一个无证书强指定验证者签名方案的安全性分析与改进

刘 唐[1,2] 汪小芬[3] 丁雪峰[4]

(四川师范大学基础教学学院 成都 610068)[1] (四川大学计算机学院 成都 610065)[2]
(电子科技大学计算机科学与工程学院 成都 611731)[3] (四川大学信息管理中心 成都 610065)[4]

摘 要 Hafizul Islam SK 和 G. P. Biswas 最近基于椭圆曲线双线性对提出一个无证书强指定验证者签名方案,并声称该方案在三类敌手攻击模型下是可证明安全的,即第一类只得到系统公开参数和公钥的敌手,第二类可替换签名和验证者公钥的敌手,第三类可得到系统主密钥的敌手。分析该强指定验证者签名方案不能抵抗第三类敌手的攻击,亦即第三类敌手可以伪造有效的签名。针对此缺陷,对该无证书强指定验证者签名方案做了改进,在改进方案中,验证者的秘密私钥(由参与者独立产生的私钥)参与签名的验证计算,因此有效避免了原有方案的安全缺陷。最后对改进方案作了安全性分析,说明改进方案确实能抵抗三类敌手的攻击。

关键词 无证书的公钥密码系统,强指定验证者签名,双线性对

中图法分类号 TP918.1 **文献标识码** A

Security Analysis and Improvement of Certificateless Strong Designated Verifier Signature Scheme

LIU Tang[1,2] WANG Xiao-fen[3] DING Xue-feng[4]

(School of Fundamental Education, Sichuan Normal University, Chengdu 610068, China)[1]
(School of Computer Science, Sichuan University, Chengdu 610065, China)[2]
(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)[3]
(Information Management Center, Sichuan University, Chengdu 610065, China)[4]

Abstract Hafizul Islam SK and G. P. Biswas recently proposed a certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairing, and claimed their scheme satisfies provable security against three types of adversaries, including the type 1 adversary who only learns the system public parameters, the type 2 adversary who can't obtain the private key of the user and the system master key, but can replace the user's public key, and the type 3 adversary who has obtained the system master key. However, this paper pointed out their signature scheme is actually not secure as claimed by presenting an attack launched by an adversary who has learned the system master key. Furthermore, to make up this flaw, we also provided an revised certificateless strong designated verifier signature scheme in which the verifier's partial private key generated by himself is included in the computation of the verification procedure, thus above attack can be efficiently resisted.

Keywords Certificateless public key cryptosystem, Strong designated verifier signature, Bilinear pairing

1 引言

Diffie 和 Hellman (1976 年) 首次提出公钥密钥系统(PKC)[1],在公钥密码系统中用公钥证书来验证对应的公钥。然而传统的公钥密码系统有以下缺陷:(1)用户必须利用公钥证书来验证对方的公钥,这带来了额外的计算开销;(2)公钥密码系统有公钥证书产生、存储、分发和恢复等问题,这也给系统带来沉重负担。针对这些问题,1984 年 Shamir 提出了基于身份的公钥密钥系统(IBC)[2],它不需要公钥证书,用户的身份直接作为公钥,而用户的私钥由密钥生成中心(PKG)产生。2001 年,Boneh 和 Franklin 首次基于椭圆曲线群[3,4],利用其上的双线性对设计了实用的基于身份的加密(IBE)方案[5]。在 IBC 系统中存在私钥分发的问题,因为用户私钥是由 PKG 产生的,因此 PKG 必须是绝对可信的。然而在现实公开网络中 PKG 可能是恶意的,恶意 PKG 可以伪造其下面任何用户的签名。

2003 年 Al-Riyami 和 Paterson 提出了无证书公钥密码系统(CL-PKC)[6],它避免了传统公钥系统中公钥证书的缺陷以及基于身份公钥系统中密钥分发的缺陷,因而近几年受到越来越多的关注。在 CL-PKC 中,用户的私钥由两部分构成,一部分是由 PKG 利用用户身份信息和系统主密钥生成的,另一部分是用户自己选择只有他本人掌握的。

到稿日期:2012-09-14 返修日期:2012-12-14 本文受四川省科技支撑计划项目(2012GZ0001),四川师范大学科研项目(13KYL06),上海市科学技术委员会基金项目(11511505300)资助。

