基于双线性配对的可证安全的代理签名方案

许 峰[1,2],崔 隽[1],黄皓[2]
(1. 南京大学计算机软件新技术国家重点实验室,江苏南京 210093;2. 河海大学计算机工程学院,江苏南京 210098)

摘 要: 代理签名是指当某个签名者由于某种原因不能签名时,将签名权委托给他人替自己行使签名权的一种签名,代理签名在实际应用中有着重要的作用. 提出了一个基于双线性配对的代理签名方案,并证明其在随机 Oracle 模型下是可证安全的. 分析表明该方案比 Zhang 等的代理签名方案有更高的效率.

关键词: 代理签名; 双线性配对; 可证安全
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2009) 03-0439-05

A Provably-Secure Proxy Signature Scheme from Bilinear Pairings

XU Feng[1,2], CUI Jun[1], HUANG Hao[2]
(1. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu* 210093, *China*;
2. *College of Computer and Information, Hehai University, Nanjing, Jiangsu* 210098, *China*)

Abstract: A proxy signature scheme enables a proxy signer to sign messages on behalf of an original signer. Proxy signature schemes have been shown to be useful in many applications. A Proxy Signature Scheme from Bilinear Pairings is proposed. It is proved that the scheme is secure in the random oracle model and more efficient than Zhang's scheme.

Key words: proxy signature; bilinear pairings; provably-security

1 引言

1996 年,Mambo、Usuda 和 Okamoto 首次提出了代理签名的概念. 代理签名是指当某个签名者由于某种原因不能签名时,将签名权委托给他人替自己行使签名权的一种签名. 此后,有很多代理签名方案陆续被提出[1-3]. 代理签名在很多应用场合能发挥重要的作用,如某公司的总经理可以委托一个可靠的助手在他出差期间代表他在一些文件上签字等. 代理签名一提出便引起国内外学者的广泛关注. 已经有很多新型代理签名方案被提出[4-7]. 但是到目前为止,代理签名领域还没有一个被广泛认可的方案,已有的方案普遍存在着安全和性能方面的问题.

一个强的代理签名方案应满足以下六条性质:强不可伪造性、可验证性、强可识别性、强不可否认性、可区分性、防止滥用.

2 预备知识

2.1 双线性映射和 GDH 群

设 G_1 是一个加法群,阶是大素数 q. G_2 是一个乘法群,同样以 q 为阶. 双线性映射 $e: G_1 \times G_1 \to G_2$ 满足如下特性:

1. 双线性: $\forall P, Q, R \in G_1$, $a, b \in Z$; $e(aP, bQ) = e(P, Q)^{ab}$;
2. 非退化性:存在 $P, Q \in G_1$,使得; $e(P, Q) \neq 1$;
3. 可计算性:对所有的 $P, Q \in G_1$,存在一个有效的算法计算 $e(P, Q)$.

假设 G 是一个椭圆曲线上的 q 阶的加法群, q 为大素数. 下面描述几个基于 G 的困难问题:

离散对数问题(DLP):给定 G 中两个元素 P 和 Q,计算整数 n,满足 $Q = nP$.

判定 Diffie-Hellman 问题(DDHP):对 $a, b, c \in Z_q^*$,给定 P, aP, bP, cP 判断 $c \equiv ab \bmod q$ 是否成立.

计算 Diffie-Hellman 问题(CDHP):对 $a, b \in Z_q^*$,给定 P, aP, bP,计算 abP.

当群 G 上的 DDHP 是容易的,而 CDHP 是困难的时,称群 G 为 Gap Diffie-Hellman(GDH)群. 这样的群可以在有限域的超椭圆曲线上找到. 利用椭圆曲线上的 Weil 配对或 *Tate* 配对可以构造满足以上条件的双线性映射.

收稿日期:2007-07-04;修回日期:2008-05-16
基金项目:国家自然科学基金(No. 60473091);国家 863 高技术研究发展计划项目(No. 2007AA01Z409)

2.2 BLS 短签名方案

在下一节中,我们将利用 BLS 短签名构造一个代理签名方案. 在这一节中,作为预备知识,将 BLS 短签名方案简单介绍一下.

