

一个可证明安全的代理签名方案

李 进, 王燕鸣

(中山大学数学与计算科学学院, 广州 510275)

摘 要: 代理签名是一方将自己签名的能力授权给另一方, 是一种很重要的密码协议, 目前已知的可证明安全的代理签名还很少。该文利用间隙 Diffie-Hellman(GDH)群的特点构造了一个新的代理签名方案, 新方案在随机预言模型下是可证明安全的。

关键词: 代理签名; 可证明安全性; GDH 群; 随机预言模型

A Provably Secure Proxy Signature Scheme

LI Jin, WANG Yanming

(School of Mathematics & Computational Science, SUN Yat-sen University, Guangzhou 510275)

【Abstract】 The paradigm of proxy signature is a method for an entity to delegate signing capabilities to other participants so that they can sign on behalf of the entity. Proxy signature is an important cryptographic protocol, however, there are only few provable secure proxy signature schemes. In this paper, a new provably secure proxy signature scheme based on Gap Diffie-Hellman (GDH) group is proposed.

【Key words】 Proxy signature; Provable security; GDH group; Random oracle model

所谓代理签名就是签名一方将自己的某些权力委托给代理人, 让代理人代表本人去对某些文件进行签名。1996年, Mambo、Usuda 和Okamoto等人^[1]第一次提出了代理签名的概念。代理签名在实际应用中起着重要作用^[2,3], 所以代理签名一提出便受到广泛关注, 迄今为止, 人们已提出了多种代理签名方案, 如门限代理签名方案、盲代理签名方案、一次性代理签名方案等^[3]。目前, 很多的代理签名方案被提出, 然而绝大部分方案中缺乏安全性证明, 因此很多方案在后来都被发现存在各种问题^[4]。造成这种局面的一个很重要的因素是代理签名的安全模型一直没有被提出, 直到2003年, Boldyreva等人^[5]第一次给出了代理签名, 详细地定义并且给出了安全模型。在文献^[5]中, Boldyreva等人不但给出了代理签名的安全定义, 同时也定义了攻击者具备的攻击能力以及攻击者的目标, 在这个安全模型下他们也提出了一个能够证明安全的代理签名方案, 然而效率不高。代理签名是在公钥基础设施下(PKI)构建的, 每个用户都有自己注册的公钥, 在代理签名中, 用户原有的私钥可以用来代理授权, 也可以用来进行标准的签名。本文提出了一个可证明安全的代理签名方案, 在文章的最后将给出详细的证明过程。新方案代理签名效率很高, 同时它产生的代理签名非常短, 新代理签名方案的另一个优点是在代理证书发放过程中不需要安全的通信信道。

1 代理签名的定义和性质

定义 1(代理签名体制) 一个代理签名体制是八元组 $(G, S, V, (D, P), PS, PV, ID)$, 每个算法过程如下:

(1) (G, S, V) 是一个标准的签名算法, 其中 G 是密钥生成算法, S 是签名算法, V 是签名的验证算法;

(2) (D, P) 是原始签名者和代理签名者之间的一个交互算法, 通过这个算法, 代理签名者获得授权证书和代理签名的私钥。

(3) PS 是一个代理签名算法, 代理签名者使用代理私钥进

行代理签名。

(4) PV 是一个代理签名验证算法, 算法的输入是原始签名者和代理签名者的公钥以及文件判断代理签名的正确性。

(5) ID 是一个鉴别算法, 给定一个有效的代理签名, 任何验证者都能判断代理签名者身份。

1996年, Mambo、Usuda 和Okamoto^[1]提出了代理签名的概念和需要满足的性质, 随后 Lee、Kim和Kim^[2]对其作了一些改进和补充, 指出代理签名方案应满足以下6条性质: 不可伪造性, 不可否认性, 可验证性, 防止滥用, 可区分性, 可识别性。

