一个安全的基于身份的强指定验证者签名方案

徐丹慧 亢保元
(天津工业大学计算机科学与软件学院 天津 300387)

摘 要 在一般的数字签名中,拥有签名者公钥的任何人都可以验证该签名的有效性;而强指定验证者签名是由签名者指定一个验证者,在签名验证阶段,只有这个指定验证者可以验证该签名的有效性,其他人都不能验证该签名。这是因为在签名的验证阶段必须用到指定验证者的私钥。基于这个性质,强指定验证者签名被广泛应用于电子商务、网上投标、电子选举中。基于双线性对提出了一个新的基于身份的强指定验证者签名方案,并基于GBDH困难问题假设,采用密码学上安全性分析的方法,证明了该方案在适应性选择消息和选择身份攻击下是不可伪造的。最后,分析了方案的计算成本,结果表明该方案具有较高的效率。

关键词 密码学,基于身份的签名,指定验证者签名,双线性对
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.010

Secure Identity-based Strong Designated Verifier Signature Scheme

XU Dan-hui KANG Bao-yuan
(School of Computer Science and Software Engineering, Tianjin Polytechnic University, Tianjin 300387, China)

Abstract Compared with ordinary digital signature in which anyone who owns the signer's public key can verify the validity of the signature, a designated verifier signature scheme makes it possible for a signer to convince a designated verifier that he has signed a message in such a way that the designated verifier cannot transfer the signature to a third party. In a strong designated verifier signature scheme, no third party can even verify the validity of a designated verifier signature, since the designated verifier's private key is required in the verifying phase, such that strong designated verifier signature is widely used in electronic commerce, online bidding and electronic elections. Based on bilinear pairing we proposed a novel identity-based strong designated verifier signature scheme. Based on the GBDH assumption, we proved that our scheme is existentially against adaptive chosen message attack. Through the analysis of the computational cost, results show that the scheme has high efficiency.

Keywords Cryptography, Identity-based signature, Designated verifier signature, Bilinear pairing

1 引言

随着现代社会信息化和数字化的发展,信息的存储与流通变得更为便捷。但同时人们对信息安全的认识和要求都在不断提高,如何保障信息的安全性已成为当今科学研究领域的热点课题之一。信息安全的研究不但具有理论价值,而且具有重大的实际应用价值。密码学作为信息安全的一个重要分支,它为解决信息安全问题提供了许多有用的实用技术。现代密码技术除了提供信息的加密解密外,还提供对信息来源的鉴别、保证信息的完整性和不可否认性等功能,而这3种功能都可以通过数字签名来实现。在一般的数字签名方案中,任何人都可以验证签名的有效性,但有时候签名者想保护自己的隐私,不希望所有人验证签名的有效性。针对这种情况,具有特殊性质的指定验证者签名应运而生。

在1996年的欧洲密码学会议上Jakobsson、Sako和Impagliazzo首次提出了指定验证者签名(DVS)的概念[1]。在指定验证者签名方案中,指定的验证者能产生一个与签名人所做的签名无法区分的副本,任何第三方都不能确定这个签名是签名者还是验证者产生的,也就是说不能识别真正的签名人,但是每个人都可以验证签名的有效性。同时,Jakobsson、Sako和Impagliazzo提出了强指定验证者签名(SDVS)的概念,即在一个强指定验证者签名方案中,只有指定验证者才能验证签名的有效性。2003年,在信息安全与密码学会议上,Saeednia、Kremer和Markowitch给出了强指定验证者的形式化定义,并提出了第一个强指定验证者签名方案[2]。强指定验证者签名一般满足以下安全性质:1)不可伪造性,除签名者和验证者之外,其他人不可能生成一个有效的签名;2)不可传递性,指定的验证者可以生成一个与签名者生成的签名不可区分的副本,也就是说指定验证者不可能向第三方证明签名是签名者生成的;3)签名源隐匿性,假设给定一个消息m和对m的签名σ,第三方不能确定这个签名是签名者生成的还是指定验证者生成的。2004年,Susilo等人在文献[3]中提出了基于身份的强指定验证者签名方案。此后,学者们提出了各种基于身份的指定验证者签名方案[4-8]。2011年,Tang F

