R_A^{'}$$

即必须满足 $x_A^{'}R_T + h(m_w, x_A^{'})Q_A + R_A^{'} = O$。

而求得 $R_A^{'} = (x_A^{'}, y_A^{'})$ 使得 $x_A^{'}R_T + h(m_w, x_A^{'})Q_A + R_A^{'} = O$ 是一个难解问题，所以，原始签名人伪造攻击不可行，即 A 也不能生成有效的代理签名。

因此，除了代理签名人，任何人都不能产生有效的代理签名，新方案满足强不可伪造性。

(3)防止滥用

1)防止代理权的转移。原始签名人 A 对代理签名人 B 的代理授权信息是 (m_w, R_A, s_A)，(R_A, s_A) 是 A 对 m_w 的签名，所以，R_A, s_A, m_w 都是不可更改的；可信任方 T 发送给代理签名人 B 的别名信息是 (h_B, R_T, s_T)，(R_T, s_T) 是 A 对 h_B 的签名，一旦 B 接受 A 的授权，R_T, s_T, h_B 都是不可更改的。代理公钥为

$$Q_P = x_A h(h_B, x_T)Q_T + x_A R_T + h(m_w, x_A)Q_A + R_A$$

即一旦代理签名人 B 接受了原始签名人 A 的授权，Q_P 就已经确定，除非 B 把 d_P 给他自己的代理签名人，否则 B 不能利用 (m_w, R_A, s_A) 再次代理授权。

2)防止代理签名者越权。代理签名验证过程的第(1)步就是验证消息 m 是否符合代理授权书 m_w，如果不符合则签名无效，A 可以充分利用代理授权书 m_w 有效约束 B 的代理权限范围。

(4)匿名性

由于 h_B 是无法得到 ID_B 的，除了代理签名人 B 和可信任方 T，任何人都无法从代理签名中确定代理签名人的身份。

(5)可跟踪性

T 在需要时可公开代理签名人的身份，因此，满足可跟踪性。

(6)强不可否认性

由于只有 B 能生成有效的代理签名，因此 B 不能对任何人否认他签过的代理签名。

综上可知，新方案能够满足匿名代理签名方案设计的6条安全性质要求。

4 结束语

本文针对一典型的需要可信任方的匿名代理签名方案——Shum-Wei 方案进行了分析，发现该方案不能抵抗原始人伪造攻击。在此基础上，基于椭圆曲线公钥密码体制，给出一个新的匿名代理签名方案。新方案不仅具有更高的安全性，而且还具有较高的实现效率和实用性。

参考文献

[1] Mambo M, Usuda K, Okamoto E. Proxy Signature: Delegation of the Power to Sign Messages[J]. IEICE Transactions on Fundamentals, 1996, E79-A(9): 1338-1353.

[2] Byoungcheon Lee, Heesun Kim, Kwangjo Kim. Strong Proxy Signature and Its Applications[Z]. (2001-01-02). caislab.icu.ac.kr/~sultan/pub.

[3] Lee J Y, Cheon J H, Kim S. An Analysis of Proxy Signatures: Is a Secure Channel Necessary?[C]//Proc. of CT-RSA'03. [S. l.]: Springer-Verlag, 2003: 68-79.

[4] Shum K. A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection[C]//Proc. of the 11th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. Pittsburgh, Pennsylvania, USA: [s. n.], 2002: 55-56.

[5] Sun Hung-Min, Hsieh B T. On the Security of Some Proxy Signature Schemes[Z]. (2007-09-20). http://www.eprint.iacr.org.

[6] Lee Narn Yih, Lee Ming Feng. The Security of a Strong Proxy Signature Scheme with Proxy Signer Privacy Protection[J]. Applied Mathematics and Computation, 2005, 161(3): 807-812.

（上接第 154 页）

随机数发生器产生一个位置的复杂度。仿真运行环境是 Windows XP 系统，P4 2.8 GHz CPU，512 MB DDR 内存，运用 FPGA 仿真实验结果如图 2 所示。从表 1 可以看出，硬件与 Matlab 攻击比较，其最突出的优势就是缩短了攻击时间，这对于攻击而言无疑是很重要的优点。

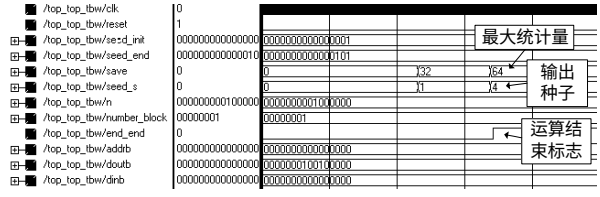

图 2 FPGA 攻击仿真时序图

表 1 攻击时间对照表

参数(消息长度)/bit	估计复杂度	应用 Matlab (时间)/min	应用 FPGA (时间)/min
10	$10^7 \cdot O_p$	<1	<1
500	$2.5\times10^{10} \cdot O_p$	≈ 40	≈ 1
2 000	$4\times10^{11} \cdot O_p$	≈ 900	≈ 5

通过表 1 还可以看出在消息长度非常小的情况下，软件攻击和硬件攻击几乎不存在差别，至少从感官上差别很小；随着消息长度的增加，软件的局限性就突显出来了，越复杂的攻击，消耗的时间越长，而硬件实现差别就很小，突出了其优点。

5 结束语

本文通过对 F5 密钥攻击理论和攻击复杂度的分析，提出一种利用硬件 FPGA 实现密钥攻击的方案。硬件方案中的每个模块都有其独特的作用，最重要的运算器模块完成所有的计算功能，通过比较输出统计量中最大的值，并且把产生该数据的种子认定为正确密钥，从而实现攻击。实验证明，此方法可以缩短攻击时间，大大提高攻击效率。

参考文献

[1] 张雪峰, 范九伦. 基于图像融合的数字图像隐藏技术[J]. 微电子与计算机, 2007, 24(2): 202-205.

[2] Fridrich J, Goljan M, Hogea D. Steganalysis of JPEG Images: Breaking the F5 Algorithm[C]//Proc. of the 5th International Workshop on Information Hiding. Noordwijkerhout, Netherlands: [s. n.], 2002: 310-323.

[3] Fridrich J, Goljan M, Soukal D. Searching for the Stego Key[C]//Proc. of the SPIE'04. San Jose, CA, USA: [s. n.], 2004: 70-82.

[4] Sun Kang, Pan Xuezeng, Wang Jimin, et al. Hardware Based Steganalysis[EB/OL]. (2007-06-22). http://www.u-bourgogne.fr/SITIS/06/Proceedings/SIT/f37.pdf.