文章编号:1001 - 9081(2009)06 - 1643 - 03

无证书广义指定多个验证者有序多重签名

韩亚宁,王彩芬
(西北师范大学 数学与信息科学学院,兰州 730070)
(hanyaning86@126.com)

摘 要:有序多重签名方案一般都是基于离散对数或身份的,存在着证书管理问题或是密钥托管问题。广义指定多个验证者签名体制允许签名的持有者指定多个签名的验证者,只有被指定的验证者可以验证签名的有效性。将无证书签名体制和广义指定多个验证者签名体制相结合,提出了无证书广义指定多个验证者有序多重签名方案及其安全模型。在随机预言模型下的安全性分析表明:该方案可以抵抗适应性选择消息攻击,其不可伪造性基于 BDH 困难假设。

关键词:无证书;有序多重签名;广义指定多个验证者;BDH 问题
中图分类号: TP309.08 **文献标志码**:A

Certificateless universal designated multi-verifiers sequential multi-signature scheme

HAN Ya-ning, WANG Cai-fen
(*College of Mathematic and Information Science, Northwest Normal University, Lanzhou Gansu 730070, China*)

Abstract: Sequential multi-signature schemes were based on discrete logarithm problem or identity, and existed certificate management and key escrow problems. Universal designated multi-verifiers signature scheme allowed a signature holder to designate a set of signature verifiers, in such a way that only designated verifiers could verify the efficiency of the signature. Combining certificateless signature with universal designated multi-verifiers signature, certificateless universal designated multi-verifiers sequential multi-signature scheme and its safety requirement were proposed. Security proofs based on the random oracle model indicate that this scheme can resist the adaptively select of message attack, and its security relies on the BDH assumption.

Key words: certificateless; sequential multi-signature; universal designated multi-verifiers; BDH problem

0 引言

多重签名指多个签名者合作产生对同一个消息的签名[1],而签名时若需要多个签名者以严格的次序进行签名,就需要有序多重签名[2]。目前所提出的有序多重签名都是基于离散对数和身份的,存在着证书管理问题和密钥托管问题,在实际应用中效率低下[3-4]。

在无证书公钥密码体制中密钥产生中心(Key Generation Center, KGC)只为用户产生部分私钥,用户自己再选择一个秘密值,两者共同产生用户私钥,从而解决了证书管理问题和密钥托管问题[5-7]。

广义指定验证者签名体制是一种保护签名者隐私的重要方法,它有着特殊的功能——允许签名的持有者去指定签名的验证者,只有指定的验证者才能够验证签名是否有效,但他并不能向其他任何人证明这一事实[8-9]。

基于以上研究,提出了无证书广义指定多个验证者有序多重签名方案及其安全模型。

1 基础知识

1.1 双线性对

令 G_1 为由 P 生成的阶为 q 的循环加法群,G_2 为具有相同阶 q 的循环乘法群,$a,b \in \mathbf{Z}_p^*$。假设 G_1 和 G_2 两个群中的离散对数问题都是困难问题。双线性对是指满足下列性质的一个映射 $e: G_1 \times G_1 \rightarrow G_2$

1) 双线性性。对所有的 $P,Q \in G_1, e(aP,bQ) = e(P,Q)^{ab}$。

2) 非退化性。存在 $P,Q \in G_1$,使得 $e(P,Q) \neq 1$。

3) 可计算性。对所有的 $P,Q \in G_1$,存在有效的算法计算 $e(P,Q)$。

1.2 双线性 Diffie-Hellman 问题(BDH 问题)

已知 aP、bP、cP(其中 a、c、b 均属于 $\mathbf{Z}_q$),计算 $e(p,p)^{abc}$。

2 安全模型

参考文献[5,9]无证书广义指定多个验证者有序多重签名要满足以下安全要求:

1) 可计算性。签名的正确性。

2) 不可传递性。签名的 n 个验证者虽然可以验证签名的有效性,但是他们不能向其他人证明此事。

3) 在适应性选择消息攻击下不可伪造。

本文采用文献[7]提出的无证书安全模型,存在两类攻击者 A_{I} 和 A_{II}。

收稿日期:2008 - 12 - 29;**修回日期**:2009 - 03 - 16。
基金项目:教育部科学技术研究重点项目(208148);甘肃省教育厅重点项目(0801-01)。
作者简介:韩亚宁(1985 -)女,甘肃环县人,硕士研究生,主要研究方向:信息安全、现代密码学; 王彩芬(1963 -),女,河北安国人,教授,博士生导师,博士,主要研究方向:信息安全、电子商务协议。