刘 唐(1980—),男,硕士,讲师,CCF 会员,主要研究方向为无线传感器网络,E-mail:crikey@163.com;汪小芬(1982—),女,博士,讲师,主要研究方向为信息与网络安全;丁雪峰(1974—),男,讲师,主要研究方向为计算机网络,E-mail:dingxf@scu.edu.cn(通信作者)。

1996 年 Jakobsson 等人提出指定验证者签名方案(DVS)[7]，即签名者例如 Alice 产生的签名只能由指定的验证者例如 Bob 来验证，进而在 DVS 方案中 Bob 能向第三方证明该签名是由 Alice 产生的。因此 DVS 方案的公开证明不能保护签名者的隐私 。为实现签名者隐私保护，1996 年 Jakobsson 等人又提出强指定验证者签名方案(SDVS)[7]，在 SDVS 方案中 Bob 不能向其他人确定该签名是 Alice 产生的还是他自己产生的。这是因为 Bob 能计算出相同的签名，而且签名验证时需要 Bob 的私钥参与计算。

2007 年，Yang 等人设计了一个无证书通用的指定验证者签名方案 (CL-UDVS)[8]，并证明该方案在随机预言机模型下对于不同类型敌手是可证明安全的。然而，2009 年 Guozheng 和 Fan 指出 yang 等人的方案对于公钥替换攻击和恶意 PKG 攻击是不安全的[9]。2006 年，Huang 等人给出了 CL-SDVS 方案的安全性概念，并构造了随机预言机模型下可证明安全的 CL-SDVS 方案[10]。然而，他们的方案不能抵抗恶意 PKG 的攻击。2007 年，Du 和 Wen[11] 以及 Chen 等人[12] 分别基于双线性对提出 CL-SDVS 方案，并作了形式化安全性证明。然而，2009 年 Fan 等人证明 Du 和 Wen 的方案不能抵抗公钥替换攻击[13]。2011 年，Tso 等人[14] 以及 Choi 等人[15]分别提出可证明安全的 CL-SDVS 方案，然而后者的方案对于公钥替换攻击是不安全的[16]。

2012 年 Hafizul Islam SK 和 G. P. Biswas 基于椭圆曲线上的双线性对提出一个最高效的强指定验证者签名方案[17]，并在随机预言机模型下证明该方案对于无证书公钥系统中的三类敌手是可证明安全的。本文对该方案作了分析，指出 Hafizul Islam SK 和 G. P. Biswas 的方案不能抵抗恶意 PKG 的攻击；同时对该方案作了改进，并进行安全性分析，证明改进后的方案能有效抵抗恶意 PKG 的攻击。

2 背景知识

2.1 双线性对

假定 q 为一个大素数(如 160 比特)，群 G_1 为由 P 生成的 q 阶加法群，G_2 为 q 阶乘法群。双线性对 $e: G_1 \times G_1 \to G_2$ 为具有如下性质的映射[18]：

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

(2)非退化性：$e(P, P) \neq 1$，1 是 G_2 的单位元，若 P 为 G_1 的生成元，则 $e(P, P)$ 是 G_2 的生成元；

(3)可计算性：对任意 $(P, Q) \in G_1 \times G_1$，存在有效多项式算法计算 $e(P, Q)$。

2.2 无证书强指定验证者签名方案

一个无证书强指定验证者签名(CL-SDVS)方案中包含 3 个角色：一个 PKG、签名者及指定验证者。一个 CL-SDVS 由以下 8 个算法构成：

Setup：算法输入安全参数 k，返回系统主密钥 msk 和系统公开参数 Ω。

ExtractIDBasedKey：算法输入系统主密钥 msk 和用户的身份信息 ID_i，返回用户的部分私钥 D_i。

SetSecretValue：算法输入系统公钥 mpk 和用户的身份信息 ID_i，返回用户的秘密值 x_i。

SetPrivateKey：输入系统公开参数 mpk，部分私钥 D_i，秘密值 x_i，输出用户 ID_i 的整体私钥 sk_i。

SetPublicKey：算法输入系统公钥 mpk，用户的部分私钥 D_i 和秘密值 x_i，返回用户的公钥 pk_i。

CL-SDVS-Sign：算法输入系统公开参数 Ω，签名者 ID_i 的私钥 sk_i，消息 $m \in \{0,1\}^*$，并指定验证者 ID_j 的公钥 pk_j，输出对消息 m 的签名 σ。

