基于身份的带凭证部分委托代理多重签名方案

田秀霞[1],曹珍富[2],叶文[illegible][1]
(1. 上海电力学院计算机与信息工程学院,上海 200090;2. 上海交通大学计算机科学与工程系,上海 200030)

摘 要: 本文基于椭圆曲线上的双线性对性质,提出了一个基于身份的带凭证部分委托代理多重签名方案,该方案具有强不可伪造性、强不可否认性、强可识别性和预防误用性.

关键词: 代理签名; 代理多重签名; 双线性对; 基于身份的密码系统
中图分类号: TP309.2 **文献标识码**: A **文章编号**: 0372-2112 (2006) 12A-2569-02

ID-Based Partial Delegation Proxy Multi-Signature with Warrant from Bilinear Pairings

TIAN Xiu-xia[1], CAO Zhen-fu[2], YE Wen-jun[1]
(1. *School of Computer and Information Engeering, Shanghai University of Electric Power, Shanghai* 200090, *China*;
2. *Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai* 200030, *China*)

Abstract: This paper proposes an identity-based (ID-based) partial delegation proxy multi-signature scheme with warrant based on bilinear pairings on elliptic curve. The scheme has strong non-forgeability, strong non-deniability, strong identifiability and prevention of misuse.

Key words: proxy signature; proxy multi-signature; bilinear pairings; ID-based cryptography

1 引言

目前基于身份的各种加密和签名体制正成为研究的热点,基于身份的加密和签名体制由 Shamir[1] 于 1984 提出,主要是为了简化基于证书的公钥体制对公钥证书的管理. 其主要思想就是利用用户的身份作为其公钥而不是一个随机的毫无意义的数字. 但是直到 2001 年,D Boneh, M Franklin[2] 和 C Cocks[6] 才分别提出了实际可用的基于身份的加密和签名方案.

代理多重签名是一种特殊的代理签名,他允许两个或多个原始签名者分别将其签名权限委托给同一个指定的代理签名者,之后代理签名者就可以代表他们进行签名. 代理多重签名的概念由 L Yi 等[3] 于 2000 年提出.

目前双射对性质被广泛应用于构造基于身份的密码系统,Weil 对和 Tate 模是基于椭圆曲线或超奇异椭圆曲线上满足双射对性质的例子. 在 Weil 对和 Tate 模被用于构造基于身份密码系统之前,主要被用来攻击椭圆曲线系统,如 MOV 和 FR 约化,近年来才被用来构造基于身份密码系统,如文献[2, 4, 5].

2 方案中的参数描述

G_1 是加法循环群, G_2 是次数为 q 的乘法循环群, P 是次数为 q 的 G_1 的生成元, q 是大素数. $\hat{e}: G_1 \times G_1 \to G_2$ 是一个双射对, $H_1: \{0,1\}^* \to G_1$, $H: \{0,1\}^* \times G_2 \to Z_q$ 两个无冲突哈希函数, PKG 是私钥生成中心.

w_1: 第 i 个原始签名者的授权凭证信息,包括指定代理签名者的身份、有效期限、签名说明和任何其它的有效证书. $H_1(w_i): G_1$ 上的一个点, $1 \le i \le n$, n 是一个大于 1 的整数, n 和 i 在下面的含义同此. S_{w_i}: 是第 i 个原始签名者对 w_i 的签名. SW_i: 是第 i 个原始签名者对总的授权凭证信息 w 的签名. o_i: 第 i 个原始签名者, ID_i, $Q_i = H_1(ID_i)$, $S_i = sQ_i$ 依次为 o_i 的身份,公钥和私钥. p: 代理签名者, ID_p, $Q_p = H_1(ID_p)$, $S_p = sQ_p$ 依次为 p 的身份,公钥和私钥. v: 签名验证者.

3 提出的方案

创建: PKG 选择一个随机数 $s \in Z_q^*$ 作为主私钥,计算 $P_{pub} = sP$, PKG 发布 $params = \{G_1, G_2, \hat{e}, q, P, P_{pub}, H_1, H\}$.

