基于对偶系统的匿名身份基哈希证明系统及其应用

侯红霞[1,2,3],杨 波[1,3],周彦伟[1,3],王 鑫[1,3,4]
(1.陕西师范大学计算机科学学院,陕西西安 710119;2.西安邮电大学通信与信息工程学院,陕西西安 710121;
3.中国科学院信息工程研究所信息安全国家重点实验室,北京 100093;4.陕西科技大学电气与信息工程学院,陕西西安 710021)

摘 要: 基于合数阶双线性群上的静态假设,通过在公开参数及密文中添加一个新的子群中的随机元素实现匿名性,构造了一个匿名的身份基哈希证明系统,利用对偶系统加密技术证明其满足所需的安全性质.将该哈希证明系统应用于抗泄露密码体制中,分别得到一个抗泄露的全安全匿名身份基加密方案和一个CCA-安全的抗泄露匿名身份基加密方案.

关键词: 身份基哈希证明系统;抗泄露;匿名身份基加密;全安全;合数阶双线性群;对偶系统加密
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)07-1675-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.07.020

Anonymous Identity-Based Hash Proof System from Dual System and Its Applications

HOU Hong-xia[1,2,3], YANG Bo[1,3], ZHOU Yan-wei[1,3], WANG Xin[1,3,4]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*; 2. *School of Telecommunication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*; 3. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
4. *College of Electrical and Information Engineering, Shaanxi University of Science and Technology, Xi'an, Shaanxi* 710021, *China*)

Abstract: An anonymous identity-based Hash proof system from static assumptions on composite order bilinear groups is constructed. To achieve the anonymity, random elements of a new subgroup are added to the public parameters and ciphertexts. The desired security properties are proved by dual system encryption technology. Applying the anonymous identity-based Hash proof system to the leakage-resilient cryptography, a leakage-resilient anonymous identity-based encryption scheme with full security and a leakage-resilient anonymous identity-based encryption scheme with CCA-security are derived from it respectively.

Key words: identity-based Hash proof system; leakage-resilience; anonymous identity-based encryption; full security; composite order bilinear groups; dual system encryption

1 引言

哈希证明系统(Hash Proof System, HPS)最初由Cramer和Shoup[1]于2002年提出,用于构造高效的CCA-安全的公钥加密方案.HPS是一种特殊的非交互零知识证明系统,可以看作是定义在集合$\mathcal{X}$上的NP语言$\mathcal{L}\subset\mathcal{X}$中的函数簇(Hash, ProjHash),这些函数以一对相关联的密钥(hk, hp)作为索引,其中哈希密钥hk被称为私钥,投影密钥hp被称为公钥.一个哈希证明系统具有两种重要的性质:"投影性"和"平滑性".所谓"投影性"是指,对于语言$\mathcal{L}$中的每个字$C\in\mathcal{L}$,均有两种方式能够计算出相同的哈希函数值,即:使用投影密钥hp和一个用来证明$C\in\mathcal{L}$的证据w作为输入的公开算法$ProjHash(\mathcal{L},C,\mathrm{hp},w)$和使用哈希密钥hk作为输入的秘密算法$\mathrm{Hash}(\mathcal{L},C,\mathrm{hk})$;所谓"平滑性"是指,若$C\in\mathcal{X}\setminus\mathcal{L}$,则不存在证据$w$,即使已知hp也无法确定$\mathrm{Hash}(\mathcal{L},$

收稿日期:2017-02-01;修回日期:2017-07-28;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61572303, No.61772326);国家重点研发计划(No.2017YFB0802000);中国科学院信息工程研究所信息安全国家重点实验室开放课题(No.2017-MS-03);"十三五"国家密码发展基金(No.MMJJ20170216);中央高校基本科研业务费(No.GK201702004);陕西省自然科学基础研究计划(No.2015JQ6262, No.2017JQ6029);陕西省教育厅专项科研计划(No.16JK1109)

C,hk)的值,即 Hash($\mathscr{L}$,C,hk)的计算结果与 hp 无关. 正是由于"投影性"和"平滑性"这两个重要的特性使得哈希证明系统成为一个重要的密码学原语,广泛应用于许多密码学构造中,尤其在抗泄露密码体制中有很重要的应用.

2010 年,Alwen 等[2]基于 Cramer-Shoup 的 HPS 首次给出身份基哈希证明系统(ID-Based Hash Proof System,IB-HPS)的概念,并表明了一种由 IB-HPS 构造抗泄露 IBE 的通用范式. Chow 等人[3]基于已有方案构造了三个基于静态假设下的 IB-HPS,并由此导出三个高效的抗泄露 IBE 方案. 但这三个方案均不具有匿名性. 2012 年,Chen 等人[4]深入挖掘 IB-HPS 的性质,给出 IB-HPS 的匿名性概念,这为抗泄露匿名 IBE 方案的设计提供了一种很好的思路. 但 Chen 等人给出的四个匿名 IB-HPS 中,有三个是在随机预言机模型下构造的,另一个虽然在标准模型下构造,但所基于的假设为非静态假设.

本文在合数阶双线性群上设计了一个匿名的身份基哈希证明系统,通过使用一个额外子群中的随机数盲化公开参数和密文实现其匿名性,并采用对偶系统加密技术[5]在标准模型下证明其所满足的安全性质. 由该匿名 IB-HPS 得到一个全安全的抗泄露匿名 IBE 方案一个 CCA-安全的抗泄露匿名身份基加密方案.

2 预备知识

2.1 合数阶双线性群

利用一个群发生器 G,以安全参数 κ 作为输入,输出一个群描述 $I=(N=p_1p_2p_3p_4,G,G_T,\mathrm{e})$,其中 p_1,p_2,p_3,p_4 分别是 $\Theta(\kappa)$ 比特的不同素数,G 和 G_T 是阶为 N 的循环群,$\mathrm{e}:G\times G\to G_T$ 是一个双线性映射,满足以下性质:

(1)(双线性性)$\forall g,h\in G,a,b\in Z_N,\mathrm{e}(g^a,h^b)=\mathrm{e}(g,h)^{ab}$.

(2)(非退化性)$\exists g\in G$,使得 $\mathrm{e}(g,g)$ 在 G_T 中的阶为 N.

(3)(可计算性)G 和 G_T 中的操作以及双线性映射 e 都是多项式时间内可计算的.

