标准模型下可证明安全的分级身份签名方案

杨旸[1]，胡予濮[1]，张乐友[2]，孙春辉[1]
(1. 西安电子科技大学通信工程学院，710071，西安；2. 西安电子科技大学理学院，710071，西安)

摘要：为使分级身份签名方案能够获得高安全性并同时缩短签名长度、降低计算量，提出一种标准模型下可证明安全的分级身份签名方案. 现有的方案通常在签名过程中将消息作为一个整体进行运算，而文中方案则对消息进行分段处理，使得方案不仅具有效率上的优势，同时在相同的效率级别上，安全性明显优于其他现有方案. 方案的安全性优势体现在：安全性证明基于完全身份的标准模型，安全性规约于计算 Diffie-Hellman (CDH)假设，并且 CDH 假设的安全性明显优于其他的困难假设而仅次于离散对数问题，因此方案具有较强的安全性. 方案的效率优势体现在：签名长度为常数，验证过程只需要进行 3 次双线性对运算，用户私钥长度随着级数的增加而减少. 性能分析和安全性分析表明，文中方案的安全性和效率均优于现有方案.

关键词：标准模型；可证明安全；分级身份；签名；双线性映射；公钥密码学
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2011)02-0027-07

Provable Secure Hierarchical Identity Based Signature Scheme in the Standard Model

YANG Yang[1], HU Yupu[1], ZHANG Leyou[2], SUN Chunhui[1]
(1. School of Communication Engineering, Xidian University, Xi′an 710071, China;
2. School of Science, Xidian University, Xi′an 710071, China)

Abstract: Aiming at the intrinsic problems in hierarchical identity based signature (HIBS) schemes, such as enhancing the security, shortening the signature length, and reducing the computational costs, a novel hierarchical identity based signature scheme is proposed. The available schemes always handle the message as an entirety in the signature process; while our scheme processes the message as segments so that the scheme is not only efficient but also achieves higher security level. The suggested scheme is more secure than the existing schemes since it is proved secure in the standard model over full identity adaptive chosen message attack, and its security is reduced to computational Diffie-Hellman (CDH) assumption. The hardness of CDH assumption is superior to the other assumptions except the discrete logarithm problem. The new scheme has some efficiency advantages over the available schemes: the size of the signature is a constant, verification requires only three bilinear pairing operations, and the private keys size shrinks as the identity depth increases. The efficiency and security analysis shows that the proposed scheme is more secure and efficient compared with the existing HIBS schemes.

Keywords: standard model; provable secure; hierarchical identity; signature; bilinear map; public key cryptography

在基于分级身份的密码系统[1-3]中，多个私钥生成中心(PKG)按照树状结构分布，根节点 PKG

收稿日期：2010-06-08. 作者简介：杨旸(1984—)，女，博士生；胡予濮(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60970119，60803149，60833008，61072067)；国家重点基础研究发展规划资助项目 (2007CB311201).

将私钥构造与身份验证的任务分配给低级的PKGs承担,从而减轻了根节点PKG的负担. 2002年,Gentry和Silverberg[4]首次提出基于分级身份的签名(HIBS)方案,但是并没有给出完整的安全性证明. Chow等[5]提出第一个可证明安全的HIBS方案,其安全模型为选择身份的随机预言机模型,并且方案的签名长度随着用户身份的级数线性增加. 随后,Yuen等[6]、Au等[7]以及Zhang等[8-9]提出标准模型下的HIBS方案,但是方案的安全性均基于较强的困难假设. Li等[10]和Cui等[11]构造的方案基于CDH假设,但是用户的私钥长度随着级数线性增长,并且验证算法需要进行大量双线性对运算. Li等[12]提出的2个方案均基于随机预言机模型以及选择身份安全模型:第一个HIBS方案签名长度随着用户级数线性增长,增加了用户的通信量,并且其安全性基于随机预言机模型;第二个HIBS方案的签名长度为常数,然而其安全性同样是基于随机预言机模型. 众所周知,基于随机预言机模型的方案并不安全. 因此,现有的方案存在的主要问题归纳为:签名长度随着级数增加;用户私钥长度随着级数线性增长;验证算法需要进行大量双线性对运算;基于较强的困难假设;基于随机预言机模型以及选择身份安全模型(标准模型及适应性选择身份模型安全性更强).

