标准模型下一种新的基于身份的分级加密方案

张乐友[①②] 胡予濮[②] 吴 青[①]
[①](西安电子科技大学应用数学系 西安 710071)
[②](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要：该文给出了一种新的基于身份的分级加密方案，在标准模型下，证明了该方案是推广selective-ID安全的。在判定BDHI假设下，该方案可以抗选择明文攻击(CPA)。另外，作为文中方案的推广应用，基于Waters方案及其变形方案，提出了一种标准模型下基于身份的分级签名方案。在DHI假设下，该方案被证明对适应性选择消息攻击是存在性不可伪造的。

关键词：基于身份的分级加密方案；标准模型；分级签名方案；双线性映射
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2009)04-0937-05

A New Hierarchical Identity-Based Encryption in the Standard Model

Zhang Le-you[①②] Hu Yu-pu[②] Wu Qing[①]
[①](*Department of Applied Mathematics*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*Key Laboratory of Computer Networks and Information Security*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: In this paper, a new Hierarchical Identity-Based Encryption(HIBE) scheme is proposed and is provable security in the generalized selective-ID model in the standard model. Under the decision Bilinear Diffie-Hellman Inversion (BDHI) assumption, this new scheme is provable security against Chosen Plaintext Attacks(CPA). Additionally, a Hierarchical Identity-Based Signature (HIBS) scheme is proposed based on the Waters's scheme and our technique in the standard model. And under Diffie-Hellman Inversion(DHI) assumption, it is provable security against existentially unforgeable under an adaptive chosen message attack.

Key words: Hierarchical identity-based encryption; Standard model; Hierarchical identity-based signature; Bilinear map

1 引言

基于身份的密码体制最初是由Shamir[1]于1984年提出，其目的是为了简化密钥管理。在基于身份的密码体制中，用户的公钥是直接从其身份信息(如姓名、身份证号、E-mail 地址等) 得到，而私钥则是由一个称为私钥生成中心(PKG)的可信方生成。基于身份的密码体制的思想提出以后，有许多基于身份的密码方案相继出现，直到2001年，一个真正有效的基于身份的加密方案才被提出。这个方案是由Boneh和Franklin[2]利用椭圆曲线上的双线性对设计的。基于身份分级加密体制是上述加密体制的推广，在基于身份的密码系统中，虽然只有一个PKG可以完全消除在线查找(online lookup)，但是单一的PKG却成了在大规模网络中应用的瓶颈。因为在大规模网络中，单一的PKG不仅使产生私钥的计算代价昂贵，而且它还必须独立完成身份有效的检验和建立安全的信道来传送私钥。这会影响到系统的效率，这点和基于证书的密码系统十分类似，因此需要一种分级的基于身份的密码系统，在这种系统中，多个PKG按照树状结构分布。它的一个优势是一个根节点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；另一个优势是当前的PKG的秘密泄露不会危及高一级的PKGs。详细的论述详见文献[3–7]。第一个有效的分级加密方案是由Gentry和Silverberg[3]提出的，在随机预言机模型下，其安全性规约到双线性 Diffie-Hellman(BDH)问题。第1个标准模型下的方案是Boneh与Boyen在2004年提出的，但是其安全性基于一个弱的模型-selective-ID 模型。2006年，Boneh等[6]提出了密文长度为常数的分级加密方案，其安全性不依赖随机预言机，但是其安全性被规约到一个强的假设-q双线性Diffie-Hellman指数问题(q-BDHE) 假设。最近，Sanjit Chattterjee与Palash Sarkar提出了一种基于广义的selective-ID(G-sID)模型的方案，这种模型是selective-ID模型与adaptive-ID模型(Full model)的推广具体描述见文献[8]。基于分级身份的签名方案是由Gentry 和Silvverberg在2002年提出的[3]，而第1个可证明安全的方案是由Chow[9]等提出的，但是安全性证明是在随机预言机模型得到的。最近文献[10]提出了一种有效的方案，在标准模型下(不依赖随机预言机)证明了安全性，

