

限制联合验证者签名

王晓峰^① 林婷婷^{①②} 王尚平^① 张亚玲^①

^①(西安理工大学理学院 西安 710054)

^②(西南科技大学理学院 绵阳 621010)

摘要: 基于门限的思想, 该文提出一种新签名方案——限制联合验证者签名的精确定义和安全模型, 并构造了一个有效的限制联合验证者签名方案。新方案支持将消息的知情权和签名的验证权控制给 t 个验证者, 并且当且仅当 t 个验证者合作才能验证签名, 同时签名的长度不随验证者的增加而增加。在随机预言模型下, 新方案达到了所需的安全要求。

关键词: 门限; 多线性映射; 限制联合验证者签名; 指定验证者签名

中图分类号: TP309

文献标识码: A

文章编号: 1009-5896(2008)04-0991-04

Limited Confederate Verifier Signatures

Wang Xiao-feng^① Lin Ting-ting^{①②} Wang Shang-ping^① Zhang Ya-ling^①

^①(School of Sciences, Xi'an University of Technology, Xi'an 710054, China)

^②(School of Sciences, Southwest University of Science and Technology, Mianyang 621010, China)

Abstract: The precise definition and security model of a new signature scheme—limited confederate verifier signatures is proposed based on the idea of threshold. An efficient limited confederate verifier signatures scheme is also constructed for the first time. The new scheme allows confining the right to learn the message and the right to verify the signature within t verifiers, the signature can be verified iff all the t verifiers cooperate. Moreover, the size of the signature does not grow with the number of verifiers. The scheme is proved to achieve the desired security request under the random oracle model.

Key words: Threshold; Multilinear map; Limited confederate verifier signatures; Designated-verifier signatures

1 引言

作为密码学的重要内容, 数字签名已越来越广泛地应用到实际生活中。针对实际生活中的不同需求, 人们设计了各种数字签名方案。1989年 Chaum 提出的不可否认签名^[1], 其签名的验证必须要有签名者的合作。这在很大程度上控制了验证者的范围。近年来所提出的指定验证者签名^[2]中, 为了保护一些敏感信息, 签名的验证权由签名者来限制, 而且验证者不能向任何第三方传递该验证。在限制验证者签名^[3]和直接签名^[4]中, 只有签名者指定的验证者才能验证签名, 但在必要的情况下, 验证者可以向第三方证明签名的有效性, 限制验证者签名是通过揭示与原签名相关的信息提供证明(不暴露原签名), 而直接签名则通过揭示原签名提供证明。

上述签名方案都从不同程度上控制了签名验证权, 这在开放网络环境中可以提供隐私保护, 提高网络业务的可信度。但目前的限制验证者签名方案和直接签名方案都只能限制一个验证者, 这在很多应用场景中是有局限的, 我们曾在

另一篇文章中, 提出了“限制多方验证者签名”方案, 它允许限制多个验证者验证签名。

然而, 在现实生活中, 有时需要下述场景的隐私保护: 例如, 遗产的分配。立嘱人打算将其财产给他所希望的 t 个人, 但不希望此 t 人之外的任何人知道遗产分配办法, 所以立嘱人需要对消息——其财产的分配办法加密并签名, 指定给 t 个人验证, 只有这 t 个人才能得知遗产的分配办法。同时为了避免 t 个人互相残害(以获得更多的遗产份额), 只有当 t 个验证者合作才能验证签名的有效性。现实中这样的场景还有很多, 比如 t 个人合伙向银行贷款, 汽车的零部件生产等等。然而, 目前已知的签名方案中还没有能完全满足这种场景的解决方案。

基于以上客观需求, 本文设计一种新签名方案。新方案继承了指定多方验证者签名^[5]和门限加密^[6, 7]的特点, 但又与他们不同。与门限加密和门限签名^[8]的不同在于: 它不仅需要解密, 还需要验证签名的有效性; 签名者只有一个, 但验证者有多个。新方案的特点是: (1) 只有签名者限定的 t 个验证者才能得知被签名的消息; (2) 只有这 t 个验证者能验证签名; (3) 当且仅当这 t 个验证者合作才能验证签名。本文称之为限制联合验证者签名。新方案中签名的长度不随验证者数

2006-10-09 收到, 2007-05-15 改回

国家自然科学基金(60273089), 陕西省教育厅专项科学研究计划(06JK213), 陕西省自然科学基金基础研究计划(2005F02)和西安理工大学校科技创新基金(108210402)资助课题