2.2 安全性假设

本文方案基于的复杂性假设如下:

假设 1,2,3,4 定义变量 $PP'=(N,G,G_T,\mathrm{e})\leftarrow G(1^\kappa),\beta,z\xleftarrow{\$}Z_N,X_1\xleftarrow{\$}G_{p_1},X_4,Y_4\xleftarrow{\$}G_{p_4},X_2,Y_2,Z_2\xleftarrow{\$}G_{p_2},X_3,Y_3\xleftarrow{\$}G_{p_3}$,令

$D^{(1)}=(X_1,X_3,X_4)$

$T_0^{(1)}\xleftarrow{\$}G_{p_1p_2},T_1^{(1)}\xleftarrow{\$}G_{p_1}$,

$D^{(2)}=(X_1,X_3,X_4,Y_2Y_4)$

$T_0^{(2)}\xleftarrow{\$}G_{p_1p_2p_4},T_1^{(2)}\xleftarrow{\$}G_{p_1p_4}$

$D^{(3)}=(X_1,Y_2Y_3,Y_1X_2Y_4,X_3)$

$T_0^{(3)}\xleftarrow{\$}G_{p_1p_2p_3},T_1^{(3)}\xleftarrow{\$}G_{p_1p_3}$

$D^{(4)}=(X_1,X_1^\beta X_2,X_1^z Y_2Y_4,Z_2X_3,X_4)$

$T_0^{(4)}\leftarrow \mathrm{e}(w,w)^{\beta z},T_1^{(4)}\xleftarrow{\$}G_T$

定义 PPT 算法 $\mathscr{A}$ 攻击 1 的优势为 $Adv_{\mathscr{A}}^{(i)}(\kappa)=|\Pr[\mathscr{A}(PP',D^{(i)},T_0^{(i)})=1]-\Pr[\mathscr{A}(PP',D^{(i)},T_1^{(i)})=1]|$,其中 $i\in\{1,2,3,4\}$. 如果对于所有的算法 $\mathscr{A}$ 都有 $Adv_{\mathscr{A}}^{(i)}(\kappa)\leqslant\mathrm{negl}(\kappa)$,则假设 i 成立.

3 匿名身份基哈希证明系统的构造

一个匿名 IB-HPS 应满足:正确性、有效/无效密文不可区分性、平滑性以及匿名性,安全模型详见文献[2]和[4].

3.1 基于对偶系统的匿名 IB-HPS

本节利用一个阶为 $N=p_1p_2p_3p_4$ 的合数阶群,构造了一个匿名的 IB-HPS(ANO-IB-HPS),其中子群 G_{p_4} 中的元素用于提供匿名性,G_{p_3} 中的元素用于随机化处理,G_{p_2} 中的元素不出现在实际方案中,仅用于构造半功能密钥和半功能密文.

ANO-IB-HPS:

$-(mpk,msk)\leftarrow\mathrm{Setup}(1^\kappa):(N,G,G_T,\mathrm{e})\leftarrow G(1^\kappa)$,随机选取 $w,u,h\xleftarrow{\$}G_{p_1},R_u,R_h,R_w\xleftarrow{\$}G_{p_4},\alpha,\beta\xleftarrow{\$}Z_N$,计算 $U=uR_u,H=hR_h,W=wR_w$,令 $mpk=(N,G,G_T,\mathrm{e},U,H,W,\mathrm{e}(w,w)^\alpha,\mathrm{e}(w,w)^\beta)$,$msk=(w,u,h,X_3,\alpha,\beta)$,其中 X_3 是 G_{p_3} 的生成元.

$-(sk_{id})\leftarrow\mathrm{KeyGen}(id,msk)$:对于 $id\in Z_N$,随机选取 $t,r,\rho,\rho'\xleftarrow{\$}Z_N$,输出 $sk_{id}=(s_1,s_2,s_3)=(w^\alpha w^{-\beta t}(u^{id}h)^rX_3^\rho,w^{-r}X_3^{\rho'},t)$.

$-(C,k)\leftarrow\mathrm{Encap}(id)$:选取 $z\xleftarrow{\$}Z_N,R_4,R_4'\xleftarrow{\$}G_{p_4}$ 对于 $id\in Z_N$,输出 $C=(c_1,c_2,c_3)=(W^zR_4,(U^{id}H)^z\cdot R_4',\mathrm{e}(w,w)^{\beta z})$ 和 $k=\mathrm{e}(w,w)^{\alpha z}$.

$-C\leftarrow\mathrm{Encap}^*(id)$:选取 $z,z'\xleftarrow{\$}Z_N$ 且 $z\neq z',R_4,R_4'\xleftarrow{\$}G_{p_4}$. 输出 $C=(c_1,c_2,c_3)=(W^zR_4,(U^{id}H)^zR_4',\mathrm{e}(w,w)^{\beta z'})$.

$-k\leftarrow\mathrm{Decap}(C,sk_{id})$:输入密文 C 和用户秘密钥 sk_{id},输出 $k=e(c_1,s_1)e(c_2,s_2)c_3^{s_3}$.

3.2 安全性证明

①解封装的正确性

容易验证对于有效密文 C 的解封装是正确的.

②有效/无效密文不可区分性

我们采用对偶系统加密技术证明 ANO-IB-HPS 满足有效/无效密文不可区分性,为此引入半功能密钥和

半功能密文.

半功能密钥　先创建一个正常密钥(s_1,s_2,s_3),选取随机元素$X_2\overset{\$}{\leftarrow}G_{p_2}$和$\theta_k\overset{\$}{\leftarrow}Z_N$,得到半功能密钥$(s'_1,s'_2,s'_3)=(s_1X_2^{\theta_k},s_2X_2^{-1},s_3)$.

半功能密文　先创建一个正常密文(c_1,c_2,c_3),选取随机元素$Y_2\overset{\$}{\leftarrow}G_{p_2}$和$\theta_c\overset{\$}{\leftarrow}Z_N$,得到半功能密文$(c'_1,c'_2,c'_3)=(c_1Y_2,c_2Y_2^{\theta_c},c_3)$.

当用半功能密钥解封装半功能密文时,会出现额外的一项$e(Y_2,X_2)^{(\theta_k-\theta_c)}$. 我们定义了一系列游戏,基于2.2节的安全性假设,利用混合论证技术证明游戏之间的不可区分性.

$Game_{Real}$:正常的安全性游戏,挑战者发送给敌手的是一个(正常的)有效密文.

$Game_{Restricted}$:与$Game_{Real}$相同,除了一个限制:敌手询问的所有身份都不能等于挑战身份$id^*\bmod p_2$. 后续游戏都要保留这个限制.