2007-12-03收到，2008-04-21改回
国家自然科学基金(60473029)资助课题

然而其安全性基于一个强的困难问题假设-q-SDH问题。

本文基于推广的模型(G-sID)， 提出了一种新型的基于身份的分级加密方案，该方案的安全性不依赖随机预言机。在一般的困难假设-判定BDHI假设(等价于判定BDH假设)下，该方案可以抗选择明文攻击(CPA)。另外，基于Waters方案及文中方案，提出了一种标准模型下基于身份的分级签名方案。在DHI(等价于CDH假设)假设下，该方案被证明对适应性选择消息攻击是存在性不可伪造的。

2 预备知识

2.1 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 $u,v\in G$, $a,b\in Z_p$，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。

2.2 复杂度假设

定义1 (DHI问题) Diffie-Hellman逆问题定义如下：给定元素 g， g^{α} ($g\in G$ ， $\alpha\in Z_p$)，计算 $g^{\frac{1}{\alpha}}$ 。

多项式算法 $\boldsymbol{A}$ 以优势 ε 解决DHI 问题如果满足：$\Pr\{\boldsymbol{A}(g\ ,g^{\alpha})=g^{\frac{1}{\alpha}}\}\geq\varepsilon$ 。称(t,ε)-DHI假设成立如果在多项式时间t内没有算法以不可忽略的概率 ε 解决DHI问题。

定义2 (判定BDHI问题) 判定BDHI问题定义如下：给定 G 中的元素 g , g^{α} ，其中 $\alpha\in Z_p$ ，任取 $T\in G_1$ ，判定 $T\stackrel{?}{=}\hat{e}(g,g)^{\frac{1}{\alpha}}$ 。

判定BDHI假设定义如下，挑战者随机选取 $b\in\{0,1\}$ ，如果 $b=1$ ，将 $(g,g^{\alpha},T=\hat{e}(g,g)^{\frac{1}{\alpha}})$ 给攻击者，若 $b=0$ ，将 (g,g^{α},T) 给攻击者 B ，其中 T 为 G_1 中的任意元素。攻击者收到 (g,g^{α},T) 后，输出 $b'\in\{0,1\}$ 作为对 b 的猜想，其优势定义为[5]

$$|\Pr\{B(g,\ g^{\alpha},\hat{e}(g,g)^{\frac{1}{\alpha}})=0\}-\Pr\{B(g,\ g^{\alpha},T)=0\}|\geq\varepsilon$$

如果在上面的游戏中攻击者的优势 ε 是可以忽略的，则称判定BDHI假设成立。

容易看出，判定BDHI问题等价于判定双线性Diffie-Hellman(DBDH)假设，文献[11]指出，DHI问题等价于计算性Diffie-Hellman问题(CDH problem)。

2.3 HIBE 方案

一个HIBE方案有4个算法构成：系统建立；私钥提取；加密和解密算法。具体算法简要描述如下(详细描述参见文献[3-7])：

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ID =($v_1,v_2,\cdots,v_j$)， 公共参数以及对应于上一级身份 ID_{j-1} =($v_1,v_2,\cdots,v_{j-1}$) 的私钥 $d_{\mathrm{ID}|j-1}$，输出对应于ID的私钥 d_{ID} 。如果 $j=1$，此时私钥由根PKG产生。

加密：输入一个身份ID，系统参数和来自于一个消息空间的消息，输出此消息的密文。

解密：输入对应于身份ID的密文，输出消息或表示密文不合法的判定。

2.4 安全模型

HIBE 的安全模型由下述游戏给出，如果在以下的游戏中，攻击者的优势可以忽略，我们称HIBE具有抗广义选择身份和选择密文攻击安全性(IND-GsID-CCA)，具体定义如下：