到稿日期:2015-06-10 返修日期:2015-07-29 本文受天津市应用基础与前沿技术研究计划项目(15JCYBJC15900)资助。
徐丹慧(1990-),女,硕士生,主要研究方向为信息安全,E-mail:mixueren123123@sina.com;亢保元(1965-),男,博士,教授,主要研究方向为信息安全与密码学,E-mail:baoyuankang@aliyun.com(通信作者)。

等人提出了一个基于身份的指定验证者签名方案[9]。Tian 等人基于椭圆曲线提出了一个强指定验证者签名方案[10]。2014 年,SK Hafizul Islam、G. P. Biswas 等人提出了一种可证明安全的基于双线性对的无证书的强指定验证者签名方案[11]。本文基于双线性对提出了一个新的基于身份的强指定验证者签名方案,通过分析得出本文的方案满足不可伪造性、不可传递性,同时给出了安全性证明。

本文第 2 节介绍了相关数学知识;第 3 节介绍了强指定验证者签名方案的定义及安全模型;第 4 节提出了一个新的基于身份的强指定验证者签名方案;第 5 节对本文方案进行安全性分析,给出了不可伪造性的证明;最后总结全文。

2 基础知识

2.1 双线性对

设 G_1 与 G_2 分别是加法循环群和乘法循环群,它们的阶均为大素数 q,P 为 G_1 的生成元。设 $e:G_1\times G_1\to G_2$ 是满足以下 3 条性质的双线性映射:

1)双线性:对任意的 $a,b\in Z_q^*$,$P,Q\in G_1$,有 $e(aP,bQ)=e(P,Q)^{ab}$。

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 $P,Q\in G_1$,存在有效算法可以计算 $e(P,Q)$。

双线性对一般可以由 Weil 或 Tate 对得到。有关的具体细节可参见文献[12]。

2.2 相关困难问题

定义 1(CBDH 问题,Computational Bilinear Diffie-Hellman Problem) 在群 G_1 上,已知(P,aP,bP,cP),其中 $a,b,c\in Z_q^*$ 未知,计算 $e(P,P)^{abc}$。

定义 2(DBDH 问题,Decisional Bilinear Diffie-Hellman Problem) 在群 G_1 上,已知(P,aP,bP,cP),其中 $a,b,c\in Z_q^*$ 未知,并给定 $h\in G_2$,判定 $h=e(P,P)^{abc}$ 是否成立,如果成立,则输出 1;否则输出 0。

定义 3(GDBH 问题,Gap Bilinear Diffie-Hellman Problem) 在群 G_1 上,已知(P,aP,bP,cP),其中 $a,b,c\in Z_q^*$ 未知,在 DBDH 预言机的帮助下,计算 $e(P,P)^{abc}$ 的值。

如果在群 G_1 上,DBDH 问题在多项式时间内是可解的,而不存在任何多项式时间算法使得 CBDH 问题能够以不可忽略的概率被求解,那么我们称 G_1 为 GAP Diffie-Hellman 群(GAP Diffie-Hellman Group,简称 GDH 群)。GDH 群通常存在于有限域中的超椭圆曲线或超奇异椭圆曲线中。

3 基于身份的强指定验证者签名方案的定义及安全模型

3.1 基于身份的强指定验证者签名的方案的定义

基于身份的强指定验证者签名(ID-SDVS)系统中有两个实体参与,即签名者 ID_A 和指定验证者 ID_B。该系统由 Setup、Extract、Sign、Verify、Simulate 5 个算法组成。

Setup:在这个阶段,PKG(Private Key Generation center)执行初始化的设置算法,输入一个安全参数 k,输出系统公开参数 $params$ 和主密钥 msk。

Extract:输入参数 $params$、主密钥 msk 和用户的身份值 $ID\in\{0,1\}^*$,返回用户的私钥-公钥对(S_{ID},Q_{ID})。

Sign:输入系统参数、签名者的私钥 S_{ID}、消息 m 和指定验证者的身份值 ID_V,返回一个对消息 m 的签名 σ。

Verify:输入系统参数、签名者的身份值 ID_S、消息 m 和指定验证者的身份值 ID_V 和私钥 S_V,返回对消息 m 签名 σ 的验证结果:接受或者拒绝该签名。

