计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180446
55(10):2164-2173,2018

标准模型下格上基于身份的门限解密方案

吴立强[1] 杨晓元[1,2] 张敏情[1]
[1](武警部队网络与信息安全保密重点实验室(武警工程大学) 西安 710086)
[2](网络信息安全教育部重点实验室(西安电子科技大学) 西安 710071)
(latticewj@163.com)

Identity-Based Threshold Decryption Scheme from Lattices under the Standard Model

Wu Liqiang[1], Yang Xiaoyuan[1,2], and Zhang Minqing[1]
[1](*Key Laboratory of Network and Information Security* (*Engineering University of Chinese Armed Police Force*), *Xi'an* 710086)
[2](*Key Laboratory of Computer Network and Information Security* (*Xi Dian University*), *Ministry of Education*, *Xi'an* 710071)

Abstract The identity-based threshold decryption (IBTD) system combines the secret sharing method with the identity-based encryption mechanism. In a (t, N) IBTD system, N decryption servers share the private key corresponding to a user's identity. When to decrypt, at least t servers are required to participate in and calculate their corresponding decryption shares. However, less than t or fewer servers are unable to obtain any information about the plaintext. At present, the existing IBTD schemes from lattices are constructed under the random model, and the main method is to divide the private key statistically close to a Gauss distribution directly. This paper constructs a non-interactive IBTD scheme. A public vector is split using the Lagrange secret partition method, and each decryption server obtains its respective characteristic vector. Each private key share is obtained by sampling the pre-image of the characteristic vectors through the private trapdoor function for each decryption server. The user's complete private key is effectively hidden and the security of the scheme is improved. The difficulty of the discrete logarithm problem is used to realize the verifiability of decryption share. The correctness of the decryption share is guaranteed by the homomorphism of the operations between the common vector and the private key shares. The IND-sID-CPA security for the proposed scheme is proved based on the decisional learning with errors (LWE) hardness assumption under the standard model.

Key words identity-based threshold decryption; lattice; standard model; publicly verfication; non-interactivity

摘 要 基于身份的门限解密体制(identity-based threshold decryption, IBTD)是将秘密共享方法和基于身份加密算法有效结合.在(t,N)门限解密方案中,N 个解密服务器共享用户私钥,当解密时,至少需要 t 个服务器参与并计算相应解密份额,才能正确恢复出明文.然而,少于 t 个或更少的服务器无法

收稿日期:2018-06-11;**修回日期**:2018-08-15
基金项目:国家自然科学基金项目(U1636114,61572521,61772550);武警工程大学基础研究项目(WJY201523)
This work was supported by the National Nature Science Foundation of China (U1636114, 61572521, 61772550) and the Foundation Funding Research Project of the Engineering University of Chinese Armed Police Force (WJY201523).

获取关于明文的任何信息.目前现存的格上IBTD方案都是在随机预言模型下证明的,主要方法是对服从高斯分布的私钥直接分割.针对该问题,构造了一种非交互的IBTD方案,采用拉格朗日秘密分割方法对一个公共向量进行拆分,每个解密服务器得到各自的特征向量,通过用户的私有陷门,对特征向量进行原像抽样,得到私钥份额,有效隐藏了用户完整私钥,提高方案的安全性.在解密份额验证时,采用离散对数问题的难解性,实现了可公开验证性.在解密份额组合时,通过公共向量分割合并和解密份额分割合并之间运算的同态性,保证解密的正确性.在标准模型下,将该方案的安全性规约为判定性LWE(learning with errors)困难假设,证明了其满足IND-sID-CPA安全.

关键词 基于身份的门限解密;格;标准模型;可公开验证性;非交互性

中图法分类号 TP391

门限解密体制是将秘密共享方法和加密算法有效结合.在(t,N)门限解密体制中,N个解密服务器共享解密私钥,当对密文进行解密时,至少需要t个服务器共同参与并返回相应的解密份额,才能正确恢复出密文所对应的明文.然而,少于t个或更少的服务器无法获取关于明文的任何信息.门限解密体制能够降低或避免因个体完全掌握解密密钥而导致的滥用权限、密钥丢失,或某个服务器被攻击者完全控制而造成系统瘫痪等安全风险,使系统的容错率和安全性得到较大提高.

传统公钥加密体制必须明确公钥与其拥有主体的对应关系.1984年,Shamir创造性地引入了基于身份密码学(identity-based encryption, IBE),在该体制中,公钥直接就是其拥有者的身份信息,如手机号码、Email等,这种公钥密码体制天然地确定了公钥与实体之间的绑定关系,无需借助可信第三方,因此简化了繁琐的证书管理环节,具有较强的实用性.

将基于身份的思想引入到门限解密环境中,某个身份所对应私钥的持有者不再是某个单一个体,而可能是多个实体.比如某个公司的总经理,当他不能处理以公司名义加密的文件时,他可以选择将解密私钥分割并分发给公司的3个副经理,当且仅当其中的2个副经理合作才能够解密公司的文件,而任何1个副经理是无法独自解密的.这样的机制,一方面限制了某个副经理独自解密的过大权限,另一方面即使在某一个副经理缺席的情况下,仍然能够正常处理公司业务.

在基于身份的门限解密系统中,非交互性和可验证性是2个重要属性.非交互性是指解密服务器在解密过程中不需要相互进行数据交换.可验证性是指可公开验证密文的合法性.如果一个基于身份的门限解密方案满足上述2个性质,那么每一个解密服务器只需要使用自己的私钥份额即可完成解密,而无需通过某种交互机制来验证密文份额合法性,从而使方案更为简洁和高效.

本文通过借鉴利用双线性映射构造基于身份门限解密的方法,采用格上陷门产生函数生成系统主密钥,采用左右基扩展技术为用户生成私钥,私钥本身是身份所对应的陷门.在秘密分割时,没有对用户私钥进行直接分割,而是采用拉格朗日方法对一个公共向量进行分割,得到每个解密服务器的特征向量.通过用户拥有的私有陷门,对特征向量进行原像抽样,得到私钥份额,有效隐藏了用户完整私钥,从而使其更为安全.在解密份额的验证中,采用离散对数问题的难解性,保证其可公开验证性.在解密份额组合时,通过公共向量拆分合并和解密份额拆分合并之间运算的同态性,保证方案解密的正确性.在标准模型下,将该方案的安全性规约为判定性LWE困难假设,证明了其能够满足IND-sID-CPA安全.同现存的格上基于身份的门限加密方案相比,本文是对满足均匀分布的向量进行分割,安全性更高,同时证明过程在标准模型下完成.

