基于椭圆曲线的不需要可信方的匿名代理签名方案

靳 虹[1] 王相海[1,2]
(辽宁师范大学计算机与信息技术学院 大连 116081)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[2]

摘 要 对Gu方案进行密码学分析,发现该方案不具有强不可伪造性,且由于基于离散对数问题,实现效率不高,数据冗余量大。基于椭圆曲线公钥密码体制(ECC)构造了一个新的不需要可信方的匿名代理签名方案,并对新方案的各项基本性质进行了具体分析。新方案具有强不可伪造性,且签名结果不含冗余数据,安全性高,实现速度快,具有更好的实际应用前景。

关键词 椭圆曲线,代理签名,匿名性,强不可伪造性,冗余数据
中图法分类号 TP309 **文献标识码** A

Anonymous Proxy Signature Scheme without Trusted Party Based on Elliptic Curve

JIN Hong[1] WANG Xiang-hai[1,2]
(Department of Computer Science, Liaoning Normal University, Dalian 116081, China)[1]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]

Abstract It is found that the Gu scheme has not got the property of strong unforgeability and low implementation efficiency and redundant data of the construction of discrete logarithm problem. This paper proposed a new anonymous proxy signature scheme without trusted party based on ECC, and analyzed the essential security characters it has. It shows that the new scheme can keep the property of the unforgeability and does not have the redundant data in signature. It also has the quality of high security and high efficiency of implementation.

Keywords Elliptic curve, Proxy signature, Anonymity, Strong unforgeability, Redundant data

1 引言

数字签名的概念是Diffie和Hellman[1]于1976年首先提出的。随着计算机和网络通信技术的发展,数字签名技术在保证信息完整性、不可否认性、不可伪造性等方面得到了广泛的应用。数字签名根据其不同用途可分为盲签名、多重签名以及代理签名等。其中,代理签名主要应用于将签名权委托给其他人,使其代表自己在一些场合中签名。1996年Mambo[2]等人提出了代理签名的概念,根据代理权限的不同,对代理签名进行了分类,主要有以下几种类型:(1)完全代理签名,即原始签名人在安全信道下直接把自己的私钥发送给代理签名人,他们的签名完全相同,这就不可避免地产生签名滥用。而且,完全代理签名也不具有可识别性和不可否认性。在这种情况下,原始签名人在经过一次代理授权后不得不修改他的签名私钥,因此这种完全代理签名不适合商业用途。(2)部分代理签名,在该方案中,原始签名人使用自己的私钥,产生一个代理签名私钥,并把代理签名私钥在安全信道下传给代理签名人。此时,代理签名人的代理签名和原始签名人的签名可以区分开来。出于安全考虑,要求用代理签名私钥不能求出原始签名人私钥。

在文献[4]中,Lee等人按代理签名的特点将代理签名分为强代理签名和弱代理签名。强代理签名表示原始签名人将自己的签名权交给代理签名人后,原始签名人不能生成同样的签名,且代理人不能向包括原始签名人在内的任何人否认自己生成的签名。弱代理签名则表示原始签名人与代理签名人的身份界限不清晰,二者能够产生相互否认、相互抵赖的现象。满足如下强代理签名[3]的安全性要求,才能确保代理签名体制的安全性。

(1)强不可否认性。代理签名人不能否认代替原始签名人产生的任何代理签名。

(2)强不可伪造性。除代理签名人外,其余包括原始签名人在内的未经授权的任何人都无法产生合法有效的代理签名。

(3)强可鉴别性。任何人都可以由某个代理签名鉴别出相应的代理签名人。

(4)可验证性。任何人对某一代理签名都可以进行验证,并得知该签名是否经过授权或是否合法。

(5)防止滥用。授权证书限定了代理签名人的代理密钥使用范围、期限以及其他情况,严格限制了代理签名人签名权限的滥用。

到稿日期:2008-12-25 返修日期:2009-05-15
靳 虹(1983-),女,硕士研究生,主要研究方向为信息安全与数字签名,E-mail:deepbule0610@126.com;王相海(1965-),男,博士,教授,主要研究方向为计算机图形学及多媒体信息处理。

在众多的代理签名方案中，有些方案结合某些特殊功能，扩大了代理签名的使用范围；有些方案提高了计算速度，提高了签名效率；有些方案则提高了整个体系的安全性能；而大多数方案都无法完全满足强代理签名的上述几点要求。2002年，Shum和Wei提出的匿名代理签名方案[5]在实际生活中得到了广泛的应用。2005年，谷利泽等人也在Shum-Wei方案的基础上提出了一个不需要可信任方的匿名代理签名方案[6]，并改进、设计了新的匿名代理签名方案[7]，以下简称Gu方案。柳菊霞等人[8]2006年指出Gu方案是不安全的，并提出了改进的方案。

