软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(5):1125−1131 [doi: 10.13328/j.cnki.jos.004526]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

安全高效基于身份签名方案的密码学分析*

禹 勇[1,2], 倪剑兵[1], 许春香[1], 牛 磊[1]

[1](电子科技大学 计算机科学与工程学院,四川 成都 611731)

[2](School of Computer Science and Software Engineering, University of Wollongong, Australia)

通讯作者: 禹勇, E-mail: yyucd2012@gmail.com

摘 要: 基于身份的数字签名方案最显著的特点是,只需要签名人的身份信息而无需签名人的证书来验证签名的有效性,这极大地简化了密钥管理.2006 年,Paterson 和 Schuldt 构造了标准模型下可证明安全的基于身份的数字签名方案,但计算效率不高.谷科等人提出了新型的改进方案来提高效率,并声称新方案在标准模型下可证明安全且比同类方案更高效.然而,新方案并不具备不可伪造性.给出了两种具体的攻击:敌手可以伪造用户的密钥或者敌手可以直接伪造任何消息的签名.进一步指出安全性证明中的缺陷,即,敌手的 view 与安全模拟成功的事件不独立.

关键词: 数字签名;基于身份签名;标准模型;密码学分析;可证明安全

中图法分类号: TP309

中文引用格式: 禹勇,倪剑兵,许春香,牛磊.安全高效基于身份签名方案的密码学分析.软件学报,2014,25(5):1125−1131. http://www.jos.org.cn/1000-9825/4526.htm

英文引用格式: Yu Y, Ni JB, Xu CX, Niu L. Cryptanalysis of a secure and efficient identity-based signature scheme. Ruan Jian Xue Bao/Journal of Software, 2014,25(5):1125−1131 (in Chinese). http://www.jos.org.cn/1000-9825/4526.htm

Cryptanalysis of a Secure and Efficient Identity-Based Signature Scheme

YU Yong[1,2], NI Jian-Bing[1], XU Chun-Xiang[1], NIU Lei[1]

[1](School of Computer Science and Engineering, University of Electronics Science and Technology of China, Chengdu 611731, China)

2(School of Computer Science and Software Engineering, University of Wollongong, Australia)

Corresponding author: YU Yong, E-mail: yyucd2012@gmail.com

Abstract: The distinguishing characteristic of identity-based signatures is that only the identity with no certificate of a signer is involved in the verification of a signature, which simplifies the key management procedures dramatically. A novel identity-based signature scheme that can be proven secure in the standard model was given by Paterson and Schuldt in 2006. Unfortunately, the scheme is not efficient in computation. An improvement due to Gu, *et al*. was proposed recently to improve the computational efficiency, and it was claimed as being provably secure in the standard model and more efficient than the known schemes in the same flavor. However, this paper shows that the new scheme by Gu, *et al*. is insecure by demonstrating two concrete attacks in which an adversary can not only forge the private key of an identity but also forge signatures on arbitrary message. The study also identifies a flaw in their security proofs, i.e., the view of the adversary in the security reduction is not independent of the event that the simulation succeeds.

Key words: digital signature; identity-based signature; standard model; cryptanalysis; provable security

为了简化密钥管理,1984 年,Shamir 提出了基于身份的密码体制[1],将标示用户身份的唯一信息如电话号码、E-mail 地址等作为用户的公钥,用户的私钥由密钥生成中心利用用户的身份和自身的主密钥生成.基于身份的密码体制具有以下 3 个特点:用户的公钥可以根据用户身份得到;不需要 PKI 基础设施;加密消息或者签名验证只需要接收人或签名人的身份信息和系统参数.因此,基于身份的密码体制减轻了用户对公钥证书的依赖,解

* 基金项目: 国家自然科学基金(61003232, 61370203, 61250110543); 教育部博士点基金(20100185120012)
收稿时间: 2012-10-28; 定稿时间: 2013-11-26

决了公钥证书的生成、验证、存储和吊销问题.基于整数分解问题,Shamir 提出了第一个基于身份的签名方案[1].2001 年,Boneh 和 Franklin 利用双线性对构造了第一个实用的基于身份的加密方案[2],此后,基于身份的密码体制[3−9]得到了快速的发展,成为 10 年来密码学研究领域重要的研究方向.

