

新的无证书代理盲签名方案

魏春艳,蔡晓秋

(洛阳师范学院 数学科学学院,河南 洛阳 471022)

(chunyan_wei@126.com)

摘要:无证书公钥密码学既不存在传统的公钥密码系统的证书管理耗费,也不存在基于身份的密码系统中的密钥托管问题,安全且高效。研究了代理盲签名方案的构造和应用,发现现有的无证书代理盲签名方案较少,而在无证书密码系统中研究代理盲签名会更容易满足其在电子投票、电子银行等应用领域中对安全性和高效性的要求。基于双线性对知识和离散对数困难问题,提出了一种无证书代理盲签名方案,该方案满足盲性、不可伪造性、可鉴别性、不可否认性等性质。

关键词:公钥密码学;无证书;代理盲签名;双线性对;离散对数

中图分类号: TP309 **文献标志码:** A

New certificateless proxy blind signature scheme

WEI Chun-yan, CAI Xiao-qi

(College of Mathematics, Luoyang Normal University, Luoyang Henan 471022, China)

Abstract: Certificateless public key cryptography is not only secure but also efficient because it does not suffer the cost of the certificate management in traditional public key cryptography and the key escrow problem inherited in ID-based public key cryptography. The study of proxy blind signature's construction and application shows that present certificateless proxy blind signature schemes are very few and proxy blind signature schemes in certificateless public key systems can fulfill the safety and high efficiency required in electronic voting and e-banking and other fields better. Based on the bilinear pairing and discrete logarithm problem, a new certificateless proxy blind signature scheme which fulfils the properties of blindness, non-forgeability, identifiability, nonrepudiation and so on was given.

Key words: Public Key Cryptography (PKC); certificateless; proxy blind signature; bilinear pairing; discrete logarithm

0 引言

代理签名^[1]于1996年由Mambo等提出,当原始签名人因某种原因不能签名时,可将签名权委托给其他人(代理人)代替自己行使签名权。盲签名于1982年由Chaum首先提出,它是一种特殊的数字签名技术。签名者不知道所签文件或消息的具体内容,且在签名被文件或消息的拥有者公布后,签名者不能追踪签名。盲签名广泛地应用于电子投票系统和电子银行现金系统等。将代理签名和盲签名结合,提出了代理盲签名方案,它同时具有两个签名的特点,从而满足应用要求,一个安全有效的代理盲签名应满足以下要求:

- 1) 盲性:代理人不能得到关于签名和被签消息的任何信息;
- 2) 不可追踪性:签名者对他签名的消息和原始消息不能进行追踪关联;
- 3) 不可伪造性:只有代理人可以产生合法的代理签名,其他人包括授权人均不能产生;
- 4) 可鉴别性:任何人可以由一个签名鉴别出代理人;
- 5) 不可否认性:代理人一旦产生了一个合法的代理签名,便不能否认这个签名。

目前已有的代理盲签名方案^[2-7]多是基于传统的基于CA的密码体制和基于身份的公钥密码体制的,也有基于自认

证体制的。在2003年亚密会上,Al-Riyami和Paterson提出了一种新的概念:无证书公钥密码系统^[8]。它既不存在传统的公钥密码系统的证书管理耗费,也不存在基于身份的密码系统中的密钥托管问题,效率较高。由于无证书公钥系统的优势非常突出,基于无证书公钥系统也陆续提出了许多签名方案^[9-11],而无证书公钥密码体制的代理盲签名方案还为数较少。基于代理盲签名应用上对安全性和高效性的要求,在无证书公钥密码学中对其进行研究是具有现实意义的。本文首先介绍了方案所涉及的数学困难问题,接着提出了一种无证书代理盲签名方案,经分析,该方案不仅正确且能够满足盲性、可验证性、不可伪造性、可鉴别性、不可否认性等安全性。