$Game_0$:与$Game_{Restricted}$相同,但返回给敌手的密文都是半功能的.

$Game_i$:用$L(\kappa)$表示密钥提取询问中不同身份的最大个数. 对于$i\in[1,L-1]$,$Game_i$和$Game_0$的区别在于:前i个身份除了挑战身份之外的私钥都是半功能的.

$Game_{SIVC}$:与$Game_{L-1}$的不同之处是挑战密文为半功能无效密文.

$Game'_i$:对于每个$i\in[1,L-1]\cup\{0\}$,除了密文是无效的之外,$Game'_i$如同$Game_i$.

$Game_{NIC}$:正常的安全性游戏,挑战者发送给敌手的是一个(正常的)无效密文.

引理 1　若存在一个PPT算法$\mathscr{A}$使得$Adv^{Game_{Real}}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}-Adv^{Game_{Restricted}}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}=\varepsilon$,则可构造一个PPT算法$\mathscr{B}$至少以$\varepsilon$的优势攻破假设1或假设2或假设3.

证明　算法$\mathscr{B}$以$X_1,X_3,X_4,T_\nu(\nu\in\{0,1\})$作为输入,均匀随机地选择$a,b,\alpha,\beta\overset{\$}{\leftarrow}Z_N$,令$u=X_1^a,h=X_1^b,w=X_1,R_u=X_4^a,R_h=X_4^b,R_w=X_4$,生成$mpk$和$msk$. 因为$\mathscr{B}$有主密钥$msk$,所以他可以为所有询问的身份生成私钥.

由$Adv^{Game_{Real}}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}-Adv^{Game_{Restricted}}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}=\varepsilon$知,$\mathscr{A}$会以$\varepsilon$的概率发起询问$id=id^*\bmod p_2$. 这意味着$\mathscr{B}$可以通过计算$Q=N/\gcd(id-id^*,N)$得到$N=p_1p_2p_3p_4$的一个非平凡因子. 存在三种情况:

①$p_1\mid Q$;②$Q=p_4$;③$Q=p_3$或$Q=p_3p_4$.

至少有一种情况发生的概率大于等于$\varepsilon/3$. 在第一种情况下,$\mathscr{B}$可以通过验证T_ν^Q是否为单位元攻破假设1. 在第二种情况下,$\mathscr{B}$可以通过验证$e((Y_2Y_4)^Q,T_\nu)$是否为单位元攻破假设2. 在第三种情况下,$\mathscr{B}$可以通过验证$e((Y_2Y_3)^Q,T_\nu)$是否为单位元攻破假设3.

引理 2　若存在一个PPT算法$\mathscr{A}$使得$Adv^{Game_{Restricted}}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}-Adv^{Game_0}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}=\varepsilon$,则可构造一个PPT算法$\mathscr{B}$以$\varepsilon$的优势攻破假设2.

证明　算法$\mathscr{B}$以$X_1,X_3,X_4,Y_2Y_4,T_\nu(\nu\in\{0,1\})$作为输入,均匀随机地选择$a,b,\alpha,\beta\overset{\$}{\leftarrow}Z_N$,如同引理1设置$mpk$和$msk$,为$\mathscr{A}$询问的身份生成私钥. 在挑战阶段,$\mathscr{B}$在收到挑战身份$id^*$后,利用$T_\nu$构造挑战密文如下:

$$(c_1^*,c_2^*,c_3^*)=(T_\nu,T_\nu^{a\cdot id^*+b},e(T_\nu,w)^\beta)$$

如果$T_\nu\in G_{p_1p_4}$,$\mathscr{A}$执行游戏$Game_{Restricted}$. 如果$T_\nu\in G_{p_1p_2p_4}$,则挑战密文是一个半功能密文($\theta_c=a\cdot id^*+b$),$\mathscr{A}$执行游戏$Game_0$. 由于$\theta_c\bmod p_2$与$a\bmod p_1p_4$和$b\bmod p_1p_4$不相关,所以挑战密文的分布是正确的. 故若$\mathscr{A}$以ε的优势成功区分$Game_{Restricted}$和$Game_0$,则$\mathscr{B}$能以同样的优势攻破假设2.

引理 3　若存在一个PPT算法$\mathscr{A}$使得$Adv^{Game_{i-1}}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}-Adv^{Game_i}_{ANO\text{-}IB\text{-}HPS,\mathscr{A}}=\varepsilon$,则可构造一个PPT算法$\mathscr{B}$以至少$\varepsilon/L$的优势攻破假设3.

证明　$\mathscr{B}$在挑战阶段之前不能确定哪一个身份是挑战身份,只能均匀随机地选择$i^*\overset{\$}{\leftarrow}[1,L-1]$作为对挑战身份的猜测,猜对的概率为$1/L$. 对于第$i^*$次密钥询问,$\mathscr{B}$总以正常密钥作为回答.

算法$\mathscr{B}$以$X_1,Y_1X_2Y_4,X_3,Y_2Y_3,T_\nu(\nu\in\{0,1\})$作为输入,均匀随机地选择$a,b,\alpha,\beta\overset{\$}{\leftarrow}Z_N$,设置$msk=(w,u,h,X_3,\alpha,\beta)$.

对于前$i-1$个密钥询问,$\mathscr{B}$构造合适分布的半功能密钥,回答如下:

$$s_1=w^\alpha w^{-\beta t}(u^{id}h)^r(Y_2Y_3)^\rho,s_2=w^{-r}(Y_2Y_3)^{\rho'}X_3^{\rho''},s_3=t$$

其中id表示被询问身份,$t,r,\rho,\rho',\rho''\overset{\$}{\leftarrow}Z_N$.

对于第i个身份,$\mathscr{B}$回答如下:

$$s_1=w^\alpha w^{-\beta t}T_\nu^{\theta_k}X_3^\rho,s_2=T_\nu^{-1},s_3=t$$

其中$t,\rho\overset{\$}{\leftarrow}Z_N,\theta_k=a\cdot id+b$. 其余的询问,$\mathscr{B}$用主密钥生成正常私钥来回答.

