•信息工程•

DOI:10.15961/j.jsuese.201801281

支持门限解密的多身份全同态加密方案

杨晓元[1,2], 涂广升[1,2], 孔咏骏[1,2], 周潭平[1,2*]

(1.武警工程大学 密码工程学院, 陕西 西安 710086; 2.网络和信息安全武警部队重点实验室, 陕西 西安 710086)

摘　要:针对传统的身份基全同态加密方案只能对同一身份下的密文进行同态运算和访问控制的问题, 提出了一个基于LWE问题的多身份全同态加密方案。首先, 使用工具矩阵得到新的加解密形式, 约减噪音, 并改变身份基加密中底层格基的维度, 对身份基全同态加密方案进行优化。其次, 利用多密钥全同态转化机制, 构造身份基全同态加密方案的屏蔽系统, 生成辅助密文。最后, 将多密钥全同态加密中的多用户场景延伸到多身份场景, 构造多身份全同态加密方案, 实现对不同身份下密文的同态运算和访问控制。结果表明, 本方案实现了身份基加密与多密钥全同态加密的结合, 并证明为选择身份下的IND–CPA安全。与其他方案相比, 本方案加密单比特明文消息时密文规模更小, 对密文进行同态运算时噪音扩张率更低, 并且允许多个PKG参与密钥的生成、分发。同时, 给出本方案的门限解密过程, 据此可以构造一个2轮多方计算协议。

关键词:身份基加密; 全同态加密; 多身份; 门限解密

中图分类号:TP309.7　　**文献标志码**:A　　**文章编号**:2096-3246(2019)04-0133-07

Multi-identity Fully Homomorphic Encryption Scheme Supporting Threshold Decryption

YANG Xiaoyuan[1,2], *TU Guangsheng*[1,2], *KONG Yongjun*[1,2], *ZHOU Tanping*[1,2*]

(1.School of Cryptographic Eng., Eng. Univ. of PAP, Xi'an 710086, China; 2.Key Lab. of Network and Information Security of PAP, Xi'an 710086, China)

Abstract: In order to solve the problem that traditional identity-based fully homomorphic encryption schemes can only perform homomorphic operations and access control on ciphertexts under the same identity, a multi-identity fully homomorphic encryption scheme was proposed based on LWE problem. Firstly, the identity-based fully homomorphic encryption scheme was optimized by using a gadget matrix and a new form of encryption and decryption was obtained, which reduced noise, and changed the dimension of the underlying lattice basis in the identity-based encryption. Secondly, by using the multi-key fully homomorphic transformation mechanism, the masking system was constructed to generate auxiliary ciphertext. Finally, the multi-identity fully homomorphic encryption scheme was constructed to handle ciphertexts under different identities in which the multi-key scenario was extended to the multi-identity scenario. The results showed that the proposed scheme combined identity-based encryption with multi-key fully homomorphic encryption, and was proved to be IND–CPA security under the selected identity. Compared with other schemes, the ciphertext size and noise expansion were reduced when encrypting a single-bit message and evaluating ciphertexts, and more PKGs were allowed to participate in the generation and distribution of private key. Meanwhile, a 2-round multi-party computation protocol could be constructed by the given threshold decryption scheme.

Key words: identity-based encryption; fully homomorphic encryption; multi-identity; threshold decryption

身份基加密[1–4](identity-based encryption, IBE)是对传统的公钥基础设施(public key infrastructure, PKI)技术的优化, 它以用户专属的身份标志(identity, ID)为公钥, 不采用数字证书的概念, 用户使用和后台管理都很简单, 具有广泛的应用前景[5]。相比于IBE, 分层身份基加密[6–9](hierarchical identity-based encryption, HIBE)将ID分为多个层次, 每一层都有自己的私钥生成器(private key generator, PKG), 负责为低层身份生成、分发私钥, 大大减轻了根PKG的负担[10]。

全同态加密[11–14](fully homomorphic encryption,

收稿日期:2018 – 11 – 14

基金项目:国家重点研发计划项目(2017YFB0802000); 国家自然科学基金项目(U1636114; 61772550; 61572521); 国家密码发展基金项目(MMJJ20170112)

作者简介:杨晓元(1959—), 男, 教授.研究方向: 信息安全; 密码学. E-mail: xyyangwj@126.com

* 通信联系人 E-mail: 1542855584@qq.com

网络出版时间:2019 – 07 – 09 09 : 49 : 00　　**网络出版地址**:http://kns.cnki.net/kcms/detail/51.1773.TB.20190705.1515.004.html

FHE)因其在密文处理的特殊性质,在云计算领域发挥重要作用。相比于FHE,多密钥全同态加密[15−18](multi-key fully homomorphic encryption, MKFHE)能够实现对不同用户的密文进行运算,应用场景更加广泛。

IBE与FHE结合,能够对身份密文进行同态运算和访问控制,数据处理更加灵活,但目前此类研究成果并不多。2013年,Gentry等[14]提出了第一个分层身份基全同态加密方案(hierarchical identity-based fully homomorphic encryption, HIBFHE),但该方案只能对同一ID下的密文进行运算。2015年,Clear等[16]利用文献[4]的IBE方案,构造一个多身份全同态加密方案(multi-identity FHE),实现对不同ID下密文的同态运算,但该方案密文扩展复杂,效率不高。2017年,Canetti等[19]提出了一个利用IBE和MKFHE构造multi-identity FHE的通用转化模型。但该模型下的密文规模大,计算复杂度高。

门限密码系统的基础是秘密共享,它对用户密钥进行分散管理,提高密码系统安全性。基于门限FHE构造多方计算(multi-party computation, MPC)协议能够有效减少通信复杂度和通信轮度[20]。2016年,Mukherjee等[17]提出了支持门限解密的MKFHE方案,并据此构造了一个2轮MPC协议。

作者对文献[14]提出的第一个HIBFHE方案和文献[17]提出的MKFHE转化机制以及门限解密展开研究,构造一个新的multi-identity FHE方案。首先,使用工具矩阵[21](gadget matrix)得到新的加解密形式,取代原方案的校平技术[14](flatting)。并改变IBE的底层格基维度,得到优化的密文规模和密钥规模更小的HIBFHE方案,但该方案仍然只能对同一ID下的密文进行运算。然后,利用文献[17]中的MKFHE转化机制,为优化的HIBFHE方案构造屏蔽系统(masking system),生成辅助密文,为密文扩展提供技术支持。最后,得到提出的multi-identity FHE方案,实现对不同ID下密文的同态运算和访问控制,并给出门限解密过程,利用文献[17]构造MPC协议的方法,同样可以构造一个公共参考字符串(common reference string, CRS)模型下的2轮MPC协议。

1 预备知识

1.1 工具矩阵

定义1[21] 对任意模数q,$\ell_q=\lceil \mathrm{lb}\, q\rceil$,行向量$\boldsymbol{g}=(2^0,2^1,\cdots,2^{\ell-1})\in\mathbb{Z}_q^{\ell_q}$,矩阵$\boldsymbol{G}_n=(\boldsymbol{I}_n\otimes\boldsymbol{g})\in\mathbb{Z}_q^{n\times n\ell_q}$。

