基于身份的强指定验证人签名方案 *

毛卫霞, 李志慧†, 薛 婷
(陕西师范大学 数学与信息科学学院, 西安 710062)

摘 要: 在有些情况下, 需要将验证者限定为某一个人。利用基于身份的密码体制, 提出了一种强指定验证人签名和一种强指定验证人多重代理签名, 并对其安全性进行了分析。在签名代价和验证代价上, 提出的强指定验证人签名比 Kang 等人的方案要低。提出的强指定验证人多重代理签名可以同时授权给 n 个代理人, 可以有效防止代理签名人对签名权的滥用。

关键词: 基于身份的签名; 指定验证人签名; 代理签名; 双线性对
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)02-0689-03
doi:10.3969/j.issn.1001-3695.2010.02.079

Identity-based strong designated verifier signature schemes

MAO Wei-xia, LI Zhi-hui†, XUE Ting
(*College of Mathematics & Information Science, Shaanxi Normal University, Xi'an* 710062, *China*)

Abstract: We should specify a verifier in some circumstances. Using identity-based cryptography, this paper proposed a strong designated verifier signature and a strong designated verifier multi-proxy signature. It also analyzed the proposed schemes. The proposed strong designated verifier signature scheme was lower than Kang et al.'s scheme in the signing cost and verifying cost. The proposed strong designated verifier multi-proxy signature scheme could delegate n proxy signers. Thus it could prevent proxy signers abusing signing authority.

Key words: identity-based signature; designated verifier signature; proxy signature; bilinear pairings

0 引言

在基于身份的密码体制中, 用户的公钥可以是任意的字符串(如姓名、电子邮件地址、IP 地址等), 而私钥由私钥生成中心(private key generator, PKG)生成。这种思想最早是由 Shamir 在文献[1]中提出的。基于身份的密码体制无须公钥证书的管理与鉴别, 在实际应用中带来很大的便利。

Jakobsson 等人在文献[2]中首先提出了指定验证人签名的概念。指定验证人签名将验证者限定为某一个人, 在许多领域(如电子现金、电子选举)中有着重要的作用。在这种签名方案中, Alice 指定一个验证人 Bob。Alice 可以使 Bob 相信他的签名是正确的, 并且 Bob 不能向第三方证明该签名是由 Alice 所签, 原因是 Bob 可以模拟出与签名者 Alice 不可区分的签名。

Saeednia 等人[3]将指定验证人的私钥应用到验证等式中, 提出了强指定验证人签名。强指定验证人签名是指只有指定的验证人才能检验签名的合法性, 并且第三方不能确定该签名到底是谁所签。在 2004 年, Susilo 等人[4]提出了基于身份的强指定验证人签名方案。后来, Kumar 等人在文献[5]中提出了新的基于身份的强指定验证人签名方案, 但没有证明安全性。与文献[4,5]的方案相比, Kang 等人[6]提出的方案签名长度较短, 签名代价和验证代价较低。

Mambo 等人[7]提出了代理签名的概念。代理签名解决了数字签名权力委托的问题, 即原始签名人将签名权委托给代理签名人, 同时又不暴露自己的私钥。多重代理签名是原始签名人将签名权分散给多个代理签名人, 这样可以有效防止代理签名人对签名权的滥用。强指定验证人多重代理签名是指定验证人签名的延伸。

1 相关知识

1.1 双线性对

令 G_1 和 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。$e: G_1 \times G_1 \to G_2$ 是一个映射, 若 e 满足下列三条性质:

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

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

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

称 e 为一个双线性对。由双线性对的性质 b)知, 若 P 为 G_1 的生成元, 则 $e(P,P)$ 为 G_2 的生成元。

1.2 与双线性对有关的数学问题

1)离散对数问题(DLP) 给定 $P,Q \in G_1$, 找出整数 a, 使得 $Q = aP$, 如果这样的整数 a 存在。

2)计算 Diffie-Hellman 问题(CDHP) 给定 $P,aP,bP \in G_1$, 对于所有的 $a,b \in Z_q^*$, 计算 abP。

收稿日期: 2009-06-19; **修回日期**: 2009-08-04 **基金项目**: 国家自然科学基金资助项目(60873119); 陕西省自然科学基础研究计划资助项目(2007A06)

作者简介: 毛卫霞(1983-), 女, 河南安阳人, 硕士研究生, 主要研究方向为有限域、密码学(ccde456@163.com); 李志慧(1966-), 女(通信作者), 副教授, 博士, 主要研究方向为有限域、密码学; 薛婷, 女, 硕士研究生, 主要研究方向为有限域、密码学.