本文所提出的新型HIBS方案的签名长度为常数(仅为3个群元素),减少了签名者与用户之间的通信量;用户私钥长度随着级数的增加而减少,降低了用户的存储量;验证算法只需要进行3次双线性对运算,从而减少了用户的运算量. 因此,该方案比现有的方案更高效. 在标准模型下,证明了该方案对适应性选择消息攻击是存在性不可伪造的,并且安全性基于计算性Diffie-Hellman(CDH)假设,因此该方案同时具有高效性和安全性的特点.

1 基础知识

1.1 双线性映射

定义1(双线性映射) 令G为阶数为素数p的加法循环群,G_1为具有相同阶次的乘法循环群. 双线性映射是指满足下列性质的映射$e:G\times G\to G_1$.

①双线性性 对任意$P,Q\in G,a,b\in Z_p^*$,满足$e(aP,bQ)=e(P,Q)^{ab}$.

②非退化性 存在$P,Q\in G$,使得$e(P,Q)\neq 1$.

③可计算性 对所有的$P,Q\in G$,存在有效的算法计算$e(P,Q)$.

1.2 困难问题

定义2(CDH问题) 给定$P,aP,bP\in G$,计算abP. 这里$a,b\in Z_p^*$,P为群G的生成元.

定义3 如果没有敌手能在时间t内以至少为ε的概率解决G中的CDH问题,则称(t,ε)CDH假设在G中成立.

1.3 基于分级身份的签名方案描述

一个分级签名方案由4个算法构成:系统建立、私钥提取、签名和验证. 对一个分级签名方案而言,存在最高级数设为h,这个分级签名方案简称为h-HIBS. 第k级的用户身份设为$\mathrm{ID}_k=(v_1,\cdots,v_k)$,其中$k\leqslant h$. 算法详细描述如下.

系统建立 输入安全参数,PKG输出公开参数与主密钥,公开参数公开,主密钥由PKG私藏.

私钥提取 输入$k-1$级身份ID_{k-1}及相应的私钥$d_{\mathrm{ID}|k-1}$,输出身份为ID_k的第k级用户的私钥$d_{\mathrm{ID}|k}$.

签名 输入身份ID、相应的私钥d_{ID}、公开参数和消息M,输出此消息的签名σ.

验证 输入身份ID、消息M的签名σ,输出签名合法或不合法.

1.4 安全定义

基于分级身份的签名方案的安全性称为EU-FullID-CMA(Existential Unforgeable for full identity adaptive Chosen Message Attacks),其形式化定义由下述的一个敌手A与挑战者C之间的交互游戏来描述,详细描述如下.

系统建立 挑战者C建立系统生成算法并向敌手A提供公开参数.

询问 敌手A进行多项式次数的适应性询问(即每次询问可以参考以前询问的结果).

私钥提取询问:敌手A对身份ID_k进行私钥提取询问. 挑战者C运行私钥提取算法,产生相应于身份ID_k的私钥并发送给敌手A.

签名询问:敌手A选择身份ID_k和明文M,挑战者C运行签名算法并把签名σ发送给敌手A.

挑战 当敌手A满意并决定停止询问时,A输出用户(身份为ID^*)对消息M^*的签名值σ^*. 注意,此时对敌手A的限制是:未提前对身份ID^*或ID^*的上一级身份进行过私钥提取询问.

如果$(M^*,\mathrm{ID}^*,\sigma^*)$经过验证是合法的,则称敌手$A$赢得游戏. 敌手$A$的优势$\varepsilon$定义为它能赢得以上游戏的概率.

定义4 称一个HIBS方案是(t,ε,q_S,q_E)EU-FullID-CMA安全的,如果没有敌手能在进行了q_S

次签名询问和 q_E 次私钥提取询问之后，在时间 t 内以至少为 ε 的概率赢得上述游戏.

2　基于分级身份的签名方案

设系统最高级数为 h，基于文献[13-15]中的方法(Chatterjee-Sarkar-Naccache Extension)，将第 k 级用户身份表示为($k\leqslant h$)：$\mathrm{ID}_k=(v_1,v_2,\cdots,v_k)$，其中 $v_i=(v_{i1},\cdots,v_{il})$是长为 n 的比特串，v_{ij} 是长为 n/l 的比特串，其中 $i\leqslant k$，$j\leqslant l$，l 为一个能整除 n 的整数，且 $l<n$. 方案具体描述如下.