初始化：在这个阶段敌手提交两个身份集合 S_1,S_2 ，并且承诺：

(1)私钥提取阶段不询问 S_1 中的任何身份；(2)挑战阶段所用的身份必需从 S_2 选取。

系统建立：模拟者建立HIBE协议并且将公共参数发给敌手，自己保留主密钥。

阶段1 敌手进行一系列的询问 $q_1,\cdots,q_m$ ，每一次询问 q_i 具体如下：

(1)私钥提取询问。模拟者运行私钥提取算法得到相应于身份 ID_i 的私钥 d_i ，并将 d_i 发给敌手。注意这个身份 ID_i 不能是 S_1 中的元素。

(2)解密询问。模拟者运行私钥提取算法得到相应于身份ID的私钥d，接着运行解密算法，用d解密敌手提交的密文，并将解密后的明文发给敌手。注意此时的身份ID不能是 S_1 中的元素。

挑战：敌手输出一个挑战身份 $\mathrm{ID}^*(\mathrm{ID}^*\in S_2)$ 和两个等长明文 M_0,M_1 。唯一的限制是敌手不能在输出前询问过 ID^* 或 ID^* 的前一级身份。模拟者随机选取一个比特 $b,b\in\{0,1\}$ ，记 M_0， M_1 中要加密度的明文为 M_b ，将挑战密文 C($C=$ Encryption(params, ID^*, M_b))发送给敌手。

阶段2 敌手继续进行一系列的询问 $q_1,\cdots,q_m$ ，每一次询问 q_i 具体如下：

(1)私钥提取询问。与阶段1类似，设询问的身份为 ID_j ，这儿的 $\mathrm{ID}_j\neq\mathrm{ID}^*$ 且不能是 ID^* 的前一级也不能来自于 S_1 。

(2)解密询问。与阶段1类似，询问的密文 $C_j\neq C$ ，且密文 C_j 对应的身份不能是 ID^* 也不能是 ID^* 的前一级。

猜想：最后，敌手输出对b猜测 b' ，敌手赢得游戏当且仅当$b=b'$ 。

本文定义敌手的优势为： $Adv_A^{\mathrm{CCA}}=|\Pr[b=b']-1/2|$，在本文方案中，规定 S_1=S_2 。

定义3 称一个HIBE方案是 (t,q_{ID},q_C) 安全的，如果在多项式时间t内，任何敌手在上面的游戏中在进行了至多 q_{ID} 次私钥提取询问和至多 q_C 次解密询问后，其优势 Adv_A^{CCA} 仍是可忽略的。

一个 (t,q_{ID},q_C) 安全的HIBE方案其安全性可抗适应性选择密文攻击(CCA)，比其弱一点的安全模型称为抗适应性选

择明文攻击(CPA)，在此模型下，敌手不允许进行解密询问。现在已有许多方法将具有抗适应性选择明文攻击的方案转化为抗适应性选择密文攻击的方案(如文献[12])，因此，文中的方案将重点讨论是否具有抗择明文攻击的安全性。

3　新方案的构造

设系统的最高分级数为 l，令 $\mathrm{ID}=(v_1,v_2,\cdots,v_l)\in(z_p^*)^l$，第 j 级的身份为 $\mathrm{ID}_j=(v_1,\cdots,v_j)$，$G$ 与 G_1 为两个阶数为素数 p 的循环群，算法具体构造如下：

系统建立：设 g 为 G 的任一生成元，α 为 Z_p^* 的任一元素，计算 $g_1=g^\alpha$，然后随机选取 $g_2,g_3,h_1,\cdots,h_n\in G$，公共参数为 $\mathrm{param}=\{g,g_1,g_2,g_3,h_1,\cdots,h_n\}$，主密钥为 g_2^α。同时定义函数 $F(x)=\prod_{j=1}^{n}h_j^{x^j}$，其中 $x\in Z_p$。

