一种新的基于身份的门限签名方案

蔡永泉,张雪迪,姜 楠
(北京工业大学计算机学院,北京 100124)

摘 要: 门限签名能够分散签名权力,比普通单人签名具有更高的安全性. 目前大多数门限签名都是随机预言模型下可证明安全的. 本文利用椭圆曲线上的双线性对,以 Paterson 签名方案为基础,提出了一种无随机预言的基于身份的门限签名方案. 该方案需要一个可信任的私钥生成中心来生成和管理私钥. 在标准模型下对该方案进行了安全性证明,表明该方案是健壮的,并且能够抵抗适应性选择消息攻击.

关键词: 基于身份; 门限签名; 无随机预言
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 0372-2112 (2009) 4A-102-04

A Novel Identity-Based Threshold Signature

CAI Yong-quan, ZHANG Xue-di, JIANG Nan
(*College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124, *China*)

Abstract: Threshold signature is designed to distribute the power of signature, therefore it is more secure than normal single signature. Most of the existing threshold signatrue schemes are provable secure in the random oracle model. An identity-based signature (IBS) is proposed from the bilinear parings based on Paterson's signature scheme In the proposed threshold signatue scheme, a trusted private key generator (PKG) is required to generate and manage the private secret key. The security of the signature scheme is proven in this paper. We show that it is strong and resisted against adapt chosen message attack.

Key words: identity-based; threshold signature; without random oracles

1 引言

门限签名[1]是指把签名私钥分成个个子密钥,这些子密钥由群的个成员持有. 签名密钥不直接参与签名过程,由不少于个成员的成员子集使用各自所拥有的子密钥共同产生最终的签名,任何小于个成员的子集都无法恢复密钥或者计算正确的签名结果. 与普通的单人签名相比,门限签名具有更高的安全性.

1984 年 Shamir[2] 首先提出了基于身份的加密、签名、认证的设想. 在基于身份的密码体制中,用户的公钥可以通过某个公开算法直接从其身份信息(如身份证号、email 地址)得到,而私钥是从 PKG(Private Key Generator) 获得. 与传统的 CA(Certification Authority) 体制相比,基于身份的体制不存在颁发公钥证书所带来的存储和管理开销的问题. 之后人们提出了许多基于身份的密码方案,但是直到 2001 年,才由 Boneh 和 Franklin[3] 利用椭圆曲线上的双线性对,提出一个真正意义上的基于身份的高效加密方案.

目前大多数基于身份的门限签名方案[4~6] 都是在随机预言模型下可证明安全的,在实际应用中用 Hash 函数代替随机预言. 如果 Hash 函数是理想的,则方案在随机预言模型下是可证明安全的. 但是,理想的 Hash 函数是一个很强的假设,而且存在在随机预言模型下可证明安全,但在具体应用中却无法构造的密码方案[7,8]. 因此,设计标准模型下可证明安全的门限签名方案更具有实际意义.

文献[9]提出了一种标准模型下的基于身份的门限签名的方案,但是其公钥一部分是根据用户的身份生成,另一部分还需要由签名者计算并公开. 而在基于身份的签名体制中,公钥是完全根据用户的身份产生的. 本文以 Paterson 签名方案[10] 为基础,提出一种标准模型下基于身份的门限签名方案. 该方案无需另外生成公钥,因而更符合基于身份签名体制的要求.

2 理论背景

2.1 双线性对

G_1 和 G_2 同为素数阶 p 的群, G_1 为加法群, G_2 为乘法群, P 为 G_1 的生成元. 假设 G_1 和 G_2 中的离散对数问

收稿日期:2008-09-11;修回日期:2008-12-20
基金项目:国家 973 重点基础研究发展计划(No. 2007CB11106)

题是难解的.一个具有密码学意义的双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 是具有如下性质的映射:

(1) 双线性:对任意的 $S, T \in G_1$, $a, b \in Z_q^*$,都有 $e(aS, bT) = e(S, T)^{ab}$.

(2) 非退化性:对于生成元 P,有 $e(P, P) \neq 1$.

(3) 可计算性:对任意的 $S, T \in G_1$,存在有效的算法计算 $e(S, T)$.

利用超奇异椭圆曲线上的 Weil 对或 Tate 对可以构造出具有密码学意义的双线性映射.

2.2 CDH 问题

定义 1 CDH(Computation Diffie-Hellman)问题:给定阶为素数 p、生成元为 P 的群 G, $aP, bP \in G$,其中 $a, b \in Z_q^*$,计算 abP.

如果没有能在运算时间 t 内以不可忽略的概率 ε 解决 CDH 问题的算法,则我们说 CDH 问题是困难的.