系统建立　随机选择生成元 $P\in G$，α 为 Z_p^* 中的任意元素，计算 $P_1=\alpha P$，选择随机元素 $P_2\in G$. 然后从群 G 中随机选取 h 维向量 $\boldsymbol{P}_3=(P_{31},\cdots,P_{3h})$及 l 维向量 $\boldsymbol{Q}=(Q_0,Q_1,\cdots,Q_l)$. 公开参数为($P,P_1,P_2,\boldsymbol{P}_3,\boldsymbol{Q}$)，主密钥为 αP_2.

私钥提取　ID_k 的私钥 $d_{\mathrm{ID}|k}=(d_0,d_1,a_{k+1},\cdots,a_h,b_1,\cdots,b_l)$的生成算法如下($k\leqslant h$).

(1)定义函数

$$V_j=V_j(v_j)=P_{3j}+\sum_{i=1}^{l}v_{ji}Q_i$$

(2)给定身份为 ID_{k-1}的用户私钥 $d_{\mathrm{ID}|k-1}$

$$d_{\mathrm{ID}|k-1}=(d'_0,d'_1,a'_k,\cdots,a'_h,b'_1,\cdots,b'_l)=$$

$$(\alpha P_2+r_1\sum_{j=1}^{k-1}V_j,\ r_1P,\ r_1P_{3k},\cdots,$$

$$r_1P_{3h},\ r_1Q_1,\cdots,\ r_1Q_l)$$

式中：r_1 是从 Z_p 中随机选取的.

(3)随机选取 $r'\in Z_p$，计算 $d_{\mathrm{ID}|k}=(d_0,d_1,a_{k+1},\cdots,a_h,b_1,\cdots,b_l)$的过程如下

$$d_0=d'_0+a'_k+\sum_{i=1}^{l}v_{ki}b'_i+r'\sum_{j=1}^{k}V_j=$$

$$\alpha P_2+r\sum_{j=1}^{k}V_j,$$

$$d_1=d'_1+r'P=rP,\quad a_j=a'_j+r'P_{3j}=rP_{3j},$$

$$b_t=b'_t+r'Q_t=rQ_t$$

式中：$r=r_1+r'$，$k+1\leqslant j\leqslant h$，$1\leqslant t\leqslant l$. 因此，得到的 $d_{\mathrm{ID}|k}$即为 ID_k 的私钥

$$d_{\mathrm{ID}|k}=$$

$$(\alpha P_2+r\sum_{j=1}^{k}V_j,rP,rP_{3,k+1},\cdots rP_{3,h},rQ_1,\cdots,rQ_l)$$

签名　设 $M=(m_1,\cdots,m_l)$是长度为 n_M(比特)的消息，m_i 长度为 n_M/l(比特). 身份为 ID_k 的签名者对消息 M 进行签名的过程如下：随机选择 $s\in Z_p$，计算

$$\sigma=(\sigma_1,\sigma_2,\sigma_3)=$$

$$(d_0+s(Q_0+\sum_{j=1}^{l}m_jQ_j),d_1,sP)$$

在签名过程中，只需使用私钥 $d_{\mathrm{ID}|k}$ 中的元素 (d_0,d_1)，其余元素用来生成下级用户的私钥.

验证　给定身份为 ID_k 的签名者对消息 M 的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，若

$$e(\sigma_1,P)=$$

$$e(P_1,P_2)e(\sigma_2,\sum_{j=1}^{k}V_j)e(\sigma_3,Q_0+\sum_{j=1}^{l}m_jQ_j)$$

成立，返回⊤；否则，返回⊥. 其中，用户可以对 $e(P_1,P_2)$进行预计算，并存储计算结果.