私钥提取：(k−1层向k层发放)令k层的身份为 $\mathrm{ID}_k=(v_1,\cdots,v_k)$，$k$−1层的身份为 $\mathrm{ID}_{k-1}=(v_1,\cdots,v_{k-1})$，其对应的私钥为 $d_{\mathrm{ID}|k-1}=(d_0',d_1',\cdots,d_{k-1}')=\left(g_2^\alpha\prod_{j=1}^{k-1}(F_j)^{r_j},g_1^{r_1},\cdots,g_1^{r_{k-1}}\right)$，其中 $r_1,r_2,\cdots,r_{k-1}$ 是 Z_p 中的任意元素，$F_j=g_3F(v_j)$，则由第k−1层的私钥可得第k层的私钥 $d_{\mathrm{ID}}=(d_0,d_1,\cdots,d_k)=\left(g^\alpha\prod_{i=1}^{k}(F_i)^{r_i},g_1^{r_1},g_1^{r_2},\cdots,g_1^{r_k}\right)$，其中 r_k 为 Z_p 中的任意元素，由第k层用户选取。

加密：用户 $\mathrm{ID}=(v_1,\cdots,v_k)$，设加密的消息 M 来自消息空间，用户随机选取一个随机数 $r\in z_p$，输出密文：$C_M=(A,B,C_1,C_2,\cdots,C_k)=(\hat{e}(g,g)^rM,g_1^r,F_1^r,F_2^r,\cdots,F_k^r)$。

解密：设 ID 以及对应的私钥为 $d_{\mathrm{ID}}=(d_0,d_1,\cdots,d_k)$，要解密的密文为 $C_M=(A,B,C_1,C_2,\cdots,C_k)$，则消息为：$M=A\prod_{i=1}^{k}\hat{e}(d_i,C_i)\Big/\hat{e}(d_0,B)$。

4　安全性分析

定理1　如果(t,ε)判定性BDHI假设是成立的，则文中的新框架是(t',q,ε)-GsID-CPA安全的，其中 $t'<t-O(\tau nq)$，q 是私钥提取询问的最多次数，τ 为指数运算所用的最多时间。

证明　假设敌手能以优势ε攻破新方案，我们将构造一模拟者以同样的优势攻破判定性BDHI问题，具体如下：

初始化：敌手提交一个身份集合 I^*，其中的元素来源于 z_p，令 $I^*=(v_1^*,v_2^*,\cdots,v_n^*)$。

系统建立：定义函数 $f(x)=\prod_{i=1}^{n}(x-v_i^*)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，其中 $a_i\in Z_p$，$v_i^*\in I^*$，故对任意 $v\in z_p\setminus I^*$，有 $f(v)\neq0$。然后再随机选取一组数 $b_0,b_1,\cdots,b_n\in Z_p$，构造另一个函数 $J(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$，定义 $g_3=g^{a_0}g_1^{b_0}$，$h_i=g^{a_i}g_1^{b_i}$，$1\le i\le n$，规定 $a_n=1$。公共参数为 $\mathrm{param}=\{g,g_1,g_2,g_3,h_1,\cdots,h_n\}$，将其发给敌手，注意这时主密钥 g_2^α 对敌手是保密的。

阶段1　敌手在此阶段进行一系列的私钥提取询问。设敌手提交的身份为 $\mathrm{ID}=(v_1,\cdots,v_k)$，$k\le l$。根据安全模型的定义，这里至少有一个 $v_j\notin I^*$，故 $f(v_j)\neq0$。定义函数 $F(x)=g_3\prod_{i=1}^{n}h_i^{x^i}$，由以上的定义显然有 $F(x)=g^{f(x)}g_1^{J(x)}$。然后，定义 $F_i=F(v_i)$，随机选取 $r_1,\cdots,r_{j-1},r_j',r_{j+1},\cdots,r_k\in z_p$，构造私钥如下：

$$d_0=g^{-\frac{J(v_j)}{f(v_j)}}(g^{f(v_j)}g_1^{J(v_j)})^{r_j'}T,\quad d_i=\begin{cases}g_1^{r_i},\ 1\le i\le k,\ \ i\neq j\\ g^{-\frac{1}{f(v_j)}}g_1^{r_j'},\qquad i=j\end{cases}$$

