第25卷第1期 华东交通大学学报 Vol. 25 No. 1
2008年2月 Journal of East China Jiaotong University Feb. ,2008

文章编号:1005-0523(2008)01-0113-04

一种高效的基于身份的代理盲签名方案

陈玲玲,亢保元,张 磊

(中南大学 数学科学与计算技术学院,湖南 长沙 410075)

摘要: 在代理签名中,原始签名人能将数字签名的权力委托给代理签名人;而在盲签名方案中,签名者不能看到被签消息的内容,签名被接受者得到后,签名者不能追踪签名. 结合代理签名与盲签名的优点,利用基于椭圆曲线上的Weil配对(Weil Pairing)的双线性映射,构造了一个高效的基于身份的代理盲签名方案. 分析表明,该方案不仅满足代理盲签名所要求的所有性质,而且其效率也优于已有同类方案.

关 键 词: 基于身份;双线性映射;代理签名;盲签名;代理盲签名

中图分类号: TP309 **文献标识码:** A

1996年Mambo,Usuda和Okamoto首先提出(代理签名的概念)[1],它指当某个签名人(称为授权人或原始签名人)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,验证人能够验证并区分原签名人的签名和代理人的签名. 1983年Chaum首先提出盲签名的概念[2],它是指签名者不知道所签消息具体内容的数字签名. 盲签名在电子现金、电子投票等应用中可提供用户匿名性. 结合代理签名和盲签名,在2000年,Lin和Jan第一个提出了代理盲签名方案[3],之后,Tan等人提出了一种基于离散对数的代理盲签名方案[4]. 1984年Shamir提出了一个基于身份的加密和签名方案[5],用来简化基于证书的公钥体系下密钥管理的开销. 在这种体制下,每个人的公钥是由惟一标志其身份的相关信息(可以是姓名、地址或电子邮件地址等)所确定.

自从2001年Boneh等提出了基于双线性对的短签名[6]后,双线性对成了构造签名的重要工具,由双线性对构造的签名具有签字短、安全、高效等特点. 本文正是利用这一密码学工具,基于椭圆曲线上的Weil配对(Weil Pairing)的双线性映射,用Hess基于身份的签名[7]的一种变体作为基本签名,构造了一个高效的基于身份的代理盲数字签名方案. 分析表明,该方案不仅满足代理盲签名所要求的所有性质,而且其效率也优于文献[8][9].

1 预备知识

1.1 双线性映射

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. 假定在G_1、G_2中计算离散对数问题是困难的. 设$\hat{e}$: $G_1 \times G_1 \to G_2$为一个双线性映射,它满足以下三个性质

(1) 双线性:对于所有的$P,Q \in G_1$和所有的$a,b \in Z_q$,$\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$.

(2) 非退化性:存在$P \in G_1$,满足$\hat{e}(P,P) \neq 1$.

(3) 可计算性:如果$P,Q \in G_1$,则$\hat{e}(P,Q)$可以在多项式时间内有效计算出来.

下面描述一些常用的与双线性映射有关的数学问题.

(1) 离散对数问题DLP(Discrete Logarithm Problem):已知(G_1中)两个{群}元素P、Q,找一整数n使得$Q = nP$成立.

(2) 决策Diffie-Hellman问题DDHP(Decision

收稿日期:2008-01-19

作者简介:陈玲玲(1982-),女,湖南岳阳人,中南大学在读研究生,研究方向为密码学.

Diffie – Hellman Problem)：对于 $a,b,c \in_R Z_q^*$，$P \in G_1$，已知 P,aP,bP,cP 判断 $c = ab \bmod q$ 是否成立.

(3) 计算 Diffie – Hellman 问题 CDHP(Computational Diffie – Hellman Problem)：对于 $a,b \in_R Z_q^*$，$P \in G_1$，已知 P,aP,bP,cP，计算 abP.

(4) 间隙 Diffie – Hellman 问题 GDHP(Gap Diffie – Hellman Problem)：如果在群 G_1 上，DHP 容易但 CDHP 困难，则 G_1 被称为 GDH 群.

