

基于双线性对的门限代理签名方案的研究

刘春刚, 周廷显

(哈尔滨工业大学 通信技术研究所, 黑龙江 哈尔滨 150001)

摘 要: 在一种概率签名方案的基础上进行改进, 构造了基于双线性对的门限代理签名方案. 双线性对又称代数曲线 Weil 对和 Tate 对, 是代数几何研究中一个很重要的工具. 双线性对有很多优点, 如签名较短等. 并且对该方案进行了详细的性能分析, 结论认为, 该方案是一个高效的安全的门限代理签名方案.

关键词: 代理签名; 门限; 双线性对

中图分类号: TN918.1 **文献标识码:** A **文章编号:** 1007-2683(2009)01-0060-03

Research on a Threshold Proxy Signature Scheme Based on Bilinear Pairing

LIU Chun-gang, ZHOU Ting-xian

(Communication Technology Research Institute, Harbin Institute of Technology, Harbin 150001, China)

Abstract: Based on a probability signature scheme, a bilinear-pairing based threshold proxy signature scheme is proposed. Bilinear pairings, namely Weil pairings and Tate pairings, are rather important tools in algebra geometry. Bilinear pairings have lots of merits such as short signatures. And security of the scheme is analyzed. The scheme is secure and efficient.

Key words: proxy signature, threshold, Bilinear-pairing

1 引 言

在现实世界里, 人们有时需要将自己的某项权力委托给一个可靠的代理人, 让代理人代表本人行使该项权力. 其中比较典型的是签名权的委托. 例如, 行政官员外出度假而暂时无法对各种文件进行签名时授权其秘书对某些文件进行签名; 总经理希望部门经理就其部门的某些问题代表他进行签名; 繁忙的高校校长希望办公室主任代替他为合格毕业生签发文凭等.

1996 年 Mambo, Usuda 和 Okamoto^[1-2] 首先引入了代理签名的概念, 给出了解决这类问题的一种

方法. 代理签名是一种新型的数字签名方案, 在一个典型的代理签名方案中, 原始签名者授权代理签名者, 代理签名者代表原始签名者产生一个有效的代理签名, 验证人在验证代理签名有效性的同时验证授权. 随着代理签名的发展, 门限代理签名也受到了广泛的关注^[3-5]. (t, n) 门限代理签名是代理签名的一种变形, 门限代理签名的代理签名私钥由 n 个代理签名者分享保存, 只有 t 个或更多的代理签名者代表原始签名者运用各自的代理签名私钥能产生对消息的签名, 少于 t 个则不可能. 把能鉴别实际签名人的门限代理签名叫作具有不可否认性的门限代理签名. 本文提出了具有同样性质的门限代理签名方案, 并分析其安全性和效率.

2 数学基础

设 $(G_1, +)$ 和 $(G_2, *)$ 是两个阶为 q 的群, q 为一个大素数. 其中, G_1 是加法群, G_2 是乘法群, P 是群 G_1 的生成元. 两个群之间的双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足以下性质:

双线性: 对于 $\forall P, Q, R \in G_1, a, b \in F_q^*$, 有 ① $e(P+Q, R) = e(P, R) e(Q, R)$; ② $e(P, Q+R) = e(P, Q) e(P, R)$; ③ $e(aP, bP) = e(P, P)^{ab}$;

非退化性: 存在 $P, Q \in G_1$, 使得 $e(P, Q)$ 不等于 G_2 的单位元;

可计算性: 对于 $\forall P, Q \in G_1$, 存在高效算法, 可计算出 $e(P, Q)$.

可以用超奇异椭圆曲线上的 Weil 对或经过改造的 Tate 对来构造双线性对.

在上述的群 $(G_1, +)$ 上, 可以定义以下几个密码学问题:

1) 离散对数 (DL) 问题: 给定 $P, P \in G_1$, 找出整数 $n \in Z_q$, 使得 $P = nP$.

2) 计算 Diffie-Hellman (CDH) 问题: 给定三元组 $(P, aP, bP) \in G_1 \times G_1 \times G_1$, 对于 $a, b \in Z_q^*$, 找出 abP .