其中 $T=\prod_{i=1,i\neq j}^{k}(F_i)^{r_i}$。显然，$(d_0,d_1,\cdots,d_k)$ 是对敌手的有效回复。事实上

$$\begin{aligned}d_0&=g^{-\frac{J(v_j)}{f(v_j)}}(g^{f(v_j)}g_1^{J(v_j)})^{r_j'}T=g^{\frac{1}{\alpha}}g^{-\frac{J(v_j)}{f(v_j)}}(g^{f(v_j)}g_1^{J(v_j)})^{r_j'}T\Big/g^{\frac{1}{\alpha}}\\&=g^{\frac{1}{\alpha}}(g^{f(v_j)}g_1^{J(v_j)})^{r_j'-\frac{1}{f(v_j)\alpha}}T\ =g^{\frac{1}{\alpha}}\prod_{i=1}^{k}(F_i)^{r_i},\end{aligned}$$

$$d_i=\begin{cases}g_1^{r_i}, & 1\le i\le k,i\neq j\\ g^{-\frac{1}{f(v_j)}}g_1^{r_j'}=g_1^{r_j'-\frac{1}{f(v_j)\alpha}}=\ g_1^{r_j}, & i=j\end{cases}$$

其中 $r_j=r_j'-\frac{1}{f(v_j)\alpha}$。

挑战：敌手输出两个等长的消息 M_0，M_1 和要挑战的身份 $\mathrm{ID}^*=(v_1^*,v_2^*,\cdots,v_k^*)$，其中 $v_i^*\in I^*$，模拟者随机选取一比特$b\in\{0,1\}$，相应回复敌手：

$$C_M=(Z^sM_b,g^s,g^{J_1(v_1^*)s},\cdots,g^{J_k(v_k^*)s})$$

这是一个对 M_b 有效的加密，事实上，由前面的定义，对任意 $v_i^*\in I_i^*$ 都有 $f_i(v_i^*)=0$，因而 $F_i=F_i(v_i)=g^{f_i(v_i^*)}g_1^{J_i(v_i^*)}=g_1^{J_i(v_i^*)}=(g^\alpha)^{J_i(v_i^*)}$，如果 $Z=\hat{e}(g,g)^{\frac{1}{\alpha}}$，令 $s=r\alpha$，则有

$$\begin{aligned}C_M&=(Z^sM_b,g^s,g^{J_1(v_1^*)s},\cdots,g^{J_k(v_k^*)s})\\&=(\hat{e}(g,g)^rM_b,g_1^r,F_1^r,F_2^r,\cdots,F_k^r)\end{aligned}$$

故模拟是完美的。

阶段2　敌手继续类似于第1阶段的询问，模拟者进行相应的回答。

猜测：最后，敌手输出猜测 b'。如果 $b=b'$，模拟者输出1，这表示 $Z=\hat{e}(g,g)^{\frac{1}{\alpha}}$；否则输出0。

当 $Z=\hat{e}(g,g)^{\frac{1}{\alpha}}$，从攻击者角度看，这是一个真实的攻击，因而敌手必需满足 $|\Pr[b=b']-1/2|>\varepsilon$，另一方面，如果$Z$是任意的，则有$\Pr[b=b']=1/2$，所以

$$\begin{aligned}&\Big|\Pr\{B(g\ ,g^\alpha,\hat{e}(g,g)^{\frac{1}{\alpha}})=0\}\\&\quad-\Pr\{B(g\ ,g^\alpha,Z)=0\}\Big|\ge\left|\left(\frac{1}{2}\pm\varepsilon\right)-\frac{1}{2}\right|=\varepsilon\end{aligned}$$