3　方案分析

3.1　正确性

若 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$是签名者对消息 M 的有效签名，则 $\sigma_1=d_0+s(Q_0+\sum_{j=1}^{l}m_jQ_j)$，$\sigma_2=d_1$，$\sigma_3=sP$，其中 d_0、d_1 为 ID_k 的部分私钥，并且 $d_0=\alpha P_2+r\sum_{j=1}^{k}V_j$，$d_1=rP$. 因此，可得

$$e(\sigma_1,P)=$$

$$e\Big(\alpha P_2+r\sum_{j=1}^{k}V_j+s(Q_0+\sum_{j=1}^{l}m_jQ_j),P\Big)=$$

$$e(\alpha P_2,P)e(r\sum_{j=1}^{k}V_j,P)e\Big[s\Big(Q_0+\sum_{j=1}^{l}m_jQ_j\Big),P\Big]=$$

$$e(P_1,P_2)e(rP,\sum_{j=1}^{k}V_j)e(sP,Q_0+\sum_{j=1}^{l}m_jQ_j)=$$

$$e(P_1,P_2)e(\sigma_2,\sum_{j=1}^{k}V_j)e(\sigma_3,Q_0+\sum_{j=1}^{l}m_jQ_j)$$

于是，等式 $e(\sigma_1,P)=e(P_1,P_2)\,e(\sigma_2,\sum_{j=1}^{k}V_j)\cdot e(\sigma_3,Q_0+\sum_{j=1}^{l}m_jQ_j)$ 成立，从而验证了上述 HIBS 方案的正确性.

3.2　效率分析

在表 1 中，将该方案与现有的经典方案做了比较.

(1)文献[5,10-12]中方案的签名长度与用户身份级数 k 呈线性关系，而本文的签名长度为常数，且仅为 3 个群元素.

(2)公开参数的长度会影响用户的存储量，文中方案的此项性能明显优于文献[8-11]中方案的性

能,但弱于[5,12]中的方案,而此项性能与其他方案的比较取决于参数 h、l 的具体取值.

(3)本文的用户私钥长度随着身份级数的增加而缩减,可以使大多数用户(即身份级数较长的用户)的私钥长度较短.该性能优于文献[5,8-9,12]中的方案.

(4)双线性对运算是验证过程中最耗时的运算,然而本文仅需要3次对运算,此项性能明显优于或不弱于其他各方案.

(5)本文的方案基于CDH假设,其困难度大于文献[6-9,12]中方案基于更特殊的困难假设,故本文中方案的安全性更强.

(6)本文的方案基于Full-ID模型,该模型比Selective-ID和Generalized Selective-ID模型安全.

(7)本文的方案在标准模型下可证明其安全,而文献[5,10,12]的安全性则依赖于随机预言机.众所周知,标准模型的安全性高于随机预言机模型.

通过以上对各方案性能的分析比较可以看出,本文方案的安全性明显高于文献[5-10,12]中的方案,而与文献[11]中方案的安全性相同.文献[10]中方案的私钥长度随着身份级数增加而线性增加,而本文方案的私钥长度随着身份级数增加而缩减,能有效减少用户的私钥存储空间.另外,本文方案在签名长度、公开参数长度上均比文献[11]中方案的短,进一步减少了用户的存储量.文献[11]中方案的双线性对的运算次数会随着用户级数的增加而线性增加,而本文方案的验证过程仅需3次对运算,大大减小了用户的计算量.综上分析,本文方案在安全性、存储量和计算量等方面均有明显的优势.

3.3 安全性分析

定理 1 假设(t',ε')CDH在G中成立,则上述HIBS方案是(t,ε,q_S,q_E)EU-FullID-CMA安全的,其中

$$\varepsilon'=\frac{\varepsilon}{(4(q_E+q_S)(l2^{n/l}+1))^h(4q_S(l2^{n_M/l}+1))}$$

$$t'=t+O((q_Ehl+q_S(hl+n_M))\rho+(q_E+q_S)\tau)$$

ρ、τ分别表示群G中加法和乘法运算所需的时间(假设$2^{n/l}<2(q_E+q_S)$,$2^{n_M/l}<2q_S$).

证明 假设存在敌手A能在时间t内以优势ε攻破上述HIBS方案,则可以构造出算法C在时间t'内以优势ε'攻破G中的计算Diffie-Hellman问题,即对于给定的P,aP,$bP\in G$,算法C能计算出abP.具体过程如下.