Simulate:指定验证者执行模拟算法来产生一个与签名者生成的签名不可区分的副本。

3.2 基于身份的强指定验证者签名方案的安全模型

基于身份的强指定验证者签名方案要满足以下 3 个安全特性,这里重点介绍不可伪造性。

• 正确性:一个正确的指定验证者签名方案能够通过验证算法的验证。

• 不可传递性:指定的验证者可以生成一个与签名者生成的签名不可区分的副本,也就是说,指定验证者不可能向第三方证明签名是签名者生成的。

• 不可伪造性:在不知道签名者和指定验证者的私钥的情况下构造一个有效的签名,在计算上是不可行的。

基于身份的强指定验证者签名的不可伪造性用下面挑战者与敌手Z之间的游戏来描述。

• Setup:挑战者执行 Setup 算法来产生系统参数。

• Extract 询问:敌手Z可以询问身份值为 ID_i 的用户的私钥,挑战者返回 S_{ID_i} 作为回答。

• Sign 询问:敌手Z询问关于消息 m 的签名,其中签名者为 ID_i,指定验证者为 ID_j。挑战者输出一个对消息 m 的签名 σ 作为回答。

• Verify 询问:敌手Z对(m,σ)向挑战者进行验证询问,其中签名者为 ID_i,指定验证者为 ID_j。若签名有效,输出 1;否则,输出 0。

• 伪造:最终敌手Z输出一个关于消息 m^* 的签名 σ^*,其中签名者的身份值为 ID_i^*,指定验证者的身份值为 ID_j^*。若满足以下条件:

(a)敌手Z从未在 Extract 询问中询问过 ID_i^* 和 ID_j^*。

(b)敌手Z从未在 Sign 询问中询问消息 m^* 的签名,其中签名者的身份值为 ID_i^*,指定验证者的身份值为 ID_j^*。

(c)σ^* 是关于消息 m^* 的有效签名,其中签名者的身份值为 ID_i^*,指定验证者的身份值为 ID_j^*。

则称攻击者伪造攻击成功。

4 基于身份的强指定验证者签名方案

在这个阶段构造了一个基于身份的强指定验证者签名方案,签名者 Alice 的身份值为 ID_A,指定验证者 Bob 的身份值为 ID_B,由 Setup、Extract、Sign、Verify,Simulate 这 5 个步骤组成。

Setup:在这个阶段,PKG(Private Key Generation center)执行初始化的设置算法来产生系统公开参数和主密钥、主公钥。$\langle G_1,G_2,e:G_1\times G_1\to G_2\rangle$,$P\in G_1$ 是 G_1 的生成元。随机地选择 $s\in Z_q^*$ 作为系统主密钥 msk,$P_{pub}=sP$ 作为系统主公钥。这里有两个强无碰撞 Hash 函数:

$H_0:\{0,1\}^*\to G_1$,$H_1:\{0,1\}^*\to Z_q$

保密系统主密钥 $msk=s$,公开系统参数:$params=\langle G_1,G_2,e,q,P,P_{pub},H_0,H_1\rangle$。

Extract:PKG 执行提取私钥算法生成用户私钥。对于一个给定的身份值 ID,PKG 计算 $S_{ID}=sQ_{ID}$,其中 $Q_{ID}=H_0(ID)$。把 $Q_{ID}=H_0(ID)$记作用户 ID 的公钥,$S_{ID}=sQ_{ID}$ 记

作用户的私钥，并通过一个安全的信道将 S_{ID} 传送给用户 ID。

Sign：假定签名者 Alice 和指定验证者 Bob 的公钥/私钥对分别是 Q_A/S_A 和 Q_B/S_B。Alice 随机地选择随机数 $r_1, r_2 \in Z_q^*$，并计算：

$U=r_1P$

$R=e(r_1P_{pub}, Q_B)$

$h=H_1(ID_A, ID_B, m, R, U)$

$W=r_1P_{pub}+(h+r_2)\cdot S_A$

生成的签名 $\sigma=(m, r_2, U, W)$。

Verify：对于给定的系统参数和签名者 Alice 的公钥 Q_A，指定验证者 Bob 收到关于消息 m 的签名 σ 后，计算：

$R=e(U, S_B)$

$h=H_1(ID_A, ID_B, m, R, U)$

然后 Bob 验证等式 $e(W, Q_B) \stackrel{?}{=} R\cdot e((h+r_2)\cdot Q_A, S_B)$，若成立，接受该签名；否则拒绝。