3) 决定性 Diffie-Hellman (DDH) 问题: 给定四元组 $(P, aP, bP, cP) \in G_1 \times G_1 \times G_1 \times G_1$, 对 $a, b, c \in Z_q^*$, 判断 $c \equiv ab \pmod{q}$ 是否成立.

4) Gap Diffie-Hellman (GDH) 问题: 这是一类 CDH 问题困难而 DDH 问题容易的问题.

Gap Diffie-Hellman (GDH) 群是在其上 CDH 问题困难而 DDH 问题容易的群.

3 新型门限代理签名方案

基于上面的概率签名方案来设计一个门限代理签名方案, 同时它也是一个代理保护的门限代理签名方案. 系统参数同于上面的概率签名方案, 原始签名人可以从 Z_q^* 中随机选取 x_0 作为私钥, 计算 $pk_0 = Y_0 = x_0 P$ 作为公钥, 并让 CA 进行认证. 令 n 个代理人为 $p_1, p_2, \dots, p_n$. 每个代理签名人都可以从 Z_q^* 中随机选取 $x_i (1 \leq i \leq n)$ 作为私钥, 计算 $pk_i = Y_i = x_i P$ 作为公钥, 一并通过 CA 进行认证. 本文方案主要由三个协议组成: 代理密钥生成协议 TPK, 无秘密泄露的代理签名生成协议 TPS 和代理签名的验证协议 TPV.

3.1 代理密钥生成协议 TPK

在代理密钥生成协议中, 原始签名人 Alice 用先前提出的概率签名方案, 对证书 m_w 进行签名, 证书 m_w 详细描述了代理的诸多事宜. 以下过程若能顺利完成, 则每个签名人都能获得自己的代理私钥.

1) 原始签名人随机选取 $r \in Z_q^*$, 计算 $U = rP$. 令 $h = H_1(m_w, U)$, $Q = H_2(m_w)$, 计算 $V = (r + hx_0)Q$, $s = n^{-1}(hr + x_0)$, 则 m_w 的签名为 $\sigma = (U, V)$, 然后 Alice (原始签名人) 将 (σ, s) 和 m_w 发送给每个代理签名人.

2) 每个代理签名人首先验证证书 m_w 的合法性, 即检验下列方程是否成立.

$$e(P, V) = e(U + hY_0, H_2(m_w)) \quad (1)$$

和

$$nsP = hU + Y_0 \quad (2)$$

当且仅当 (1) 和 (2) 两个等式成立时接受 (σ, s) 有效, 代理签名人 $p_i (1 \leq i \leq n)$ 便可在 Z_q^* 中随机选取 k_i , 计算并广播 $k_i P$, 同时计算出 $s_i = s + x_i + k_i$ 作为自己的代理秘密.

3) 代理签名人 $p_i (1 \leq i \leq n)$ 随机选取系数在 Z_q 中, 次数为 $t-1$ 的多项式 $f_i(z)$, 并使 $f_i(0) = s_i = a_{i,0}$, 即

$$f_i(z) = s_i + a_{i,1}z + a_{i,2}z^2 + \dots + a_{i,t-1}z^{t-1} \quad (3)$$

然后 p_i 计算并广播 $a_{i,j}P (1 \leq j \leq t-1)$. 但无需广播 $a_{i,0}P$, 因为 $a_{i,0}P = s_iP = n^{-1}hU + n^{-1}Y_0 + Y_i + k_iP$. 最后将 $f_i(j)$ 秘密发送给其他代理签名人 $p_j (1 \leq j \leq n, j \neq i)$.

4) 代理签名人 $p_i (1 \leq i \leq n)$ 从其他签名人 $p_j (1 \leq j \leq n, j \neq i)$ 那里收到 $f_j(i)$ 后, 用下面的等式来验证 $f_j(i)$ 的有效性, 有

$$f_j(i)P = \sum_{k=0}^{t-1} i^k \cdot a_{j,k}P \quad (4)$$

如果未通过验证, p_i 给 p_j 数据无效的反馈意见. 假设这里没有这种情况, 则代理签名人 p_i 可以计算出

秘密的代理密钥 $x_i' = \sum_{k=0}^{t-1} f_k(i)$ 和广播公开的 $Y_i' = x_i'P$.

在此协议中, 若令 $f(z) = \sum_{i=1}^n f_i(z)$, 则代理私钥事实即为 $x_i' = f(i)$, 对应的代理公钥 Y_i' 为 $f(i)P$.