定义2[21] 随机化函数$\boldsymbol{g}^{-1}:\mathbb{Z}_q\to\mathbb{Z}^{\ell_q}$,对于任意$a\in\mathbb{Z}_q$,列向量$\boldsymbol{x}\leftarrow\boldsymbol{g}^{-1}(a)$的元素为0、1,并且有$\langle\boldsymbol{g},\boldsymbol{x}\rangle=a$。

定义3[21] 随机化函数$\boldsymbol{G}^{-1}:\mathbb{Z}_q^{n\times m}\to\mathbb{Z}_q^{n\ell_q\times m}$,对任意矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$\boldsymbol{X}\leftarrow\boldsymbol{G}^{-1}(\boldsymbol{A})$的元素为0、1,并且有$\boldsymbol{G}\cdot\boldsymbol{X}=\boldsymbol{G}\cdot\boldsymbol{G}^{-1}(\boldsymbol{A})=\boldsymbol{A}$。

1.2 门限解密

定义4[17] 一个支持一轮门限分布式解密协议的MKFHE方案还包括两个算法:

1)MKFHE.PartDec:输入扩展密文$\hat{\boldsymbol{c}}$、公钥串$(pk_1,pk_2,\cdots,pk_N)$和第i个用户的私钥sk_i,输出部分解密值p_i。

2)MKFHE.FinDec:重复执行N次上述步骤,得到N个部分解密值,运行最终解密函数,得到$\mu'=\mathrm{MKFHE.FinaDec}(p_1,p_2,\cdots,p_N)$。

设$\boldsymbol{c}_i$为第i个用户对μ_i加密的密文,$\hat{\boldsymbol{c}}_i\leftarrow\mathrm{Expand}((pk_1,pk_2,\cdots,pk_N),i,\boldsymbol{c}_i)$为$\boldsymbol{c}_i$的扩展密文,$\{p_1,p_2,\cdots,p_N\}$为部分解密值集合,$f$表示任意有效的同态运算函数,$\hat{\boldsymbol{C}}=\mathrm{Eval}(f,\hat{\boldsymbol{c}}_1,\hat{\boldsymbol{c}}_2,\cdots,\hat{\boldsymbol{c}}_t)$表示对扩展密文进行同态运算后的结果密文。一个门限多密钥全同态加密方案还应当满足以下两条性质:

1)正确性:

$$\mathrm{FinDec}(\hat{\boldsymbol{C}},p_1,p_2,\cdots,p_N)=f(\mu_1,\mu_2,\cdots,\mu_t)。$$

2)可模拟性:存在一个多项式时间的模拟器$\mathrm{Sim}^{\mathrm{thr}}$,对于上述输入$\mu=f(\mu_1,\mu_2,\cdots,\mu_t)$、$\hat{\boldsymbol{c}}$以及除$sk_i$之外的所有密钥,输出$p_i'\leftarrow\mathrm{Sim}^{\mathrm{thr}}(\mu,\hat{\boldsymbol{c}},i,\{sk_j\}_{j\in N\setminus\{i\}})$满足$p_i'$和$p_i$的统计不可区分性。

2 多身份全同态加密方案构造

2.1 优化的HIBFHE方案

对文献[14]提出的第一个HIBFHE方案进行改进,得到密文规模和密钥规模更小的优化方案。

1)HIBFHE.Setup$(1^\lambda,1^L,1^d)$:设λ为安全参数,L为计算电路的最大深度,d为分层的最大深度。选择$\chi=\chi(\lambda,L)$,得到B_χ有界的误差分布。选择n、m、q作为标准误差学习(learning with errors, LWE)问题的参数,$m=\omega(n\mathrm{lb}\,q)=[(k+1)n+1]\,\ell_q$,$\ell_q=\lceil\mathrm{lb}\,q\rceil$。采用$\mathrm{GenBasis}(1^n,1^m,q)$[9]算法,可以得到随机均匀矩阵$\boldsymbol{A}_0\in\mathbb{Z}_q^{m\times n}$和对应格$\Lambda^\perp(\boldsymbol{A}_0)=\{\boldsymbol{x}\in\mathbb{Z}^m:\boldsymbol{x}\boldsymbol{A}=\boldsymbol{0}\bmod q\}$的一组短基$\boldsymbol{S}_0\in\mathbb{Z}^{m\times m}$。对每个$(i,b)\in[k]\times\{0,1\}$,得到均匀独立矩阵$\boldsymbol{A}_{i,b}\in\mathbb{Z}_q^{n\times m}$,随机选择$\boldsymbol{z}\leftarrow\mathbb{Z}_q^m$。输出系统参数$pp=(n,m,q,\chi,B_\chi)$,$mpk=(\boldsymbol{A}_0,\{\boldsymbol{A}_{i,b}\},\boldsymbol{z})$,$msk=\boldsymbol{S}_0$。所有的算法都默认以$pp$为输入。

2)HIBFHE.KeyGen(msk,ID):设身份$ID=(id_1,id_2,\cdots,id_k)=\{0,1\}^k$,则有$\boldsymbol{A}_{ID}=\boldsymbol{A}_0\|\boldsymbol{A}_{1,id_1}\|\boldsymbol{A}_{2,id_2}\|\cdots\|\boldsymbol{A}_{k,id_k}\in\mathbb{Z}_q^{m\times(k+1)n}$,$\boldsymbol{A}_{i,id_i}=\boldsymbol{A}_{i,b}\in\mathbb{Z}_q^{m\times n}$。采用$\mathrm{ExtBasis}(\boldsymbol{S}_0,\boldsymbol{A}_{ID})$[9]算法,输出格$\Lambda^\perp(\boldsymbol{A}_{ID})$的一组短基$\boldsymbol{S}_{ID}$;采用$\mathrm{SampleD}(\boldsymbol{S}_{ID},\boldsymbol{A}_{ID},\boldsymbol{z})$[4]算法,输出$\boldsymbol{t}_{ID}\in\{0,1\}^{(k+1)n}$满足$\boldsymbol{A}_{ID}\cdot\boldsymbol{t}_{ID}=$

$z \bmod q$。令私钥$sk_{ID}=\boldsymbol{s}=(1,-\boldsymbol{t}_{ID}^{\mathrm{T}})\in\mathbb{Z}_q^{(k+1)n+1}$, $\boldsymbol{A}'_{ID}=\boldsymbol{z}\,\|\,\boldsymbol{A}_{ID}\in\mathbb{Z}_q^{m\times[(k+1)n+1]}$, 则有$\boldsymbol{s}\cdot(\boldsymbol{A}'_{ID})^{\mathrm{T}}=\boldsymbol{0}\bmod q\in\mathbb{Z}_q^m$成立。

设ID'为低层身份信息, 即$ID'=(ID\,\|\,\overline{ID})$, $\boldsymbol{A}_{ID'}=\boldsymbol{A}_{ID}\,\|\,\boldsymbol{A}_{\overline{ID}}$, 采用上述算法ExtBasis($\boldsymbol{S}_{ID},\boldsymbol{A}_{ID'}$)得到$\boldsymbol{S}_{ID'}$; 采用算法SampleD($\boldsymbol{S}_{ID'},\boldsymbol{A}_{ID'},\boldsymbol{z}$)得到$\boldsymbol{t}_{ID'}$。由此, 从高层PKG得到低层$ID$对应的私钥。