在安全性方面,大部分基于身份的密码方案[3−5]都只能在随机预言机模型(random oracle model)[10]下证明是安全的.随机预言机模型是 Bellare 等人于 1993 年提出的用于安全性证明的理想模型,此模型在理想条件下对敌手的能力进行模拟,把 Hash 函数看作随机函数,对于敌手的每次询问,挑战者给出一个随机应答.但是在特定的数字签名方案中,因为使用的 Hash 函数是具体的,对于每次 Hash 询问的应答是特定 Hash 函数的真实输出,此输出一定不是随机的,这就可能导致方案的不安全.1998 年,Canetti 等人[11]特意构造了一些密码方案,虽然在随机预言机下可证明是安全的,但却不安全.因此,设计在标准模型下可证明安全的密码方案更有意义和价值.

2005 年,Waters[12]提出了标准模型下可证明安全的基于身份的加密方案,并利用其密钥提取算法设计出一个标准模型下安全的签名方案(记为 Waters 签名).2006 年,Paterson 等人[13]基于 Waters 签名[12]构造了标准模型下安全的基于身份签名方案(记为 PS 签名方案),具有签名长度短、不可伪造性规约到计算性 Diffie- Hellman 问题(CDH)等优势,但不足之处在于需要多次群 G 上的乘法运算,计算效率不高.针对此问题,谷科等人[14]指出:可以通过转变 PS 方案中的群元素乘法运算为整数加法运算的方法提高计算效率,并给出了一个具体的构造.他们声称:在标准模型下,可以证明新方案的安全性归约到 CDH 问题,并且比同类方案高效.

然而我们发现,文献[14]提出的方案无法达到数字签名的最基本性质——不可伪造性.给出了两种具体攻击:在第 1 种攻击中,敌手可以伪造任意用户的私钥,利用此私钥对任意消息签名;在第 2 类攻击中,敌手可以直接伪造目标用户对任意消息的签名.进一步指出文献[14]中安全性证明的缺陷:敌手的 view 与安全模拟成功的事件不独立.

1 谷等人方案及安全性分析

本节首先回顾文献[14]提出的改进的签名方案,然后在基于身份签名的安全模型中对方案进行安全性分析.

1.1 谷等人方案

文献[14]提出的基于身份的数字签名方案包含以下几种算法:

(1) 系统设置(setup)

PKG 选择两个 q 阶循环群 G_1,G_2,q 为素数,g 是 G_1 的生成元,$e:G_1\times G_1\to G_2$ 表示双线性对.H_u 和 H_m 是两个安全的 Hash 函数: $H_u:\{0,1\}^*\to\{0,1\}^{n_u}$ 和 $H_m:\{0,1\}^*\to\{0,1\}^{n_m}$, 分别用于将身份和消息映射成 n_u,n_m 长度的比特串.PKG 随机选择 $u',m'\in Z_q,n_u$ 维的向量 $\vec{U}=(u_i)$, n_m 维的向量 $\vec{M}=(m_i)$, 其中,$u_i\in Z_q,m_i\in Z_q$.随机选择 $x\in Z_q,g_2\in G_1$,计算 $g_1=g^x$.PKG 的系统参数 $params=(G_1,G_2,e,g,g_1,g_2,u',\vec{U},m',\vec{M},H_u,H_m)$, 系统主密钥为 g_2^x.

