计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
48(8): 1357-1362, 2011

标准模型下一种新的基于分级身份的短签名方案

吴 青[1] 张乐友[2] 胡予濮[3]
[1](西安邮电学院自动化学院 西安 710121)
[2](西安电子科技大学数学系 西安 710071)
[3](计算机网络与信息安全教育部重点实验室(西安电子科技大学) 西安 710071)
(xidianwq@yahoo.com.cn)

A New Construction of Short Hierarchical Identity-Based Signature in the Standard Model

Wu Qing[1], Zhang Leyou[2], and Hu Yupu[3]
[1](*School of Automation, Xi'an Institute of Posts and Telecommunications, Xi'an* 710121)
[2](*Department of Mathematics, Xidian University, Xi'an* 710071)
[3](*Key Laboratory of Computer Networks and Information Security* (*Xidian University*), *Ministry of Education, Xi'an* 710071)

Abstract Hierarchical identity based signature (HIBS) has wide application in large scale networks. However, the existing work cannot solve the trade-off between security and efficiency. The main challenge at present is to construct a high efficient and strongly secure HIBS with low computation cost. To overcome the drawbacks in the previous work, a new hierarchical identity-based signature scheme is introduced. The proposed scheme has some advantages over the available. For examples, the private keys size shrinks as the identity depth increases, the signature only consists of three group elements and three bilinear pairs are needed in verifying algorithm, which are independent of hierarchy depth. Furthermore, the security of the new scheme is based on the general selective-identity security model(Gs-ID) which is a general security model based on full security model and selective identity model. Under the h-computational Diffie-Hellman exponent problem (h-CDH) assumption, our scheme is proven to be secure against Gs-ID and adaptive chosen message attack. In addition, the security analysis does not rely on the random oracles. The assumption in our scheme is more natural than many of the hardness assumptions recently introduced to HIBS in the standard model, which solves the trade-off between the security and computation efficiency.

Key words hierarchical identity-based signature; standard model; h-CDH problem; provably secure; general selective-identity security model

摘 要 基于分级身份的签名在大规模网络中具有重要应用前景,为克服已有方案的私钥或签名长度依赖于分级级数及最大分级级数的缺陷,提高计算效率,提出了一种新的基于分级身份的签名方案.与已有方案相比,新方案优势明显,如身份分级级数越大,私钥长度越短,且签名长度为常数,仅含有3个群元素.验证算法仅需要3个双线性对运算,同样不依赖于分级级数.另外,新方案的安全性建立在推广的选择身份安全模型,该模型为适应性选择身份安全模型及选择身份安全模型的推广,在计算h-CDH困难假设下,新方案被证明是安全存在性不可伪造的,且其安全性不依赖于随机预言机.与已有的标准模型

收稿日期:2011-04-07;**修回日期**:2011-06-24
基金项目:国家自然科学基金项目(60970119,60803149);国家"九七三"重点基础研究计划基金项目(2007CB311201);陕西省自然科学基金项目(2010JQ8004)

下的分级方案相比,新方案的安全性基于的困难假设更具有一般性.

