软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(6):1350−1360 [doi: 10.3724/SP.J.1001.2011.04002]

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

高效安全的基于身份的签名方案*

谷 科[1+], 贾维嘉[1,2], 姜春林[1]

[1](中南大学 信息科学与工程学院,湖南 长沙 410083)

[2](香港城市大学 计算机科学系,香港)

Efficient and Secure Identity-Based Signature Scheme

GU Ke[1+], JIA Wei-Jia[1,2], JIANG Chun-Ling[1]

[1](School of Information Science and Engineering, Central South University, Changsha 410083, China)

[2](Department of Computer Science, City University of Hong Kong, Hong Kong, China)

+ Corresponding author: E-mail: gk4572@163.com

Gu K, Jia WJ, Jiang CL. Efficient and secure identity-based signature scheme. *Journal of Software*, 2011, 22(6):1350−1360. http://www.jos.org.cn/1000-9825/4002.htm

Abstract: Paterson, *et al*. have studied identity-based signature scheme based on Waters' signature scheme in a standard model, which has proved to have a security reduction to CDHP assumption, but has low computational efficiency. Although Li-Jiang, *et al*. improves Paterson's scheme, Li-Jiang's scheme has low online computational efficiency. This paper shows a more efficient identity-based signature scheme based on Paterson's scheme in standard model. The new scheme improves computational efficiency by changing multiplicative operation to addition operation and pre-computing bilinear pairing operation. The scheme comparing with Paterson's scheme decreases the number of multiplicative operation and the number of bilinear pairing operation of verifier. The scheme comparing with Li-Jiang's scheme decreases the on-line computation of signer and verifier and the output parameters of system. Also, the scheme has proved to have a security reduction to CDHP assumption and the existential unforgeability under an adaptive chosen message attack. Comparing with other identity-based signature schemes in standard model, the new scheme is more efficient.

Key words: standard model; signature; CDHP; provable security; computational efficiency

摘 要: Paterson 等人在 Waters 签名方案的基础上提出的基于身份的签名方案,虽然在标准模型下被证明能够归约于 CDH 问题假定,但方案的计算效率不高.此后,李-姜等人对 Paterson 方案虽然进行了改进,但方案的在线计算效率不高.在 Paterson 方案的基础上,提出了一种在标准模型下更高效的基于身份的签名方案.该方案采用转变原方案中的群元素乘法运算为整数加法运算的方法来提高计算效率,而且利用预先计算双线性对的方法来改进方案的在线计算性能.与 Paterson 方案相比,消除了多次乘法运算,减少了验证方的双线性对计算次数;与李-姜方案相比,减少了签名方和验证方的在线运算量以及系统输出参数;同时,该方案在标准模型下被证明具有在自适应选择消息攻击

* 基金项目: 香港城市大学应用研究项目基金(9681001); 香港城市大学战略研究发展基金(7008110); 深港创新圈基金(ZYB200907080078A)

收稿时间: 2010-10-26; 定稿时间: 2011-02-15

CNKI 网络优先出版: 2011-03-24 15:08, http://www.cnki.net/kcms/detail/11.2560.TP.20110324.1508.002.html

下存在不可伪造性,其安全性能够归约于 CDH 问题假定.与现有的标准模型下基于身份的签名方案相比,该方案的计算效率更高.

关键词: 标准模型;签名;CDH 问题;可证安全;计算性能

中图法分类号: TP309 **文献标识码**: A

为了提高密钥管理,Shamir 于 1984 年首次提出了基于身份的密码体制(identity-based cryptography)[1].在基于身份的密码体制中,用户的公钥可以根据用户的身份信息(姓名、身份证号码、电话号码、E-mail 地址等)直接计算出来,用户的私钥则由一个称为可信第三方的私钥生成中心(private key generator,简称 PKG)生成.这种体制没有证书的概念,也被称为无证书的注册密钥模式(registered key model).2008 年,Boneh 等人在亚洲密码学年会上提出了广义的基于身份的加密方案(generalized identity-based encryption)[2],该方案给出了广义的 4 个算法,为研究者在标准模型(standard model)下或者在随机预言模型(random oracle model)下建立自己的基于身份的加密方案提供了基准.不过,早在 2001 年,Boneh 等人利用双线性对提出了第 1 个基于身份的加密方案(identity-based encryption)[3].该方案安全实用,但仅能在随机预言模型[4,5]下证明其安全性.此后,该方案被众多学者引用.因此,大部分利用双线性对实现的基于身份的签名方案[6−13]都只能在随机预言模型下给出安全性证明.但是因为在随机预言模型下的随机函数是理想函数,因此在实际应用中,随机函数(一般为 hash 函数)的输出值并不确定.所以,随机函数是否会带来严重的安全问题依然值得进一步研究[14].同时,在部分随机预言模型下的签名方案中,由于分叉定理(forking lemma)[13,15]的引用,使得方案的安全性进一步降低,很多方案只能松归约(loose reduction)或者渐进归约(close reduction)[15]到困难问题假定上.而在标准模型下,敌手要攻破方案的难度等同于攻破困难问题假定的难度,方案的安全性得到提高.因此,在标准模型下的方案与在随机预言模型下的方案相比,具有更高的可证安全性.