(2) 用户密钥生成(KeyGen)

设用户身份 u 为一个长度为 n_u 的比特串,$V\subseteq\{1,\ldots,n_u\}$表示 u 中比特值为 1 的位置 i 的集合.PKG 随机选择 $r\in Z_q$,计算用户 u 的私钥:

$$d_u=(d_1,d_2)=\left(g_2^x\cdot(g_2^x)^{r\left(u'+\sum_{i\in V}u_i\right)},e(g_2,g_1)^r\right),$$

并通过安全信道将 d_u 发送给用户.用户得到私钥 d_u 后,先通过以下验证式对密钥进行检验:

$$e(d_1,g)=e(g_2,g_1)\cdot d_2^{\left(u'+\sum_{i\in V}u_i\right)}.$$

如果等式成立,则证明密钥有效;否则,要求 PKG 重新生成密钥.

(3) 签名(sign)

密钥通过验证后,用户就可以利用它来签名消息.令 m 为长度为 n_m 的消息比特串,$W\subseteq\{1,\ldots,n_m\}$表示 m 中比特值为 1 的位置 j 的集合.用户随机选择 $s\in Z_q$,计算 m 的签名:

$$\sigma=(Q_1,Q_2,Q_3)=\left(d_1\cdot(g_2^s)^{m'+\sum_{j\in W}m_j},e(g_2,g)^s,d_2\right)=\left(g_2^x\cdot(g_2^x)^{r\left(u'+\sum_{i\in I'}u_i\right)}\cdot(g_2^s)^{\left(m+\sum_{j\in W}m_j\right)},e(g_2,g)^s,e(g_2,g_1)^r\right).$$

(4) 验证(verify)

收到消息、签名对(m,σ)后,验证人检验以下验证式是否成立:

$$e(Q_1,g)=e(g_2,g_1)\cdot Q_2^{m'+\sum_{j\in W}m_j}\cdot Q_3^{u'+\sum_{i\in I'}u_i}.$$

若等式成立,则签名有效;否则,签名无效.

1.2 谷科等人的方案的安全性分析

本节首先回顾基于身份数字签名的安全模型[13,15],然后,在该模型下分析文献[14]中提出的签名方案的安全性.

1.2.1 基于身份签名的安全模型

基于身份数字签名方案的不可伪造性模型刻画了以下安全行为和目标:即使敌手具备了很强的攻击能力,即对任意身份进行密钥提取询问和对任意消息进行签名询问,它能够伪造目标身份 u^*对目标消息 m^*的有效签名的概率是可忽略的.攻击模型通过敌手和挑战者之间的如下游戏来定义:

(1) 系统设置

挑战者运行系统设置算法得到系统参数和主密钥;敌手得到系统参数,但不能获得主密钥,挑战者秘密保存主密钥.

(2) 询问

敌手向挑战者自适应地进行一系列询问,询问方式如下:

1) 密钥生成询问:敌手选择任意选择身份 u 进行密钥生成询问;挑战者通过运行密钥生成算法计算相应私钥 d_u,并将 d_u 返回给敌手.
2) 签名询问:敌手任意选择身份 u 和消息 m 进行签名询问;挑战者首先通过密钥生成算法计算身份 u 的私钥 d_u,然后运行签名算法计算消息 m 的签名σ,并将签名σ返回给敌手.

(3) 伪造

敌手输出身份 u^*对消息 m^*的签名σ^*.若以下 3 个条件成立,则攻击成功:

1) 敌手未对身份 u^*进行密钥生成询问;
2) 敌手未对(u^*,m^*)进行签名询问;
3) σ^*是身份 u^*对消息 m^*的有效签名.

定义 1. 如果敌手 A 经过最多 q_E 次密钥提取询问和 q_S 次签名询问,至少在 t 时间内以不小于ε的概率赢得上诉游戏,则敌手 A 称为基于身份签名的(ε,t,q_E,q_S)-伪造者;如果基于身份签名方案中不存在(ε,t,q_E,q_S)-伪造者,则称方案是(ε,t,q_E,q_S)-安全的.

1.2.2 两种具体的攻击

虽然文献[14]在标准模型下证明了改进方案的不可伪造性可以归约到 CDH 假设,然而本节对新方案进行安全性分析,给出两种具体的攻击,证明其不安全,并指出文献[14]安全性证明中的缺陷.