(1)系统建立 在算法C中,$n_1=2\max(2(q_E+q_S),2^{n/l})=4(q_E+q_S)$,$n_2=2\max(2q_S,2^{n_M/l})=4q_S$,随机选取$x'_0,x'_1,\cdots,x'_h,x_1,\cdots,x_l\in Z_{n_1}$,以及$y'_0,y'_1,\cdots,$

表1 各方案的性能比较

方案	签名长度	公开参数长度	私钥长度	验证运算量	假设	安全模型	R.O.
文献[5]中方案	$k+2$	$h+3$	$k+1$	$k+2$	CDH	s-ID	是
文献[6]中方案	4	$h+6$	$h-k+2$	7	orcYW	s-ID	否
文献[7]中方案	3	$2h+1$	$h-k+3$	4	q-SDH	Full	否
文献[8]中方案	3	$n_1+\cdots+n_h+n_m+5$	$h-k+2$	4	h-CDH	Gs-ID	否
文献[9]中方案	3	$hl+h+l_m+3$	$2(h-k)+2$	5	h-CDH	Full	否
文献[10]中方案	$k+2$	$h(n_1+\cdots+n_h)+h+5$	$k+1$	$k+3$	CDH	Gs-ID	是
文献[11]中方案	$k+2$	$h+n+n_m+4$	$k+1$	$k+3$	CDH	Full	否
文献[12]中方案1	$k+2$	$l+3$	$k+1$	$k+3$	CDH	s-ID	是
文献[12]中方案2	3	$l+3$	$h-k+2$	3	$(l+1)$-BDHE	s-ID	是
本文方案	3	$h+l+3$	$h-k+l+2$	3	CDH	Full	否

注:R.O.表示是否基于随机预言机模型;假设表示方案所基于的困难假设;Full表示Full-ID model;s-ID表示Selective-ID model;Gs-ID表示Generalized Selective-ID model;h为系统的最高级数;k为用户的身份级数;l为与身份的分割相关的整数且$l<h$;n_m为消息m的长度;l_m为消息m被分割的份数[10];$n_1,n_2,\cdots,n_h$为随机选取的取值较小的正整数[8,10];orcYW为文献[6]设计的困难假设;q-SDH表示q-Strong Diffie-Hellman假设;h-CDH表示h-Computational Diffie-Hellman假设.

y'_h，$y_1,\cdots,y_l\in Z_{n_2}$，随机选择 $k_1,\cdots,k_h\in\{0,\cdots,\mu_l\}$，$l_M\in\{0,\cdots,\mu_M\}$，其中 $\mu_l=l(2^{n/l}+1)$，$\mu_M=l(2^{n_M/l}+1)$. 对于 $1\leqslant j\leqslant h$，令 $v_j=(v_{j1},\cdots,v_{jl})$，$M=(m_1,\cdots,m_l)$，定义函数

$$F_j(v_j)=-mk_j+x'_j+\sum_{i=1}^{l}v_{ji}x_i$$

$$J_j(v_j)=y'_j+\sum_{i=1}^{l}v_{ji}y_i$$

$$K_j(v_j)=\begin{cases}0, & x'_j+\sum_{i=1}^{l}v_{ji}x_i=0\bmod n_1\\ 1, & x'_j+\sum_{i=1}^{l}v_{ji}x_i\neq 0\bmod n_1\end{cases}$$

$$F(M)=-ml_M+x'_0+\sum_{i=1}^{l}m_ix_i$$

$$J(M)=y'_0+\sum_{i=1}^{l}m_iy_i$$

$$K(M)=\begin{cases}0, & x'_0+\sum_{i=1}^{l}m_ix_i=0\bmod n_2\\ 1, & x'_0+\sum_{i=1}^{l}m_ix_i\neq 0\bmod n_2\end{cases}$$

然后，C 构造 HIBS 方案的公开参数. 设 $(P,aP,bP)\in G$ 为系统输入，公开参数构造过程如下

$$P_1=aP,\quad P_2=bP,$$

$$P_{3j}=(-mk_j+x'_j)P_2+y'_jP,\quad 1\leqslant j\leqslant h$$

$$Q_0=(-ml_M+x'_0)P_2+y'_0P,$$

$$Q_i=x_iP_2+y_iP,\quad 1\leqslant i\leqslant l$$

这样，C 构造出公开参数 $(P,P_1,P_2,\boldsymbol{P}_3,\boldsymbol{Q})$ 并发送给敌手 A. 然而，主密钥 $aP_2=abP$ 对于 C 和敌手 A 都是未知的. 并且由上述构造可知

