标准模型下可证安全的基于身份的高效签名方案

李继国 姜平进
(河海大学计算机及信息工程学院 南京 210098)

摘 要 基于身份的公钥密码体制克服了传统公钥密码体制所带来的公钥证书存储和管理开销问题;目前大多数基于身份的数字签名方案的安全性是基于随机预言模型进行证明,但随机预言机的实现方式可能会导致方案的不安全,如 Hash 函数,往往返回的结果并不是随机的.文中提出一种安全、高效的基于身份的签名方案,并且在标准模型下证明该方案对自适应选择消息攻击是存在不可伪造的,方案的安全性可规约为 CDH 困难假定.与现有的标准模型下安全的基于身份的签名方案相比,方案的通信代价更小,执行效率更高.

关键词 基于身份的签名;双线性对;标准模型;CDH-问题;选择消息攻击
中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2009.02130

An Efficient and Provably Secure Identity-Based Signature Scheme in the Standard Model

LI Ji-Guo JIANG Ping-Jin
(*College of Computer & Information Engineering, Hohai University, Nanjing* 210098)

Abstract Compared with the traditional public key cryptosystem, identity-based cryptosystem can simplify the key management procedure from the view point of the efficiency and convenience. Most of identity-based signature schemes are secure in the random oracle model, but for which any implementation of the random oracle results in insecure schemes. For example, when random oracle is instantiated with concrete hash functions, the resulting scheme is nonrandom which may not be secure. This paper proposes an efficient and provably secure identity-based signature scheme. The scheme is existentially unforgeable against adaptive chosen message attacks under the computational Diffie-Hellman assumption in the standard model. Compared with the known identity-based scheme secure in the standard model, the scheme enjoys shorter signature length and less operation.

Keywords identity-based signature; bilinear pairings; standard model; CDH-problem; chosen message attack

1 引 言

1984 年,Shamir 提出基于身份的公钥密码体制[1],在这种体制中,Shamir 建议使用能标识用户身份的信息为公钥,比如名字、IP 地址或者 Email 地址.基于身份密码体制的主要优势在于它减轻了用户对公钥证书的需要和依赖.2001 年,Boneh 和 Franklin 利用 Weil 配对技术(Weil pairing)提出了第一个安全、实用的基于身份的加密方案[2],自从那

收稿日期:2008-01-27;最终修改稿收到日期:2009-06-07.本课题得到国家自然科学基金(60842002,60673070)、国家"八六三"高技术研究发展计划项目基金(2007AA01Z409)、江苏省公安厅项目(200503002)及河海大学优秀创新人才支持计划资助.**李继国**,男,1970 年生,博士,教授,博士生导师,主要研究领域为信息安全、密码学理论与技术.E-mail: lijiguo@hhu.edu.cn. **姜平进**,男,1984 年生,硕士,主要研究方向为密码学理论与技术.

之后,基于身份的密码体制引起了国内外众多学者的广泛关注并得到迅速发展,提出了大量的基于身份的加密和签名方案[3-10],这些方案都是在随机预言模型(Random Oracle Model)下被证明是安全的.随机预言模型作为一种理想化的计算模型,是由Bellare和Rogoway于1993年提出的[11].在这个模型中,任何具体的对象例如Hash函数,都被当作随机对象.它允许人们规约参数到相应的计算,Hash函数被作为一个随机预言返回值,对每一个新的询问,将得到一个随机的应答.但在具体的数字签名方案中,因为使用的Hash函数是具体的,对于询问的应答结果不一定是随机的,这就有可能导致方案的不安全[12-14].而另一方面,不需要随机预言模型(Without Random Oracle Model)的证明,即在标准模型(Standard Model)下的证明能够清楚地表明,除非其所基于的困难问题被破解,否则一个可证安全的密码方案不可能被攻破.因此,如果我们在方案的安全证明过程中不依赖理想化的随机预言模型,那么该方案的安全性证明将能够提供更充分的保障[15].因此,设计在标准模型下可证安全的基于身份的数字签名方案是本文研究工作的动机之一.

近年来,基于标准模型下的安全性证明受到广泛关注.2004年,Boneh和Boyen构造了两种在标准模型下证明安全的基于身份的加密方案[16],第一个构造是基于经典的双线性Diffie-Hellman(Bilinear Diffie-Hellman)假定,第二个构造是基于非标准的双线性Diffie-Hellman求逆(Bilinear Diffie-Hellman Inversion)假定.方案安全性证明中所使用的攻击模型是选择身份攻击模型,比Boneh和Franklin方案[2]证明中所用的攻击模型弱.后来他们又提出一种新的方案[17],在Boneh和Franklin方案中的攻击模型下,证明了方案的安全性,但是方案的运行效率不高,他们也提出一个公开问题:基于判定双线性Diffie-Hellman(Decision Bilinear Diffie-Hellman)假定或同等标准假定,设计标准模型下安全、高效的基于身份的加密体制.因此,研究标准模型下安全的基于身份的高效密码体制是当前需要迫切解决的问题,这也是本文研究工作的另外一个动机.2005年,Waters首次创造性地提出了标准模型下安全的基于身份的高效加密方案[18],并且方案的安全性可规约为判定双线性Diffie-Hellman假定,从而很好地解决了Boneh和Boyen提出的公开问题[17],同时他也指出该方法可用来构造标准模型下安全、高效的基于身份的签名方案,方案的安全性可规约为计算Diffie-Hellman假定.2006年,Paterson和Schuldt基于Waters方案[18],提出一个标准模型下安全、高效的基于身份的签名方案[19].由此可见,Waters方法已经成为当前构造标准模型下安全的密码协议的主流技术之一.

