一种强不可伪造无证书签名方案的密码学分析与改进

吴 涛,景晓军
(北京邮电大学信息与通信工程学院,北京 100876)

摘 要: 无证书密码体制是无线网络中一种非常有效安全保护工具. 2016年,Hung等人提出了标准模型下一种强不可伪造性的无证书签名方案,该方案声称在抗哈希碰撞问题和计算Diffle-Hellman困难问题假设下是安全不可伪造的. 事实上,该方案对类型II敌手是不安全的. 本文给出对Hung等的方案的安全性分析,并证明对于类型II敌手可以伪造出合法签名,针对存在问题提出一种改进的无证书签名方案.

关键词: 无证书签名; 双线性对; 安全性分析; 抗哈希碰撞; Diffle-Hellman假设
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2018)03-0602-05
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.03.013

Cryptanalysis and Improvement of a Certificateless Signature Scheme with Strong Unforgeability

WU Tao, JING Xiao-jun
(*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: Certificateless cryptographic schemes are very useful secure protection tools in wireless network. Quite recently, a certificateless signature with strong unforgeability in the standard model was presented by Hung et al. in 2016. Although they demonstrated that their scheme was secure and unforgeable under the collision resistant hash and computational Diffie Hellman assumptions, but we find that it is not secure against type II adversary. In this paper, we give security analysis to their scheme, and show that by giving concrete attack, a type II adversary could forge a legal signature of any message. We also put forward a possible fix of certificateless scheme which can solve secure problem.

Key words: certificateless signature; bilinear pairings; cryptanalysis; collision resistant hash; Diffie-Hellman assumptions

1 引言

通过无线传感网络节点或者用户传输的消息,必须得到验证才能成为有用的信息. 基于公钥基础设施(Public Key Infrastructure, PKI)[1]的签名算法为信息安全提供了一种保障工具,此类签名方案需要提供一个由权威认证中心发布的证书来证明这个公钥是对应用户的,并且这个公钥没有被第三方篡改或者替换. 权威认证中心管理证书的撤销、存储、分发和验证,这些操作引发的计算、通信延迟以及存储空间等问题在无线传感网络中是不可接受的,因此,人们将基于身份的无证书密码体制(Identity Public Key Cryptography, ID-PKC)[2]用在无线传感网络中实现对消息的认证. 在基于身份的无证书密码体制[3~5]中,存在一个可信任的密钥生成中心(Key Generation Center, KGC),KGC生成系统主密钥,利用用户的身份和主密钥生成用户的部分私钥,同时解决证书管理与密钥托管问题.

Al-Riyami和Paterson等在2003年的亚密会上首先提出了无证书的公钥密码体制模型[3],构造了基于椭圆曲线上的双线性对构造了第一个无证书签名方案,但是作者没有提供该方案的安全性证明,Hung等指出该方案不能抵抗公钥替换攻击[6]. 随后大量的无证书签名方案被研究者提出[7~16]. Choi等[7]在2011年提出一种可证明安全的无证书签名方案,但是陈等在文献

收稿日期: 2016-09-27;修回日期:2017-05-07;责任编辑:梅志强

[8]中指出该方案对于强的或者超级 Type I 敌手是不安全的. 文献[9]基于双线性对提出一个高效的无证书聚合签名方案,但是文献[10,11,15]中分别指出其存在安全漏洞以及伪造签名的方法. 文献[13]指出文献[12]中的无证书签名改进方案是不安全的,它不能抵抗消极不诚实 KGC 下的公钥替换攻击,也不能抵抗积极不诚实的 KGC 攻击,并对该方案进行了改进,而且给出了改进方案的安全性证明. 但实际上,文献[13]的方案仍然不能抵抗消极不诚实 KGC 下的公钥替换攻击. 文献[14]找出文献[15]中提出的无证书签名方案的弱点,其安全性证明以及改进方案在文献[9]中被提出. 2016 年,Hung 等在文献[16]中提出一种强不可伪造的安全无证书签名方案,尽管其声称该方案在抗哈希碰撞问题和计算 Diffle-Hellman (Computational Diffle-Hellman,CDH) 困难问题假设下是安全不可伪造的,但事实上,该方案对类型 II 敌手是不安全的. 本文指出文献中方案存在的缺陷,对应给出具体的攻击步骤,证明对于类型 II 敌手可以伪造出合法签名. 针对存在问题,提出一种改进的无证书签名方案.