CL-SDVS-Verify：算法输入系统公开参数 Ω，签名者 ID_i 的公钥 pk_j，指定验证者 ID_j 的私钥 sk_j，以及消息和签名对 (m, σ)，若验证有效则输出“T”，若签名无效则输出“F”。

CL-SDVS-Smulation：指定验证者 ID_j 执行该算法并产生相同的签名 σ'，该签名与签名者 ID_i 的签名 σ 是无法区分的。

2.3 无证书强指定验证者签名方案的敌手类型

无证书强指定验证者签名方案的敌手根据其攻击能力的不同分为 3 个类型，类型 I 的敌手 $\mathcal{A}_1$ 是系统外部人员，他只能获得系统的公开参数；类型 II 的敌手 $\mathcal{A}_2$ 是不诚实的系统内部用户；类型 III 的敌手 $\mathcal{A}_3$ 是恶意的 PKG。对这 3 个类型敌手的正式说明如下：

类型 I 的敌手 $\mathcal{A}_1$——这种类型的敌手只能获得系统公开参数，并试图获得用户的私钥或系统主密钥来伪装成合法用户。

类型 II 的敌手 $\mathcal{A}_2$——这种类型的敌手也称为公钥替换攻击者，他们知道系统公开参数，不知道用户的部分私钥，但可以用他们自己选择的公钥替换用户的原有公钥。

类型 III 的敌手 $\mathcal{A}_3$——这种类型的敌手也称为恶意 PKG，他们能获得用户的部分私钥(由 PKG 产生的部分私钥)，但不能替换用户的公钥。

3 Hafizul Islam SK 和 G. P. Biswas 的无证书强指定验证者签名方案

本节介绍 Hafizul Islam SK 和 G. P. Biswas 的基于双线性对的无证书强指定验证者签名方案[17]。在该方案中签名者 Alice 的公钥为 $pk_A = (Q_A, P_A)$，私钥为 $sk_A = (D_A, x_A)$；指定验证者 Bob 的公钥为 $pk_B = (Q_B, P_B)$，私钥为 $sk_B = (D_B, x_B)$。该方案由 8 个子算法构成：

1. Setup：算法输入安全参数 k，返回系统参数和主密钥。令 G_1 为由 P 生成的 q 阶加法群，G_2 为 q 阶乘法群，$e: G_1 \times G_1 \to G_2$ 为双线性对。系统初始化步骤如下：

1)随机选取 $s \in_R Z_q^*$，s 为主密钥；计算 $P_0 = sP$；

2)选取 Hash 函数 $H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^* \times G_1 \to Z_q^*$ 和 $H_3: \{0,1\}^* \times G_2 \times G_2 \to Z_q^*$；

3)设置系统公开参数 $\Omega = \{G_1, G_2, q, P, P_0, H_1, H_2, H_3\}$，系统主密钥 s 保密。

2. ExtractIDBasedKey：输入系统公开参数 Ω，主密钥 s 和用户的身份信息 ID_i，按下列方法产生部分私钥：

1)计算 $Q_i = H_1(ID_i)$；

2)计算部分私钥 $D_i = sQ_i$，并将其通过安全信道发送给用户 ID_i。

3. SetSecretValue：身份信息为 ID_i 的用户随机选择 $x_i \in_R Z_q^*$，计算 $P_i = x_i P$，设置它的秘密值为 x_i。

4. SetPrivateKey：用户 ID_i 设置其完整私钥为 $sk_i = (D_i, x_i)$。

5. SetPublicKey：用户 ID_i 设置其完整公钥为 $pk_i=(Q_i, P_i)$。

6. CL-SDVS-Sign：签名者 Alice 随机选取 $r\in_R Z_q^*$，然后计算指定验证者为 Bob 的消息 $m\in\{0,1\}^*$ 的签名，方法如下：

1)计算 $g=e(D_A,Q_B)$，$h=H_2(m,x_AP_B)$；

2)计算 $R=e(P_0,Q_B)^h$，$t=H_3(m,g,R)$；

3)计算 $V=rhP_0+tD_A$，$S=e(V,Q_B)$；

4)将签名(R,S)发送给 Bob。

7. CL-SDVS-Verify：在收到消息 m 和签名(R,S)，Bob 按照下列方法进行验证：

1)计算 $g=e(Q_A,D_B)$，$t=H_3(m,g,R)$；

2)计算 $S'=R\cdot g^t$，然后检查 $S'=S$ 是否成立，若等式成立，则 Bob 接受(R,S)为 Alice 对于消息 m 的有效签名；否则，拒绝该签名。