本文使用Waters方法,在Paterson和Schuldt方案(简记为PS方案)[19]的基础上,在不改变攻击模型和困难问题假设的前提下加以改进,提出一个新的标准模型下安全、高效的基于身份的签名方案.方案的安全性可规约为计算Diffie-Hellman假定.方案的通信代价与PS方案相当,方案的签名算法计算量与PS方案相当,方案的验证算法计算量减小了三分之一.

本文第2节介绍相关的背景知识和定义;第3节提出新的标准模型下安全的基于身份的高效签名方案;第4节给出方案的安全性分析;第5节分析方案的计算量和通信代价并与Paterson和Schuldt方案进行比较;第6节总结全文.

2　预备知识

2.1　双线性对(Bilinear Pairing)

这里简要介绍双线性配对的基本定义和它需满足的性质,更详细的介绍请参考文献[2].令G、G_T是两个p阶循环群,其中p为素数,g是G的生成元.定义两个群上的双线性映射为$e:G\times G\rightarrow G_T$,且满足下面的性质:

(1)双线性性. $e(g^a,g^b)=e(g,g)^{ab}$,对所有的$a,b\in Z_p^*$均成立.

(2)非退化性. $e(g,g)\neq 1_{G_T}$,其中1_{G_T}是G_T的幺元.

(3)可计算性. 存在有效算法来计算e.

可以注意到:e运算是可交换的,因为$e(g^a,g^b)=e(g,g)^{ab}=e(g^b,g^a)$.

2.2　困难问题假定

这里简要介绍方案证明中所使用的计算Diffie-Hellman问题和假定,更详细的介绍请参考文献[18-19].

定义1.　CDH-问题.给定p阶循环群G,其中p为素数,g是G的生成元,则群G上的CDH-问题是:已知$g^a,g^b\in G$,其中a,b是从Z_p随机选择的,计算g^{ab}.

定义2.　(ε,t)-CDH假定.如果不存在任何一种概率多项式算法在时间t内,以至少ε的概率解

决群 G 上的 CDH-问题，则称群 G 上的(ε,t)-CDH 假定成立.

2.3 基于身份的签名

基于身份的签名方案由以下 4 个算法构成[19]：

(1) 系统参数设置(Setup). 输入一个安全参数，PKG(Private Key Generation)以此来产生它的系统参数 *params* 和主密钥，然后 PKG 将系统参数 *params* 予以公开，主密钥保密.

(2) 用户密钥的产生(Extract). 给定身份 u，PKG 利用系统参数 *params* 和主密钥，产生身份 u 的密钥 d_u，且 PKG 能够为所有用户产生密钥，并通过安全信道发送给用户.

(3) 签名(Sign). 用户得到密钥，先对密钥验证，验证密钥是否由 PKG 产生. 若验证通过，则用户利用其身份 u、密钥 d_u、PKG 的系统参数 *params* 来产生消息 m 的签名 σ.

(4) 验证(Verify). 验证者利用 PKG 的系统参数 *params* 和用户身份 u 对消息 m 的签名 σ 验证.

2.4 基于身份签名的安全模型

基于身份签名的安全模型是自适应选择消息攻击下存在不可伪造性安全模型[20]的一种自然扩展. 这个模型是通过 *challenger* 与攻击者之间的攻击游戏来进行定义的[19]，攻击游戏分为以下 3 个步骤：

1. 系统参数设置(Setup). *challenger* 运行系统参数设置算法，得到系统参数 *params* 和主密钥. 攻击者得到系统参数 *params*，但不能获取主密钥，*challenger* 保密主密钥.

2. 询问(Queries). 攻击者向 *challenger* 自适应做一系列不同的询问，询问方式如下：

2.1. 密钥询问(Extract Queries). 攻击者能够获取任何身份 u 对应的密钥. *challenger* 通过运行 $Extract(params,u)$ 来进行响应，并将私钥 d_u 发送给攻击者.

2.2. 签名询问(Sign Queries). 攻击者能够获取任意身份 u 对消息 m 的签名. *challenger* 首先通过运行 $Extract(params,u)$ 获取身份 u 的私钥 d_u 来进行响应，然后通过运行 $Sign(params,d_u,u,m)$ 来获取签名 σ，并将其发送给攻击者.