2　预备知识

2.1　双线性映射与困难假设

设 G 和 G_T 是两个 p 阶乘法群,p 为素数,双线性映射 $\hat{e}:G\times G\to G_T$ 是满足以下性质的一个映射:

(1)双线性:对于所有的 $g_1,g_2\in G,\beta,\gamma\in Z_p$,均有 $\hat{e}(g_1^{\beta},g_2^{\gamma})=\hat{e}(g_1,g_2)^{\beta\gamma}$ 成立.

(2)非退化性:存在 $g_1,g_2\in G$,使得 $\hat{e}(g_1,g_2)\neq 1$.

(3)可计算性:给定任意 $g_1,g_2\in G$,存在多项式时间算法能成功计算 $\hat{e}(g_1,g_2)$.

定义 1　CDH 问题:对于任意 $g,g^{\beta},g^{\gamma}\in G,\beta,\gamma\in Z_p$,计算 $g^{\beta\gamma}$.

定义 2　CDH 假设:不存在多项式时间算法以不可忽略的优势 ε 解决 CDH 问题.

2.2　无证书签名的定义

一个无证书签名方案通常由以下几个算法构成.

系统初始化算法:输入一个安全参数 k,输出系统主密钥 msk 和系统参数 params. 这个算法由 KGC 执行.

部分私钥产生算法:输入用户身份 ID,msk 和 params,由 KGC 输出部分私钥 d_{ID},并通过安全信道传输给用户.

秘密值产生算法:输入用户 ID 和 params,由用户输出秘密值 x_{ID}.

私钥产生算法:输入 ID,params,d_{ID} 和 x_{ID},由用户输出私钥 $\mathrm{sk}_{\mathrm{ID}}$.

公钥产生算法:输入 ID 和 x_{ID},输出公钥 $\mathrm{PK}_{\mathrm{ID}}$. 算法由用户完成.

签名算法:输入 ID,params,d_{ID},x_{ID} 以及一个消息 m,由用户输出这个消息的签名 σ.

验证算法:这个算法由验证者完成. 输入 ID,params,$\mathrm{PK}_{\mathrm{ID}}$,$m$ 以及 σ,算法输出 1,表示签名有效,或者输出 0,表示签名无效.

一些文献将无证书签名方案的定义进行简化,将秘密值产生算法、私钥产生算法、公钥产生算法合并成一个用户密钥生成算法,无证书签名方案即由初始化算法、部分私钥产生算法、用户密钥生成算法、签名算法和验证算法五个算法组成.

2.3　无证书签名的安全模型

在无证书签名体系中,有两种类型的敌手:类型Ⅰ敌手 A_I 和类型Ⅱ敌手 A_{II}. A_{I}模拟一个外部的敌手,它可以获得用户的秘密值和更换用户的公钥,但是不能获得系统主密钥也不知道用户的部分私钥. 我们把类型Ⅰ的敌手发起的攻击称为密钥代替攻击. A_{II}代表一个恶意的 KGC,它知道系统主密钥但是不能更换任何用户的公钥.

无证书签名的安全性可用挑战者 C 与敌手 A_{I} 和类型Ⅱ手 A_{II} 进行以下两个游戏来模拟.

游戏Ⅰ(类型Ⅰ敌手 A_{I}):

初始化:挑战者 C 输入安全参数 k,运行初始化算法,生成主密钥 msk 和系统参数 params,并将 params 发送给 A_{I},同时保存 msk.

攻击:A_{I} 进行公钥询问、部分私钥询问、秘密值询问、公钥替换、签名询问等过程,C 模拟签名方案中算法并做出相应应答.