目前,标准模型[16,17]已经成为当前主流的密码学技术之一.如何在标准模型下提出自己的方案,已经被众多学者研究.2005 年,Waters 利用双线性判定(decision bilinear diffie-Hellman)问题在标准模型下给出了第 1 个基于身份的加密方案[17].该方案具有可证的安全性,并在方案中给出了一个在标准模型下的签名方案.2006 年,Paterson 等人在 Waters 签名方案的基础上提出了基于身份的签名方案[18],该方案被证明能够归约于 CDH (computational diffie-Hellman)问题;同时,在该方案中给出了基于身份的签名方案的可证安全模型.但该方案的计算效率不高,需要多次乘法运算和多次双线性对计算.2009 年,李-姜等人提出了基于 Paterson 方案的改进方案[19],但改进后的方案输出更多的系统参数;同时,在线签名计算(on-line signature)效率不高.此后,马小龙等人在 2010 年提出了在标准模型下基于身份的传递签名方案[20].同样,该方案的计算效率不高.与随机预言模型下的方案相比,标准模型下的方案虽然除去了随机函数,构造了确定的结果,但确定性的结果需要更多的计算支持.因此,标准模型下的方案都存在计算效率不高的问题,如 Paterson 方案、李-姜方案以及它们的一些扩展方案[21,22]等.所以,如何在标准模型下权衡方案的效率和安全性,改进方案提升性能,使方案的实用性进一步提高是非常有必要的.

本文在分析 Paterson 方案的基础上,根据 Boneh 等人在文献[2]中提出的广义基于身份的加密方案思想,提出了一种新方案.该方案在不改变 Paterson 方案整体安全模型和困难问题假定的前提下,减少了原方案的运算量,消除了多次乘法运算,减少了验证方的双线性对计算次数;同时,根据文献[23,24]的方法对方案进行脱线/在线签名(off-line/on-line signature)处理,增加方案在脱线状态下的计算步骤,通过签名联票(signature coupon)机制完成签名.本文的主要工作是:(1) 对 Paterson 方案进行改进,在不改变原方案安全模型和困难问题假定的前提下,尽可能地减少运算量;在新的方案中消除了多次乘法运算,减少了双线性对的计算次数;(2) 根据 Shamir 等人在文献[23]中提出的方法对方案进行脱线/在线签名处理,减少在线计算步骤,通过签名联票机制完成签名;(3) 对新方案进行安全性证明,证明其在标准模型下具有抗适应性选择消息攻击的能力,并能够归约于 CDH 问题假定.

1 相关知识

1.1 双线性变换

双线性变换:设 G_1 和 G_2 分别为 q 阶的循环群,g 为 G_1 的生成元,则有 e:$G_1\times G_1\to G_2$,并且 e 满足条件 $e(g^a,g^b)=e(g,g)^{a\cdot b}$ 以及 $e(g,g)\neq 1$.即 e 满足双映射性、非退化性和可计算性.

1.2 计算diffie-Hellman问题及问题假设

定义 1(CDH 问题). 设 G_1 为 q 阶的循环群,g 为 G_1 的生成元,对于$\forall(g,g^a,g^b)\in G_1$,其中 $a,b\in Z_q$,计算 $g^{a\cdot b}$.

定义 2. 如果不存在一个概率多项式的算法 A 在时间 t 内以至少ε的概率解决 G_1 上 CDH 问题,我们则称 (t,ε)-CDH 问题假设在该群 G_1 上成立.

2 Paterson 方案回顾

2.1 Paterson方案

Paterson 等人提出的在标准模型下基于身份的签名方案,具有可证的安全性,在自适应选择消息攻击下存在不可伪造性,并能够归约于 CDH 问题假定.虽然该方案具有较高的安全性和实用性,但计算效率不高.本文简要回顾该方案.Paterson 方案由 4 个算法(Setup,Extract,Sign,Verify)组成,每个算法定义如下:

Setup 算法. PKG 系统选择两个 q 阶的循环群 G_1 和 G_2,g 为 G_1 的生成元,并存在一个映射 e:$G_1\times G_1\to G_2$;同时,存在两个无碰撞的 Hash 函数: $H_u:\{0,1\}^*\to\{0,1\}^{n_u}$ 和 $H_m:\{0,1\}^*\to\{0,1\}^{n_m}$,两个 Hash 函数分别用于把身份和消息的二进制串映射成固定长度为 n_u 和 n_m 的二进制串;

PKG 随机选择 $a\in Z_q$,计算 $g_1=g^a$,并随机选择 $g_2\in G_1$;同时,随机选择 $u',m'\in G_1$ 以及两个向量 $U=(u_i)$和 $M=(m_i)$,其中,$u_i\in G_1,m_i\in G_1$,U 和 M 的长度分别为 n_u 和 n_m;最后,PKG 输出公共参数 $params=(G_1,G_2,e,g,g_1,g_2,u',U,m',M)$,系统主密钥为 g_2^a .

Extract 算法. 设用户身份 u 为一个长度是 n_u 的二进制串,V 表示 u 中比特值为 1 的位置 i 的集合,即 $V\subseteq\{1,2,\ldots,n_u\}$;PKG 随机选择 $r_u\in Z_q$,则计算用户 u 的私钥为

$$d_u=\left(g_2^a\cdot\left(u'\prod_{i\in V}u_i\right)^{r_u},g^{r_u}\right).$$

PKG 通过安全的方式发送私钥 d_u 给用户 u.

Sign 算法. 用户 u 通过与 Extract 算法同样的方式获得 V 集合;同理,根据长度为 n_m 的消息 m 的二进制串获得 W 集合,W 表示 m 中比特值为 1 的位置 j 的集合,即 $W\subseteq\{1,2,\ldots,n_m\}$;随机选择 $r_m\in Z_q$,然后对消息 m 计算签名:

$$\sigma=(Q,R_u,R_m)=\left(g_2^a\cdot\left(u'\prod_{i\in V}u_i\right)^{r_u}\cdot\left(m'\prod_{j\in W}m_j\right)^{r_m},g^{r_u},g^{r_m}\right)\in G_1^3.$$

Verify 算法. 签名接收者收到用户 u 对消息 m 的签名$\sigma=(Q,R_u,R_m)$后,可以通过下面的等式验证签名:

$$e(Q,g)=e(g_1,g_2)\cdot e\left(u'\prod_{i\in V}u_i,R_u\right)\cdot e\left(m'\prod_{j\in W}m_j,R_m\right).$$

2.2 方案分析

(1) 效率分析

在 Paterson 方案中,方案需要多次乘法运算和 4 次双线性对运算,因此,Paterson 方案的计算效率不高.