3) HIBFHE.Enc(μ,mpk,ID): 随机选择矩阵$\boldsymbol{R}\in\{0,1\}^{m\times m}$, $\mu\in\{0,1\}$, $\boldsymbol{E}\leftarrow\chi^{[(k+1)n+1]\times m}$, 得到密文:

$$\boldsymbol{C}_{ID}=(\boldsymbol{A}'_{ID})^{\mathrm{T}}\cdot\boldsymbol{R}+\mu\boldsymbol{G}_{(k+1)n+1}+\boldsymbol{E}\tag{1}$$

计算:

$$\boldsymbol{s}\cdot\boldsymbol{C}=\mu\boldsymbol{s}\boldsymbol{G}_{(k+1)n+1}+\boldsymbol{s}\boldsymbol{E}\tag{2}$$

4) HIBFHE.Eval($(\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_t),f$): 设$\boldsymbol{C}_1$、$\boldsymbol{C}_2$分别为某一$ID$下加密的不同密文, 私钥为$\boldsymbol{s}$, 定义同态加法运算$\boldsymbol{C}^{(+)}=\boldsymbol{C}_1+\boldsymbol{C}_2$, 则$\boldsymbol{s}\cdot\boldsymbol{C}^{(+)}=(\mu_1+\mu_2)\boldsymbol{s}\boldsymbol{G}+(\boldsymbol{e}_1+\boldsymbol{e}_2)$满足同态加法性质; 定义同态乘法运算$\boldsymbol{C}^{(\times)}=\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)$, 则$\boldsymbol{s}\boldsymbol{C}^{(\times)}=(\mu_1\boldsymbol{s}\boldsymbol{G}+\boldsymbol{e}_1)\boldsymbol{G}^{-1}(\boldsymbol{C}_2)=\mu_1\boldsymbol{s}\boldsymbol{C}_2+\boldsymbol{e}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)=\mu_1\mu_2\boldsymbol{s}\boldsymbol{G}+\mu_1\boldsymbol{e}_2+\boldsymbol{e}_1\cdot\boldsymbol{G}^{-1}(\boldsymbol{C}_2)$满足同态乘法性质。因此, 通过加法和乘法组合, 可以对密文做任意同态运算, 满足$\boldsymbol{s}\boldsymbol{C}_{\mathrm{Eval}}=f(\mu_1,\mu_2,\cdots,\mu_t)\boldsymbol{s}\boldsymbol{G}+\boldsymbol{e}'$。

5) HIBFHE.Dec($\boldsymbol{C},\boldsymbol{s}$): 定义向量$\boldsymbol{\omega}=(\lceil q/2\rceil,0,\cdots,0)^{\mathrm{T}}\in\mathbb{Z}_q^{(k+1)n+1}$, 若$\boldsymbol{C}$为初始密文, 则:

$$\begin{aligned}\mu'=&\boldsymbol{s}\boldsymbol{C}\boldsymbol{G}^{-1}(\boldsymbol{\omega})=(\mu\boldsymbol{s}\boldsymbol{G}+\boldsymbol{e}')\boldsymbol{G}^{-1}(\boldsymbol{\omega})=\mu\boldsymbol{s}\boldsymbol{\omega}+\\&\left\langle\boldsymbol{e}'\cdot\boldsymbol{G}^{-1}(\boldsymbol{\omega})\right\rangle=\mu(1,-\boldsymbol{t}_{ID}^{\mathrm{T}})(\lceil q/2\rceil,0,\cdots,0)^{\mathrm{T}}+\\&\left\langle\boldsymbol{e}'\cdot\boldsymbol{G}^{-1}(\boldsymbol{\omega})\right\rangle=\mu\cdot\lceil q/2\rceil+e'。\end{aligned}$$

若$\mu'=small$, 则$\mu=0$; 若$\mu'-\lceil q/2\rceil=small$, 则$\mu=1$。

同理, 若$\boldsymbol{C}$为同态运算结果密文, 则$\mu'=\boldsymbol{s}\boldsymbol{C}_{\mathrm{Eval}}\cdot\boldsymbol{G}^{-1}(\boldsymbol{\omega})=f(\mu_1,\mu_2,\cdots,\mu_t)\cdot\lceil q/2\rceil+e$。

由于$B_\chi\ll q$, 计算

$$\left\lfloor\frac{\mu'}{\lceil q/2\rceil}\right\rfloor=\left\lfloor f(\mu_1,\mu_2,\cdots,\mu_t)+\frac{e}{\lceil q/2\rceil}\right\rfloor=f(\mu_1,\mu_2,\cdots,\mu_t),$$

满足同态方案性质。

2.2 优化的HIBFHE方案屏蔽系统

定义5[17] 算法Lcomb($(\boldsymbol{C}_{1,1},\boldsymbol{C}_{1,2},\cdots,\boldsymbol{C}_{m,m}),\boldsymbol{v}$)执行以下步骤:

1) 对于所有的$i\in[m]$、$j\in[m]$, $[m]=\{1,2,\cdots,m\}$, 定义矩阵$\boldsymbol{Z}_{i,j}\in\mathbb{Z}_q^{[(k+1)n+1]\times m}$的形式如下:

$$Z_{i,j}[a,b]=\begin{cases}v_i, & a=1,b=j;\\0, & \text{其他。}\end{cases}$$

2) 输出$\boldsymbol{C}_{\mathrm{lc}}=\sum_{i=1,j=1}^{m,m}\boldsymbol{C}_{i,j}\boldsymbol{G}^{-1}(\boldsymbol{Z}_{i,j})$。

对于一个矩阵$\boldsymbol{M}\in\mathbb{Z}_q^{m\times m}$, $M_{i,j}$表示矩阵中的各元素, $\boldsymbol{C}_{i,j}\in\mathbb{Z}_q^{[(k+1)n+1]\times m}$为$M_{i,j}$的密文, 对应私钥$\boldsymbol{s}\in\mathbb{Z}_q^{[(k+1)n+1]}$, 向量$\boldsymbol{v}\in\mathbb{Z}_q^m$表示一个函数。该同态操作以$M_{i,j}$、$\boldsymbol{C}_{i,j}$、$\boldsymbol{s}$和$\boldsymbol{v}$为输入, 输出一个密文$\boldsymbol{C}_{\mathrm{lc}}$, 则

$$\begin{aligned}\boldsymbol{s}\boldsymbol{C}_{\mathrm{lc}}=&\sum_{i=1,j=1}^{m,m}\boldsymbol{s}\boldsymbol{C}_{i,j}\cdot\boldsymbol{G}^{-1}(\boldsymbol{Z}_{i,j})=\\&(1,-\boldsymbol{t}_{ID}^{\mathrm{T}})\begin{bmatrix}\boldsymbol{v}\boldsymbol{M}\\\boldsymbol{0}^{m-1}\end{bmatrix}+\boldsymbol{e}''=\boldsymbol{v}\boldsymbol{M}+\boldsymbol{e}''\end{aligned}\tag{3}$$

本屏蔽系统包括两个多项式时间算法[17]:

1) UniEnc(μ,ID,mpk): 运行HIBFHE.Enc(μ,mpk,ID)算法, 对$\boldsymbol{R}\in\{0,1\}^{m\times m}$的每个元素进行加密, 得到$m^2$个密文, 令$\boldsymbol{U}=(\boldsymbol{V}^{(1,1)},\boldsymbol{V}^{(1,2)},\cdots,\boldsymbol{V}^{(m,m)})\in(\mathbb{Z}_q^{[(k+1)n+1]\times m})^{m^2}$。

2) Extend(μ,mpk,ID,ID'): 令$\boldsymbol{X}=\mathrm{Lcomb}(\boldsymbol{U},\boldsymbol{t}_{ID'}^{\mathrm{T}}\cdot(\boldsymbol{A}_{ID}^{\mathrm{T}}-\boldsymbol{A}_{ID'}^{\mathrm{T}}))$, 则

$$\begin{aligned}\boldsymbol{s}'\boldsymbol{C}=&\boldsymbol{s}'[(\boldsymbol{A}'_{ID})^{\mathrm{T}}\cdot\boldsymbol{R}+\mu\boldsymbol{G}+\boldsymbol{E}]=\\&(1,-\boldsymbol{t}_{ID'}^{\mathrm{T}})\begin{pmatrix}\boldsymbol{z}^{\mathrm{T}}\\\boldsymbol{A}_{ID}^{\mathrm{T}}\end{pmatrix}\boldsymbol{R}+\mu\boldsymbol{s}'\boldsymbol{G}+\boldsymbol{s}'\boldsymbol{E}=\\&(\boldsymbol{t}_{ID'}^{\mathrm{T}}\boldsymbol{A}_{ID'}^{\mathrm{T}}-\boldsymbol{t}_{ID'}^{\mathrm{T}}\boldsymbol{A}_{ID}^{\mathrm{T}})\boldsymbol{R}+\mu\boldsymbol{s}''\boldsymbol{G}+\boldsymbol{s}'\boldsymbol{E}=\\&\boldsymbol{t}_{ID'}^{\mathrm{T}}(\boldsymbol{A}_{ID'}^{\mathrm{T}}-\boldsymbol{A}_{ID}^{\mathrm{T}})\boldsymbol{R}+\mu\boldsymbol{s}'\boldsymbol{G}+\boldsymbol{s}'\boldsymbol{E}\end{aligned}\tag{4}$$

由式(3)可得:

$$\boldsymbol{s}\boldsymbol{X}=\boldsymbol{t}_{ID'}^{\mathrm{T}}(\boldsymbol{A}_{ID}^{\mathrm{T}}-\boldsymbol{A}_{ID'}^{\mathrm{T}})\boldsymbol{R}+\boldsymbol{e}_X\tag{5}$$

式(4)和(5)相加, 得到:

$$\boldsymbol{s}\boldsymbol{X}+\boldsymbol{s}'\boldsymbol{C}=\mu\boldsymbol{s}'\boldsymbol{G}+\boldsymbol{s}'\boldsymbol{E}+\boldsymbol{e}_X\tag{6}$$

2.3 提出的multi-identity FHE方案

利用以上优化的HIBFHE方案和屏蔽系统, 构造一个新的multi-identity FHE方案, 记为ε。

1) ε.Setup($1^\lambda,1^L,1^d$): 设κ为参与方身份的最大个数, 则定义身份集合$I=(ID_1,ID_2,\cdots,ID_\kappa)$, $|ID_i|\le d$。$m=[(d+1)n+1]\ell_q$, $q\ge2^{\omega(L\mathrm{llb}\,\lambda)}B_\chi$。运行HIBFHE.Setup($1^\lambda,1^L,1^d$), 得到$pp$、$mpk$和$msk$。算法都默认以$pp$为输入。

2) ε.KeyGen(ID_i,msk): 运行HIBFHE.KeyGen(msk,ID)算法, 得到私钥sk_{ID_i}和对应的$\boldsymbol{A}'_{ID_i}$。为保证解密时的密钥级联, 用0对私钥进行填充, 将其维度扩大到$\mathbb{Z}_q^{(d+1)n+1}$。

3) ε.Enc(ID_i,μ,mpk): 运行屏蔽系统的UniEnc(μ,ID,mpk)算法, 输出一对值$(\boldsymbol{U},\boldsymbol{C})$。为保证密文间的同态运算, 用0对密文矩阵进行补充, 将其维度扩大到$\mathbb{Z}_q^{[(d+1)n+1]\times m}$, $\boldsymbol{c}=(\boldsymbol{U},\boldsymbol{C})$。

4) ε.Expand($I,\boldsymbol{C},mpk$): 以身份集合和初始密文为输入, 得到扩展密文$\hat{\boldsymbol{C}}\in\mathbb{Z}_q^{\kappa[(d+1)n+1]\times\kappa m}$。具体过程如下:

①对于任意的$j\in[\kappa]\backslash i$, 运行$\boldsymbol{X}_j\leftarrow$Extend($\boldsymbol{U},mpk,ID_i,ID_j$)算法。

②扩展密文可分解为κ^2个部分, 每部分都是$\hat{\boldsymbol{C}}[a,b]\in\mathbb{Z}_q^{[(d+1)n+1]\times m}$的矩阵, 定义如下:

$$\hat{\boldsymbol{C}}[a,b]=\begin{cases}\boldsymbol{C}, & a=b;\\\boldsymbol{X}_j, & a=i\ne j,b=j;\\\boldsymbol{0}^{[(d+1)n+1]\times m}, & \text{其他。}\end{cases}$$

对第i个用户，对应的身份为ID_i，$\boldsymbol{C}\in\mathbb{Z}_q^{[(d+1)n+1]\times m}$为初始密文，则扩展密文为：

$$\hat{\boldsymbol{C}}_i=\begin{bmatrix}\boldsymbol{C}&0&\cdots&0&\cdots&0\\0&\boldsymbol{C}&\cdots&0&\cdots&0\\\vdots&\vdots&&\vdots&\vdots&\vdots\\\boldsymbol{X}_1&\boldsymbol{X}_2&\cdots&\boldsymbol{C}&\cdots&\boldsymbol{X}_\kappa\\\vdots&\vdots&\vdots&\vdots&&\vdots\\0&0&\cdots&0&\cdots&\boldsymbol{C}\end{bmatrix}\tag{7}$$

式中，$\boldsymbol{X}_j$位于第i行，$j\in[\kappa]$。

令$\hat{\boldsymbol{s}}=(\boldsymbol{s}_{ID_1},\boldsymbol{s}_{ID_2},\cdots,\boldsymbol{s}_{ID_\kappa})$，计算$\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}=(\boldsymbol{s}_1\boldsymbol{C}+\boldsymbol{s}_i\boldsymbol{X}_1,\boldsymbol{s}_2\boldsymbol{C}+\boldsymbol{s}_i\boldsymbol{X}_2,\cdots,\boldsymbol{s}_\kappa\boldsymbol{C}+\boldsymbol{s}_i\boldsymbol{X}_\kappa)$，由式(6)可知，$\boldsymbol{s}_i\boldsymbol{X}_j+\boldsymbol{s}_j\boldsymbol{C}_i=\mu\boldsymbol{s}_j\boldsymbol{G}+\boldsymbol{s}_j\boldsymbol{e}+\boldsymbol{e}_X$，因此，

$$\begin{aligned}\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}=&(\mu\boldsymbol{s}_1\boldsymbol{G}+\hat{\boldsymbol{e}}_1,\mu\boldsymbol{s}_2\boldsymbol{G}+\hat{\boldsymbol{e}}_2,\cdots,\mu\boldsymbol{s}_\kappa\boldsymbol{G}+\hat{\boldsymbol{e}}_\kappa)=\\&\mu\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+(\hat{\boldsymbol{e}}_1,\hat{\boldsymbol{e}}_2,\cdots,\hat{\boldsymbol{e}}_\kappa)\end{aligned}\tag{8}$$