私钥生成: o_i 和 p 提交他们的身份信息 ID_i, ID_p, PKG 计算他们对应的私钥 S_i, S_p, $1 \le i \le n$.

原始签名者之间的通信: o_i 随机选择 $r_i \in Z_q^*$,计算签名 $S_{w_i} = r_i H_1(w_i) + S_i$,然后将 S_{w_i} 通过安全信道给 o_j, $1 \le j \le n$, $j \ne i$,并发布 $r_i P$, w_i. 当 o_i 接收到 o_j 的授权信息 w_j, $1 \le j \le n$, $j \ne i$ 后,通过等式 $(S_{w_j}, P) = (H_1(w_j), r_j P)(P_{pub}, Q_j)$ 是否成立,验证 w_j 的签名 S_{w_j} 的有效性,如果等式成立,则接受 w_j,并生成总的授权信息 $w = w_1 \| \cdots \| w_n$,和对 w 的签名 $SW_i = r_i H_1(w) + S_i$,最后 o_i 将 SW_i 通过安全信道给 p,并发布 $H_1(w)$.

收稿日期:2006-05-29;修回日期:2006-08-10
基金项目:国家自然科学基金(No. 60072018);上海市重点学科建设资助项目(No. P1303);上海高校选拔培养优秀青年教师科研专项基金(No. Z-2006-52)

$o_j, 1 \le j \le n, j \ne i$ 也经过上述类似的过程.

代理签名密钥生成: p 接收到 SW_i,利用 o_i 的公钥 Q_i,验证等式 $(SW_i, P) = (H_1(w), r_i P)(P_{pub}, Q_i)$,如果成立,则接受签名,否则拒绝或要求 o_i 再次传送签名. 如果 $SW_i, 1 \le i \le n$ 有效, p 计算代理签名私钥 S_{wp} 和代理签名公钥 Q_{wp}, $S_{wp} = \sum_{i=1}^{n} SW_i + S_p$, $Q_{wp} = \sum_{i=1}^{n} Q_i + Q_{ID_p}$.

代理签名生成: p 随机选取 $x \in Z_q^*$,计算 $K = \hat{e}(P, P_{pub})^x$, $k = H(m, K)$, $S = xP_{pub} - kS_{wp}$,有效的代理签名就是 $\langle m, r_i p, w_i, H_1(w), S, k \rangle, 1 \le i \le n$.

签名验证: v 通过计算 $H_1(w) = H_1(w_1 \| \cdots \| w_n)$, $K = \hat{e}(P, S)\hat{e}(P_{pub}, Q_{wp})^k \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k$,如果 $k = H(m, K)$ 成立,则接受签名.

签名等式验证过程如下:

$$
\begin{aligned}
&H_1(w) = H_1(w_1 \| \cdots \| w_n)\\
&\hat{e}(P, S)\hat{e}(P_{pub}, Q_{wp})^k \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k\\
&= \hat{e}\left(P, xP_{pub} - k\left(\sum_{i=1}^{n} SW_i + S_p\right)\right)\hat{e}\left(P_{pub}, \sum_{i=1}^{n} Q_i + Q_p\right)^k\\
&\quad \cdot \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k\\
&= \hat{e}\left(P, xP_{pub} - k\left(\sum_{i=1}^{n} r_i H_1(w) + \sum_{i=1}^{n} S_i + S_p\right)\right)\\
&\quad \cdot \hat{e}\left(P_{pub}, \sum_{i=1}^{n} Q_i + Q_p\right)^k \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k\\
&= \hat{e}\left(P, xP_{pub} - k\left(\sum_{i=1}^{n} r_i H_1(w) + \sum_{i=1}^{n} sQ_i + sQ_p\right)\right)\\
&\quad \cdot \hat{e}\left(P_{pub}, \sum_{i=1}^{n} Q_i + Q_p\right)^k \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k\\
&= \hat{e}(P, xP_{pub})\hat{e}\left(P, -k\left(\sum_{i=1}^{n} r_i H_1(w) + \sum_{i=1}^{n} sQ_i + sQ_p\right)\right)\\
&\quad \cdot \hat{e}\left(P_{pub}, \sum_{i=1}^{n} Q_i + Q_p\right)^k \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k\\
&= \hat{e}(P, P_{pub})^x \hat{e}\left(P, \sum_{i=1}^{n} r_i H_1(w) + \sum_{i=1}^{n} sQ_i + sQ_p\right)^{-k}\\
&\quad \cdot \hat{e}\left(P_{pub}, \sum_{i=1}^{n} Q_i + Q_p\right)^k \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k\\
&= K\hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^{-k} \hat{e}\left(P_{pub}, \sum_{i=1}^{n} Q_i + Q_p\right)^{-k}\\
&\quad \cdot \hat{e}\left(P_{pub}, \sum_{i=1}^{n} Q_i + Q_p\right)^k \hat{e}\left(\sum_{i=1}^{n} r_i P, H_1(w)\right)^k\\
&= K
\end{aligned}
$$