3. 伪造(Forgery). 攻击者输出消息 m^*、身份 u^*、签名 σ^*.

若以下 3 个条件成立，则攻击成功：

(1) $Verify(params,u^*,m^*,\sigma^*)=accept$；

(2) 攻击者未对身份 u^* 做密钥询问；

(3) 攻击者未对(u^*,m^*)做签名询问.

定义 3. 如果攻击者 A 最多运行 t 时间，最多做 q_E 次密钥询问和 q_S 次签名询问，以不小于 ε 的概率赢得上述游戏，则称攻击者 A 是基于身份签名方案的(ε,t,q_E,q_S)-伪造者. 如果在基于身份的签名方案中不存在(ε,t,q_E,q_S)-伪造者，则称方案是(ε,t,q_E,q_S)-安全的.

3 基于身份的高效签名方案

为了使得方案更加灵活，对于不同长度的身份和消息比特串，利用抵抗碰撞的 Hash 函数进行处理，分别将它们映射到方案所要求的长度，即 $H_u:\{0,1\}^*\rightarrow\{0,1\}^{n_u}$，$H_m:\{0,1\}^*\rightarrow\{0,1\}^{n_m}$. 本文的方案由以下算法构成：

(1) 系统参数设置(Setup). 令 G、G_T 是 p 阶循环群，其中 p 为素数，g 为 G 的生成元，双线性配对为 $e:G\times G\rightarrow G_T$. PKG 随机选择 $g_2\in G,\alpha\in Z_p$，计算 $g_1=g^\alpha\in G$. 随机选择$u'\in Z_p$，$m'\in G$，n_u维的向量 $\boldsymbol{U}_v=(u_i)$，n_m 维的向量 $\boldsymbol{M}_v=(m_i)$，其中 $u_i\in Z_p$，$m_i\in G$. 令 $z_1=e(g_1,g_2)$，$z_2=e(g,g_2)$，则 PKG 的系统参数为 $params=(p,g,g_1,g_2,u',\boldsymbol{U}_v,m',\boldsymbol{M}_v,z_1,z_2)$，主密钥为 α.

(2) 用户密钥的产生(Extract). 假定用户身份 u 为一个长度为 n_u 的比特串，令 U 为 u 中比特值为 1 的位置的集合，则 $U\subseteq\{1,\cdots,n_u\}$. PKG 随机选择 $t\in Z_p$，计算用户的密钥 $d_u=(d_0,d_1)=(g_2^{\alpha+t(u'+\sum_{i\in U}u_i)},z_2^t)$，并通过安全信道把密钥传给用户. 若 $\alpha+t\left(u'+\sum_{i\in U}u_i\right)=0 \bmod p$，则 PKG 返回步(1)，重新选择主密钥 α.

(3) 签名(Sign). 用户得到密钥 d_u 后，先对密钥进行验证：$e(g,d_0)=z_1\cdot d_1^{(u'+\sum_{i\in U}u_i)}$. 若等式成立，则用户可以确认密钥是由 PKG 产生的；反之，重新向 PKG 询问密钥. 若密钥验证通过，可对消息签名. 假定消息 m 为一个长度为 n_m 的比特串，类似上面身份处理方法，令 M 为 m 中比特值为 1 的位置的集合，则 $M\subseteq\{1,\cdots,n_m\}$. 随机选择 $s\in Z_p$，消息 m 的签名为 $\sigma=(w,x,y)=\left(d_0\cdot\left(m'\prod_{j\in M}m_j\right)^s,g^s,d_1\right)$.

(4) 验证(Verify)：验证者用 PKG 系统参数 $(p,g,g_1,g_2,u',\boldsymbol{U}_v,m',\boldsymbol{M}_v,z_1,z_2)$和身份 u 对消息 m 的签名 σ 验证，若等式 $e(g,w)=z_1\cdot y^{(u'+\sum_{i\in U}u_i)}\cdot e\left(x,\left(m'\prod_{j\in M}m_j\right)\right)$成立，则签名有效，反之签名无效.

如果方案中各方按照上述算法的步骤执行，则本文方案的密钥验证算法和签名验证算法都是正确有效的. 方案的正确性证明如下.