本文假设 DLP 和 CDHP 在 G_1、G_2 中是难解的，GDH 群能在有限域上的超奇异椭圆曲线或超椭圆曲线上获得，双现线性映射可通过 Weil 对或 Tate 对构造. 本文方案基于 GDH 群，关于 GDH 群的构造可参看文献[6].

1.2 代理盲签名的性质

一个安全有效的代理盲签名应满足以下要求：

可验证性：盲签名消息持有者 R 能够像验证原始签名一样验证代理签名.

不可伪造性：只有代理人可以产生代表授权人的合法签名，而授权人和其他人都不能.

可鉴别性：任何人可以由一个签名鉴别出代理人.

不可否认性：一旦代理人代表授权人产生了一个合法的代理签名，他和授权人都不能否认这个签名.

可区别性：任何人都可以区别代理人产生的代理签名与正常签名.

盲性：签名者(代理人)不能得到关于签名和被签消息的任何信息.

2 基于身份的代理盲签名

本文方案中涉及的四个参与方分别是：密钥生成中心 KGC(key generation center)、原始签名人 A、代理签名人 B、盲签名的持有者 C. 包括 5 个阶段，分别是：系统参数设置、密钥提取、代理密钥生成、代理签名生成和签名验证.

2.1 系统参数设置

KGC 选择 $q,G_1,G_2,\hat{e}$，其含义与 1.1 中相同. 然后，选择 $P \in G_1$ 为 G_1 的生成元，定义密码学上 3 个强无碰撞安全的 Hash 函数：$H(\cdot)$：$\{0,1\}^* \to G_1$，$H_2(\cdot):\{0,1\}^* \times G_2 \to Z_q^*$，$H_3(\cdot):G_1 \to Z_q^*$，KGC 再选择 $t^R Z_q^*$，计算 $P_{pub} = tP$，t 保密，t 称为系统主密钥. 公开系统参数 params $= \{G_1,G_2,\hat{e},q,P,P_{pub},H_1(\cdot),H_2(\cdot),H_3(\cdot)\}$.

2.2 密钥提取

原始签名人 A 和代理签名人 B 提交他们的身份信息 ID_A,ID_B 给 KGC，KGC 计算它们相应的公钥/密钥对为 $PK_A = H_1(ID_A)$，$SK_A = tPK_A$，$PK_B = H_1(ID_B)$，$SK_B = tPK_B$，然后分别安全地发送给 A,B.

2.3 代理密钥生成

A 建立一个许可证 W 来明确说明包含 A 和 B 的身份信息和授权关系，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，$S_W = H_3(H_1(W))SK_A$，然后将 (W,S_W) 发送给 B，B 计算并验证以下等式是否成立

$$\hat{e}(S_W,P) = \hat{e}(PK_A,P_{pub})^{H_3(H_1(W))}$$

如若成立，则 B 计算代理签名密钥：

$$S_P = S_W + H_3(H_1(W))SK_B$$

2.4 代理签名生成

代理签名人 B 给 C 的消息 m 进行盲数字签名，过程如下：

B		C
选择 $P_1 \in G_1$		选择 $P_2 \in G_1, b \in_R Z_q^*$
计算 $K = \hat{e}(P_1,P)$	$\xrightarrow{(K,W)}$	
$R = \hat{e}((PK_A + PK_B))^{H_3(H_1(W)b}, P_{pub})$		
	$\xleftarrow{c} U = K\hat{e}(P_2,P)$，$c = (H_2(m,RU) + b) \bmod q$	
计算 $S = cS_p + P_1$	$\xrightarrow{S}$	
		计算 $S' = S + P_2, c' = c - b$

则 $\sigma(m) = (S',c',m,W)$ 为消息 m 的基于身份的代理盲签名.