BLS 短签名方案[8]包括以下三个算法:一个密钥产生算法 KeyGen,一个签名产生算法 Sign 和一个签名验证算法 Verify. BLS 算法介绍如下:

1. KeyGen:算法任意选择 $x \in_R Z_q^*$ 作为系统私钥,并计算 $P_{pub} = xP$ 作为系统公钥.

2. Sign:给定私钥 x 和消息 m,算法计算得到签名.

3. Verify:给定公钥 P_{pub},消息 m,以及其签名 σ,验证 $e(P, \sigma) = e(P_{pub}, H(m))$.

BLS 短签名的安全性是基于 CDH 数学困难问题的.

3 代理签名方案的形式化定义及攻击模型

3.1 代理签名方案的形式化定义

一个代理签名方案包括五个算法:初始算法,密钥生成算法,代理密钥生成算法,代理签名生成算法,签名验证算法. 一个代理签名方案还包括三个参与方:原始签名者 A,代理签名者 B 和签名验证者 V.

初始算法:输入一个安全参数,算法产生并且公布系统参数 $params$.

密钥生成算法:输入一个安全参数,算法分别产生 A 和 B 的公私钥对 (xA, P_A) 和 (xB, P_B).

代理密钥生成算法:A 创建一个授权委托证书 m_ω,并且与 B 交互产生代理密钥 S.

代理签名生成算法:输入待签名 σ 的消息 m,B 产生代理签名 σ.

签名验证算法:输入签名 σ,消息 m 和公钥 Q_P,V 验证 σ 是不是 B 关于消息 m 的合法代理签名,若是,则输出“TRUE”,否则输出“FALSE”.

3.2 代理签名方案的攻击模型

代理签名方案的攻击模型可以分为以下三种类型[9]:

1. 类型 Ⅰ:攻击者仅仅有 A 和 B 的公钥.

2. 类型 Ⅱ:攻击者除了有 A 和 B 的公钥,还有 A 的私钥.

3. 类型 Ⅲ:攻击者除了有 A 和 B 的公钥,还有 B 的私钥.

从这三个类型的攻击模型的定义很容易就可以看出,如果一个代理签名方案对类型 Ⅱ和类型 Ⅲ的攻击是安全的,那么这个方案就是对类型 Ⅰ的攻击是安全的.

3.2.1 类型 Ⅱ攻击模型的形式化定义

类型 Ⅱ攻击者除了有 A 和 B 的公钥,还有 A 的私钥. 类型 Ⅱ攻击模型的参与者为攻击者 $A_{Ⅱ}$ 和挑战者 C. 攻击模型的形式化定义如下:

初始算法:C 运行这个算法,得到原始签名者 A 的私钥-公钥对 (x_A, P_A),并将 (x_A, P_A) 传送给攻击者 $A_{Ⅱ}$.

公钥询问算法:$A_{Ⅱ}$ 可以指定任意某一个用户(一般设为用户 i)为代理签名者. $A_{Ⅱ}$ 可以询问用户 i 的公钥 P_{Bi},C 用 i 的身份信息 ID_{Bi} 产生 P_{Bi},并把 P_{Bi} 传送给 $A_{Ⅱ}$.

代理签名询问算法:$A_{Ⅱ}$ 可以询问用户 i 的签名 σ,C 用 i 的身份信息 ID_{Bi} 产生关于消息 m 的签名 σ 并输出.

输出算法:$A_{Ⅱ}$ 输出目标消息 m 及其代理签名 σ,其中 m 从来没有在**代理签名询问算法**中被询问过,并且 σ 是原始签名者 A 和代理签名者 B 合作产生的有效代理签名.

3.2.2 类型 Ⅲ攻击模型的形式化定义

类型 Ⅲ攻击者除了有 A 和 B 的公钥,还有 B 的私钥. 类型 Ⅲ攻击模型的参与者为攻击者 $A_{Ⅲ}$ 和挑战者 C. 攻击模型的形式化定义如下:

初始算法:

C 运行这个算法,得到原始签名者 A 的私钥-公钥对 (x_A, P_A) 以及代理签名者 B 的私钥-公钥对 (x_B, P_B),并将 (x_B, P_B, P_A) 传送给攻击者 $A_{Ⅲ}$.