1 相关工作

门限密码体制起源于著名密码学家Shamir和Blakley提出的(t,N)门限秘密共享方法[1-2].前者采用多项式插值的方法设计了门限秘密共享方案,而后者则使用了有限几何方法.Boneh等人[3]最早将门限思想引入到了基于身份的加密中.其初衷是解决密钥管理中心PGK完全掌握系统主私钥,从而造成权限过大的问题,主要方法是将主PKG的系统主密钥采用秘密分割方法分发给了N个分PKG,每个分PKG为用户生成部分私钥份额,至少需要t个分PKG产生的私钥份额,才能构成用户的完整私钥,完成解密功能,因此该机制也称为分布式

PKG. 2006 年,Boneh 等人[4]扩展了这种思想,构造了基于身份的(t,N)门限加密体制(threshold identity-based encryption, TIBE). 之后,考虑到分 PKG 也可以执行解密的功能,因而解密操作由原来的用户端转移到了分 PKG 上,但是这种机制存在 2 个弊端:1)要求分 PKG 必须实时在线处理解密请求;2)如果可用的 PKG 数量不足 t 个,就无法完成解密.

因此,Baekand 和 Zheng 认为[5]:在基于身份密码学中,对用户私钥进行分割比对系统主密钥进行分割更为合适,每个解密服务器拥有用户部分私钥,可直接解密基于身份的密文,得到解密份额,合并这些解密份额即可恢复出明文. 利用这种思路,他们提出了基于身份的门限解密方案(identity-based threshold decryption, IBTD),并基于双线性对,构造了一个选择密文攻击安全的基于身份门限解密方案,同时将其扩展为了一个可仲裁的身份加密方案. 文献[6-7]分别构造了选择明文攻击安全的 IBTD 方案.

上述 IBTD 方案都是基于双线性映射实现. 量子计算具有天然的并行性,其超强的计算能力,可用于密码破译. 特别是 Shor 量子算法,可对目前广泛使用的、基于经典困难问题构造的公钥密码方案进行有效攻击,严重威胁其安全性. 在目前已知的抗量子攻击候选密码体制中,基于格上困难问题设计的密码体制[8],不但能够抵抗 Shor 算法攻击,而且具有最困难实例与一般实例等价、高效易实现等优势,是后量子密码中最典型的代表,已经成为当前密码学领域研究的热点.

在利用格上困难问题,构造门限加解密方面,已有部分成果. Bendlin 等人[9]利用 Regev 加密系统[10],构造了第一个格上门限公钥加密方案,其安全性能够规约到格上困难问题的最难实例. Xie 等人[11]利用有损陷门函数,给出了一种高效门限加密方案的构造方法,并利用格工具进行了实例化. Singh 等人[12]提出了一个高效的 TPKE 方案,其满足可重拆分属性,即如果拆分算法输出腐化私钥份额的数量小于 t,则私钥的拆分能进行任意多项式次.

上述这些格上 TPKE 都是非基于身份环境下的. 2014 年,Singh 等人[13]将格上门限解密方案[12]扩展到了基于身份环境中,构造了格上第 1 个基于身份的门限解密方案. 在该方案中,用户身份所对应的私钥满足正态分布,直接对于该私钥进行分割,每个参与者获得一个私钥份额,当需要解密时,采用私钥份额进行解密得到解密份额,合并即可恢复出明文. 文献[14]在标准模型下,基于 LWE 困难问题,采用 Shamir 门限秘密共享的方法,构造了一种标准模型下选择身份安全的模糊身份加密方案(fuzzy identity based encryption, FIBE),即当用户公钥属性集与加密公钥属性集的交集等于或大于规定的门限值时,可正常解密. 文献[15]基于格上困难问题提出了一种基于身份的门限加密方案,同时利用通用转化方法,得到了一种带关键字的密文搜索加密方案.

当前,格与双线性是设计密码方案的两大重要工具,双线性对映射群具有灵活代数结构,已经存在很多成熟的关键技术、安全模型、证明方法,而格密码学主要依赖于线性运算及巧妙的陷门设计,且具有抗量子攻击的性能,因此,将格这一新兴的密码学工具与成熟的双线性密码方案构造方法相结合,可以有效推动格密码学的发展. 本文工作就是基于这样的思路展开.

2 预备知识

定义$[j]=\{1,2,\cdots,j\}$,$\mathbb{Z}$ 表示整数. 假设 $\boldsymbol{a}$,$\boldsymbol{b}$,$\boldsymbol{c}$ 表示列向量,用 $\boldsymbol{A}$,$\boldsymbol{B}$,$\boldsymbol{C}$ 表示矩阵. 对矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$,符号$[\boldsymbol{A}|\boldsymbol{B}]$代表他们横向联结,$[\boldsymbol{A};\boldsymbol{B}]$表示纵向联结. C_N^t 表示从 N 个不同元素中取出 t 个元素的组合数.

2.1 格和 LWE 假设

定义 1. 整数格. 设 $\boldsymbol{B}=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m]\in\mathbb{Z}^{n\times m}$是一个矩阵,其列向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\in\mathbb{Z}^n$线性无关,$\boldsymbol{B}$ 生成的 n 维满秩格为

$$L(\boldsymbol{B})=\{\boldsymbol{y}\in\mathbb{Z}^n \quad \text{s.t. } \exists\boldsymbol{s}\in\mathbb{Z}^m,\ \boldsymbol{y}=\boldsymbol{B}\boldsymbol{s}=\sum_{i=1}^{m}s_i\boldsymbol{b}_i\}.$$

对于素数 q,$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和 $\boldsymbol{u}\in\mathbb{Z}_q^n$,$q$-ary 格定义为

$\Lambda_q(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m \quad \text{s.t. } \exists\boldsymbol{s}\in\mathbb{Z}_q^n$ 满足 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}=\boldsymbol{e}(\mathrm{mod}\ q)\}$;

$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m \quad \text{s.t. } \boldsymbol{A}\boldsymbol{e}=\boldsymbol{0}(\mathrm{mod}\ q)\}$;

$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m \quad \text{s.t. } \boldsymbol{A}\boldsymbol{e}=\boldsymbol{u}(\mathrm{mod}\ q)\}$.

定义 2. 格的高斯分布. 用 $\rho_\sigma(\boldsymbol{x})$ 表示标准 n 维高斯分布,其均值为 0,方差为 σ,即 $\rho_\sigma(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}\|^2/\sigma^2)$,对于一个给定的格 L 和实数 $\sigma>0$,若 $\rho_\sigma(L)=\sum_{\boldsymbol{x}\in L}\rho_\sigma(\boldsymbol{x})$ 是有限的,可以定义格的高斯分布为

$$\exists\,\boldsymbol{y}\in L, D_{L,\sigma}(\boldsymbol{y})=\frac{\rho_\sigma(\boldsymbol{y})}{\rho_\sigma(L)}.$$

定义 3. LWE 问题[10]. 包括计算性 LWE 问题和判定性 LWE 问题.

