

新的无证书的代理签名方案

樊 睿,王彩芬,蓝才会,左为平

(西北师范大学 数学与信息科学学院,兰州 730070)

(ruifan83@126.com)

摘 要:已有的代理签名方案,大多是基于证书的密码体制或者基于身份的密码体制提出的,都存在证书的管理问题或密钥的托管问题。基于无证书密码体制的优点,在无证书公钥密码体制的基础上提出了一种新的代理签名方案。分析表明,该方案不需要证书的管理,也没有密钥的托管问题,满足代理签名所要求的所有性质,且在效率上优于已有的基于身份的代理签名方案。

关键词:代理签名;无证书公钥体制;双线性对 Diffie-Hellman (DH) 问题

中图分类号: TP309.7;TP393.08 **文献标志码:** A

A new certificateless proxy signature

FAN Rui, WANG Cai-fen, LAN Cai-hui, ZUO Wei-ping

(College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu 730070, China)

Abstract: The existing proxy signature schemes are based on certificate public key cryptography and identity-based cryptography, which have the problems of certificate management or key escrow. Based on the merit of certificateless public key cryptography, a new certificateless proxy signature was proposed. The result shows that the new proxy signature scheme solves all the problems of certificate management and key escrow, and also satisfies all the required characteristics of proxy signature. It is more efficient than the existed ID-based proxy signatures.

Key words: proxy signature; certificateless public key cryptography; bilinear Diffie-Hellman problem

0 引言

2003 年 S. S. Al-Riyami 等人^[1]提出了无证书公钥体制。无证书的公钥签名方案不需要公钥证书,解决了 PKI/CA 技术中证书管理与认证的问题,在应用中带来极大的便利。无证书的公钥签名方案需要一个可信第三方命名为 KGC (Key Generating Centre),但不同于基于身份的密码体制下的 PKG (Private Key Generator),KGC 根据用户的身份 ID 为用户生成部分私钥,这里 KGC 必须保证为用户生成的部分私钥是正确的。用户根据 KGC 产生的部分私钥和自己产生的秘密值共同生成私钥,所以 KGC 不知道用户的私钥,这就解决了基于身份的密码体制中密钥托管的问题。例如,PKG 可以解密任何人用公钥加密过的密文,同时,PKG 也可以伪造任何人的签名。所以基于身份的密码体制不能实现真正的不可否认性。虽然,密钥的托管问题也可以通过引入多个 PKG 用门限的方法来解决,但是这样会带来额外的通信代价及设施的浪费。另外 PKG 的密钥一旦泄露,后果比 PKI 中 CA 的密钥泄露更为严重。2004 年 Y. -R. Lee 和 H. -S. Lee 在文献[1]的基础上提出了一种无证书公钥认证加密方案^[2],同年 Dae-Hyun Y 等人^[3]又提出了一种无证书签名方案的构造方法,该方法利用基于身份的签名方案和基于证书的签名方案来实现,其安全性将由上述两种密码体制的安全性决定。2005 年 Cheng. Z. H. 等人指出他们的方案存在一种公钥替换攻击,并提出了一种更有效的无证书公钥加密方案^[4]。

代理签名的概念是 1996 年由 Mambo 等人^[5]首先提出的,它指当某个签名人因某种原因不能签名时,将签名权委托

给他人(称为代理人)替自己行使签名权。根据授权对代理签名作了分类,即完全授权方案、部分授权方案和证书授权方案;部分授权方案又分为代理人受保护和代理人不受保护两种。代理签名由原始签名人、代理签名人及验证者三方共同参与,一般由四个或更多算法组成,包括系统初始化、代理密钥生成、代理签名生成和代理签名验证。

分析已有的代理签名方案,发现大多都是在基于证书或者基于身份的密码体制上提出的,鉴于无证书公钥密码体制的优点,我们在其基础上提出了一种无证书的代理签名方案,该方案在授权时采用基于文献[6]的短签名方案,提高了签名效率。该方案的安全性基于文献[1]的无证书签名方案和文献[6]的短签名方案,且效率优于基于身份的代理签名方案^[7,8]。