式(8)与(2)具有相同的形式，满足加解密正确性。

5) ε.Eval$((\hat{\boldsymbol{C}}_1,\hat{\boldsymbol{C}}_2,\cdots,\hat{\boldsymbol{C}}_t),f)$：同态运算的定义与HIBFHE.Eval$((\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_t),f)$相同。定义同态加法运算为$\hat{\boldsymbol{C}}^{(+)}=\hat{\boldsymbol{C}}_1+\hat{\boldsymbol{C}}_2$，则$\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}^{(+)}=(\mu_1+\mu_2)\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+(\hat{\boldsymbol{e}}_1+\hat{\boldsymbol{e}}_2)$；定义同态乘法运算为$\hat{\boldsymbol{C}}^{(\times)}=\hat{\boldsymbol{C}}_1\boldsymbol{G}^{-1}(\hat{\boldsymbol{C}}_2)$，则$\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}^{(\times)}=(\mu_1\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+\hat{\boldsymbol{e}}_1)\boldsymbol{G}^{-1}(\hat{\boldsymbol{C}}_2)=\mu_1\mu_2\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+\hat{\boldsymbol{e}}'$；二者均满足同态运算性质。因此，同态运算结果密文满足$\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}_{\text{Eval}}=f(\mu_1,\mu_2,\cdots,\mu_t)\cdot\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+\hat{\boldsymbol{e}}_{\text{Eval}}$。

6) ε.Dec$(\hat{\boldsymbol{C}},\hat{\boldsymbol{s}})$：解密过程与HIBFHE.Dec$(\boldsymbol{C},\boldsymbol{s})$类似。定义向量$\hat{\boldsymbol{\omega}}=(0,\cdots,0,\lceil q/2\rceil,0,\cdots,0)^{\mathrm{T}}\in\mathbb{Z}_q^{\kappa[(d+1)n\times1]}$，对第$i$个用户，$\lceil q/2\rceil$位于第$(i-1)[(d+1)n+1]+1$行。若$\hat{\boldsymbol{C}}$为初始密文，则$\mu'=\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}\hat{\boldsymbol{G}}^{-1}(\hat{\omega})=\mu\cdot\lceil q/2\rceil+e'$；若$\hat{\boldsymbol{C}}$为同态结果密文，则$\mu'=\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}_{\text{Eval}}\hat{\boldsymbol{G}}^{-1}(\hat{\omega})=f(\mu_1,\mu_2,\cdots,\mu_t)\cdot\lceil q/2\rceil+\hat{e}$。由此可求出$\mu$和$f(\mu_1,\mu_2,\cdots,\mu_t)$，满足同态方案性质。

3 方案分析

3.1 噪音分析

定义6[14] (β-noisy ciphertext)设μ为明文消息，$\boldsymbol{C}$为Enc过程得到的密文，$\boldsymbol{s}$为对应的私钥，则有$\boldsymbol{s}\boldsymbol{C}=\mu\boldsymbol{s}\boldsymbol{G}+\boldsymbol{e}$。若对于$\|\boldsymbol{e}\|_\infty\leq\beta$，则称$\boldsymbol{C}$为$\beta$噪音密文。

在优化的HIBFHE方案中，密文$\boldsymbol{C}=(\boldsymbol{A}'_{ID})^{\mathrm{T}}\cdot\boldsymbol{R}+\mu\boldsymbol{G}+\boldsymbol{E}$，$\boldsymbol{E}=(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_m)$，$\|\boldsymbol{e}\|_\infty\leq B_\chi\cdot\boldsymbol{s}\cdot\boldsymbol{C}=\mu\boldsymbol{s}\boldsymbol{G}+\boldsymbol{s}\boldsymbol{E}$，对应的噪音$\|\boldsymbol{s}\boldsymbol{E}\|_\infty\leq[(k+1)n+1]B_\chi$，则$\beta=[(k+1)n+1]B_\chi$。

在提出的multi-identity FHE方案中，设$\hat{\boldsymbol{C}}$为β'密文，$\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}=\mu\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+\hat{\boldsymbol{e}}$，对应噪音$\|\hat{\boldsymbol{e}}\|_\infty=\|\boldsymbol{s}\boldsymbol{E}+\boldsymbol{e}_X\|_\infty$，其中，$\|\boldsymbol{s}\boldsymbol{E}\|=\beta$，$\|\boldsymbol{e}_X\|\leq\left\|\sum_{i=1,j=1}^{m,m}\boldsymbol{e}_{i,j}\cdot\boldsymbol{G}^{-1}(\boldsymbol{Z}_{i,j})\right\|_\infty=m^3\beta$，$\|\hat{\boldsymbol{e}}\|_\infty=(m^3+1)\beta$。因此$\beta'=(m^3+1)\beta$。同理，在同态运算阶段，噪音的增长主要来自于同态乘法，$\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}^{(\times)}=\mu_1\mu_2\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+\mu_1\hat{\boldsymbol{e}}_2+\hat{\boldsymbol{e}}_1\cdot\boldsymbol{G}^{-1}(\hat{\boldsymbol{C}}_2)$，$\|\hat{\boldsymbol{e}}_{\text{Eval}}\|_\infty=(1+\kappa m)\beta'$。设$L$表示进行同态操作的电路深度，则进行同态操作后噪音最多增长为$\|\hat{\boldsymbol{e}}_{\text{Eval}}\|_\infty=(1+\kappa m)^L\beta'$。同理，解密密文$\mu'=\hat{\boldsymbol{s}}\hat{\boldsymbol{C}}\cdot\hat{\boldsymbol{G}}_\kappa^{-1}(\hat{\omega})$，若$\hat{\boldsymbol{C}}$为初始密文，对应噪音$\|\hat{\boldsymbol{e}}_{\text{Dec}}\|_\infty\leq\kappa m\beta'$；若$\hat{\boldsymbol{C}}$为同态运算密文，对应噪音$\|\hat{\boldsymbol{e}}_{\text{Dec}}\|_\infty\leq\kappa m(1+\kappa m)^L\beta'$。为保证解密正确，$\|\hat{\boldsymbol{e}}_{\max}\|_\infty\leq\dfrac{q}{4}$。由上述公式可知：

$$\begin{aligned}\|\hat{\boldsymbol{e}}_{\max}\|_\infty=&\kappa m(1+\kappa m)^L\beta'=\\&\kappa m(1+\kappa m)^L(m^3+1)[(k+1)n+1]B_\chi\leq\frac{q}{4},\end{aligned}$$

满足解密正确条件。

3.2 安全性分析

定理1 优化的HIBFHE方案为选择身份下的选择明文攻击不可区分性(IND–sID–CPA)安全，困难性可规约到LWE问题。

证明：优化的HIBFHE方案与HIBE方案相比，增加了一个Eval算法。在Eval算法中，输入均为密文，不影响方案的安全性。因此，优化的HIBFHE方案的安全性与HIBE方案相同，证明过程可参考文献[9]。