1 预备知识

1.1 离散对数问题

对于一个有限循环群 $G = \langle g \rangle$ 和元素 $y \in G$,寻找整数 $x(0 \leq x \leq |G|)$,使得 $y = g^x$ 成立。

1.2 双线性对映射

G_1 和 G_2 分别是阶为素数 q 的加群和乘群, P 为 G_1 的生成元,假设 G_1 和 G_2 这两个群中的离散对数都是困难问题。 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 为满足下列三条性质的双线性对:

- 1) 双线性性: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$,对所有的 $P, Q \in$

收稿日期:2010-06-17;修回日期:2010-08-10。

基金项目:河南省教育厅自然科学研究计划项目(2010B120008);洛阳师范学院青年基金资助项目(2008-QNJ-112)。

作者简介:魏春艳(1982-),女,江苏邳州人,讲师,硕士,主要研究方向:密码学、信息安全;蔡晓秋(1980-),女,河南许昌人,讲师,硕士,主要研究方向:密码学、电子商务。

G_1 和所有的 $a, b \in \mathbf{Z}_q$ 。

2) 非退化性: 若 $\hat{e}(P, Q) = 1, \forall Q \in G_1$, 则 $P = \Theta$ 。

3) 可计算性: 对所有 $P, Q \in G_1$, 存在有效算法可以计算 $\hat{e}(P, Q)$ 。

2 无证书代理盲签名方案

无证书代理盲签名方案涉及的成员有: 密钥生成中心 KGC、原签名者 A、代理签名者 B、用户 C 和验证者。它由如下 6 个算法组成: 系统参数的生成、部分私钥提取、用户密钥生成、代理密钥生成、代理盲签名和验证。该方案可以描述如下:

1) 系统参数的生成: G_1 与 G_2 分别是阶为大素数 q 的加群和乘群, P 为 G_1 的生成元, $e: G_1 \times G_1 \rightarrow G_2$ 是双线性映射, $g = e(P, P)$, 定义 3 个安全 Hash 函数 $H_1: \{0, 1\}^* \rightarrow G_1^*$, $H_2: \{0, 1\}^* \times G_1^* \rightarrow \mathbf{Z}_q^*$, $H_3: \{0, 1\}^* \rightarrow \mathbf{Z}_q^*$ 。任选 $s \in \mathbf{Z}_q^*$ 作为 KGC 的私钥 mk , KGC 的公钥为 $P_{pub} = sP$, 则系统的公开参数为 $Params = \{G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2, H_3\}$, 将私钥 mk 秘密保存。

2) 部分私钥提取: 设原始签名人 A、代理签名者 B 的身份信息分别为 ID_A, ID_B , KGC 计算 $U_A = H_1(ID_A), U_B = H_1(ID_B)$, 并为其生成部分私钥 $psk_A = sU_A, psk_B = sU_B$, 并将 psk_A, psk_B 通过安全信道分别发送给 A、B。

3) 用户密钥生成: A、B 分别随机选择 $x_A, x_B \in \mathbf{Z}_q^*$ 作为各自的秘密值, 计算并公开各自的公钥 $PK_A = x_A P, PK_B = x_B P$, A、B 的私钥分别为 (psk_A, x_A) 和 (psk_B, x_B) 。

4) 代理密钥的生成:

① 原始签名者 A 建立一个用于说明 A、B 的身份、授权范围期限等内容的授权许可信息 m_w , 然后计算 $U_B = H_1(ID_B)$, 生成一个短签名 $S_w = x_A H_3(m_w) U_B + psk_A$, 并将 (m_w, S_w) 通过安全信道发送给 B;

② 代理签名者 B 首先验证等式:

$$e(S_w, P) = e(U_B, PK_A)^{H_3(m_w)} e(U_A, P_{pub}) \quad (1)$$

是否成立, 如果不成立终止代理过程, 等式成立则计算代理签名密钥: $S_p = S_w + x_B H_3(m_w) U_A + psk_B$ 。

5) 代理盲签名的生成: 对于消息 $m \in \{0, 1\}^*$:

① B 随机选择 $r \in \mathbf{Z}_q^*$, 计算 $R = g^r$ 并发送给用户 C;

② C 任选 $\alpha, \beta \in \mathbf{Z}_q^*$, 计算 $R' = R^\alpha g^\beta, t' = H_2(m, R'), t = \alpha^{-1} t'$ 并发送 t 给 B;

③ B 计算 $V' = tS_p + rP$, 并发送 V' 给 C;

④ C 首先计算 $U_A = H_1(ID_A), U_B = H_1(ID_B)$, 然后验证:

$$e(V', P) = \left\{ [e(U_B, PK_A) e(U_A, PK_B)]^{H_3(m_w)} e(U_A + U_B, P_0) \right\}^t R \quad (2)$$

若不成立, 拒绝 V' , 否则, 计算 $V = \alpha V' + \beta P$, 则消息 m 的代理盲签名方案为 $\sigma = (V, t', m_w)$ 。

6) 签名的验证: 验证者首先计算 $U_A = H_1(ID_A), U_B = H_1(ID_B)$:

$$R'' = e(V, P) \left\{ [e(U_B, PK_A) e(U_A, PK_B)]^{H_3(m_w)} e(U_A + U_B, P_0) \right\}^{-t'} \quad (3)$$

然后验证:

$$t' = H_2(m, R'') \quad (4)$$

是否成立, 如果等式成立接受签名, 否则拒绝签名。

3 方案的分析

3.1 正确性分析

1) 授权签名验证式(1)的证明。

证明

$$\begin{aligned} e(S_w, P) &= e(x_A H_3(m_w) U_B + sU_A, P) = \\ &= e(H_3(m_w) U_B, PK_A) e(U_A, P_{pub}) = \\ &= e(U_B, PK_A)^{H_3(m_w)} e(U_A, P_{pub}) \end{aligned}$$

证毕。

2) 验证式(2)的证明。

证明

$$\begin{aligned} e(V', P) &= e(tS_p + rP, P) = e(S_p, P)^t e(P, P)^r = \\ &= [e(x_A U_B + x_B U_A, P)^{H_3(m_w)} e(ps k_A + ps k_B, P)]^t R = \\ &= \{ [e(U_B, PK_A) e(U_A, PK_B)]^{H_3(m_w)} e(U_A + U_B, P_0) \}^t R \end{aligned}$$

证毕。

3) 验证式(4)的证明。

证明

$$\begin{aligned} e(V, P) &= e(\alpha(tS_p + rP) + \beta P, P) = e(t'S_p + (\alpha r + \beta)P, P) = \\ &= [e(x_A U_B + x_B U_A, P)^{H_3(m_w)} e(ps k_A + ps k_B, P)]^{t'} e(P, P)^{\alpha r + \beta} = \\ &= \{ [e(U_A, PK_B) e(U_B, PK_A)]^{H_3(m_w)} e(U_A + U_B, P_0) \}^{t'} R^\alpha g^\beta = \\ &= \{ [e(U_A, PK_B) e(U_B, PK_A)]^{H_3(m_w)} e(U_A + U_B, P_0) \}^{t'} R' \end{aligned}$$

因此:

$$R'' = e(V, P) \{ [e(U_B, PK_A) e(U_A, PK_B)]^{H_3(m_w)} e(U_A + U_B, P_0) \}^{-t'} = R'$$

代入式(3) 结论成立。

证毕。

3.2 安全性分析

1) 盲性: 由于代理人在签名时消息受 Hash 函数 H_2 的保护, 因此代理人不能得到关于签名和被签消息的任何信息。

2) 不可追踪性: 由于代理人不知道 α 和 β , 而从 $R' = R^\alpha g^\beta$ 中求出 α 和 β 难度不亚于解离散对数困难问题, 从 $t = \alpha^{-1} t'$ 中得到 t' 是离散对数困难问题, 而从 $V = \alpha V' + \beta P$ 中得到 V' 难度不亚于解离散对数问题, 因此签名者通过签名 $\sigma = (V, t', m_w)$ 和已掌握的信息 t, V' 对他签名的消息和原始消息进行追踪关联是不可能的。