计算性 LWE 问题:选取一个公开参数 $n>1$,一个模数 $q\geqslant 2$,定义噪声概率分布为 $\psi_s=D_{\mathbf{Z},s}$,秘密选取均匀分布的向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$. 随机选取均匀分布的向量 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{e}\in\psi_s^m$,输出样本 $(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$. 如果存在一个算法,能够利用给定的若干个样本以很大的概率恢复出 $\boldsymbol{s}\in\mathbb{Z}_q^n$,那么该算法能够解决计算性 LWE 问题.

判定性 LWE 问题:存在一个敌手 $\mathcal{A}$ 和 LWE 预言机 $\mathcal{O}$,该预言机包含 2 个抽样算法 $\mathcal{O}_{\mathrm{S}}$(根据 LWE 分布输出样本 $(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$,其中随机选择矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,选择服从 ψ_s^m 分布的 $\boldsymbol{e}\in\mathbb{Z}_q^m$,选择服从均匀分布的 $\boldsymbol{s}\in\mathbb{Z}_q^n$. 实际上,$\boldsymbol{s}\in\psi_s^n$ 同样可以被证明是安全的)和 $\mathcal{O}_{\$}$(从均匀分布 $U(\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m)$ 中输出一个随机样本),如果 $\mathcal{A}$ 可以解决判定性 LWE 问题当且仅当优势

$$Adv(\mathcal{A})=|Pr[\mathcal{A}^{\mathcal{O}_{\mathrm{S}}}=1]-Pr[\mathcal{A}^{\mathcal{O}_{\$}}=1]|$$

是不可忽略的.

下面的定理将 LWE 困难假设规约到了格上经典困难问题.

定理 1[10]. 设 n,q 是整数,$a\in(0,1)$,取 $aq>2\sqrt{n}$. 如果存在一个高效的算法解决了 LWE 问题,就存在一个有效的量子算法,在最坏的情况下以复杂度 $\tilde{O}(n/a)$ 解决判定性的最短向量问题(gap shortest vector problem, GapSVP)和最短无关向量问题(shortest independent vectors problem, SIVP).

2.2 相关的函数和数学工具

1) 陷门产生函数

定理 2[16]. 假设 $q>3$ 是奇数,$m=\lceil 6n\log q\rceil$,TrapGen 是一个概率多项式时间内算法,能够以绝对的优势同时输出一组矩阵 $(\boldsymbol{A}\in\mathbb{Z}_q^{n\times m},\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m})$,其中 $\boldsymbol{A}$ 统计上满足均匀分布,$\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一个优良基,且以压倒一切的概率满足 $\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\leqslant O(\sqrt{n\lg q})$ 和 $\|\boldsymbol{T}_{\boldsymbol{A}}\|\leqslant O(n\lg q)$,$\boldsymbol{T}_{\boldsymbol{A}}$ 通常称为陷门.

2) 抽样算法

引理 1[16]. 假设 $q>2$,整数 $m>n$,矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一个陷门,且 $\sigma\geqslant\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\omega(\sqrt{\log m})$,那么,对于 $c\in\mathbb{R}^m$ 和 $u\in\mathbb{Z}_q^n$:

① $Pr[x\sim\Lambda_q^{\perp}(\boldsymbol{A}):\|x\|>\sqrt{n}\sigma]\leqslant negl(n)$.

② 对于任意的 $\boldsymbol{u}\in\mathbb{Z}_q^n$,存在多项式时间内的随机原像抽样算法 $SamplePre(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},\sigma)$,能够返回一个统计上服从 $D_{\Lambda_q^u(\boldsymbol{A}),\sigma}$ 分布的向量 $\boldsymbol{x}\in\Lambda_q^u(\boldsymbol{A})$.

③ 存在多项式时间内的高斯抽样算法 $Sample(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},c)$,能够返回一个统计上服从 $D_{\Lambda,\sigma,c}$ 分布的向量 $\boldsymbol{x}\in\Lambda_q^{\perp}(\boldsymbol{A})$.

④ 如果采用 $SamplePre$ 获取 $O(m\lg m)$ 个采样 $e_i\in D_{\Lambda_q^u(\boldsymbol{A}),\sigma}(1\leqslant i\leqslant m\lg m)$,那么从中找到 m 个线性无关向量,形成满秩矩阵 $\boldsymbol{E}=\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_m\}\in\mathbb{Z}_q^{m\times m}$ 的概率接近于 1.

3) 左采样基算法

在 HIBE 方案中[16],左采样基算法使用一个低维格的陷门生成一个更高维数格的陷门,从而实现格基授权. 具体方法是利用矩阵 $\boldsymbol{A}$ 的陷门 $\boldsymbol{T}_{\boldsymbol{A}}$ 进行多次采样,形成一个扩展矩阵的短基. 根据引理 1 中第④条,这些短基是满秩的且尺寸较短,可以作为陷门,为更高维数的矩阵进行抽样.

算法 1. 左抽样基算法 $SampleBasisLeft(\boldsymbol{A}_0,\boldsymbol{A}_1+H(id)\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{A}},\sigma)$.

输入:用户 id,$\boldsymbol{A}_1+H(id)\boldsymbol{B}$,和陷门 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$,$\sigma\geqslant\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\omega(\sqrt{\lg m})$.

输出:身份 $\boldsymbol{F}_{id}=(\boldsymbol{A}_0|\boldsymbol{A}_1+H(id)\boldsymbol{B})$ 的陷门 $\boldsymbol{T}_{id}\sim D_{\mathbf{Z}^{2m\times 2m},\sigma}$,满足 $\boldsymbol{F}_{id}\cdot\boldsymbol{T}_{id}=\boldsymbol{0}$.

① 随机选取统计服从 $D_{\mathbf{Z}^{m\times n},\sigma}$ 分布的 $\boldsymbol{e}_1\in\mathbb{Z}^m$;

② 计算 $\boldsymbol{u}_1=(\boldsymbol{A}_1+H(id)\boldsymbol{B})\cdot\boldsymbol{e}_1$;

③ $\boldsymbol{e}_2=SamplePre(\boldsymbol{A}_0,\boldsymbol{T}_{\boldsymbol{A}},-\boldsymbol{u}_1,\sigma)\in\mathbb{Z}^{m\times n}$;

④ 设置 $\boldsymbol{e}=(\boldsymbol{e}_2,\boldsymbol{e}_1)$,重复上述过程,直到得到 $2m$ 个线性无关向量;

⑤ 将上述 $2m$ 个向量组合成 $\boldsymbol{T}_{id}\in\mathbb{Z}^{2m\times 2m}$.

