# 基于双线性对的前向安全短门限代理签名方案

肖 鹏[1,2],毛 明[2],张艳硕[2]
XIAO Peng[1,2],MAO Ming[2],ZHANG Yan-shuo[2]

1.西安电子科技大学 通信工程学院,西安 710071
2.北京电子科技学院,北京 100070
1.Department of Communication Engineering,Xidian University,Xi'an 710071,China
2.Beijing Electronic Science and Technology Institute,Beijing 100070,China
E-mail:luolanjuban@163.com

**XIAO Peng,MAO Ming,ZHANG Yan-shuo.Forward secure short threshold proxy signature scheme from bilinear pairing.Computer Engineering and Applications,2009,45(24):84-86.**

**Abstract:** A forward secure short threshold proxy signature scheme from bilinear pairing is proposed by combining the concept of forward security with threshold signature from bilinear pairing.In this scheme,the key updating algorithm is used by the original signer,so the security of the proxy signature key is promoted to a higher level.The performance of the scheme is also analyzed,and it is shown that this proposed scheme is secure and effective.

**Key words:** bilinear pairing;forward secure;short signature;threshold signature;proxy signature

**摘 要:**将前向安全的概念结合到基于双线性对的门限签名方案中,提出了一个基于双线性对的前向安全短门限代理签名方案。该方案将密钥更新算法应用在原始签名者计算过程中,更有效增强了代理签名密钥的安全性。对该方案的性能进行了分析,表明该方案是安全有效的。

**关键词:**双线性对;前向安全;短签名;门限签名;代理签名
**DOI:**10.3778/j.issn.1002-8331.2009.24.026 **文章编号:**1002-8331(2009)24-0084-03 **文献标识码:**A **中图分类号:**TP309

## 1 引言

Boneh,Lynn 和 Shacham[1]在 2001 年的亚密会上使用双线性对构造了一种短签名方案(BLS),生成的签名在相同的安全水平下长度是 DSA 签名的一半,且在经典密码中是签名长度最短的签名方案,这为数字签名开辟了一个新的研究领域。短签名的应用范围比较广泛,当要求人工秘密输入数字签名时,就需要用到短签名,如产品注册系统常常要求用户在 CD 标签上提供一个秘密的嵌入签名;更一般地,在低带宽通信环境中也需要用到短签名。

随着代理签名的发展,门限代理签名受到了广泛的关注[2-4]。$(t,n)$门限代理签名是代理签名的一种变形,门限代理签名私钥由 $n$ 个代理签名者分享保存,只有 $t$ 个或更多个代理签名者代表原始签名者使用各自拥有的部分密钥共同产生最终的签名结果,任何少于 $t$ 个都无法恢复密钥或者计算正确的签名结果[4]。

门限数字签名的安全性很大程度上都取决于签名密钥的安全性,将签名密钥定期更新,并结合前向安全算法。以往的前向安全代理签名方案中,如 WCF 方案[5]、TL 方案[6]等,都是更新代理签名者的代理密钥,此密钥都是由原始签名者的私钥产生,如果一旦原始签名者的私钥泄露,无论代理签名者的代理密钥是否单向进化,攻击者都有可能伪造或盗取代理密钥以伪造代理签名。因此,根据文献[4],将具有前向安全的密钥更新算法引入到原始签名者的计算过程中,提出了一种基于双线性对的前向安全短门限代理签名方案。

## 2 预备知识

### 2.1 双线性对

双线性对是指两个循环群之间相对的线性映射关系。设 $G_1$ 是一个加法群,阶是大素数 $q$。$G_2$ 是一个乘法群,也以 $q$ 为阶。双线性映射 $e:G_1\times G_1\rightarrow G_2$ 满足如下特性:

(1)双线性:$\forall P,Q,R\in G_1,a,b\in Z,e(P+Q,R)=e(P,R)\cdot e(Q,R),e(P,Q+R)=e(P,Q)e(P,R),e(aP,bQ)=e(P,Q)^{ab}$;