如果设用户身份 u 表示长度为 n_u 的二进制串,消息 m 表示长度为 n_m 的二进制串,C_{mul} 表示群元素的乘

法运算时间,C_{expt} 表示指数运算时间,$C_{pairing}$ 表示双线性对 e 的运算时间,则计算 $\left(u'\prod_{i\in V}u_i\right)^{r_u}$ 大约平均需要 $\left(\frac{n_u+1}{2}\right)C_{mul}+C_{expt}$.同样,计算 $\left(m'\prod_{j\in W}m_j\right)^{r_m}$ 大约平均需要 $\left(\frac{n_m+1}{2}\right)C_{mul}+C_{expt}$,而验证方的平均运算时间为

$$\left(\frac{n_u+n_m+6}{2}\right)C_{mul}+4C_{pairing}.$$

虽然方案中有些部分的计算可以预先进行,但总的来说,方案计算效率不高.因此,本文接下来直观地分析(intuitive analysis)如何改进该方案.

(a) 消除多次群元素的乘法运算

在 Paterson 方案中,用户身份 u 表示为一个二进制串,然后,通过比特值为 1 的位置集合 V 映射到向量 $U=(u_i)$ 中,并被表示为 $u'\prod_{i\in V}u_i$,即多个 G_1 中元素 u_i 相乘的形式.如果设 $u'=g^t, u_i=g^{t_i}$,其中,$t,t_i\in Z_q$,则 $u'\prod_{i\in V}u_i$ 可以表示为 $g^{t+\sum_{i\in V}t_i}$.当然,任何人(包括 PKG 系统)只知道 g^t 和 g^{t_i},不能知道 t 和 t_i.因此,如果我们换个思路,把 u'和向量 U 中的 u_i 随机选至于 Z_q,计算 $u'+\sum_{i\in V}u_i$,则处理用户身份 u 时仅用到整数加运算.但是,在方案中如果把 $u'+\sum_{i\in V}u_i$ 用到 g 上,会有 $g^{u'+\sum_{i\in V}u_i}$.很明显,这样的设计与原方案相违背,等于任何人在原方案中不仅知道了 g^t 和 g^{t_i},也知道了 t 和 t_i,方案难度降低.但是我们可以注意到,方案中的 g_2 是个很特殊的参数,如果设 $g_2=g^b$,我们仅知道 g_2,并不知道 b,因此,如果我们在方案中把 $u'+\sum_{i\in V}u_i$ 用到 g_2 上,则有 $g_2^{u'+\sum_{i\in V}u_i}=g^{b\cdot u'+\sum_{i\in V}b\cdot u_i}$.那么,任何人仅知道 $g^{b\cdot u_i}$,不会知道 $b\cdot u_i$,这与原方案是一致的.当然,这样的设计已经在 Paterson 等人对自己方案的安全性证明中用到,但没有对方案本身进行这样的改进;而李-姜方案也仅对用户身份 u 进行了这样的处理.同样,我们对消息 m 也进行这样的处理,即 m'和向量 M 中的 m_i 随机选至于 Z_q,那么计算消息 m 时,有 $m'+\sum_{j\in W}m_j$.这样改进后,方案消除了多次群元素的乘法运算,处理用户身份 u 变为一次向量元素求和运算.由于模下群元素的相乘运算时间大于两个整数的相加运算时间,因此,如果设两个整数的相加运算时间为单位时间 $O(1)$,那么处理用户身份 u 所需平均时间仅为 $\frac{n_u+1}{2}$.同样,处理消息 m 所需平均时间仅为 $\frac{n_m+1}{2}$.

(b) 减少双线性对的计算次数

在方案中,验证方需要 4 次双线性对计算,非常占用计算时间.分析验证式:

$$e(Q,g)=e(g_1,g_2)\cdot e\left(u'\prod_{i\in V}u_i,R_u\right)\cdot e\left(m'\prod_{j\in W}m_j,R_m\right).$$

虽然 $e(g_1,g_2)$可以预先计算,但总的来说,验证方的计算量依然很大.因此,减少双线性对的计算次数成为关键.在验证式中,由于 $e(g_1,g_2)$中的 g_1 和 g_2 是公共的参数,因此我们可以把上式变换成如下形式:

$$\frac{e(Q,g)}{e(g_1,g_2)}=e\left(u'\prod_{i\in V}u_i,R_u\right)\cdot e\left(m'\prod_{j\in W}m_j,R_m\right).$$

我们可以直观地看出,如果假设 g_1 和 g_2 与右边的两个双线性对 $e\left(u'\prod_{i\in V}u_i,R_u\right)$ 和 $e\left(m'\prod_{j\in W}m_j,R_m\right)$ 没有关系,那么 $e(g_1,g_2)$完全可以被省去.但 g_1 和 g_2 作为公共的参数,很明显与 $e\left(u'\prod_{i\in V}u_i,R_u\right)$ 和 $e\left(m'\prod_{j\in W}m_j,R_m\right)$ 有着直接的变换关系,因此,如果我们能把 g_1 和 g_2 直接做到另外的两个双线性对中去,并预先计算出双线性对,然后根据对 $u'+\sum_{i\in V}u_i$ 和 $m'+\sum_{j\in W}m_j$ 的处理把 $u'+\sum_{i\in V}u_i$ 和 $m'+\sum_{j\in W}m_j$ 变为以 g_2 为底的指数形式,这样就可以把双线

性对计算转变为指数运算,并且转变后的方案如果依然能够成功归约于 CDH 问题假定,那么改进的方案至少可以省去两个双线性对的计算时间,直觉上是有希望的.