证明. 用户得到密钥 $d_u=(d_0,d_1)=$

$(g_2^{\alpha+t(u'+\sum_{i\in U}u_i)}, e(g,g_2)^t)$,则有

$$\begin{aligned}e(g,d_0)&=e(g,g_2^{\alpha+t(u'+\sum_{i\in U}u_i)})\\&=e(g,g_2^{\alpha})\cdot e(g,g_2^{t(u'+\sum_{i\in U}u_i)})\\&=e(g_1,g_2)\cdot e(g,g_2)^{t(u'+\sum_{i\in U}u_i)}\\&=z_1\cdot d_1^{(u'+\sum_{i\in U}u_i)}.\end{aligned}$$

验证者得到签名 $\sigma=(w,x,y)$,则有

$$\begin{aligned}e(g,w)&=e\left(g,d_0\cdot\left(m'\prod_{j\in M}m_j\right)^s\right)\\&=e\left(g,g_2^{\alpha+t(u'+\sum_{i\in U}u_i)}\cdot\left(m'\prod_{j\in M}m_j\right)^s\right)\\&=e(g,g_2^{\alpha})\cdot e(g,g_2^{t(u'+\sum_{i\in U}u_i)})\cdot e\left(g,\left(m'\prod_{j\in M}m_j\right)^s\right)\\&=e(g_1,g_2)\cdot e(g,g_2)^{t(u'+\sum_{i\in U}u_i)}\cdot e\left(g^s,\left(m'\prod_{j\in M}m_j\right)\right)\\&=z_1\cdot y^{(u'+\sum_{i\in U}u_i)}\cdot e\left(x,\left(m'\prod_{j\in M}m_j\right)\right),\end{aligned}$$

所以本方案的密钥验证算法和签名验证算法都是正确有效的.

4　安全性分析

在本节,在标准模型下(即不利用随机预言假设)证明方案的安全性,方案的安全性可规约为计算 Diffie-Hellman 假定.根据本文第 2.4 节给出的基于身份签名的安全模型及定义,给出如下定理.

定理 1.　若 (ε',t')-CDH 假定成立,那么上述基于身份的签名方案是 $(\varepsilon,t,q_{\mathrm{E}},q_{\mathrm{S}})$-安全的,其中 $\varepsilon'=\dfrac{\varepsilon}{16(q_{\mathrm{E}}+q_{\mathrm{S}})q_{\mathrm{S}}(n_u+1)(n_m+1)}$, $t'=t+O(q_{\mathrm{E}}n_u+q_{\mathrm{S}}(\rho\cdot n_m+\tau\cdot n_u)+q_{\mathrm{S}}\tau)$, q_{E} 为密钥询问次数, q_{S} 为签名询问次数, ρ 为群 G 中多项式乘法运算时间, τ 为群 G 中指数运算时间.

证明.　证明的主要思路基于文献[17-18].假定 $(\varepsilon,t,q_{\mathrm{E}},q_{\mathrm{S}})$-攻击者 A 存在,构造一个算法 B,在至多 t' 的时间内,以至少 ε' 的概率解决 CDH-困难问题.给定 G 中元素 g,g^a,g^b,为了计算 g^{ab},算法 B 模拟 *challenger* 与 A 进行交互.算法 B 模拟 *challenger* 与 A 交互的过程具体如下:

系统参数设置(Setup). 令 $l_u=2(q_{\mathrm{E}}+q_{\mathrm{S}})$, $l_m=2q_s$,随机选择 $k_u\in Z_{l_u}$, $k_m\in Z_{l_m}$,且 $0\le k_u\le n_u$, $0\le k_m\le n_m$,对于给定的 $q_{\mathrm{E}},q_{\mathrm{S}},n_u,n_m$,假定 $l_u(n_u+1)<p$, $l_m(n_m+1)<p$.随机选择 $x'\in Z_{l_u}$, n_u 维向量 $\boldsymbol{X}=(x_i)$,且 $x_i\in Z_{l_u}$;随机选择 $z'\in Z_{l_m}$, n_m 维向量 $\boldsymbol{Z}=(z_j)$,且 $z_j\in Z_{l_m}$.最后,随机选择 $w'\in Z_p$ 和 n_m 维向量 $\boldsymbol{W}=(w_j)$,且 $w_j\in Z_p$.为了便于分析,定义如下 3 个函数:

$$F(u)=x'+\sum_{i\in U}x_i-l_uk_u,$$

$$K(m)=z'+\sum_{j\in M}z_j-l_mk_m,$$

$$L(m)=w'+\sum_{j\in M}w_j.$$

B 按照如下方式构造系统参数:

$$g_1=g^a,\ g_2=g^b,$$

$$u'=-l_uk_u+x',\ u_i=x_i,\ 1\le i\le n_u,$$

$$m'=g_2^{-l_m\cdot k_m+z'}g^{w'},\ m_j=g_2^{z_j}g^{w_j},\ 1\le j\le n_m,$$

则 $g_2^a=g_2^a=g^{ab}$, $u'+\sum_{i\in U}u_i=F(u)$, $m'\prod_{j\in M}m_j=g_2^{K(m)}g^{L(m)}$.