关键词 基于分级身份的签名;标准模型;h-CDH 问题;可证明安全;推广的选择身份安全模型

中图法分类号 TP309

基于身份的加密在文献[1]中首次被提出.它允许用户可以利用接收者的身份作为公钥加密,避免了公钥证书的分发,因此简化了公钥密码的应用,是目前研究的热点之一[2-4].基于分级身份加密体制是上述加密体制的推广[5],它的优势是一个根节点 PKG(root PKG)将私钥构造与身份验证的工作量分配给低级的 PKGs 承担.一个 k 级的身份可以为其子身份($k+1$ 级)产生私钥,却不能为其他身份解密.第 1 个有效的分级加密方案是由 Gentry 和 Silverberg 提出的[5],在随机预言机模型下,其安全性规约到判定型双线性 Diffie-Hellman(DBDH)问题.第 1 个标准模型下的分级加密方案由 Boneh 与 Boyen 在 2004 年提出[6].基于分级身份的签名方案由 Gentry 和 Silverberg 在 2002 年提出[5].第 1 个可证明安全的方案是由 Chow 等人提出的[7],但是其安全性证明是在随机预言机模型下得到的.Yuen 与 Wei 在文献[8]中提出了一个标准模型下的方案,其签名长度与分级级数无关,但其安全性却依赖于一个强的假设 OrcYW 假设.另外,在文献[9-10]中,也提出了 2 种标准模型下的方案,然而安全性是基于一个强的困难问题假设——q-SDH 问题.不仅如此,Hu 等人在文献[11]中指出这 2 种方案存在安全缺陷.2006 年,李进等人[12]基于文献[13]提出了一种新方案,尽管具有很好的效率,然而该方案的安全证明基于随机预言机;随后他们提出了 2 种基于分级身份的签名方案[14],这 2 种方案的安全性证明都依赖于随机预言机,其中第 1 种方案虽然基于 CDH 问题,但签名长度随着分级层数的增加而增加,第 2 种方案的签名长度为常数,但基于的困难问题不具有一般性.2008 年,张乐友等人在文献[15]中提出了一种基于 Gs-ID 的方案,其签名长度随着分级级数的增加而线性增加,随后在文献[16]中他们又提出了一种有效方案,该方案基于 h-CDH 问题,并且达到了强安全性——full security,不足之处是公钥长度达到了$(l+1)h+t+3$,最近他们又提出了另外一种有效方案[17],虽然解决了文献[16]公钥的长度过大的问题,然而,安全性却依赖于一个强的假设 q-SDH 问题.

本文给出了一种有效的标准模型下的基于分级身份的签名方案,本方案的安全性基于 h-CDH 问题,该问题在 $h=1$ 时等价于 CDH 问题.然而随着分级级数的增加,私钥长度随之缩减,并且,新方案的签名长度不依赖于分级级数,这一点比基于证书或分层认证树下的方案有效得多.不仅如此,该方案所依赖的安全模型为一般的安全模型——Gs-ID,它是适应性选择身份安全模型及选择身份安全模型的一般形式,因而比已有的标准模型下的方案在安全性上更具有一般性.

1 预备知识

1.1 双线性对

设 G,G_1 为素数阶 p 的循环群,g 为 G 的生成元,则双线性映射 $\hat{e}:G\times G\to G_1$ 具有如下性质:

1) 双线性性.对所有的 $u,v\in G,a,b\in\mathbb{Z}_p$,都有 $\hat{e}(u^a,v^b)=\hat{e}(u,v)^{ab}$.

2) 非退化性.$\hat{e}(g,g)\neq 1$.

3) 实效性.对于任意 $u,v\in G$,$\hat{e}(u,v)$是实际有效可计算的.

1.2 h-CDH 问题

定义 1. h-CDH(h-exponent computational Diffie-Hellman problem).设 G 为一阶数是素数 p 的群,g 为其任一生成元,h-CDH 问题定义为:已知元素 g^a,$g^{a^2},\cdots,g^{a^h}$,计算 $g^{a^{h+1}}$,其中 $h\geqslant 1,a\in\mathbb{Z}_p$.

文献[18]中指出,当 $h=1$ 时,该问题等价于 CDH 问题.

定义 2. 如果没有敌手在多项式时间 t 内以不可忽略的优势 ε 解决 h-CDH 问题,则称(t,ε) h-CDH 困难假设成立.

1.3 分级签名方案

系统建立:输入安全参数,输出系统参数与主密钥.

私钥提取:输入一个身份 $\boldsymbol{ID}=(v_1,v_2,\cdots,v_j)$,公共参数以及对应于上一级身份 $\boldsymbol{ID}_{j-1}=(v_1,v_2,\cdots,v_{j-1})$的私钥 $\boldsymbol{d}_{ID_{j-1}}$,输出对应于 $\boldsymbol{ID}$ 的私钥 $\boldsymbol{d}_{ID}$.如果 $j=1$,此时私钥由根 PKG 产生.

签名:给定消息 $\boldsymbol{M}$ 和接收者的身份信息 $\boldsymbol{ID}$ 以及私钥 $\boldsymbol{d}_{ID}$,产生相应的签名.

