一种标准模型下的强指定验证者签名方案①

师鸣若

(北京物资学院, 北京 101149)

摘 要: 强指定验证者签名方案(SDVS)能让指定的接收方确认消息发送方的身份, 但不能向第三方证明发送方的身份, 在电子商务和电子政务中有广泛应用. 在DBDH问题和Gap BDH问题困难的前提下, 利用双线性对, 构造了基于身份的强指定验证者签名方案, 并在标准模型下证明了方案的安全性. 分析结果表明新提出的方案具有签名者身份的隐私性、不可传递性以及对签名验证的不可委托性. 该方案使用双线性对, 不需要证书, 可简化密钥管理; 其通信和计算效率高, 实现简单, 可用于计算能力受限的设备.

关键词: 双线性映射; 强指定验证者签名; 标准模型; 签名者身份的隐私性; 不可委托性

Strong Designated Verifier Signature Scheme under Standard Model

SHI Ming-Ruo

(Beijing Wuzi University, Beijing 101149, China)

Abstract: Strong designated verifier signature scheme enables the designated receiver to identify the source of a received message and prevent a third party from identifying the source of the message, which is well suitable for E-commerce and E-government applications. Based on decisional bilinear Diffie-Hellman assumption and gap bilinear Diffie-Hellman assumption, using bilinear pairing, a new strong designated verifier signature scheme is proposed. The security of the scheme is proved under standard model. The analytical results show that the new proposed protocol has unforgeability, non-transferability, privacy of the signer's identity and non-delegatability for signature verification. This scheme is based on bilinear pairing, which means that it needs no certificate and has a simple key management. On the other hand, it is efficient in communications and computation, and implementation is simple, so that it could be implemented in mobile devices with low power and small processor.

Key words: bilinear mapping; designated verifier signature; standard model; privacy of the signer's identity; non-delegatability

数字签名是电子商务的重要安全组件, 用于实现商务应用中的完整性和不可抵赖性. 然而标准的数字签名方案中, 任何人都可以验证数字签名的有效性, 这不能有效保护签名者的身份, 因而网络安全中指定验证者签名(DVS)成为研究热点. 1996 年文献[1]提出了指定验证者概念. 在指定验证者签名方案中, 只有指定的验证者才能验证签名的有效性, 而且验证者不能向第三方验证该签名来自特定签名者, 即该方案具备: (1)消息认证功能; (2)可否认性. 目前, 研究工作集中在环签名[2,3]、通用指定验证者签名[4,5]、多指定验证者签名[3]以及基于身份的指定验证者签名[6]的设计和分析, 使其满足如下安全属性: (1)不可传递性, 除非知道指定验证者的私钥, 任何第三方不能生成有效的签名副本; (2)签名身份隐私性(PSI), 第三方除非知道指定验证者的私钥, 否则不能判断签名者是签名者还是指定验证者; (3)不可委托性, 指定验证者能证明签名的有效性, 但不能将签名验证过程转移给第三方.

具有PSI属性的DVS称为强指定验证者签名(SDVS),

① 基金项目:十一五国家科技支撑计划重点项目(2009BAH46B06); 北京市教委专项(PXM2012_014214_000067,PXM2012_014214_000022)
收稿时间:2012-07-18;收到修改稿时间:2012-09-03

2004 年文献[7]定义了强指定验证者签名, 即验证阶段需要验证者私钥的参与才能完成. SDVS 在投票、微博及艺术品拍卖等新兴的电子商务及电子政务应用有广泛的应用前景. 例如在电子选举投票或项目投标中, 唱票中心需要确认投票者投票行为的真实性及投票者身份的可验证性, 然而, 又不希望第三方证实投票者身份. 在微博实名制验证中, 指定验证者签名既可以保护网民身份的隐私, 又可为监管者提供身份验证, 从而有效地抵制网络谣言的滋生. 文献[8,9]给出了两种随机预言模型下的 SDVS 方案, 随机预言器在现实中用 Hash 函数代替, 因此随机预言模型下的方案往往不能保证现实方案的安全性. 文献[10]和文献[11]分别提出了基于标准模型证明的 SDVS 方案, 其中文献[10]基于伪随机函数, 其安全假定强, 而文献[11]没有给出 PSI 安全性的证明.

2005 年 Waters 等提出了的基于身份的加密方案, 并在标准模型下给出了安全证明[12].