3)判定 Diffie-Hellman 问题(DDHP)　给定 $P,aP,bP,cP\in G_1$,对于所有 $a,b,c\in Z_q^*$,判定 $c=ab \bmod q$ 是否成立。

4)双线性 Diffie-Hellman 问题(BDHP)　给定 $P,aP,bP,cP\in G_1$,对于所有 $a,b,c\in Z_q^*$,计算 $e(P,P)^{abc}$。

假设群上的 DLP、CDHP 和 BDHP 都是难解问题。当群上的 DDHP 容易而 CDHP 难解时,这样的群叫 GDH(gap Diffie-Hellman)群。这样的群可以在超椭圆曲线中找到,并且可以利用超椭圆曲线上的 Weil 对或经改造的 Tate 对来构造双线性对。具体细节可参考文献[8]。

2　基于身份的强指定验证人签名

2.1　系统初始化

(1)私钥生成中心 PKG 选取阶都为素数 q 的 GDH 群 G_1 和乘法群 G_2,双线性映射 $e:G_1\times G_1\to G_2$,P 为 G_1 的生成元。任取 $s\in Z_q^*$ 为主密钥,公钥为 $P_{pub}=sP$。$H_1:\{0,1\}^*\to G_1$ 和 $H_2:\{0,1\}^*\times G_2\to G_1$ 为两个安全的哈希函数。系统参数为 $(G_1,G_2,q,e,P,P_{pub},H_1,H_2)$。参与者为签名者 A 和指定验证人 C。

(2)私钥生成中心 PKG 利用身份 ID 计算 $S_{ID}=sH_1(ID)$,并发送给其身份为 ID 的用户,$Q_{ID}=H_1(ID)$为其公钥。

2.2　签名阶段

签名者 A 对消息 m 进行签名。签名者 A 任意选取 $r\in Z_q^*$,计算 $R=rQ_{ID_A}$,$\sigma=H_2(m,e(P_{pub}+rS_{ID_A},Q_{ID_C}))$,把$(R,\sigma)$发送给指定验证人 C。

2.3　验证阶段

指定验证人 C 收到(R,σ)后,验证下式是否成立。若成立,则(R,σ)就是关于消息 m 的签名。

$$\sigma=H_2(m,e(P+R,S_{ID_C}))$$

2.4　签名模拟阶段

指定验证人 C 任取 $r'\in Z_q^*$,计算 $R'=r'Q_{ID_A}$,$\sigma'=H_2(m,e(P+R',S_{ID_C}))$。

2.5　方案分析

1)正确性

$$e(P_{pub}+rS_{ID_A},Q_{ID_C})=e(P+rQ_{ID_A},S_{ID_C})=e(P+R,S_{ID_C})$$

故

$$\sigma=H_2(m,e(P_{pub}+rS_{ID_A},Q_{ID_C}))=H_2(m,e(P+R,S_{ID_C}))$$

并且指定验证人 C 的私钥 S_{ID_C}出现在验证等式中,因此只有指定验证人 C 才能检验签名的合法性。

2)不可伪造性

由于

$$\sigma=H_2(m,e(P_{pub}+rS_{ID_A},Q_{ID_C}))=H_2(m,e(P+R,S_{ID_C}))$$

攻击者不知道 S_{ID_A}和 S_{ID_C}就无法伪造 σ,从而也就无法伪造签名。求 S_{ID_A}和 S_{ID_C}必须知道 s,而求 s 将会面临离散对数问题(DLP)。

3)签名源的隐匿性

只有指定验证人 C 才能验证和模拟签名,并且指定验证人 C 不能向第三方证明该签名是由 A 所签,即签名是由签名者 A 或指定验证人 C 两者之一产生。因此,对于消息 m 和关于消息 m 的签名(R,σ),攻击者不可能确定该签名到底是谁所签。