验证:给定签名和用户身份,如果它是一个有效签名,输出 1,否则输出 0.

1.4　存在性不可伪造性安全模型

基于身份的密码存在着 2 种主要的安全模型:

1) 适应性选择身份安全模型,攻击者可以适应性地选择要攻击的身份.

2) 选择身份安全模型,攻击者必须在游戏开始前提供要攻击的身份对象,显然比 Full 安全模型要弱一些.

文献[14]提出了 2 种推广的模型 $\boldsymbol{M}_1$ 与 $\boldsymbol{M}_2$,本文只用到 $\boldsymbol{M}_2$,现将其修改以适合签名方案,叙述如下.

初始化:敌手提供要攻击的对象集合:$\boldsymbol{I}_1^*,\cdots,\boldsymbol{I}_j^*$,其中 $1\leqslant j\leqslant h$,h 是最大层数,设 $|\boldsymbol{I}_i^*|=n_i$,$\boldsymbol{I}_i^*$ 对应于第 i 层的身份集合.

系统建立:模拟者产生系统参数并发给敌手.

询问:此阶段敌手要进行私钥提取询问与签名询问.注意,此阶段进行询问的身份$(v_1,\cdots,v_j)$满足 $v_i\notin\boldsymbol{I}_i^*$,$1\leqslant i\leqslant j$.

伪造:敌手利用身份 $\boldsymbol{ID}^*=(v_1^*,\cdots,v_j^*)$输出一个关于消息 $\boldsymbol{M}^*$ 的签名 $\boldsymbol{\sigma}^*$,其中 $v_i^*\in\boldsymbol{I}_i^*$,$\boldsymbol{ID}^*$ 或其任何一级父代身份没有进行私钥提取询问,$(\boldsymbol{ID}^*,\boldsymbol{M}^*)$没有进行签名询问.

注意:如果 $n_1=n_2=\cdots=n_l=1$,则 $\boldsymbol{M}_2$ 即为 Selective-ID 安全模型.

如果满足 $Valid=Verify(\boldsymbol{ID}^*,\boldsymbol{M}^*,\boldsymbol{\sigma}^*)$,则敌手获胜,详细的描述见文献[13-15].

2　新签名方案的构造

2.1　新方案构造

系统建立:设最大分级数为 h,随机选取 G 的一个生成元 g 与一些元素 $h_{ij},g_2,g_3,u_0,u_l\in G$,其中 $i=1,\cdots,h$,$j=1,\cdots n_i$,$l=1,\cdots,n_M$.继续随机选取 $\alpha\in\mathbb{Z}_p$,计算 $g_1=g^\alpha$.设 $\boldsymbol{H}_i=(h_{ij})$及 $\boldsymbol{U}=(u_l)$,最后输出公共参数 $param$ 为:

$$param=(g,g_1,g_2,g_3,u_0,\boldsymbol{H}_1,\cdots,\boldsymbol{H}_h,\boldsymbol{U}),$$

主密钥为 g_2^α.

私钥提取:输入 $j-1$ 代的身份 $\boldsymbol{ID}_{j-1}=(v_1,v_2,\cdots,v_{j-1})$及对应的私钥 $\boldsymbol{d}_{ID_{j-1}}=(d_0',d_1',d_j',\cdots,d_h')$,第 j 代的身份 $\boldsymbol{ID}=(v_1,v_2,\cdots,v_j)$,$v_i\in\mathbb{Z}_p$.对应的私钥 $\boldsymbol{d}_{ID}=(d_0,d_1,d_{j+1},\cdots,d_h)$ 可由如下方式产生:设 $d_0'=g_2^\alpha(g_3\prod_{i=1}^{j-1}F_i(v_i))^r$,$d_1'=g^r$,$\boldsymbol{d}_t'=\boldsymbol{H}_t^r=(h_{ti}^r)=(D_{ti})$,$i=1,\cdots,n_i$,$t=j,\cdots,h$,其中 $\bar{r}\in\mathbb{Z}_p$,$F_i(x)=\prod_{j=1}^{n_i}h_{ij}^{x^j}$,$i=1,\cdots,h$.随机选取 $r'\in\mathbb{Z}_p$,计算:

$$d_0=d_0'\prod_{k=1}^{n_j}D_{jk}^{v_j^k}(g_2\prod_{i=1}^{j}F_i(v_i))^{r'},$$

$$d_1=d_1'g^{r'},\boldsymbol{d}_t=\boldsymbol{d}_t'\boldsymbol{H}_t^{r'}=(h_{tj}^{\bar{r}+r'}),$$