Mambo、Usuda 和Okamoto^[1]把代理签名分为3大类: 完全代理签名, 部分代理签名和具有证书的代理签名。由于完全代理签名中原签名者需要将自己的密钥给代理签名者, 因此代理签名者拥有和原始签名人相同的权利, 很多情况下是不适用的。而对于后面两种代理签名, 因为原始签名者和代理签名者拥有的权利和责任是可区分的, 因此主要研究都是从这两方面进行。本文的方案是第3种, 即具有证书的代理签名方案。

在文献^[5]中, 代理签名的攻击者模型如下: 攻击者在攻击过程中拥有两个应答机 (oracle): 一个是标准签名的应答机, 另一个是代理签名的应答机。类似于文献^[5], 为说明方便, 本文始终假定攻击目标用户为用户1, 第1种应答机下, 攻击者选择明文 m 给标准签名的应答机得到用户1对明文 m 的标准签名; 在代理签名应答机模型下, 攻击者可以得到用户1代理用户 i 的代理签名。在询问结束之后, 攻击者输出如下3种结果中任何一种都是攻击成功。

基金项目: 国家自然科学基金资助项目(10271119)

作者简介: 李 进(1981-), 男, 博士, 主研方向: 密码学; 王燕鸣, 教授、博导

收稿日期: 2005-11-30 **E-mail:** sysjinli@yahoo.com.cn

(1) 伪造用户 1 的对文件 M 的标准签名, 其中文件 M 在标准签名应答中攻击者未曾询问过其签名;

(2) 伪造用户 1 未曾授权过的用户 i 的代理签名或者用户 i 有用户 1 的授权证书 m_{ω} , 但是伪造了用户 1 未曾授权用户 i 的另一个授权证书 m'_{ω} 的代理签名;

(3) 伪造用户 1 代理用户 i 的关于文件 M 的代理签名, 其中文件 M 在代理签名应答中攻击者未曾询问过其相应的代理签名(i 可以等于 1, 即用户 1 的自我代理签名)。

关于代理签名安全模型更为详尽的论述可以参考文献[5]。

2 双线性对

在这一节, 将简要介绍双线性对的基础知识。设 G_1 和 G_2 是两个阶为 p 的循环群, p 为大素数。在 G_1 中群元素运算定义为加法, G_2 中元素运算为乘法运算, 然后定义双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足以下性质。

(1) 双线性: $e(aP, bQ) = e(P, Q)^{ab}$, 对 $\forall P, Q \in G_1, \forall a, b \in Z_p$ 成立;

(2) 非退化性: $\exists P, Q \in G_1$, 使 $e(P, Q) \neq 1$;

(3) 可计算性: 存在一个有效算法计算 $e(P, Q)$, 对 $\forall P, Q \in G_1$ 。

下面描述椭圆曲线上的数学问题:

(1) 离散对数问题(DLP): 给定 G_1 中的两个元素 P, Q , 计算整数 n , 使 $Q = nP$;

(2) 计算离散对数问题(CDHP): 对 $a, b \in Z_p^*$, 给定 G_1 中元素 P, aP, bP , 计算 abP ;

(3) 决策离散对数问题(DDHP): 对 $a, b, c \in Z_p^*$, 给定 G_1 中元素 P, aP, bP, cP , 判断是否 $c \equiv ab \pmod{p}$;

如果在一个群 G 中, DDHP 容易求解而 CDHP 仍是困难问题, 则称这样的群 G 为间隙群(Gap Diffie-Hellman group, GDH 群)。很易看出, GDH 群可以从双线性对构造出来。