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

**基金项目:**北京市教改立项网络对抗实验平台(the Network Confrontation Experimental Platform Projected by Beijing Municipal Education Reform);北京电子科技学院信息安全与保密重点实验室(the Foundation of Beijing Electronic Science and Technology Institute's Information Security and Confidentiality Key Laboratory under Grant No.YZDJ0712)。

**作者简介:**肖鹏(1984-),女,硕士研究生,主要研究领域为信息安全、密码学;毛明(1963-),男,教授,主要研究领域为信息安全、密码学;张艳硕(1979-),男,博士研究生,讲师,主要研究领域为密码学和编码学。

**收稿日期:**2008-05-07 **修回日期:**2008-08-31

(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 $e(P,Q)$。

### 2.2　GDH(Gap Diffie-Hellman)群

假设 $G$ 是一个椭圆曲线上的 $q$ 阶的加法群,$q$ 为大素数。以下是几个基于 $G$ 的困难问题:

(1)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 $Q=nP$。

(2)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。

(3)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。

### 2.3　前向安全的数字签名方案

前向安全的概念最早是由 Anderson 首先提出的[7],Bellare 和 Miner 第一次给出了前向安全签名的正式定义,并基于 A.Fiat 和 A.Shamir 的签名方案[8]给出了两个前向签名方案[9]。其基本思想是把一对公钥和私钥的有效期分为若干个时间段,用于验证签名的公钥保持不变,而私钥是由单向函数和前一时间段的私钥产生。这样,每一时间段的签名私钥都互不相同,并且每一次签名后都把上一次的密钥删除,使得攻击者即使窃取到当前时间段的私钥也无法伪造过去时间段里的签名,从而减少密钥泄露带来的威胁。

将前向安全的概念结合到门限代理签名方案中,并将密钥更新引入在原始签名者计算过程中,有效的保证了最终代理签名的安全性。

## 3　基于双线性对的前向安全短门限代理签名方案

### 3.1　系统初始化

给定安全参数 $k$,群 $G_1$ 和 $G_2$ 的阶数为素数 $q$,$P$ 是 GDH 群 $G_1$ 的生成元,$e:G_1\times G_1\to G_2$ 是一个安全的双线性对映射。选取两个相同值域的 hash 函数 $H_1,H_2:\{0,1\}^*\to G_1$,并且输出公共系统参数$\{G_1,G_2,P,q,H_1,H_2\}$。

### 3.2　密钥生成

给定安全参数 $k$,算法生成 $n+1$ 个签名者 $P_0,P_1,P_2,\cdots,P_n$ 的公私钥对。签名者选取 $x_i\in Z_q^*(i=0,1,2,\cdots,n)$作为其私钥,计算 $Y_i=x_iP$ 作为其公钥。其中,$P_0$ 是原始签名者,$P_1,P_2,\cdots,P_n$ 是 $n$ 个代理签名者。

### 3.3　代理签名权授予

(1)代理组生成

原始签名者 $P_0$ 指定 $n$ 个人 $P_1,P_2,\cdots,P_n$ 作为代理签名者,他们构成代理组$\{P_1,P_2,\cdots,P_n\}$。

第一步,代理签名者 $P_i$ 随机选取系数在 $Z_q$ 中 $t-1$ 次多项式 $f_i(z)$:

$$f_i(z)=x_i+\alpha_{i,1}z+\alpha_{i,2}z^2+\cdots+\alpha_{i,t-1}z^{t-1} \bmod q$$

其中,$x_i$ 是代理签名者 $P_i$ 的私钥,且该多项式满足 $f_i(0)=x_i$,$f(0)=\sum_{i=1}^{n}x_i$。之后 $P_i$ 计算并广播 $\alpha_{i,j}P(j=1,2,\cdots,t-1)$。最后将 $f_i(j)$秘密地发送给其他代理签名人 $P_j(j=1,2,\cdots,n;j\neq i)$。