其中 $t=j+1,\cdots,h$,设 $r=r'+\bar{r}$,由此可得

$$\boldsymbol{d}_{ID}=(d_0,d_1,d_{j+1},\cdots,d_h)=$$

$$(g_2^\alpha(g_3\prod_{i=1}^{j}F_i(v_i))^r,g^r,\boldsymbol{H}_{j+1}^r,\cdots,\boldsymbol{H}_h^r).$$

签名:设待签信息为 $\boldsymbol{M}=(m_1,\cdots,m_{n_M})$,$m_i\in\mathbb{Z}_p$,随机选取 $s\in\mathbb{Z}_p$,计算签名如下:

$$\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\sigma_3)=(d_0(u_0\prod_{i=1}^{n_M}u_i^{m_i})^s,d_1,g^s).$$

验证:设消息 $\boldsymbol{M}$ 关于身份 $\boldsymbol{ID}$ 的签名为 $\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\sigma_3)$,验证者首先计算 $F_i(v_i)$,然后验证如下等式是否成立:

$$\hat{e}(\sigma_1,g)=\hat{e}(g_1,g_2)\hat{e}(g_3\prod_{i=1}^{j}F_i(v_i),\sigma_2)$$

$$\hat{e}(u_0\prod_{i=1}^{n_M}u_i^{m_i},\sigma_3),$$

如果成立则接受,否则拒绝.

2.2　有效性

公共参数与已有的方案相比,略有增加,然而由 2.1 节可看到,新方案的私钥长度随着身份级数的增加而减小,并且签名长度为一常数,仅仅含有 3 个群元素.由于双线性对 $\hat{e}(g_1,g_2)$可以预先计算,所以验证算法仅需 3 个双线性对运算,这一点是非常有效的.另外,新方案的安全性基于 h-CDH 困难假设而不是其他更强的假设,并且其安全性证明不依赖于随机预言机.表 1 给出了几种方案的效率比较.

Table 1　Comparison of Efficiency

表 1　效率比较

Scheme	Hardness	Security Model	Random Oracle	Signature Size	Pair
Ref[7]	CDH	s-ID	YES	$(k+2)\|G\|$	3
Ref[8]	orcYW	s-ID	NO	$4\|G\|$	7
Ref[12]	CDH	Gs-ID	YES	$(k+2)\|G\|$	$k+2$
Ref[14]1st	CDH	s-ID	YES	$O(l)\|G\|$	$l+2$
Ref[14]2nd	l-BDHE	s-ID	YES	$3\|G\|$	3
Ref[15]	DHI	s-ID	NO	$(k+2)\|G\|$	$k+2$
Ref[16]	h-CDH	Full	YES	$3\|G\|$	4
Ref[17]	q-SDH	Full	YES	$5\|G\|+p$	4
Ours	h-CDH	Gs-ID	NO	$3\|G\|$	3

注意:在表 1 中,s-ID 表示 selective-identity[6] 安全性,Gs-ID 表示推广的 selective-identity 模型,Full 表示 Full 安全性.