介绍一个困难问题, 称为 q -Strong Diffie-Hellman (q -SDH)。

定义 1(q -SDH) 给定 $P, xP, x^2P, \dots, x^qP \in G_1$, 输出 $(h, \frac{1}{h+x}P)$, $h \in Z_p^*$ 。

q -SDH 假设是指多项式时间中没有算法能以不可忽略概率解决 q -SDH 问题。

当 $q=1$ 时, 很容易可验证 q -SDH 问题等价于 CDH 问题。

3 一个安全的代理签名方案

在这一节中, 将利用双线性对构造一个新的可证明安全的代理签名方案。代理签名中一般包含两方: 原始签名人和代理签名人。类似于文献[5], 为了区分标准签名和代理签名, 用 $H_1(M)$ 表示对文件 M 的标准签名, 用 $H_1(M)$ 表示代理授权, 其中 M 为授权信息。原始签名者在开始代理授权之前先准备授权文件 m_{ω} , 其中包含代理人信息如代理签名人公钥以及代理签名的文件类型, 时间等信息。代理签名方案由以下算法构成。

系统参数设置: 设 $(G_1, +)$ 和 (G_2, \times) 两个阶为 p 的循环群, p 为大素数, P 为 G_1 的生成元。定义 G_1 上的一个双线性映

射 $e: G_1 \times G_1 \rightarrow G_2$, 同时定义两个哈希函数 $H_1: \{0,1\}^* \rightarrow G_1, H_2: \{0,1\}^* \rightarrow Z_p^*$;

(1) 密钥生成算法(G): 假设 A 和 B 分别选择私钥 x_A 和 x_B 注册并公布其相应公钥为 $PK_A = x_A P, PK_B = x_B P$;

(2) 标准签名算法(S): 给定用户 A 的私钥和需要签署的文件 M, 输出标准签名为 $\sigma_A = x_A H_1(H_1(M))$;

(3) 标准签名验证算法(V): 给定用户 A 的公钥 PK_A , 文件 M 以及标准签名 σ_A , 验证等式 $e(\sigma_A, P) = e(H_1(H_1(M)), PK_A)$ 是否成立。若成立, 则 σ_A 是一个有效签名; 否则无效;

(4) 代理授权算法(D): 假定 A 要授权 B 为其进行代理签名, 则 A 首先计算一个授权文件 m_{ω} , 然后计算 $S_{\omega} = x_A H_1(H_1(m_{\omega}))$ 作为授权证书(授权证书传送给 B 时可以公开, 不需要秘密信道);

(5) 代理密钥生成算法(P): B 得到授权证书 S_{ω} 后, 生成代理用户 A 的代理密钥为 (x_B, S_{ω}) ;

(6) 代理签名产生算法(PS): B 如果要对文件 M 进行代理签名, B 首先选择 $r \in_R Z_p^*$, 计算 $U = rH_1(H_1(m_{\omega}))$, 最后计算 $V = \frac{r + H_2(m, U)}{x_B + m} S_{\omega}$, 则代理签名为 (U, V) ;

(7) 代理签名验证算法(PV): 任何人给定文件 M, PK_A, PK_B 和 m_{ω} 以及代理签名 (U, V) , 验证等式 $e(V, PK_B + mP) = e(U + H_2(m, U), PK_A)$ 是否成立, 其中 $H_2(m, U) = h$ 。若等式成立, 则表示签名有效; 否则为无效签名;

(8) 鉴别算法(ID): 给定明文 M 及验证信息 PK_A, PK_B 和 m_{ω} 以及代理签名 (U, V) , 可以很容易确定代理签名者为用户 B。

正确性分析 如果 (U, V) 是一个正确的代理签名, 则

$$V = \frac{r + H_2(m, U)}{x_B + m} S_{\omega}, \text{ 从而 } e(V, PK_B + mP) = e\left(\frac{r + H_2(m, U)}{x_B + m} S_{\omega}, PK_B + mP\right)$$

$$= e((r + H_2(m, U))x_A H_1(H_1(m_{\omega})), P)$$

$$= e(U + H_2(m, U)H_1(H_1(m_{\omega})), PK_A)$$

效率分析 在这个代理签名算法中, 代理签名的产生需要两次点乘运算和一次 Z_p^* 中的求逆运算, 而其中 U 的运算可以离线进行, 从而在线运算只需要一次点乘和一次 Z_p^* 中的求逆运算, 代理签名的验证算法需要两次双线性对运算。本文的另一个优点是代理签名长度很短: 代理签名是群 G_1 中的两个元素, 利用点压缩技术, 每个元素的表示只需要 160 位, 从而代理签名的长度为 320 位 相对以前基于 RSA 或者 Z_p^* 离散对数难题构造的代理签名长度都要短很多。且在新代理签名中不需要安全的通信信道来进行代理授权证书的发放。