- 第 1 种攻击

在第 1 种攻击中,敌手 A 能够伪造任意用户的私钥,然后利用该私钥计算任何消息的签名.敌手 A 与挑战者进行如下游戏:

(1) 系统生成

挑战者运行系统设置算法得到系统参数 *params* 和主密钥,挑战者秘密保存主密钥,将公开参数 *params*=$(G_1,G_2,e,g,g_1,g_2,u',\vec{U},m',\vec{M},H_u,H_m)$发送给敌手 *A*.

(2) 询问

敌手 *A* 在这一阶段不进行任何询问.

(3) 伪造

目标用户的身份记为 $u^*,V^*\subseteq\{1,\ldots,n_u\}$表示 u^*中比特值为 1 的位置 i 的集合,敌手要伪造签名的目标消息为 $m^*,W^*\subseteq\{1,\ldots,n_m\}$表示 m^*中比特值为 1 的位置 j 的集合.敌手 *A* 通过以下步骤伪造 u^*的私钥,并进一步计算消息 m^*的签名:

① 随机选择 $d_1^*\in G_1$;

② 利用扩展的欧几里得算法计算 $t=\left(u'+\sum_{i\in V^*}u_i\right)^{-1} \bmod q$;

③ 计算 $d_2^*=\left(\frac{e(d_1^*,g)}{e(g_2,g_1)}\right)^t \bmod q$;

④ 随机选择 $s^*\in Z_q$,利用伪造的目标用户 u^*的私钥 $d_u^*=(d_1^*,d_2^*)$ 计算目标消息 m^*的签名:

$$\sigma^*=(Q_1^*,Q_2^*,Q_3^*)=\left(d_1^*\cdot(g_2^{s^*})^{\left(m'+\sum_{j\in W^*}m_j\right)},e(g_2,g)^{s^*},d_2^*\right).$$

在敌手 *A* 伪造中,容易验证 (d_1^*,d_2^*) 是目标身份 u^*有效密钥,因为

$$\begin{aligned}e(g_2,g_1)\cdot(d_2^*)^{\left(u'+\sum_{i\in V^*}u_i\right)}&=e(g_2,g_1)\cdot\left(\left(\frac{e(d_1^*,g)}{e(g_2,g_1)}\right)^t\right)^{\left(u'+\sum_{i\in V^*}u_i\right)}\\&=e(g_2,g_1)\cdot\left(\left(\frac{e(d_1^*,g)}{e(g_2,g_1)}\right)^{\left(u'+\sum_{i\in V^*}u_i\right)^{-1}}\right)^{\left(u'+\sum_{i\in V^*}u_i\right)}\\&=e(d_1^*,g).\end{aligned}$$

计算得到的 $\sigma^*=(Q_1^*,Q_2^*,Q_3^*)$ 是目标用户 u^*对目标消息 m^*的一个有效签名,因为

$$\begin{aligned}e(g_2,g_1)\cdot(Q_2^*)^{\left(m'+\sum_{j\in W^*}m_j\right)}\cdot(Q_3^*)^{\left(u'+\sum_{i\in V^*}u_i\right)}&=e(g_2,g_1)\cdot(e(g_2,g)^{s^*})^{\left(m'+\sum_{j\in W^*}m_j\right)}\cdot(d_2^*)^{\left(u'+\sum_{i\in V^*}u_i\right)}\\&=(e(g_2,g)^{s^*})^{\left(m'+\sum_{j\in W^*}m_j\right)}\cdot e(d_1^*,g)\\&=e((g_2^{s^*})^{\left(m'+\sum_{j\in W^*}m_j\right)},g)\cdot e(d_1^*,g)\\&=e(Q_1^*,g).\end{aligned}$$

- 第 2 种攻击

在第 2 种攻击中,敌手 *B* 可以直接伪造目标用户对任意消息的签名.敌手 *B* 与挑战者进行如下游戏:

(1) 系统生成

挑战者运行系统设置算法得到系统参数 *params* 和主密钥,挑战者秘密保存主密钥,将公开参数 *params*=$(G_1,G_2,e,g,g_1,g_2,u',\vec{U},m',\vec{M},H_u,H_m)$发送给敌手 *B*.