第二步,代理签名者 $P_i$ 从其他代理签名者 $P_j$ 那里收到 $f_j(i)$ 后$(j=1,2,\cdots,n;j\neq i)$,通过下面的式子来验证 $f_j(i)$ 的有效性:

$$f_j(i)P=Y_j+\sum_{k=1}^{t-1}i^k\alpha_{j,k}P,\ \ Y_j=x_jP$$

如未通过验证,$P_i$ 指出 $P_j$ 给出的数据无效,要求重发。若通过验证,代理签名者 $P_i$ 计算 $x_i'=\sum_{k=1}^{n}f_k(i)$,$Y_i'=x_i'P$,并广播 $Y_i'$。

(2)代理密钥生成

原始签名者 $P_0$ 首先生成一个授权委托证书 $m_w$,它详细描述了原始签名者对代理签名者的授权关系,包括必要的授权信息,如原始签名者和代理组的身份,授权范围和有效时限等等。

然后 $P_0$ 选取 $r_0\in Z_q^*$,计算 $\beta_0=(x_0+r_0)H_1(m_w)$。$\beta_0$ 即为代理密钥更新初始阶段的值。

签名进入第 $L$ 时段,原始签名者 $P_0$ 利用第 $L-1$ 时段的 $\beta_{L-1}$ 计算第 $L$ 时段的 $\beta_L$:

$P_0$ 选取 $r_L\in Z_q^*$,计算 $\beta_L=\beta_{L-1}+r_LH_1(m_w)=H_1(m_w)\left(x_0+\sum_{i=0}^{L}r_i\right)$,$T=\sum_{i=0}^{L}r_LP$ 并发送$(\beta_L,m_w,T)$给代理组$\{P_1,P_2,\cdots,P_n\}$。之后立即删除 $r_L$ 和 $\beta_{L-1}$。

每个代理签名者 $P_i$ 计算 $e(\beta_L,P)=e(H_1(m_w),T+Y_0)$是否成立,来验证 $P_0$ 发送的信息是否有效。验证通过,那么代理签名者 $P_i$ 的代理签名私钥就是$(\beta_L,x_i')$。

### 3.4　代理签名生成

代理组$\{P_1,P_2,\cdots,P_n\}$代表原始签名者 $P_0$ 签名时,设 $P_1,P_2,P_3,\cdots,P_t$ 为 $t$ 个实际的代理签名者对消息 $m$ 进行签名。

第一步,每个代理签名者 $P_i(i=1,2,3,\cdots,t)$先计算 $\omega_i=\prod_{j\in\{1,2,\cdots,t\},j\neq i}\frac{j}{j-i}$,再用自己的代理私钥 $x_i'$对消息 $m$ 进行签名,得到消息 $m$ 的部分签名 $\sigma_i=x_i'\omega_iH_2(m\parallel m_w)$。

第二步,$t$ 个代理签名者收集完所有部分签名 $\sigma_i$ 后,对其用以下等式一一验证其有效性:

$$e(\sigma_i,P)=e(\omega_iY_i',H_2(m\parallel m_w))$$

若上式不成立,则说明 $P_i$ 没有给出他的正确的部分签名 $\sigma_i$,或者 $P_i$ 是一个欺诈者,要求他重新发送或者另找其他的代理签名者重做。

第三步,所有的部分签名均通过验证后,代理签名者 $P_i(i=1,2,3,\cdots,t)$合作计算产生 $\sigma=\beta_L+\sum_{i=1}^{t}\sigma_i$,于是完整有效的代理签名为$<m,m_w,\sigma,L,T>$。

### 3.5　代理签名验证

任何人都可以通过以下方程验证代理签名的有效性。

$$e(\sigma,P)=e(H_1(m_w),T+Y_0)e\left(H_2(m\parallel m_w),\sum_{i=1}^{n}Y_i\right)$$