安全性分析 对于这个代理签名方案的安全性, 可以得出

如下的结论：

定理 1 如果CDH困难假设在 G_1 中成立,那么在自适应选择明文和选择授权攻击下,新的代理签名方案就是安全的。

证明 使用反证法,假设有一个攻击者A以不可忽略的概率成功伪造代理签名,就可以构造一个算法B使CDH困难假设在 G_1 不成立。首先给定B任意的 P, xP, yP ,求 xyP 或者 $\frac{1}{x+h}P$,其中 $h \in Z_p^*$,很容易验证这个问题等价于CDH问题。

B首先令 $pk_1 = xP$ 为用户1的公钥并传送给攻击者A,然后回答A的如下询问：

(H_1 询问)：假设攻击者最多询问 q_{H_1} 次哈希 H_1 值询问, B首先选择一个 $k \in [1, q_{H_1}]$,当A在第 i 次询问 $H_1(M_i)$ 或者 $H_1(00 \parallel M_i)$ 相应的 H_1 值时, B回答 $H_1(11 \parallel M_i)$ 或者 $H_1(00 \parallel M_i) = a_i P$ 。当 $i \neq k$ 时,其中 $a_i \in Z_p^*$;否则当 $i = k$ 时,回答 $H_1(11 \parallel M_k)$ 或者 $H_1(00 \parallel M_k) = yP$;

(H_2 询问)：假设攻击者最多询问 q_{H_2} 次 H_2 值询问,当A提交 M_i 询问相应的 H_2 值时, B选择 $b_i \in Z_p^*$ 并回答 $H_2(M_i) = b_i$;

(用户 i 注册 pk_i)：当攻击者A要注册一个新用户 i 时,给定值 (pk_i, sk_i) , B验证 sk_i 确实是 pk_i 对应的私钥并将其存储;

(用户1授权给用户 i)：当攻击者要求用户1给用户 i 代理授权时, B首先计算一个授权文件 m_{oi1} ,假设 $H_1(00 \parallel m_{oi1}) = a_j P$,从而B计算一个模拟授权证书为 $xH_1(00 \parallel m_{oi1}) = a_j pk_1$;

(用户 i 授权给用户1)：当攻击者A扮演用户 i 给用户1代理授权时, A首先计算一个授权文件 m_{oi1} 并假设 $H_1(00 \parallel m_{oi1}) = a_s P$,则授权证书可以计算为 $sk_i \times H_1(00 \parallel m_{oi1}) = a_s pk_i$;

(用户1自我授权)：当攻击者要求用户1自我授权时,用户1首先计算一个授权文件 m_{oi1} 并假设 $H_1(00 \parallel m_{oi1}) = a_t P$,则B计算一个模拟授权证书为 $xH_1(00 \parallel m_{oi1}) = a_t pk_1$;

(用户1标准签名)：当攻击者A询问文件M的标准签名时,假设 $H_1(11 \parallel M) = a_u P$,则模拟标准签名为 $xH_1(11 \parallel M) = a_u pk_1$;

(用户1代理用户 i 的代理签名)：B可以如下模拟文件M的代理签名：选择 $r, h \in_R Z_p^*$,计算 $U = -h \times H_1(00 \parallel m_{oi1}) + r \times (pk_i + MP)$, $V = r \times pk_i$,令 $h = H_2(m, U)$,很容易验证 (U, V) 是对M的代理签名,这是因为将 (U, V) 代入可以使验证等式 $e(V, pk_i + mP) = e(U + hH_1(00 \parallel m_{oi1}), pk_i)$ 成立;