(2) 询问

敌手 B 在这一阶段不进行任何询问.

(3) 伪造

目标用户的身份记为 $u^*,V^*\subseteq\{1,\ldots,n_u\}$表示 u^*中比特值为 1 的位置 i 的集合;敌手要伪造的目标消息为 m^*, $W^*\subseteq\{1,\ldots,n_m\}$表示 m^*中比特值为 1 的位置 j 的集合.敌手 B 通过以下步骤直接伪造目标用户 u^*对目标消息 m^*的签名:

① 随机选择 $Q_1^*\in G_1,Q_2^*\in G_2$;

② 利用扩展的欧几里德算法计算 $t=\left(u'+\sum_{i\in V^*}u_i\right)^{-1} \bmod q$;

③ 计算 $Q_3^*=\left(\dfrac{e(Q_1^*,g)}{e(g_2,g_1)\cdot(Q_2^*)^{m'+\sum_{j\in W^*}m_j}}\right)^t \bmod q$;

④ $\sigma^*=(Q_1^*,Q_2^*,Q_3^*)$ 为敌手 B 伪造的目标用户 u^*对目标消息 m^*的签名.

计算得到的 $\sigma^*=(Q_1^*,Q_2^*,Q_3^*)$ 是目标用户 u^*对目标消息 m^*的一个有效签名,因为

$$e(g_2,g_1)\cdot(Q_2^*)^{m'+\sum_{j\in W^*}m_j}\cdot(Q_3^*)^{u'+\sum_{i\in V^*}u_i}=e(g_2,g_1)\cdot(Q_2^*)^{m'+\sum_{j\in W^*}m_j}\cdot\left(\left(\frac{e(Q_1^*,g)}{e(g_2,g_1)\cdot(Q_2^*)^{m'+\sum_{j\in W^*}m_j}}\right)^t\right)^{u'+\sum_{i\in V^*}u_i}$$

$$=e(g_2,g_1)\cdot(Q_2^*)^{m'+\sum_{j\in W^*}m_j}\cdot\left(\frac{e(Q_1^*,g)}{e(g_2,g_1)\cdot(Q_2^*)^{m'+\sum_{j\in W^*}m_j}}\right)$$

$$=e(Q_1^*,g).$$

虽然文献[14]在标准模型下对该签名方案的不可伪造性给出了安全性证明,但是我们发现,其安全性证明过程存在缺陷,正是此缺陷导致上述伪造攻击的存在.在文献[14]的安全性证明中,挑战者令 $l_u=2(q_e+q_s),l_m=2q_s$, 随机选择 $k_u\in Z_{l_u},k_m\in Z_{l_m}$, 且 $0\leqslant k_u\leqslant n_u,0\leqslant k_m\leqslant n_m$,对于给定的 q_e,q_s,n_u,n_m,假设有 $l_u(n_u+1)<q,l_m(n_m+1)<q$;随机选择 $x'\in Z_{l_u}$, 长度为 n_u的向量 $\vec{X}=(x_i)$, 其中, $x_i\in Z_{l_u}$, 随机选择 $y'\in Z_{l_m}$, 长度为 n_m的向量 $\vec{Y}=(y_j)$, 其中, $y_j\in Z_{l_m}$;定义两个函数: $F(u)=x'+\sum_{i\in V}x_i-l_u\cdot k_u,K(m)=y'+\sum_{j\in W}y_j-l_m\cdot k_m$. 挑战者构造:

$$u'=x'-l_u\cdot k_u,u_i=x_i(1\leqslant i\leqslant n_u),\ m'=y'-l_m\cdot k_m,\ m_j=y_j(1\leqslant j\leqslant n_m).$$

在这种设置下得到 $u'+\sum_{i\in V}u_i=F(u),m'+\sum_{j\in W}m_j=K(m)$. 完整的安全性证明见文献[14].