定义1 当一个无证书广义指定多个验证者有序多重签名体制能够抵抗上述两类攻击者时就称它在适应性选择消息攻击下是不可伪造的。

3 无证书广义指定多个验证者有序多重签名方案

方案的参与者有:消息发送者 u_I、n 个消息签名者 $u_S=\{u_{S1},\cdots,u_{Sn}\}$、$n$ 个消息验证者 $u_V=\{u_{V1},\cdots,u_{Vn}\}$、消息的持有者 SH。包括9个算法,k 为安全参数,消息发送者预先设计一种签名顺序$(u_{S1},\cdots,u_{Sn})$,并将这种签名顺序发送给每一个签名者。具体签名过程如下:

1) 系统初始化。KGC输入 k,输出系统参数 $params=\{k,e,P,q,G_1,G_2,P_{Pub},H,H_1\}$,其中 $P_{Pub}=sP$,s 是系统主密钥,H 和 H_1 是两个 Hash 函数,$H_1:\{0,1\}^*\times G_1->G_1$,$H:\{0,1\}^*->Z_q^*$,公开 $params$ 保密 s。

2) 用户选择秘密值。u_i 随机选择 $x_i\in\mathbf{Z}_q^*$ 作为自己的秘密值。

3) 设置用户公钥。u_i 计算自己的公钥 $\langle X_i,Y_i\rangle=\langle x_iP,x_isP\rangle$。

4) 设置用户部分私钥。给定用户身份 $ID_i\in\{0,1\}^*$ 及其公钥 Y_i,KGC 计算 $Q_i=H_1(ID_i,Y_i)$,将 $D_i=sQ_i$ 作为用户的部分私钥。

5) 设置用户私钥。u_i 计算私钥 $PR_i=x_iD_i$。

6) 签名。u_I 将消息 m 发送给第一位签名者 u_{S1},u_{S1} 收到后:a) 随机选取 $k_1\in[1,p-1]$,计算 $r_1=k_1P$ 和 $S_1=H(m)PR_{S1}+r_1k_1$。b) 将签名消息$(m,(S_1,r_1))$ 发送给下一个签名者 u_{S2}。

每一位签名者 $u_{Si}(i\geqslant 2)$ 收到 u_{Si-1} 发送的签名$(m,(S_{i-1},r_1,r_2,\cdots,r_{i-1}))$ 后:a) 验证 $e(S_{i-1},P)=(\prod_{j=1}^{i-1}e(Q_{Sj},Y_{Sj}))^{H(m)}\prod_{j=1}^{i-1}e(r_j,r_j)$,如果成立就继续进行下一步,否则拒绝签名。b) 随机选择 $k_i\in[1,p-1]$,计算 $r_i=k_iP$ 和 $S_i=S_{i-1}+H(m)PR_{Si}+r_ik_i$。c) 将签名消息$(m,(S_i,r_1,r_2,\cdots,r_i))$ 发送给下一个签名者 u_{i+1}。

最后一位签名者 u_{Sn} 在得到签名$(m,(S_n,r_1,r_2,\cdots,r_n))$ 后,将其作为消息 m 的无证书有序多重签名输出。

7) 公开验证。验证等式 $e(S_n,P)=(\prod_{j=1}^{n}e(Q_{Sj},Y_{Sj}))^{H(m)}\prod_{j=1}^{n}e(r_j,r_j)$ 是否成立,如果成立认为 $u_{S1},u_{S2},\cdots,u_{Sn}$ 对消息 m 的签名有效,否则认为签名无效。

8) 广义指定多个验证者签名。SH 要指定 $u_V=\{u_{V1},\cdots,u_{Vn}\}$ 为消息 m 签名的多个验证者则 SH 计算 $\hat{S}_n=e(S_n,\sum_{i=1}^{n}X_{Vi})$,将$(m,(\hat{S}_n,r_1,\cdots,r_n))$ 作为消息 m 的无证书广义指定多个验证者有序多重签名。