Simulate：对于任意一个消息 $m' \in \{0,1\}^*$，Bob 能产生一个签名 σ'，随机选择 $a, k \in Z_q^*$，并且令 $U'=aP-kQ_A$，计算：

$R'=e(aP-kQ_A, S_B)$

$h'=H_1(ID_A, ID_B, m', U', R')$

$W'=aP_{pub}$

$r_2'=(k-h') \bmod q$

那么签名 $\sigma'=(m', r_2', U', W')$ 就是一个有效的签名。

5 安全性分析与证明

5.1 正确性

算法的正确性可通过以下等式验证：

$$\begin{aligned} R\cdot e((h+r_2)\cdot Q_A, S_B) &= e(r_1P_{pub}, Q_B)e((h+r_2)\cdot Q_A, S_B) \\ &= e(r_1P_{pub}, Q_B)e((h+r_2)\cdot S_A, Q_B) \\ &= e(r_1P_{pub}+(h+r_2)\cdot S_A, Q_B) \\ &= e(W, Q_B) \end{aligned}$$

所以方案的验证等式成立。

模拟算法的正确性可通过以下等式验证：

$$\begin{aligned} R'\cdot e((h'+r_2')\cdot Q_A, S_B) &= e(aP-kQ_A, S_B)e((h'+r_2')\cdot Q_A, S_B) \\ &= e(aP, S_B) \\ &= e(aP_{pub}, Q_B) \\ &= e(W, Q_B) \end{aligned}$$

所以，模拟算法产生的签名 $\sigma'=(m', r_2', U', W')$ 可以通过验证等式的验证，因此该签名是有效的。

5.2 不可传递性

由方案的副本模拟过程可知，模拟签名是有效的签名，可以通过验证算法的验证。对于任意一个消息 $m' \in \{0,1\}^*$，指定验证者 Bob 随机地选择 $a, k \in Z_q^*$，并且令 $U'=aP-kQ_A$，计算：$R'=e(aP-kQ_A, S_B)$，$h'=H_1(ID_A, ID_B, m', U', R')$，$W'=aP_{pub}$，$r_2'=(k-h') \bmod q$，生成模拟签名 $\sigma'=(m', r_2', U', W')$，并且也能使验证等式 $e(W, Q_B) \stackrel{?}{=} R\cdot e((h+r_2)\cdot Q_A, S_B)$ 成立。也就是说指定验证者 Bob 能够产生与签名者 Alice 的签名不可区分的签名副本，所以本文提出的方案满足不可传递性。

5.3 不可伪造性

给定一个 GBDH 问题实例，$P, P_1, P_2, P_3 \in G_1$，其中 $P_1=aP$，$P_2=bP$，$P_3=cP$，然而，a, b, c 未知。构造算法 E，E 模拟挑战者与敌手 Z 交互，并在 DBDH 预言机的帮助下，计算 $e(P,P)^{abc} \in G_2$ 的值。

设置：将系统公钥设为 $P_{pub}=bP$。方案中的签名者 ID_A 和指定验证者 ID_B 的公钥设为 $Q_A=aP$，$Q_B=cP$，其中 $a, b, c \in Z_q^*$。

H_1 询问：挑战者保存一个包含元组 (ID_i, Q_i) 的列表 $H_1\text{-}list$。$H_1\text{-}list$ 初始化为空，当敌手 Z 询问的身份值为 ID_i 时，若 $H_1\text{-}list$ 表中已有相应记录，则直接返回 Q_i；若没有记录，算法 E 做如下操作，并将回答后的 (ID_i, Q_i) 的值加入到列表 $H_1\text{-}list$ 中。

$$Q_i=H_1(ID_i)=\begin{cases} aP, & \text{if } ID_i=ID_A \\ bP, & \text{if } ID_i=ID_B \\ r_iP, & \text{if } ID_i\neq ID_A, ID_B, r_i\in Z_q^* \end{cases}$$

密钥询问：挑战者保存一个包含元组 (ID_i, Q_i, S_i) 的列表 $Extract\text{-}list$。敌手 Z 询问的身份值为 ID_i 的私钥时，若 $i\neq A$ 并且 $i\neq B$，挑战者返回 $S_i=r_i(bP)$ 作为身份值为 ID_i 的私钥，否则放弃。