最后,如果在密钥生成询问、签名询问和签名伪造这 3 个过程中,挑战者都不会终止,即以下 3 个条件同时满足,则挑战者能成功解决 CDH 问题的一个实例:

(1) 密钥生成询问阶段,对所有的身份 $u_i,F(u_i)\neq 0 \bmod l_u$;

(2) 签名询问阶段,对所有的消息 $m_i,K(m_i)\neq 0 \bmod l_m$;

(3) 签名伪造阶段,对目标身份 u^*和目标消息 $m^*,F(u^*)=0 \bmod q$ 且 $K(m^*)=0 \bmod q$.

然而容易看出,敌手在安全性证明中的 view 与挑战者解决 CDH 问题成功的条件是不独立的.具体来说,挑战者能否解决 CDH 问题是由函数 $F(u)$和 $K(m)$的值决定的,而 u',u_i,m',m_j 是系统参数的一部分,对于已知的身份 u 和消息 m,任何人都可以计算 $F(u)$和 $K(m)$.故而在伪造阶段,在敌手输出目标用户 u^*对目标消息 m^*的伪造签名 σ^*时,可以先计算 $F(u^*)$和 $K(m^*)$的值,如果 $F(u^*)=0 \bmod q$ 且 $K(m^*)=0 \bmod q$ 成立,则敌手不返回σ^*;否则,敌手将签名伪造σ^*返回给挑战者.因此,敌手返回给挑战者的伪造签名对应的目标身份 u^*和目标消息 m^*总能使 $F(u^*)\neq 0 \bmod q$ 或 $K(m^*)\neq 0 \bmod q$ 成立.条件(3)的不成立,使挑战者无法成功解决 CDH 问题.所以,该签名方案的不可伪造性无法归约到 CDH 问题.

2 结束语

文献[14]在 PS 签名方案[13]的基础上提出了改进的基于身份签名方案,并在标准模型下将新方案的不可伪造性规约到 CDH 假设.然而,本文对改进的方案[14]进行了安全性分析,发现其安全性证明过程存在缺陷,此缺陷导致签名方案容易遭受两种具体攻击.如何构造计算效率高、系统参数短、可证明安全(标准模型下)的基于身份签名,仍然是密码学研究中的一个重要问题.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, Chaum D, des. Advances in Cryptology—CRYPTO'84. LNCS 196, Berlin: Springer-Verlag, 1985. 47−53. [doi: 10.1007/3-540-39568-7_5]

[2] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Advances in Cryptology—CRYPTO 2001. LNCS 2139, Berlin: Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[3] Paterson KG. ID-Based signatures from pairing on elliptic curves. Electrics Letters, 2002,38(8):1025−1026. [doi: 10.1049/el:20020682]

[4] Cha JC, Cheon JH. An identity-based signature from gap Diffie-Hellman groups. In: Desmedt YG, ed. Proc. of the Public Key Cryptography—PKC 2003. LNCS 2567, Berlin: Springer-Verlag, 2003. 18−30. [doi: 10.1007/3-540-36288-6_2]

[5] Xun Y. An identity-based signature scheme from the Weil pairing. IEEE Communications Letters, 2003,7(2):76−78. [doi: 10.1109/LCOMM.2002.808397]

[6] Gu CX, Zhu YF, Pan XY. Forking lemma and the security proofs for a class of ID-based signatures. Ruan Jian Xue Bao/Journal of Software, 2007,18(4):1007−1024 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1007.htm [doi: 10.1360/jos181007]

[7] Ma XL, Gu LZ, Cui W, Yang YX, Hu ZX. ID-Based transitive signature schemes without random oracle. Journal on Communications, 2010,31(5):37−43 (in Chinese with English abstract).