3 安全性分析

3.1 正确性

设 $\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\sigma_3)$ 是一个有效的签名,则有

$$\hat{e}(\sigma_1,g)=\hat{e}(d_0(u_0\prod_{i=1}^{n_M}u_i^{m_i})^s,g)=$$

$$\hat{e}(g_2^{\alpha}(g_3\prod_{i=1}^{j}F_i(v_i))^r(u_0\prod_{i=1}^{n_M}u_i^{m_i})^s,g)=$$

$$\hat{e}(g_2^{\alpha},g)\hat{e}((g_3\prod_{i=1}^{j}F_i(v_i))^r,g)\hat{e}((u_0\prod_{i=1}^{n_M}u_i^{m_i})^s,g)=$$

$$\hat{e}(g_1,g_2)\hat{e}(g_3\prod_{i=1}^{j}F_i(v_i),\sigma_2)\hat{e}(u_0\prod_{i=1}^{n_M}u_i^{m_i},\sigma_3).$$

3.2 存在性不可伪造

设 q_e 与 q_s 表示允许敌手进行的私钥提取与签名最大次数,$n=\sum_{i=1}^{h}n_i$,则有:

定理 1. 如果 (t',ε')-CDH 假设成立,则新方案是 (t,q_e,q_s,ε) 安全的,且有 $\varepsilon\leqslant\varepsilon'$,$t'=t+O((q_e n+q_s(n+n_M))\rho+(nq_e+q_s)\tau)$,其中 t 表示敌手所用的最长多项式时间,ρ 表示乘法运算所需时间,τ 表示指数运算时间.

证明. 设存在一个 (t,q_e,q_s,ε),敌手 A 能攻破新方案,则利用 A 可构造一算法 B 解决 (t',ε')-CDH 问题.下面所用方法来源于文献[13,19],具体构造如下:

初始化.敌手提供要攻击的身份集合:$\boldsymbol{I}_1^*,\cdots,\boldsymbol{I}_j^*$,$1\leqslant j\leqslant h$.

系统建立.B 随机选取 $v_0,z_0,m_i,x_i,y_i\in\mathbb{Z}_p$,$1\leqslant i\leqslant n_M$,并设 $\boldsymbol{M}=(m_i)$,$\boldsymbol{X}=(x_i)$,$\boldsymbol{Y}=(y_i)$,构造如下函数:

$$f_i(x)=\begin{cases}\prod_{v\in\boldsymbol{I}_i^*}(x-v)=\sum_{j=1}^{n_i}a_{ij}x^j, & 1\leqslant i\leqslant j;\\ x, & j+1\leqslant i\leqslant h;\end{cases}$$

$$J_i(x)=b_{i,n_i}x^{n_i}+b_{i,n_i-1}x^{n_i-1}+\cdots+b_{i,1}x+b_{i,0};$$

$$f(\boldsymbol{M})=p+v_0+\sum_{i=1}^{n_M}x_im_i;$$

$$J(\boldsymbol{M})=z_0+\sum_{i=1}^{n_M}m_iy_i;$$

其中 $a_{ij},b_{ij}\in\mathbb{Z}_p$,$1\leqslant i\leqslant h$,$1\leqslant j\leqslant n_i$,$x\in\mathbb{Z}_p^*$.注意系数 a_{ij},当 $1\leqslant i\leqslant j$ 时,$a_{in_i}=1$;当 $j+1\leqslant i\leqslant h$,$l\neq 1$ 时,$a_{il}=0$,而 $a_{i1}=1$.

接下来,B 要构造系统公共参数.首先,给定 h-CDH 数组 $\{g,Y_1,Y_2,\cdots,Y_h\}$,其中 g 是 G 的生成元,$Y_i=g^{\alpha^i}$,$\alpha\in\mathbb{Z}_p$.B 的目的是在游戏结束时,能解决 h-CDH 问题,即能计算 $g^{\alpha^{h+1}}$.为此,B 首先选取一 $\beta\in\mathbb{Z}_p$,然后置

$$g_1=Y_1=g^{\alpha},g_2=Y_hg^{\beta}=g^{\alpha^h+\beta},$$

$$g_3=\prod_{i=1}^{h}(g^{b_{i0}}Y_{h-i+1}^{a_{i0}}),$$

对 $1\leqslant i\leqslant h$,$1\leqslant j\leqslant n_i$,定义

$h_{ij}=g^{b_{ij}}Y_{h-i+1}^{a_{ij}}$,$u_0=g_2^{p+v_0}g^{z_0}$,$u_k=g_2^{x_k}g^{y_k}$,$1\leqslant k\leqslant n_M$.最后,$B$ 将公共参数 $param=(g,g_1,g_2,g_3,u_0,\boldsymbol{H}_1,\cdots,\boldsymbol{H}_h,\boldsymbol{U})$ 发送给 A,而主密钥 g_2^{α},B 是不知道的.