代理签名询问算法:$A_{Ⅲ}$ 可以询问用户 i 的签名,C 用 i 的身份信息 ID_{Bi} 产生关于消息 m 的签名 σ 并输出.

输出算法:最后,$A_{Ⅲ}$ 输出目标消息 m 及其代理签名 σ,其中 m 从来没有在**代理签名询问算法**中被询问过,并且 σ 是原始签名者 A 和代理签名者 B 合作产生的有效代理签名.

4 本文提出的方案

初始算法:输入一个安全参数 k,初始算法输出 $\{G_1, G_2, q, e, P\}$,其中 G_1 为阶为素数的加法群,G_2 为阶为素数的乘法群,e 是 $G_1 \times G_1 \rightarrow G_2$ 的一个双线性映射. P 是 G_1 的生成元. 算法还输出两个 Hash 函数:

$H: \{0,1\}^* \rightarrow G_1$ 和 $h: \{0,1\}^* \times G_1 \rightarrow Z_q^*$.

. **密钥生成算法**:算法产生原始签名者 A 的私钥 x_A 和其对应公钥 $P_A = x_A P$,同理产生代理签名者 B 的私钥 x_B 和其对应公钥 $P_B = x_B P$.

代理密钥生成算法:

(1) A 创建一个授权委托证书 m_ω,它是对原始签名者对代理签名者的授权关系的一个详细描述. 并计算

$S' = x_A H(m_\omega, ID_B)$. ID_B 是代理签名者 B 的身份信息.

(2) A 公布 (m_ω, ID_B),并将 S 传送给 B.

(3) B 验证 $e(S', P) = e(H(m_\omega, ID_B), P_A)$ 是否成立,若成立,则转到(4),否则,要求 A 重新传送新的 S'.

(4) B 计算代理密钥: $S = x_B^{-1} S'$.

代理签名生成算法:

B 随机选取 $t \in Z_q^*$,计算, $U = tP_B$. $V = tP + h(m, U) S$. (U, V) 就是关于消息 m 的代理签名.

签名验证算法: V 验证方程 $e(V, P_B) = e(U, P) e(hH, P_A)$ 是否成立. 方程中, h 是 $h(m, U)$ 的缩写, H 是 $H(m_\omega, ID_B)$ 的缩写. 在本文的以下部分都将沿用这个缩写.

上述验证方程的正确性可以很容易由下式验证:

$$\begin{aligned} e(V, P_B) &= e(tP + hS, P_B) \\ &= e(tP, P_B)\, e(hS, P_B) \\ &= e(U, P)\, e(hx_B^{-1} S', P_B) \\ &= e(U, P)\, e(hS', P) \\ &= e(U, P)\, e(hx_A H, P) \\ &= e(U, P)\, e(hH, P_A) \end{aligned}$$

5　方案的效率与安全性分析

5.1　效率分析

在这里,将上文中提出的方案与文献[7]中的代理签名方案的效率进行比较,结果总结在表 1 和表 2 中,我们知道,计算配对函数是最耗费时间的. 从表 1 和表 2 中可以看到,新提出的方案与文献[7]的方案相比,在代理密钥生成阶段有几乎相同的效率,而在代理签名生成阶段有更高的效率.

表 1　代理密钥生成阶段的效率比较

	本文方案		文献[7]方案	
	A	B	A	B
配对函数		2		2
哈希函数	1	1	1	1
G_1 乘法运算	1	1	1	1
G_1 加法运算				1
Z_q 取逆运算		1		

表 2　代理签名生成阶段的效率比较

	本文方案	文献[7]方案
配对函数		1
哈希函数	1	1
G_1 乘法运算	3	2
G_1 加法运算	1	1

5.2　安全性分析

5.2.1　基于类型 II攻击者的不可伪造性

任意选取 $a, b \in Z_q^*$,计算得到 aP, bP,如果在仅仅知道 aP, bP 的情况下,能够计算出 abP,那么,就可以称解决了 CDH 数学难题. 如果类型 II攻击者 A_{II} 能够伪造出本文提出方案的代理签名,那么我们可以证明 C 能够利用这个签名计算出 abP,从而解决了 CDH 数学难题. 而我们知道 CDH 数学难题迄今为止仍是难以解决的,故我们可得到攻击者 A_{II} 无法伪造本文提出方案的代理签名.