本文通过分析Gu方案的安全性，指出它存在两个缺陷，即原始签名人可对代理签名进行伪造攻击和原方案中存在少量冗余数据[9]。改进并设计了一个建立在椭圆曲线上的不需要可信方的匿名代理签名方案。通过验证，该方案的签名结果不含冗余数据且方案具有强不可伪造性，使系统整体具有实现速度快、安全性高的特点。

2 Gu方案描述及分析

2.1 Gu方案[7]

2.1.1 授权并产生代理签名人别名

A将授权证书m_w通过安全信道发送给B。B检验m_w，若符合自己的要求，则任意选择两个数$k_B, k_1 \in z_q^*$，计算$r_B = g^{k_B} \bmod p$，$r_1 = g^{k_1} \bmod p$和$s_1 = x_B h(r_B, ID_B, r_1) + k_1 \bmod q$，将$(r_B, ID_B, r_1, s_1)$返还给$A$。$A$通过验证$g^{s_1} = y_B^{h(r_B, ID_B, r_1)} r_1 \bmod q$是否成立，来选择是否接受$(r_B, y_B, ID_B)$。若接受则计算$Y_p = y_B r_B^{r_B} \bmod p$，将$Y_p$写入$m_w$中，即生成了$B$的身份标志$Y_p$。

2.1.2 发送新的授权证书(含代理签名人B的身份标志)

A选择$k_A \in z_q^*$计算$r_A = g^{k_A} \bmod p$，$s_A = x_A h(m_w, r_A) + k_A \bmod q$，即对新的授权证书$m_w$进行数字签名。通过安全信道将$(r_A, s_A)$和新的$m_w$发送给$B$。$B$通过验证$g^{s_A} = y_A^{h(m_w, r_A)} r_A \bmod q$是否成立，选择是否接受$A$的信息，成立则接受并秘密保存$(r_A, s_A, m_w, s_B)$。

2.1.3 生成代理签名

B计算代理签名私钥：$x_p = s_A + s_B \bmod q$，用基于离散对数的数字签名算法对消息m生成普通的数字签名$\sigma = \mathrm{sign}(x_p, m)$，得到代理签名为$(m, \sigma, m_w, r_A, y_A)$。

2.1.4 验证代理签名

验证人V先验证消息m是否符合授权证书m_w。若符合，则从m_w中取得B的身份标志Y_p，计算代理签名公钥$y_P = y_A^{h(m_w, r_A)} r_A Y_p \bmod p$，并验证$\mathrm{Verify}(y_p, \sigma, m) = True(\ )$是否成立。成立，则代理签名有效。

2.1.5 必要时揭示代理签名人身份

验证人V向原始签名人A出示代理签名$(m, \sigma, m_w, r_A, y_A)$。$A$先验证消息$m$是否符合授权证书$m_w$。若签名有效，取出在授权并产生代理签名人别名阶段保存的(r_B, y_B, ID_B)，利用从授权证书m_w中取得的B的身份标识Y_p判断等式$Y_p = y_B r_B^{r_B} \bmod p$是否成立。如果存在$(r_B, y_B, ID_B)$满足等式，则$ID_B$对应的签名人是生成签名$(m, \sigma, m_w, r_A, y_A)$的代理签名人。

2.2 安全性分析

在文献[7]中，作者认为原始签名人A无法获得代理签名人B的私钥x_B和k_B，因$s_B = s_B + k_B r_B \bmod q$，故$A$无法得到$s_B$，从而无法计算$x_p$，因此$A$不可能伪造$B$生成代理签名，因而该方案具有强不可伪造性。但通过如下证明得知，该方案存在原始签名人伪造攻击，不具有强不可伪造性。

在授权并产生代理签名人别名的阶段，A在确认B接受授权，得到B的身份信息后，选择一随机数r_B'，计算$Y_p' = y_B (r_B')^{r_B'} \bmod p$，将$Y_p'$写入伪造的授权书$m_w'$中。$A$计算$r_A' = (Y_p')^{-1} \bmod p$，再计算$x_p' = x_A h(m_w, r'_A) \bmod q$，将其作为代理签名私钥，用$x'_p$对消息$m$进行离散对数的数字签名$\sigma' = \mathrm{sign}(m, x_p')$，从而得到伪造的代理签名为$(m, \sigma', m_w', r_A', y_A)$。

证明：

$$y_p' = y_A^{h(m_w, r_A')} r_A' Y_p' \bmod p = g^{x_A h(m_w, r_A')} (Y_p')^{-1} Y_p' \bmod p = g^{x_A h(m_w, r_A')} \bmod p = g^{x_p'} \bmod p$$