这样, 私钥就生成了.

3.2 代理签名生成协议 TPS

设 m 为要签名的消息, 将无秘密泄露地生成代

理签名.不失一般性,这里设 $p_1, p_2, \dots, p_t$ 为 t 个代表原始签名人对消息 m 进行签名的代理签名人,步骤如下:

1) 每个代理签名人 p_i ($1 \leq i \leq t$) 用他的代理私钥 x_i' 对消息 m 进行部分签名时,代理签名人对消息 m 计算 $\omega_i = \prod_{j \in \{1, 2, \dots, t\}, j \neq i} \frac{1}{t-j-i}$, 便得到消息 m 的部分签名 $\sigma_i = x_i' \omega_i H_2(m)$.

2) t 个代理签名人收集完所有的部分签名 σ_i 后,对 σ_i 用下面等式一一验证其有效性,即

$$e(P, \sigma_i) = e(\omega_i Y_i', H_2(m)) \quad (5)$$

若式 (5) 不成立,则知 p_i 没有给出正确的部分签名,或 p_i 是一个欺骗者,则可以另找其他代理签名人重做第一步.现在假设对每一部分签名都能通过上述

的验证,则他们合作产生 $\sigma' = \sum_{i=1}^t \sigma_i$ 和 $K = \sum_{m=1}^n k_m P$. 于是完整有效的代理签名为 $\langle m, U, m_w, \sigma', K \rangle$.

3.3 代理签名验证协议 TPV

代理签名的接收人可以用式 (6) 来验证签名,即

$$e(P, \sigma') = e(H_1(m_w, U)U + Y_o + K + \sum_{i=1}^n Y_i, H_2(m)) \quad (6)$$

如果式 (6) 成立,接收人可以确认签名是合法有效的,否则就予以拒绝.

4 安全性分析

由方案的描述可以分析出方案满足如下安全性要求:对于消息来说,完整有效的代理签名为 $\langle m, U, m_w, \sigma', K \rangle$,通过原始签名人发送的 (σ, s) 及其验证过程,验证人可以确信代理签名人拥有原始签名人对授权证书 m_w 的签名.

只有指定的代理签名者能够创建有效的代理签名,原始签名者和没有被指定为代理签名者的第三方都不能生成有效的代理签名.若第三方想冒充代理签名人和原始代理人对消息 m 伪造代理签名,但他没有原始签名人对授权证书 m_w 的签名,则不可能伪造;另一方面,原始签名人也不能伪造消息 m 的代理签名,因为代理签名人用原始签名人所不知的代理私钥和安全 GDH 签名产生代理签名,代理私钥中包含代理签名人的私钥信息.

任何人都能够从代理签名来确定代理签名者的身份.完整有效的代理签名有原始签名人的授权证

书 m_w ,于是任何人都能从授权证书 m_w 上确定相应代理签名人的身份.

一旦代理签名者代替原始签名者生成了有效的代理签名,他就不能向任何人否认他所签过的代理签名.完整有效的代理签名有原始签名人的授权证书 m_w ,在验证过程中都要用 m_w ,而代理签名人不可能更改证书 m_w .所以代理签名人一旦产生了代理签名,他将不能否认所产生的代理签名.在验证过程中,验证者必须用到代理签名人的公钥,因而他们也不能否认自己产生的签名.

通过安全性分析指出一点:在本文的代理签名方案中无需安全的信道发送签了名的证书和 (σ, s) ,因为已经证明攻击者即使知道 (σ, s) ,所提的方案依旧安全,确切的说,原始签名人可以通过公开信道发送 (σ, s) ,包括证书 m_w 给代理签名人.

另外,该方案能够抵制来自原始签名者或代理签名者的公钥替换攻击.方案中,证书是必须的.如果原始签名者或任何代理签名者要替换原来的公钥为新的公钥,他必须知道和新的公钥所对应的私钥.一般来说,在公钥替换攻击下,攻击者是不知新公钥所对应的私钥的.如此,攻击者不能更改在系统目录中由 CA 维护的公钥.因此,公钥替换攻击不能成功.