4 方案的安全性分析

可验证性:根据 p 对信息 m 的签名, v 信服 p 拥有 $S_{w_i}, 1 \le i \le n$.

强不可伪造性:对手不能伪造 p 对信息 m 的签名,如果对手想对 m 签名,他必须首先获得 S_{w_i},而签名 S_{w_i} 是一个已经被 BLS[4] 证明的数学难题. 一个原始签名者如 o_1 也不能伪造 p 对信息 m 的签名,因为他没有 $o_1, 1 \le i \le n$,的私钥,也没有 p 的私钥.

强可识别性:由于 w_i 和 w 包含在有效的验证等式中,因此任何人都可以从 w_i 和 w 识别出 p 的身份.

强不可否认性: 由于 w_i 和 w 包含在有效的验证等式中,因此 w_i 和 w 不能被 p 修改,因此一旦 p 创建了有效的代理签名,他也不能否认自己的签名.

预防误用性: w_i 包括 p 的身份、有效期限、签名说明和任何其它的有效证书,因此 p 不能签署原始签名者未授权的信息,他更不能把签名权利转让给他人.

5 总结

本方案可以用于电子委托投票、电子委托签名等领域,具有一定的实用价值. 本方案的安全特性不但可以有效地保护原始签名者,也可以保护代理签名者的合法权益. 根据授权凭证信息签名,原始签名者不能否认自己对授权凭证信息的签名,因为只有原始签名者拥有自己的私钥,而根据最后的代理签名,代理签名者不能否认自己的签名,因为只有代理签名者拥有代理签名私钥-通过代理签名者的私钥计算.

参考文献:

[1] A Shamir. Identity-based cryptosystems and signature schemes [A]. LNCS 196, Advances in Cryptology-Crypto 1984 [C]. Berlin: Springer-Verlag, 1984. 47 - 53.

[2] D Boneh, M Franklin. Identity-based encryption from the Weil pairing[A]. LNCS 2139, Advances in Cryptology-Crypto 2001 [C]. Berlin: Springer-Verlag, 2001. 213 - 229.

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

[4] D Boneh, B Lynn, H Shacham. Short signatures from the Weil pairing[A]. LNCS 2248, Advances in Cryptology-Crypto 2001 [C]. Berlin: Springer-Verlag, 2001. 514 - 532.

[5] F Zhang, K Kim. Efficient ID-based blind signature and proxy signature from bilinear pairings [A]. LNCS 2727, ACISP 2002 [C]. Berlin: Springer-Verlag, 2002. 312 - 323.

[6] C Cocks. An identity based encryption scheme based on quadratic residues [A]. LNCS 2260, Cryptography and Coding 2001 [C]. Berlin: Springer-Verlag, 2001. 360 - 363.

作者简介:

田秀霞 女,讲师,1976 年出生于河南,1999 年于洛阳工学院计算机科学与工程系获得学士学位,并于同年留校任教,2005 年于上海交通大学计算机科学与工程系获工学硕士学位,目前在上海电力学院计算机与信息工程学院任专业教师. 主要研究领域:网络安全、密码学与电子商务中的安全问题.

E-mail: tianxxsmile @yahoo. com. cn