4) 身份编码

在基于身份的门限解密方案中,采用有限域 $\mathbb{Z}_q$ 上 n 维向量表示用户身份. 选择域 $\mathbb{F}$,对于系数小于 n 的多项式 $\boldsymbol{g}\in\mathbb{F}[x]$,定义 $coeffs(\boldsymbol{g})\in\mathbb{F}^n$ 表示 $\boldsymbol{g}$ 的 n 维系数向量,如果 $\boldsymbol{g}$ 系数小于 $n-1$,可以给右边填充 0 使其成为 n 位. 如果 $\boldsymbol{f}\in\mathbb{F}[x]$ 是一个次数为 n 的不可逆多项式,那么对于任何一个多项式 $\boldsymbol{g}\in\mathbb{F}[x]$,多项式 $\boldsymbol{g}\bmod\boldsymbol{f}$ 的次数不超过 n,系数 $coeffs(\boldsymbol{g}\bmod\boldsymbol{f})\in\mathbb{F}^n$ 即为 n 维向量. 设用户身份为 $\boldsymbol{g}=(g_1,g_2,\cdots,g_n)\in\mathbb{Z}_q^n$,定义

$$H(\boldsymbol{g})=\begin{pmatrix}coeffs(\boldsymbol{g})\\coeffs(\boldsymbol{g}x\bmod\boldsymbol{f})\\coeffs(\boldsymbol{g}x^2\bmod\boldsymbol{f})\\\vdots\\coeffs(\boldsymbol{g}x^{n-1}\bmod\boldsymbol{f})\end{pmatrix}\in\mathbb{F}^{n\times n}.$$

定义 4. 假设 q 是素数,n 是一个整数,定义身份编码函数 $H:\mathbb{Z}_q^n\to\mathbb{Z}_q^{n\times n}$ 差分满秩编码函数,它具有 2 个性质[16]:

① 对于所有不同的身份 $\boldsymbol{g}_1, \boldsymbol{g}_2 \in \mathbb{Z}_q^n$，矩阵 $H(\boldsymbol{g}_1)-H(\boldsymbol{g}_2)\in\mathbb{Z}_q^{n\times n}$ 是满秩的；

② H 的计算能够在多项式时间内完成.

5) Shamir 的(t,N)门限方案

使用 Shamir 的(t,N)门限方案分享一个秘密 S 的过程为：

① 随机选择 $t-1$ 个系数 $a_1, a_2, \cdots, a_{t-1}\in\mathbb{Z}_q$.

② 构造一个 $t-1$ 阶多项式函数：

$$f(x)=S+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}.$$

③ 定义用户的编号为 $1,2,\cdots,N$，对于 $1\leqslant i\leqslant N$，计算每个份额 $S_i=f(i)$，并发送 S_i 给第 i 个用户.

④ 当用户的有效份额数达到门限值 t 时，函数 $f(x)$可以被重构：

$$f(x)=\sum_{j=1}^{t}S_iM_j,$$

其中，M_j 表示 Lagrange 系数：

$$M_j=\prod_{i=1,i\neq j}^{t}\frac{-i}{j-i}(\mathrm{mod}\ q),$$

那么，秘密 $S=f(0)$，秘密被恢复.

Shamir 门限方案具有一些优良性质：

① 完善性. 对于每个秘密 S，当份额数量大于或者等于 t 个，有且仅有唯一的一个 $t-1$ 次多项式满足条件；而少于 t 个份额得不到关于 S 的任何有用信息.

② 同态性.

Ⅰ. 如果对所有的秘密份额 $S_i(1\leqslant i\leqslant N)$ 都相加或者相乘一个常数，那么新的秘密相当于原来秘密 S 与这个常数相加或者相乘.

Ⅱ. 如果存在 2 个秘密值 S 和 T，选择的多项式是分别是 $f(x)$和 $g(x)$，相应的份额分别为 $f(1)$，$f(2),\cdots,f(N)$和 $g(1),g(2),\cdots,g(N)$. 定义一个新的秘密份额为 $h(j)=f(j)+g(j)$，$1\leqslant j\leqslant N$，那么这些新份额可重构出秘密 $f(0)+g(0)=S+T$.

6) 离散对数问题

定义 5. 离散对数(discrete logarithm, DL)假设. 循环群 G_1 的阶是素数 p，G_1 的生成元是 g. 离散对数(DL)问题是指，给定二元组(g,g^a)，求出 a 的值，其中 $a\in\mathbb{Z}_q^*$. 该问题在密码学的典型离散对数群上是困难问题，设敌手为 $\mathcal{A}$，则：

$$Adv_{\mathcal{A}}^{\mathrm{DL}}(k)=Pr[\mathcal{A}(g,g^a)\rightarrow a]\leqslant\varepsilon$$

成立，其中 ε 是可忽略的概率，$Adv_{\mathcal{A}}^{\mathrm{DL}}$ 表示攻击 DL 问题成功的概率. DL 假设是指没有多项式时间内运行的概率性算法能够解决离散对数困难问题.

2.3 相关定义和安全模型

1) TIBE 的定义

定义 6. 一个基于身份的门限解密 IBTD 方案包含 7 个算法：

① 系统初始化算法 *Setup*. 输入安全参数 λ，密钥生成中心 PKG 输出公共的系统参数 pp，以及主私钥 msk.

② 密钥生成算法 *KeyGen*. 输入一个用户身份 id，以及 PKG 私钥 msk，输出用户私钥 S_{id}.

③ 私钥分割算法 *DisKey*. 输入一个身份 id 和对应私钥 S_{id}，解密服务器的个数 N，以及门限参数 t. 该算法生成 id 对应的 N 个私钥份额 $TSK_{id,i}(1\leqslant i\leqslant N)$. 同时，为了能够验证各个解密服务器输出的解密份额是否有效，还应当生成与秘密份额 $TSK_{id,i}$ 相对应的验证信息 $TVK_{id,i}$. 注意，$TSK_{id,i}$ 被秘密交给对应的第 i 个解密服务器，而 $TVK_{id,i}(1\leqslant i\leqslant N)$ 公开.

④ 加密算法 *Enc*. 输入一个用户的身份 id 和待加密的明文 M，输出密文 $\boldsymbol{C}$.

⑤ 部分解密算法 *SubDec*. 输入一个密文 $\boldsymbol{C}$，解密服务器 i 的私钥份额 $TSK_{id,i}$ 和 $TVK_{id,i}$，输出一个解密份额 θ_i.

⑥ 份额验证算法 *ShareVery*. 输入一个密文 $\boldsymbol{C}$，解密服务器 i 的解密份额 θ_i，以及验证密钥 $TVK_{id,i}$，验证 θ_i 是否为有效的解密份额，如果无效，则算法输出“$\perp$”. 否则，验证通过.

⑦ 联合算法 *Combine*. 输入至少 t 个解密份额 $\{\theta_i,C\}$，$i\in S$，$S\in\{1,2,\cdots,N\}$，$|S|\geqslant t$. 首先检测 θ_i 的有效性，如果无效，返回“$\perp$”. 否则联合 t 个有效解密份额，输出解密结果 M.

定义 7. IBTD 方案的 IND-sID-CPA(Indistinguishability of ciphertexts under a selective-identity chosen-plaintext attack)安全性. 其是根据攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏定义的.