(2) 安全性分析

Paterson 等人对该方案的安全性分析是非常完善的.在标准模型下,文献[18]给出了一个完整的基于身份的可证安全模型.在该模型中,攻击者与挑战者之间进行一个询问游戏(query game),游戏分为系统设置、密钥询问(key queries)、签名询问(signature queries)、伪造(forgery)等 4 个阶段,如果攻击者想要获得成功,需要有以下 3 个条件同时成立:(1) 对身份 u 的密钥询问成功;(2) 对身份 u 和消息 m 的签名询问成功;(3) 伪造签名成功.因此,本文方案的安全性证明也将基于这个思路.

基于以上分析,第 3 节给出我们的方案.

3 新的方案

根据 Boneh 等人[2]提出广义的基于身份的加密方案思想,在 Paterson 方案的基础上,本文提出了一种更高效、安全的基于身份的签名方案.新方案由 4 个算法(Setup,keyGen,Sign,Verify)组成,每个算法的定义如下:

系统设置(Setup):PKG 系统选择两个 q 阶的循环群 G_1 和 G_2,g 为 G_1 的生成元,并存在一个映射 $e:G_1\times G_1\to G_2$;同时,存在两个无碰撞的 Hash 函数: $H_u:\{0,1\}^*\to\{0,1\}^{n_u}$ 和 $H_m:\{0,1\}^*\to\{0,1\}^{n_m}$,两个 Hash 函数分别用于把身份和消息的二进制串映射成固定长度为 n_u 和 n_m 的二进制串.

PKG 随机选择 $x\in Z_q$,计算 $g_1=g^x$,并随机选择 $g_2\in G_1$;同时,随机选择 $u',m'\in Z_q$ 以及两个向量 $U=(u_i)$和 $M=(m_i)$,其中,$u_i\in Z_q$,$m_i\in Z_q$,U 和 M 的长度分别为 n_u 和 n_m;最后,PKG 输出公共参数 $params=(G_1,G_2,e,g,g_1,g_2,u',U,m',M)$,系统主密钥为 g_2^x.

用户密钥生成(keyGen):设用户身份 u 为一个长度为 n_u 的二进制串,V 表示 u 中比特值为 1 的位置 i 的集合,即 $V\subseteq\{1,2,\ldots,n_u\}$;PKG 随机选择 $r\in Z_q$,则计算用户 u 的私钥为

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

PKG 通过安全的方式发送私钥 d_u 给用户 u,用户 u 通过与 keyGen 算法同样的方式获得 V 集合,然后对收到的私钥 d_u 进行验证 $e(d_1,g)\overset{?}{=}e(g_2,g_1)\cdot d_2^{\left(u'+\sum_{i\in V}u_i\right)}$:如果相等,则接受;否则,可以要求 PKG 重新生成私钥 d_u.

签名算法(Sign):用户 u 通过与 keyGen 算法同样的方式对长度为 n_m 的消息 m 的二进制串进行处理,获得 W 集合,W 表示 m 中比特值为 1 的位置 j 的集合,即 $W\subseteq\{1,2,\ldots,n_m\}$;随机选择 $s\in Z_q$,然后对消息 m 计算签名:

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

验证算法(Verify):签名接收者收到用户 u 对消息 m 的签名 $\sigma=(Q_1,Q_2,Q_3)$后,可以通过等式验证签名:

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

4 方案分析

4.1 正确性分析

我们对方案中使用的两个验证式进行推导分析.

(1) 用户 u 对私钥 d_u 进行验证,有

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

(2) 签名接收者对用户 u 对消息 m 的签名σ=(Q_1,Q_2,Q_3)进行验证,有

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

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

4.2 效率分析

对于新方案,我们可以采用文献[23,24]中提到的在线/脱线联票机制再次提升方案的性能.在新方案中,签名方的计算主要由 $Q_1=d_1\cdot(g_2^s)^{m'+\sum_{j\in W}m_j}$ 和 Q_2=$e(g_2,g)^s$组成,因此,我们可以在脱线状态下预先计算 g_2^s 和$e(g_2,g)^s$产生签名联票.那么,在线签名计算仅需要一次向量元素求和运算、一次指数运算和一次乘法运算;同时,在验证方,验证签名的计算量主要来自于两个双线性对计算 $e(Q_1,g),e(g_2,g_1)$以及两次指数运算 $Q_2^{m'+\sum_{j\in W}m_j}$ 和 $Q_3^{u'+\sum_{i\in V}u_i}$.由于$e(g_2,g_1)$可以预先计算,因此,验证方的在线计算可以减少到两次向量元素求和运算、两次指数运算、一次双线性对的计算和两次乘法运算.

与 Paterson 方案相比,新方案消除了多次乘法运算,减少了验证方的双线性对计算次数,方案的总运算量减少近一半;与李-姜方案相比,新方案减少了系统输出参数,并进一步减少了签名方和验证方的在线计算量.如果设用户身份 u 表示为长度为 n_u 的二进制串,消息 m 表示为长度为 n_m 的二进制串,整数求和运算时间为单位时间 $O(1)$,C_{mul} 表示群元素的乘法运算时间,C_{expt} 表示指数运算时间,$C_{pairing}$ 表示双线性对 e 的运算时间,$|G_1|$表示 G_1 群元素的长度,$|G_2|$表示 G_2 群元素的长度,则 3 种方案在相同标准下的量化比较见表 1 和表 2.

与 Paterson 方案相比,李-姜方案在签名方的计算量没有减少,而在验证方通过输出更多的系统参数减少计算量[19];同时,签名长度稍有增加.与 Paterson 方案相比,本文方案输出的系统参数相当,虽然签名长度稍有增加,但签名方和验证方的计算量都有很大程度的减少,签名方消除了多次群元素的相乘运算,在线计算量减少到 $\frac{n_m+1}{2}+C_{mul}+C_{expt}$;同时,验证方不仅减少了总的双线性对计算次数,而且也消除了多次群元素的相乘运算,验证方的在线计算量减少到 $\frac{n_u+n_m+2}{2}+2C_{mul}+2C_{expt}+C_{pairing}$,其中仅需一次双线性对计算.