2.3 门限签名方案及其安全性

定义 2 一个门限签名方案由以下步骤组成:

(1) 生成系统参数 I.

(2) 密钥生成算法:给定系统参数 I,输出公钥 pk 和每个成员的私钥 sk_i. 其中 $(sk_1, sk_2, \cdots, sk_n)$ 构成 (t, n) 门限秘密共享.

(3) 签名算法:给定公共参数 I、消息 M 和私钥 sk,输出签名 σ.

(4) 验证算法:给定签名 σ 和公钥 pk,验证签名是否有效.

定义 3 门限签名是安全的,如果一下两个条件成立:

(1) 不可伪造性:给定系统参数 I,攻击者最多可破坏 $t-1$ 个成员,可以进行 k 次的选择消息提问,最终不能产生一个新消息的有效签名.

(2) 健壮性:攻击者最多可破坏 $t-1$ 个成员,最终仍能产生正确的签名.

3 无随机预言的门限签名方案

我们以 Paterson 签名方案为基础,利用 Feldman 可验证秘密共享技术[11],提出一个新的无随机预言的门限签名方案. 该方案需要一个 PKG 和一个可信任的管理者(可以由 PKG 充当),全体签名用户集合为 $B_1, B_2, \cdots, B_N$.

3.1 系统初始化

$e: G_1 \times G_1 \rightarrow G_2$ 为双线性映射, P 为 G_1 的任意生成元. PKG 随机选取 $x \in Z_p$,计算 $P_1 = xP$. 随机选取 P_2, $U', M' \in G_1$ 及 n_u 维向量 $\mathrm{U} = (U_i)$ 和 n_m 维向量 $\mathrm{M} = (M_i)$. 公共参数为 $(G_1, G_2, e, P_1, P_2, U', M', U, M)$,系统私钥为 xP_0.

3.2 密钥生成和分发

(1) 给定身份 ID,设 ID 的二进制序列为 $(id_1, id_2, \cdots, id_{n_u})$. PKG 随机选择 $r_u \in Z_p$,计算:

$$S_u = \alpha P_2 + r_u\left(U' + \sum_{i=1}^{n_u} id_i U_i\right)$$

$$R_u = r_u P$$

将 $D_u = (S_u, P_u)$ 通过秘密信道发送给管理者.

(2) 管理者选择随机多项式:

$$f(x) = S_u + C_1 x + \cdots + C_{t-1} x^{i-1}$$

其中 $C_i \in G_1$

计算 $S_i = f(i)$ 并通过秘密信道发送给 B_i. 然后计算 $c_i = e(S_i, P)$ 并广播 c_i, R_u. B_i 验证是否 $e(S_i, P) = c_i$. 若通过,则 B_i 拥有的部分密钥为 S_i. $(S_1, S_2, \cdots, S_N)$ 构成了关于私钥 S_u 的 (t, N) 门限共享.

3.3 门限签名生成

不失一般性,假设参与签名的用户集合为 $B_1, B_2, \cdots, B_t$.

(1) 联合生成随机数

用户 B_i 选择 $t-1$ 次多项式:

$$g_i(x) = r_i + b_{i,1} x + \cdots + b_{i,t-1} x^{t-1}$$

计算并广播 $\beta_{i,0} = r_i P$, $\beta_{i,j} = b_{i,j} P$. 然后计算 $w_{i,j} = g_i(j)$ 并秘密发给用户 B_j. 用户 B_j 验证 $w_{i,j} P = \sum_{k=0}^{i-1} j^k \beta_{i,k}$ 是否成立来判断从 U_i 收到的随机数份额 $w_{i,j}$ 是否正确. 若正确,则计算 $w_i = \sum_{j=1}^{t} w_{j,i}$ 和 $W_i = w_i P$,广播 W_i.

(2) 部分签名

待签名消息为 $m = (m_1, m_2, \cdots, m_{n_m})$.

用户 B_i 计算并广播:

$$V_i = S_i + w_i\left(M' + \sum_{j=1}^{n_m} m_j M_j\right)$$

(3) 签名的合成

签名的合成可由参与签名的任一成员来完成. 对于所收到的部分签名,合成者首先验证下面的公式是否成立:

$$e(V_i, P) = c_i e\left(M' + \sum_{j=1}^{n_m} m_i M_j, W_i\right)$$

若成立,则部分签名是正确的. 若所有的部分签名都正确,则计算:

$$V = \sum_{i=1}^{t} \eta_i V_i, \quad R_m = \sum_{i=1}^{t} \eta_i W_i$$

其中 $\eta_i = \prod_{j \in B, j \neq i} \frac{-j}{i-j}$

最终签名为 $\sigma = (V, R_u, R_m)$.