$$V_j=P_{3j}+\sum_{i=1}^{l}v_{ji}Q_i=$$

$$(-mk_j+x'_j)P_2+y'_jP+$$

$$\sum_{i=1}^{l}v_{ji}x_iP_2+\sum_{i=1}^{l}v_{ji}y_iP=F_j(v_j)P_2+J_j(v_j)P$$

$$Q_0+\sum_{j=1}^{l}m_jQ_j=(-ml_M+x'_0)P_2+y'_0P+$$

$$\sum_{i=1}^{l}m_ix_iP_2+\sum_{i=1}^{l}m_iy_iP=F(M)P_2+J(M)P$$

(2)询问　敌手 A 允许进行至多 q_E 次私钥提取询问以及 q_S 次签名询问. 询问过程模拟如下.

私钥提取询问. 首先选取 $\mathrm{ID}_k=(v_1,v_2,\cdots,v_k)$，$k\leqslant h$，作为私钥提取询问的输入身份. C 计算是否存在 $u\in\{1,\cdots,k\}$ 使得 $K_u(v_u)\neq 0$ 成立，若不存在，C 结束该模拟过程；否则 C 随机选取 $r'\in Z_p$. 私钥构造如下.

$$d_{0\mid u}=-\frac{J_u(v_u)}{F_u(v_u)}P_1+r'(F_u(v_u)P_2+J_u(v_u)P)=$$

$$aP_2-\frac{a}{F_u(v_u)}(F_u(v_u)P_2+J_u(v_u)P)+$$

$$r'(F_u(v_u)P_2+J_u(v_u)P)=$$

$$aP_2+\left(r'-\frac{a}{F_u(v_u)}\right)(F_u(v_u)P_2+J_u(v_u)P)=$$

$$aP_2+rV_u$$

$$d_0=d_{0\mid u}+r\sum_{j=1,j\neq u}^{k}v_j=aP_2+r\sum_{j=1}^{k}v_j$$

$$d_1=-\frac{1}{F_u(v_u)}P_1+r'P=-\frac{a}{F_u(v_u)}P+r'P=rP$$

式中：$r=r'-a/F_u(v_u)$.

此外，$(a_{k+1},\cdots,a_h,b_1,\cdots,b_l)$ 的构造过程与之类似，不再赘述. 因此，由算法 C 模拟生成的私钥与实际生成的私钥是不可区分的. 然后将这个为身份 ID_k 构造出的合法私钥发送给敌手 A.

签名询问. 考虑用身份 ID_k 对消息 M 的签名询问，$k\leqslant h$. 算法 C 用上述的私钥提取算法得到 ID_k 的私钥，构造对 M 的签名过程如下：若 $K(M)=0$，C 结束该模拟过程；否则，随机选择 $r,s\in Z_p$，计算

$$\sigma=(\sigma_1,\sigma_2,\sigma_3)=$$

$$\left(r\sum_{j=1}^{k}V_j-\frac{J(M)}{F(M)}P_1+s'\left(Q_0+\sum_{j=1}^{l}m_jQ_j\right),\right.$$

$$\left.-\frac{1}{F(M)}P_1+s'P,\ rP\right)=$$

$$\left(r\sum_{j=1}^{k}V_j+\left[aP_2-\frac{a}{F(M)}F(M)P_2\right]-\right.$$

$$\frac{J(M)}{F(M)}(aP)+s'\left(Q_0+\sum_{j=1}^{l}m_jQ_j\right),$$

$$\left.-\frac{1}{F(M)}P_1+s'P,\ rP\right)=$$

$$\left(aP_2+r\sum_{j=1}^{k}V_j+\left(s'-\frac{a}{F(M)}\right)[F(M)P_2+\right.$$

$$\left.J(M)P],\left(s'-\frac{a}{F(M)}\right)P,\ rP\right)=$$

$$\left(aP_2+r\sum_{j=1}^{k}V_j+s\left(Q_0+\sum_{j=1}^{l}m_jQ_j\right),\ sP,\ rP\right)$$

因此 $(\sigma_1,\sigma_2,\sigma_3)$ 是一个有效的签名.

(3)伪造　敌手 A 输出身份 $\mathrm{ID}_k^*=(v_1^*,\cdots,v_k^*)$ 对消息 M^* 的伪造签名 $(\sigma_1^*,\sigma_2^*,\sigma_3^*)$.