1 预备知识

1.1 线性 Diffie-Hellman 问题

设 G_1 与 G_2 是两个阶为 q 的循环群, q 为大素数,其中 G_1 是以加法的形式表示的, G_2 是以乘法的形式表示的。 P 为 G_1 的生成元。假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题。若映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 满足下列性质则此映射称为可容许的双线性映射。

性质 1 线性性。 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, 对所有 $P, Q \in G_1$ 和所有 $a, b \in Z$ 。

性质 2 非退化性。如果 P 是 G_1 的生成元, 则 $\hat{e}(P, P)$ 是 G_2 的生成元。

性质 3 可计算性。存在一个高效的算法, 计算 $\hat{e}(P, Q)$, $\forall P, Q \in G_1$ 。

收稿日期: 2007-10-18; **修回日期:** 2008-02-15。 **基金项目:** 甘肃省自然科学基金资助项目(3ZS051-A25-042); 甘肃省科技攻关项目(2GS064-A52-035-03); 西北师范大学学生学术科研资助项目。

作者简介: 樊睿(1983-), 女, 甘肃通渭人, 硕士研究生, 主要研究方向: 信息安全、现代密码学; 王彩芬(1963-), 女, 河北安国人, 教授, 博士生导师, 博士, 主要研究方向: 信息安全、电子商务协议的设计与分析。

定义以下几个密码学问题:

1) 计算双线性 Diffie-Hellman 问题 (Computable Diffie-Hellman Problem, CDHP):

输入 P, aP, bP, cP ; 输出 $\hat{e}(P, P)^{abc} \in G_2, \forall a, b, c \in Z_q$ 。

2) 判定双线性 Diffie-Hellman 问题 (Decision Diffie-Hellman Problem, DDHP):

给定四元组 $(P, aP, bP, cP) \in G_1^4$, 对 $a, b, c \in F_q^*$ 判断 $c = ab \pmod{q}$ 是否成立。

3) GDH (Gap Diffie-Hellman) 问题:

如果在群 G_1 上, DDHP 容易但 CDHP 困难, 则 G_1 被称为 GDH 群。

1.2 无证书的代理签名的性质

可验证性 从代理签名中, 验证者可以验证签名的正确性并确信原始签名人对所签消息的认可。

不可伪造性 包括 KGC 在内的任何第三方都不能伪造原始签名人的授权签名和代理签名人的代理签名。

可区分性 任何人都能区分出代理签名和一般签名的不同, 并确定出原始签名人和代理签名人的关系。

不可否认性 一旦代理签名人代表原始签名人建立了有效的代理签名, 他便不能否认自己的行为。

防滥用性 代理签名人不能签署未经授权的信息, 代理签名人也不能把签名权力非法转给其他人。

2 无证书公钥签名方案

一个无证书公钥签名方案的定义由七个随机算法构成。

2.1 系统生成

设 G_1 为循环加法群, G_2 为循环乘法群, G_1, G_2 的阶均为素数 q , $P \in G_1$ 作为 G_1 的生成元, 定义一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 和两个单向哈希函数 $H_1: \{0, 1\}^* \rightarrow G_1^*$, $H_2: \{0, 1\}^n \times G_2 \rightarrow Z_q^*$ (n 为明文长度)。KGC 选择 $s \in_R Z_q^*$ 作为自己的私钥, 计算 $P_{\text{pub}} = sP$, 将 s 秘密保存, 公开系统参数: $params = \{G_1, G_2, e, q, P, P_{\text{pub}}, H_1, H_2\}$ 。

2.2 部分私钥生成

该算法输入 $params$ 和用户 A 的身份信息 ID_A , 返回部分私钥 D_A 。该算法由 KGC 执行, 其中 $D_A = sQ_A$, $Q_A = H_1(ID_A)$ 。KGC 将 D_A 通过安全信道发送给 A 。通过等式 $e(D_A, P) = e(Q_A, P_{\text{pub}})$ 来验证 D_A 的真实性。

2.3 秘密值生成

该算法输入 $params$ 和用户 A 的身份信息 ID_A , 输出用户 A 的秘密值 $x_A \in_R Z_q^*$ 。

2.4 私钥生成

该算法输入 $params$ 、用户 A 的部分私钥 D_A 和用户 A 的秘密值 x_A , 输出用户 A 的私钥 S_A , 其中 $S_A = x_A D_A = x_A s Q_A$ 。