5　应用

5.1　基于身份的分级签名体制

基于身份的分级签名体制由以下算法构成：

系统建立与私钥提取算法与加密方案相同。

签名：给定消息M和接收者的身份信息ID以及私钥d_{ID}，产生相应的签名；

验证：给定签名和用户身份，输出1，如果它是一个有效签名，否则输出0。

一个基于身份的分级签名方案是安全的，如果满足：

(1)正确性；(2)存在性不可伪造性。具体的安全模型定义详见文献[9,10]。

5.2 方案的构造

设系统的最高分级数为 l，令 ID=$(v_1,v_2,\cdots,v_l)(z_p^*)^l$，第 j 级的身份为 $\mathrm{ID}_j=(v_1,\cdots,v_j)$，$G$ 与 G_1 为两个阶数为素数 p 的循环群，算法具体构造如下：

系统建立与私钥提取算法与文中的加密方案相同。

签名：令M是n比特长的消息，m_i表示其第i比特，则对消息的签名如下：

随机选取 $r\in z_p$，输出

$$\sigma=(\sigma_0,\sigma',\sigma_1,\cdots,\sigma_k)=\left(d_0\left(u_0\prod_{k=1}^{n}u_k^{m_k}\right)^r,g_1^r,g_1^{r_1},g_1^{r_2},\cdots,g_1^{r_k}\right)$$

验证：给定消息M及身份ID以及对应的签名 $\sigma=(\sigma_0,\sigma',\sigma_1,\cdots,\sigma_k)$，如果满足 $\hat{e}(\sigma_0,g_1)=\hat{e}(g,g)\hat{e}\left(\sigma',u_0\prod_{k=1}^{n}u_k^{m_k}\right)\cdot\prod_{i=1}^{k}\hat{e}(F_i,\sigma_i)$，则接受，否则拒绝。

5.2.1有效性 与已有的方案相比，本文方案在私钥提取算法阶段指数运算略有增加，但在签名阶段只需两次指数运算，因而效率大大提高。而且，本文方案的安全性不依赖于随机预言机。

5.2.2正确性 如果 $\sigma=(\sigma_0,\sigma',\sigma_1,\cdots,\sigma_k)$ 是有效的，则

$$\begin{aligned}\hat{e}(\sigma_0,g_1)&=\hat{e}\left(d_0\left(u_0\prod_{k=1}^{n}u_k^{m_k}\right)^r,g_1\right)=\hat{e}\left(g^{\frac{1}{\alpha}}\prod_{i=1}^{k}(F_i)^{r_i}\left(u_0\prod_{k=1}^{n}u_k^{m_k}\right)^r,g_1\right)\\&=\hat{e}\left(g^{\frac{1}{\alpha}},g_1\right)\hat{e}\left(\prod_{i=1}^{k}(F_i)^{r_i}\left(u_0\prod_{k=1}^{n}u_k^{m_k}\right)^r,g_1\right)\\&=\hat{e}(g,g)\hat{e}\left(\sigma',u_0\prod_{k=1}^{n}u_k^{m_k}\right)\prod_{i=1}^{k}\hat{e}(F_i,\sigma_i)\end{aligned}$$

