一种基于组合阶双线性对群的HIBE方案

邹秀斌[1,2] 崔永泉[1] 付 才[1]
(华中科技大学计算机科学与技术学院信息安全实验室 武汉 430074)[1]
(江汉大学数计学院 武汉 430056)[2]

摘 要 目前,大多数HIBE方案都是基于素数阶双线性群的,其密钥和密文中的参数都是在素数阶双线性群上的取值。构造了一种基于组合阶双线性群的HIBE方案。密钥元组中各个参数从一素数阶群中取值,而密文元组的各个参数等于两个不同素数阶群的元素之积,其中一素数阶群的元素充当盲化因子。盲化后的密文能够增强新HIBE方案的安全性。在实际解密过程中,密文中的盲化因子对解密并没有任何影响。新的HIBE方案在标准模型下实现了选择身份攻击安全。

关键词 HIBE,IBE,组合阶双线性群,CCA
中图法分类号 TP309.7 **文献标识码** A

HIBE Scheme Based on Composite Order Bilinear Groups

ZOU Xiu-bin[1,2] CUI Yong-quan[1] FU Cai[1]
(Laboratory of Information Security, College of Computer, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(College of Computer and Mathematics, Jianghan University, Wuhan 430056, China)[2]

Abstract Presently, most of the HIBE schemes are based on the prime order bilinear groups. The author constructed a HIBE scheme based on composite order bilinear groups. The component parameters of secret key tuple are those elements in an group of prime order while the ones of ciphertext tuple are the products of some elements in two groups, which are of different prime order, and elements in one of these groups, which act as blind factors. The blinded ciphertext enhances the security of the new HIBE scheme. The blind factors of the ciphertext have no effects on the decryption. The new HIBE scheme is selective-ID secure in the standard model.

Keywords HIBE, IBE, Composite order bilinear groups, CCA

1 引言

1985年,Shamir[1]提出了基于身份加密(Identity Based Encryption,简称IBE)系统。IBE系统是公钥为任何串(身份、地址、e-mail地址)的公钥密码系统。在此系统中,存在一可信中心,它拥有主密钥,利用该主密钥,它可以为指定身份信息产生私钥信息,并将私钥信息分发给相应身份的用户。

后来,提出的层次化IBE(Hierarchical Identity Based Encryption,简称HIBE)系统[2-4]反映了组织的层次关系。在HIBE系统中,身份等级为k的用户能够托管身份等级比他低的子孙密钥。

在文献[4]中,Boneh等人提出了一种常量大小密文的HIBE方案,该方案的密文由3个元素构成,加密跟其它的HIBE系统一样有效,而解密仅仅需要两次双线性映射计算,也不需要考虑用户身份等级深度。该方案在标准模型下实现了选择身份安全,而在随机预言机模型下是完全安全的。然而,文献[4]中的方案是建立在素数阶双线群基础上的。

2005年,Boneh首次提出组合阶双线群[5],从而组合阶双线映射对可以应用于公钥密码系统中,如文献[6,7]等。2011年,王皓等人[8]提出了抗适应性选择身份攻击的匿名HIBE方案,该方案构造了一个匿名基于身份加密(IBE)方案,并将其扩展为一个匿名分等级的基于身份加密(HIBE)方案。在该方案的构造中使用了合数阶双线性群,利用相同子群中的元素来对公共参数和密文进行盲化,从而实现方案的匿名性;利用不同子群中的元素构造用户私钥,从而达到正确解密的目的。其安全性证明使用了Lewko和Waters提出的构造双系统加密的新技术。

在文献[4,8]的基础上,结合组合阶双线群知识,构造了一种基于组合阶双线性群的HIBE方案,使用了组合阶双线性群。设G是阶为$n(n=pq)$的双线性群,密钥元组中各个分量等于G_p中的元素,而密文元组的各个分量等于G_p中的元素和盲化因子(G_q中的元素)之积。盲化因子仅仅是对密文进行了盲化作用,从而提高了系统的安全性,而在实际解密过程中,密文的各个分量中的盲化因子不会对其产生任何影响。

到稿日期:2011-08-15 返修日期:2011-11-03 本文受国家自然科学基金(60903175,60703048),湖北省自然科学基金(2009CBD307,2008CDB352)资助。

邹秀斌(1974—),男,博士生,讲师,主要研究方向为公钥密码体制及其安全分析,E-mail:xbz1234@163.com;崔永泉(1976—),男,博士,讲师,主要研究方向为计算机病毒;付 才(1976—),男,博士,讲师,主要研究方向为无线网络安全、路由协议安全与软件脆弱性。