伪造:A_{I} 输出$(\mathrm{ID}^*,m^*,\sigma^*,\mathrm{PK}_{\mathrm{ID}}^*)$,当且仅当

(1)σ^* 是用户 ID^*、公钥 $\mathrm{PK}_{\mathrm{ID}}^*$、消息 m^* 的一个有效签名;

(2)A_{I} 没有询问过用户的部分私钥;

(3)A_{I} 没有询问过用户 ID^*、公钥 $\mathrm{PK}_{\mathrm{ID}}^*$ 对消息 m^* 的签名.

游戏Ⅱ(类型Ⅱ敌手 A_{II}):

初始化:挑战者 C 输入安全参数 k,运行初始化算法,生成主密钥 msk 和系统参数 params,并将 msk 和 params 发送给 A_{II}.

攻击:A_{II} 进行公钥询问、部分私钥询问、秘密值询问、签名询问等过程,C 模拟签名方案中算法并做出相应应答.

伪造:A_{II} 输出$(\mathrm{ID}^*,m^*,\sigma^*)$,当且仅当

(1)σ^* 是用户 ID^*、公钥 $\mathrm{PK}_{\mathrm{ID}}$、消息 m^* 的一个有效签名;

(2)A_{I} 没有询问过用户的秘密值并替换用户的公钥 $\mathrm{PK}_{\mathrm{ID}}$.

2.4　KGC 的信任级别

在无证书签名方案中,KGC 存在 3 类信任级别. 第

1 级,KGC 知道用户的私钥,可以假冒任何用户而不被发现;第 2 级,KGC 不知道用户的私钥,但是可以伪造用户的公钥而不被发现;第 3 级,KGC 不知道用户私钥,若伪造用户的公钥,可被察觉并证明该公钥是伪造的. 现有的大多数无证书签名方案的安全性都属于第 2 级.

在传统的基于 PKI 的密码系统中,若用户的公钥被替换,那么同一用户就存在两个不同的公钥证书,从而被发现伪造;而在无证书的密码体系中,用户必须相信 KGC 不会乱用用户的公钥. 所以,无证书体制本身是不可能抵抗消极不诚实的 KGC 攻击和积极不诚实 KGC 的攻击的.

3 Hung 等方案及安全性分析

Hung 等在 2016 年提出了一种具有强不可伪造性的安全无证书签名方案,我们首先回顾 Hung 等的方案,然后对其进行安全性分析,发现 Hung 等方案存在被伪造的可能.

3.1 Hung 等无证书签名方案

Hung 等方案由简化的无证书签名五个算法组成,简要描述如下.

初始化算法:给定安全参数 k,KGC 选择两个 p 阶循环群 G_1 和 G_2,以及一个双线性映射 $\hat{e}:G_1\times G_1\to G_2$. KGC 随机选择 $\alpha\in Z_p^*$ 和 $g_2\in G_1$,将 g_2^{α} 作为系统主密钥. 同时,KGC 选择 $g\in G_1$,$g_1=g^{\alpha}$,$H_1\sim H_5$ 是 5 个不同的哈希函数,$\boldsymbol{u}=(u_i)$,$\boldsymbol{s}=(s_i)$,$\boldsymbol{t}=(t_i)$,$\boldsymbol{w}=(w_i)$是长度为 m、n、n、l 的向量,KGC 公开系统参数 params = $\{G_1, G_2, \hat{e}, g, g_1, g_2, H_1\sim H_5, \boldsymbol{u}, \boldsymbol{s}, \boldsymbol{t}, \boldsymbol{w}\}$.

部分私钥产生算法:给定用户的身份 ID,计算 $\boldsymbol{v}=H_1(\mathrm{ID})=(v_1,v_2,\cdots,v_m)$,KGC 随机选择 $r_v\in Z_p^*$,计算部分私钥 $D_{\mathrm{ID}}=(D_1,D_2)=(g_2U^{r_v},g^{r_v})$,其中,$U=u'\prod_{j=1}^{m}u_j^{v_j}$.