询问:A 将进行私钥提取询问与签名询问,B 作相应的回答如下.

私钥提取询问:设敌手对身份 $\boldsymbol{ID}=(v_1,\cdots,v_j)$ 进行私钥提取询问,其中 $j\leqslant h$.B 首先检测是否存在 $k\in\{1,\cdots,j\}$,使得 $f_k(v_k)\neq 0$,如果没有,B 则停止游戏.事实上,必有 $k\in\{1,\cdots,j\}$,使得 $f_k(v_k)\neq 0$,否则必有 $v_i\in\boldsymbol{I}_i^*$,这与前面的安全模型的定义矛盾.利用此 k,B 将为身份 $\boldsymbol{ID}$ 构造一个有效的私钥,详细叙述如下(方法来源于文献[13,19],有些推导在此省略):任意选取 $r\in\mathbb{Z}_p$,定义

$$A_1=Y_1^{\beta}(\prod_{i=1}^{j}Y_k^{J_i(v_i)})^{-\frac{1}{f_k(v_k)}}(\prod_{i=1}^{j}Y_{h-i+1}^{f_i(v_i)}g^{J_i(v_i)})^r;$$

$$A_2=(\prod_{i=1,i\neq k}^{j}Y_{h+k-i+1}^{f_i(v_i)})^{-\frac{1}{f_k(v_k)}};$$

$$A_3=\prod_{i=j+1}^{h}((g^{b_{i0}}Y_{h-i+1}^{a_{i0}})^r(Y_k^{b_{i0}}Y_{h+k-i+1}^{a_{i0}})^{-\frac{1}{f_k(v_k)}});$$

则有

$$d_0=A_1A_2A_3=Y_{h+1}Y_{h+1}^{-1}A_1A_2A_3=$$

$$g_2^{\alpha}(g_3\prod_{i=1}^{j}F_i(v_i))^{r-\frac{k}{f_k(v_k)}}=g_2^{\alpha}(g_3\prod_{i=1}^{j}F_i(v_i))^{r'}$$

及 $d_1=Y_k^{-\frac{1}{f_k(v_k)}}g^r=g^{r-\frac{\alpha k}{f_k(v_k)}}=g^{r'}$.

为了得到有效的 $\boldsymbol{H}_i^r=(h_{i1}^r,\cdots,h_{in_i}^r)$,$j+1\leqslant i\leqslant h$.$B$ 计算

$$(g^{b_{il}}Y_{h-i+1}^{a_{il}})^r(Y_k^{b_{il}}Y_{h+k-i+1}^{a_{il}})^{-\frac{1}{f_k(v_k)}}=$$

$$(g^{b_{il}}Y_{h-i+1}^{a_{il}})^{r-\frac{\alpha k}{f_k(v_k)}}=h_{il}^{r'}.$$

最后,B 对 A 作出应答:

$$\boldsymbol{d}_{ID}=(d_0,d_1,d_{j+1}\cdots,d_h)=$$

$$(g_2^{\alpha}(g_3\prod_{i=1}^{j}F_i(v_i))^{r'},g^{r'},\boldsymbol{H}_{j+1}^{r'},\cdots,\boldsymbol{H}_h^{r'}).$$

签名询问:设 A 在身份 $\boldsymbol{ID}$ 下对消息 $\boldsymbol{M}$ 进行签名询问. A 首先对身份作上一步的私钥提取询问,然后验证 $F(\boldsymbol{M})$ 是否为 0,若为 0 则停止,否则,任意选取 $r,s\in\mathbb{Z}_p^*$,计算

$$\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\sigma_3)=$$

$$((g_3\prod_{i=1}^{j}F_i(v_i))^r g_1^{-\frac{J(M)}{F(M)}}(u_0\prod_{i=1}^{n_M}u_i^{m_i})^s, g_1^{-\frac{1}{F(M)}}g^s, g^r)=$$

$$(g_2^a(g_3\prod_{i=1}^{j}F_i(v_i))^r(g_2^{F(M)}g^{J(M)})^{s-\frac{\alpha}{F(M)}}, g^{s-\frac{\alpha}{F(M)}}, g^r)=$$

$$(g_2^a(g_3\prod_{i=1}^{j}F_i(v_i))^r(u_0\prod_{i=1}^{n_M}u_i^{m_i})^{s'}, g^{s'}, g^r),$$

其中 $s'=s-\dfrac{\alpha}{F(M)}$,易得 $u_0\prod_{i=1}^{n_M}u_i^{m_i}=g_2^{F(M)}g^{J(M)}$.