2.5 签名验证

已知基于身份的代理盲签名 $\sigma(m) = (S',c',m,W)$，验证人可以验证其有效性：

$$c' = H_2(m,\hat{e}(S',P)\hat{e}(PK_A + PK_B,P_{pub})^{-ct})$$

其中 $t = H_3(H_1(W))$

3 安全性分析

3.1 可验证性

从代理签名的生成过程来分析，我们可计算

$$\begin{aligned}
&H_2(m,\hat{e}(S',P)\hat{e}(PK_A + PK_B,P_{pub})^{-ct})\\
&= H_2(m,\hat{e}(S_2 + P_2,P)\hat{e}(PK_A + PK_B,P_{pub})^{-ct})\\
&= H_2(m,\hat{e}(cS_p + P_1 + P_2,P)\hat{e}(PK_A + PK_B,P_{pub})^{-ct})\\
&= H_2(m,\hat{e}(cH_3(H_1(W))(SK_A + SK_B) + P_1 + P_2,P)\hat{e}(-c'H_3(H_1(W))(PK_A + PK_B),P_{pub}))\\
&= H_2(m,\hat{e}(cH_3(H_1(W))(SK_A + SK_B),P)\hat{e}(P_1
\end{aligned}$$

$+P_2,P)\hat{e}(-c'H_3(H_1(W))(PK_A+PK_B),P_{pub}))$

$=H_2(m,\hat{e}(cH_3(H_1(W))(PK_A+PK_B),P_{pub})\hat{e}(P_1+P_2,P)\hat{e}(-c'H_3(H_1(W))(PK_A+PK_B),P_{pub}))$

$=H_2(m,\hat{e}((c-c')H_3(H_1(W))(PK_A+PK_B),P_{pub})\hat{e}(P_1+P_2,P))$

$=H_2(m,\hat{e}(H_3(H_1(W))(PK_A+PK_B),P_{pub})^b\hat{e}(P_1,P)\hat{e}(P_2,P)))$

$=H_2(m,RU)=c'$

所以,代理签名是可验证的.

3.2　不可伪造性

因为主密钥 t 被 KGC 秘密保存,通过 $P_{pub}=tP$ 得到 t,相当于破解 DLP,H_1,H_2,H_3 均为密码学上的单向哈希函数,因此,除代理签名人 B 以外的其他人,包括原始签名人和其他第三方,都不能通过原始签名人和其他代理签名人的公钥来建立有效的代理密钥. 没有 B 的密钥 SK_B 和代理密钥 S_p 来伪造 B 的有效签名等价于攻破 Hess 的基于身份的签名(我们在盲签名中用到的基于身份的签名是 Hess 签名的一种简单变形,实质上完全等价),而 Hess 的基于身份的签名在随机图灵机模型中对伪造攻击是安全的.

3.3　可鉴别性

由于验证等式中含 W,其中包括了授权人和代理人的相关信息,因此任何人可由一个签名鉴别出代理人.

3.4　不可否认性

一旦代理签名人 V 建立了一个有效的代理盲签名,他不能向原始签名人否认这个事实. 因为 B 已将他的身份信息嵌入到代理密钥中去了.

3.5　可区分性

由于代理签名者本人的公钥与代理签名公钥不同,因而任何人都可区别由代理人产生的代理盲签名和正常盲签名.

3.6　盲性

在代理盲签名生成过程中,由于接收者对待签消息进行了盲化,且签名 $\sigma(m)=(S',c',m,W)$ 也是由接收者计算的,因而签名者无法获知待签消息和签名结果的内容.

4　性能分析

下面将我们提出的方案与文献 [8]　[9] 中的方案从计算复杂性方面进行分析,并将结果总结在下表中. 表中有关符号的定义如下: P_a 表示双线性映射中的对操作,P_m 表示 G_1 上的标量乘,A_d 表示 G_1 上的点加操作,M_uG_2 表示 G_2 上的乘操作,E_xG_2 表示 G_2 上的指数运算,H_s 表示哈希函数. 考虑到双线性对 $\hat{e}(PK_A+PK_B,P_{pub})$ 可进行预计算,因此计算复杂性时不予考虑,文献 [8]　[9] 也同样考虑了预计算.