引理[9] 存在一个多项式时间的预言机算法$\mathcal{S}$攻击$\text{LWE}_{q,\chi}$问题，对于任意多项式时间敌手$\mathcal{A}$在IND–CPA游戏中攻击优化的HIBFHE方案的密钥封装机制(key encapsulation mechanism, KEM)，满足$Adv_{\text{LWE}_{q,\chi}}(\mathcal{S}^{\mathcal{A}})\geq Adv_{\text{KEM}}^{\text{IND–CPA}}(\mathcal{A})-\text{negl}(n)$，其中，$\text{negl}(n)$表示值可忽略的函数。

采用密钥封装机制(KEM)对优化的HIBFHE方案的加密和解密过程进行封装，具体过程如下：

1)随机均匀选取$\boldsymbol{A}\in\mathbb{Z}_q^{m\times(d+1)n}$，$\boldsymbol{z}\leftarrow\mathbb{Z}_q^m$，$\boldsymbol{t}\in\{0,1\}^{(d+1)n}$，满足$\boldsymbol{A}\boldsymbol{t}=\boldsymbol{z}\bmod q$。令$\boldsymbol{A}'=\boldsymbol{z}\,\|\,\boldsymbol{A}\in\mathbb{Z}_q^{m\times((d+1)n+1)}$，$\boldsymbol{s}=(1,-\boldsymbol{t}^{\mathrm{T}})\in\mathbb{Z}_q^{(d+1)n+1}$，则有$\boldsymbol{s}\cdot(\boldsymbol{A}')^{\mathrm{T}}=\boldsymbol{0}\bmod q\in\mathbb{Z}_q^m$。其中，$(\boldsymbol{A},\boldsymbol{A}',\boldsymbol{z})$公开，$(\boldsymbol{t},\boldsymbol{s})$私有。

2)随机选取$\boldsymbol{R}\in\{0,1\}^{m\times m}$作为加密时的随机数。选取$b\in\{0,1\}$，$\boldsymbol{E}_1\in\chi^{(d+1)n\times m}$，$\boldsymbol{E}_2\in\chi^{((d+1)n+1)\times m}$，令$\boldsymbol{B}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{R}+\boldsymbol{E}_1$，$\boldsymbol{P}=(\boldsymbol{A}')^{\mathrm{T}}\cdot\boldsymbol{R}+\mu_b\boldsymbol{G}+\boldsymbol{E}_2$。

3)令$\boldsymbol{\eta}=(\lceil q/2\rceil,0,\cdots,0)^{\mathrm{T}}\in\mathbb{Z}_q^{((d+1)n+1)}$，计算$\mu'=\boldsymbol{s}\boldsymbol{P}\cdot\boldsymbol{G}^{-1}(\boldsymbol{\eta})=\mu_b\cdot\lceil q/2\rceil+e$进行解密。

分析封装过程可知：

1)优化的HIBFHE方案中由GenBasis$(1^n,1^m,q)$生成的矩阵$\boldsymbol{A}$接近于均匀分布，统计距离可忽略不计，并且对于任意的$\boldsymbol{A}\in\mathbb{Z}_q^{m\times(k+1)n}$，$k\leq d$同样成立。

2)在未获得密钥的情况下，攻击者从矩阵$\boldsymbol{P}$中获取明文信息，等价于从矩阵$\boldsymbol{B}$中获取随机选取的矩阵$\boldsymbol{R}$，等价于解决LWE问题。

3)攻击者$\mathcal{A}$在IND–CPA游戏中获胜的优势不大于$\mathcal{S}$在求解LWE问题中获胜的优势。

因此, 引理成立。

定理2[9]　存在一个多项式时间的预言机算法$\mathcal{S}$攻击KEM, 对于任意多项式时间敌手$\mathcal{B}$在IND–sID–CPA游戏中攻击作者优化的HIBFHE方案, 满足$Adv_{\mathrm{KEM}}(\mathcal{S}^{\mathcal{B}}) \geq Adv_{\mathrm{HIBFHE}}^{\mathrm{IND-sID-CPA}}(\mathcal{B}) - \mathrm{negl}(n)$。

文献[9]中给出了$\mathcal{S}$模拟攻击者$\mathcal{B}$的攻击过程, 分析模拟攻击过程可知:

1)优化的HIBFHE方案中由GenBasis($1^n, 1^m, q$)生成的矩阵$\boldsymbol{A}$接近于均匀分布, 统计距离可忽略不计。

2)攻击者$\mathcal{B}$可以通过询问检验预言机是否为真实世界, 即是否可信。

3)攻击者$\mathcal{B}$在IND–sID–CPA游戏中获胜的优势不大于$\mathcal{S}$攻击KEM获胜的优势。

因此, 定理2成立。

由上述引理和定理2可以得到, $Adv_{\mathrm{LWE}_{q,\chi}}(\mathcal{S}^{\mathcal{A}}) \geq Adv_{\mathrm{HIBFHE}}^{\mathrm{IND-sID-CPA}}(\mathcal{B}) - \mathrm{negl}(n)$, 即将优化的HIBFHE方案的安全性归约到LWE问题, 得到优化的HIBFHE方案的IND–sID–CPA安全性。

因此, 定理1证明完毕。

定理3　优化的HIBFHE方案的屏蔽系统为IND–CPA安全。

证明: 优化的HIBFHE方案的屏蔽系统安全性证明过程可参考文献[9]。

攻击者$\mathcal{A}$在IND–CPA游戏中可以获得系统参数和对加密预言机的询问, 在此条件下, 攻击者想要以一个不可忽略的优势识别出μ_b。为此, 假设Game 0为标准的IND–CPA游戏, 攻击者的攻击对象为分布(pp, $\boldsymbol{C}, \boldsymbol{U}$), 其中, $\boldsymbol{C} = \mathrm{GSW.Enc}(\mu_b, pk)$, $\boldsymbol{U} = \mathrm{GSW.Enc}(R(a, b), pk)$。

Game 1: 与Game 0相比, 不同之处在于令$\boldsymbol{U} = \mathrm{GSW.Enc}(0, pk)$。由文献[11]的语义安全性可知, 攻击者无法以不可忽略的优势区分Game 1与Game 0, 即$\left|Adv_{G_1}[\mathcal{A}] - Adv_{G_0}[\mathcal{A}]\right| = \mathrm{negl}(n)$。

Game 2: 与Game 1相比, 不同之处在于令$\boldsymbol{C} = \mathrm{GSW.Enc}(0, pk)$。由文献[11]的语义安全性可知, 攻击者无法以不可忽略的优势区分Game 2与Game 1, 即$\left|Adv_{G_2}(\mathcal{A}) - Adv_{G_1}(\mathcal{A})\right| = \mathrm{negl}(n)$。

因此, 有$\left|Adv_{G_2}(\mathcal{A}) - Adv_{G_0}(\mathcal{A})\right| = \mathrm{negl}(n)$成立。即攻击者从已知密文中区分$\mu_b$的优势可以忽略不计。