H_2 询问：挑战者保存一个包含元组 $(ID_i, ID_j, m_i, U_i, R_i, h_i)$ 的列表 $H_2\text{-}list$。当敌手 Z 询问 $(ID_i, ID_j, m_i, U_i, R_i)$ 的值时，若 $H_2\text{-}list$ 表中已有相应记录，则直接返回 h_i；若没有，算法 E 随机地选取 $h_i \in Z_q^*$ 返回给 A_1，并将 $(ID_i, ID_j, m_i, U_i, R_i, h_i)$ 的值添加到列表 $H_2\text{-}list$ 中。

签名询问：若敌手 Z 向挑战者询问关于消息 m_i 的签名，其中签名者的身份值为 ID_i，指定验证者的身份值为 ID_j，挑战者作如下回答：

· 若 $i\neq A$ 并且 $i\neq B$，那么挑战者计算签名人 ID_i 的私钥为 $S_{ID_i}=r_iP_{pub}=r_ibP$，任选 $r_1, r_2 \in Z_q^*$ 并计算：

$U_i=r_1P$

$R_i=e(r_1P_{pub}, Q_B)$

$h_i=H_1(ID_i, ID_j, m_i, R_i, U_i)$

$W_i=r_1P_{pub}+(h_i+r_2)\cdot S_{ID_i}$

$\sigma_i=(m_i, r_2, U_i, W_i)$

· 若 $j\neq A$ 并且 $j\neq B$，那么挑战者计算指定验证者 ID_j 的私钥为 $S_{ID_j}=r_jP_{pub}=r_jbP$，任选 $a, k \in Z_q^*$ 并计算：

$U_i=aP-kQ_{ID_i}$

$R_i=e(aP-kQ_{ID_i}, S_{ID_j})$

$h_i=H_1(ID_i, ID_j, m_i, R_i, U_i)$

$W_i=aP_{pub}$

$r_2=(k-h_i) \bmod q$

· 否则，放弃。

验证询问：敌手 Z 向挑战者对于签名 σ 进行验证询问，其中签名者的身份值为 ID_i，指定验证者的身份值为 ID_j。挑战者检查是否有 $(i,j)=(A,B)$ 或者 $(i,j)=(B,A)$，若等于，挑战者终止询问；若不等于，挑战者计算指定验证者的私钥 $S_{ID_j}=r_jP_{pub}$，通过验证算法来验证签名的有效性。若签名有效，输出 1；否则，输出 0。

最终，敌手 Z 可以输出一个关于消息 m^* 有效的签名 σ^*，其中签名者的身份值为 ID_i，指定验证者的身份值为 ID_j。如果 $(i,j)=(A,B)$ 或者 $(i,j)=(B,A)$，挑战者成功伪造签名 σ^*；否则，挑战者输出“失败”并退出。$(i,j)=(A,B)$ 或者 $(i,j)=(B,A)$ 的有效签名 σ^* 必满足验证等式 $e(W, Q_B)=R\cdot e((h+r_2)\cdot Q_A, S_B)$。

（下转第 57 页）

splitting of an arbitrary three-qubit state by using two four-qubit cluster states[J]. Quantum Information Processing, 2011, 10(3): 297-305

[15] Li Dong-fen, Wang Rui-jin, Zhang Feng-li, et al. Quantum information splitting of arbitrary two-qubit state by using four-qubit cluster state and Bell-state[J]. Quantum Information Processing, 2015, 14: 1103-1116

[16] Kang Shuang-yong, Chen Xiu-bo, Yang Yi-xian. Asymmetric Quantum Information Splitting of an Arbitrary N-qubit State via GHZ-like State and Bell States[J]. International Journal of Theoretical Physics, 2014, 53: 1848-1861

[17] Saha D, Panigrahi P K. N-qubit quantum teleportation information splitting and superdense coding through the composite GHZ-Bell channel[J]. Quantum Information Processing, 2012, 11(2): 615-628

[18] Li Dong-fen, Wang Rui-jin, Zhang Feng-li. Quantum information splitting of arbitrary three-qubit state by using four-qubit cluster state and GHZ-state[J]. International Journal of Theoretical Physics, 2015, 54: 1142-1153

[19] Bai Ming-qiang, Mo Zhi-wen. Hierarchical quantum information splitting with eight-qubit cluster states[J]. Quantum Information Processing, 2013, 12: 1053-1064