9) 广义指定多个验证者验证。验证$(m,(\hat{S}_n,r_1,\cdots r_n))$ 的有效性,每个指定的验证者如下操作:a) 验证原始签名者的公钥 $e(X_{Sj},P_{Pub})=e(Y_{Sj},P)$。b) 计算 $e_i=(\prod_{j=1}^{n}e(x_{Vi}Q_{Sj},Y_{Sj}))^{H(m)}\prod_{j=1}^{n}e(r_j,x_{Vi}r_j)$ 其中 x_{Vi} 为验证者 u_{Vi} 的秘密值,并将 e_i 发送给其他的 $n-1$ 个指定的验证者(假设所有的验证者都是诚实的)。c) 验证:$\hat{S}_n=\prod_{i=1}^{n}e_i$ 是否成立,如果成立接受这个签名,否则拒绝。

4 安全性分析

签名的正确性很容易通过直观运算来验证,这里就不赘述。

4.1 不可传递性

定理1 我们的签名方案是不可传递的。

证明 指定的多个验证者 $u_V=\{u_{V1},\cdots,u_{Vn}\}$ 能够模拟出接收到的消息签名$(m,(\hat{S}_n,r_1,\cdots r_n))$,所以他们不能向其他任何人证明此签名的有效性。比如,指定的多个验证者要模拟对 m' 的签名:a) 某个验证者 u_{Vi} 随机选择 $r'_i\in G_1(i=1,\cdots,n)$ 并发送给其他 $n-1$ 个验证者。b) 每个验证者计算 $e_i=(\prod_{j=1}^{n}e(x_{Vi}Q_{Sj},Y_{Sj}))^{H(m')}\prod_{j=1}^{n}e(r'_j,x_{Vi}r'_j)$ 发送给其他 $n-1$ 个验证者。c) 计算 $\hat{S}'_n=\prod_{i=1}^{n}e_i$,并输出对 m' 的签名$(m',(\hat{S}'_n,r'_1,..,r'_n))$。

显然,此签名与原始签名者 $\{u_{S1},\cdots,u_{Sn}\}$ 对消息 m' 的指定 u_V 验证的签名无法区分。

4.2 不可伪造性

定理2 假设 BDH 问题是困难性问题,我们的方案可以抵抗类型 Ⅰ 攻击者 A_I 的伪造攻击。

证明 不妨设 A_I 的挑战目标为用户 u_{Si}^* 的身份 ID_{Si}^*。如果 A_I 能够以不可忽略的概率优势攻破本方案,我们要构造一个算法 B 利用 A_I 来解决 BDH 问题。任意给定 B 一个随机的 BDH 实例(P,aP,bP,cP),B 令 $P_{Pub}=bP$,将系统参数给 A_I。B 保存表 $L_1=\{ID_i,x_i,\langle X_i,Y_i\rangle,l_i,h_i,D_i,PR_i\}$ 用来存储身份 ID_i 所对应的秘密值、公钥、随机数 l_i、H_1 询问的结果 h_i、部分私钥以及私钥。(以下询问结果均保存在 L_1 中)

H_1 询问:A_I 提交 ID_i 进行询问时,B 先在 L_1 中查找,若 L_1 中存在相应的 h_i 就直接回复,否则,若 $ID_i=ID_{Si}^*B$,则回复 $Q_{Si}^*=aP$,若 $ID_i\neq ID_{Si}^*$ 则随机选取 $l_i\in\mathbf{Z}_q^*$ 回复 $h_i=l_iP$ 给 A_I。

公钥询问:A_I 询问 ID_i 的公钥时,B 先在 L_1 中查找,若 L_1 中存在相应的$\langle X_i,Y_i\rangle$ 就直接回复,否则,若 $ID_i=ID_{Vi}^*$(ID_{Vi}^* 为 A_I 最后指定的多个验证者中的某一个验证者的身份)回复$\langle X_{Vi}^*,Y_{Vi}^*\rangle=\langle cP,\perp\rangle$,若 $ID_i\neq ID_{Vi}^*$ 则随机选择 $x_i\in\mathbf{Z}_q^*$ 并回复$\langle x_iP,x_iP_{Pub}\rangle$ 给 A_I。

部分私钥询问:A_I 询问 ID_i 的部分私钥时,B 先在 L_1 中查找,若 L_1 中存在相应的 D_i 就直接回复,否则,若 $ID_i=ID_{Si}^*$ 终止,若 $ID_i\neq ID_{Si}^*$ 就在 L_1 中找到相应的 l_i 回复 l_iP_{Pub}。