8. CL-SDVS-Simulation：Bob 按照下列方法，能模拟一个 Alice 对消息 m 的有效签名$(\hat{R},\hat{S})$：

1)计算$\hat{g}=e(Q_A,D_B)$和$\hat{h}=H_2(m,x_BP_A)$；

2)随机选取$\hat{r}\in_R Z_q^*$，计算$\hat{R}=e(P_0,Q_B)^{\hat{r}\hat{h}}$，$\hat{t}=H_3(m,\hat{g},\hat{R})$；

3)计算$\hat{S}=\hat{R}\cdot\hat{g}^{\hat{t}}$，并输出签名$(\hat{R},\hat{S})$。

可验证模拟签名$(\hat{R},\hat{S})$是一个消息 m 的有效签名。

4 Hafizul Islam SK 和 G. P. Biswas 签名方案的攻击与改进

Hafizul Islam SK 和 G. P. Biswas[17] 声称他们的强指定验证者签名方案在随机预言机模型下对于第一、第二和第三类敌手都是可证明安全的。然而，我们将给出一个有效的攻击，即敌手掌握了 PKG 的主密钥 s，就可以伪造签名。

4.1 攻击

假设第三类敌手 $\mathcal{A}$ 获得了 PKG 的主密钥 s，则 $\mathcal{A}$ 可以按照下述的攻击方法伪造签名者 Alice 的签名。

1)随机选取 $\tilde{r}\in_R Z_q^*$；

2)计算 $\tilde{g}=e(Q_A,Q_B)^s$；

3)随机选取 $\tilde{h}\in_R Z_q^*$，计算 $\tilde{R}=e(P_0,Q_B)^{\tilde{r}\tilde{h}}$；

4)计算 $\tilde{t}=H_3(m,\tilde{g},\tilde{R})$；

5)计算 $\tilde{S}=\tilde{R}\cdot\tilde{g}^{\tilde{t}}$；

6)输出对消息 m 的伪造签名$(\tilde{R},\tilde{S})$。

显然，Bob 验证签名$(\tilde{R},\tilde{S})$时，等式成立。因此敌手 $\mathcal{A}$ 可以成功伪造 Alice 的签名。

4.2 改进方案

从上述的安全性分析来看，Hafizul Islam SK 和 G. P. Biswas 的强指定验证者签名方案不安全是因为用户自生成的私钥 x_A 虽然参与计算签名，但在签名验证时没有体现自生成私钥 x_A 在签名中的作用。下面对 Hafizul Islam SK 和 G. P. Biswas 的强指定验证者签名方案做了改进，使得签名能抵抗上述攻击。改进方案中 Setup、ExtractIDBasedKey、SetSecretValue、SetPublicKey 和 SetPrivateKey 与第 3 节相同，只对 CL-SDVS-Sign、CL-SDVS-Verify、CL-SDVS-Simulation 部分做了修改，具体如下：

6′. CL-SDVS-Sign：签名者 Alice 随机选取 $r\in_R Z_q^*$，然后计算指定验证者为 Bob 的消息 $m\in\{0,1\}^*$ 的签名，方法如下：

1)计算 $g=e(D_A,Q_B)$，$h=H_2(m,x_AP_B)$；

2)计算 $R=e(P_0,Q_B)^r$，$t=H_3(m,g,R)$；

3)计算 $V=rhP_0+tD_A$，$S=e(V,Q_B)$；

4)将签名(R,S)发送给 Bob。

7′. CL-SDVS-Verify：在收到消息 m 和签名(R,S)后，Bob 按照下列方法进行验证：

1)计算 $g=e(Q_A,D_B)$，$h=H_2(m,x_BP_A)$，$t=H_3(m,g,R)$；

2)计算 $S'=R^h\cdot g^t$，然后检查 $S'=S$ 是否成立，若等式成立，则 Bob 接受(R,S)为 Alice 对于消息 m 的有效签名；否则，拒绝该签名。

8′. CL-SDVS-Simulation：Bob 按照下列方法，能模拟一个 Alice 对消息 m 的有效签名$(\hat{R},\hat{S})$：

1)计算$\hat{g}=e(Q_A,D_B)$和$\hat{h}=H_2(m,x_BP_A)$；

2)随机选取$\hat{r}\in_R Z_q^*$，计算$\hat{R}=e(P_0,Q_B)^{\hat{r}}$，$\hat{t}=H_3(m,\hat{g},\hat{R})$；