询问(Queries). 算法 B 模拟 *challenger* 与攻击者 A 进行交互,交互过程如下:

1.密钥询问(Extract Queries).考虑对一个身份 u 的密钥询问.算法 B 事先不知道系统的主密钥,当 $F(u)\ne 0 \bmod p$ 时,算法 B 可以产生对应于身份 u 的密钥.即,算法 B 随机选择 $t\in Z_p$,计算

$$d_u=(d_0,d_1)=(g_1^{-1}(gg_2)^{t(u'+\sum_{i\in U}u_i)}, e(gg_2,g^tg_1^{-\frac{1}{(u'+\sum_{i\in U}u_i)}})),$$

算法 B 将 d_u 发送给攻击者 A, A 对其进行验证:

$$\begin{aligned}e(d_0,g)&=e(g_1^{-1}(gg_2)^{t(u'+\sum_{i\in U}u_i)},g)\\&=e(g_1^{-1}(gg_2)^{tF(u)},g)=e(g_2^a\cdot((gg_2)^{F(u)})^{t-\frac{a}{F(u)}},g)\\&=e(g_2^a,g)\cdot e(((gg_2)^{F(u)})^{t-\frac{a}{F(u)}},g)\\&=e(g_1,g_2)\cdot e((gg_2)^{F(u)},g^{t-\frac{a}{F(u)}})\\&=e(g_1,g_2)\cdot e(gg_2,g^tg_1^{-\frac{1}{F(u)}})^{F(u)}\\&=z_1\cdot d_1^{F(u)}=z_1\cdot d_1^{(u'+\sum_{i\in U}u_i)},\end{aligned}$$

则对于攻击者 A 来说,由算法 B 所产生的某个身份 u 的密钥与 *challenger* 所产生密钥是不可区分的.

若 $F(u)=0 \bmod p$,上述算法 B 不能进行,模拟过程终止.

为了分析模拟算法概率方便,将 $F(u)\ne 0 \bmod l_u$ 作为伪造成功密钥的条件(因为参数设置中假定 $0\le l_u(n_u+1)<p$, $0\le k_u\le n_u$, $F(u)=x'+\sum_{i\in U}x_i-l_uk_u$,所以 $0\le l_u(n_u+1)<p\Rightarrow 0\le l_uk_u<p$, $0\le x'+\sum_{i\in U}x_i<p$,则容易得出 $F(u)=0 \bmod p\Rightarrow F(u)=0 \bmod l_u$,所以 $F(u)\ne 0 \bmod l_u\Rightarrow F(u)\ne 0 \bmod p$,将 $F(u)\ne 0 \bmod l_u$ 作为伪造密钥成功的条件).

2.签名询问(Sign Queries):考虑一个身份 u 对于一个消息 m 的签名询问.当 $K(m)\ne 0 \bmod p$ 时,随机选择 $s\in Z_p$, $t\in Z_p$,计算:

$$\begin{aligned}\sigma=(w,x,y)&=(g_2^{t(u'+\sum_{i\in U}u_i)}g_1^{-\frac{L(m)}{K(m)}}(m'\prod_{j\in M}m_j)^s, g^sg_1^{-\frac{1}{K(m)}}, z_2^t)\\&=(g_2^{t(u'+\sum_{i\in U}u_i)}g_2^a(m'\prod_{j\in M}m_j)^{s'}, g^{s'}, z_2^t),\text{其中 } s'=s-\frac{a}{K(m)}.\end{aligned}$$

算法 B 将 $\sigma=(w,x,y)$ 发送给攻击者 A, A 对其进行

验证：

$$e(g,w)=e\left(g,g_2^{t(u'+\sum_{i\in U}u_i)}g_2^{a}\left(m'\prod_{j\in M}m_j\right)^{s'}\right)$$
$$=e(g,g_2)^{t(u'+\sum_{i\in U}u_i)}\cdot e(g_1,g_2)\cdot e\left(g^{s'},\left(m'\prod_{j\in M}m_j\right)\right)$$
$$=y^{(u'+\sum_{i\in U}u_i)}\cdot z_1\cdot e\left(x,\left(m'\prod_{j\in M}m_j\right)\right).$$

可以看出，对于攻击者 A 来说，由算法 B 所产生的某个身份 u 对某个消息 m 的签名与 *challenger* 所产生的真正签名是不可区分的.

当 $K(m)=0 \bmod p$ 时，上述算法 B 不能进行，模拟过程终止.类似于密钥询问中的处理，将 $K(m)\neq 0 \bmod l_m$ 作为伪造签名成功的条件.