本文基于 Waters 的加密方案, 提出了一种基于身份的 SDVS 方案, 具有签名者身份隐私性(PSI)、不可传递性及不可委托性, 并在标准安全模型下给出了证明. 与现有方案相比, 其安全性和性能都具有优势.

1 预备知识

设 $(G,.)$ 和 $(G_T,.)$ 是两个 p 阶循环群, g 是 G 的生成元, $e:G\times G\to G_T$ 是双线型映射, 满足性质:

(1) 双线性性: 任意 $Q,R\in G, a,b\in Z_p$, 有等式 $e(Q^a,R^b)=e(Q,R)^{ab}$ 成立.

(2) 非退化性: $e(g,g)\neq 1$.

(3) 可计算性: 任意 $Q,R\in G$, 存在有效算法计算 $e(Q,R)$.

BDH 问题: 假定 p 阶循环群 $(G,.)$ 和 $(G_T,.)$, g 是 G 的生成元, 给定 $(g,g^a,g^b,g^c\in G)$, 计算 $e(g,g)^{abc}$, 其中 $a,b,c\in Z_p$ 未知.

DBDH 问题: 假定 p 阶循环群 $(G,.)$ 和 $(G_T,.)$, g 是 G 的生成元, 给定 $(g,g^a,g^b,g^c\in G)$, 其中 $a,b,c\in Z_p$ 未知, 以及 $Z\in G_T$, 判断 $Z=e(g,g)^{abc}$ 是否成立.

DBDH 预言器 O_{DBDH}: 以 $g,g^a,g^b,g^c\in G$ 和 $Z\in G_T$ 作为输入, 若 $Z=g^{abc}$, 输出 1, 否则输出 0.

GBDH 问题: 给定 (g,g^a,g^b,g^c), 其中 $a,b,c\in Z_p$ 未知, 在 O_{DBDH} 的帮助下, 计算 $e(g,g)^{abc}$. GBDH 假定是指求解 GBDH 问题的概率 $Succ_A^{GBDH}$ 是可忽略的.

基于身份的强指定验证者签名方案通常由以下五个算法组成:

参数生成算法(Setup): 给定安全参数 1^k, 系统输出系统参数 param.

密钥生成算法(Extract): 输入安全参数 1^k, PKG 生成公私钥对 (pk_i,sk_i), 其中 $i\in\{S,V\}$. 公开公钥 pk_i, 并通过安全信道将私钥 sk_i 发送给签名者.

签名生成算法(Sign): 算法以签名者 S 私钥 sk_s, 指定验证者 V 公钥 pk_v, 对消息 m 签名得到 σ, 并将 (m,σ) 发送给验证者 V.

签名验证算法(Verify): 当得到消息 m, 签名 σ', V 使用自己的私钥 sk_V, 签名者公钥 pk_S, 执行本算法, 如果签名有效, 返回 1, 否则返回 “Invalid”.

副本生成算法(Transcript): 将指定验证者 V 私钥 sk_V, 签名者 S 公钥 pk_S, 消息 m 作为算法输入, 输出签名副本 σ', 满足 σ' 与 σ 同分布而且不可区分.

2 强指定验证者签名方案

G, G_T, e, S, V 如上节所定义, $|G|=|G_T|=p$, 其中 p 为素数, 假定消息 M 的长度为 n 比特. 为了支持任意长度消息, 可使用一个抗碰撞哈希函数. 方案细节如下:

参数生成算法: g 是 G 的任意生成元, 任选 m', 及 n 维向量 $\mathbf{m}=(m_i)$, 其中 $m',m_i\in G$. 公开参数 param 为 $(G,G_T,e,m',\mathbf{m})$.

密钥生成算法: 签名者 S 选择 $x_S,y_S\in_R Z_p^*$, 私钥 $sk_S=(x_S,y_S)$, 公钥 $pk_S=(pk_{1_S},pk_{2_S})=(g^{x_S},g^{y_S})$. 类似地, 验证者 V 选择 $x_V\in_R Z_p^*$, 私钥 $sk_V=x_V$, 公钥 $pk_V=g^{x_V}$.

签名生成算法: 设 M 为待签名 n 比特消息, M_i 表示 M 的第 i 比特, $\tilde{M}=\{i\mid M_i=1\}\subseteq\{1,2,...,n\}$. S 选择 $r\in_R Z_p^*$, 计算 $\sigma_1=g^r$, $\sigma_2=e(g^{x_Sy_S}(m'\prod_{i\in\tilde{M}}m_i)^r,g^{x_V})$, 输出 $\sigma=(\sigma_1,\sigma_2)$ 作为签名.