3) 不可伪造性: 由于代理密钥中使用了代理签名者的私钥, 而从 $V' = tS_p + rP$ 中得到代理密钥 S_p 不亚于解离散对数困难问题。若直接从验证式伪造签名有 3 种思路: ① 先给出 t' , 再由式(4) 中求 R'' , 从式(3) 中求出 V , 这种难度不低于 Hash 函数求逆和离散对数困难问题; ② 先给出 R'' , 带入式(4) 中求 t' , 再将 R'' 和 t' 带入式(3) 求 V , 这种难度也不低于离散对数困难问题; ③ 先给出 V , 再由式(3)、(4) 来找符合条件的 t' 和 R'' , 这种难度不低于 Hash 函数求逆和离散对数困难问题。因此只有代理人可以产生合法的代理签名, 其他人包括授权人均不能产生。

4) 可鉴别性: 由于授权信息 m_w 被包含在代理密钥中且受 Hash 函数包含, 任何人可以由一个签名鉴别出代理人。

5) 不可否认性: 根据不可伪造性的分析知, 只有代理人能够产生合法的代理盲签名, 因此, 代理人一旦产生了一个合法的代理签名, 便不能否认这个签名。

(下转第 3345 页)

据时的计算量。具体过程如下:

设新的根为 s' , 系统任意选择 n 个用户的数据分片 $E_i = (x_{i1}, x_{i2}, \dots, x_{in}), i = 1, 2, \dots, n$, 与新的根 s' 一起代入圆的方程, 即式(1), 可得:

$$\begin{cases} \sum_{j=1}^n (x_{1j} - a_j')^2 \equiv s' \pmod{p} \\ \sum_{j=1}^n (x_{2j} - a_j')^2 \equiv s' \pmod{p} \\ \dots \\ \sum_{j=1}^n (x_{nj} - a_j')^2 \equiv s' \pmod{p} \end{cases}$$

求解该方程组, 即可得新的秘密圆圆心 $(a_1', a_2', \dots, a_n')$, 把 a_1', a_2', \dots, a_n' 和 s' 代入式(1), 可得新的秘密圆 SC_j 方程。

保持这 n 个数据分片不变, 根据数据分离算法, 在 n 维圆 SC_j 上另外选择一个点作为新的跟 s' 的分片数据。此举极大地减少了计算量, 降低了系统的开销。

3) 复杂性分析。本文从存储容量与计算量两方面考虑本系统的复杂性。

存储容量 对客户端的存储要求为分离后的数据 $d_1, d_2, d_3, \dots, d_{n+1}$ 以及所要使用的 Hash 函数的根, 授权服务器需要存储下条 Hash 函数根的份额及上次认证信息。这比传统 Hash 链存储量略大一些, 但是存储量的增大给存储系统提供了更高的安全性。

计算量 客户端和服务端需要计算数据分离—恢复算法, 一个显著的特点是所有计算均为在 $GF(p)$ 上的线性计算。

4) 抗重放攻击。重放攻击是指用原有通过验证的数据包再次请求验证以获得合法身份。在本方案中每一次认证均采用不同的 $h^i(s)$, 所以已通过认证的数据包将不能通过下次认证, 从而避免了重放攻击的威胁。

4 结语

随着电子商务和一次性口令认证的应用越来越广泛, 本

文提出了一种安全高效的自更新 Hash 链构造方案, 充分利用 n 维空间圆的几何特性进行数据的分离和恢复。与以往方案相比, 新方案具有更高的安全性, 且计算简单, 在目前复杂网络环境中具有较高的实用价值。在本方案的基础上可以构造微支付协议、一次性动态口令协议、认证协议、高效密钥分配协议等。