在挑战阶段,若$\mathscr{B}$对于挑战身份id^*的猜测不正确,则退出. 否则$\mathscr{B}$给$\mathscr{A}$返回挑战密文:

$$(c_1^*,c_2^*,c_3^*)=((Y_1X_2Y_4),(Y_1X_2Y_4)^{a\cdot id^*+b},e((Y_1X_2Y_4),w)^\beta)$$

这是一个合适分布的半功能密文,其中$\theta_c=a\cdot id^*+b$. 因为只要非挑战身份$id\neq id^*\bmod p_2$,在$\mathscr{A}$看来$\theta_k=a\cdot id+b$和$\theta_c=a\cdot id^*+b$就是模p_2下的随机分布.

如果$T_\nu\in G_{p_1p_3}$,$\mathscr{A}$执行游戏$Game_{i-1}$;如果$T_\nu\in G_{p_1p_2p_3}$,$\mathscr{A}$执行游戏$Game_i$. 故若$\mathscr{A}$以ε的优势成功区分$Game_{i-1}$和$Game_i$,则$\mathscr{B}$能以ε/L的优势攻破假设3.

引理 4 若存在一个 PPT 算法 $\mathscr{A}$ 使得 $Adv^{\mathrm{Game}_{L-1}}_{\text{ANO-IB-HPS},\mathscr{A}} - Adv^{\mathrm{Game}_{SIVC}}_{\text{ANO-IB-HPS},\mathscr{A}} = \varepsilon$,则可构造一个 PPT 算法 $\mathscr{B}$ 以 ε/L 的优势攻破假设 4.

证明 由假设 4,算法 $\mathscr{B}$ 以 $X_1, X_1^{\beta}X_2, X_1^{z}Y_2Y_4, Z_2, X_3, X_4, T_{\nu}(\nu \in \{0,1\})$ 作为输入,均匀随机地选择 $a, b, t^*, \tilde{\alpha} \xleftarrow{\$} Z_N$,隐式地令 $\alpha = t^*\beta + \tilde{\alpha}$,$\mathscr{B}$ 并不知道主密钥. 计算:$\mathrm{e}(w,w)^{\beta} = \mathrm{e}(X_1^{\beta}X_2, X_1)$,$\mathrm{e}(w,w)^{\alpha} = (\mathrm{e}(w,w)^{\beta})^{t^*} \cdot \mathrm{e}(w,w)^{\tilde{\alpha}}$,其余参数设置如前. 将公开参数发送给 $\mathscr{A}$. 同样,$\mathscr{B}$ 以 $1/L$ 的概率猜对挑战身份的位置 $i^* \xleftarrow{\$} [1, L-1]$.

阶段 1 中,当 $\mathscr{A}$ 对 $id \neq id^*$ 的身份发起询问时,$\mathscr{B}$ 如下生成半功能密钥作为回答:

选取随机指数 $\tilde{t}, r, \rho, \rho', \rho'', \rho''' \xleftarrow{\$} Z_N$ 并计算

$$s'_1 = (X_1^{\beta}X_2)^{\tilde{t}} w^{\tilde{\alpha}} (u^{id} h)^{r} (X_3)^{\rho} (Z_2)^{\rho'''}$$

$$s'_2 = w^{-r} (X_3)^{\rho'} Z_2^{\rho''}$$

$$s'_3 = t^* - \tilde{t}$$

因为 $w^{\tilde{\alpha}}(w^{\beta})^{\tilde{t}} = w^{\alpha} w^{-\beta s'_3}$,所以这样构造的半功能密钥是合适分布的.

对于 id^* 的私钥,$\mathscr{B}$ 随机选取 $r, \rho, \rho' \xleftarrow{\$} Z_N$ 并计算正常密钥:$s_1^* = w^{\tilde{\alpha}} (u^{id^*} h)^{r} (X_3)^{\rho}$,$s_2^* = w^{-r} (X_3)^{\rho'}$,$s_3^* = t^*$,$\mathscr{A}$ 将挑战身份 id^* 发送给 $\mathscr{B}$,$\mathscr{B}$ 返回 $(c_1^*, c_2^*, c_3^*) = ((X_1^{z}Y_2Y_4), (X_1^{z}Y_2Y_4)^{a \cdot id^* + b}, T_{\nu})$,因为 $a, b \bmod p_1$ 与 $\theta_c \bmod p_2$ 不相关,所以 $\theta_c = a \cdot id^* + b$ 在敌手 $\mathscr{A}$ 看来是随机的.

如果 $T_{\nu} = \mathrm{e}(w,w)^{\beta z}$,$\mathscr{A}$ 执行游戏 Game_{L-1};如果 $T_{\nu} \in G_T$,$\mathscr{A}$ 执行游戏 Game_{SIVC}. 故若 $\mathscr{A}$ 以 ε/L 的优势成功区分 Game_{L-1} 和 Game_{SIVC},则 $\mathscr{B}$ 以同样的优势攻破假设 4.

引理 5 若存在一个 PPT 算法 $\mathscr{A}$ 使得 $Adv^{\mathrm{Game}'_{i}}_{\text{ANO-IB-HPS},\mathscr{A}} - Adv^{\mathrm{Game}'_{i-1}}_{\text{ANO-IB-HPS},\mathscr{A}} = \varepsilon$,则可构造一个 PPT 算法 $\mathscr{B}$ 以 ε/L 的优势攻破假设 3.

引理 6 若存在一个 PPT 算法 $\mathscr{A}$ 使得 $Adv^{\mathrm{Game}'_{0}}_{\text{ANO-IB-HPS},\mathscr{A}} - Adv^{\mathrm{Game}_{NIC}}_{\text{ANO-IB-HPS},\mathscr{A}} = \varepsilon$,则可构造一个 PPT 算法 $\mathscr{B}$ 以 ε/L 的优势攻破假设 2.

证明 引理 5 和 6 的证明与引理 3 和 2 的证明类似.

定理 1 如果假设 1,2,3,4 成立,则 ANO-IB-HPS 是有效/无效密文不可区分的.

证明 设 $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ 分别是攻击假设 1,2,3,4 的最大优势,则对于任意敌手 $\mathscr{A}$,有以下结论成立:

$$Adv^{\mathrm{Game}_{Real}}_{\text{ANO-IB-HPS},\mathscr{A}} - Adv^{\mathrm{Game}_{NIC}}_{\text{ANO-IB-HPS},\mathscr{A}}$$

$$\leqslant 3\max(\varepsilon_1, \varepsilon_2, \varepsilon_3) + \varepsilon_2 + L(L-1)(\varepsilon_3 + \varepsilon_4) + L(\varepsilon_2 + \varepsilon_4)$$

故若 $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ 是可忽略的,则任意 PPT 敌手区分有效密文和无效密文的优势可忽略.