新的 HIBE 方案在标准模型下实现了选择身份攻击安全。

2 预备知识

2.1 组合阶双线群

定义 1 令 Γ 是一个算法，该算法以安全参数 $\lambda(\lambda\in\mathbb{Z}$，且$\lambda>0)$作为输入，并输出元组$(p,q,G,G',e)$，此处 p,q 是两个不同的大素数，G 和G'是阶为 $n(n=pq)$的循环群，e 是双线性映射，即 $e:G\times G\to G'$，且它满足下面性质：

(1)双线性

$\forall u,v\in G,\forall a,b\in\mathbb{Z},e(u^a,v^b)=e(u,v)^{ab}$

(2)非退化性

若 g 是G的生成元，且满足 $e(g,g)$是G'的生成元，令 G_p,G_q分别表示循环群G 的 p,q 阶子群。如果 $u\in G_p,v\in G_q$，则 $e(u,v)$是G'的单位元。令 g 是G的生成元，由于 g^q，g^p 分别是G_p,G_q的生成元，因此存在 $a,b\in\mathbb{Z}$ 满足 $u=(g^q)^a$，$v=(g^p)^b$，于是有 $e(u,v)=e((g^q)^a,(g^p)^b)=e(g,g)^{abpq}=e(g,g)$。

2.2 ℓ-*wBDHI** 假设(weak Bilinear Diffie-Hellman Inversion Assumption)

令 g 和 h 是G_p的生成元，H 是G_q的生成元。设 $\alpha\in\mathbb{Z}_p^*$，存在任意 $f\in\mathbb{Z}$，我们定义 ℓ-*wBDHI** 问题如下：

给定 $g,h,H,g^{\alpha},g^{(\alpha^2)},\cdots,g^{(\alpha^\ell)}$，计算 $e(g,hH^f)^{(\alpha^{\ell+1})}$ 或 $e(g,h)^{(\alpha^{\ell+1})}$。

注意：计算 $e(g,hH^f)^{(\alpha^{\ell+1})}$ 和 $e(g,h)^{(\alpha^{\ell+1})}$ 是等价的。

令 $y_i=g^{(\alpha^i)}\in G_p^*$，$\vec{y}_{g,\alpha,\ell}=(y_1,y_2,\cdots,y_\ell)$，则 ℓ-*wBDHI** 问题可以简记为：如果 $\Pr[A(g,h,H,\vec{y}_{g,\alpha,\ell})=e(g,hH^f)^{(\alpha^{\ell+1})}]\geqslant\varepsilon$，算法 A 解决 ℓ-*wBDHI** 问题有优势 ε。

定义 2 如果 t 时间内算法 A 解决 ℓ-*wBDHI** 问题有优势 ε，则 ℓ-*wBDHI** 假设成立。

2.3 HIBE 安全(IND-ID-CCA 和 IND-sID-CCA)

设 $\mathcal{E}$ 是 HIBE 方案，其安全(IND-ID-CCA)可以通过敌手 A 和挑战者 C 之间进行的游戏来定义。该游戏由设置参数、密钥查询阶段 1、挑战密文阶段、密钥查询阶段 2、猜测阶段等 5 个阶段构成。

设置参数：挑战者 C 运行设置参数算法，产生系统参数和主密钥，则挑战者 C 把系统参数发送给敌手 A，而自己保留主密钥。

密钥查询阶段 1：敌手 A 适应性发起查询 $q_1,q_2,\cdots,q_m$，此处的 $q_i(i=1,\cdots,m)$是下面两种查询之一。

给定身份 ID_i 信息，挑战者 C 运行密钥产生算法产生私钥 d_i(对应于公钥 ID_i)，并将 d_i 发送给敌手 A。

给定身份 ID_i 和密文 C_i，挑战者 C 首先运行密钥产生算法产生私钥 d_i(对应于公钥 ID_i)，然后借助私钥 d_i，运行解密算法，从而得到明文，并将明文发送给敌手 A。

挑战密文阶段：一旦敌手 A 决定密钥查询阶段 1 结束，他就输出身份 ID^* 和两个等长的明文 M_0,M_1，其中这两个明文是他希望挑战的；唯一的限制是以前未发起针对 ID^* 以及 ID^* 前缀的密钥查询。挑战者 C 随机选择 $b\in\{0,1\}$，设挑战密文等于 $Encrypt(ID^*,M_b)$，并把该挑战密文发送给敌手 A。