参考文献:

- [1] GOYAL V. How to re-initialize a hash chain[EB/OL]. [2010-01-01]. <http://eprint.iacr.org/2004/097.pdf>.
- [2] BICAKCI K, BAYKAL N. Infinite length hash chains and their applications[C]// WETICE'02: Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Pittsburgh, US: IEEE, 2002: 57-61.
- [3] MOUSSAKHANI B, MSAFAVI S, EBRAHIMZAD H, et al. A probabilistic signature scheme to provide authentication through a Hash chain[C]// Communications and Networking in China. [S. l.]: IEEE, 2006: 1-5.
- [4] ZHANG HAO-JUN, LI XIAO-XUE, LIU YU-KUN. An efficient authentication scheme based on the self-updating hash chain for campus network[C]// Proceedings of 2008 IEEE International Symposium on IT in Medicine and Education. [S. l.]: IEEE, 2008: 268-271.
- [5] ZHANG HAO-JUN, LI XIAO-XUE, REN RUI. A novel self-renewal hash chain and its implementation[C]// 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. Washington, DC: IEEE Computer Society, 2008: 144-149.
- [6] ZHANG MIN-QING, DONG BIN, YANG XIAO-YUAN. A new self-updating hash chain structure scheme[C]// 2009 International Conference on Computational Intelligence and Security. Beijing: IEEE, 2009: 315-318.
- [7] WANG SHIH-JENG. Yet another log-in authentication using n -dimensional construction based on circle property[J]. IEEE Transactions on Consumer Electronics, 2003, 49(2): 337-341.
- [8] LAMPORT L. Password authentication with insecure communication [J]. Communications of the ACM, 1981, 24(11): 770-772.

(上接第 3342 页)

4 结语

无证书公钥密码学是目前信息安全领域研究的热点, 基于无证书公钥密码学提出了一种代理盲签名方案, 经分析该方案是正确安全的, 能够应用于电子选举、电子现金、电子拍卖等方面。

参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: Delegation of the power to sign message [J]. IEICE Transactions on Fundamentals, 1996, E79-A (9): 1338-1353.
- [2] 谭作文, 刘卓军, 唐春明. 基于离散对数的代理盲签名[J]. 软件学报, 2003, 14(11): 1931-1935.
- [3] 夏满民, 谷利泽. 一种新型的代理盲签名方案[J]. 北京邮电大学学报, 2006, 29(3): 48-52.
- [4] 陈逢林, 胡万宝. 基于超椭圆曲线的代理盲签名方案[J]. 计算机应用, 2010, 30(5): 1224-1226.
- [5] TAN Z W, LIU Z J, TANG C M. Digital proxy blind signature

schemes based on DLP and ECDLP[J]. MM Research Preprints, 2002, 21(7): 212-217.

- [6] 王天银, 蔡晓秋, 张建中. 一种安全有效的代理盲签名方案[J]. 计算机工程, 2007, 33(2): 148-149.
- [7] 张学军, 王育民. 高效的基于身份的代理盲签名[J]. 计算机应用, 2006, 26(11): 2586-2588.
- [8] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]// Proceedings of Asiacrypt 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 452-473.
- [9] BESSIE C, DUNCAN S, ZHANG Z, et al. Certificateless signature: a new security model and an improved generic construction[J]. Designs, Codes and Cryptography, 2007, 42(2): 109-126.
- [10] ZHANG Z F, WONG D S, XU J, et al. Certificateless public-key signature: security model and efficient construction[C]// Proceedings of ACNS 2006, LNCS 3989. Berlin: Springer-Verlag, 2006: 293-308.
- [11] 张建中, 魏春艳. 一种新的无证书代理签名方案[J]. 计算机工程, 2010, 36(10): 168-172.