用户密钥产生算法:用户随机选择 $\theta_1,\theta_2\in Z_p^*$,计算公钥 $\mathrm{PK}=(\mathrm{PK}_1,\mathrm{PK}_2)=(g^{\theta_1},g^{\theta_2})$,$\boldsymbol{b}=H_2(\mathrm{PK}_1,\mathrm{PK}_2)$,$\boldsymbol{c}=H_3(\mathrm{PK}_1,\mathrm{PK}_2)$,$S=s'\prod_{j=1}^{n}s_j^{b_j}$,$T=t'\prod_{j=1}^{n}t_j^{c_j}$,用户计算私钥 $\mathrm{SK}_{\mathrm{ID}}=g_2^{\theta_1}S^{\theta_1}T^{\theta_2}$.

签名算法:签名者随机选择 $r_m\in Z_p^*$,计算 $\boldsymbol{a}=H_4(\mathrm{ID})=(a_1,a_2,\cdots,a_l)$,$h=H_5(M\parallel g^{r_m})$,$W=w'\prod_{k=1}^{l}w_k^{a_k}$,那么签名

$$\sigma=(\sigma_1,\sigma_2,\sigma_3)=(D_1^h(\mathrm{SK}_{\mathrm{ID}})^hW^{r_m},D_2^h,g^{r_m})$$

验证算法:给出消息签名(M,σ,ID),找出对应的公钥 $\mathrm{PK}=(\mathrm{PK}_1,\mathrm{PK}_2)$,同时验证者计算 $U=u'\prod_{j=1}^{m}u_j^{v_j}$,$S=s'\prod_{j=1}^{n}s_j^{b_j}$,$T=t'\prod_{j=1}^{n}t_j^{c_j}$,$W=w'\prod_{k=1}^{l}w_k^{a_k}$,并计算下式是否成立,若成立则签名为真.

$$\hat{e}(g,\sigma_1)=\hat{e}(g_1,g_2)^h\hat{e}(\sigma_2,U)\hat{e}(\mathrm{PK}_1,g_2S)^h\hat{e}(\mathrm{PK}_2,T)^h\hat{e}(\sigma_3,W)$$

3.2 对 Hung 等方案的安全性分析

虽然 Hung 等人声称其无证书环签名方案具有强不可伪造性,但是通过分析可以发现,该方案对类型Ⅱ敌手 $A_{\mathrm{Ⅱ}}$ 可以伪造的.

3.2.1 自适应选择消息和身份的伪造攻击

假设敌手 $A_{\mathrm{Ⅱ}}$ 不可替换用户的公钥,$A_{\mathrm{Ⅱ}}$ 只要获得用户 ID 的一个消息/签名对,就可以冒充用户对任意消息进行签名($A_{\mathrm{Ⅱ}}$ 截获一个签名是很容易的,因为发送消息/签名的信道是公开的). 操作如下:

(1)系统运行系统初始化算法,$A_{\mathrm{Ⅱ}}$ 获得系统主密钥 g_2^{α}. 然后,$A_{\mathrm{Ⅱ}}$ 选择或者创造一个用户身份 ID^*,$A_{\mathrm{Ⅱ}}$ 选择 $r_v^*\in Z_p^*$,运行部分私钥生成算法,得到对应的部分私钥 $D_{\mathrm{ID}}^*=(D_1^*,D_2^*)=(g_2^{\alpha}(U^*)^{r_v^*},g^{r_v^*})$,并将 D_{ID}^*发送给一个合法用户 ID.

(2) 用户 ID 选择要签名的消息 M,得到签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$.

(3)$A_{\mathrm{Ⅱ}}$ 通过某些渠道获得这份签名(M,σ,ID),准备伪造消息 M^* 的签名 σ^*.

① $A_{\mathrm{Ⅱ}}$ 计算 $h=H_5(M\parallel\sigma_2)$,$h^*=H_5(M^*\parallel\sigma_2)$,存在 $x\in Z^*$,$h^*=xh$.