③平滑性

对于 ANO-IB-HPS 中无效密文的解封装为:

$$\mathrm{e}(c_1, s_1)\mathrm{e}(c_2, s_2)c_3^{s_3} = \mathrm{e}(w,w)^{\alpha z}\mathrm{e}(w,w)^{t\beta(z'-z)}$$

对于任意无效密文 C,$\mathrm{Decap}(C, sk_{id})$ 的输出是 G_T 上的均匀分布. 故平滑性成立.

④匿名性

给定任意两个身份 $id_0, id_1 \in \mathscr{ID}$,令 $C_i \leftarrow \mathrm{Encap}^*(id_i)$,对于无效密文 C_i 的解封装为 $k_i = \mathrm{e}(w,w)^{\alpha z_i}\mathrm{e}(w,w)^{t\beta(z'_i - z_i)}$,其中 $i \in \{0,1\}$. 显然,k_i 为 G_T 上的均匀分布,由平滑性和三角不等式可得:

$$SD((C_0,k_0),(C_1,k_1)) \leqslant SD((C_0,k_0),(C_0,k'_0)) + SD((C_0,k'_0),(C_1,k'_1)) + SD((C_1,k'_1),(C_1,k_1)) \leqslant \mathrm{negl}(\kappa)$$

其中 $k'_i \xleftarrow{\$} K$. 故匿名性成立.

3.3 安全性分析

表 1 将 ANO-IB-HPS 与文献[3]和[4]中的 IB-HPS 进行了对比,其中 ROM 表示随机预言机模型;STM 表示标准模型. 通过比较分析发现,我们的方案在安全性方面有很大提升.

表 1 本文方案与现有 IB-HPS 的安全性对比

方案	复杂性假设(静/非静态)	安全模型	匿名性
文献[3]-1	DBDH(静态)	STM	非匿名
文献[3]-2	DBDH(静态)	STM	非匿名
文献[3]-3	假设 1,3,4(静态)	STM	非匿名
文献[4]-1	DBDH(静态)	ROM	匿名
文献[4]-2	q-ABDHE(非静态)	STM	匿名
文献[4]-3	QR(静态)	ROM	匿名
文献[4]-4	LWE (静态)	ROM	匿名
本文	假设 1,2,3,4(静态)	STM	匿名

4 ANO-IB-HPS 的应用

4.1 抗泄露全安全的匿名 IBE 方案

Alwen 等人在 2010 年表明利用提取器可以将平滑 IB-HPS 转化为 ℓ-抗泄露的 IBE. 故基于该理论,由 ANO-IB-HPS 可以得到一个 ℓ-抗泄露的全安全的匿名 IBE 方案(LR-ANO-IBE). 该方案中的 Setup 和 KenGen 算法与 ANO-IB-HPS 相同,Encrypt 和 Decrypt 算法描述如下:

Encrypt(id, M):对于消息 $M \in \mathscr{M}$,选取 s 做为提取器的随机种子,计算 $(C_1, k) \leftarrow \mathrm{Encap}(id)$,令 $C_2 = \mathrm{Ext}(k,s) \oplus M$. 输出 $CT = (C_1, s, C_2)$.

Decrypt(CT, sk_{id}):由接收到的 $CT = (C_1, s, C_2)$,计算 $k \leftarrow \mathrm{Decap}(C, sk_{id})$. 输出 $M = C_2 \oplus \mathrm{Ext}(k,s)$.

其中,Ext:$\mathscr{K}\to\{0,1\}^{v}$ 是一个$(\mu-\ell,\varepsilon)$-提取器,$\varepsilon\leqslant\mathrm{negl}(\kappa)$.

该方案的安全性证明与文献[2]相类似.

4.2　抗泄露 CCA-安全的匿名 IBE 方案

2016 年,Baek 等人[6]在标准模型下提出了一种由 2-平滑的 IB-HPS 构造 CCA-安全的 IBE 方案的通用方法. 基于该方法和 Alwen 的理论,我们构造了一个 CCA-安全的抗泄露匿名 IBE 方案(LR-ANO-IBE′),并对其安全性加以证明.

首先应用 4-wise 独立的哈希函数将 ANO-IB-HPS 转变为 ε_2-2-平滑的 ANO-IB-HPS′.

- $(mpk,msk)\leftarrow\mathrm{Setup}(1^{\kappa})$:$(N,G,G_T,e)\leftarrow G(1^{\kappa})$,随机选取 $w,u,h\xleftarrow{\$}G_{p_1},R_u,R_h,R_w\xleftarrow{\$}G_{p_4},\alpha,\beta\xleftarrow{\$}Z_N$,计算 $U=uR_u,H=hR_h,W=wR_w$,令 $\mathscr{H}=\{H:\mathscr{K}\to\{0,1\}^{2\log N}\}$ 是一个 4-*wise* 独立的哈希函数簇,随机选取 $H\in\mathscr{H}$. $mpk=(N,G,G_T,e,U,H,W,H,\mathrm{e}(w,w)^{\alpha},e(w,w)^{\beta})$,$msk=(w,u,h,X_3,\alpha,\beta)$,其中 X_3 是 G_{p_3}的生成元.
- $(sk_{id})\leftarrow\mathrm{KeyGen}(id,msk)$:对于 $id\in Z_N$,随机选取 $t,r,\rho,\rho'\xleftarrow{\$}Z_N$,输出 $sk_{id}=(s_1,s_2,s_3)=(w^{\alpha}w^{-\beta t}\cdot(u^{id}h)^{r}X_3^{\rho},w^{-r}X_3^{\rho'},t)$.
- $(C,(k_1,k_2))\leftarrow\mathrm{Encap}(id)$:选取 $z\xleftarrow{\$}Z_N,R_4,R_4'\xleftarrow{\$}G_{p_4}$. 对于 $id\in Z_N$,计算 $C=(c_1,c_2,c_3)=(W^{z}R_4,(U^{id}H)^{z}R_4',\mathrm{e}(w,w)^{\beta z})$,$k=\mathrm{e}(w,w)^{\alpha z}$,$(k_1,k_2)\leftarrow H(k)$. 输出 C 和(k_1,k_2).
- $C\leftarrow\mathrm{Encap}^{*}(id)$:选取 $z,z'\xleftarrow{\$}Z_N$ 且 $z\neq z'$,$R_4,R_4'\leftarrow G_{p4}$. 输出 $C=(c_1,c_2,c_3)=(W^{z}R_4,(U^{id}H)^{z}\cdot R_4',e(w,w)^{\beta z'})$.
- $(k_1,k_2)\leftarrow\mathrm{Decap}(C,sk_{id})$:输入密文 C 和用户私钥 sk_{id},计算 $k=e(c_1,s_1)e(c_2,s_2)c_3^{s_3}$,$(k_1,k_2)\leftarrow H(k)$,输出$(k_1,k_2)$.