密钥查询阶段 2：类似于密钥查询阶段 1，但要求 ID_i 不等于 ID^* 或者 ID^* 的前缀。

猜测阶段：最后，敌手 A 输出猜测 b'，并且如果 $b'=b$，则敌手即游戏获胜。

我们认为上面的敌手 A 是 IND-ID-CCA 敌手。敌手 A 攻击下 $\mathcal{E}$ 优势定义为：$Adv_{\mathcal{E},A}=|\Pr[b=b']-\frac{1}{2}|$。

在弱的安全概念情况下，敌手 A 在攻击之前，事先确定要攻击的公钥(即身份)。我们把这种概念称为选择身份，并选择了密文安全的 HIBE(IND-sID-CCA)。

定义 3 如果任意 t 时间 IND-ID-CCA (相应地 IND-sID-CCA) 敌手 A 至多 q_{ID} 次选择私钥查询并且至多 q_C 次选择密钥查询时有 $Adv_{\mathcal{E},A}<\vartheta$，我们称 HIBE 方案 $\mathcal{E}$ 是(t,q_{ID},q_C,ϑ)安全的。速记之，我们说 ε 是(t,q_{ID},q_C,ϑ)-IND-ID-CCA(相应地，(t,q_{ID},q_C,ϑ)-IND-sID-CCA)安全。

3 新的 HIBE 方案

3.1 新的 HIBE 方案

基于组合阶双线性群的 HIBE 方案由 5 个算法构成：设置系统参数算法 Setup、密钥产生算法 KeyGen(ID_k)、密钥托管算法 Delegate($SK_{ID_{k-1}},ID_k$)、加密算法 Encrypt(ID_k,M)、解密算法 Decrypt(C,SK_{ID_k})。

Setup 算法　输入系统参数 λ，密钥管理中心初始化过程如下：

运行 $\Gamma(\lambda)$，得到元组(p,q,G,G',e)，此处 p,q 是两个不同的大素数，G 和G'是阶为 $n(n=pq)$的循环群。规定合法用户的身份 ID 向量的分量最大个数为 ℓ，即 $ID\in\mathbb{Z}_n^{\ell}$。

随机选择 $g_1,v\in G_p$，随机选择 $a_1,a_2,\cdots,a_\ell\in G_p,b_1,b_2,\cdots,b_\ell\in G_p,d_1,d_2,\cdots,d_\ell\in G_p,R_1,R_2,\cdots,R_\ell\in G_q,S_1,S_2,\cdots,S_\ell\in G_q,T_1,T_2,\cdots,T_\ell\in G_q,R_v\in G_q,V=vR_v$。

$$PubM_1=\begin{pmatrix}a_1&b_1&d_1\\ \vdots&\vdots&\vdots\\ a_\ell&b_\ell&d_\ell\end{pmatrix}$$

$$BlindM=\begin{pmatrix}R_1&S_1&T_1\\ \vdots&\vdots&\vdots\\ R_\ell&S_\ell&T_\ell\end{pmatrix}$$

$$PubM_2=\begin{pmatrix}A_1=a_1R_1&B_1=b_1S_1&D_1=d_1T_1\\ \vdots&\vdots&\vdots\\ A_\ell=a_\ell R_\ell&B_\ell=b_\ell S_\ell&D_\ell=d_\ell T_\ell\end{pmatrix}$$

密钥管理者随机选择 $\alpha\in\mathbb{Z}_p$，把 α 作为自己的私钥 SK。其公钥 PK 为 g_1^{α}。令 $\overline{A}=e(g_1,v)^{\alpha}$，对外公开 PK 以及参数$(p,q,n,G,G',e,\overline{A},V,PubM_1,PubM_2)$。

KeyGen(ID_k)算法　给定用户身份 $ID_k(I_1,\cdots,I_k)$，其中 $I_i\in\mathbb{Z}_p,i=1,\cdots,k$。令身份为 ID_k 的用户的私钥为 SK_{ID_k}，随机选择 $\rho_{k,1},\rho_{k,2}\in\mathbb{Z}_p$，令 $\Lambda=\{1,\cdots,k\}$，则有：

$$SK_{ID_k}=(K_0=g_1^{\alpha}\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}),K_{k,1}=v^{\rho_{k,1}},K_{k,2}=v^{\rho_{k,2}},E_{k+1}=a_{k+1}^{\rho_{k,1}},\cdots,E_\ell=a_\ell^{\rho_{k,1}},F_{k+1}=b_{k+1}^{\rho_{k,1}},\cdots,F_\ell=b_\ell^{\rho_{k,1}},H_{k+1}=d_{k+1}^{\rho_{k,2}},\cdots,H_\ell=d_\ell^{\rho_{k,2}})$$