本文方案与其它方案的性能比较

方案	代理密钥生成	代理签名	验证
文献 [8] 的方案	$2P_a+4P_m+1M_uG_2+1E_xG_2+4A_d+1H_s$	$2P_a+2P_m+1E_xG_2+1A_d+4H_s$	$3P_a+1P_m+1M_uG_2+1E_xG_2+1A_d+2H_s$
文献 [9] 的方案	$1P_a+2P_m+1E_xG_2+1A_d+4H_s$	$1P_a+6P_m+5A_d+3H_s$	$1P_a+1M_uG_2+1E_sG_2+1A_d+2H_s$
本文方案	$1P_d+2P_m+1E_sG_2+1A_d+4H_s$	$2P_a+P_m+2M_uG_2+2A_d+1E_xG_2+H_s$	$1P_a+1M_uG_2+1E_sG_2+H_s$

从各种操作的计算来看,P_a 计算最耗时,其次是 P_m. 从上表中可以看出本文方案的计算复杂度大约为 $4P_a+3P_m$ 数量级,文献 [8] 的方案的计算复杂度大约为 $7P_a+11P_m$ 数量级,文献 [9] 的方案的计算复杂度大约为 $3P_a+8P_m$ 数量级. 因此,本文方案优于文献 [8]　[9] 中提出的方案.

5　结论

代理盲签名在电子投票和电子现金和电子拍卖等商务领域发挥着重要作用. 本文结合代理签名和盲签名的特点,利用双线性映射,构造了一个高效的基于身份的代理盲签名,在分析了其安全性同时和已有方案进行了对比. 结果表明,本文方案更安全有效.

参考文献:

[1] Mambo M, Usdua K, Okamoto E. Proxy Signature: Delegation of the Power to Sign Messages [J]. IEICE Transactions on Fundations, 1996, E792A(9): 1338 - 1353.

[2] Chaum D. Bind Signature for Untraceable Payments [A]. Chaum D, Rivest R L, Shepman A T. Advances in Cryptolo-

gy: Crypto 1982 [C]. New York: Plemum, 1982. 199 – 203.

[3] Lin W, Jan J K. A Security Personal Learning Tools Using a Proxy Bind Signature Scheme [C]. Proceedings of International Conference on Chinese Language Computing. USA: Chinese Language Computer Society Knowledge Systems Institute, 2000. 273 – 277.

[4] Tan Z W, Liu Z J, Tang C M. A Proxy Digital Blind Signature Schemes Based on DLP [J]. Journal of Software, 2003, 14(11): 1931 – 1935.

[5] Shamir A.. Identity – based cryptosystems and signature schemes [A]. Blakley G R, Chaum D. Advances in Cryptology: CRYPTO 1982 [C]. Berlin: Springer, 1984. 47 – 53.

[6] Boneth D, Lynn B, Shacham H. Short signatures from the Weil pairing [A]. Boyf C. Advances in Cryptology: ASIA CRYPT 2001 [C]. Berlin: Springer, 2001. 514 – 532.

[7] Hess F. Efficient identity based signature schemes based on pairings [A]. Proceedings of the 2002 ACM Symposium on Applied Computing (SAC 2002) [C]. New York: ACM Press, 2003. 310 – 324.

[8] Dong Z, Zheng H, Chen K F, *et al* ID – based proxy blind signature [A]. Proceedings of the 18th International Conferences on Advanced Information Networking and Applications (AINA 2004) [C]. Los Alamipos: IEEE Computer Society, 2004. 380 – 383.

[9] Lang W M, Tan Y M, Yang Z K, *et al*. A new efficient ID – based proxy blind signature scheme [A]. Proceedings of the Ninth Internations (ISCC 2004) [C]. Los Alamipos: IEEE Computer Society, 2004. 407 – 411.

An Efficient ID – based Proxy Blind Signature Scheme

CHEN Ling – ling, KANG Bao – yuan, ZHANG Lei

(School of Mathematical Science and Computing Technology, Central South University, Changsha 410075)

Abstract: With proxy signature, an original signer can delegate his signing authority to a proxy signer who signs a message on behalf of the original signer. In blind signature scheme, a signing messages are unknown to the signer, which makes the blind signature and the identity of the requester cannot be traced. Based on bilinear projection of Weil Pairing, an efficient ID – based proxy blind signature scheme is presented by combining proxy signature with blind signature scheme. The analysis shows that the proposed scheme can satisfy all the required properties of a proxy blind signature. Furthermore, its efficiency is also better than that of the exiting schemes.

Key words: ID – based; bilinear pairings; proxy signature; blind signature; proxy blind signature

(责任编辑: 周尚超)