完成上述模拟过程以后,如果A以不可忽略的概率伪造

了一个代理签名,那么至少下面3种情况的1种将会发生：

(1)成功伪造用户1的标准签名;

(2)成功伪造一个用户1没有发放相应授权证书的用户 i 的代理签名;

(3)成功伪造一个用户1代理用户 i 的代理签名。

下面说明以上3种情况的任何1种都可以用来解决CDH困难问题：

如果第(1)种情况发生,也就是说攻击者成功伪造了用户1的一个对新文件M的标准签名 $\sigma' = xH_1(11 \parallel M)$,因为攻击者必定询问过 $H_1(11 \parallel M)$ 的值,如果刚好 $H_1(11 \parallel M) = yP$ (概率是 $\frac{1}{q_{H_1}}$),则 $\sigma' = xyP$,从而B解决了CDH困难问题;

如果第(2)种情况发生,也就是说攻击者成功伪造了用户1的没有发放相应授权证书用户 i 的代理签名 (U, V) ,使等式 $e(V, pk_i + mP) = e(U + hH_1(00 \parallel m_{oi1}), pk_i)$ 成立,其中

$h = H_2(m, U)$,则 $V = \frac{r + H_2(m, U)}{sk_i + m} \times xH_1(00 \parallel m_{oi1})$,利用

哈希函数回放攻击的方法,提供攻击者不同的 H_2, H_2' ,使 $H_2(m, U) = h$ 以及 $H_2'(m, U) = h'$,从而可以得到 m 的另一个

有效代理签名 (U, V') ,其中 $V' = \frac{r + H_2'(m, U)}{sk_i + m} \times xH_1(00$

$\parallel m_{oi1})$,可以求出 $V - V' = \frac{h - h'}{sk_i + m} \times xH_1(00 \parallel m_{oi1})$,由于B

在用户 i 注册时保存了 sk_i 的值,因此 $xH_1(00 \parallel m_{oi1}) = \frac{sk_i + m}{h - h'} \times (V - V')$,如果刚好 $H_1(00 \parallel m_{oi1}) = yP$ (概率仍是 $\frac{1}{q_{H_1}}$),

则 $xH_1(00 \parallel m_{oi1}) = xyP$,从而B解决了CDH困难问题;

如果第3种情况发生,也就是说攻击者成功伪造了用户1代理用户 i 对文件 m 的代理签名 (U, V) ,满足 $e(V, pk_i + mP) = e(U + hH_1(00 \parallel m_{oi1}), pk_i)$,其中 $h = H_2(m, U)$,则

$V = \frac{r + H_2(m, U)}{x + m} \times sk_i \times H_1(00 \parallel m_{oi1})$,同样利用哈希函数

回放攻击的方法,提供攻击者不同的 H_2, H_2' ,使 $H_2(m, U) = h$ 以及 $H_2'(m, U) = h'$,从而可以得到 m 的另一个有效代理

签名 (U, V') ,其中 $V' = \frac{r + H_2'(m, U)}{x + m} \times sk_i \times H_1(00 \parallel m_{oi1})$,

那么此时B可以利用和上面情况一样的方法首先求出

$V - V' = \frac{h - h'}{x + m} \times sk_i \times H_1(00 \parallel m_{oi1})$,则 $\frac{1}{x + m} P =$

$\frac{1}{sk_i \times (h - h') \times a_i} \times (V - V')$,其中 $H_1(00 \parallel m_{oi1}) = a_i P$,

从而解决1-SDH困难问题,而1-SDH困难问题等价于CDH困难问题,从而也就解决了CDH困难问题。

综合上述3种情况可以得出以下结论:如果A以不可忽

(下转第 21 页)