如果等式成立,则签名是合法有效的,否则就予以拒绝。

## 4 方案的性能分析

### 4.1 安全性

(1)签名<$m,m_w,\sigma,L,T$>的正确有效性

$$e(\sigma,P)=e\left(\beta_L+\sum_{i=1}^{t}\sigma_i,P\right)=e(\beta_L,P)e\left(\sum_{i=1}^{t}\sigma_i,P\right)=$$

$$e(\beta_L,P)e\left(\sum_{i=1}^{t}x_i'\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}H_2(m\parallel m_w),P\right)=$$

$$e\left(H_1(m_w)\left(x_0+\sum_{i=0}^{L}r_i\right),P\right)e(f(0)H_2(m\parallel m_w),P)=$$

$$e\left(H_1(m_w)\left(x_0+\sum_{i=0}^{L}r_i\right),P\right)e(\sum_{i=1}^{n}x_iH_2(m\parallel m_w),P)=$$

$$e\left(H_1(m_w),\left(x_0+\sum_{i=0}^{L}r_i\right)P\right)e\left(H_2(m\parallel m_w),\sum_{i=1}^{n}x_iP\right)=$$

$$e(H_1(m_w),T+Y_0)e\left(H_2(m\parallel m_w),\sum_{i=1}^{n}Y_i\right)$$

(2)强不可伪造性

因为选取的 $G$ 是 GDH 群,在 $G$ 上的 CDH 问题是难解的,所以任何人在不知道原始签名者 $P_0$ 私钥 $x_0$ 的情况下,不能够计算出 $\beta_0$,也就无法生成代理签名私钥中的 $\beta_L$ 来伪造代理签名;同时,攻击者或者原始签名者 $P_0$ 都不能冒充代理签名者 $P_i$ 对消息 $m$ 伪造代理签名,同样是因为代理签名私钥中的 $x_i'$ 是由 $P_i$ 他们各自的私钥 $x_i$ 生成。

(3)可区分性

因为完整有效的代理签名中有授权证书 $m_w$,而且签名验证的过程中同时出现了原始签名者 $P_0$ 的公钥 $Y_0$、代理签名者 $P_i$ 的公钥 $Y_i$ 和证书 $m_w$,故有效地区分了签名权和代理权。

(4)强不可抵赖性

对消息 $m$ 完整有效的签名<$m,m_w,\sigma,L,T$>中包含了授权证书 $m_w$,并且在验证过程中用到 $m_w$、原始签名者和代理签名者的公钥,而代理签名者 $P_i$ 不能更改 $m_w$,故代理签名者 $P_i$ 一旦产生了代理签名,他就不能够否认所产生的签名,具有强抗抵赖性。

(5)身份证实性(可识别性)

原始签名者 $P_0$ 可以通过验证方程来确定代理签名者的身份是 $P_i$,也就是说原始签名者可以根据此有效的代理签名确定出相应的代理签名者的身份,具有身份证实性。

(6)密钥依赖性

代理签名私钥($\beta_L,x_i'$)中的 $\beta_L$ 是由原始签名者 $P_0$ 的秘密密钥 $x_0$ 生成的 $\beta_0$ 产生的,所以方案具备了密钥依赖性。

(7)可注销性

授权委托证书 $m_w$ 指出签名的权限和时限,只允许代理签名者在一定时间内拥有代理签名的能力,代理密钥只在规定的时间内有效。

(8)可验证性

任何验证签名的人都可以验证代理签名是否有效,并且根据有效的代理签名中的授权证书 $m_w$ 能够确认原始签名者认同了这份签名消息。

(9)前向安全性

在代理密钥生成之初,原始签名者可以通过随机选取 $r_L$ 来控制代理签名私钥 $\beta_L$ 的更新,这个随机数的选取不会受时间周期的影响,与总的时间周期无关,代理签名私钥可以不受时间周期数量的限制,无限地更新下去。