因此, 定理3证明完毕。

定理4　若优化的HIBFHE方案为IND–sID–CPA安全, 且所构造的屏蔽系统为IND–CPA安全, 则提出的multi-identity FHE方案为IND–sID–CPA安全。

证明: 提出的multi-identity FHE方案是IND–sID–CPA安全的, 当且仅当多项式时间敌手无法以不可忽略的优势赢得以下的攻击者–挑战者交互游戏:

1)挑战者C选择身份信息$ID^* \leftarrow I$, 生成(mpk, msk) $\leftarrow$ Setup($1^\lambda, 1^d, 1^L$), 并将mpk返还给攻击者$\mathcal{B}$。

2)对于$\alpha = 1, 2, \cdots, poly$; $\mathcal{B}$向C询问ID_α。如果ID_α=ID^*或ID_α在分层结构中为ID^*的任意一个祖先, 则游戏结束, $\mathcal{B}$失败; 如果$ID_\alpha \neq ID^*$且ID_α在分层结构中不是ID^*的任意一个祖先, C生成$\boldsymbol{s}_{ID_\alpha} \leftarrow$ Extract(msk, ID_α), 并返回给$\mathcal{B}$。

3)$\mathcal{B}$将一对等长消息μ_0、μ_1发送给C。

4)C随机选择$b \in \{0, 1\}$, 生成$\boldsymbol{C}^* \leftarrow$ Enc(pp, ID^*, μ_b), 并将密文返还给攻击者。

5)$\mathcal{B}$输出$b' \in \{0, 1\}$, 如果$b' = b$, 则攻击成功。

对任意的多项式时间敌手$\mathcal{B}$, 其攻击成功的优势为$Adv_{\mathcal{B}} = |\Pr(b' = b) - 1/2|$。

定理1证明了攻击者在询问ID对应的私钥条件下, 区分μ_b的优势忽略不计, 定理2证明了攻击者在获得扩展密文的情况下区分μ_b的优势忽略不计。因此, 本游戏的中敌手攻击成功的优势忽略不计, 即$Adv_{\mathcal{B}} = |\Pr(b' = b) - 1/2| = \mathrm{negl}(n)$。

因此, 提出的multi-identity FHE方案为IND–sID–CPA安全。

3.3　性能分析

在应用场景上, 将提出的multi-identity FHE方案与文献[14, 16–17]方案进行比较。利用文献[17]的MKFHE转化机制, 将IBFHE方案转化为multi-identity FHE方案, 因此, 提出的multi-identity FHE方案实现了IBE与MKFHE的结合, 在功能上兼具二者的优势。具体分析见表1。

表 1　提出的multi-identity FHE方案与相关方案的应用场景比较

Tab. 1　Comparison of application scenarios for the proposed multi-identity FHE scheme and related schemes

方案	多身份	多密钥	分层
文献[14]方案	NO	NO	YES
文献[16]方案	YES	YES	NO
文献[17]方案	NO	YES	NO
提出的multi-identity FHE方案	YES	YES	YES

设参数n、m、q为标准LWE问题的参数, $m = \omega(n\ell_q)$, $\ell_q = \lceil \mathrm{lb}\, q \rceil$。$\kappa$为参与方不同身份的最大个数。

在效率上, 将提出的multi-identity FHE方案与文献[16]方案进行对比。设密文明文比为加密单比特明文消息对应的扩展密文大小, 则文献[16]方案中密文明文比为$\kappa^2(m+1)^2\ell_q$, 提出的multi-identity FHE方案密文明文比为$\kappa^2[(d+1)n+1]m$。由于$m = \omega(n\ell_q)$, 模数q为n的指数级, 在分层深度$d \leq O(\ell_q^3)$的情况下, 提出

的方案密文明文比更小。设扩展密文为ρ噪音密文，考虑同态乘法运算，则一次同态运算后，文献[16]方案的同态密文噪音为$(\kappa(m+1)\ell_q+1)\rho$，噪音扩张为$(\kappa(m+1)\ell_q+1)$，由第3.1节噪音分析可知，提出的方案的同态密文噪音为$(1+\kappa m)\rho$，噪音扩张为$(1+\kappa m)$。因此，提出的方案同态运算的噪音扩张率更小。与文献[16]方案相比，提出的方案使用的底层IBE方案具有分层性质，高层PKG可以为低层ID分配密钥，允许多个PKG参与密钥的生成分发，大大减轻了根PKG的负担。因此，提出的方案效率更高。具体分析见表2。

表 2 提出的multi-identity FHE方案与文献[16]方案的效率比较

Tab. 2 Comparison of the efficiency for the proposed multi-identity FHE scheme and the literature [16] scheme

方案	密文 明文比	一次同态运算 噪音扩张	PKG参与 个数
文献[16]方案	$\kappa^2(m+1)^2\ell_q^2$	$\kappa(m+1)\ell_q+1$	1
提出的multi-identity FHE方案	$\kappa^2(dn+1)m$	$\kappa m+1$	>1

4 门限解密过程

上述提出的multi-identity FHE方案的门限解密过程由以下两个算法实现[17]：

1）ε.PartDec$(\hat{\boldsymbol{C}},mpk,I,i,sk_{ID_i})$：将扩展密文分解为$\kappa$个子块，$\hat{\boldsymbol{C}}=\left[\hat{\boldsymbol{C}}^{(1)}\quad\hat{\boldsymbol{C}}^{(2)}\quad\cdots\quad\hat{\boldsymbol{C}}^{(\kappa)}\right]^{\mathrm{T}}$，其中，$\hat{\boldsymbol{C}}^{(i)}\in\mathbb{Z}_q^{[(d+1)n+1]\times\kappa m}$。定义$\hat{\boldsymbol{\omega}}=(\lceil q/2\rceil,0,\cdots,0)^{\mathrm{T}}\in\mathbb{Z}_q^{\kappa[(d+1)n+1]}$，第$i$个用户使用私钥对扩展密文进行运算，有$\gamma_i=\boldsymbol{s}_i\hat{\boldsymbol{C}}^{(i)}\hat{\boldsymbol{G}}^{-1}(\hat{\boldsymbol{\omega}})\in\mathbb{Z}_q$，输出$p_i=\gamma_i+e_i^{\mathrm{sim}}\in\mathbb{Z}_q$，其中，$e_i^{\mathrm{sim}}\xleftarrow{\$}[-B_{\mathrm{smdg}}^{\mathrm{dec}},B_{\mathrm{smdg}}^{\mathrm{dec}}]$，$B_{\mathrm{smdg}}^{\mathrm{dec}}=2^{L\mathrm{llb}\,\lambda}B_\chi$为随机的模糊噪音。

2）ε.FinalDec$(p_1,p_2,\cdots,p_\kappa)$：每个用户分别运行$\varepsilon$.PartDec算法，重复执行$\kappa$次，得到$(p_1,p_2,\cdots,p_\kappa)$，计算：

$$\sum_{i\in\{\kappa\}}p_i=\sum_{i\in\{\kappa\}}\gamma_i+\sum_{i\in\{\kappa\}}e_i^{\mathrm{sim}}=e^{\mathrm{sim}}+\sum_{i\in\{\kappa\}}\boldsymbol{s}_i\hat{\boldsymbol{C}}^{(i)}\hat{\boldsymbol{G}}^{-1}(\hat{\boldsymbol{\omega}})=$$
$$e^{\mathrm{sim}}+\left(\mu\hat{\boldsymbol{s}}\hat{\boldsymbol{G}}_\kappa+\hat{\boldsymbol{e}}\right)\hat{\boldsymbol{G}}^{-1}(\hat{\boldsymbol{\omega}})=\mu\cdot\lceil q/2\rceil+\hat{e}'+e^{\mathrm{sim}},$$