私钥询问:A_{I} 询问 ID_i 的私钥时,B 先在 L_1 中查找,若 L_1 中存在相应的 PR_i 就直接回复,若不存在并且 $ID_i = ID_{Si}^*$ 或 $ID_i = ID_{Vi}^*$ 终止,否则 B 在 L_1 中找到相应的 x_i 与 D_i 回复 x_iD_i。

公钥替换询问:在任何时候对于身份信息为 ID_i 的用户 u_i,攻击者 A_{I} 都可以重新选择一个秘密值 x 并计算新的公钥 (xP, xP_{Pub}) 来代替其原有的公钥,并且 A_{I} 将其提交给 B,B 保存这个记录。

签名询问:A_{I} 询问 $u_S = \{u_{S1}, \cdots, u_{Sn}\}$ 对 m 的签名时,若 $u_{Si}^* \in u_S B$,则终止;否则在 L_1 中查找身份为 ID_i 的用户 u_{Si} 的各项信息,并且选取 n 个随机值 k_i,按照正确的签名方法进行签名以后将结果回复给 A_{I} 即可。

最终 A_{I} 选取 n 个签名者集合 $u_S(u_{Si}^* \in u_S)$ 和 n 个验证者集合 $u_V(u_{Vi}^* \in u_V)$,输出 u_S 对消息 m^* 的签名 $(m^*, (\hat{S}_n, r_1, \cdots, r_n))$。根据分叉引理[10],$B$ 可以利用 A_{I} 得到 u_S 对 m^* 的两个有效签名 $(m^*, (\hat{S}_n, r_1, \cdots, r_n))$ 和 $(m^*, (\hat{S'}_n, r_1, \cdots, r_n))$ 满足两个签名中 $H(m^*)$ 的值不一样,即:$h \neq h'$。B 计算:

$$\frac{\hat{S}_n}{\prod_{i=1, IDi \neq IDvi^*}^{n} \left[\prod_{j=1}^{n} e(hx_{Vi}Q_{Sj}, Y_{Sj}) \prod_{j=1}^{n} e(r_j, x_{Vi}r_j)\right] \prod_{j=1}^{n} e(hx_{Vi}^*Q_{Sj}, Y_{Sj}) \prod_{j=1}^{n} e(r_j, x_{Vi}^*r_j)} = \tag{1}$$

$$\frac{\hat{S'}_n}{\prod_{i=1, IDi \neq IDvi^*}^{n} \left[\prod_{j=1}^{n} e(h'x_{Vi}Q_{Sj}, Y_{Sj}) \prod_{j=1}^{n} e(r_j, x_{Vi}r_j)\right] \prod_{j=1}^{n} e(h'x_{Vi}^*Q_{Sj}, Y_{Sj}) \prod_{j=1}^{n} e(r_j, x_{Vi}^*r_j)} = \tag{2}$$

$$\frac{\prod_{j=1}^{n} e(hx_{Vi}^*Q_{Sj}, Y_{Sj}) \prod_{j=1}^{n} e(r_j, x_{Vi}^*r_j)}{\prod_{j=1}^{n} e(h'x_{Vi}^*Q_{Sj}, Y_{Sj}) \prod_{j=1}^{n} e(r_j, x_{Vi}^*r_j)} = \prod_{j=1}^{n} e((h-h')x_{Vi}^*Q_{Sj}, Y_{Sj}) \tag{3}$$

$$\frac{\prod_{j=1}^{n} e((h-h')x_{Vi}^*Q_{Sj}, Y_{Sj})}{\prod_{j=1, IDj \neq IDsj^*}^{n} e((h-h')x_{Vi}^*Q_{Sj}, Y_{Sj})} = e((h-h')x_{Vi}^*Q_{Sj}^*, Y_{Sj}^*) \tag{4}$$

$$e((h-h')x_{Vi}^*Q_{Sj}^*, Y_{Sj}^*)^{(h-h')^{-1}x^*\bar{s}_j^{-1}} = e(caP, x_{Sj}^*bP)^{x^*\bar{s}_j^{-1}} = e(P,P)^{abc} \tag{5}$$

由此 B 解决了 BDH 问题,这与 BDH 问题是困难性问题相矛盾,所以我们的方案可以抵抗 A_{I} 的伪造攻击。

定理 3　假设 BDH 问题是困难性问题,我们的方案可以抵抗类型 Ⅱ 攻击者 A_{II} 的伪造攻击。

证明　首先,B 将主密钥 s 与系统参数都发送给 A_{II}。H_1 询问、H 询问、私钥询问,以及签名询问都与定理 2 中完全一样,不同的是公钥询问:

A_{II} 询问 ID_i 的公钥时,B 先在 L_1 中查找,若 L_1 中存在相应的 $\langle X_i, Y_i\rangle$ 就直接回复,否则,若 $ID_i = ID_{Vi}^*$ 回复 $\langle cP, scP\rangle$,若 $ID_i = ID_{Si}^*$ 回复 $\langle bP, sbP\rangle$ 给 A_{II},其他情况下 B 随机选择 $x_i \in \mathbf{Z}_q^*$ 回复 $\langle x_iP, x_iP_{Pub}\rangle$ 给 A_{II}。

最终 A_{II} 任意选取 n 个签名者集合 $u_S(u_{Si}^* \in u_S)$ 和任意 n 个验证者集合 $u_V(u_{Vi}^* \in u_V)$,输出 u_S 对消息 m^* 的签名 $(m^*, (\hat{S}_n, r_1, \cdots, r_n))$ 根据分叉引理[10],B 得到两个有效签名 $(m^*, (\hat{S}_n, r_1, \cdots, r_n))$ 和 $(m^*, (\hat{S'}_n, r_1, \cdots, r_n))$ 满足两个签名中 $h \neq h'$。B 同定理 2 中完全一样的计算出(1) ~ (4) 式,然后计算出:

$$e((h-h')x_{Vi}^*Q_{Sj}^*, Y_{Sj}^*)^{(h-h')^{-1}s^{-1}} = e(caP, sbP)^{s^{-1}} = e(P,P)^{abc} \tag{6}$$

所以我们的方案可以抵抗 A_{II} 的伪造攻击。

5　结语

为了结合无证书签名体制与有序多重签名的优势,并且能够让签名的持有者指定多个签名的验证者,我们提出了无证书广义指定多个验证者有序多重签名方案,我们的方案满足不可传递性并且在随机预言模型下证明了它在适应性选择消息攻击下是不可伪造的。相比文献[5]所提出的广播式的多重签名我们的方案具有有序性的优势,可以满足需要多个签名者按特定的顺序进行签名的实际应用。在文献[5]方案的广播过程中恶意的攻击者可以通过侦听整个线路来对签名进行破坏,我们的方案可以减少这种攻击,具有实际的应用价值。

参考文献:

[1] ITAKURA K, NAKAMURA K. A public-key cryptosystem suitable for digital multisignatures [R]. NEC Research & Development, 1983, 71: 1 - 8.

[2] 李子臣, 杨义先. ELGamal 多重数字签名方案[J]. 北京邮电大学学报, 1999, 22(2): 30 - 34.

[3] 王晓明. 一种多重数字签名方案的安全性分析[J]. 南开大学学报, 2003, 36(1): 33 - 38.

[4] LU S, OSTROUSKY R, SAHAIA A, *et al.* Sequential aggregate signatures and multisignatures without random oracles [EB/OL]. [2008 - 10 - 10]. http://eprint.iacr.org/2006/096.pdf.

[5] 梁红梅, 黄慧, 吴晨煌, 等. 无证书多重签名[J]. 集美大学学报, 2008, 13(2): 127 - 131.

[6] AL-RIYAMI S, PATERSON K G. Certificateless public key cryptography [C]// Proceedings of ASIACR YFT'03. Berlin: Springer-Verlag, 2003: 452 - 473.

[7] ZHANG Z-F, WONG DC S, XU J, *et al.* Certificateless public-key signature: Security model and efficient construction [C]// ACNS'06: Proceedings of 4th International Conference on Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2006: 293 - 308.

[8] STEINFELD R, BULL L, WANG H, *et al.* Universal designated-verifier signatures [C]// Proceedings of ASIACRYPT'03. Berlin: Springer-Verlag, 2003: 523 - 542.

[9] SEO S H, HWANG J Y, CHOI K Y, *et al.* Identity-based u-niversal designated multi-verifiers signature schemes [J]. Computer Standards & Interfaces, 2008, 30(5): 288 - 295.

[10] POINTCHEVAL D, STEM J. Security proofs for signature schemes [EB/OL]. [2008 - 10 - 10]. http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E96/387.PDF.