伪造:A 首先输出一个消息 $\boldsymbol{M}^*=(m_1^*,\cdots,m_{n_M}^*)$ 和身份 $\boldsymbol{ID}^*=(v_1^*,\cdots,v_j^*)$,然后输出一个有效签名 $\boldsymbol{\sigma}^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$,如果存在 v_i^* 使得 $f_i(v_i^*)\neq 0$ 或 $F(\boldsymbol{M}^*)\neq 0$,$B$ 将停止游戏,否则,利用 $\boldsymbol{\sigma}^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$,$B$ 能解决 h-CDH 问题,详细如下:

$$\sigma^*/(\sigma_2^{J(M^*)}\sigma_3^{\sum_{i=1}^{j}J_i(v_i^*)}Y_1^{\beta})=$$

$$(g_2^a(g_3\prod_{i=1}^{j}F_i(v_i^*))^r(u_0\prod_{i=1}^{n_M}u_i^{m_i^*})^s)/$$

$$(g^{sJ(M^*)}g^{r\sum_{i=1}^{j}J_i(v_i^*)}g^{\alpha\beta})=g^{\alpha^h+1},$$

注意计算过程中

$$g_3\prod_{i=1}^{j}F_i(v_i^*)=\prod_{i=1}^{j}Y_{h-i+1}^{f_i(v_i^*)}g^{J_i(v_i^*)}=g^{\sum_{i=1}^{j}J_i(v_i^*)},$$

$$u_0\prod_{i=1}^{n_M}u_i^{m_i^*}=g_2^{F(M^*)}g^{J(M^*)}=g^{J(M^*)},g_2^{\alpha}=g^{\alpha^h+1}g^{\alpha\beta}.$$

类似于文献[13,19],可从上述推导中得到 $\varepsilon\leqslant\varepsilon'$. 时间复杂度主要由询问阶段的指数与乘法运算体现,既然在私钥提取与签名阶段分别至多有 $O(n)$ 与 $O(n+n_M)$ 次乘法运算及 $O(n)$ 与 $O(1)$ 次指数运算,所以时间复杂度为 $t'=t+O((q_e n+q_s(n+n_M))\rho+(nq_e+q_s)\tau)$. 证毕.

4　结　　论

基于分级密码的最新进展,提出了一种新的分级身份签名方案. 该方案的签名长度短,具有高效的签名算法与验证算法,尤其在执行预运算的前提下验证算法仅需 3 个双线性对运算. 另外,本文的方案安全性基于 h-CDH 假设,此假设比现有的标准模型的下的方案具有一般性.

参　考　文　献

[1] Shamir A. Identity-based cryptosystems and signature schemes [G] //LNCS 196: Proc of the Advances in Cryptography-Crypto'84. Berlin: Springer, 1984: 47-53

[2] Waters B. Efficient identity-based encryption without random oracles [G] //LNCS 3494: Proc of the Advances in Cryptography—Eurocrypt'05. Berlin: Springer, 2005: 114-127

[3] Hu Liang, Liu Zheli, Sun Tao, et al. Survey of security of identity-based cryptography [J]. Journal of Computer Research and Development, 2009, 46 (9): 1537-1548 (in Chinese)
(胡亮, 刘哲理, 孙涛, 等, 基于身份密码学的安全研究综述 [J]. 计算机研究与发展, 2009, 46 (9): 1537-1548)

[4] Paterson K G, Schuldt J C. Efficient identity-based signatures secure in the standard model [G] //LNCS 4058: Proc of Information Security and Privacy—ACISP'06. Berlin: Springer, 2006: 207-222