4)签名者身份的匿名性

在签名阶段,攻击者知道 $r\in Z_q^*$ 和 S_{ID_A}才能对消息进行签名。在验证阶段,攻击者知道 S_{ID_C}才能对签名进行验证。攻击者不知道 r,S_{ID_A},S_{ID_C}就无法求出 σ。因此,攻击者不可能确定签名到底是谁所签,从而也就无法知道签名者的身份。

5)效率分析

C_p 为双线性对运算,C_* 为 G_1 上的乘法,C_e 为 G_2 上的指数运算,C_h 为哈希函数运算,C_i 为求逆运算,省略 G_1 上的加法。假设 G_1 的元素的比特长度为$|G_1|$($|G_1|=|G_2|$)。分别用[4]、[5]、[6]表示文献[4,5,6],用[0]表示本文所提方案。从表 1 可以看出,所提出的方案明显优于文献[4,5,6]。

表 1　不同方案的比较

方案	长度	签名代价	验证代价
[5]	$4\|G_1\|$	$1C_p+5C_*+1C_h+1C_i$	$4C_p+1C_h$
[4]	$2\|G_1\|+\|H\|$	$1C_p+2C_*+1C_e+1C_h+1C_i$	$2C_p+1C_*+2C_e+1C_h$
[6]	$2\|G_1\|$	$2C_p+2C_*+1C_e+1C_h$	$1C_p+1C_*+1C_e+1C_h$
[0]	$2\|G_1\|$	$1C_p+2C_*+1C_h$	$1C_p+1C_h$

3　基于身份的强指定验证人多重代理签名

3.1　系统初始化

1)$(G_1,G_2,q,e,P,P_{pub},H_1,H_2)$与 2.1 节中的参数相同。选取 $H_3:\{0,1\}^*\to Z_q^*$ 为另一个安全的哈希函数,公布 H_3。消息 $m\in\{0,1\}^*$,$\|$ 表示比特串并联。参与者分别为原始签名人 A、代理签名组$\{P_1,P_2,\cdots,P_n\}$和指定验证人 C。

2)私钥生成中心 PKG 利用身份 ID 计算 $S_{ID}=sH_1(ID)$,把 S_{ID}发送给其身份为 ID 的用户,$Q_{ID}=H_1(ID)$为其公钥。

3.2　代理密钥生成阶段

1)原始签名人 A 制定代理授权书 m_w(其中包括原始签名人 A 和代理签名人 $P_i(1\leqslant i\leqslant n)$的身份、代理签名文件的范围、代理终止时间等信息)。原始签名人 A 任取 $r_i\in Z_q^*$,计算 $R_i=r_iH_3(m_w\|Q_{ID_{P_i}})$,$T_i=R_iS_{ID_A}$,把$(m_W,R_i,T_i)$发送给代理签名人 P_i。

2)代理签名人 P_i 收到(m_w,R_i,T_i)后,检验 $e(T_i,P)=e(R_iQ_{ID_A},P_{pub})$是否成立。若成立,计算代理签名密钥 $S_{P_i}=T_i-S_{ID_{P_i}}$,代理签名公钥为 $Q_{P_i}=R_iQ_{ID_A}-Q_{ID_{P_i}}$。

3.3　代理签名阶段

代理签名人 P_i 对消息 m 进行签名。代理签名人 P_i 任意选取 $u_i,v_i\in Z_q^*$,计算

$$U_i=u_iS_{P_i}$$
$$V_i=H_2(m_w,e(u_iQ_{ID_C},v_iS_{P_i}))$$
$$h_i=H_3(m\|U_i\|V_i)$$
$$\sigma_i=u_iQ_{P_i}+h_iP$$

然后把(m_w,m,U_i,V_i,h_i,Q_i)发送给指定验证人 C。

3.4　代理签名验证阶段

1)指定验证人 C 收到$(m_w,m,U_i,V_i,h_i,\sigma_i)$后,首先检查一下消息 m 是否包含在代理授权书 m_w 中,A 和 P_i 是否是真正的原始签名人和代理签名人。