3)计算$\hat{S}=\hat{R}^{\hat{h}}\cdot\hat{g}^{\hat{t}}$，并输出签名$(\hat{R},\hat{S})$。

可验证模拟签名$(\hat{R},\hat{S})$是一个消息 m 的有效签名。

9. 正确性：若(R,S)为 Alice 对于消息 m 的有效签名，则

$$\begin{aligned}S&=e(V,Q_B)=e(rhP_0+tD_A,Q_B)\\&=e(rhP_0,Q_B)e(tD_A,Q_B)=e(P_0,Q_B)^{rh}e(D_A,Q_B)^t\\&=R^he(Q_A,D_B)^t=R^hg^t\end{aligned}$$

5 安全性分析

在这部分，我们分析改进方案的安全性。我们的强指定验证者签名方案是基于 Hafizul Islam SK 和 G. P. Biswas 的强指定验证者签名方案的改进，因此改进的签名方案满足 Hafizul Islam SK 和 G. P. Biswas 的强指定验证者签名方案已有的安全性。下面分析改进的强指定验证者签名方案能抵抗第三类敌手的攻击。

假设敌手 $\mathcal{A}$ 获得了 PKG 的主密钥 s，则

1)敌手可计算 $g=e(Q_A,Q_B)^s$；

2)通过随机选取 $r\in_R Z_q^*$，敌手可计算 $R=e(P_0,Q_B)^r$；

3)敌手可计算 $t=H_3(m,g,R)$。

然而敌手 $\mathcal{A}$ 没有 Alice 的私钥 x_A，也没有 Bob 的私钥 x_B，因此敌手 $\mathcal{A}$ 不能计算 $h=H_2(m,x_AP_B)=H_2(m,x_BP_A)=H_2(m,x_Ax_BP)$。而改进的签名方案中，签名的验证需要 h 的参与，而且 $h=H_2(m,x_Ax_BP)$ 必须成立。因此，敌手无法计算能通过验证等式的有效签名。

通过上述分析可知，改进的强指定验证者签名方案能抵抗第三类敌手的攻击。

结束语 本文我们通过具体的攻击发现 Hafizul Islam SK 和 G. P. Biswas 的强指定验证者签名方案在他们给出的安全模型下是不安全的，只要敌手得到系统主密钥，敌手就可以伪造有效的签名。本文对强指定验证者签名方案做了改

(下转第 166 页)

模板，与以往工作不同，本文通过统计获得大量的模板，因此，模板更详细、更全面；其次，本文分别统计评价对象与评价短语对应的模板，没有像以往方法那样固定评价对象模板与评价短语模板之间的搭配，这样进一步丰富了模板的数量；再次，本文通过调节评价对象与评价短语之间的距离，并利用评价搭配的出现概率完成评价搭配的筛选，取得了较好的实验效果；最后，以 HowNet 情感词典为基础，通过挖掘情感词的同义词信息完成情感强度修正，并通过综合考虑修饰成分与情感词的影响进行倾向性判断。

在今后的工作中，我们会尝试消除模板数量增加与最远距离增加时引入的噪音，从而提高本文评价搭配抽取方法的准确率。

参 考 文 献

[1] 赵妍妍，秦兵，刘挺. 文本情感分析[J]. 软件学报，2010，21(8)：1834-1848

[2] Liu Bing. Sentiment Analysis and Subjectivity(Second Edition)[M]. Indurkhya N, Damerau F J, eds. Handbook of Natural Language Processing, 2010

[3] 徐冰，赵铁军，王山雨，等. 基于浅层句法特征的评价对象抽取研究[J]. 自动化学报，2011，37(10)：1241-1247

[4] 张姝，贾文杰，夏迎炬，等. 基于 CRF 的评价对象抽取技术研究[C]// 黄萱菁，许洪波，赵军. 第一届中文倾向性分析评测会议. 北京：2008：70-76

[5] Kobayashi N, Inui K, Matsumoto Y. Collecting evaluative expressions for opinion extraction [C]// Nagao M, ed. Proc. of the Int'l Joint Conf. on Natural Language Processing (IJCNLP). Morristown: ACL, 2004: 584-589