伪造(Forgery). 若算法 B 在上述询问阶段没有终止，则攻击者 A 至少以概率 ε 成功伪造身份为 u^* 的用户对消息 m^* 的有效签名 $\sigma^*=(w^*,x^*,y^*)$，其中 $w^*=g_2^{a+t^*(u'+\sum_{i\in U}u_i)}\cdot\left(m'\prod_{j\in M}m_j\right)^{s^*}$，$x^*=g^{s^*}$，$y^*=z_2^{t^*}$，且 A 对身份 u^* 没有做过密钥询问，对消息 m^* 没有做过签名询问. 当 $K(m^*)\neq 0 \bmod p$ 或 $F(u^*)\neq 0 \bmod p$ 时，算法 B 停止；当 $K(m^*)=0 \bmod p$ 且 $F(u^*)=0 \bmod p$ 时，算法 B 计算：

$$\frac{w^*}{(x^*)^{L(m^*)}}=\frac{g_2^{a+t^*(u'+\sum_{i\in U}u_i)}\cdot\left(m'\prod_{j\in M}m_j\right)^{s^*}}{g^{L(m^*)\cdot s^*}}=g_2^{a}=g^{ab},$$

即为 CDH-问题的输出.

上述算法描述了算法 B 的模拟过程，下面分析算法 B 模拟成功的概率. 因为需要完整的运行整个模拟算法，才能解决 CDH-问题，所以在密钥询问、签名询问和伪造签名的时候，算法 B 均不能终止. 从上述算法知，要使得算法 B 不终止需满足 3 个条件：

(1) 密钥询问成功 $F(u_i)\neq 0 \bmod l_u$；

(2) 签名询问成功 $K(m_i)\neq 0 \bmod l_m$；

(3) 伪造签名成功 $K(m^*)=0 \bmod p, F(u^*)=0 \bmod p$.

为了方便下面计算，定义 $A_i: F(u_i)\neq 0 \bmod l_u$，$A^*: F(u^*)=0 \bmod p$，$B_i: K(m_i)\neq 0 \bmod l_m$，$B^*: K(m^*)=0 \bmod p$. 则算法 B 模拟成功的概率为 $P(\neg abort)\geq P(\bigcap_{i=1}^{q_e+q_s}A_i\wedge A^*\wedge\bigcap_{j=1}^{q_s}B_j\wedge B^*)$.

$$P(A^*)=P(F(u^*)=0 \bmod p\wedge F(u^*)=0 \bmod l_u)$$
$$=P(F(u^*)=0 \bmod l_u)\cdot P(F(u^*)$$
$$=0 \bmod p\mid F(u^*)=0 \bmod l_u)=\frac{1}{l_u}\cdot\frac{1}{n_u+1}.$$

因为事件 A_i、A^* 是独立的，则

$$P(\bigcap_{i=1}^{q_E+q_S}A_i\wedge A^*)=P(A^*)P(\bigcap_{i=1}^{q_E+q_S}A_i)$$
$$=P(A^*)\cdot(1-P(\bigcup_{i=1}^{q_E+q_S}\neg A_i))$$
$$\geq\left(\frac{1}{l_u}\cdot\frac{1}{n_u+1}\right)\left(1-\frac{q_E+q_S}{l_u}\right),$$

而 $l_u=2(q_E+q_S)$，则

$$P(\bigcap_{i=1}^{q_E+q_S}A_i\wedge A^*)\geq\frac{1}{4(q_E+q_S)(n_u+1)};$$

类似处理，求得 $P(\bigcap_{j=1}^{q_S}B_j\wedge B^*)\geq\frac{1}{4q_S(n_m+1)}$. 则

$$P(\neg abort)\geq P(\bigcap_{i=1}^{q_E+q_S}A_i\wedge A^*\wedge\bigcap_{j=1}^{q_S}B_j\wedge B^*)$$
$$\geq\frac{1}{16(q_E+q_S)q_S(n_u+1)(n_m+1)},$$

即 $\varepsilon'=\frac{\varepsilon}{16(q_E+q_S)q_S(n_u+1)(n_m+1)}$.

若模拟算法 B 没有终止，攻击者 A 可以以概率 ε 伪造出一个有效签名，并且算法 B 可以通过伪造的签名来计算得到 g^{ab}.

算法 B 运行时间是由签名询问中的乘法运算时间、指数运算时间来决定的，可以容易看出算法 B 的时间复杂度为

$$t'=t+O(q_E n_u+q_S(\rho\cdot n_m+\tau\cdot n_u)+q_S\tau).$$

则上述算法 B 在不多于 t' 的时间内，以概率 ε' 成功解决了 CDH 困难问题，这与 (ε',t')-CDH 假定相矛盾，所以本文的方案是安全的.

5 方案比较

将 Paterson 和 Schuldt 方案[19] 简称为 PS 方案，在 PS 方案中，由于 $e(g_1,g_2)$ 可以进行预计算，所以在计算验证计算量时，略去这个部分的计算量. 由表 1 可以看出：本文方案的验证算法计算量减小了一个 e 运算的计算量(因为指数运算的计算量相对于 e 运算的计算量可以忽略不计). 本文方案与 PS 方案比较结果如下.

表 1 计算量与通信量比较

方案	签名长度	签名计算量	验证计算量
PS 方案	$3\|G\|$	$2Exp$	$3E$
本文方案	$2\|G\|+\|G_T\|$	$2Exp$	$2E+Exp$

表 1 中各个符号的定义如表 2 所示.