对应噪音为$\left\|\hat{e}'+e^{\mathrm{sim}}\right\|_\infty$。由第3.1节噪音分析可知，$\|\hat{e}'\|_\infty\le 2^{O(L\mathrm{llb}\,\lambda)}B_\chi$，$\left\|e^{\mathrm{sim}}\right\|_\infty\le\kappa B_{\mathrm{smdg}}^{\mathrm{dec}}=2^{O(L\mathrm{llb}\,\lambda)}B_\chi$。已知模数$q\ge 2^{\omega(L\mathrm{llb}\,\lambda)}B_\chi$，因此$\left\|\hat{e}'+e^{\mathrm{sim}}\right\|_\infty\le\frac{q}{4}$成立。输出$\mu'=\left\|\left[\frac{p}{q/2}\right]\right\|=\left\|\left[\mu+\frac{\hat{e}'+e^{\mathrm{sim}}}{q/2}\right]\right\|$，最终得出正确密文。

根据提出的multi-identity FHE方案，结合门限解密，利用文献[17]中的方法，可以构造一个CRS模型下的2轮MPC协议。

5 结 论

针对已有的IBFHE方案进行研究，将其扩展到多身份场景中，得到新的multi-identity FHE方案。结果表明，本方案加密单比特明文消息时，对应密文规模更小，同态运算的噪音扩张率更小，且允许多个PKG参与密钥的生成分发。因此，本方案效率更高。最后，给出了本方案的门限解密过程。此外，属性基密码体制既克服了传统密码体制访问控制单一的缺点，又能同时实现对机密性和不可伪造性的保护[22]，与MKFHE的结合具有重要的研究价值，如何构造安全高效的多属性全同态加密方案是下步研究的重点。

参考文献：

[1] Shamir A.Identity-based cryptosystems and signature schemes[M]//Advances in Cryptology.Berlin:Springer, 1984:47–53.

[2] Boneh D,Franklin M.Identity-based encryption from the Weil pairing[M]//Advances in Cryptology— CRYPTO 2001. Berlin:Springer,2001:213–229.

[3] Cocks C.An identity based encryption scheme based on quadratic residues[M]//Cryptography and Coding.Berlin: Springer,2001:360–363.

[4] Gentry C,Peikert C,Vaikuntanathan V.Trapdoors for hard lattices and new cryptographic constructions[C]//Proceedings of the 40th Annual ACM Symposium on Theory of Computing.New York:ACM, 2008: 197–206.

[5] Zeng Mengqi,Qing Yu,Tan Pingzhang,et al.An overview of identity-based cryptography research[J].Computer Application Research,2010,27(1):27–31.[曾梦岐,卿昱,谭平璋,等.基于身份的加密体制研究综述[J].计算机应用研究,2010,27(1):27–31.]

[6] Horwitz J,Lynn B.Towards hierarchical identity-based encryption[M]//Advances in Cryptology—EUROCRYPT 2002.Berlin:Springer,2002:466–481.

[7] Boyen X,Waters B.Anonymous hierarchical identity-based encryption (without random oracles)[M]//Advances in Cryptology—CRYPTO 2006.Berlin:Springer,2006: 290–307.

[8] Boneh D,Boyen X.Efficient selectice-ID secure identity based encryption without random oracles[M]//Advances in Cryptology—EUROCRYPT 2004.Berlin:Springer, 2004:223–238.

[9] Cash D,Hofheinz D,Kiltz E,et al.Bonsai trees,or how to delegate a lattice basis[M]//Advances in Cryptology— EUROCRYPT 2010.Berlin:Springer,2010:523–552.

[10] Zhang Xi,Yang Ling.An efficient identity-based hierarchical encryption scheme[J].Computer Engineering and Applications,2012,48(24):101–105.[张席,杨玲.一个高效的基于身份的分层加密方案[J].计算机工程与应用,2012, 48(24):101–105.]

[11] Rivest R,Adleman L,Dertouzos M.On data banks and pri-

vacy homomorphisms[J].Foundations of Secure Computation,1978,4:169–179.

[12] Gentry C.Fully homomorphic encryption using ideal lattices[C]//Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing.New York:ACM,2009:169–178.

[13] Brakerski Z,Vaikuntanathan V.Efficient fully homomorphic encryption from (standard) LWE[C]//Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science.Palm Springs:IEEE,2011:97–106.

[14] Gentry C,Sahai A,Waters B.Homomorphic encryption from learning with errors:Conceptually-simpler,asymptotically-faster,attribute-based[M]//Advances in Cryptology—CRYPTO 2013.Berlin:Springer,2013:75–92.

[15] L'opez-Alt A,Tromer E,Vaikuntanathan V.On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]//Proceedings of the 44th Annual ACM Symposium on Theory of Computing.New York:ACM,2012:1219–1234.

[16] Clear M,McGoldrick C.Multi-identity and multi-key leveled FHE from learning with errors[M]//Advances in Cryptology—CRYPTO 2015.Berlin:Springer,2015:630–656.

[17] Mukherjee P,Wichs D.Two round multiparty computation via multi-key FHE[M]//Advances in Cryptology—EUROCRYPT 2016.Berlin:Springer,2016:735–763.

[18] Chen Long,Zhang Zhenfeng,Wang Xueqing.Batched multi-hop multi-key FHE from ring-LWE with compact ciphertext extension[M]//Theory of Cryptography.Cham:Springer,2017:597–627.

[19] Canetti R,Raghuraman S,Richelson S,et al.Chosen-ciphertext secure fully homomorphic encryption[M]//Public-Key Cryptography—PKC 2017.Berlin:Springer,2017:213–240.

[20] Li Zengpeng,Ma Chunguang,Zhou Hongsheng.Study of all homomorphic encryption[J].Journal of Cryptography,2017,4(6):561–578.[李增鹏,马春光,周红生.全同态加密研究[J].密码学报,2017,4(6):561–578.]

[21] Micciancio P,Peikert C.Trapdoors for lattices:Simpler,tighter,faster,smaller[M]//Advances in Cryptology—EUROCRYPT 2012.Berlin:Springer,2012:700–718.

[22] Han Yiliang,Lu Wanyi,Yang Xiaoyuan.Attribute-based signcryption for circuits from multi-linear maps[J].Journal of Sichuan University(Engineering Science Edition),2013,45(6):27–32.[韩益亮,卢万谊,杨晓元.支持电路结构的多线性映射属性签密方案[J].四川大学学报(工程科学版),2013,45(6):27–32.]

（编辑　赵　婧）

引用格式: Yang Xiaoyuan,Tu Guangsheng,Kong Yongjun,et al.Multi-identity fully homomorphic encryption scheme supporting threshold decryption[J].Advanced Engineering Sciences,2019,51(4):133–139.[杨晓元,涂广升,孔咏骏,等.支持门限解密的多身份全同态加密方案[J].工程科学与技术,2019,51(4):133–139.]