Table 1 Performance comparison of three schemes

表 1 3 种方案的计算性能比较

	On-Line computation of signer	On-Line computation of verifier
Paterson's scheme	$\left(\frac{n_m+3}{2}\right)C_{mul}+C_{expt}$	$\left(\frac{n_u+n_m+6}{2}\right)C_{mul}+3C_{pairing}$
Li-Jiang's scheme	$\left(\frac{n_m+3}{2}\right)C_{mul}+C_{expt}$	$\frac{n_u+1}{2}+\left(\frac{n_m+5}{2}\right)C_{mul}+C_{expt}+2C_{pairing}$
The scheme	$\frac{n_m+1}{2}+C_{mul}+C_{expt}$	$\frac{n_u+n_m+2}{2}+2C_{mul}+2C_{expt}+C_{pairing}$

Table 2 Signature size comparison of three schemes

表 2 3 种方案的签名长度比较

	Signature size
Paterson's scheme	$3\|G_1\|$
Li-Jiang's scheme	$2\|G_1\|+\|G_2\|$
The scheme	$\|G_1\|+2\|G_2\|$

4.3 安全性分析

本文方案的安全性证明基于文献[17,18]的思路,在标准模型下,通过攻击者与挑战者之间的一个询问游戏证明方案的安全性,证明其可归约于 CDH 问题假定.在开始询问游戏之前,我们给出如下定理:

定理. 如果对于(t',ε')-CDH 问题假定成立,那么本文签名方案是(t,ε,q_e,q_s)-安全的,其中,

$$\varepsilon'=\frac{\varepsilon}{16(q_e+q_s)q_s(n_u+1)(n_m+1)},$$

$$t'=t+O\left((4q_e+5q_s)C_{expt}+(q_e+q_s)C_{pairing}+q_s\left(\frac{n_m+1}{2}\right)+q_e\left(\frac{n_u+1}{2}\right)\right).$$

q_e 是密钥询问次数,q_s 是签名询问次数,n_u 是用户身份 u 的二进制串长度,n_m 是消息 m 的二进制串长度,C_{expt} 是指数运算时间,$C_{pairing}$ 是双线性对计算时间.

为了证明上述定理,我们开始游戏.假设存在一个(t,ε,q_e,q_s)的攻击者 A,构造一个算法 B,在至多 t'时间内以至少ε'的概率解决 CDH 问题.因此,对于给定的$(g,g^a,g^b)\in G_1$,其中,$a,b\in Z_q$,为了能够计算 $g^{a\cdot b}$,算法 B 模拟挑战者与攻击者 A 进行交互,具体交互过程如下:

系统设置(Setup):令 $l_u=2(q_e+q_s)$,$l_m=2q_s$,随机选择 $k_u\in Z_{l_u}$,$k_m\in Z_{l_m}$,且有 $0\leqslant k_u\leqslant n_u$,$0\leqslant k_m\leqslant n_m$,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 $X=(x_i)$,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 $Y=(y_j)$,其中,$y_j\in Z_{l_m}$;同时,为了使符号更容易转换,定义如下两个函数:

$$F(u)=x'+\sum_{i\in V}x_i-l_u\cdot k_u,$$

$$K(m)=y'+\sum_{j\in W}y_j-l_m\cdot k_m.$$

现在,算法 B 构造系统参数:$g_1=g^a$,$g_2=g^b$,$u'=-l_u\cdot k_u+x'$,$u_i=x_i(1\leqslant i\leqslant n_u)$,$m'=-l_m\cdot k_m+y'$,$m_j=y_j(1\leqslant j\leqslant n_m)$,则有系统主密钥: $g_2^a=g^{a\cdot b}$,$u'+\sum_{i\in V}u_i=F(u)$,$m'+\sum_{j\in W}m_j=K(m)$.

询问(Queries):算法 B 与攻击者 A 进行交互,回答攻击者 A 的如下询问:

(1) 密钥询问:进行一个身份为 u 的密钥询问.算法 B 不知道系统主密钥,当 $F(u)\neq 0 \bmod q$ 时,算法 B 可以产生一个对应于身份 u 的密钥.即算法 B 随机选择 $r\in Z_q$,计算 $d_u=(d_1,d_2)=\left((g_2^r)^{u'+\sum_{i\in V}u_i},e\left(g^r\cdot g_1^{-\frac{1}{F(u)}},g_2\right)\right)$,假设可进行如下变换:

$$d_u=(d_1,d_2)=\left((g_2^r)^{u'+\sum_{i\in V}u_i},e\left(g^r\cdot g_1^{-\frac{1}{F(u)}},g_2\right)\right)=\left((g_2^r)^{u'+\sum_{i\in V}u_i}\cdot g_2^a\cdot g_2^{-a},e\left(g^r\cdot g_1^{-\frac{1}{F(u)}},g_2\right)\right)$$

$$=\left(g_2^a\cdot(g_2^r)^{F(u)}\cdot g_2^{-a},e\left(g^r\cdot g_1^{-\frac{1}{F(u)}},g_2\right)\right)=\left(g_2^a\cdot g_2^{r\cdot F(u)}\cdot g_2^{-a},e\left(g^{\frac{r}{a}\cdot a}\cdot g_1^{-\frac{1}{F(u)}},g_2\right)\right)$$

$$=\left(g_2^a\cdot g_2^{a\cdot\frac{r}{a}\cdot F(u)}\cdot g_2^{-a\cdot\frac{1}{F(u)}\cdot F(u)},e\left(g_1^{\frac{r}{a}}\cdot g_1^{-\frac{1}{F(u)}},g_2\right)\right)=\left(g_2^a\cdot(g_2^a)^{\left(\frac{r}{a}-\frac{1}{F(u)}\right)F(u)},e\left(g_1^{\frac{r}{a}-\frac{1}{F(u)}},g_2\right)\right).$$

令 $r'=\frac{r}{a}-\frac{1}{F(u)}$,那么有 $d_u=(d_1,d_2)==(g_2^a\cdot(g_2^a)^{r'\cdot F(u)},e(g_1^{r'},g_2))=\left(g_2^a\cdot(g_2^a)^{r'\left(u'+\sum_{i\in V}u_i\right)},e(g_2,g_1)^{r'}\right)$.然后,算法 B 将 d_u 发送给攻击者 *A*,*A* 对其验证:

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

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

则对攻击者 *A* 来说,算法 *B* 所产生的关于某个用户身份 u 的密钥与挑战者所产生的密钥不可区分.