目的增加而增加,并且在随机预言模型下达到了期望的安全需求。

2 预备知识

2.1 t -线性映射

t -线性映射(t -multilinear map)的概念是在文献[9]中首次提出的,描述如下:

定义 1 (文献[9]定义 2.1) 假设 G_1 和 G_2 是乘法群,称映射 $\hat{e}: G_1^t \rightarrow G_2$ 为 t -线性映射,如果满足以下性质:

(1) G_1 是 q 阶循环群,生成元是 g , G_2 也是 q 阶循环群。

(2) 如果 $a_1, a_2, \dots, a_t \in Z_q^*$, $x_1, x_2, \dots, x_t \in G_1$, 则 $\hat{e}(x_1^{a_1}, \dots, x_t^{a_t}) = \hat{e}(x_1, \dots, x_t)^{a_1 \cdots a_t}$ 。

(3) t -线性映射 \hat{e} 是非退化的,如果 $g \in G_1$ 是 G_1 的生成元,则 $\hat{e}(g, \dots, g)$ 是 G_2 的生成元。

2.2 基本数学问题

(1) 给定 $g, g^a \in G_1$, 计算 a 。该问题是著名的密码学困难问题——有限域上离散对数问题。

(2) 对于多项式 $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1} \pmod q$, 系数 a_i 未知, 其中 $i = 1, \dots, t-1$, 若只知 $r_i = f(d_i) \pmod q$, $i = 1, 2, \dots, t-1$, 则 a_0 的解有无穷多个。

3 限制联合验证者签名(LCVS)

3.1 限制联合验证者签名定义

系统由签名者 A 、验证者集合 $\{B_1, B_2, \dots, B_n\}$ 和指定合成者 DC(Designated Combiner)组成,假定 DC 是完全诚实的。给定参数 k , 限制联合验证者签名定义如下:

系统预设(Beforehand setup) 输入安全参数 k , 输出一个有限域上的 $t-1$ 次多项式 $f(x)$, 其中 $t \leq n$ 。签名者将验证者集合中每个验证者 B_i 在系统中的唯一身份作为 $f(x)$ 的输入, 输出每个验证者的秘密份额 r_i , 通过安全信道将 r_i 发送给每个验证者, $i \in \{1, \dots, n\}$, 将秘密 $f(0)$ 保密。

系统公共参数设置(Params setup) 这是一个概率算法, 输入安全参数 k , 输出系统公共参数。

密钥生成(keyGen) 这是一个概率算法, 输入公共系统参数, 输出每个用户的私钥/公钥对 (sk, pk) 。

限制联合验证者签名(LCVS.Sign) 这是一个概率算法, 输入消息 m 、签名者私钥 sk_A 、签名者秘密 $f(0)$ 以及签名者所限定的 t 个验证者的公钥, 不妨设为 $\{pk_1, pk_2, \dots, pk_t\}$, 其中 $t \leq n$, 输出签名 σ 。

限制联合验证者验证(LCVS.Ver) 这是一个确定算法, 输入签名 σ , 签名者公钥 pk_A , t 个验证者的秘密份额 r_i 和验证者各自的私钥 sk_i , 输出验证判断 $b \in \{0, 1\}$, 当 $b = 0$, 则拒绝签名, 否则接受。

3.2 限制联合验证者签名的安全模型

对于数字签名, 最强的安全概念是文献[10]中定义的抗适应性选择消息攻击存在伪造(EF-CMA)。在本文的限制联合验证者签名的安全模型中, 一个 EF-CMA 攻击者 Malice

不仅拥有签名者和所有验证者的公钥, 有权询问随机预言机 H 和签名预言机 Σ , 而且还拥有 t 个验证者的私钥和 t 份秘密份额。由于假定 DC 是完全诚实的, 所以, 这里 Malice 的攻击即是最强的攻击。而且, Malice 拥有 t 个验证者的私钥和 t 份秘密份额, 因此他自己可以验证签名, 所以验证预言机可以忽略。本文允许攻击者 Malice 针对消息 m 询问签名预言机, 但 Malice 对消息 m 的签名输出必须是 Σ 没有回答过的。

定义 2 (抗适应性选择消息攻击—存在伪造安全) 令 $\{B_1, B_2, \dots, B_t\}$ 是 t 个实体的集合, k 和 T 是整数, ϵ 是 $[0, 1]$ 中的实数, 令 LCVS 是一个以 k 为安全参数的限制联合验证者签名方案。令 A 是一个对 LCVS 的 EF-CMA 敌手。考虑下面的随机实验:

$\text{Exp}_{\text{LCVS}}^{\text{ef-cma}}(k)$:

(1) $\left. \begin{array}{l} \text{Beforehand setup} \\ \text{params setup} \end{array} \right\} \rightarrow \text{params}$

(2) $\text{keyGen}(\text{params}, A, B_1, \dots, B_t) \rightarrow (sk_A, pk_A)(sk_{B_1}, pk_{B_1}) \dots (sk_{B_t}, pk_{B_t})$

(3) $\text{Malice}^{H, \Sigma}(\text{params}, pk_1, \dots, pk_t, sk_1, \dots, sk_t, r_1, \dots, r_t, pk_A) \rightarrow \sigma$

(4) $\text{LCVS.Ver}(\sigma, pk_A, r_1, \dots, r_t, sk_i) \rightarrow b$, 其中 $i \in \{1, \dots, t\}$ 将 Malice 的成功概率定义为 $\text{Succ}(k) = \Pr[b = 1]$, LCVS 称作是 (k, T, ϵ) -EF-CMA 安全的, 如果不存在多项式时间攻击者 Malice 能在时间 T 内以概率 $\text{Succ}(k) \geq \epsilon$ 成功。

4 限制联合验证者签名方案(LCVS)

本节, 利用 Boneh 等人^[9]提出的一轮多方 Diffie-Hellman 密钥协商协议和门限的思想, 构造一种有效的限制联合验证者签名方案, 包括签名者 A 、验证者集合 $\{B_1, B_2, \dots, B_n\}$ 和指定合成者 DC。这种新签名支持只有签名者限定的 t 个验证者合作才能验证签名, 其中 $t \leq n$, 并且签名的长度不随验证者的增加而增加。

系统预设 设所有可能的验证者为集合 $\{B_1, B_2, \dots, B_n\}$, 签名者对所有可能的验证者预操作如下:

(1) 随机选择一个 $t-1$ 次的多项式 $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1} \pmod q$, 将 $f(x)$ 保密, 其中 $a_0 = f(0) \pmod q$ 也保密。(2) 假设每个验证者 B_i 在系统中拥有一个唯一身份 d_i , 签名者计算 $r_i = f(d_i) \pmod q$, $i = 1, 2, \dots, n$, 通过安全信道将 r_i 发送给每个验证者。

系统公共参数设置 q 是足够大的素数, G_1 是 q 阶乘法循环群, 生成元是 g , G_2 也是 q 阶乘法循环群, t -线性映射 $\hat{e}: G_1^t \rightarrow G_2$, 其中 $\hat{e}(g^{a_1}, \dots, g^{a_t}) = \hat{e}(g, \dots, g)^{a_1 \cdots a_t}$, $H_1: \{0, 1\}^l \times G_2 \rightarrow Z_q^*$, $H_2: Z_q^* \times G_2 \rightarrow \{0, 1\}^l$, $H_3: \{0, 1\}^l \rightarrow Z_q^*$, $H_4: \{0, 1\} \times G_1 \rightarrow Z_q^*$, 其中 l 表示消息比特长度的界。系统公共参数为: $\{q, G_1, G_2, \hat{e}, H_1, H_2, H_3, H_4, l\}$

密钥生成 每个用户随机选取 $x_u \in Z_q^*$, 计算 $y_u = g^{x_u}$,

则用户私钥/公钥对为 (x_u, y_u) 。

签名 签名者 A 对所希望的 t 个验证者, 不妨设为 $\{B_1, B_2, \dots, B_t\}$, 签名如下: 计算 $R = H_3(m)$; 任选 $k \in Z_q^*$, 计算 $W = g^{R-k}$; 任选 $u \in Z_q^*$, 计算 $Q = g^u \cdot (W)^{-f(0)R} \bmod q$; 计算 $\mu = H_1(m, \hat{e}(y_1, \dots, y_t)^u)$, $\omega = H_4(m, W)$; 计算 $S = -x_A \mu \omega + k \bmod q$; 计算 $P = \hat{e}(y_1, \dots, y_t)^{x_A}$; $M = H_2(S, P) \oplus m$; 签名即是 $\sigma = (M, Q, W, S)$ 。

验证 每个验证者都进行如下相同的操作:

(1) 计算 $P = \hat{e}(y_1, \dots, y_{i-1}, y_A, y_{i+1}, \dots, y_t)^{x_i}$, $m = H_2(S, P) \oplus M$, $R = H_3(m)$, $sh_i = r_i \prod_{j \neq i, j=1}^t \frac{-d_j}{d_i - d_j} \bmod q$, 将 $(sh_i R, W)$