3.4 验证

接收者收到身份为 ID 的签名者对消息 m 的签名 σ

$= (V, R_u, R_m)$ 后,验证:

$$e(V, P) = e(P_2, P_1)\, e(U' + \sum_{i=1}^{n_u} id_i U_i, R_u)\, e(M' + \sum_{i=1}^{n_m} m_i M_i, R_m)$$

若公式成立,则签名是有效的.

4 签名方案分析

4.1 正确性分析

(1) 部分签名验证公式

$$\begin{aligned} e(V_i, P) &= e(S_i + w_i(M' + \sum_{j=1}^{n_m} m_j M_j), P) \\ &= e(S_i, P)\, e(M' + \sum_{j=1}^{n_m} m_j M_j, w_i P) \\ &= (\prod_{j=0}^{t-1} c_j^j)\, e(M' + \sum_{j=1}^{n_m} m_j M_j, W_i) \end{aligned}$$

(2) 门限签名验证公式

$$\begin{aligned} e(V, P) &= e(S_u + r_m(M' + \sum_{i=1}^{n_m} m_i M_i), P) \\ &= e(\alpha P_2 + r_u(U' + \sum_{i=1}^{n_u} id_i U_i) + r_m(M' + \sum_{i=1}^{n_m} m_i M_i), P) \\ &= e(P_2, \alpha P)\, e(U' + \sum_{i=1}^{n_u} id_i U_i, r_u P)\, e(M' + \sum_{i=1}^{n_m} m_i M_i, r_m P) \\ &= e(P_2, P_1)\, e(U' + \sum_{i=1}^{n_u} id_i U_i, R_u)\, e(M' + \sum_{i=1}^{n_m} m_i M_i, R_m) \end{aligned}$$

4.2 安全性证明

定义 4 门限签名是可模拟的,如果以下两个条件成立:

(1) 密钥分发过程是可模拟的. 存在模拟器,以系统参数 I、公钥 pk 和密钥生成过程中的公开数值为输入,能够模拟攻击者的视图.

(2) 门限签名生成过程是可模拟的. 存在模拟器,以系统参数 I、公钥 pk、消息 m 及其签名 σ 和 $t-1$ 个密钥分享输入,能够模拟攻击者的签名视图.

定理 1 如果基本签名方案是不可伪造的,并且相应的门限签名方案是可模拟的,则门限签名是不可伪造的.

引理 1 门限签名方案是可模拟的.

不失一般性,假设攻击者贿赂了 $t-1$ 个用户 $B_1, B_2, \cdots, B_{t-1}$.

(1) 密钥分发过程是可模拟的

给定系统参数 I 和身份 ID. 攻击者可以计算 $e(S_u, P) = e(P_2, P_1)\, e(U' + \sum_{i=1}^{n_u} id_i U_i, R_u)$. 由 $e(S_u, P) = \prod_{i=1}^{t} e(S_i, P)^{\eta_i}$ 可以计算出 B_i 的公开验证信息 $e(S_i, P)$. 因此,密钥分发过程是可模拟的.

(2) 签名算法是可模拟的

给定系统参数 I、身份 ID、消息 m 及其对应的签名 $\sigma = (V, R_u, R_m)$. 由 $R_m = \sum_{i=1}^{t} \eta_i W_i$ 和 $\sum_{i=1}^{t} \eta_i V_i$ 可分别计算出 W_t 和 V_t. 因此,签名过程是可模拟的.

定理 2 本文所提出的门限签名方案是安全的.

(1) 不可为造性:Paterson 已经证明基本方案是不可伪造的,而本文所提出的门限签名方案是可模拟的. 根据定理 1,本方案是不可伪造的.

(2) 健壮性:在本文方案的私钥分发和联合随机数的生成过程中,通过广播部分私钥和随机数的验证信息来保证接受者收到正确的份额,因此私钥分发和随机数的生成具有健壮性. 签名合成时通过验证公式 $e(V_i, P) = c_i e(M' + \sum_{j=1}^{n_m} m_j M_j, W_i)$ 即可判断签名成员是否诚实. 因此本方案是健壮的.

5 结论

本文以 Paterson 方案为基础,采用 Feldman 秘密共享方案分发密钥,构造了一种标准模型下可证安全的基于身份的门限签名方案. 该方案在 CDH 假设下是健壮的,并且可以抵抗适应性选择消息攻击.

参考文献:

[1] Y Desmedt, Y Frankel. Shared generation of authenticators and signatures[A]. Advances in Crypto '91[C]. Berlin: Springer-Verlag, 1992. 45 - 469.