②$A_{\mathrm{Ⅱ}}$ 计算 $W=w'\prod_{k=1}^{l}w_k^{a_k}$,$W^*=w'\prod_{k=1}^{l}w_k^{a_k^*}$,存在 $y\in Z^*$,$(W^*)^y=W$.

$$\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)=((\sigma_1)^x(W^*)^{(xy)^{-1}},\sigma_2^x,\sigma_3)$$

(4)$A_{\mathrm{Ⅱ}}$ 赢得游戏Ⅱ的胜利,因为

$$\begin{aligned}\hat{e}(g,\sigma_1^*)&=\hat{e}(g,(\sigma_1)^x(W^*)^{(xy)^{-1}})\\&=\hat{e}(g,(D_1^h(\mathrm{SK}_{\mathrm{ID}})^h(W)^{r_m})^x(W^*)^{(xy)^{-1}})\\&=\hat{e}(g,D_1^{xh}(\mathrm{SK}_{\mathrm{ID}})^{xh}(W^*)^{xyr_m}(W^*)^{(xy)^{-1}})\\&=\hat{e}(g,D_1^{h^*}(\mathrm{SK}_{\mathrm{ID}})^{h^*}(W^*)^{r_m})\end{aligned}$$

$A_{\mathrm{Ⅱ}}$ 成功伪造了用户 ID^*,消息 M^* 的合法签名 σ^*. 虽然 Hung 等提供了算法对类型Ⅱ敌手的安全性证明,但是我们仍然发现了一种自适应选择消息和身份的伪造攻击,因此在 Hung 等的算法中必然存在漏洞. 仔细研究 Hung 等的算法以及证明,我们可以发现,在部分私钥生成算法之后的算法,都没有提及用户的身份信息 ID,这已经为伪造过程提供了一个条件.

3.2.2 消极 KGC 的公钥替换攻击

上面的攻击过程是假定 KGC 不能实施公钥替换攻击和用户的部分私钥对其他人保密为前提,假定 KGC 是消极的,KGC 将用户的部分私钥 D_{ID}泄露给了敌手 A. A 随机选择 $\theta_1^*,\theta_2^*\in Z_p$,计算公钥 $\mathrm{PK}^*=(\mathrm{PK}_1^*,\mathrm{PK}_2^*)=(g^{\theta_1^*},g^{\theta_2^*})$并替换用户的原始公钥 PK. 然后计算 $Q=g_2^{\theta_1^*}S^{\theta_1^*}T^{\theta_2^*}$. 选择消息 M^*,按照签名生成算法生成签名 $\sigma^*=(D_1^h(Q)^h(W)^{r_m},D_2^h,g^{r_m})$.

由上文可知,KGC 可以伪造用户的私钥,因此 KGC

安全级别只能达到 1 级,造成这种情况的原因是用户先生成公钥,再由公钥生成私钥.

4　一种改进的无证书签名方案

为了抵抗类型Ⅱ的敌手攻击,加强算法的安全性,本文对文献[16]的算法提出一种改进的算法.

初始化算法:给定安全参数 k,KGC 选择 p 阶循环群 G_1 和 G_2,双线性映射 $\hat{e}:G_1\times G_1\to G_2$. KGC 随机选择 $\alpha\in Z_p^*$ 和 $g_2\in G_1$,将 g_2^{α} 作为系统主密钥. 同时,KGC 选择 $g\in G_1$,$g_1=g^{\alpha}$,$H_1\sim H_5$ 是 5 个不同的哈希函数,$\boldsymbol{u}=(u_i)$,$\boldsymbol{s}=(s_i)$,$\boldsymbol{t}=(t_i)$,$\boldsymbol{w}=(w_i)$是长度为 m、n、n、l 的向量,KGC 公开系统参数 params = $\{G_1,G_2,e,g,g_1,g_2,H_1\sim H_5,\boldsymbol{u},\boldsymbol{s},\boldsymbol{t},\boldsymbol{w}\}$.