初始化. 攻击者 $\mathcal{A}$ 输出准备要攻击的身份 id^* 和一个腐化的解密服务器集合 $S\in\{1,2,\cdots,t-1\}$.

设置. 挑战者 $\mathcal{C}$ 运算 Setup(λ)，将获取的公开参数给攻击者，自己保留系统主私钥.

第 1 阶段询问：

① 私钥询问，攻击者 $\mathcal{A}$ 询问身份 $id(id\neq id^*)$ 所对于的私钥 S_{id}，挑战者 $\mathcal{C}$ 运行 KeyGen 算法并将结果 S_{id} 返回给 $\mathcal{A}$.

② 私钥份额询问，当被询问用户 id 的第 i 个解密份额时，$\mathcal{C}$ 运行 $ShareKeyGen(id,S_{id},N,t)$ 算法

获取私钥份额 $TSK_{id,i}(1\leqslant i\leqslant N)$,和相应的门限验证密钥 $TVK_{id,i}$,如果$(id\neq id^*)$或者$(id=id^*, i\in S)$,那么挑战者返回相应份额给攻击者,否则输出"⊥".

挑战阶段. 攻击者 $\mathcal{A}$ 输出 2 个等长的消息 $M_0, M_1(M_0\neq M_1)$,挑战者随机选择一个 $b\in\{0,1\}$,并计算挑战密文 $\boldsymbol{C}^*=Encrypt(id,M_b)$,将其发送给 $\mathcal{A}$.

第 2 阶段询问. 与第 1 阶段相同.

猜测. 攻击者 $\mathcal{A}$ 给出一个对 b 值的猜测 $b'\in\{0,1\}$,如果 $b'=b$ 那么攻击者获胜.

攻击者 $\mathcal{A}$ 在上述游戏中的优势为

$$Adv_{\mathcal{A}}^{\text{IND-sID-CPA}}(t,N,id^*)=\left|Pr[b=b']-\frac{1}{2}\right|.$$

定义 8. 解密一致性. 其游戏中定义的初始化、设置和询问步骤与定义 7 中的相同,攻击者输出 2 组解密份额 $S=\{\theta_1,\theta_2,\cdots,\theta_t\}$ 和 $S'=\{\theta'_1,\theta'_2,\cdots,\theta'_t\}$. 如果 3 个条件成立,攻击者获胜:

① S 和 S' 在身份 id^* 和 TVK_{id^*} 下都是合法份额;

② S 和 S' 中解密份额来自 t 个不同解密服务器;

③ $Combine(TVK_{id^*}, id^*, S, \boldsymbol{C})\neq Combine(TVK_{id^*}, id^*, S', \boldsymbol{C})$;

攻击者 $\mathcal{A}$ 在上述解密一致性游戏中的优势定义为 $Adv_{\mathcal{A},k,N}^{\text{CD-ID}}(\mathcal{A})$.

定义 9. 如果一个 IBTD 方案是 IND-sID-CPA 安全的,那么对于任意的 N, t $(0<t\leqslant N)$,$Adv_{\mathcal{A}}^{\text{IND-sID-CPA}}(k,N,id^*)$ 和 $Adv_{\mathcal{A},k,N}^{\text{CD-ID}}(\mathcal{A})$ 都是可以忽略的.

3 方案描述

1) 系统设置 $Setup(\lambda)$

输入安全参数 λ,设置 $n\in\mathbb{Z}$,$q=\text{ploy}(n)$,$m=O(n\log q)$.

① 根据 $TrapGen$ 算法,PKG 生成随机均匀分布的矩阵 $\boldsymbol{A}_0\in\mathbb{Z}_q^{n\times m}$ 和陷门 $\boldsymbol{T}_{\boldsymbol{A}_0}\in\mathbb{Z}_q^{m\times m}$;

② 选择 2 个均匀分布的矩阵 $\boldsymbol{A}_1\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$,选择一个均匀分布的向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$;

③ 选择身份编码函数 $H:\mathbb{Z}_q^n\to\mathbb{Z}_q^{n\times n}$;

④ 定义映射函数 $\varphi:\{0,1\}^{m+1}\times\{0,1\}^*\to\mathbb{Z}_q$,其输入为密文 $\boldsymbol{C}$ 和密钥 K_A,其输出为$[-\sqrt{q},\sqrt{q}]$之间的随机值.

⑤ 选择一个素数 p 使得离散对数问题在以 g 为生成元的循环群 $\mathbb{Z}_p$ 上是困难的.

公开系统主要参数 $pp=(\boldsymbol{A}_0,\boldsymbol{A}_1,\boldsymbol{B},\boldsymbol{u},H,\varphi,g)$,保留主密钥 $msk=\boldsymbol{T}_{\boldsymbol{A}_0}\in\mathbb{Z}_q^{m\times m}$.

2) 私钥提取 $Extract(msk,pp,id)$

输入用户 $id\in\mathbb{Z}_q^n$ 和系统主密钥 $\boldsymbol{T}_{\boldsymbol{A}_0}$,利用身份编码函数计算 $H(id)\in\mathbb{Z}_q^{n\times n}$,则 id 对应公钥为 $\boldsymbol{F}_{id}=(\boldsymbol{A}_0\mid\boldsymbol{A}_1+H(id)\boldsymbol{B})$. 使用左基采样算法 SampleBasisLeft$(\boldsymbol{A}_0,\boldsymbol{A}_1+H(id)\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{A}_0},\sigma)$计算 $\boldsymbol{F}_{id}$ 对应的陷门 $\boldsymbol{T}_{id}\in\mathbb{Z}_q^{2m\times 2m}$,满足 $\boldsymbol{F}_{id}\cdot\boldsymbol{T}_{id}=\boldsymbol{0}$,且 $\boldsymbol{T}_{id}$ 服从噪声分布 $\psi_\sigma^{2m\times 2m}$.

返回私钥 $\boldsymbol{T}_{id}$ 给用户 id.

3) 私钥分割算法 $DisKey(id,\boldsymbol{T}_{id},N,t)$

给定解密服务器数量 N、门限值 t 和公共参数 pp,标记 $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)\in\mathbb{Z}_q^n$.

① 随机选择 n 个多项式 $l_i(x)\leftarrow\mathbb{Z}_q[x]$ $(1\leqslant i\leqslant n)$ 满足最高次数等于 $t-1$ 且 $l_i(0)=u_i$. 对于 $1\leqslant i\leqslant N$,第 i 个解密服务器的特征向量为 $\boldsymbol{u}_{id,i}=(l_1(i),l_2(i),\cdots,l_n(i))$.