如果 $F(u)=0 \bmod q$,则算法 *B* 不能进行,模拟终止;同时,如果将 $F(u)\neq 0 \bmod q$ 作为密钥伪造成功的条件,那么由于 $0\leqslant l_u(n_u+1)<q, 0\leqslant k_u\leqslant n_u$, $F(u)=x'+\sum_{i\in V}x_i-l_u\cdot k_u$,所以 $0\leqslant l_u(n_u+1)<q\Rightarrow 0\leqslant l_u\cdot k_u<q$, $0\leqslant x'+\sum_{i\in V}x_i<q$,那么有 $F(u)=0 \bmod q\Rightarrow F(u)=0 \bmod l_u$.于是,$F(u)\neq 0 \bmod l_u\Rightarrow F(u)\neq 0 \bmod q$.所以将 $F(u)\neq 0 \bmod l_u$ 作为密钥伪造成功的条件,这样方便分析后面的概率计算.(2) 签名询问:进行一个身份为 u 和该身份 u 对消息 m 的签名询问.当 $K(m)\neq 0 \bmod q$ 时,算法 *B* 随机选择 $r\in Z_q, s\in Z_q$,计算 $\sigma=(Q_1,Q_2,Q_3)=\left((g_2^s)^{m'+\sum_{j\in W}m_j},e\left(g^s g_1^{-\frac{1}{K(m)}-\frac{r\cdot F(u)}{K(m)}},g_2\right),e(g_2,g_1)^r\right)$. 为了方便证明,我们假设能作如下变换

$$\sigma=(Q_1,Q_2,Q_3)=\left((g_2^s)^{m'+\sum_{j\in W}m_j},e\left(g^s g_1^{-\frac{1}{K(m)}-\frac{r\cdot F(u)}{K(m)}},g_2\right),e(g_2,g_1)^r\right)$$

$$=\left((g_2^s)^{K(m)}\cdot g_2^{a\cdot r\cdot F(u)}\cdot g_2^{-a\cdot r\cdot F(u)}\cdot g_2^a\cdot g_2^{-a},e\left(g^s g_1^{-\frac{1}{K(m)}-\frac{r\cdot F(u)}{K(m)}},g_2\right),e(g_2,g_1)^r\right)$$

$$=\left(g_2^a\cdot g_2^{a\cdot r\cdot F(u)}\cdot(g_2^s)^{K(m)}\cdot g_2^{-a}\cdot g_2^{-a\cdot r\cdot F(u)},e\left(g^s g_1^{-\frac{1}{K(m)}-\frac{r\cdot F(u)}{K(m)}},g_2\right),e(g_2,g_1)^r\right)$$

$$=\left(g_2^a\cdot g_2^{a\cdot r\cdot F(u)}\cdot g_2^{s\cdot K(m)}\cdot g_2^{-\frac{a}{K(m)}\cdot K(m)}\cdot g_2^{-a\cdot r\cdot\frac{F(u)}{K(m)}\cdot K(m)},e\left(g^s g^{-\frac{a}{K(m)}-\frac{a\cdot r\cdot F(u)}{K(m)}},g_2\right),e(g_2,g_1)^r\right)$$

$$=\left(g_2^a\cdot g_2^{a\cdot r\cdot F(u)}\cdot g_2^{\left(s-\frac{a}{K(m)}-a\cdot r\cdot\frac{F(u)}{K(m)}\right)K(m)},e\left(g^{s-\frac{a}{K(m)}-\frac{a\cdot r\cdot F(u)}{K(m)}},g_2\right),e(g_2,g_1)^r\right)$$

$$=\left(g_2^a\cdot g_2^{a\cdot r\cdot F(u)}\cdot g_2^{\left(s-\frac{a}{K(m)}-a\cdot r\cdot\frac{F(u)}{K(m)}\right)K(m)},e(g_2,g)^{s-\frac{a}{K(m)}-\frac{a\cdot r\cdot F(u)}{K(m)}},e(g_2,g_1)^r\right).$$

令 $s'=s-\frac{a}{K(m)}-a\cdot r\cdot\frac{F(u)}{K(m)}$,则有 $\sigma=(Q_1,Q_2,Q_3)=(g_2^a\cdot g_2^{a\cdot r\cdot F(u)}\cdot g_2^{s'\cdot K(m)},e(g_2,g)^{s'},e(g_2,g_1)^r)$.然后,算法 *B* 将 σ

发送给攻击者 A,A 对其验证:

$$\begin{aligned}e(Q_1,g)&=e(g_2^a\cdot g_2^{a\cdot r\cdot F(u)}\cdot g_2^{s'\cdot K(m)},g)=e(g_2^a,g)\cdot e(g_2^{a\cdot r\cdot F(u)},g)\cdot e(g_2^{s'\cdot K(m)},g)\\&=e(g_2,g_1)\cdot e(g_2^{r\cdot F(u)},g_1)\cdot e(g_2,g)^{s'\cdot K(m)}=e(g_2,g_1)\cdot e(g_2,g_1)^{r\cdot F(u)}\cdot e(g_2,g)^{s'\cdot K(m)}\\&=e(g_2,g_1)\cdot Q_3^{F(u)}\cdot Q_2^{K(m)}=e(g_2,g_1)\cdot Q_2^{m'+\sum_{j\in W}m_j}\cdot Q_3^{u'+\sum_{i\in V}u_i},\end{aligned}$$

则对攻击者 A 来说,算法 B 所产生的某个用户 u 对消息 m 的签名与挑战者所产生的真实签名不可区分.