文献[6]中已表明上述转变可得到的 ε_2-2-平滑的 ANO-IB-HPS′. 进一步,我们给出 ℓ抗泄露的 CCA-安全匿名 IBE 方案(LR-ANO-IBE′). 该方案中的 Setup 和 KenGen 算法与 ANO-IB-HPS′相同,Encrypt 和 Decrypt 算法描述如下:

Encrypt(id,M):随机选取 $z\xleftarrow{\$}Z_N,R_4,R_4'\xleftarrow{\$}G_{p_4}$. 对于 $id\in Z_N$,计算$(C,(k_1,k_2))\leftarrow$ ANO-IB-HPS′. Encap(id),其中$|k_1|=|k_2|=\log N$. 令 Ext:$\{0,1\}^{\log N}\times\mathrm{Seed}\to\{0,1\}^{v}$ 是一个$(\log N-\ell,\varepsilon)$-提取器,MAC:$\log N\times\{0,1\}^{v}\to\{0,1\}^{\lambda}$ 是一个抗一次性选择消息攻击(OT-CMA)的消息认证码. 选取 $s\xleftarrow{\$}Z_N$ 作为提取器的随机种子,计算 $C_1=\mathrm{Ext}(k_1,s)\oplus M$ 和 $C_2=\mathrm{MAC}_{k_2}(C_1)$. 返回密文 $CT=(C,C_1,C_2,s)$.

Decrypt(CT,sk_{id}):输入密文 $CT=(C,C_1,C_2,s)$ 和用户私钥 sk_{id},计算$(k_1,k_2)\leftarrow$ ANO-IB-HPS′. Decap(C,sk_{id}),验证 $C_2=\mathrm{MAC}_{k_2}(C_1)$是否成立. 若成立,则返回 $M=\mathrm{Ext}(k_1,s)\oplus C_1$;否则拒绝.

定理 2　若 ANO-IB-HPS′是 ε_2-2-平滑的匿名 IB-HPS,MAC 是抗 OT-CMA 攻击的消息认证码,则 LR-ANO-IBE′是一个 CCA-安全的抗泄露匿名 IBE 方案.

证明　依然采用混合论证的方法证明相邻两个游戏之间的不可区分性.

以下令 $\Pr[G_i]=\Pr[\mathrm{Game}_i\text{ 中 }b'=b]$.

Game_0:正常的 CCA-安全抗泄露匿名 IBE 游戏.

Game_1:与 Game_0 的区别在于:挑战阶段挑战者用私钥 sk_{id_i}做解封装计算,由 ANO-IB-HPS′解封装的正确性可知 $\Pr[G_0]=\Pr[G_1]$.

Game_2:在 Game_1 基础上进一步修改游戏:挑战阶段中挑战者用无效封装算法计算 C_b^{*},由有效/无效密文不可区分性知,若 $\mathscr{A}$ 能成功区分 Game_1 与 Game_2,则可构建 PPT 敌手 $\mathscr{B}$ 攻破 ANO-IB-HPS 的有效/无效密文不可区分性. 故$|\Pr[G_1]-\Pr[G_2]|\leqslant Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}$.

Game_3:在 Game_2 的基础上修改解密预言机如算法 1 所示. 令(id_i,CT_i)是一个解密询问,$1\leqslant i\leqslant Q$(Q 是最大询问次数).

算法 1　Game_3 中的解密预言机

```
1:if id_i ≠ id_b^* then
2:      sk_{id_i} ← ANO-IB-HPS′. KeyGen(id_i, msk)
3:      (k_{1_i}, k_{2_i}) ← ANO-IB-HPS′. Decap(C_i, sk_{id_i})
4:      if C_{2_i} ≠ MAC_{k_{2_i}}(C_{1_i}) then return ⊥
5:      return M_i = Ext(k_{1_i}, s_i) ⊕ C_{1_i}
6:else
7:      if C_i = C_b^* then
8:          if C_{2_i} ≠ MAC_{k_{2_b}^*}(C_{1_i}) then return ⊥
9:          return M_i = Ext(k_{1_b}^*, s_i) ⊕ C_{1_i}
10:     else if C_i ∉ V // C_i ← ANO-IB-HPS′. Eecap^*(id_i^*)
11:         sk_{id_b^*} ← ANO-IB-HPS′. KeyGen(id_b^*, msk)
12:         (k_{1_i}, k_{2_i}) ← ANO-IB-HPS′. Decap(C_i, sk_{id_b^*})
13:         if C_{2_i} ≠ MAC_{k_{2_i}}(C_{1_i}) then return ⊥
14:         return ⊥
15:     else
16:         sk_{id_b^*} ← ANO-IB-HPS′. KeyGen(id_b^*, msk)
17:         (k_{1_i}, k_{2_i}) ← ANO-IB-HPS′. Decap(C_i, sk_{id_b^*})
18:         if C_{2_i} ≠ MAC_{k_{2_i}}(C_{1_i}) then return ⊥
19:         return M_i = Ext(k_{1_b}^*, s_i) ⊕ C_{1_i}
```

令 E_3 表示事件:密文仅被 Game_3 中解密预言机的第 14 条规则拒绝. E'_3 表示事件:第 j 次解密询问仅在第 14 条规则被拒绝,$1\leqslant j\leqslant Q$. 显然 $\Pr[E_3]\leqslant$

$Q\Pr[E'_3]$. 只要 E_3 不发生,Game_2 与 Game_3 就是相同的,故有 $|\Pr[G_2]-\Pr[G_3]|\leqslant\Pr[E_3]\leqslant Q\Pr[E'_3]$.