② 对于 $1\leqslant i\leqslant N$,利用陷门 $\boldsymbol{T}_{id}$,采用 $SamplePre(\boldsymbol{F}_{id},\boldsymbol{T}_{id},\boldsymbol{u}_{id,i},2\sigma)$算法抽取出 $\boldsymbol{e}_{id,i}\in\mathbb{Z}_q^{2m}$,满足 $\boldsymbol{F}_{id}\cdot\boldsymbol{e}_{id,i}=\boldsymbol{u}_{id,i}$,那么第 i 个服务器拥有的用户 id 部分私钥份额为 $TSK_{id,i}=\boldsymbol{e}_{id,i}$,并将其表示为向量 $\boldsymbol{e}_{id,i}=(\boldsymbol{e}_{id,i,1},\boldsymbol{e}_{id,i,2},\cdots,\boldsymbol{e}_{id,i,2m})$,验证份额为 $TVK_{id,i}=(g^{\boldsymbol{e}_{id,i,1}},g^{\boldsymbol{e}_{id,i,2}},\cdots,g^{\boldsymbol{e}_{id,i,2m}})$.

所有解密服务器对于用户 id 的门限验证密钥为 $TVK_{id}=(TVK_{id,1},TVK_{id,2},\cdots,TVK_{id,N})$,其可以公开.

③ 对于任意一个解密服务器 $i\in N$,在除去 i 的所有 $N-1$ 个服务器中,选择 t 个服务器组成一个群,使用 A 表示其群号,并选择一个随机整数 K_A 分发给此群中的所有解密服务器,那么每一个服务器将获得 C_{N-1}^t 个随机整数.

第 i 个解密服务器的私钥份额为 $TSK_{id,i}=(\boldsymbol{e}_{id,i},C_{N-1}^t$个随机整数$)$,将其通过保密信道发送给第 i 个解密服务器.

4) 加密算法 Enc(id,M)

① 计算 id 的公钥 $\boldsymbol{F}_{id}=(\boldsymbol{A}_0\mid\boldsymbol{A}_1+H(id)\boldsymbol{B})$;

② 随机选择均匀分布的 $\boldsymbol{s}\in\mathbb{Z}_q^n$;

③ 选择均匀分布的矩阵 $\boldsymbol{R}\in\mathbb{Z}_q^{m\times m}$,其系数随机取自$\{-1,1\}$;随机选取噪声分布 $x\in\psi_s$ 和噪声 $\boldsymbol{y}\in\psi_s^m$,计算 $\boldsymbol{z}=\boldsymbol{R}^{\mathrm{T}}\boldsymbol{y}\in\psi_s^m$.

④ 待加密消息 $M\in\{0,1\}$,计算密文 $\boldsymbol{c}_1=\boldsymbol{F}_{id}^{\mathrm{T}}\boldsymbol{s}+(\boldsymbol{y}\mid\boldsymbol{z})\in\mathbb{Z}_q^{2m}$ 和 $\boldsymbol{c}_2=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+M\lfloor q/2\rfloor\in\mathbb{Z}_q$,输出密文 $\boldsymbol{C}=(\boldsymbol{c}_1,\boldsymbol{c}_2)\in\mathbb{Z}_q^{2m}\times\mathbb{Z}_q$.

5) 部分解密算法 $SubDec(TSK_{id,i},\boldsymbol{C}=(\boldsymbol{c}_1,\boldsymbol{c}_2))$

利用私钥份额 $TSK_{id,i}$,计算出密文 $\boldsymbol{C}$ 所对应的解密份额,过程如下.

① 遍历 $TSK_{id,i}$ 得到 $TSK_{id,i}=(\boldsymbol{e}_{id,i},\mathrm{C}_{N-1}^{t}$ 个整数);

② 计算 $d_i=\boldsymbol{c}_2-\boldsymbol{c}_1^{\mathrm{T}}\boldsymbol{e}_{id,i}$;

③ 对于 C_{N-1}^{t} 个整数中的每一个,标记为 $K_{A,j}$ $(1\leqslant j\leqslant \mathrm{C}_{N-1}^{t})$,计算 $x_{i,j}=\varphi_{K_{A,j}}(\boldsymbol{c}_1,\boldsymbol{c}_2)$;并对所有的计算结果求和 $x_i=\sum_{j=1}^{\mathrm{C}_{N-1}^{t}}x_{i,j}$.

④ 第 i 个解密服务器的部分解密份额为 $M_i=d_i+x_i$. 第 i 个解密服务器解密份额为 $\theta_i=(M_i,g^{x_i})$.

6) 份额验证算法 $ShareVery(TVK_{id,i},\theta_i,\boldsymbol{C})$

利用验证密钥 $TVK_{id,i}$,验证解密份额 θ_i 是否为密文 $\boldsymbol{C}$ 的合法解密份额.

① 第 1 部分密文 $\boldsymbol{c}_1=(c_{1,1},c_{1,2},\cdots,c_{1,2m})$,$TVK_{id,i}=(g^{\boldsymbol{e}_{id,i,1}},g^{\boldsymbol{e}_{id,i,2}},\cdots,g^{\boldsymbol{e}_{id,i,2m}})$,遍历 θ_i 得到 $\theta_i=(M_i,g^{x_i})$.

② 验证 $g^{M_i}=g^{x_i}\cdot g^{\boldsymbol{c}_2}\cdot\prod_{j=1}^{2m}(g^{\boldsymbol{e}_{id,i,j}})^{-c_{1,j}}$,如果等式验证失败,返回"⊥",否则通过验证.

7) 组合算法 $Combine(TVK_{id},\boldsymbol{C},\theta_1,\theta_2,\cdots,\theta_t)$

t 个解密服务器,构成集合 S,他们的解密份额分别为 $\theta_1,\theta_2,\cdots,\theta_t$,利用这些份额可以恢复出密文 $\boldsymbol{C}$ 所对于的明文信息,过程如下.

① 对于每一个解密份额 θ_i $(1\leqslant i\leqslant t)$,如果 $ShareVery(TVK_{id,i},\theta_i,\boldsymbol{C})$ 验证失败,输出"⊥",并退出.

② 遍历 $\theta_i(i\in S)$ 得到 $\theta_i=(M_i,g^{x_i})$,采用拉格朗日插值公式,以解密服务器的编号作为 x 值,以解密份额 M_i 作为 y 的值. 计算拉格朗日系数为

$$\lambda_i=\prod_{j\in[1,N],i\neq j}\frac{-i}{i-j}.$$

计算解密结果 $M'=\sum_{i\in S}\lambda_iM_i+\boldsymbol{c}_2\left(1-\sum_{i\in S}\lambda_i\right)$,如果 $M'\in(\lfloor q/4\rfloor,\lfloor 3q/4\rfloor]$,那么 $M'=1$,否则 $M'=0$.

输出消息 M'.

4 方案分析

4.1 正确性

定理 3. 对于任意的实数 $s>0,T>0$ 和 $\boldsymbol{x}\in\mathbb{R}^n$,有 $Pr[|\langle\boldsymbol{x},\mathcal{D}_{\mathbb{Z}^n,s}\rangle|>Ts\|\boldsymbol{x}\|]\leqslant 2\exp(-\pi T^2)$.