[2] A Shamir. Identity-based cryptosystems and signature schemes [A]. Advances in Crypto '84[C]. Berlin: Springer-Verlag, 1984. 47 - 53.

[3] D Boneh, M Franklin. Identity based encryption from the weil pairing[A]. Proc. of Crypto '01[C]. Berlin: Springer-Verlag, 2001. 213 - 229.

[4] Baek J, Zheng Yu-liang. Identity-based threshold signature scheme from the bilinear pairings[A]. ITCC 04[C]. New York: IEEE Computer Society, 2004. 124 - 128.

[5] Chen Xiao-feng, ZHANG Fang-guo, Kwangjo Kim. New ID-based threshold signature scheme from bilinear pairings[A]. Progress in Indocrypt 2004[C]. Berlin: Springer-Verlag, 2004. 371 - 383.

[6] 刘颖,胡予濮,王飞,卢晓君. 一个高效的基于身份的门限签名方案[J]. 西安电子科技大学学报(自然科学版), 2006, 33(2): 311 - 315.
LIu Ying, Hu Yu-pu, Wang Fei, et al. An efficient ID-based threshold signature[J]. Journal of Xidian University, 2006, 33(2): 311 - 315. (in Chinese)

[7] Bellare M, Boldyreva A, Palacio A. An un-instantiable random oracle model scheme for a hybrid-encryption problem[A]. Ad-

vances in Eurocrypt 2004[C]. Berlin: Springer-Verlag, 2004. 171 - 188.

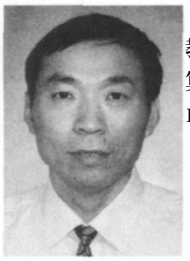
[8] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[A]. Proc of the 13th Annual ACM STOC[C]. New York: ACM Press, 1998. 209 - 218.

[9] 张乐友,胡予濮,刘振华. 标准模型下基于身份的可证安全门限签名方案[J]. 西安电子科技大学学报(自然科学版),2008,35(1):81 - 86.
Zhang Le-you, Hu Yu-pu, Liu Zhen-hua. Provable secure ID-based threshold signature scheme without random oracle. Journal of Xidian University, 2008, 35(1): 81 - 86. (in Chiese)

[10] Kenneth G Paterson, Jacob C N Schuldt. Efficient identity-based signatures secure in the standard model[A]. ACISP 2006[C]. Berlin: Springer-Verlag, 2006. 207 - 222.

[11] Feldman P. A practical scheme for non-interactive verifiable secret sharing[A]. Proc. of the 28th IEEE Symp on the Foundations of Computer Science[C]. New York: IEEE Computer Society, 1987. 427 - 437.

作者简介:



蔡永泉　男,1956 年生于安徽合肥,博士、教授、博士生导师. 主要研究方向为信息安全、计算机网络.
E-mail: cyq@bjut.edu.cn

张雪迪　男,1984 年 8 月生于山东淄博. 在读硕士研究生,主要研究方向为密码学.
E-mail: sk218zxd@163.com

姜　楠　女,1977 年 8 月生于山东,博士,讲师. 主要研究方向为信息安全.

(上接第 111 页)

[5] Mens T. A survey of software refactoring[J]. IEEE Transactions on Software Engineering, 2004, 30(2): 126 - 139.

[6] 刘辉,麻志毅,邵维忠. 模型转换中的特性保持的描述与验证[J]. 软件学报,2007,18(10):2369 - 2379.
Liu Hui, Ma Zhiyi, Shao Weizhong. Description and proof of property preservation of model transformations[J]. Journal of Software, 2007, 18(10): 2369 - 2379. (in Chinese)

[7] Barr Michael, Wells Charies. Category Theory for Computing Science[M]. New Jersey: Prentice-Hall, 1990.

[8] Bernardo M, Ciancarini P, Donatiello L. Architecting families of software systems with process algebras[J]. ACM Transactions on Software Engineering and Methodology, 2002, 11(4): 386 - 426.

[9] 顾宁,杨江明,张琦炜. 协同组编辑中基于地址空间转换的一致性维护方法[J]. 计算机学报,2007,30(5):763 - 774.
Gu Ning, Yang Jiangming, Zhang Qiwei. Consistency maintenance based on the address space transformation technique in group editors[J]. Chinese Journal of Computers, 2007, 30(5): 763 - 774. (in Chinese)

[10] Lu Ruqian. Towards a mathematical theory of knowledge[J]. Journal of Computer Science and Technology, 2005, 20(6): 751 - 757.