如果 $K(m)=0 \bmod q$,则算法 B 不能进行,模拟终止;同时,如果将 $K(m)\neq 0 \bmod q$ 作为签名伪造成功的条件,那么同样将 $K(m)\neq 0 \bmod l_m$ 作为签名伪造成功的条件.

伪造阶段(Forgery):如果算法 B 在询问阶段没有终止,那么攻击者 A 至少可以 ε 的概率返回一个身份 u^*、一个消息 m^* 以及一个身份 u^* 对消息 m^* 的可验证的签名:

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

因此,当 $F(u^*)\neq 0 \bmod q$ 或者 $K(m^*)\neq 0 \bmod q$ 时,算法 B 停止;当 $F(u^*)=0 \bmod q$ 且 $K(m^*)=0 \bmod q$ 时,算法 B 则可计算:

$$Q_1^*=g_2^a\cdot(g_2^a)^{r^*\left(u'+\sum_{i\in V}u_i\right)}\cdot(g_2^{s^*})^{m'+\sum_{j\in W}m_j}=g_2^a\cdot(g_2^{a\cdot r^*})^{F(u)}\cdot(g_2^{s^*})^{K(m)}=g_2^a=g^{a\cdot b}.$$

即输出 CDH 问题.

现在我们分析算法 B 模拟成功的概率.因为需要完整地运行整个算法才能解决 CDH 问题,所以算法 B 在密钥询问、签名询问、伪造阶段都不能终止.如果算法 B 不终止,那么根据上述的过程可知,需要有 3 个条件成立:

(a) 密钥询问成功 $F(u_i)\neq 0 \bmod l_u$;

(b) 签名询问成功 $K(m_j)\neq 0 \bmod l_m$;

(c) 伪造阶段成功 $F(u^*)=0 \bmod q$ 且 $K(m^*)=0 \bmod q$.

为了更好地分析,我们定义 4 个事件:A_i:$F(u_i)\neq 0 \bmod l_u$,A^*:$F(u^*)=0 \bmod q$,B_j:$K(m_j)\neq 0 \bmod l_m$,B^*:$K(m^*)=0 \bmod q$;并且如果设 $q_I\leqslant q_e+q_s$,$q_M\leqslant q_s$,q_I 表示出现在密钥询问中的身份序列长度或者出现在签名询问中但不包括挑战身份 u^* 的身份序列长度,q_M 表示签名询问中包含了挑战身份 u^* 询问的消息序列长度,则算法 B 成功模拟的概率为

$$P(B\_Success)\geqslant P\left(\bigcap_{i=1}^{q_I}A_i\wedge A^*\wedge\bigcap_{j=1}^{q_M}B_j\wedge B^*\right),$$

其中,$\bigcap_{i=1}^{q_I}A_i\wedge A^*$ 和 $\bigcap_{j=1}^{q_M}B_j\wedge B^*$ 互为独立事件.那么计算,

$$\begin{aligned}P(A^*)&=P(F(u^*)=0 \bmod q\wedge F(u^*)=0 \bmod l_u)\\&=P(F(u^*)=0 \bmod l_u)\cdot P(F(u^*)=0 \bmod q/F(u^*)=0 \bmod l_u)=\frac{1}{l_u}\cdot\frac{1}{n_u+1}.\end{aligned}$$

又 $P\left(\bigcap_{i=1}^{q_I}A_i\Big/A^*\right)=1-P\left(\bigcup_{i=1}^{q_I}\neg A_i\Big/A^*\right)\geqslant 1-\frac{q_I}{l_u}\geqslant 1-\frac{q_e+q_s}{l_u}$,其中,$\neg A_i\Big/A^*$ 为独立事件,所以有,

$$P\left(\bigcap_{i=1}^{q_I}A_i\wedge A^*\right)=P\left(\bigcap_{i=1}^{q_I}A_i\Big/A^*\right)\cdot P(A^*)\geqslant\left(1-\frac{q_e+q_s}{l_u}\right)\cdot\frac{1}{l_u}\cdot\frac{1}{n_u+1}.$$

又因为 $l_u=2(q_e+q_s)$,则容易计算出 $P\left(\bigcap_{i=1}^{q_I}A_i\wedge A^*\right)\geqslant\frac{1}{4(q_e+q_s)(n_u+1)}$,

同理可以求出 $P\left(\bigcap_{j=1}^{q_M}B_j\wedge B^*\right)\geqslant\frac{1}{4q_s(n_m+1)}$,则

$$P(B\_Success) \geqslant P\left(\bigcap_{i=1}^{q_I} A_i \wedge A^* \wedge \bigcap_{j=1}^{q_M} B_j \wedge B^*\right) \geqslant \frac{1}{4(q_e+q_s)(n_u+1)} \cdot \frac{1}{4q_s(n_m+1)} = \frac{1}{16(q_e+q_s)q_s(n_m+1)(n_u+1)}.$$

所以有 $\varepsilon' = \dfrac{\varepsilon}{16(q_e+q_s)q_s(n_u+1)(n_m+1)}$.

因此,如果算法 B 没有被终止,攻击者可以ε的概率伪造一个有效签名,并且算法 B 可以通过解决 CDH 问题计算出 $g^{a\cdot b}$.算法 B 完成整个过程的运行时间则需要:

$$t' = t + O\left((4q_e+5q_s)C_{expt} + (q_e+q_s)C_{pairing} + q_s\left(\frac{n_m+1}{2}\right) + q_e\left(\frac{n_u+1}{2}\right)\right).$$

因此,算法 B 能够在时间 t'内以ε'的概率解决 G_1 上 CDH 问题,但这与(t',ε')-CDH 问题假定矛盾.因此,本文的签名方案是(t,ε,q_e,q_s)-安全的.