2.5 公钥生成

该算法输入 $params$ 和用户 A 的秘密值 x_A , 输出用户 A 的公钥 P_A 。其中 $P_A = \langle X_A, Y_A \rangle$, $X_A = x_A P$, $Y_A = x_A P_{\text{pub}} = x_A s P$ 。

2.6 签名

该算法输入 $params$ 、用户 A 的私钥 S_A 和要签名的消息 M , 输出签名 $Sig \in S$ 。

当要对消息 M 签名时, 用户 A 随机选择 $a \in_R Z_q^*$, 计算 $r = e(P, P)^a$, $v = H_2(M, r)$, $U = vS_A + aP$ 。用户 A 对消息 M 的签名为 $Sig = (U, v)$ 。

2.7 验证

该算法输入 $params$ 、消息 M 、要验证的签名 $Sig \in S$ 、用户

A 的身份信息 ID_A 和公钥 P_A , 输出签名有效或者 \perp 。

1) 验证者验证等式 $e(X_A, P_{\text{pub}}) = e(Y_A, P)$ 来验证用户 A 的公钥是否正确, 如果等式成立则用户 A 的公钥是正确的。

2) 计算 $Q_A = H_1(ID_A)$, $r = e(U, P)e(Q_A, -Y_A)^v$, 然后验证等式 $v = H_2(M, r)$, 若成立则接受签名, 否则拒绝。

3 无证书的代理签名方案

该方案基于上述无证书签名方案, 且在授权时为了缩短签名长度, 提高传输效率, 采用文献[6]中不可伪造的短签名方案。

3.1 系统设置

G_1 与 G_2 是两个阶为 q 的循环群, 满足 2.1 中定义, $P \in G_1$ 作为 G_1 的生成元, 定义三个密码学上的单向哈希函数 $H_1: \{0, 1\}^* \rightarrow G_1, H_2: \{0, 1\}^* \times G_2 \rightarrow Z_q^*, H_3: G_1 \rightarrow Z_q^*$ 。最后, KGC 选择 $s \in_R Z_q^*$ 作为自己的私钥, 计算公钥 $P_{\text{pub}} = sP$, 将 s 秘密保存, 公开系统参数: $params = \{G_1, G_2, e, q, P, P_{\text{pub}}, H_1, H_2, H_3\}$ 。

3.2 密钥提取

原始签名人 A 和代理签名人 B 分别根据以上介绍的无证书的签名方案产生用户的公私钥, A 的私钥为 $S_A = x_A s Q_A$, 公钥为 $P_A = \langle X_A, Y_A \rangle$ 。 B 的私钥为 $S_B = x_B s Q_B$, 公钥为 $P_B = \langle X_B, Y_B \rangle$ 。

3.3 代理密钥的生成

A 建立一个授权许可信息 m_w 来明确说明包含 A 和 B 的身份信息的授权关系, 同时也说明该授权关系的使用限制等内容。 A 计算一个短签名 $S_w = S_A H_3(H_1(m_w))$, 将 (S_w, m_w) 发送给 B 。 B 首先验证等式 $e(X_A, P_{\text{pub}}) = e(Y_A, P)$ 是否成立来验证 A 的公钥, 若成立说明 A 的公钥正确, 然后验证等式 $e(S_w, P) = e(Q_A, Y_A)^{H_3(H_1(m_w))}$ 是否成立。如果成立, B 计算代理签名密钥: $S_p = S_w + H_3(H_1(m_w))S_B = H_3(H_1(m_w))(S_A + S_B)$ 。

3.4 签名

当要对消息 m 签名时, 代理签名人 B 选择 $a \in_R Z_q^*$, 计算 $r = e(P, P)^a$, $v = H_2(m, r)$, $U = vS_p + aP$, 则 (U, v, m_w) 为 B 对 m 的代理签名。

3.5 验证

验证者首先验证等式 $e(X_A, P_{\text{pub}}) = e(Y_A, P)$ 和 $e(X_B, P_{\text{pub}}) = e(Y_B, P)$ 来验证 A, B 的公钥。然后计算 $Q_A = H_1(ID_A)$, $Q_B = H_1(ID_B)$, $r = e(U, P)[e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))}$, 然后验证等式 $v = H_2(m, r)$, 若成立则接受签名, 否则拒绝。