定理 4. 选择合适的参数,在新的 IBTD 方案中,解密份额能够通过验证,且解密算法能够正确还原出消息.

证明.

1) 验证算法的正确性.

$$g^{x_i}\cdot g^{\boldsymbol{c}_2}\cdot\prod_{j=1}^{2m}(g^{\boldsymbol{e}_{id,i,j}})^{-c_{1,j}}=g^{x_i}\cdot g^{\boldsymbol{c}_2}\cdot g^{\sum_{j=1}^{2m}(-\boldsymbol{e}_{id,i,j}\cdot c_{1,j})}=g^{x_i+\boldsymbol{c}_2+\boldsymbol{c}_1^{\mathrm{T}}\boldsymbol{e}_{id,i}}=g^{x_i+d_i}=g^{M_i}.$$

2) 解密结果的正确性.

来自服务器 i 的部分解密份额为 $M_i=d_i+x_i$. 根据解密份额合成算法,在获取 t 个这样的份额后,根据拉格朗日运算的同态性质,计算

$$M'=\sum_{i\in S}\lambda_iM_i+\boldsymbol{c}_2\left(1-\sum_{i\in S}\lambda_i\right)=\sum_{i=1}^{k}\lambda_i(d_i+x_i)+\boldsymbol{c}_2\left(1-\sum_{i=1}^{k}\lambda_i\right)=\sum_{k=1}^{t}\lambda_i(\boldsymbol{c}_2-\boldsymbol{e}_{id,i}^{\mathrm{T}}\boldsymbol{c}_1+x_i)+\boldsymbol{c}_2\left(1-\sum_{k=1}^{t}\lambda_i\right)=$$

$$-\sum_{k=1}^{t}\lambda_i\boldsymbol{e}_{id,i}^{\mathrm{T}}\boldsymbol{c}_1+\sum_{k=1}^{t}\lambda_ix_i+\boldsymbol{c}_2=-\sum_{k=1}^{t}\lambda_i(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{F}_{id}^{\mathrm{T}}\boldsymbol{s}+(\boldsymbol{y}\mid\boldsymbol{z}))+\sum_{i=1}^{t}\lambda_ix_i+\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+M\lfloor q/2\rfloor=$$

$$x+\sum_{k=1}^{t}\lambda_i(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{y}\mid\boldsymbol{z})+\sum_{i=1}^{t}\lambda_ix_i+M\lfloor q/2\rfloor.$$

要解密正确,只需要

$$noise=x+\sum_{k=1}^{t}\lambda_i(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{y}\mid\boldsymbol{z})+\sum_{i=1}^{t}\lambda_ix_i\leqslant\lfloor q/4\rfloor.$$

$noise$ 可以分为 3 部分,第 1 部分是 x,其满足 $x\in\psi_s$,即服从参数为 $\boldsymbol{s}$ 的高斯分布. 第 2 部分是 $\sum_{k=1}^{t}\lambda_i(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{y}\mid\boldsymbol{z})$. 其中 $(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{y}|\boldsymbol{z})$,表示 2 个长度为 $2m$ 向量的内积,而 2 组向量中的每一个分量分别服从参数为 2σ 和参数为 $\boldsymbol{s}$ 的高斯分布. 利用定理 3,可求出其上界.

设 $\boldsymbol{e}_{id,i}=(\boldsymbol{e}_1,\boldsymbol{e}_2)$,那么 $\|\boldsymbol{e}_{id,i}\|\leqslant 2\sigma\sqrt{2m}$,$\|\boldsymbol{e}_1-\boldsymbol{R}\boldsymbol{e}_2\|\leqslant\|\boldsymbol{e}_1\|+\|\boldsymbol{R}\boldsymbol{e}_2\|\leqslant O(\sigma m)$,$\boldsymbol{z}=\boldsymbol{R}^{\mathrm{T}}\boldsymbol{y}$,因此 $\|(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{y}|\boldsymbol{z})\|\leqslant\|(\boldsymbol{e}_1-\boldsymbol{R}\boldsymbol{e}_2)^{\mathrm{T}}\boldsymbol{y}\|\leqslant O(\sigma m^{3/2})$.

$\sum_{k=1}^{t}\lambda_i(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{y}\mid\boldsymbol{z})$ 可以看成是拉格朗日函数 $h(x)$ 的所对应的秘密,其采用解密服务器编号为 x 坐标,$(\boldsymbol{e}_{id,i})^{\mathrm{T}}(\boldsymbol{y}|\boldsymbol{z})$ 为 y 坐标,容易证明 $h(0)$ 的值不超过 $t(\sigma m^{3/2})$.

对于第3部分,这里是拉格朗日函数 $f(x)$ 的结果,其采用解密服务器编号为 x 坐标,x_i 为 y 坐标,可以证明 $f(0)$ 的值不超过 $x_1+x_2+\cdots+x_t$,$x_i=\varphi_{K_A}(\boldsymbol{C})$,其值在$[-\sqrt{q},\sqrt{q}]$之间,因此,第3部分的上限为 $C_{N-1}^{t}t\sqrt{q}$.

要解密正确,只需要 *noise* 的3部分之和不超过 $\lfloor q/4\rfloor$,实际上第一个部分非常小,通常可忽略,因此只需要 $t(\sigma m^{3/2})+C_{N-1}^{t}t\sqrt{q}\leqslant\lfloor q/4\rfloor$. 通过设置适当参数,方案能够正确解密.

4.2 安全性证明

先介绍安全性证明过程中需要使用的引理2和定理5.

引理2. 假设 $mn>(n+1)\log q+\omega(\log n)$,其中 q 是一个素数,矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$\boldsymbol{B}$ 是一个 $m\times m$ 方阵,其值随机取自$\{-1,1\}$,那么$(\boldsymbol{A},\boldsymbol{AR})$的分布在统计上与分布$(\boldsymbol{A},\boldsymbol{B})$不可区分.

定理5. 在二维平面上给定 t 个点(x_1,y_1),(x_2,y_2),…,(x_t,y_t),其中 x_i 的值各不相同,那么存在且唯一存在最高次数为 $t-1$ 的多项式 f,对于所有的点$(x_i,y_i)(1\leqslant i\leqslant t)$,满足 $f(x_i)=y_i$.

定理6. 安全性. 如果LWE问题是困难的,那么上述基于格的IBTD方案可以满足IND-sID-CPA安全性.

证明. 证明过程分2步:证明密文满足语义安全和证明解密一致性.

语义安全性证明. 先构造一系列游戏,第一个游戏是真实的IND-sID-CPA攻击,而最后一个游戏是攻击者无法获胜的;然后基于一些格上的困难性假设,证明相邻游戏之间在多项式时间内不可区分.