签名验证算法: 当得到消息 M 和签名 $\sigma'=(\sigma_1',\sigma_2')$ 后, 验证者 V 使用私钥 sk_V 验证等式 $\sigma_2'=e(g^{x_S},g^{y_S})^{x_V}e(m'\prod_{i\in\tilde{M}}m_i,\sigma_1')^{x_V}$ 是否成立. 若等式成立, V 接受 σ', 返回 1, 否则返回 “invalid”.

副本生成算法: 给定消息 M', 验证者选择

$r'\in_R Z_p$，计算签名副本(σ_1', σ_2'). 其中$\sigma_1' = g^{r'}, \sigma_2' = e(g^{x_S}, g^{y_S})^{x_V} e(m'\prod_{i\in\tilde{M}'} m_i, \sigma_1')^{x_V}$.

3 协议安全性分析

本节论证方案的正确性和安全性、不可伪造性、不可传递性和签名验证不可委托性.

定理 1. 正确性.

证明: 方案的正确性验证如下:

$$\begin{aligned}\sigma_2 &= e(g^{x_S y_S}(m'\prod_{i\in\tilde{M}} m_i)^r, g^{x_V}) \\ &= e(g^{x_S y_S}, g^{x_V}) e((m'\prod_{i\in\tilde{M}} m_i)^r, g^{x_V}) \\ &= e(g^{x_S}, g^{y_S})^{x_V} e((m'\prod_{i\in\tilde{M}} m_i), \sigma_1)^{x_V}\end{aligned}$$

定理 2. 不可伪造性. 标准模式下, 如果敌手 A 能以不可忽略的优势ε对方案进行签名伪造, 则应答者 B 可以$O(\varepsilon)$优势ε'利用 A 求解 GBDH 问题.

证明: A 在多项式时间 t 内, 可向 B 签名查询q_s次、模拟签名查询q_{sim}次及签名验证查询q_v次. 假定 B 收到(g, g^a, g^b, g^c), g 是 G 的生成元, B 利用 DBDH 预言模型O_{DBDH}和 A 来计算$e(g,g)^{abc}$.

参数生成: 设$l = 4(q_s + q_{sim} + q_v)$，选择$k \in_R [0, n)$, 选择整数$x'$和 n 维变量$x = (x_i)$, 其中$x', x_i \in_R Z_l$; 选择指$y'$和 n 维变量$y =_R (y_i)$, 其中$y', y_i \in_R Z_p$. B 内部保存这些值, 然后设置: 签名者公钥$pk_S = (pk_{1_S}, pk_{2_S}) = (g^a, g^b)$; 签名验证者公钥$pk_V = g^c$; 令$m' = pk_{2_S}^{p-kl+x'} g^{y'}$, $m_i = pk_{2_S}^{x_i} g^{y_i}$及$\vec{m} = \{m_1, m_2, ..., m_n\}$.有$(m'\prod_{i\in\tilde{M}} m_i) = pk_{2_S}^{F(M)} g^{J(M)}$成立. B 将公共参数$(G, G_T, e, p, g, m', \vec{m})$和公钥$(pk_{1_S}, pk_{2_S}, pk_V)$发送给 A.

签名查询和模拟查询: 当A查询消息M的签名时. 模拟器 B 处理: 若$K(M) = 0$, 挑战失败, B 终止模拟. 否则对任意p, n, l，有$p > nl$成立[12], 即$F(M) \neq 0 (\mathrm{mod}\, p)$. B 选择$r \in_R Z_p$，计算$\sigma = (\sigma_1, \sigma_2)$, 其中:

$$\sigma_1 = pk_{1_S}^{-1/F(M)} g^r,$$

$$\sigma_2 = e(pk_{1_S}^{-J(M)/F(M)} (m'\prod_{i\in\tilde{M}} m_i)^r, pk_V)$$

签名验证查询: 假定 A 提交签名(M, σ)查询. 若$F(M) = 0$, B 向O_{DBDH}提交(g , g^a , g^b , g^c , $\sigma 2/(e(g^c, \sigma_1))^{J(M)}$). 若O_{DBDH}返回 1, B 输出“valid”, 否则 B 输出 “invalid”. 如果 B 不跳过, A 伪造签名(M^*, σ^*)的概率为.