Delegate($SK_{ID_{k-1}},ID_k$)算法　输入用户身份为 $ID_{k-1}=(I_1,\cdots,I_{k-1})$的密钥 $SK_{ID_{k-1}}=(K_0',K_{k-1,1}',K_{k-1,2}',E_k',\cdots,E_\ell',F_k',\cdots,F_\ell',H_k',\cdots,H_\ell')$，以及 $ID_k=(I_1,\cdots,I_k)$，密钥委托算法为身份是 ID_k 的用户产生密钥 SK_{ID_k} 的过程如下：

随机选择 $\eta_{k,1},\eta_{k,2}\in\mathbb{Z}_p$，令 $\Lambda=\{1,\cdots,k\}$。

$$K_0=K_0'\cdot(E_k')^{I_k}\cdot F_k'\cdot H_k'\cdot\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\eta_{k,1}}d_i^{\eta_{k,2}})$$

$$K_{k,1}=K_{k-1,1}'\cdot v^{\eta_{k,1}}$$

$K_{k,2}=K'_{k-1,2}\cdot v^{\eta_k,2}$

$E_{k+1}=E'_{k+1}a_{k+1}^{\eta_{k+1}},\cdots,E_\ell=E_\ell' a_\ell^{\eta_\ell}$

$F_{k+1}=F'_{k+1}a_{k+1}^{\eta_{k+1}},\cdots,F_\ell=F_\ell' a_\ell^{\eta_\ell}$

$H_{k+1}=H'_{k+1}a_{k+1}^{\eta_{k+1}+2},\cdots,H_\ell=H_\ell' a_\ell^{\eta_k+2}$

于是得到 $SK_{ID_k}=(K_0,K_{k,1},K_{k,2},E_{k+1},\cdots,E_\ell,F_{k+1},\cdots,F_\ell,H_{k+1},\cdots,H_\ell)$

Encrypt(ID_k,M)算法　给定用户身份 $ID_k=(I_1,I_2,\cdots,I_k)$和明文 $M\in G'$,其加密过程如下:

随机选择 $s\in Z_n$和 $Y_{1,1},Y_{1,2},Y_{2,1},Y_{2,2},\cdots,Y_{k,1},Y_{k,2},Y\in G_q$,输出密文 C 为:

$$C=\begin{pmatrix} C'=M\cdot\overline{A}^s, C_0=V^s, \\ \begin{pmatrix} C_{1,1}=(A_1^{I_1}B_1)^sY_{1,1} & , & C_{1,2}=D_1^sY_{1,2} \\ & \vdots & \\ C_{k,1}=(A_k^{I_k}B_k)^sY_{k,1} & & C_{k,2}=D_k^sY_{k,2} \end{pmatrix} \end{pmatrix}$$

Decrypt(C,SK_{ID_k})算法　给定密文 $C=\left(C',C_0,\begin{pmatrix} C_{1,1} & , & C_{1,2} \\ & \vdots & \\ C_{k,1} & & C_{k,2}\end{pmatrix}\right)$,设 $\Lambda=\{1,\cdots,k\}$,令私钥为:

$SK_{ID_k}=(K_0=g_1^q\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}})$

$K_{k,1}=v^{\rho_{k,1}},K_{k,2}=v^{\rho_{k,2}}$

$E_{k+1}=a_{k+1}^{\rho_{k,1}},\cdots,E_\ell=a_\ell^{\rho_{k,1}}$

$F_{k+1}=b_{k+1}^{\rho_{k,1}},\cdots,F_\ell=b_\ell^{\rho_{k,1}}$,

$H_{k+1}=d_{k+1}^{\rho_{k,2}},\cdots,H_\ell=d_\ell^{\rho_{k,2}})$

解密过程如下:

$M=C'/(e(C_0,K_0)/\prod_{i\in\Lambda}(e(C_{i,1},K_{k,1})e(C_{i,2},K_{k,2})))$。

3.2 Decrypt(C,SK_{ID_k})算法的验证过程

由于

$e(C_{i,1},K_{k,1})e(C_{i,2},K_{k,2})$

$=e((A_i^{I_i}B_i)^sY_{i,1},v^{\rho_{k,1}})e(D_i^sY_{i,2},v^{\rho_{k,2}})$

$=e((A_i^{I_i}B_i)^s,v^{\rho_{k,1}})e(Y_{i,1},v^{\rho_{k,1}})e(D_i^s,v^{\rho_{k,2}})e(Y_{i,2},v^{\rho_{k,2}})$