5.2.3存在性不可伪造

定理2 如果DHI假设成立，则本文的新签名方案是在给定攻击身份，选择消息攻击下是存在性不可伪造的。

证明 由于本文的签名方案来源于文中的加密方案和Waters签名方案[13]及改进方案[14]，故方案的安全性证明简要的给出如下：

假设敌手能攻破新方案，我们将构造一模拟者以同样的优势攻破DHI问题，具体如下：

系统初始化、系统建立类似文中加密方案及文献[14]。

私钥提取询问类似文中加密方案，签名询问类似于文献[14]。

伪造：经过上面的询问如果模拟者没有终止，则类似文献[14]，我们得到如果敌手成功伪造签名，模拟者可解决DHI问题。

6 结束语

本文提出了一种新型的基于身份的分级加密方案，该方案的安全性不依赖随机预言机。在一般的困难假设--判定BDHI假设下，该方案可以抗选择明文攻击(CPA)。另外，作为本方案的应用，结合Waters签名方案及其变形方案，提出了一种标准模型下基于身份的分级签名方案。在DHI假设下，该方案被证明对适应性选择消息攻击是存在性不可伪造的。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]. Advances in Cryptology-Crypto, California, USA, 1984, LNCS 196: 47–53.

[2] Boneh D and Franklin M. Identity based encryption from the weil pairing [C]. Advances in Cryptology-CRYPTO, California, USA, August 19–23, 2001, LNCS 2139: 213–229.

[3] Gentry C and Silverberg A. Hierarchical ID-based cryptography [C]. Advances in Cryptology-ASIACRYPT, New Zealand, December 1–5, 2002, LNCS 2501: 548–566.

[4] Horwitz J and Lynn B. Towards hierarchical identity-based encryption[C]. Advances in Cryptology-EUROCRYPT, The Netherlands, April 28 – May 2, 2002, LNCS 2332: 466–481.

[5] Boneh D and Boyen X. Efficient selective-ID secure identity based encryption without random oracles [C]. Advances in Cryptology-EUROCRYPT, Switzerland, May 2-6, 2004, LNCS 3027: 223–238.

[6] Boneh D, Boyen X, and Goh E. Hierarchical identity based encryption with constant ciphertext[C]. Advances in Cryptology-EUROCRYPT, Denmark, May 22-26, 2004, LNCS 3494: 440–456.

[7] Lin J and Zhang F G, *et al*.. A new hierarchical ID-based cryptosystem and CCA-secure PKE [C]. Emerging Directions in Embedded and Ubiquitous Computing, Korea, August 1-4, 2006, LNCS 4097: 362–371.

[8] Chattterjee S and Sarkar P. Generalization of the selectve-ID security model for HIBE protocols[C]. International Workshop on Practice and Theory in Public Key Cryptography, New York, USA, April 24-26, 2006, LNCS 3958: 241–256.

[9] Chow S S M, Hui C K, Yiu S, and Chow K P. Secure hierarchical identity based signature and its application[C]. International Conference on Information and Communications Security, Malaga, Spain, October 27-29, 2004, LNCS 3269: 480–494.

[10] Au M H, Liu J K, and Yuen T H, *et al*, Efficient hierarchical identity based signature in the standard model. http://eprint.iacr.org/2006/080, 2007.5.

[11] Zhang F, Safavi-Naini R, and Susilo W. An efficient signature scheme from bilinear pairings and its applications [C]. International Workshop on Practice and Theory in Public Key Cryptography, Singapore, March 1-4, 2004, LNCS 2947: 277–290.

[12] Canetti R, Halevi S, and Katz J. Chosen-ciphertext security from identity-based encryption[C]. Advances in Cryptology-EUROCRYPT, Switzerland, May 2-6, 2004, LNCS 3027: 207–222.

[13] Waters B. Efficient identity-based encryption without random oracles[C]. In: Advances in Cryptology-Eurocrypt 2005, Aarhus, Denmark, May 22-26, 2005, LNCS 3494: 114–127.

[14] Paterson K G and Schuldt J C N. Efficient identity-based signatures secure in the standard Model[C]. Australasian Conference on Information Security and Privacy, Melbourne, Australia, July 3-5, 2006, LNCS 4058: 207–222.

张乐友：　男，1977 年生，博士生，研究方向为公钥密码体制设计与分析.

胡予濮：　男，1955 年生，教授，博士生导师，主要研究方向为序列密码与分组密码、公钥密码、密码技术应用、网络安全架构.