表 2 符号定义

符号	定义
$\|G\|$	G 中元素的长度
$\|G_T\|$	G_T 中元素的长度
Exp	指数运算的计算量
E	e 运算的计算量

注. 在上述签名方案中,签名为 $\sigma=(w,x,y)=\left(d_0\cdot\left(m'\prod_{j\in M}m_j\right)^s,g^s,d_1\right)$,其中的 $y=e(g,g_2)^t=d_1$ 作为签名和用户密钥的一部分始终是不变的,主要用于验证则用户密钥和签名的有效性,因此可将这部分签名作为系统参数的一部分公开,即签名为 $\sigma=(w,x)=\left(d_0\cdot\left(m'\prod_{j\in M}m_j\right)^s,g^s\right)$,从而通信代价比原来减小了三分之一.

6　结束语

本文利用 Waters 方法,基于 PS 方案,提出一种在标准模型下安全的基于身份的高效签名方案. 证明过程中的攻击模型和困难问题假设均没有变化,这说明本文的方案和 PS 方案具有同样的安全性. 从上述方案比较可以看到:本文方案的通信代价和签名算法计算量与 PS 方案相当,本文方案将 PS 方案的验证算法的计算量减小了三分之一. 在实际使用中可以将签名中始终不变的部分作为系统参数的一部分公开,签名长度可以减小三分之一. 在这种情况下,本文方案的签名长度与 Boneh 和 Boyen 提出的短签名[21]长度相当,验证算法的计算量比他们的方案多一个 e 运算. 但是 Boneh 和 Boyen 方案的安全性规约为非标准的强 Diffie-Hellman 假定,而本文方案的安全性可规约为经典的计算 Diffie-Hellman 假定. 本文方案的主要缺点是 PKG 的系统参数过长(文献[18-19]也有同样的问题),事实上,PKG 的系统参数 *params* 中的 g_1,g_2 是为了证明的需要,实际应用时可以省略,可以略微缩短 PKG 系统参数的长度. 正如文献[19]所指出的那样,本文可以使用文献[22]①的方法对方案进行改进,进一步减少 PKG 系统参数的长度. 本文提出的方案可用于构造安全、高效的基于证书的签名和加密方案以及无证书的签名方案[23-27].

参　考　文　献

[1] Shamir A. Identity-based cryptosystems and signature schemes//Proceedings of the CRYPTO'1984. Santa Barbara, CA, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//Proceedings of the CRYPTO'2001. LNCS 2139. Springer-Verlag, 2001: 213-229

[3] Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing//Proceedings of the Symposium on Cryptography and Information Security (SCIS'2000). 2000: 26-28

[4] Paterson K G. ID-based signatures from pairings on elliptic curves. Cryptology ePrint Archive, Report 2002/003, 2002

[5] Chen X, Zhang F, Kim K. A new ID-based group signature scheme from bilinear pairings//Proceedings of the WISA'2003. LNCS 2908. Springer-Verlag, 2003: 585-592

[6] Hess F. Efficient identity based signature schemes based on pairings//Proceedings of the SAC'2002. LNCS 2595. Springer-Verlag, 2003: 310-324

[7] Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups//Proceedings of the PKC'2003. LNCS 2567. Springer-Verlag, 2003: 18-30

[8] Yi X. An identity-based signature scheme from the Weil pairing. IEEE Communications Letters, 2003, 7(2): 76-78

[9] Yoon H, Cheon J H, Kim. Y. Batch verifications with ID-based signatures//Proceedings of the ICISC'2004. LNCS 3506. Springer-Verlag, 2005: 233-248

[10] Li Jin, Zhang Fang-Guo, Wang Yan-Ming. Two efficient hierarchical identity based signature schemes. Acta Electronic Sinica, 2007, 35(1): 150-152(in Chinese)
(李进, 张方国, 王燕鸣. 两个高效的基于分级身份的签名方案. 电子学报, 2007, 35(1): 150-152)

[11] Bellare M, Rogoway P. Random oracles are practical: A paradigm for designing efficient protocols//Proceedings of the 1st Conference on Computer and Communications Security. ACM, 1993: 62-73

[12] Canetti R, Goldreich O, Halevi S. The random oracle methodology, Revisited (preliminary version)//Proceedings of the 30th Annual ACM Symposium on the Theory of Computing (STOC'98). ACM, New York, 1998: 209-218

[13] Bellare M, Boldyreva A, Palacio A. A uninstantiable random oracle-model scheme for a hybrid-encryption problem//Cachin C, Camenisch J eds. EUROCRYPT'2004. LNCS 3027. Springer, 2004: 171-188

[14] Feng Deng-Guo. Research on theory and approach of provable security. Journal of Software, 2005, 16(10): 1743-1756 (in Chinese)
(冯登国. 可证明安全性理论与方法研究. 软件学报, 2005, 16(10): 1743-1756)