初始算法: C 选取 $x_A \in Z_q^*$ 并设原始签名者的公钥为: $P_A = x_A = x_A P$. C 将 (x_A, P_A) 传送给攻击者 A_{II}.

公钥询问算法: 在这一步骤中, A_{II} 至多可以做 q_P 次公钥询问. C 任意选取 $1 \leq j \leq q_P$, A_{II} 提交 ID_{Bi} $(1 \leq i \leq q_P)$ 的公钥询问,如果 $i \neq j$, C 任意选取 $x_{Bi} \in Z_q^*$,设 $P_{Bi} = x_{Bi} P$;否则(即 $i = j$),设 $P_{Bi} = bP$,然后将项 (ID_{Bi}, x_{Bi}) 添加到列表 $PK\text{-}List$ 中,并把 P_{Bi} 传送给 A_{II}.

H 询问算法: 在这一步骤中, A_{II} 至多可以做 q_H 次 H 询问. A_{II} 关于 (m_ω, ID_{Bi}) $(1 \leq i \leq q_H)$ 的每一次询问, C 首先检查列表 $H\text{-}List$:

a. 如果在列表 $H\text{-}List$ 已经存在项 $((m_\omega, ID_{Bi}), H_i)$, C 将 H_i 返回给 A_{II} 作为 (m_ω, ID_{Bi}) 的哈希值.

b. 否则,也就是 A_{II} 从来没做过 (m_ω, ID_{Bi}) 的 H 询问. 这时,如果 $i = j$, C 宣告失败. 否则, C 先从列表 $PK\text{-}List$ 中找到项 (ID_{Bi}, x_{Bi}),得到 x_{Bi},并计算 $H_i = x_A^{-1} x_{Bi} aP$. C 将项 $((m_\omega, ID_{Bi}), H_i)$ 添加到列表 $H\text{-}List$ 中,并将 H_i 返回给 A_{II}. 如果列表 $PK\text{-}List$ 中没有项 (ID_{Bi}, x_{Bi}), C 先运行上一步骤中的公钥询问得到 (ID_{Bi}, x_{Bi}).

h 询问算法:

在这一步骤中, A_{II} 至多可以做 q_h 次 h 询问. A_{II} 关于 (m_i, U_i) $(1 \leq i \leq q_h)$ 的每一次询问, C 首先检查列表 $h\text{-}List$:

a. 如果在列表 $h\text{-}List$ 已经存在项 $((m_i, U_i), h_i)$, C 将 h_i 返回给 A_{II} 作为 (m_i, U_i) 的哈希值.

b. 否则,也就是 A_{II} 从来没做过 (m_i, U_i) 的 h 询问. 这时, C 随机选择 $h_i \in Z_q^*$,满足列表 $H\text{-}List$ 中不存在项 $(*, h_i)$. C 将项 $((m_i, U_i), h_i)$ 添加到列表 $h\text{-}List$ 中,并将 h_i 返回给 A_{II}.

代理签名询问算法: 在这一步骤中, A_{II} 至多可以做 q_s 次代理签名询问. A_{II} 关于 (m_i, ID_{Bi}) $(1 \leq i \leq q_s)$ 的每一次询问, C 首先检查列表 $H\text{-}List$ 和 $h\text{-}List$:

a. 如果在列表 $H\text{-}List$ 已经存在项 $((m_\omega, ID_{Bi}), H_i)$,同时在列表 $h\text{-}List$ 也已经存在项 $((m_i, U_i), h_i)$,那么 C 直接获得 H_i and hi.

b. 否则 $i = j, c$ 如果 $i = j$, C 宣告失败;如果 $i \neq j$, C 首先运行 H 询问和 h 询问算法. 然后计算 $S_i = x_{Bi}^{-1} x_A$, $H_i, U_i = t_i P_{Bi}, V_i = t_i P + h_{S_i}$ $(t_i \in Z_q^*)$,然后输出 (U_i, V_i) 作为代理签名询问的输出.