4 安全性及效率分析

4.1 正确性证明

1) 授权签名的正确性证明
验证等式 $e(S_w, P) = e(Q_A, Y_A)^{H_3(H_1(m_w))}$ 是否成立, 若成立则为 A 合法的授权签名。

证明 $\because e(S_w, P) = e(S_A H_3(H_1(m_w))), P) = e(x_A s Q_A H_3(H_1(m_w))), P) = e(Q_A, x_A s P)^{H_3(H_1(m_w))}$
 $\therefore e(S_w, P) = e(Q_A, Y_A)^{H_3(H_1(m_w))}$

2) 代理签名的正确性证明

验证 r 是否等于 $e(U, P)[e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))}$, 若等于则 $v = H_2(m, r)$ 成立。

证明

$\because e(U, P)[e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))} =$

$$\begin{aligned}
& e(vS_p + aP, P)[e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))} = \\
& re(S_p, P)^v[e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))} = \\
& re(H_3(H_1(m_w))(S_A + S_B), P)^v \\
& [e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))} = \\
& re((x_A sQ_A + x_B sQ_B), P)^{vH_3(H_1(m_w))} = \\
& [e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))} = \\
& r[e(Q_A, Y_A)e(Q_B, Y_B)]^{vH_3(H_1(m_w))} = r \\
& [e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))} = r \\
& \therefore r = e(U, P)[e(Q_A, -Y_A)e(Q_B, -Y_B)]^{vH_3(H_1(m_w))}
\end{aligned}$$

4.2 不可伪造性证明

定理 假设 CDHP 难解, 则该代理签名方案具有不可伪造性。

证明

1) 授权签名的不可伪造性。因本方案的授权签名基于文献[6]的不可伪造短签名, 文献[6]已证明是安全的不可伪造的, 所以本方案的授权签名也是安全的不可伪造的。

2) 代理签名的不可伪造性。本代理签名方案基于文献[1]的无证书的签名方案, 该方案已证明是安全的不可伪造的, 所以本方案的基本签名也是安全的不可伪造的。

将攻击者分为三类: 普通攻击者、原始签名者和 KGC。

普通攻击者 C 不能伪造消息 m 的代理签名, 因为他不知道原始签名人 A 和代理签名人 B 的私钥 S_A 和 S_B , 他无法计算代理密钥 S_p , 也就无法伪造代理签名。

原始签名者 A 不能伪造消息 m 的代理签名, 在计算代理密钥 S_p 时用到 B 的私钥 S_B , 所以 A 也不能伪造消息 m 的代理签名。

KGC 不能伪造消息 m 的代理签名, 因为虽然 KGC 知道用户 A, B 的部分私钥 D_A 和 D_B , 但是他不知道用户的秘密信息 x_A 和 x_B , 所以 KGC 无法得到用户私钥, 更得不到代理签名密

钥 S_p , 所以 KGC 也无法伪造消息 m 的代理签名。

4.3 可区分性

原始签名者的公钥及代理签名者的公钥都会出现在代理签名的验证等式里, 而且代理签名的组成为 (U, v, m_w) , 授权信息 m_w 也包含在代理签名和签名验证等式里面, 因此任何人都可以从授权信息里决定代理签名者的身份, 很好地满足可区分性。

4.4 不可否认性

由于授权信息 m_w 包含在有效的验证等式里, 因此代理签名人不能更改。原始签名人对授权信息进行了签名, 而代理签名的验证等式中包含了此授权, 一旦做了授权签名原始签名人就不能否认自己的签名, 并且原始签名人私钥包含 $Q_A = H_1(ID_A)$, A 想要伪造一个他自己的私钥来否认授权签名, 等价于求 hash 函数的单向性问题。代理密钥里面有代理签名者的私钥, 一旦代理签名者为原始签名者创建了一个有效的代理签名, 他就无法否认自己的签名。

4.5 防止签名权力的滥用

由于有了授权信息 m_w 的限制, 而 m_w 就出现在代理签名的验证等式中, 因此代理签名人不能签署未经授权的信息, 当然代理签名人也不能把签名权力非法转给其他人。