[20] Muralidharan S, Jain S, Panigrahi P K. Splitting of quantum information using N-qubit linear cluster states[J]. Optics Communications, 2011, 284(4): 1082-1085

[21] Thomas M C, Thomas J A. Elements of information theory[M]. United States of America, 2006: 187-189

[22] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2000: 356-386

(上接第 52 页)

因此，可以计算得到

$$e(P,P)^{abc}=e(aP,bcP)=e(aP,bQ_B)=e(Q_A,S_B)=\left(\frac{e(W,Q_B)}{R}\right)^{(h+r_2)^{-1}}$$

这与计算 CBDH 问题相矛盾，所以我们提出的方案是不可伪造的。

5.4 效率分析

下面将本文方案与 FeiTang 的方案[10]和 Hafizul Islam 的方案[11]做性能上的比较，并将结果列于表 1 中。表 1 中的 P 表示双线性映射中的对操作。

表 1 比较结果

方案	签名阶段	验证阶段	模拟阶段	总和
本文方案	1P	3P	1P	5P
FeiTang	3P	4P	4P	11P
Hafizul Islam	3P	1P	2P	6P

FeiTang 等人提出的方案中，签名阶段使用了 3 次双线性对的计算，验证和模拟阶段各使用了 4 次双线性对的计算，共需要计算双线性对 11 次；Hafizul Islam 等人的方案在签名阶段、验证阶段、模拟阶段共使用了 6 次双线性对的计算；本文的方案共使用 5 次双线性对。双线性对的计算是极其耗时的，所以本文的方案比文献[9,11]中的方案更有效。

结束语 指定验证者签名由于其具有的特殊性质，已经被广泛地应用在生活的各个领域。本文首先提出了基于身份的强指定验证者签名方案的定义和安全模型，然后构造了一个基于身份的强指定验证者签名方案，并证明了该方案的正确性、不可传递性和不可伪造性。基于 GBDH 假设，证明了方案对适应性选择消息攻击是存在不可伪造的。最后分析了方案的计算代价，结果表明本文的方案具有较高的效率。

参 考 文 献

[1] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications[M]// Advances in Cryptology (EUROCRYPT'96). Springer Berlin Heidelberg, 1996: 143-154

[2] Saeednia S, Kremer S, Markowitch O. An efficient strong designated verifier signature scheme[M]// Information Security and Cryptology (ICISC 2003). Springer Berlin Heidelberg, 2004: 40-54

[3] Susilo W, Zhang F, Mu Y. Identity-based strong designated verifier signature schemes[M]// Information Security and Privacy. Springer Berlin Heidelberg, 2004: 313-324

[4] Kancharla P K, Gummadidala S, Saxena A. Identity based strong designated verifier signature scheme[J]. Informatica, 2007, 18(2): 239-252

[5] Kang B, Boyd C, Dawson E. Identity-based strong designated verifier signature schemes: attacks and new construction[J]. Computers & Electrical Engineering, 2009, 35(1): 49-53

[6] Kang B, Boyd C, Dawson E D. A novel identity-based strong designated verifier signature scheme[J]. Journal of Systems and Software, 2009, 82(2): 270-273

[7] Zhang J, Mao J. A novel ID-based designated verifier signature scheme[J]. Information Sciences, 2008, 178(3): 766-773

[8] Islam S H, Biswas G P. An efficient and secure strong designated verifier signature scheme without bilinear pairings[J]. J. Appl. Math. Info, 2013, 31(3/4): 425-441

[9] Tang F, Lin C, Li Y, et al. Identity-based strong designated verifier signature scheme with full non-delegatability[C]// 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2011: 800-805

[10] Tian H, Chen X, Zhang F, et al. A non-delegatable strong designated verifier signature in ID-based setting for mobile environment[J]. Mathematical and Computer Modelling, 2013, 58(5): 1289-1300

[11] Hafizul I S K, Biswas G P. Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings[J]. Journal of King Saud University-Computer and Information Sciences, 2013, 25(1): 51-61

[12] Schnorr C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174

[13] Joux A. A one round protocol for tripartite Diffie-Hellman[M]// Algorithmic Number Theory. Springer Berlin Heidelberg, 2000: 385-393

[14] Smart N P. Identity-based authenticated key agreement protocol based on Weil pairing[J]. Electronics Letters, 2002, 38(13): 630-632