输出算法:

完成上述所有询问后, A_{II} 输出 (m, U, V, ID_B),其

中(m, U, V, ID_B)满足 $e(V, P_B) = e(U, P) = e(hH, P_A)$.

如果 $ID_B \neq ID_{Bj}$, C 宣告失败. 否则, C 运用文献中的方法输出对相同的消息 m 的另外一个签名,这个签名与 A_{II}输出的签名(m, U, V, ID_B)相比有不同的 U 和 h,记作 U^*和 h^*. 根据对消息 m 的两个不同的签名, C 能够计算出,从而解决了 CDH 数学难题,故我们可得到攻击者 A_{II}无法伪造本文提出方案的代理签名. $abP = (h - h^*)^{-1}(U^* - U)$ 计算过程如下:

因为

$$U = tP_B, V = tP + haP \Rightarrow U = tP_B = tbP = b(V - haP) = bV - habP$$

$$U^* = tP_B, V = tP + h^* aP \Rightarrow U^* = bV - h^* abP$$

$$U^* - U = (bV - h^* abP) - (bV - habP) = (h - h^*) abP \Rightarrow abP = (h - h^*)^{-1}(U^* - U)$$

5.2.2 基于类型 III 攻击者的不可伪造性

在这一部分中,我们来证明如果类型 III攻击者 A_{III}能够伪造出本文提出方案的代理签名,那么我们可以证明 C 能够利用这个签名伪造出一个 BLS 短签名. 而 BLS 短签名已被证明是安全的,故我们可得到攻击者 A_{III}无法伪造本文提出方案的代理签名.

初始算法:C 选取 $x_A, x_B \in Z_P^*$ 并设原始签名者和代理签名者的公钥分别为: $P_A = x_A P$. C 将(x_B, P_B, P_A)传送给攻击者 A_{III}.

H 询问算法:在这一步骤中, A_{III}至多可以做 q_H 次 H 询问. A_{III}关于(m_ω, ID_{Bi}) $(1 \leq i \leq q_H)$的每一次询问, C 首先检查列表 H-$List$:

a. 如果在列表 H-$List$ 已经存在项$((m_\omega, ID_{Bi}), H_i)$, C 将 H_i 返回给 A_{III}作为$((m_\omega, ID_{Bi}), H_i)$的哈希值.

b. 否则,也就是 A_{III}从来没做过 (m_ω, ID_{Bi}) 的 H 询问. 这时, C 随机选择,满足列表 H-$List$ 中不存在项 $(*, H_i)$. C 将项$((m_\omega, ID_{Bi}), H_i)$添加到列表 H-$List$ 中,并将 H_i 返回给 A_{III}.

h 询问算法:在这一步骤中, A_{III}至多可以做 q_h 次 h 询问. A_{III}关于(m_i, U_i) $(1 \leq i \leq q_h)$的每一次询问, C 首先检查列表 h-$List$:

a. 如果在列表 h-$List$ 已经存在项$((m_i, U_i), h_i)$, C 将 h_i 返回给 A_{III}作为(m_i, U_i)的哈希值.

b. 否则,也就是 A_{III}从来没做过(m_i, U_i) 的 h 询问. 这时, C 随机选择 $h_i \in Z_q^*$,满足列表 h-$List$ 中不存在项$(*, h_i)$. C 将项$((m_i, U_i), hi)$添加到列表 h-$List$ 中,并将 h_i 返回给 A_{III}.

代理签名询问算法:在这一步骤中, A_{III}至多可以做 q_s 次代理签名询问. A_{III}关于(m_i, ID_{Bi}) $(1 \leq i \leq q_s)$的每一次询问, C 首先检查列表 H-$List$ 和 h-$List$:

a. 如果在列表 H-$List$ 已经存在项$((m_w, ID_{Bi}), H_i)$,同时在列表 h-$List$ 也已经存在项$((m_i, U_i), h_i)$,那么 C 直接获得 H_i and h_i.

b. 否则, C 首先运行 H 询问和 h 询问算法. 然后计算 $S_i = x_B^{-1} x_{Ai} H_i$, $U_i = t_i P_B$, $V_i = t_i P + h_i S_i$ $(t_i \in Z_q^*)$, (U_i, V_i),然后输出(Ui, Vi)作为代理签名询问的输出.