2)因为有 n 个代理签名人,就有 n 个签名。指定验证人 C 计算 $\sigma=\sum_{i=1}^{n}\sigma_i$,并验证下式是否成立。若成立,则 σ 就是关于消息 m 的签名。

$$e(\sigma,S_{ID_C})=\prod_{i=1}^{n}e(U_i+h_iP_{pub},Q_{ID_C})$$

3.5　代理签名模拟阶段

指定验证人 C 任取 $u'_i, v'_i \in Z_q^*$,计算

$$U'_i = u'_i S_{\mathrm{ID}_C}$$

$$V'_i = H_2(m_w, e(v'_i S_{\mathrm{ID}_C}, u'_i Q_{P_i}))$$

$$h'_i = H_3(m \parallel U'_i \parallel V'_i)$$

$$\sigma'_i = u'_i Q_{\mathrm{ID}_C} + h'_i P$$

然后计算 $\sigma' = \sum_{i=1}^{n} \sigma'_i$,此时$(U'_i, h'_i, \sigma')$能通过下面等式的验证。

$$e(\sigma', S_{\mathrm{ID}_C}) = \prod_{i=1}^{n} e(U'_i + h'_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C})$$

3.6　方案分析

1)正确性

$$e(\sigma, S_{\mathrm{ID}_C}) = e\left(\sum_{i=1}^{n} \sigma_i, S_{\mathrm{ID}_C}\right) = \prod_{i=1}^{n} e(\sigma_i, S_{\mathrm{ID}_C}) =$$

$$\prod_{i=1}^{n} e(u_i Q_{P_i} + h_i P, S_{\mathrm{ID}_C}) =$$

$$\prod_{i=1}^{n} e(u_i S_{P_i} + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C}) =$$

$$\prod_{i=1}^{n} e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C})$$

2)不可伪造性

攻击者想伪造关于消息 m 的签名 σ,需知代理签名密钥 S_{P_i}或者指定验证人 C 的私钥 S_{ID_C}。而 $S_{P_i} = T_i - S_{\mathrm{ID}_{P_i}} = R_i S_{\mathrm{ID}_A} - S_{\mathrm{ID}_{P_i}}$。其中 $R_i = r_i H_3(m_w \parallel Q_{\mathrm{ID}_{P_i}})$具有随机性,$S_{\mathrm{ID}_A}$和 $S_{\mathrm{ID}_{P_i}}$分别为原始签名人 A 和代理签名人 P_i 的私钥。求解 S_{ID_A}、$S_{\mathrm{ID}_{P_i}}$和 S_{ID_C}将会面临离散对数问题(DLP)或计算 Diffie-Hellman 问题(CDHP)。

此外,攻击者已经知道某个代理签名人 P_i 的签名$(U_i, V_i, h_i, \sigma_i)$,想从验证等式 $e(\sigma, S_{\mathrm{ID}_C}) = \prod_{i=1}^{n} e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C})$ 中求出 S_{ID_C}也是不可能的。

$$e(\sigma, S_{\mathrm{ID}_C}) = \prod_{i=1}^{n} e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C}) \Rightarrow$$

$$e(\sigma_i, S_{\mathrm{ID}_C}) = e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C})$$

由于 $\sigma_1, S_{\mathrm{ID}_C}, U_i, Q_{\mathrm{ID}_C} \in G_1$,设 $\sigma_i = aP$, $S_{\mathrm{ID}_C} = xP$, $U_i = bP$, $Q_{\mathrm{ID}_C} = cP$。

$$e(\sigma_i, S_{\mathrm{ID}_C}) = e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C}) \Leftrightarrow$$

$$e(aP, xP) = e(bP + sh_i P, cP) \Leftrightarrow$$

$$e(P, P)^{ax} = e(P, P)^{c(b + sh_i)}$$

但求解 $e(P,P)^{ax}$与 $e(P,P)^{c(b+sh_i)}$ 将会面临双线性 Diffie-Hellman 问题(BDHP),并且确定 a、b、c、s 将会面临离散对数问题(DLP)。因此,攻击者不可能从等式 $e(P,P)^{ax} = e(P,P)^{c(b+sh_i)}$ 中求出 x,也就求不出 S_{ID_C}。