若 $F(M^*)\neq 0$ 或 $F_j(v_j^*)\neq 0$，C 结束该模拟过程；否则，意味着 $F(M^*)=0$，$F_j(v_j^*)=0$，$1\leqslant j\leqslant k$，则 C 可以利用该伪造签名解决 CDH 问题.

$$\sigma_1^*-J(M^*)\sigma_2^*-\sum_{j=1}^{k}J_j(v_j^*)\ \sigma_2^*=$$

$$[aP_2 + r\sum_{j=1}^{k} V_j^* + s(Q_0 + \sum_{j=1}^{l} m_j^* Q_j)] -$$

$$J(M^*)(sP) - \sum_{j=1}^{k} J_j(v_j^*)(rP) = aP_2$$

因为

$$J(M^*)P = F(M^*)P_2 + J(M^*)P =$$

$$(Q_0 + \sum_{j=1}^{l} m_j^* Q_j)$$

$$\sum_{j=1}^{k} [J_j(v_j^*)P] =$$

$$\sum_{j=1}^{k} [F_j(v_j^*)P_2 + J_j(v_j^*)P] = \sum_{j=1}^{k} V_j^*$$

由于在系统建立过程中 $aP_2 = abP$，于是上述过程解决了群 G 中的 CDH 问题. 因此，如果 CDH 假设在群 G 中成立，则该 HIBS 方案是安全的.

根据文献[16-18]中的方法，可以计算出 C 不结束模拟过程的概率为

$$P_a \geqslant \frac{1}{(4(q_E + q_S)(l2^{n/l} + 1))^h (4q_S(l2^{n_M/l} + 1))}$$

时间复杂度主要体现在询问阶段的加法和乘法运算，所以有

$$t' = t + O((q_E hl + q_S(hl + n_M))\rho + (q_E + q_S)\tau)$$

证毕.

4 结 论

本文提出了一个签名长度固定的基于分级身份的签名方案，在标准模型下证明了该方案是安全的. 与现有的 HIBS 方案相比，该方案的用户私钥长度随着级数的增加而减少，签名长度仅包含 3 个群元素，具有较高的效率. 同时，利用 CDH 问题的困难性，对方案进行了安全性证明. 由于方案设计过程中采用了标准模型的框架，从而提升了方案的安全性. 因此，新方案在效率和安全性上都有较大改善.

参考文献：

[1] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]// Proceedings of the 29th International Cryptology Conference. Berlin, Germany: Springer-Verlag, 2009: 619-636.

[2] 肖龙，王标，孙琦. 基于环 Zn 上的圆锥曲线数字签名和多重数字签名 [J]. 西安交通大学学报，2006，40(6)：648-650，718.
XIAO Long, WANG Biao, SUN Qi. Digital signature and multiple digital signatures based on the conic curve over Zn [J]. Journal of Xi'an Jiaotong University, 2006, 40(6): 648-650, 718.

[3] RUCKERT M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles [C]// Proceedings of the third International Workshop on Post-quantum Cryptography. Berlin, Germany: Springer-Verlag, 2010: 182-200.

[4] GENTRY C, SILVERBERG A. Hierarchical ID-based cryptography [C] // Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer-Verlag, 2002: 548-566.

[5] CHOW S, LUCAS C, YIU S, et al. Secure hierarchical identity based signature and its application [C]// Proceedings of International Conference on Information and Communications Security. Berlin, Germany: Springer-Verlag, 2004: 480-494.

[6] YUEN T H, WEI V K. Constant-size hierarchical identity-based signature/signcryption without random oracles [EB/OL]. (2006-06-02) [2007-09-08]. http://eprint.iacr.org/2005/412.

[7] AU M H, LIU J K, YUEN T H, et al. Practical hierarchical identity based encryption and signature schemes without random oracles [EB/OL]. (2006-12-04) [2007-09-16]. http://eprint.iacr.org/2006/368.

[8] ZHANG Leyou, HU Yupu. A new construction of short hierarchical identity-based signature in the standard model [J]. International Journal of Computer Science and Network Security, 2009, 9 (4): 180-186.

[9] ZHANG Leyou, HU Yupu, WU Qing. New construction of short hierarchical ID-based signature in the standard model [J]. Fundamenta Informaticae, 2009, 90 (1): 191-201.