提交给 DC, DC 计算 $C = W^{\left[\sum_{i=1}^t sh_i R \right]}$, 并将 C 发送给每个验证者。(这里假设 DC 是诚实的, 不会故意发送错误信息给验证者或与攻击者勾结)

(2) 计算 $g^u = Q \cdot C$, $\mu = H_1(m, \hat{e}(g^u, y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_t)^{x_i})$, $\omega = H_4(m, W)$

(3) 验证是否 $g^R = W \cdot y_A^{\mu} \cdot g^S$, 若成立, 说明该签名确实是由签名者 A 对验证者 $\{B_1, B_2, \dots, B_t\}$ 的签名。

5 安全性证明

正如在第3节所述, 数字签名最重要的安全概念是不可伪造性。考虑第3节所述最强攻击下的抗适应性选择消息攻击存在伪造(EF-CMA)安全性。并假定 DC 是完全诚实的。

定理 1 在随机预言模型下, 如果存在 LCVS 的攻击者 Malice 分别经过 q_{H_1} , q_{H_2} , q_{H_3} , q_{H_4} 次的 H_1, H_2, H_3, H_4 的 hash 询问和 q_Σ 次签名询问后, 能以优势 ϵ , 在时间 T 内成功伪造本文提出的新方案, 则存在算法 Sim 能在时间 $T_0 \leq 2(T + q_{H_4} \cdot \tau + q_\Sigma \cdot \tau)$, 以优势 $\epsilon_0 \geq (\epsilon - q_\Sigma 2^{-l})/q^2$ 解有限域中离散对数问题。

证明 假设 Malice 与 t 个验证者勾结, 拥有 t 个验证者的所有秘密信息, 即验证者私钥和秘密份额 r_i 。签名者的公钥为 $y_A = g^{x_A}$ 。构造算法 Sim, 假设 Malice 在适应性选择消息攻击下能成功伪造本文的新方案中的签名, 则 Sim 可以利用 Malice 解离散对数问题。(在这个攻击系统中, Malice 唯一不知道的是签名者私钥 x_A)。

Hash 询问 (1) 对于 hash 函数 H_1, H_2, H_3 , 当 Malice 询问时, Sim 利用正确的 H_1, H_2, H_3 函数进行回答, 并将答案存入 H_1 、 H_2 和 H_3 列表。(2) H_4 询问: 当 Malice 提交 (m, W) 给 H_4 预言机, Sim 首先检查 H_4 列表中是否存在 (m, W, ω) , 若存在, 则返回 ω 。否则, Sim 随机选取 $\omega \in Z_q^*$, 将 ω 返回, 并将 (m, W, ω) 存入 H_4 列表。

签名询问 当 Malice 提交消息 m_0 进行签名询问, Sim 首先检查 H_4 列表, 如果 m_0 已存在列表中, Sim 终止。否则, Sim 计算 $R_0 = H_3(m_0)$, 任选 $u_0 \in Z_q^*$, 计算 $\mu_0 = H_1(m_0, \hat{e}(y_1, \dots, y_t)^{u_0})$, 任选 $\omega_0, k_0 \in Z_q^*$, 计算 $W_0 = (y_A^{-1})^{\mu_0 \omega_0}$

$\cdot g^{-k_0}$, 同时, 将 (m_0, W_0, ω_0) 存入 H_4 列表。然后计算 $Q_0 = g^{R_0} \cdot W_0^{\sum_{i=1}^t sh_i}$, $S_0 = R_0 + k_0 \bmod q$, $M_0 = H_2(S_0, \hat{e}(y_1, \dots, y_{i-1}, y_A, y_{i+1}, \dots, y_t)^{x_i}) \oplus m_0$, 则 Sim 将 $\sigma_0 = (M_0, Q_0, W_0, S_0)$ 发送给 Malice 作为对消息 m_0 的回答, 经过验证可知这是一个有效的签名。

伪造输出 假设 Malice 伪造消息 m^* 的有效签名 $\sigma^* = (M^*, Q^*, W^*, S^*)$, 经过一系列的验证步骤能够得到式(1):

$$g^{R^*} = W^* \cdot y_A^{\mu^*} \cdot g^{S^*} \quad (1)$$

由分叉引理, 对同样的消息 m^* , W^* , μ^* , Sim 改变对 H_4 的回答, 又可从 Malice 处获得另一有效签名 $\sigma' = (M', Q', W', S')$, 从该签名可得到式(2):

$$g^{R^*} = W^* \cdot y_A^{\mu^*} \cdot g^{S'} \quad (2)$$

将式(1)和式(2)相比, Sim 可以得到:

$$\begin{aligned} y_A^{\mu^* \omega^* - \mu^* \omega'} g^{S^* - S'} &= g^0 \Leftrightarrow x_A (\mu^* \omega^* - \mu^* \omega') + (S^* - S') \\ &= 0 \Leftrightarrow x_A = (S' - S^*) (\mu^* \omega^* - \mu^* \omega')^{-1} \end{aligned}$$