用户公钥产生算法:用户 ID 随机选择 $\theta_1,\theta_2\in Z_p^*$,计算公钥 $\mathrm{PK}=(\mathrm{PK}_1,\mathrm{PK}_2)=(g^{\theta_1},g^{\theta_2})$.

部分私钥产生算法:给定用户的身份 ID,计算 $\boldsymbol{v}=H_1(\mathrm{ID},\mathrm{PK}_1)=(v_1,v_2,\cdots,v_m)$,KGC 随机选择 $r_v\in Z_p^*$,计算部分私钥 $D_{\mathrm{ID}}=(D_1,D_2)=(g_2U^{r_v},g^{r_v})$,其中,$U=\prod_{j=1}^{m}u_j^{v_j}$.

用户私钥产生算法:用户接到 KGC 发送的部分私钥,计算 $\boldsymbol{v}=H_1(\mathrm{ID},\mathrm{PK}_1)$,$U=\prod_{j=1}^{m}u_j^{v_j}$,验证 $\hat{e}(g_1,D_1)=\hat{e}(g_1,g_2)\,\hat{e}(D_2,U)$是否成立,成立则接受部分私钥,用户的私钥为 $\mathrm{SK}=\{(\theta_1,\theta_2),(D_1,D_2)\}$;不成立,则返回部分私钥生成算法.

签名算法:用户随机选择 $r_m\in Z_p^*$,计算 $\boldsymbol{a}=H_4(\mathrm{ID})=(a_1,a_2,\cdots,a_l)$,$W=\prod_{k=1}^{l}w_k^{a_k}$,$h=H_5(M\parallel g^{r_m}\parallel\mathrm{ID}\parallel\mathrm{PK}_1\parallel\mathrm{PK}_2)$,$S=\prod_{j=1}^{n}s_j^{b_j}$,$\boldsymbol{b}=H_2(M\parallel g^{r_m}\parallel\mathrm{PK}_1\parallel\mathrm{PK}_2)=(b_i)$,$T=\prod_{j=1}^{n}t_j^{c_j}$,$\boldsymbol{c}=H_3(\mathrm{ID}\parallel\mathrm{PK}_1\parallel\mathrm{PK}_2)=(c_i)$,那么签名

$$\sigma=(\sigma_1,\sigma_2,\sigma_3)=(D_1^h(S)^{\theta_1 h}T^{\theta_2}W^{r_m},D_2^h,g^{r_m})$$

验证算法:给出消息签名(M,σ,ID),找出对应的公钥 $\mathrm{PK}=(\mathrm{PK}_1,\mathrm{PK}_2)$,同时验证者计算 $U=\prod_{j=1}^{m}u_j^{v_j}$,$S=\prod_{j=1}^{n}s_j^{b_j}$,$T=\prod_{j=1}^{n}t_j^{c_j}$,$W=\prod_{k=1}^{l}w_k^{a_k}$,并计算下式是否成立,若成立则签名为真.

$$\hat{e}(g,\sigma_1)=\hat{e}(g_1,g_2)^h\hat{e}(\sigma_2,U)\hat{e}(\mathrm{PK}_1,S)^h\hat{e}(\mathrm{PK}_2,T)\hat{e}(\sigma_3,W)$$

可以验证,改进的无证书签名方案是正确的. 事实上,

$$\begin{aligned}\hat{e}(g,\sigma_1)&=\hat{e}(g,D_1^h(S)^{\theta_1 h}T^{\theta_2}(W)^{r_m})\\&=\hat{e}(g,(g_2^{\alpha}U^{r_v})^h)\hat{e}(g,(S)^{h\theta_1})\hat{e}(g,(T)^{\theta_2})\hat{e}(g,(W)^{r_m})\\&=\hat{e}(g^{\alpha},g_2)^h\hat{e}(g^{hr_v},U)\hat{e}(g^{\theta_1},S)^h\hat{e}(g^{\theta_2},T)\hat{e}(g^{r_m},W)\\&=\hat{e}(g_1,g_2)^h\hat{e}(\sigma_2,U)\hat{e}(\mathrm{PK}_1,S)^h\hat{e}(\mathrm{PK}_2,T)\hat{e}(\sigma_3,W)\end{aligned}$$

5　结论

本文对 Hung 等在 2016 年提出的强不可伪造性无证书签名算法进行了安全性分析,证明其对第二类敌手的自适应选择消息和身份的伪造攻击以及消极 KGC 的公钥替换攻击都是不安全的. 针对 Hung 等算法的安全缺陷,提出一种改进的无证书签名方案,并证明方案正确.