[15] Wang Sheng-Bao, Cao Zhen-Fu, Dong Xiao-Lei. Provably secure identity-based authenticated key agreement protocols in the standard model. Chinese Journal of Computers, 2007, 30(10): 1842-1852(in Chinese)
(王圣宝, 曹珍富, 董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议. 计算机学报, 2007, 30(10): 1842-1852)

[16] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles//Cachin C, Camenisch J eds. EUROCRYPT'2004. LNCS 3027. Springer, 2004: 223-238

[17] Boneh D, Boyen X. Secure identity based encryption without random oracles//Franklin M K ed. CRYPTO'2004. LNCS 3152. Springer, 2004: 443-459

① Naccache D. Secure and practical identity-based encryption. Cryptology ePrint Archive, Report 2005/369, 2005. http://eprint.iacr.org/

[18] Waters B. Efficient identity-based encryption without random oracles//Cramer R ed. EUROCRYPT'2005. LNCS 3494. Springer, 2005: 114-127

[19] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model//Proceedings of the ACISP'2006. LNCS 4058. Springer-Verlag, 2006: 207-222

[20] Goldwasser S, Micali S, Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 1988, 17(2): 281-308

[21] Boneh D, Boyen X. Short signatures without random oracles//Cachin C, Camenisch J eds. EUROCRYPT'2004. LNCS 3027. Springer, 2004: 56-73

[22] Chatterjee S, Sarkar P. Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model//Won D, Kim S eds. ICISC'2005. LNCS 3935. Springer, 2006: 424-440

[23] Li J G, Huang X Y, Mu Y, Susilo W, Wu Q H. Certificate-based signature: Security model and efficient construction//Proceedings of the EuroPKI'2007. LNCS 4582. Springer-Verlag, 2007: 110-125

[24] Kang B G, Park J H, Hahn S G. A certificate-based signature scheme//Proceedings of the CT-RSA'04. LNCS 2964. Springer-Verlag, 2004: 99-111

[25] Wang L H, Shao J, Cao Z F, Mambo M, Yamamura A. A certificate-based proxy cryptosystem with revocable proxy decryption power//Proceedings of the Indocrypt'2007. LNCS 4859. Springer-Verlag, 2007: 297-311

[26] Li J G, Huang X Y, Mu Y, Wu W. Cryptanalysis and improvement of an efficient certificateless signature scheme. Journal of Communications and Networks, 2008, 10(1): 10-17

[27] Lu Y, Li J G, Xiao J M. Constructing efficient certificate-based encryption with paring. Journal of Computers, 2009, 4(1): 19-26

LI Ji-Guo, born in 1970, Ph. D., professor. His main research interests include information security and cryptography theoryand technology.

JIANG Ping-Jin, born in 1984, M. S.. His current research interests focus on cryptography theoryand technology.

Background

This research is supported by the National Natural Science Foundation of China under grant No. 60673070, the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z409, the Project of Jiangsu Province Police Ministry under grant No. 200503002, and Program for New Century Excellent Talents in Hohai University.

The concept of Identity-Based Cryptography (IBC) was proposed by Shamir in 1984. In an IBC system, the master secret is generated by a trusted authority, which we call the Private Key Generator (PKG), and the key generation mechanism is called an identity-based key extraction algorithm. Shamir's original motivation for identity-based encryption was to simplify certificate management in e-mail systems. Nowadays, identity-based signature (IBS) has been discussed in the application of securing IPv6 neighbor and router discovery. However, improving the efficiency of IBS scheme is still an interesting research topic, which is one of the authors' motivations.

Another motivation of our research is to find an efficient and provably secure identity-based signature in the standard model (without random oracle model). Towards this goal, several recent results construct IBE systems secure without random oracles in weaker versions of the Boneh-Franklin model. However, building a fully secure IBE remained open problem three years ago. In Eurocrypt'2005, Waters presented the first efficient IBE scheme that was fully secure without random oracles and reduced the security of his scheme to the decisional bilinear Diffie-Hellman (BDH) problem, which solved the open problem proposed by Boneh and Boyen. Additionally, he showed that his techniques can be used to build a new signature scheme that is secure under the computational Diffie-Hellman assumption without random oracles. The only known construction of identity-based signatures that can be proven secure in the standard model is based on the approach of attaching certificates to non-identity-based signatures. This folklore construction method leads to schemes that are somewhat inefficient and leaves open the problem of finding more efficient direct constructions. Paterson and Schuldt presented an efficient identity-based signatures secure in the standard model in 2006. Based on Waters' techniques, the authors propose an efficient identity-based signature scheme in the paper. The scheme is existentially unforgeable against adaptive chosen message attacks under the computational Diffie-Hellman assumption in the standard model. Compared with the known identity-based scheme secure in the standard model, the proposed scheme enjoys shorter signature length and less operation.