[10] LI Jin, CHEN Xiaofeng, ZHANG Fangguo, et al. Generalization of the selective-ID security model for HIBS protocols [C]// Proceedings of the 2006 International Conference on Computational Intelligence and Security. Piscataway, NJ, USA: IEEE, 2006: 1583-1586.

[11] CUI Wei, XIN Yang, YANG Yixian, et al. Practical hierarchical identity based signature in the standard model [C] // Proceedings of the 2008 International Conference on Neural Networks and Signal Processing. Piscataway, NJ, USA: IEEE, 2008: 416-421.

[12] 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.
LI Jin, ZHANG Fangguo, WANG Yanmin. Two efficient hierarchical identity based signature schemes

[J]. Chinese Journal of Electronics, 2007, 35(1): 150-152.

[13] BONEH D, BOYEN X, GOH E. Hierarchical identity based encryption with constant size ciphertext [C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer-Verlag, 2005: 440-456.

[14] NACCACHE D. Secure and practical identity based encryption [J]. IET Information Security, 2007, 1(2): 59-64.

[15] CHATTERJEE S, SARKAR P. Trading time for space: towards an efficient IBE scheme with short(er) public parameters in the standard model [C]// Proceedings of the International Conference on Information Security and Cryptology. Berlin, Germany: Springer-Verlag, 2006: 424-440.

[16] WATERS B. Efficient identity-based encryption without random oracles [C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer-Verlag, 2005: 114-127.

[17] PATERSON K, SCHULDT J. Efficient identity-based signatures secure in the standard model [C]// Proceedings of the 11th Australian Conference on Information Security and Privacy. Berlin, Germany: Springer-Verlag, 2006: 207-222.

[18] CHATTERJEE S, SARKAR P. HIBE with short public parameters secure in the full model without random oracle [C]// Proceedings of the 12th International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer-Verlag, 2006: 424-440.

[本刊相关文献链接]

面向命题投影时序逻辑的安全协议模型检测. 西安交通大学学报，2010，44(8)：30-35.

采用离散粒子群算法的网格任务安全级调度. 西安交通大学学报，2010，44(6)：21-26.

无线局域网自适应安全管理框架及其应用. 西安交通大学学报，2010，44(4)：34-38.

可废除并发签名机制. 西安交通大学学报，2009，43(12)：45-49.

无线局域网 802.1X 协议安全性分析与检测. 西安交通大学学报，2009，43(10)：52-55.

分布式环境中高效信任管理的研究. 西安交通大学学报，2009，43(6)：15-19.

NSIS 下通用访问控制信令协议的设计与验证. 西安交通大学学报，2009，43(4)：34-38.

采用中国剩余定理的群签名方案的安全性分析与改进. 西安交通大学学报，2009，43(2)：77-80.

利用构造类别代数的协议安全测试方法. 西安交通大学学报，2008，42(12)：1481-1485.

网络安全协同防卫系统研究与实现. 西安交通大学学报，2008，42(12)：1495-1499.

排序问题的多方保密计算协议. 西安交通大学学报，2008，42(2)：231-233.

基于鼠标动力学模型的用户身份认证与监控. 西安交通大学学报，2008，42(10)：1235-1239.

一个可验证秘密共享新个体加入协议的安全性分析. 西安交通大学学报，2008，42(8)：1059-1060.

交通网络最优安全路径选择模型与算法. 西安交通大学学报，2008，42(4)：395-398.

无线传感器网络低时延能量均衡安全路由. 西安交通大学学报，2008，42(2)：161-165.

基于随机密钥预分布模型的安全定向扩散协议. 西安交通大学学报，2007，41(12)：1423-1426.

一种基于规则的工作票描述语言自动生成算法. 西安交通大学学报，2007，41(10)：1224-1228.

新的有效叛逆者追踪方案. 西安交通大学学报，2007，41(8)：931-933.

一种新型的分布式隐私保护计算模型及其应用. 西安交通大学学报，2007，41(8)：954-58.

基于 SWIM 卡公钥认证的二阶段握手加密套接层协议. 西安交通大学学报，2007，41(6)：669-673.

一种防破坏广播型匿名通信网的多路访问协议. 西安交通大学学报，2007，41(6)：674-678.

网络流的层次化分析及其在蠕虫早期检测中的应用. 西安交通大学学报，2007，41(4)：393-397.

（编辑　武红江）