输出算法:完成上述所有询问后, A_{III}输出(m, U, V, ID_B),其中(m, U, V, ID_B)满足 $e(V, P_B) = e(U, P)\, e(hH, P_A)$.

C 利用 A_{III}输出的这个代理签名(m, U, V, ID_B),在不知道 x_A 的情况下能够计算出

$S' = h^{-1}(x_B V - U)$,

满足

$e(S', P) = e(H, P_A)$,

因为:

$$\begin{aligned} e(S', P) &= e(h^{-1}(x_B V - U), P) \\ &= e(h^{-1} x_B V, P)\, e(-h^{-1} U, P) \\ &= e(h^{-1} V, P_B)\, e(-h^{-1} U, P) \\ &= e(V, P_B)^{h^{-1}}\, e(-h^{-1} U, P) \\ &= e(U, P)^{h^{-1}}\, e(hH, P_A)^{h^{-1}}\, e(h^{-1} U, P) \\ &= e(U, P)^{h^{-1}}\, e(H, P_A)\, e(-h^{-1} U, P) \\ &= e(H, P_A) \end{aligned}$$

从上式很容易可以看出 $S' = x_A H$,即 $S' = x_A H(m_\omega, ID_B)$,这个式子与 BLS 短签名实质上是相同的. 也就是说, C 能够利用 A_{II}输出的本文提出方案的代理签名伪造出一个 BLS 短签名. 而 BLS 短签名已被证明是安全的,故我们可得到攻击者 A_{III}无法伪造本文提出方案的代理签名.

6 小结

本文首先给出了代理签名方案的形式化定义以及代理签名方案的攻击模型,然后提出了一个代理签名方案,并证明在代理签名的攻击模型下本方案是可证安全的. 本文还将提出的方案与文献[7]中的代理签名方案的效率进行比较,说明了本方案具有更好的实用性.

参考文献:

[1] H M Sun. Design of Time-Stamped Proxy Signatures with Traceable Receivers[J]. IEEE Proc Computers & Digital Techniques, 2000, 147(6): 462 - 466.

[2] J Li, Z Cao, Y Zhang. Improvement of M-U-O and K-P-W Proxy Signature Schemes[J]. Journal of Harbin Institute of Technology, 2002, 9(2): 145 - 148.

[3] F Zhang, K Kim. Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings[A]. ACISP 2003[C]. Berlin: Springer-Verlag, LNCS 2727, 2003: 312 - 323.

[4] K Zhang. Threshold Proxy Signature Schemes[A]. 1997 Information Security Workshop[C]. Japan: Academic Press, 1997, 191 - 197.

[5] L Yi, G Bai, G Xiao. Proxy multi-signature scheme: A new type of proxy signature scheme[J]. Electron Lett, 2000, 36(6): 527 - 528.

[6] R Lu, Z Cao. Designated Verifier Proxy Signature Scheme with Message Recovery[J]. Applied Mathematics and Computation, 2005, 169(7): 1237 - 1246

[7] F Zhang, R Safavi-Naini, C Lin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings[R]. Cryptology ePrint Archive, 2003.

[8] D Boneh, B Lynn, H Shacham. Short Signatures from the Weil Pairing[A]. Advances in Cryptology- ASIACRYPT 2001[C]. Berlin: Springer-Verlag, LNCS 2248, 2001, 514 - 532.

[9] X Huang, Y Mu, W Susilo et al. A Short Proxy Signature Scheme: Efficient Authentication in the Ubiquitous World[A]. Second International Symposium on Ubiquitous Intelligence and Smart Worlds (UISW2005)[C]. Berlin: Springer-Verlag, LNCS 3823, 2005, 480 - 489.

作者简介:

许　峰　男,1975 年生于陕西,博士研究生,研究方向为信息安全.
E-mail: njxufeng@163.com

崔　隽　男,1981 年生于江苏,博士研究生,研究方向为信息安全.
E-mail: ctops@sina.com

黄　皓　男,1957 年生于福建,南京大学教授、博士生导师,研究方向为信息安全和计算机网络.
E-mail: hhuang@nju.edu.cn