3)签名源的隐匿性

代理签名人 P_i 的签名为$(U_i, V_i, h_i, \sigma_i)$,签名中不包括代理签名人 P_i 的任何信息。在验证等式 $e(\sigma, S_{\mathrm{ID}_C}) = \prod_{i=1}^{n} e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C})$中,出现了指定验证人 C 的私钥 S_{ID_C}而没有代理签名人 P_i 的公钥 $Q_{\mathrm{ID}_{P_i}}$,即代理签名人 P_i 的签名对于外界而言具有不确定性。因此,其他人仅根据消息 m 和签名 σ,无法确定该签名到底是谁所签。

4)签名者身份的匿名性

由于有 n 个代理签名人,就有 n 个签名$(U_i, V_i, h_i, \sigma_i)$ $(1 \leqslant i \leqslant n)$。攻击者想确定消息 $m \in \{0,1\}^*$ 是谁所签,需知签消息 m 的每个代理签名人 P_i 的身份。由 3)可知,攻击者无法确定消息 m 到底是谁所签,从而也就不能确定代理签名人 P_i 的身份。

另外,签名过程中使用了代理授权书 m_w,并且指定验证人 C 的私钥 S_{ID_C}出现在验证等式 $e(\sigma, S_{\mathrm{ID}_C}) = \prod_{i=1}^{n} e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C})$中,故强指定验证人多重代理签名与一般的签名是可以区分的。代理授权书 m_w 中已明确规定了代理签名人所签消息的具体内容、代理终止时间等信息,故代理签名人 P_i 不能滥用自己的权利任意地对消息进行签名。从以上分析可以看出,代理签名的可验证性、不可伪造性、可区分性、防止滥用性也是满足的。

5)效率分析

C_p、C_*、C_h 与 2.5 节的参数相同,省略 G_1 上的加法和 G_2 上的乘法。假设 G_1 的元素的比特长度为$|G_1|$($|G_1| = |G_2|$)。单重代理签名的验证等式为 $e(\sigma_i, S_{\mathrm{ID}_C}) = e(U_i + h_i P_{\mathrm{pub}}, Q_{\mathrm{ID}_C})$。从表2 可以看出,签名长度无变化,签名代价和验证代价也没有明显增加。

表 2　单重代理与多重代理的比较

方案	长度	签名代价	验证代价
单重	$\|G_1\|$	$1C_p + 5C_* + 2C_h$	$2C_p + 1C_*$
多重	$\|G_1\|$	$nC_p + 5nC_* + 2nC_h$	$(n+1)C_p + nC_*$

4　结束语

指定验证人签名在电子现金、电子选举中有着重要的应用。目前所提出的指定验证人签名方案要么签名长度较长,要么签名代价和验证代价较高。利用基于身份的密码体制,提出了两个强指定验证人签名方案。分析表明所提出的方案是安全高效的。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of CRYTO'84. Berlin: Springer-Verlag,1984: 47-53.

[2] JAKOBSSON M, SAKO K, IMPAGLIAZZO R. Designated verifiers proofs and their applications[C]//Lecture Notes in Computer Science 1070: Advances in Cryptology - Eurocrypt'96. Berlin: Springer-Verlag,1996:143-154.

[3] SAEEDNIA S, KRAMER S, MARKOWITCH O. An efficient strong designated verifier signature scheme[C]//Proc of the 6th International Conference on Information Security and Cryptology'03. Berlin: Springer-Verlag,2003:40-54.

[4] SUSILO W, ZHANG F, MU Y. Identity-based strong designated verifier signature schemes[Z]. 2004:313-324.

[5] KUMAR K, SHAILAJA G, SAXENA A. Identity-based strong designated verifier signature scheme[EB/OL]. http://eprint. jacr. org/complete/134. pdf.

[6] KANG Bao-yuan, BOYD C, DAWSON E. A novel identity-based strong designated verifier signature scheme[J]. The Journal of Systems and Software,2009,82(2):270-273.

[7] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans on Fundamentals, 1996(9):1338-1354.

[8] GALBRAITH S D, HARRISON K, SOLDERA D. Implementing the tate pairing[C]//Proc of the 5th International Symposium on Algorithmic Number Theory. Berlin: Springer-Verlag,2002:324-337.