$=e((A_i^{I_i}B_i)^{\rho_{k,1}},v^s)e(D_i^{\rho_{k,2}},v^s)$

$=e((A_i^{I_i}B_i)^{\rho_{k,1}}D_i^{\rho_{k,2}},v^s)$

$=e((a_iR_i)^{I_i}(b_iS_i))^{\rho_{k,1}}(d_iT_i)^{\rho_{k,2}},v^s)$

$=e(v^s,(a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}})e(v^s,(R_i^{I_i}S_i)^{\rho_{k,1}}T_i^{\rho_{k,2}})$

$=e(v^s,(a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}})e(v,R_i)^{sI_i\rho_{k,1}}e(v,S_i)^{s\rho_{k,1}}e(v,T_i)^{s\rho_{k,2}}$

$=e(v^s,(a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}})$

因此

$\prod_{i\in\Lambda}(e(C_{i,1},K_{k,1})e(C_{i,2},K_{k,2}))$

$=e(v^s,\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))$

又由于

$e(C_0,K_0)$

$=e(V^s,g_1^q\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))$

$=e(V^s,g_1^q)e(V^s,\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))$

$=e(V,g_1)^{\alpha s}e(V^s,\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))$

$=e(vR_v,g_1)^{\alpha s}e((vR_v)^s,\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))$

$=e(v,g_1)^{\alpha s}\cdot e(R_v,g_1)^{\alpha s}\cdot e((v^s,\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))\cdot e(R_v^s,\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))$

$=e(v,g_1)^{\alpha s}e(v^s,\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}))$

$=e(v,g_1)^{\alpha s}\prod_{i\in\Lambda}(e(C_{i,1},K_{k,1})e(C_{i,2},K_{k,2}))$

$=\overline{A}^s\prod_{i\in\Lambda}(e(C_{i,1},K_{k,1})e(C_{i,2},K_{k,2}))$

因此

$C'/(e(C_0,K_0)/\prod_{i\in\Lambda}(e(C_{i,1},K_{k,1})e(C_{i,2},K_{k,2})))$

$=M\overline{A}^s/(\overline{A}^s)=M$

4　安全证明

证明:假定算法 A 攻击 3.1 节的新方案优势 ε。建立算法 B 来解决判定 ℓ-$wBDHI^*$ 假设。

给算法 B 输入判定 ℓ-$wBDHI^*$ 假设的实例元组$(g,h,H,\vec{y}_{g,\alpha,\ell},T)$。该元组中的 T 或等于 $e(g,hH^f)^{(\alpha^{\ell+1})}$,或者 T 在群 G'^* 内随机取值。算法 B 的目标是:当输入元组$(g,h,H,\vec{y}_{g,\alpha,\ell},T)$的 T 等于 $e(g,hH^f)^{(\alpha^{\ell+1})}$时,算法 B 就输出 1,否则就输出 0。算法 B 通过在选择身份游戏中与敌手 A 交互,其中,描述算法 B 与算法 A 交互的过程包括:初始化、设置系统参数、密钥查询阶段 1、挑战密文阶段、密钥查询阶段,以及猜测等 6 个阶段。

1)初始化

敌手开始输出他打算攻击的身份 $ID^*=(I_1^*,\cdots,I_m^*)$,且 $ID^*\in(Z_P^*)^m$,该身份深度为 $m(m<\ell)$。

2)设置系统参数

算法 B 利用自己的数据$(g,h,H,\vec{y}_{g,\alpha,\ell},T)$,并选择一些随机数,为敌手 A 产生一些系统参数。算法 B 随机选择 $\gamma,g_1=y_\ell\cdot g^\gamma=g^{\gamma+(\alpha^\ell)}$,$v=g$;算法 B 随机选择 $\gamma_1,\cdots,\gamma_\ell,\lambda_1,\cdots,\lambda_\ell\in Z_p,\xi_1,\xi_2,\cdots,\xi_\ell\in Z_p$,对于 $i=1,\cdots,\ell$,设 $a_i=g^{\gamma_i}/y_{\ell-i+1}$,$b_i=g^{\lambda_i}y_{\ell-i+1}^{I_i^*}$,$d_i=g^{\xi_i}$。随机选择 $r_1,r_2,\cdots,r_\ell\in Z_q,s_1,s_2,\cdots,s_\ell\in Z_q,t_1,t_2,\cdots,t_\ell\in Z_q$,则对于 $i=1,\cdots,\ell$,有 $R_i=H^{r_i}$,$S_i=H^{s_i}$,$T_i=H^{t_i}$,$A_i=a_iR_i=g^{\gamma_i}/y_{\ell-i+1}H^{r_i}$,$B_i=g^{\lambda_i}y_{\ell-i+1}^{I_i^*}H^{s_i}$,$D_i=d_iT_i=g^{\xi_i}H^{t_i}$。随机选择 $r_v\in G_q$,$R_v=H^{r_v}$,$V=vR_v=gH^{r_v}$。于是得到:

$$PubM_1=\begin{pmatrix} a_1 & b_1 & d_1 \\ \vdots & \vdots & \vdots \\ a_\ell & b_\ell & d_\ell \end{pmatrix},BlindM=\begin{pmatrix} R_1 & S_1 & T_1 \\ \vdots & \vdots & \vdots \\ R_\ell & S_\ell & T_\ell \end{pmatrix}$$

$$PubM_2=\begin{pmatrix} A_1 & B_1 & D_1 \\ \vdots & \vdots & \vdots \\ A_\ell & B_\ell & D_\ell \end{pmatrix}$$

$\overline{A}=e(g_1,v)^\alpha$

算法 B 将公共参数$(p,q,n,G,G',e,\overline{A},V,PubM_1,PubM_2)$发送给算法 A。

3)查询密钥阶段 1

算法 A 发起 q_s 私钥查询。考虑一次对于身份 $ID=(I_1,\cdots,I_u)\in(Z_p^*)^u$(此处 $u<\ell$)的查询密钥。唯一限制的是 ID,而不是 ID^* 或者不是 ID^* 的前缀,即确保存在 $k\in\{1,\cdots,u\}$ 满足 $I_k\neq I_k^*$(否则,ID 即是 ID^* 的前缀)。设 $ID=(I_1,\cdots,I_k,\cdots,I_u)$,算法 B 首先得到身份为$(I_1,\cdots,I_k)$的密钥,然后利用该密钥,构造身份为$(I_1,\cdots,I_k,\cdots,I_u)$的密钥。

为了产生身份为$(I_1,\cdots,I_k)$的密钥,算法 B 随机选择 $\omega_{k,1},\rho_{k,2}\in Z_p$,令 $\rho_{k,1}=\frac{\alpha^k}{(I_k-I_k^*)}+\omega_{k,1}$,得到:

$SK_{ID_k}=(K_0=g_1^q\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}}),K_{k,1}=v^{\rho_{k,1}},K_{k,2}=$

$v^{\rho_{k,2}}, E_{k+1}=a_{k+1}^{\rho_{k,1}}, \cdots, E_\ell=a_\ell^{\rho_{k,1}}, F_{k+1}=b_{k+1}^{\rho_{k,1}}, \cdots,$

$F_\ell=b_\ell^{\rho_{k,1}}, H_{k+1}=d_{k+1}^{\rho_{k,2}}, \cdots, H_\ell=d_\ell^{\rho_{k,2}})$

对于 SK_{ID_k} 的第一部分 K_0，

$$K_0=g_1^{\alpha}\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}})$$

$$=g^{\gamma+(\alpha^\ell)}\cdot(\prod_{i\in\Lambda}(a_i^{I_i})^{\rho_{k,1}})\cdot(\prod_{i\in\Lambda}(b_i)^{\rho_{k,1}})\cdot(\prod_{i\in\Lambda}(d_i)^{\rho_{k,2}})$$

对于上式 K_0，发现：

$$(\prod_{i\in\Lambda}(a_i^{I_i})^{\rho_{k,1}})=\prod_{i=1}^{k}(g^{\gamma_i}/y_{\ell-i+1})^{I_i\rho_{k,1}}$$

$$=(g_{i=1}^{\sum_{i=1}^{k}I_i\gamma_i}/\prod_{i=1}^{k}(y_{\ell-i+1}^{I_i}))^{\rho_{k,1}}(\prod_{i\in\Lambda}(b_i)^{\rho_{k,1}})$$

$$=\prod_{i=1}^{k}(g^{\lambda_i}y_{\ell-i+1}^{I_i^*})^{\rho_{k,1}}$$

$$=(g_{i=1}^{\sum_{i=1}^{k}\lambda_i}(\prod_{i=1}^{k}y_{\ell-i+1}^{I_i^*}))^{\rho_{k,1}}(\prod_{i\in\Lambda}(d_i)^{\rho_{k,2}})$$

$$=\prod_{i=1}^{k}(g^{\xi_i})^{\rho_{k,2}}=(g_{i=1}^{\sum_{i=1}^{k}\xi_i})^{\rho_{k,2}}$$