[8] Gu K, Jia WJ, Wang SC, Shi LW. Proxy signature in the standard model: Constructing security model and proving security. Ruan Jian Xue Bao/Journal of Software, 2012,23(9):2416−2429 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4246.htm [doi: 10.3724/SPJ.1001.2012.04246]

[9] Lu L, Hu L. Multi-Recipient public key encryption scheme based on Weil pairing. Ruan Jian Xue Bao/Journal of Software, 2008, 19(8):2159−2166 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/2159.htm [doi: 10.3724/SP.J.1001.2008.02159]

[10] Bellare M, Rogoway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Denning D, Pyle R, Ganesan R, Sandhu R, Ashby V, eds. Proc. of the 1st Conf. on Computer and Communications Security. ACM Press, 1993. 62−73. [doi: 10.1145/168588.168596]

[11] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. Journal of the ACM, 2004,51(4):557−594. [doi: 10.1145/1008731.1008734]

[12] Waters B. Efficient identity-based encryption without random oracles. In: Cramer R, ed. Advances in Cryptology of EUROCRYPT 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 114−127. [doi: 10.1007/11426639_7]

[13] Paterson KG, Schuldt J. Efficient identity-based signature secure in the standard model. In: Batten L, Safavi-Nain R, eds. Proc. of the ACISP 2006. LNCS 4058, Berlin: Springer-Verlag, 2006. 207−222. [doi: 10.1007/11780656_18]

[14] Gu K, Jia WJ, Jiang CL. Efficient and secure identity-based signature scheme. Ruan Jian Xue Bao/Journal of Software, 2011,22(6):1350−1360 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4002.htm [doi: 10.3724/SP.J.1001.2011.04002]

[15] Li JG, Jiang PJ. An efficient and provably secure identity-based signature scheme in the standard model. Chinese Journal of Computers, 2009,32(11):2130−2136 (in Chinese with English abstract). [doi: 10.3724%2fSP.J.1016.2009.02130]

附中文参考文献:

[6] 顾纯祥,祝跃飞,潘晓豫.Forking 引理与一类基于身份签名体制的安全性证明.软件学报,2007,18(4):1007−1024. http://www.jos.org.cn/1000-9825/18/1007.htm [doi: 10.1360/jos181007]

[7] 马小龙,古利泽,崔巍,杨义先,胡正名.标准模型下基于身份的传递签名.通信学报,2010,31(5):37−43.

[8] 谷科,贾维嘉,王四春,石良武.标准模型下的代理签名:构造模型与证明安全性.软件学报,2012,23(9):2416−2429. http://www.jos.org.cn/1000-9825/4246.htm [doi: 10.3724/SPJ.1001.2012.04246]

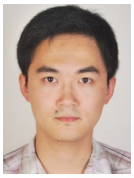
[9] 鲁力,胡磊.基于 Weil 对的多接收者公钥加密方案.软件学报,2008,19(8):2159−2166. http://www.jos.org.cn/1000-9825/19/2159.htm [doi: 10.3724/SP.J.1001.2008.02159]

[14] 谷科,贾维嘉,姜春林.高效安全的基于身份的签名方案.软件学报,2011,22(6):1350−1360. http://www.jos.org.cn/1000-9825/4002.htm [doi: 10.3724/SP.J.1001.2011.04002]

[15] 李继国,姜平进.标准模型下可证安全的基于身份的高效签名方案.计算机学报,2009,32(11):2130−2136. [doi: 10.3724%2fSP.J.1016.2009.02130]

禹勇(1980－),男,山东泰安人,博士,副教授,主要研究领域为公钥密码学.
E-mail: yyucd2012@gmail.com

许春香(1965－),女,博士,教授,博士生导师,主要研究领域为信息安全.
E-mail: chxxu@uestc.edu.cn



倪剑兵(1988－),男,硕士生,主要研究领域为公钥密码学.
E-mail: nimengze@gmail.com

牛磊(1989－),男,硕士生,主要研究领域为公钥密码学.
E-mail: uestc.nl@163.com