5 结束语

本文提出了一种基于身份的高效签名方案,与 Paterson 方案相比,减少了签名方和验证方的运算量,总的运算量减少近一半,提高了计算效率;同时,新方案与 Paterson 方案的安全强度相当,在标准模型下,具有在自适应选择消息攻击下存在不可伪造性,并可归约于 CDH 问题假定.与李-姜方案相比,新方案不仅减少了系统输出参数,而且进一步减少了签名方和验证方的在线运算量.因此,新方案具有可证的安全性和更高的实用性.新方案的主要缺点在于方案依赖于双线性对,计算时间消耗较多,在某些场景的计算中会有性能上的影响.因此,安全与性能的权衡将是值得进一步研究的问题.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, Chaum D, eds. Advances in Cryptology-CRYPTO'84. LNCS 196, Berlin: Springer-Verlag, 1985. 47−53.

[2] Boneh D, Hanburg M. Generalized identity based and broadcast encryption schemes. In: Pieprzyk J, ed. Advances in Cryptology-ASIACRYPT 2008. LNCS 5350, Berlin: Springer-Verlag, 2008. 455−470. [doi: 10.1007/978-3-540-89255-7_28]

[3] 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]

[4] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 62−73. [doi: 10.1145/168588.168596]

[5] Bellare M, Rogaway P. The exact security of digital signatures—How to sign with RSA and Rabin. In: Maurer U, ed. Proc. of the Advances in Cryptology-EUROCRYPT'96 Proc. LNCS 1070, Berlin: Springer-Verlag, 1996. 399−416. [doi: 10.1007/3-540-68339-9_34]

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

[7] 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]

[8] 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]

[9] Yoon H, Cheon JH, Kim.Y. Batch verifications with ID-based signatures. In: Park C, Chee S, eds. Proc. of the Information Security and Cryptology-ICISC 2004. LNCS 3506, Berlin: Springer-Verlag, 2005. 233−248.

[10] Zhou L, Li DP, Yang YX. ID-Based signature without trusted PKG. Journal on Communications, 2008,29(6):8−12 (in Chinese with English abstract).

[11] Zhao ZM, Wang XY, Xu CG. An identity signature scheme based on iris information. Journal of Electronics & Information Technology, 2010,32(10):2388−2392 (in Chinese with English abstract).

[12] Zhang JZ, Guo Z, Lan JQ. Identity-Based signcrytion without trusted party. Computer Engineering and Applications, 2010,46(13): 80−81 (in Chinese with English abstract).

[13] Gu CX, Zhu YF, Pan XY. Forking lemma and the security proofs for a class of ID-based signatures. Journal of Software, 2007, 18(4):1007−1014 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1007.htm [doi: 10.1360/jos181007]

[14] Coron JS, Dodis Y, Malinaud C, Puniya P. Merkle-Dåmgard revisited: How to construct a Hash function. In: Shoup V, ed. Advances in Cryptology-CRYPTO 2005. LNCS 3621, Berlin: Springer-Verlag, 2005. 430−448.

[15] Goh EJ, Jarecki S. A signature scheme as secure as the diffie-Hellman problem. In: Biham E, ed. Proc. of the Advances in Cryptology- EUROCRYPT 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 401−415. [doi: 10.1007/3-540-39200-9_25]

[16] Boneh D, Boyen X. Secure identity based encryption without random oracles. In: Franklin MK, ed. Proc. of the Advances in Cryptology- CRYPTO 2004. LNCS 3152, Berlin: Springer-Verlag, 2004. 443−459. [doi: 10.1007/978-3-540-28628-8_27]

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

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

[19] 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).

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

[21] Cai YQ, Zhang XD, Jiang N. A novel identity-based threshold signature. ACTA ELECTRONICA SINICA, 2009,37(4S1):102−105 (in Chinese with English abstract).

[22] Xu J. Provably secure threshold signature schemes without random oracles. Chinese Journal of Computers, 2006,29(9):1636−1640 (in Chinese with English abstract).

[23] Shamir A, Tauman Y. Improved online/offline signature schemes. In: Kilian J, ed. Advances in Cryptology-CRYPTO 2001. LNCS 2139, Berlin: Springer-Verlag, 2001. 355−367. [doi: 10.1007/3-540-44647-8_21]

[24] Mehta M, Harn L. Efficient one-time proxy signatures. IEE Proceedings-Communications, 2005,152(2):129−133. [doi: 10.1049/ip-com:20045251]

附中文参考文献:

[10] 周亮,李大鹏,杨义先.基于身份的无需可信任 PKG 的签名方案.通信学报,2008,29(6):8−12.

[11] 赵泽茂,王向阳,许春根.基于虹膜信息的身份签名方案.电子与信息学报,2010,32(10):2388−2392.

[12] 张建中,郭振,兰建青.一个基于身份的无需可信中心的签密方案.计算机工程与应用,2010,46(13):80−81.

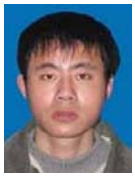
[13] 顾纯祥,祝跃飞,潘晓豫.Forking 引理与一类基于身份签名体制的安全性证明.软件学报,2007,18(4):1007−1014. http://www.jos.org.cn/1000-9825/18/1007.htm [doi: 10.1360/jos181007]

[19] 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.

[20] 马小龙,谷利泽,催巍,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.

[21] 蔡永泉,张雪迪,姜楠.一种新的基于身份的门限签名方案.电子学报,2009,37(4S1):102−105.

[22] 徐静.标准模型下可证安全的门限签名方案.计算机学报,2006,29(9):1636−1640.



谷科(1980－),男,湖南长沙人,博士生,主要研究领域为信息安全,移动电子商务,密码学应用.

贾维嘉(1957－),男,博士,教授,博士生导师,CCF 会员,主要研究领域为移动计算,下一代无线网络通信及协议,异构网络,无线网络安全.

姜春林(1983－),男,博士生,主要研究领域为异构网络安全,异构网络协议.