于是有：

$$K_0=g_1^{\alpha}\prod_{i\in\Lambda}((a_i^{I_i}b_i)^{\rho_{k,1}}d_i^{\rho_{k,2}})$$

$$=(g^{\gamma+(\alpha^\ell)})^{\alpha}\cdot(g_{i=1}^{\sum_{i=1}^{k}\xi_i})^{\rho_{k,2}}\cdot(g_{i=1}^{\sum_{i=1}^{k}(I_i\gamma_i+\lambda_i)}/\prod_{i=1}^{k}(y_{\ell-i+1}^{I_i})$$

$$g_{i=1}^{\sum_{i=1}^{k}\lambda_i}(\prod_{i=1}^{k}y_{\ell-i+1}^{I_i^*}))^{\rho_{k,1}}$$

$$=y_{\ell+1}y_1^{\gamma}\cdot(g_{i=1}^{\sum_{i=1}^{k}I_i\gamma_i+\lambda_i}\cdot\prod_{i=1}^{k-1}(y_{\ell-i+1}^{I_i^*-I_i})\cdot y_{\ell-k+1}^{I_k^*-I_k})^{\rho_{k,1}}\cdot$$

$$(g_{i=1}^{\sum_{i=1}^{k}\xi_i})^{\rho_{k,2}}$$

又注意到 $\prod_{i=1}^{k-1}(y_{\ell-i+1}^{I_i^*-I_i})=1$，而

$$y_{\ell-k+1}^{\rho_{k,1}(I_k^*-I_k)}=y_{\ell-k+1}^{\omega_{k,1}(I_k^*-I_k)}\cdot y_{\ell-k+1}^{-\alpha^k}$$

$$=y_{\ell-k+1}^{\omega_{k,1}(I_k^*-I_k)}/(y_{\ell-k+1}^{\alpha^k})=y_{\ell-k+1}^{\omega_{k,1}(I_k^*-I_k)}/y_{\ell+1}$$

所以有：

$$K_0=y_{\ell+1}y_1^{\gamma}\cdot(y_{\ell-k+1}^{I_k^*-I_k})^{\rho_{k,1}}\cdot(g_{i=1}^{\sum_{i=1}^{k}(I_i\gamma_i+\lambda_i)})^{\rho_{k,1}}\cdot g_{i=1}^{\sum_{i=1}^{k}\xi_i\rho_{k,2}}$$

$$=y_1^{\gamma}\cdot y_{\ell-k+1}^{\omega_{k,1}(I_k^*-I_k)}\cdot(g_{i=1}^{\sum_{i=1}^{k}(I_i\gamma_i+\lambda_i)\rho_{k,1}})\cdot g_{i=1}^{\sum_{i=1}^{k}(\xi_i\rho_{k,2})}$$

$$=y_1^{\gamma}\cdot y_{\ell-k+1}^{\omega_{k,1}(I_k^*-I_k)}\cdot g_{i=1}^{\sum_{i=1}^{k}(\xi_i\rho_{k,2}+(I_i\gamma_i+\lambda_i)\rho_{k,1})}$$

4)挑战密文阶段

算法 B 为敌手提供的明文产生随机密文，算法 A 向算法 B 发送消息 $M_0, M_1\in G_p'$ 以及挑战身份 $ID_k^*=(I_1^*, I_2^*, \cdots, I_k^*)$，算法 B 抛币决定 β 值。我们逐步描述创建挑战密文的过程。算法 B 调用 $Encrypt(ID^*, M_\beta)$。

对于 $i=1,\cdots,k$，有：

$$C_{i,1}=(hH^f)^{I_i^*\gamma_i+\lambda_i}H^{f_{i,1}}=h^{I_i^*\gamma_i+\lambda_i}H^{(I_i^*\gamma_i+\lambda_i)f}$$

$$=(g^{I_i^*\gamma_i+\lambda_i})^{c}H^{(I_i^*\gamma_i+\lambda_i)f}H^{f_{i,1}}$$

$$(g^{I_i^*\gamma_i+\lambda_i})^{c}=((g^{\gamma_i}/y_{\ell-i+1})^{I_i^*}g^{\lambda_i}y_{\ell-i+1}^{I_i^*})^{c}=(a_i^{I_i^*}b_i)^{c}$$