假定攻击者获得了代理签名者 $P_i$ 在第 $L$ 时段的代理签名私钥 $\beta_L$,要想获得第 $j(j<L)$ 时段的代理签名密钥,他就必须知道 $P_0$ 在 $k=0,1,2,\cdots,j$ 时段所选取的 $r_k$,而 $r_k$ 在每次计算完当时时刻的代理密钥后就删除了,所以攻击者不能通过获得在第 $L$ 时段的代理签名密钥 $\beta_L$ 的方式来伪造第 $j(j<L)$ 时段的代理签名。

(10)门限性

在代理组生成过程中,每个代理签名者 $P_i$ 都会用自己的私钥生成次数为 $t-1$ 的多项式 $f_i(z)$,且之后 $f_i(z)$ 要检验从其他代理人 $P_j$ 那里收到的 $f_j(z)$,因此 $t-1$ 个代理签名者无法进行欺骗或伪造。在代理签名过程中,每个 $P_i$ 产生的部分签名 $\sigma_i$ 也都要一一验证,因此在不多于 $t-1$ 个代理签名者被收买的情况下,攻击者仍然需要从其他签名者那里获取另一个或更多的部分签名,才能伪造产生完整的代理签名。也就是说,只有得到 $t$ 个有效的部分签名,才能生成最终有效的代理签名。

(11)防移动攻击性

在移动攻击模型中,攻击者虽然在某一段时间内只能入侵得到少于 $t$ 个的签名密钥,但他可以在很长一段时间内入侵获得更多,使得到的密钥个数达到并超过门限值 $t$,从而威胁签名密钥的安全。

假设攻击者在第 $i$ 时段窃取到 $r(r<t)$ 个代理签名私钥 $(\beta_i,x_1'),(\beta_i,x_2'),\cdots,(\beta_i,x_r')$,在第 $j$ 时段窃取到 $s(s<t)$ 个代理签名私钥 $(\beta_j,x_1'),(\beta_j,x_2'),\cdots,(\beta_j,x_s')$ 等等,但由于 $\beta_L$ 是不断单向变化更新的,故 $\beta_i$ 与 $\beta_j$ 无法相互得知。也就是说无法得到同一个时间段内超过门限值 $t$ 个代理签名密钥,攻击者不能伪造签名,从而有效的防止了移动攻击。

### 4.2 效率分析

表 1~表 3 分别列举了 SLH 方案[3]和该文方案在代理签名生成及验证过程中效率的比较。

方案是基于椭圆曲线的,因此产生的密钥长度小,且代理

**表 1 产生部分签名 $\sigma_i$ 效率比较**

| 运算 | SLH 方案 | 该文方案 |
|---|---|---|
| 模加 | $t$ | 0 |
| 模乘 | $2(t-1)+2$ | 1 |
| 指数 | $(t-1)(t-2)$ | 0 |
| 求逆 | 0 | 0 |
| 点加 | 无计算 | 0 |
| 数乘 | 无计算 | 1 |
| 配对 | 无计算 | 0 |

**表 2 验证部分签名 $\sigma_i$ 及生成代理签名效率比较**

| 运算 | SLH 方案 | 该文方案 |
|---|---|---|
| 模加 | $t$ | 0 |
| 模乘 | $t(t-1)^2+5t+t(t+1)(n-1)$ | 0 |
| 指数 | $2(t-1)(t-2)t+nt+4t$ | 0 |
| 求逆 | 1 | 0 |
| 点加 | 无计算 | $t+1$ |
| 数乘 | 无计算 | $t+1$ |
| 配对 | 无计算 | $2t$ |

**表 3 验证代理签名效率比较**

| 运算 | SLH 方案 | 该文方案 |
|---|---|---|
| 模加 | 0 | 0 |
| 模乘 | $n+2$ | 0 |
| 指数 | 4 | 0 |
| 求逆 | 0 | 0 |
| 点加 | 无计算 | $n$ |
| 数乘 | 无计算 | 0 |
| 配对 | 无计算 | 3 |

(下转 90 页)