所以该方案不具有强不可伪造性，是不安全的。

另外，根据刘木兰等人对数字签名中冗余数据的分析方法[9]，在授权并产生代理签名人别名生成阶段中A保存了B的身份信息：公钥y_B以及代理签名结果中的公钥y_A属于冗余数据，可以去掉。

3 基于椭圆曲线的不需要可信方的匿名代理签名方案

3.1 具体方案

该方案设计6个阶段，包括初始化、授权并产生代理签名人别名、发送新的授权证书(含代理签名人B身份标志)、生成代理签名、验证代理签名、必要时揭示代理签名人身份。具体内容如下。

(1)初始化

设F_q是一个q阶有限域，E是定义在F_q上的一条椭圆曲线，令$G \in E(F_q)$，G是一阶为n的加法群，其中n是大素数，则可用$\langle G \rangle$来构造公钥加密体制。其中，A为原始签名人，B为代理签名人，V为签名验证人。A的身份标识为ID_A，B的身份标识为ID_B。设A的私钥为d_A，其中$1 \leqslant d_A \leqslant n-1$，公钥为$Q_A$，$Q_A = d_A G$。同样地，$B$的私钥为$d_B$，其中$1 \leqslant d_B \leqslant n-1$，公钥为$Q_B$，$Q_B = d_B G$。$h()$为安全的单向散列函数，$m_w$为$A$给$B$的授权证书。

(2)授权并产生代理签名人别名

A将授权证书m_w通过安全信道发送给B。B检验m_w，若符合自己的要求，则任意选择两个数$1 \leqslant k_B, k_1 \leqslant n-1$，计算$r_B = k_B G$，$r_1 = k_1 G$，$s_B = d_B + k_B r_B \bmod n$，$s_1 = d_B h(r_B, ID_B, r_1) + k_1 \bmod n$，将$(r_B, ID_B, r_1, s_1)$返还给$A$。$A$通过验证$s_1 G = Q_B h(r_B, ID_B, r_1) + r_1$是否成立，选择是否接受$(r_B, ID_B)$。若接受，则计算$Y_p = r_B^2 + Q_B \bmod n$，将$Y_p$写入$m_w$中，即生成了$B$的身份标志$Y_p$。

(3)发送新的授权证书(含代理签名人B的身份标志)

A选择$1 \leqslant k_A \leqslant n-1$，计算$r_A = k_A G \bmod n$，$s_A = d_A h(m_w, r_A) + k_A \bmod n$，即对新的授权证书$m_w$进行数字签名。通过安全信道将$(r_A, s_A)$和新的$m_w$发送给$B$。$B$通过验证$s_A G = Q_A h(m_w, r_A) + r_A \bmod n$是否成立，选择是否接受$A$的信息。若成立，则接受并秘密保存$(r_A, s_A, m_w, s_B)$。

(4) 生成代理签名

B计算代理签名私钥$x_p = s_A + r_A s_B \bmod n$，用基于椭圆

曲线离散对数的数字签名算法对消息 m 生成普通的数字签名 $\sigma=\mathrm{sign}(x_p,m)$，得到代理签名为 (m,σ,m_w,r_A)。

(5)验证代理签名

验证人 V 先验证消息 m 是否符合授权证书 m_w。若符合，则从 m_w 中取得 B 的身份标志 Y_p，计算代理签名公钥 $y_P=Q_Ah(m_w,r_A)+r_A+r_AY_p \bmod n$，并验证 $\mathrm{Verify}(y_p,\sigma,m)=True(\ )$ 是否成立。若成立，则代理签名有效。

(6)必要时揭示代理签名人身份

验证人 V 向原始签名人 A 出示代理签名 (m,σ,m_w,r_A)。A 先验证消息 m 是否符合授权证书 m_w。若签名有效，再取出在授权并产生代理签名人别名阶段保存的 (r_B,ID_B)，利用从授权证书 m_w 中取得的 B 的身份标识 Y_p 判断等式 $Y_p=r_B^2+Q_B \bmod n$ 是否成立。如果存在 (r_B,ID_B) 满足等式，则 ID_B 对应的签名人是生成代理签名 (m,σ,m_w,r_A) 的代理签名人。

3.2 安全性分析

从以下 6 个代理签名应满足的特性对方案进行分析。

(1)强不可伪造性（即除代理签名人外，其他任何人无法伪造合法签名）

这里，仍然利用原始签名人 A 的伪造攻击方法对本文提出的方案进行安全性分析。原始签名人 A 首先伪造一个 Y_p'，并把它写入到授权证书 m_w'。然后，就可以计算出来一个新的 r_A'，并且由它计算出 $x_p'=d_Ah(m_w',r_A') \bmod n$，使得 x'_p 作为有效的代理签名私钥，验证方 V 所计算出来的代理签名公钥为 $y_p'=Q_Ah(m_w',r_A')+r_A'+r_A'Y_p' \bmod n$ 显然，如果此式能够成立，则必须使得 $r_A'+r_A'Y_p'=0 \bmod n$。然而，根据等式 $r_A'+r_A'Y_p'=0 \bmod n$ 求解满足条件的 r_A' 是一个数学难解问题，所以这种原始签名人伪造攻击方法并不可行。