参考文献

[1] Zhang Y,Jiguo L I,Wang Z,et al. A new efficient certificate-based signature scheme[J]. Chinese Journal of Electronics,2015,24(4):776 – 782.

[2] Wu T Y,Tsai T T,Tseng Y M. A revocable ID-based signcryption scheme[J]. Journal of Information Hiding & Multimedia Signal Processing,2011,3(3):240 – 251.

[3] Shamir A. Identity-based cryptosystems and signature schemes [A]. Advances in Cryptology[C]. Berlin: Springer-Verlag, 1984. 47 – 53.

[4] Chen Y C,Tso R,Susilo W,et al. Certificateless Signatures: Structural Extensions of Security Models and New Provably Secure Schemes[EB/OL]. http://eprint. iacr. org/2013/193. pdf,2013-06-28.

[5] Tso R,Huang X,Susilo W. Strongly secure certificateless short signatures[J]. Journal of Systems & Software,2012, 85(6):1409 – 1417.

[6] Huang X,Susilo W,Mu Y,et al. On the security of certificateless signature schemes from asiacrypt 2003[A]. Cryptology and Network Security[C]. Berlin: Springer-Verlag, 2005. 13 – 25.

[7] Choi K Y,Park J H,Dong H L. A new provably secure certificateless short signature scheme[J]. Computers & Mathematics with Applications,2011,61(7):1760 – 1768.

[8] Chen Y C,Tso R,Horng G. Security analysis of choi et al. 's certificateless short signature scheme[J]. Journal of Information Hiding & Multimedia Signal Processing,2013,4 (3):147 – 154.

[9] Xiong H,Guan Z,Chen Z,et al. An efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences,2013,219(10):225 – 235.

[10] He D,Tian M,Chen J. Insecurity of an efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2014, 268 (2): 458 – 462.

[11] Zhang F,Shen L,Wu G. Notes on the security of certificateless aggregate signature schemes[J]. Information Sciences,2014,287:32 – 37.

[12] Yu Y,Mu Y,Wang G,et al. Improved certificateless signature scheme provably secure in the standard model[J]. Iet Information Security,2012,6(2):102 – 110.

[13] Yuan Y,Wang C. Certificateless signature scheme with security enhanced in the standard model[J]. Information Processing Letters,2014,114(9):492 – 499.

[14] Chen Y C, Tso R, Horng G, et al. Strongly secure certificateless signature: Cryptanalysis and improvement of two schemes[J]. Journal of Information Science & Engineering, 2015, 31(1): 297 – 314.

[15] Fan C I, Hsu R H, Ho P H. Truly Non-repudiation certificateless short signature scheme from bilinear pairings[J]. Journal of Information Science & Engineering, 2011, 27(27): 969 – 982.

[16] Hung Y H, Huang S S, Tseng Y M, et al. Certificateless signature with strong unforgeability in the standard model [J]. Informatica, 2015, 26(4): 663 – 684.

作者简介

吴 涛 男. 1984 年 7 月出生, 四川省达州市人. 2010 年于西南交通大学信息科学与技术学院取得密码学硕士学位. 2013 年进入北京邮电大学信息与通信工程学院, 现攻读博士学位, 主要从事无线与移动通信技术, 保密传输技术方面有关研究.

E-mail: wootao@ foxmail. com

景晓军 男. 现为北京邮电大学信息与通信工程学院教授, 博士生导师. 1999 年获国防科技大学信息与通信系统专业博士学位, 主要从事信息融合、图像处理、模式识别方面有关研究.

E-mail: jxiaojun@ bupt. edu. cn