Game_4:生成挑战密文时用一个随机密钥 (k'_{1_b},k'_{2_b}) 替代 $(k^*_{1_b},k^*_{2_b})$. 假设 (id^*_b,CT_i) 是敌手提交的解密询问,$CT_i\neq CT^*_b$. Game_3 与 Game_4 的不同由以下统计距离来界定:$\text{SD}[(mpk,\text{ID}^*_b,(k_{1_i},k_{2_i}),(k^*_{1_b},k^*_{2_b})),(mpk,\text{ID}^*_b,(k_{1_i},k_{2_i}),(k'_{1_b},k'_{2_b}))]$. 故由 ANO-IB-HPS′的 ε_2-2-平滑性可知,$|\Pr[G_3]-\Pr[G_4]|\leqslant\varepsilon_2$.

Game_5:更改算法 1 中解密预言机的规则 9 为"return $\perp$". 令 E_5 表示事件:Game_5 中第 9 条规则被执行. 若 E_5 不发生,则 Game_4 与 Game_5 相同. 故有 $|\Pr[G_4]-\Pr[G_5]|\leqslant\Pr[E_5]$.

下面表明 $\Pr[E_5]\leqslant QAdv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}}(\kappa)$.

我们可以构造一个敌手 $\mathscr{F}$ 攻破 MAC 方案的 OT-CMA 安全性. $\mathscr{F}$ 为 $\mathscr{A}$ 模拟 Game_5 的环境:即随机选取 (k'_{1_b},k'_{2_b}),生成 $C^*_{1_b}=\text{Ext}(k'_{1_b},s_b)\oplus M_b$,随后 $\mathscr{F}$ 用 $C^*_{1_b}$ 询问其 MAC 预言机,得到 $C^*_{2_b}=\text{MAC}_{k'_{2_b}}(C^*_{1_b})$. 若 $\mathscr{A}$ 提交解密询问 $CT_i=(C^*_b,C_{1_i},C_{2_i},s_i)$ 且规则 9 被执行,则说明 CT_i 包含一个伪造 (C_{1_i},C_{2_i}),其中 $C_{1_i}\neq C^*_{1_b}$,而 C_{2_i} 是 C_{1_i} 在随机密钥 k'_{2_b} 加密下的一个有效 MAC. 这样的 CT_i 存在于 Q 次解密询问中. 故有 $\Pr[E_5]\leqslant QAdv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}}(\kappa)$.

Game_6:与 Game_5 的区别在于:随机选取 k'_{2_b},生成挑战密文 $CT^*_b=(C^*_b,C^*_{1_b},C^*_{2_b},s_b)$,其中 $C^*_{1_b}\leftarrow U_\nu$,$C^*_{2_b}=\text{MAC}_{k'_{2_b}}(C^*_{1_b})$. 显然,$\text{Game}_6$ 中敌手获胜的优势为 0. 故 $|\Pr[G_5]-\Pr[G_6]|\leqslant\varepsilon_{ext}$.

Game'_4:如同 Game_3,但修改解密预言机的规则 12 为均匀随机地选取 (k'_{1_i},k'_{2_i}). 令 $E'_{4'}$ 表示事件:在 Game'_4 中第 j 次解密询问时规则 14 被执行. 显然,Game_3 和 Game'_4 的两个输入分布由以下统计距离界定:$\text{SD}[(mpk,\text{ID}^*_b,(k^*_{1_b},k^*_{2_b}),(k_{1_j},k_{2_j})),(mpk,\text{ID}^*_b,(k^*_{1_b},k^*_{2_b}),(k'_{1_j},k'_{2_j}))]$. 故由 ANO-IB-HPS′的 ε_2-2-平滑性可知 $|\Pr[E'_3]-\Pr[E'_{4'}]|\leqslant\varepsilon_2$,如果 $\mathscr{A}$ 提交的解密询问 CT_j 在算法 1 的第 14 行被执行,这意味着存在一个伪造 (C_{1_j},C_{2_j}). 由此可构造一个伪造者 $\mathscr{F}'$. 故 $\Pr[E'_{4'}]\leqslant Adv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}'}(\kappa)$.

由以上分析可知:

$$\begin{aligned}\Pr[G_0]&=\Pr[G_1]\leqslant\Pr[G_2]+Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}\\&\leqslant\Pr[G_3]+Q\Pr[E'_3]+Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}\\&\leqslant\Pr[G_4]+\varepsilon_2+Q\Pr[E'_3]+Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}\\&\leqslant\Pr[G_5]+\Pr[E_5]+\varepsilon_2+Q\Pr[E'_3]\\&\quad+Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}\\&\leqslant\Pr[G_6]+\varepsilon_{ext}+QAdv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}}(\kappa)+\varepsilon_2\\&\quad+Q(Adv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}'}(\kappa)+\varepsilon_2)+Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}\\&=\frac{1}{2}+\varepsilon_{ext}+QAdv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}}(\kappa)+\varepsilon_2\\&\quad+Q(Adv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}'}(\kappa)+\varepsilon_2)+Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}\end{aligned}$$

故

$$Adv^{\text{LR-ANO-IBE}'}_{\text{CCA},\mathscr{A}}(\kappa,\mathscr{C})=\left|\Pr[G_0]-\frac{1}{2}\right|\leqslant\varepsilon_{ext}+\varepsilon_2+QAdv^{\text{OT-CMA}}_{\text{MAC},F}(\kappa)+Q(Adv^{\text{OT-CMA}}_{\text{MAC},\mathscr{F}'}(\kappa)+\varepsilon_2)+Adv^{\text{VI-IND}}_{\text{ANO-IB-HPS},\mathscr{B}}$$

4.3 安全性分析

表 2 将本文方案与现有匿名 IBE 方案就复杂性假设、安全模型、抗泄露等方面进行比较,通过比较发现,本文方案在安全性方面有很大提升.

表 2 本文方案与已有匿名 IBE 方案的安全性对比

方案	复杂性假设(合/素数阶群-静/非静态)	安全模型	攻击类型	是否抗泄露	安全性
文献[4]-1	DBDH(素数阶群-静态)	ROM	Adaptive-ID	是	CPA
文献[4]-2	q-ABDHE(素数阶群-非静态)	STM	Adaptive-ID	是	CPA
文献[4]-3	QR(素数阶群-静态)	ROM	Adaptive-ID	是	CPA
文献[4]-4	LWE (素数阶群-静态)	ROM	Adaptive-ID	是	CPA
文献[7]	DBDH(素数阶群-静态)	STM	Selective-ID	否	CPA
文献[8]	假设 1,3(合数阶群-静态)	STM	Adaptive-ID	否	CPA
文献[9]	假设 1,2,3,4(合数阶群-静态)	STM	Adaptive-ID	否	CPA
文献[10]	假设 1,2,3,4(合数阶群-静态)	STM	Adaptive-ID	否	CPA
文献[11]	假设 1,2,3,4(合数阶群-静态)	STM	Adaptive-ID	是	CPA
文献[12]	BDH(素数阶群-静态)	ROM	Adaptive-ID& Adaptive-chosen-ciphertext	否	CCA
文献[13]	q-ABDHE(素数阶群-非静态)	STM	Adaptive-ID& Adaptive-chosen-ciphertext	否	CCA
LR-ANO-IBE	假设 1,2,3,4(合数阶群-静态)	STM	Adaptive-ID	是	CPA
LR-ANO-IBE′	假设 1,2,3,4(合数阶群-静态)	STM	Adaptive-ID& Adaptive-chosen-ciphertext	是	CCA