4.6 效率分析

从计算复杂性方面分析比较我们提出的方案和文献[7, 8]的方案, 并将结果总结在表1中。表1中的相关符号定义如下: P_a 表示双线性对操作, P_m 表示 G_1 上的标量乘, A_d 表示 G_1 上的点加操作, M_u 表示 Z_q^* 上的乘操作, $M_u G_2$ 表示 G_2 上的乘操作, ExG_2 表示 G_2 上的指数运算, H_s 表示哈希函数。考虑到 $Q_A = H_1(ID_A)$, $Q_B = H_1(ID_B)$, $e(Q_A, Y_A)$, $e(Q_B, Y_B)$ 可提前进行计算, 因此我们的方案在考虑计算复杂性时以上操作进行了预计算, 同等起见, 文献[7, 8]的方案也考虑了预计算。

表1 我们的方案与其他方案的计算复杂性比较

方案	代理密钥生成	代理签名	签名验证
文献[7] 方案	$2P_a + 3P_m + M_u G_2 + 2A_d + 3H_s$	$2P_m + A_d + H_s$	$3P_a + 3M_u G_2 + ExG_2 + 2H_s$
文献[8] 方案	$2P_a + 3P_m + M_u G_2 + 2ExG_2 + 2A_d + 2H_s$	$P_a + 2P_m + ExG_2 + A_d + H_s$	$P_a + 2M_u G_2 + 2ExG_2 + H_s$
我们的方案	$P_a + 2P_m + ExG_2 + A_d + 4H_s$	$P_a + 2P_m + ExG_2 + A_d + H_s$	$P_a + ExG_2 + M_u + H_s$

以上操作中 P_a 计算最耗时, 然后是 P_m 。分析表1可以看出我们的方案的计算复杂度大约为 $3P_a + 4P_m$ 数量级, 文献[7]方案的计算复杂度大约为 $5P_a + 5P_m$ 数量级, 文献[8]方案的计算复杂度大约为 $4P_a + 5P_m$ 数量级, 并且在其他操作上我们方案的效率也远比它们的高。因此, 我们的方案整体效率要比文献[7]和[8]的高。

5 结语

本文基于无证书公钥密码体制的优点, 提出了一种无证书的代理签名方案, 该方案在授权时基于文献[6]的短签名方案, 提高了签名效率。该方案的安全性基于文献[1]的无证书签名方案和文献[6]的短签名方案, 且效率优于基于身份的代理签名方案[7, 8]。

参考文献:

- [1] AL-RIYAMI S S, PATERSON K G. Cryptology ePrint Archive, 2003/126, Certificateless public key cryptography[R/OL]. [2007-10-10]. <http://eprint.iacr.org/2003/126.pdf>.
- [2] LEE Y-R, LEE H-S. Cryptology ePrint Archive, 2004/150, An Authenticated Certificateless Public Key Encryption Scheme[EB/OL].

- [3] DAE-HYUN Y, PIL-JOONG L. Generic construction of certificateless signature[C]// Information Security and Privacy, ACISP'2004, LNCS 3108. Berlin: Springer-Verlag, 2004: 200-211.
- [4] CHENG Z H, COMLEY R. Cryptology ePrint Archive, 2005/012, Efficient Certificateless Public Key Encryption[EB/OL]. [2007-10-10]. <http://citeseer.ist.psu.edu/cheng05efficient.html>.
- [5] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation[C]// Advances in 3rd ACM Conference on Computer and Communications Security (CCS'96). New York: ACM Press, 1996: 48-57.
- [6] BONEH D, LYNN B, SHACHAM H. Short signature from the Weil pairing[C]// Advances in Cryptology, Asiacrypt 2001, LNCS 2248. Berlin: Springer-Verlag, 2001: 514-532.
- [7] XU J, ZHANG Z F, FENG D G. ID-based proxy signature using bilinear pairings[C]// CHEN G, ed. Advances in Parallel and Distributed Processing and applications - ISPA 2005 Workshops, LNCS 3759. Berlin, Heidelberg: Springer-Verlag, 2005: 359-367.
- [8] ZHANG F, KIM K. Efficient ID-based blind signature and proxy signature from bilinear pairings[C]// ACISP 2003, LNCS 2727. Berlin: Springer-Verlag, 2003: 312-323.