令 $f_{i,1}=c\cdot c_1$，当然，c, c_1 都不为算法 B 所知。$H^{(I_i^*\gamma_i+\lambda_i)f_{i,1}}=((H^{\gamma_i c_1})^{I_i^*}H^{\lambda_i c_1})^{c}$，所以：

$$(hH^f)^{I_i^*\gamma_i+\lambda_i}H^{f_{i,1}}=((a_iH^{\gamma_i c_1})^{I_i^*}b_iH^{\lambda_i c_1})^{c}H^{f_{i,1}}$$

$$C_{i,2}=(hH^f)^{\xi_i}=(g^{\xi_i}H^{\xi_i c_1})^{c}=(d_iH^{\xi_i c_1})^{c}$$

$$e(g,h)^{(\alpha^{\ell+1})}\cdot e(y_1,h^{\gamma})$$

$$=(e(g,g)^{(\alpha^{\ell+1})}\cdot e(y_1,g^{\gamma}))^{c}$$

$$=(e(y_1,y_\ell)e(y_1,g^{\gamma}))^{c}$$

$$=(e(y_1,y_\ell g^{\gamma}))^{c}=e(g^{\alpha},g_1)^{c}=e(v,g_1)^{\alpha c}$$

对于 $i=1,\cdots,k$，令 $R_i=H^{\gamma_i c_1}, S_i=H^{\lambda_i c_1}, T_i=H^{\xi_i c_1}, A_i=a_iR_i, B_i=b_iS_i, D_i=d_iT_i, Y_{k,1}=H^{f_{k,1}}, Y_{k,2}=H^{f_{k,2}}$。如果 $T=e(g,hH^f)^{(\alpha^{\ell+1})}$，得到的挑战密文是针对身份为 $(I_1^*,\cdots,I_m^*)$、对 M_b 有效加密的密文，该密文如下所示：

$$C=\begin{pmatrix}C'=M_b\cdot e(v,g_1)^{\alpha c}, C_0=g^{c},\\ \begin{pmatrix}C_{1,1}=(A_1^{I_1}B_1)^{c}Y_{1,1} & C_{1,2}=D_1^{c}Y_{1,2}\\ \vdots & \\ C_{k,1}=(A_m^{I_m}B_m)^{c}Y_{k,1} & C_{m,2}=D_m^{c}Y_{m,2}\end{pmatrix}\end{pmatrix}$$

另一方面，当 T 均匀从 G_p 中取值，就算法 A 而言，密文 C 是独立于 b 的。

5)密钥查询阶段 2

敌手 A 发起若干查询(这些查询在密钥查询阶段 1 中没有被发起)，算法 B 跟以前一样地回应。

6)猜测阶段

最后，敌手 A 输出 $b'\in\{0,1\}$。算法 B 通过输出如下猜测，总结其游戏。如果 $b=b'$，则算法 B 输出 1(这意味着 $T=e(g,hH^f)^{(\alpha^{\ell+1})}$)，否则，算法 B 输出 0(意味着 T 随机取值于 G_p')。当输入元组的 $T=e(g,hH^f)^{(\alpha^{\ell+1})}$，敌手 A 所看到的结果跟在实际攻击游戏中看到的结果是一样的。因此，敌手 A 满足 $|\Pr[b=b']-1/2|\geqslant\varepsilon$。当输入元组的 T 随机取值 G_p'，则 $\Pr[b=b']=1/2$。有：

$$|\Pr[B(g,h,H,\vec{y}_{g,a,\ell},e(g,hH^f)^{(\alpha^{\ell+1})})=0]-B(g,h,\vec{y}_{g,a,\ell},T)=0]|\geqslant|(1/2\pm\varepsilon)-1/2|=\varepsilon$$

结束语 提出了一种基于组合阶双线性对的 HIBE 方案，该方案使用了组合阶双线性群，密钥元组中各个分量是 G_p 中的元素。而密文元组的各个分量等于 G_p 的元素和盲化因子(G_q 中的元素)之积。盲化因子仅仅是对密文进行盲化作用，在实际解密过程中，密文的各个分量中的盲化因子不会对其产生任何影响。新的 HIBE 方案在标准模型下实现了选择身份攻击安全。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology. Springer, 1985

[2] Gentry C, Silverberg A. Hierarchical ID-based cryptography[C]// Advances in Cryptology Asiacrypt 2002. 2002: 149-155

[3] Horwitz J, Lynn B. Toward hierarchical identity-based encryption[C]// EUROCRYPT'02 Proceedings of the International Conference on the Theory and Applications of Crytographic Techniques: advances in Cryptology. Springer, 2002

[4] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext[C]// Advances in Cryptology CEUROCRYPT 2005. 2005: 440-456

[5] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF formulas on ciphertexts[C]// Proceeding of Theory of Cryptography(CTCCy'05). 2005: 325-341

[6] Lewko A, Waters B. New techniques for dual system encryption and fully secure hibe with short ciphertexts[C]// Theory of Cryptography. 2010: 455-479

[7] Boyen X, Waters B. Compact group signatures without random oracles[C]// Advances in Cryptology-Eurocrypt. 2006: 427-444

[8] 王皓，徐秋. 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)：25-36