概率分析: 令模拟过程中 B 跳过的事件为E_1. E_1成立需要B满足两个条件[12], 即β: 在签名生成查询、模拟查询和验证查询过程中 B 不跳过; γ: $F(M^*) = 0 (\mathrm{mod}\, p)$. 则 B 解决 GBDH 问题概率:

$$Succ_B^{GBDH} \geq 9/(16(n+1)(q_s + q_{sim} + q_v))\varepsilon .$$

定理 3. 该协议具有不可传递性, 即签名者生成的签名和验证者创建的副本之间不可区分.

证明: 为证明 S 生成的签名σ和 V 生成签名副本σ'不可区分, 只需验证σ和σ'同分布. 首先 S 和 V 选择$r, r' \in_R Z_p^*$, 并计算(σ_1, σ_2)和(σ_1', σ_2'). 如果$r = r'$, 则$(\sigma_1, \sigma_2) = (\sigma_1', \sigma_2')$. 设$(\overline{\sigma_1}, \overline{\sigma_2})$是 S 产生的签名集合的随机实例，有$\Pr[(\sigma_1, \sigma_2) = (\overline{\sigma_1}, \overline{\sigma_2})] = 1/(p-1)$, 即两者的概率分布相同, 因此满足不可传递性.

定理 4. 协议具有签名者身份隐私性(PSI).

证明: 需证明A对S的私钥具有不可区分性. 设A是$(t, q_s, q_v, \varepsilon)$签名者隐私区分器, 则模拟器 B 在时间$t'$以概率$\varepsilon'$攻破 DBDH 的随机实例$(g, g^{a_0}, g^{a_1}, g^c, Z)$, 其中$a_0, a_1, c \in_R Z_p$且秘密保存. B 的目标是输出$e(g,g)^{a_0 a_1 c} = Z$是否成立.

参数建立: B 选择值y'和随机向量$y = (y_i)$, 其中$y', y_i \in Z_p$，并秘密保存. 对消息 M 定义函数$J'(M) = y' + \sum_{i\in\tilde{M}} y_i$. B 选择$b_0$和$b_1 \in_R Z_p$，置签名者$S_0$和$S_1$的公钥分别为$pk_{s_0} = (g^{a_0}, g^{a_1})$和$pk_{s_1} = (g^{b_0}, g^{b_1})$. 指定验证者 V 公钥为$pk_V = g^c$. B 设置$k_{S_0 V} = Z$为$S_0$与 V 的共享秘密，$k_{s_1 V} = (g^{b_0}, g^c)^{b_1}$. 其中$g^{a_0}$，$g^{a_1}$，$g^c$和，是该 DBDH 问题的输入. B 设置$m' = g^{y'}$和$m_i = g^{y_i}$及$\vec{m} = (m_1, m_2, ..., m_n)$. B 将$(G, G_T, e, p, g, m', m)$和$(pk_{S_0}, pk_{S_1}, pk_V)$发生给 A.

签名查询: 敌手 A 提交签名(M, S_d)查询, 其中$d = \{0,1\}$. 模拟器 B 选择$r \in_R Z_p$，利用 V 和S_d的共享秘密, 计算签名$\sigma = (\sigma_1, \sigma_2)$，其中$\sigma_1 = g^r$，$\sigma 2 = k_{S_d V} e((m'\prod_{i\in\tilde{M}} m_i), g^c)^r$.

签名验证查询: A 发送签名验证查询(M, σ, d). B 知道$k_{S_d V}$和$J'(M)$,因此使用$\sigma_2 = k_{S_d V} e(\sigma_1, g^c)^{J'(M)}$验签. A 提交挑战消息$M^*$, B 选择$d \in_R \{0,1\}$，并返回$\sigma^*$. A 输出$d'$，如果$d' = d$，则 B 输出 1, 否则返回 0. 如果 B 输出 1 且 d=0, 则求解了给定的 DBDH 问题.

假定 A 区分签名者身份的优势是ε，则 B 求解给定 GBDH 问题的概率为$\varepsilon/2$.

定理 5. 协议具有签名验证的不可委托性.