[6] 王菲，吴云芳，徐艺峰，等. 词语搭配情感倾向的自动判别方法[C]// 许洪波，孙乐，姚天昉. 第三届中文倾向性分析评测会议. 济南，2011：52-64

[7] Popescu A M, Etzioni O. Extracting product features and opinions from reviews [C]// Mooney R J, ed. Proc. of HLT/EMNLP 2005. Morristown: ACL, 2005: 339-346

[8] Yao T F, Peng S W. A study of the classification approach for Chinese subjective and objective texts [C]// Zhu QM, et al., eds. Proc. of NCIRCS 2007. 2007: 117-123

[9] Ku L, Liang, Chen H. Opinion Extraction, Summarization and Tracking in News and Blog Corpora [C]// American Association for Artificial Intelligence (AAAI). 2006: 100-107

[10] Ku L, Lo Y, Chen H. Using opinion scores of words for sentence-level opinion extraction [C]// Proceeding of the 6th NTCIR Workshop Meeting on Evaluation of Information Access Technologies. 2007: 316-322

[11] 许洪波，孙乐，姚天昉，等. 第三届中文倾向性分析评测总结报告[C]// 第三届中文倾向性分析评测会议. 济南，2011：1-24

(上接第 128 页)

进，而且分析说明改进方案可以抵抗第三类敌手的攻击。

参 考 文 献

[1] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[2] Shamir A. Identity based cryptosystems and signature scheme [C]// Crypto 1984, LNCS. vol. 196, Springer-Verlag, 1984: 47-53

[3] Miller V S. Use of elliptic curves in cryptography [C]// Proceeding of the Crypto'85. New York: Springer-Verlag, 1985: 417-426

[4] Koblitz N. Elliptic curve cryptosystem [J]. Journal of Mathematics of Computation, 1987, 48(177): 203-209

[5] Boneh D, Franklin M K. Identity-based encryption from the Weil pairing[C]// Proceedings of the Crypto'01, LNCS. vol. 2139, Springer-Verlag, 2001: 213-229

[6] Al-Riyami S, Paterson K. Certificateless public key cryptography [C]// Proceedings of the Asiacrypt'03, LNCS. vol. 2894, Springer-Verlag, 2003: 452-473

[7] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications[C]// Proceedings of the Eurocrypt'96, LNCS. vol. 1070, Springer-Verlag, 1996: 143-154

[8] Yang M, Shem X-Q, Wang Y-M. Certificateless universal designated verifier signature scheme[J]. The Journal of China Universities of Posts and Telecommunications, 2007, 14(3): 85-94

[9] Guozheng H, Fan H. Attacks against two provably secure certificateless signature schemes[C]// Proceedings of the WASE International Conference on Information Engineering. 2009: 246-249

[10] Huang X, Susilo W, Mu Y, et al. Certificateless designated verifier signature schemes[C]// Proceedings of the 20th International Conference on AINA'06. vol. 2, 2006: 15-19

[11] Du H, Wen Q. Efficient and provably-secure certificateless short signature scheme from bilinear pairings. Cryptology ePrint Archive[R]. Report 2007/250

[12] Chen H, Song R, Zhang F, et al. An efficient certificateless short designated verifier signature scheme[C]// Proceedings of the International Conference on WiCOM'08. Dalian, 2008: 1-6

[13] Fan C-I, Hsu R-H, Ho P-H. Cryptanalysis on Du-Wen certificateless short signature scheme[C]// Proceedings of the JWIS'09, Institute of Electrical and Electronics Engineers. Kaohsiung, 2009: 1-7

[14] Tso R, Yi X, Huang X. Efficient and short certificateless signatures secure against realistic adversaries[J]. Journal of Supercomputer, 2011, 55: 173-191

[15] Choi K Y, Park J H, Lee D H. A new provably secure certificateless short signature scheme[J]. Computers and Mathematics with Applications, 2011, 61(7): 1760-1768

[16] Tian M, Huang L, Yang W. On the security of a certificateless short signature scheme. Cryptology ePrint Archive [OL]. http://eprint.iacr.org/2011/419, 2011

[17] Hafizul Islam 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

[18] Boneh D, Lynn B, Shacham H. Short Signature from the Weil Paring[C]// Proceeding of Asiacrypt'01, LNCS 2248. Springer-Verlag, 2001: 514-532