表 3　本文方案与现有合数阶群上的匿名 IBE 方案的效率比较

方案	公钥长度	用户私钥长度	密文长度	加密效率	解密效率
文献[8]	$2\|G\|+\|G_T\|$	$\|G\|$	$2\|G\|+\|G_T\|$	$1p+3e$	$1p$
文献[9]	$5\|G\|+\|G_T\|$	$2\|G\|$	$2\|G\|+\|G_T\|$	$1p+4e$	$2p$
文献[10]	$3\|G\|+\|G_T\|$	$2\|G\|$	$2\|G\|+\|G_T\|$	$1p+4e$	$2p$
文献[11]	$(5+n)\|G\|+\|G_T\|$	$(n+2)\|G\|$	$(n+2)\|G\|+\|G_T\|$	$1p+(n+2)e$	$(n+2)p$
本文	$3\|G\|+2\|G_T\|$	$2\|G\|+\|Z_N\|$	$2\|G\|+\|G_T\|$	$1p+4e$	$2p+1e$

4.4　效率分析

本文方案是在合数阶双线性群上构造的,因此在效率分析时我们仅与合数阶群上的方案[8~11]进行比较,通过比较发现,本文方案在提高安全性能的同时仍能保证较高的实现效率,具体如表 3 所示. 其中 p 表示双线性映射运算,e 表示指数运算,$|G|$ 表示群 G 中元素的长度,$|G_T|$ 表示群 G_T 中元素的长度,$|Z_N|$ 表示 Z_N 中元素的长度.

5　结论

本文基于对偶系统在标准模型下基于合数阶双线性群上的静态假设构造了一个匿名 IB-HPS,并对其所满足的安全性质进行了严格的证明. 但基于我们所构造的匿名 IB-HPS 得到的抗泄露匿名 IBE 方案没有考虑到系统主密钥的泄露情况. 在已有抗泄露 IBE 方案中,文献[14]虽然实现了抗主密钥的 IBE,但没有采用 IB-HPS 技术,且其庞大的公开参数导致方案实现效率非常低. 因此如何基于 IB-HPS 构造高效的抗主密钥泄露的匿名 IBE 方案是我们今后研究工作中一个亟待解决的问题.

参考文献

[1] Cramer R, Shoup V. Universal Hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption [A]. Proceedings of the 2002 International Conference on the Theory and Applications of Cryptographic Techniques [C]. Berlin: Springer, 2002. 45 – 64.

[2] Alwen J, Dodis Y, Naor M, Segev G, Walfish S, Wichs D. Public-key encryption in the bounded-retrieval model[A]. Proceedings of the 2010 International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin: Springer, 2010. 113 – 134.

[3] Chow S, Dodis Y, Rouselakis Y, Waters B. Practical leakage-resilient identity-based encryption from simple assumptions[A]. Proceedings of the 17th ACM Conference on Computer and Communications Security[C]. USA: ACM, 2010. 152 – 161.

[4] Chen Y, Zhang Z, Lin D, Cao Z. Anonymous identity-based Hash proof system and its applications[A]. Proceedings of the 6th International Conference on Provable Security[C]. Berlin: Springer, 2012. 143 – 160.

[5] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions[A]. Proceedings of the 2009 International Conference on the Theory and Applications of Cryptographic Techniques [C]. Berlin: Springer, 2009. 619 – 636.

[6] Baek J, Wong D S, Li J, Au H M. Efficient generic construction of CCA-secure identity-based encryption from randomness extraction[J]. The Computer Journal, 2016, 59(4): 508 – 521.

[7] Boyen X, Waters B. Anonymous hierarchical identity-based encryption(without random oracles)[A]. Proceedings of the 26th Annual International Cryptology Conference[C]. Berlin: Springer, 2006. 290 – 307.

[8] Wee H. Déjà Q: Encore! Un Petit IBE[A]. Proceedings of the 13th Theory of Cryptography Conference[C]. Berlin: Springer, 2016. 237 – 258.

[9] 王皓,徐秋亮. 抗适应性选择身份攻击的匿名 HIBE 方案[J]. 计算机学报, 2011, 34(1): 25 – 37.
Wang H, Xu Q. Anonymous HIBE scheme secure against full adaptive-ID attacks[J]. Chinese Journal of Computers, 2011, 34(1): 25 – 37. (in Chinese)

[10] De Caro A, Iovino V, Persiano G. Fully secure anonymous HIBE and secret-key anonymous IBE with short ciphertexts[A]. Proceedings of the 4th Pairing Based Cryptography[C]. Berlin: Springer, 2010. 347 – 366.

[11] Hu C, Yang R, Liu P, Yu Z, Zhou Y, Xu Q. Public-key encryption with keyword search secure against continual memory attacks [J]. Security and Communication Networks, 2016, 9: 1613 – 1629.

[12] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[A]. Proceedings of the 2001 International Cryptology Conference [C]. Berlin: Springer, 2001. 213 – 229.

[13] Gentry C. Practical identity-based encryption without ran-

dom oracles[A]. Proceedings of the 2006 International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin: Springer, 2006. 445 -464.

[14] Lewko A, Rouselakis Y, Waters B. Achieving leakage resilience through dual system encryption[A]. Proceedings of the 8th Theory of Cryptography Conference[C]. Berlin: Springer, 2011. 70 -88.

作者简介

侯红霞 女,1980 年生于山西朔州,陕西师范大学计算机科学学院博士研究生,研究方向为密码学、信息安全.
E-mail: hongxiahou@ snnu. edu. cn

杨 波(通信作者) 男,1963 年生于陕西富平,教授、博士生导师,陕西省"百人计划"特聘教授,研究方向为密码学、信息安全.
E-mail: byang@ snnu. edu. cn