[5] Gentry C, Silverberg A. Hierarchical ID-based cryptography [G] //LNCS 2501: Proc of the Advances in Cryptography—Asiacrypt'02. Berlin: Springer, 2002: 548-566

[6] Boneh D, Boyen X. Efficient selective-ID secure identity based encryption without random oracles [G] //LNCS 3027: Proc of the Advances in Cryptography—Eurocrypt'04. Berlin: Springer, 2004: 223-238

[7] Chow S M, Hiu C K, Yiu S M, et al. Secure hierarchical identity based signature and its application [G] //LNCS 3269: Proc of Information and Communications Security—ICICS'04. Berlin: Springer, 2004: 480-494

[8] Yuen T H, Wei V K. Constant-size hierarchical identity-based signature/signcryption without random oracles [R/OL]. (2005-06-03) [2011-04-07]. http://eprint.iacr.org/2005/412

[9] Man H A, Joseph K L, Tsz H Y, et al. Efficient hierarchical identity based signature in the standard model [R/OL]. (2007-11-02) [2011-04-07]. http://eprint.iacr.org/2007/068

[10] Man H A, Joseph K L, Tsz H Y, et al. Practical hierarchical identity based encryption and signature schemes without random oracles [R/OL]. (2006-12-04) [2011-04-07]. http://eprint.iacr.org/2006/368

[11] Hu X, Huang S, Fan X. Practical hierarchical identity based encryption scheme without random oracles [J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92.A(6): 1494-1499

[12] Li J, Zhang F. A new hierarchical ID-based cryptosystem and CCA-secure PKE [G] //LNCS 4097: Proc of Emerging Directions in Embedded and Ubiquitous Computing—EUCWorkshops'06. Berlin: Springer, 2006: 362-371

[13] Chattterjee S, Sarkar P. Generalization of the selective-ID security model for HIBE protocols [G] //LNCS 3958: Proc of Public Key Cryptography—PKC'06. Berlin: Springer, 2006: 241-256

[14] Li Jin, Zhang Fangguo, Wang Yanming. Two efficient hierarchical ID-based signature [J]. Acta Electronica 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[J]. 电子学报, 2007, 35(1): 150-152)

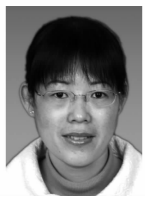
[15] Zhang Leyou, Hu Yupu, Wu Qing. A new hierarchical identity-based signature scheme in the standard model [J]. Journal of Electronics & Information Technology, 2009, 31(4): 937-941 (in Chinese)
(张乐友, 胡予濮, 吴青. 标准模型下一种新的基于身份的分级加密方案[J]. 电子与信息学报, 2009, 31(4): 937-941)

[16] Zhang Leyou, Hu Yupu, Wu Qing. New construction of short hierarchical ID-based signature in the standard model [J]. Fundamenta Informaticae, 2009, 90(1/2): 191-201

[17] Zhang Leyou, Hu Yupu, Wu Qing. Adaptively secure hierarchical identity-based sign ature in the standard model [J]. The Journal of China Universities of Posts and Telecommunications, 2010, 17(6): 95-100

[18] Zhang F, Safavi-Naini R, Susilo W. An efficient signature scheme from bilinear pairings and its applications [G] // LNCS 2947: Proc of Public Key Cryptography—PKC'04. Berlin: Springer, 2004: 277-290

[19] Chatterjee S, Sarkar P. New constructions of constant size ciphertext HIBE without random oracle [G] //LNCS 4296: Proc of Int Conf on Information Security and Cryptology—ICISC'06. Berlin: Springer, 2006: 310-327



Wu Qing, born in 1975. PhD, lecturer. Her current research interests include information security and applied mathematics.

Zhang Leyou, born in 1977. PhD, associate Professor. His current research interests include network security, computer security, and cryptography.

Hu Yupu, born in 1955. PhD. Professor and PhD supervisor. Member of China Institute of Communications and director of Chinese Association for Cryptologic Research. His current research interests include information security and cryptography.