显然，除了代理签名人 B 之外，其他任何人包括原始签名人在内都不能产生合法的代理签名，因此新方案满足强不可伪造性。

(2)强不可否认性（代理签名人不能否认自己的代理签名）

由上述强不可伪造性可知，只有代理签名人 B 能生成合法的代理签名，所以 B 不能对任何人否认自己的代理签名。

(3)防止滥用(授权证书限定了代理签名人的代理密钥使用范围、期限以及其他情况，严格限制了代理签名人签名权限的滥用)

1)有效地防止代理签名权转移的问题。新方案中，原始签名人 A 对代理签名人 B 的代理授权信息是一个三元组 (m_w,r_A,s_A)，原始签名人 A 对 m_w 的数字签名是 (r_A,s_A)，所以 m_w,r_A,s_A 都是不可更改的。代理公钥是 $y_P=Q_Ah(m_w,r_A)+r_A+r_AY_p \bmod n$。也就是说，只要代理签名人 B 同意并且接受了原始签名人 A 给他的授权，那么代理签名的公钥 y_p 实际上就已经给定了。可见，只要 B 不把 x_p 无条件给别的代理签名人，让其代理签名，他就不可能利用已有的三元组 (m_w,r_A,s_A) 对这个签名做再次代理授权。

2)有效地防止代理签名者的越权问题。

如果要验证代理签名的有效性，首先就要验证消息 m 是否能够符合公开的授权证书 m_w。如果符合，再做进一步的验证；如果不符合，则可以声明此签名无效。由此可见，原始签名人 A 能够利用授权证书 m_w 来有效地限制 B 的代理权限范围，解决代理签名人的越权问题。

(4)匿名性（不能从代理签名中确定代理签名人的身份）

因为代理签名人的身份 ID_B 对其他人是保密的，该身份标志生成后，(r_B,ID_B) 就被原始签名人 A 保存，其他人无法从单纯的代理签名中就确定出代理签名人 B 的身份。

(5)可验证性（证明代理签名人已经被原始签名人授权）

验证代理签名的有效性，首先就要验证消息 m 是否能够符合公开的授权证书 m_w。如果符合，验证人 V 就可以确定出该代理签名人的代理签名是经过原始签名人 A 授权的。

(6)可跟踪性（必要的时候可以公开代理签名人的身份）

在必要的时候，比如代理签名人否认自己的签名，那么验证人 V 就可以通过找到满足 $Y_p=r_B^2+r_AQ_B \bmod n$ 成立的 (r_B,ID_B) 来确认并公开代理签名人的身份。可见，新方案能够满足可跟踪性。

由此可以得出结论，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。

结束语 本文对一个典型的无可信中心的匿名代理签名方案——Gu 方案进行分析，发现该方案不具有强不可伪造性，即不能抵抗原始签名人伪造攻击，且原方案基于离散对数数学难题设计，安全性较低。针对以上问题，本文基于椭圆曲线公钥密码体制，设计了一个新的不需要可信方的匿名代理签名方案。新方案不仅能够抵抗原始签名人伪造攻击，而且具有更高的安全性和较高的实现效率，提高了方案的实用性。

参 考 文 献

[1] Diffie W, Hellman M E. New Direction in Cryptography[J]. IEEE Trans. Inform. Theory, 1976: 644-654

[2] Mambo M, Usuda K, Okamoto E. Proxy Signature: Delegation of the Power to Sign Messages[J]. IEICE Trans. on Fundamental, 1996, 79(9): 1338-1353

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

[4] 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

[5] Shum K, Wei V K. A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection[C]// Proc. of the 11th Int'l Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprises. Pittsburgh, Pennsylvania, USA: [s. n.], 2002: 55-56

[6] 谷利泽，李献中，杨义先. 不需要可信任方的匿名代理签名方案[J]. 北京邮电大学学报，2005，28(1)：48-50

[7] 谷利泽，张胜，杨义先. 一种新型的代理签名方案[J]. 电子与信息学报，2005，27(9)：1463-1466

[8] 柳菊霞，吴良杰，苏靖枫，等. 匿名代理签名方案的研究与改进[J]. 信息安全与通信保密，2006(3)：75-77

[9] 曹正军，刘木兰. 数字签名方案中的孤悬因子和冗余数据[J]. 计算机学报，2006，29(2)：249-255