原始签名者和任何一个或 $(t-1)$ 个代理签名者也不能协作产生有效的代理签名.相应的,第三方更不能伪造有效的代理签名.在本方案中,第三方比原始签名者和 $(t-1)$ 个代理签名者知道更少的代理共享和私钥.原始签名者和 $(t-1)$ 个代理签名者都不能产生有效的代理签名,就更不用说第三方了.

5 门限代理签名方案的性能分析

在所提方案中,尽可能地少用双线性对以提高效率,本文方案的签名密钥生成协议 TPK 在计算量上与传统方案有很大程度上的改善,而代理签名生成协议 TPS 除了在点加运算上增加较多以外,也是有很大程度改善的.只有在签名验证阶段,本方案的计算量基本与传统方案相同,并没有增大运算量.

因为本文方案是基于椭圆曲线或超奇异椭圆曲线的 Weil 配对,所以有一个很大的优势,即密钥的长度很小.并且门限代理签名方案的代理签名长度也很短,因为它们都是椭圆曲线或超奇异椭圆曲线上的点.

(下转第 66 页)

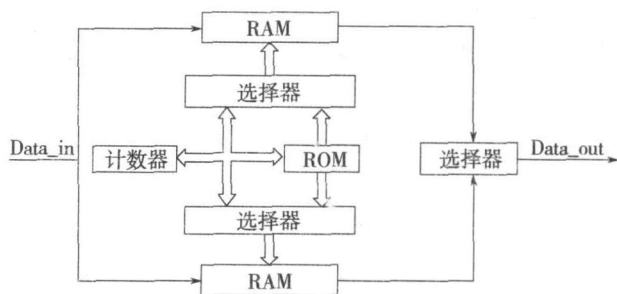


图 6 对数据的连续处理框图

6 结 语

在增余汉明码的基础上进行交织的方法可使通信中的突发错误得以纠正,交织使得在码率不变的前提下,提高系统的可靠性.文中给出了基于 FPGA 的该方案的实现方法,该方法具有通用性,对于不同的交织方法,只是 ROM 中存储的交织表不一

样,易于仿真测试和修改,加强了系统的灵活性.该方案已成功应用于某数据指令传输系统中,证明该方案切实可行.

参 考 文 献:

- [1] 卢明林,毕成余. Turbo 码中交织器的设计及性能分析 [J]. 信息技术, 2007 (5): 150 - 152
- [2] 左艳军,席志红. 无线突发信道中抗突发错误 BCH 码交织编码的性能分析 [J]. 应用科技, 2004, 31 (8): 19 - 21.
- [3] 杨海芬. Turbo 码编译码方法研究与实现 [D]. 成都:西南交通大学, 2003: 32 - 35.
- [4] ANDERSON J D, GLAVIKUS A. Interleaver Design for Turbo Coding [J]. Proc. Inter Symp. on Turbo Codes and Related Topics, 1997, 9: 255 - 258
- [5] 江 森,苏祥芳,肖东亮. 卷积 Turbo 码编码器及 CPLD 实现 [J]. 武汉大学学报 (理学版), 2001, 47 (3): 359 - 363.

(编辑:付长缨)

(上接第 62 页)

6 结 语

本文构造了一类新型门限代理签名. 这个新型的代理签名是基于双线性对的门限代理签名方案,并且能够进行代理保护. 经过分析,该方案既安全又有效率,适合应用于移动电子商务的各个方面.

参 考 文 献:

- [1] MANBO M, USUDA K, OKAMOTO E. Proxy Signatures for Delegating Signing Operation [C] // Proc. 3rd ACM Conference on Computer and Communications Security, ACM Press, 1996: 48 - 57.

- [2] MANBO M, USUDA K, OKAMOTO E. Proxy Signatures: Delegation of the Power to Sign Messages [J]. IECE Trans. Fundam., 1996, E79 - A (9): 1338 - 1354.
- [3] SUN H M, LEE N Y, WANG H T. Threshold Proxy signatures [J]. IEEE Proc. Computers & Digital Techniques, 1999: 146 (5): 259 - 263.
- [4] 李继国,曹珍富. 一个改进的门限代理签名方案 [J]. 计算机研究与发展, 2002, 39 (11): 1513 - 1518
- [5] SUN H M. A Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers [J]. Computer Communications, 1999, 22 (8): 717 - 722.

(编辑:付长缨)