从而 Sim 利用 Malice 伪造的签名, 可以解决有限域上离散对数问题。由于 Sim 在签名询问中会因为 m_0 已存在于 H_4 列表而终止的最大概率是 $q_\Sigma 2^{-l}$, 所以由分叉引理^[11], Sim 至多在时间 $T_0 \leq 2(T + q_{H_4} \cdot \tau + q_\Sigma \cdot \tau)$ 内成功解决有限域上离散对数问题的概率至少是 $\epsilon_0 \geq (\epsilon - q_\Sigma 2^{-l})/q^2$, 其中 τ 是回答 hash 询问的时间。证毕

6 结束语

本文基于实际生活中的一些客观需求, 提出了一种新的签名方案——限制联合验证者签名方案的精确定义和安全模型, 并构造了一个有效的方案, 该签名方案不仅将消息保密, 而且仅仅允许签名者所限定的 t 个验证者合作, 才能验证签名的有效性。虽然多线性对运算并不高效, 但是, 由于对的运算可以预先计算并保存到数据库中, 所以并不影响本文方案的效率。而且, 本方案所生成的签名只有 4 项, 并且签名的长度不随验证者的增加而增加。本文的方案在随机预言模型下达到了所需的安全需求。

本文保留以下问题作为公开问题, 以便对限制联合验证者签名更进一步研究: (1) 如果有验证者由于客观原因(比如意外死亡)确实不能参与签名的验证, 是否可以让 DC 代为参与。(2) 考虑由 DC 或某个验证者向仲裁者证明签名确由签名者生成。

参考文献

- [1] Chaum D and Antwerpen H van. Undeniable signatures. Advances in Cryptology-Crypto 1989, LNCS 435, 212-216.
- [2] Steinfeld R, Bull L, Wang H, and Pieprzyk J. Universal designated-verifier signatures. Advances in Cryptology-Asiacrypt 2003, LNCS 2894: 523-542.
- [3] Chen Xiaofeng, Zhang Fangguo, and Kim Kwangjo. Limited verifier signatures from bilinear pairings. ACISP 2004: 313-

- 324.18, EE. [Http://caislab.Icu.ac.kr/paper/2004/ACNS/](http://caislab.Icu.ac.kr/paper/2004/ACNS/)
- [4] Laguillaumie F, Paillier P, and Vergnaud D. Universally convertible directed signatures. Proc. of Asiacrypt'05. 2005, LNCS Vol. 3788: 682-701.
- [5] Laguillaumie F and Vergnaud D. Multi-designated verifiers signatures. In Information and Communications Security-ICICS 2004, LNCS, vol. 3269: 495-507.
- [6] Gemmel P. An introduction to threshold cryptography. *RSA CryptoBytes*, 1997, 2(3): 7-12.
- [7] Dan Boneh, Xavier Boyen, and Shai Halevi. Chosen ciphertext secure public key threshold encryption without random oracles. Manuscript, 2005. <http://crypto.Stanford.edu/~dabo/abstracts/threshold.html>.
- [8] Lal S and Kumar M. A directed threshold-signature scheme. eprint arXiv:cs/0411005. <http://arxiv.org/abs/cs/0411005>.
- [9] Boneh D and Silverberg A. Applications of multi-linear forms to cryptography. Report2002/080, <http://eprint.Iacr.Org>, 2002.
- [10] Goldwasser S, Micali S, and Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. of Computing*, 1988. 17(2): 281-308.
- [11] 毛文博. 现代密码学理论与实践. 北京: 电子工业出版社, 2004: 549-566.
Mao Wenbo. Modern Cryptography: Theory and Practice. Beijing: Publishing House of Electronics Industry, 2004: 549-566.
- 王晓峰: 女, 1966年生, 副教授, 硕士生导师, 研究方向为密码理论与网络安全.
- 林婷婷: 女, 1982年生, 硕士生, 研究方向为密码理论与网络安全.
- 王尚平: 男, 1963年生, 教授, 研究方向为密码理论与网络安全.
- 张亚玲: 女, 1966年生, 副教授, 研究方向为信息安全理论与技术.