证明: 需证明若签名验证者 A 能在多项式时间内违反签名验证不可委托性, 则存在算法 B 能解决给定的 BDH 问题. 给定 BDH 问题的随机实例 (g,g^a,g^b,g^c), B 的目标是利用 A 计算 $e(g,g)^{abc}$. B 采用与定理 2 证明中相同方法应答 A 的签名和签名副本查询. 如果在模拟过程中 B 不跳过, 且 A 能输出 1, 这意味者该签名是有效的. 当 $F(M)=0$, B 则计算求解指定的 BDH 问题, 即 $e(g,g)^{abc}=(\sigma_2/e(g_c,\sigma_1))^{J(M)}$.

B 成功的概率为 $\varepsilon'=Suss_B^{BDH}=\Pr[\beta\wedge\gamma]\varepsilon$, $\Pr[\beta\wedge\gamma]$ 定义同定理 2.

4 性能和安全性比较

本文方案与已有的可证明 DVS 方案的安全特性比较见表 1. 文献[8]不具有 PSI 属性, 且基于随机预言模型. 本方案基于标准模型, 且签名验证具有不可委托性.

表 1 本文方案与方案[8]的安全性比较

方案	不可委托性	PSI	不可传递性
文献[8]方案	√	×	√
本文方案	√	√	√

本文方案签名: 计算 σ_1 需要一次幂运算; 计算 σ_2, 可缓存 $g^{x_S y_S}$ 和 g^{x_V}, 故需幂运算 $(m'\prod_{i\in\tilde{M}}m_i)^r$ 和双线性对运算各一次. 验证签名: 计算 σ_2', 可缓存 $e(g^{x_S},g^{y_S})^{x_V}$, 故需幂运算和双线性对运算各一次. 与文献[8]方案的比较见表 2, 表明本文方案的运算量更小.

表 2 本方案与已有方案的运算效率比较

方案	文献[8]方案		本文方案	
	签名	验证	签名	验证
双线性对次数	0	1	1	1
幂运算次数	3	2	2	1

5 结语

提出了一种新的强指定验证者签名方案, 可解决在电子商务及电子政务实践中的大量涉及有限个指定验证者的应用, 不仅满足不可伪造性基本要求, 且不能向第三方证实发送方的真实身份. 使用双线性对函数, 故使用短密钥, 设计简单, 可用于计算能力、存储空间受限的设备上, 如智能卡、PDA 等.

参考文献

1 Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications. In: Markus J, ed. Eurocrypt'96. LNCS 1070, Springer, 1996:143–154.

2 Rivest R, Shamir A, Tauman Y. How to leak a secret. In: Boyd C, ed. ASIACRYPT'01. LNCS 2248, Springer, 2001: 552–565.

3 Shacham H, Waters B. Efficient ring signatures without random Oracles. In: Okamoto T, ed. PKC'07. LNCS 4450, Springer, 2007: 166–180.

4 Steinfeld R, Bull L, Wang H, Pieprzyk J. Universal designated verifier signatures. In: Laih C, ed. ASIACRYPT'03. LNCS 2894, Springer, 2003: 523–542.

5 Zhang R, Furukawa J, Imai H. Short signature and universal designated verifier signature without random oracles, ACNS'05. LNCS 3531, Springer, 2005: 135–173.

6 Huang X, Susilo W, Mu Y, Zhang F. Short designated verifier signature scheme and its identity-based variant. International Journal of Network Security, 2008,6(1):82–93.

7 Saeednia S, Kramer S, Markovitch O. An Efficient Strong Designated Verifier Signature Scheme. ICISC'03. LNCS 2971, Springer, 2004:40–54.

8 Huang Q, Yang G, Wong DS, Susilo W. Identity-based strong designated verifier signature revisited. International Journal of Systems and Software, 2011,84(1):120–129.

9 Laguillaumie F, Vergnaud D. Multi-designated verifiers signatures. In: Lopez J, ed. ICICS'04. LNCS 3269, Springer, 2004: 495–507.

10 Huang Q, Yang G, Wong DS, Susilo W. Efficient strong designated verifier signature schemes without Random Oracle or with non-delegatability. International Journal of Information Security, 2011,10(6):373–385.

11 Zhang J, Ji C. An efficient designated verifier signature scheme without Random Oracles. ISDPE'07. IEEE Computer Society, 2007:338–340.

12 Waters B. Efficient identity based encryption without random oracles. Eurocrypt'05. LNCS 3494, Springer, 2005: 114–127.