Game0. 攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间真实的IND-sID-CPA游戏,设攻击者 $\mathcal{A}$ 输出准备要攻击的身份 id^* 和一个已经腐化的解密服务器集合 $S\in\{1,2,\cdots,t-1\}$. 挑战者运算 *Setup* 算法,将获取的公开参数给攻击者 $\mathcal{A}$,自己保留系统主私钥 *msk*. 且如下回答攻击者的询问.

1) 私钥询问,攻击者 $\mathcal{A}$ 询问身份 $id(id\neq id^*)$ 所对应的私钥 $\boldsymbol{T}_{id}$,挑战者运行 *KeyGen* 算法并将结果 $\boldsymbol{T}_{id}$ 返回给挑战者.

2) 私钥份额询问,当被询问用户 id 的第 i 个解密份额时,挑战者运行 $ShareKeyGen(id,\boldsymbol{T}_{id},N,t)$ 算法获取门限份额密钥 $TSK_{id,i}(1\leqslant i\leqslant N)$,和相应的门限验证密钥 $TVK_{id,i}(1\leqslant i\leqslant N)$,如果$(id\neq id^*)$或者$(id=id^*,i\in S)$,那么挑战者返回相应的份额给攻击者,否则输出"⊥".

Game1. 在Game0中,挑战者公开的系统参数 $\boldsymbol{A}_1$ 取自均匀分布,Game1中环多项式 $\boldsymbol{A}_1$ 不再是随机选取,而是通过 $\boldsymbol{A}_1=\boldsymbol{A}_0\boldsymbol{R}^*-H(id^*)\boldsymbol{B}$ 计算得到,$\boldsymbol{R}^*$ 为加密阶段选取的随机向量,其余参数的选取与Game0相同.

Game0到Game1:对多项式时间内的攻击者 $\mathcal{A}$ 而言,Game0和Game1概率不可区分,使用引理2可以证明.

Game2. 对Game1中参数进行如下修改,$\boldsymbol{A}_0$ 在 $\mathbb{Z}_q$ 上随机均匀选取,不含陷门. 利用陷门函数产生含有陷门 $\boldsymbol{T}_{\boldsymbol{B}}$ 的 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$,那么,用户 id 对应的身份矩阵为 $\boldsymbol{F}_{id}=(\boldsymbol{A}_0\,|\,\boldsymbol{A}_0\boldsymbol{R}^*+(H(id)-H(id^*))\boldsymbol{B})$. 挑战者拥有的系统主密钥为 $\boldsymbol{T}_{\boldsymbol{B}}$. 其在挑战阶段如此回答询问.

1) 私钥询问,攻击者询问身份 $id(id\neq id^*)$ 所对应的私钥 $\boldsymbol{T}_{id}$,挑战者运行右采样基算法 $\boldsymbol{T}_{id}\leftarrow SampleBasisRight(\boldsymbol{A}_0,\boldsymbol{B},\boldsymbol{R}^*,\boldsymbol{T}_{\boldsymbol{B}},2\sigma)$(具体算法参见文献[16]),将结果 $\boldsymbol{T}_{id}$ 返回给挑战者.

2) 私钥份额询问,当被询问用户 id 的第 i 个解密份额时,如果 $id\neq id^*$,挑战者首先通过私钥询问获取 $\boldsymbol{T}_{id}$,之后运行 $ShareKeyGen(id,\boldsymbol{T}_{id},N,t)$ 算法获取门限份额密钥 $TSK_{id,i}(1\leqslant i\leqslant N)$,和相应的门限验证密钥 $TVK_{id,i}(1\leqslant i\leqslant N)$,那么挑战者返回相应的份额给攻击者. 如果 $id=id^*$,$i\in S$,挑战者随机选择长度为 $2m$ 的向量 $\boldsymbol{e}_{id,i}\in\psi_{2\sigma}^{2m}$,返回给挑战者. 其余情况输出"⊥".

Game1到Game2:从攻击者 $\mathcal{A}$ 角度来看,私钥份额生成过程是不可见的,$\mathcal{A}$ 获得的私钥 $\boldsymbol{e}_{id,i}$ 在统计上仍然服从分布 $\mathcal{D}_{\boldsymbol{\Sigma}^{2m},2\sigma}$,且满足 $\boldsymbol{F}_{id}\cdot\boldsymbol{e}_{id,i}=\boldsymbol{u}_{id,i}$. 所以攻击者 $\mathcal{A}$ 在Game1中得到的优势与Game2中的优势相当.

Game3. 挑战密文为随机选取且互相独立的向量 $\boldsymbol{C}=(\boldsymbol{c}_1,\boldsymbol{c}_2)\in U(\mathbb{Z}_q^{2m}\times\mathbb{Z}_q)$,其余设置与Game2中相同.

Game2到Game3:假设攻击者 $\mathcal{A}$ 有不可忽略的优势来区分Game2和Game3,那么可以如下构造仿真者 $\mathcal{S}$ 来解决判定性LWE问题.

假设存在一个LWE采样预言机 $\mathcal{O}$,其随机从 $\mathcal{O}_\$$ 或 $\mathcal{O}_s$ 中选取一些采样作为输出,仿真者 $\mathcal{S}$ 通过与攻击者 $\mathcal{A}$ 进行交互后判断这些采样取自 $\mathcal{O}_s$ 或 $\mathcal{O}_\$$.

实例化:$\mathcal{C}$ 向预言机 $\mathcal{O}$ 询问并接收 $m+1$ 个LWE采样,标记为$\{(\boldsymbol{w}_1,v_1),(\boldsymbol{w}_2,v_2),\cdots,(\boldsymbol{w}_{m+1},v_{m+1})\}$.

攻击目标:设攻击者 $\mathcal{A}$ 输出准备要攻击的身份 id^* 和一个已经腐化的解密服务器的集合 $S\in\{1,2,\cdots,t-1\}$.

$\mathcal{S}$构造如下系统参数：

1) $\boldsymbol{A}_0=(\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_m)^{\mathrm{T}}$；

2) $\boldsymbol{u}=(\boldsymbol{w}_{m+1})$；

3) 其余系统参数设置与 Game2 中相同.

第 1 阶段询问. 与 Game2 中定义的询问相同.

挑战. 当攻击者 $\mathcal{A}$ 给仿真者 $\mathcal{S}$ 发送加密消息 $M\in\{0,1\}$时，仿真者 $\mathcal{S}$ 如下构造挑战密文：

1) 设 $\boldsymbol{c}_1'=(v_1,v_2,\cdots,v_m)^{\mathrm{T}}$，$\boldsymbol{c}_1''=\boldsymbol{c}'\cdot\boldsymbol{R}^*$，$\boldsymbol{c}_1=(\boldsymbol{c}_1'|\boldsymbol{c}_1'')$；

2) $\boldsymbol{c}_2=(v_{m+1})+M\lfloor q/2\rfloor$；

3) 仿真者 $\mathcal{S}$ 从$\{0,1\}$中随机选取 β，如果 $\beta=0$，密文 $\boldsymbol{C}^*=(\boldsymbol{c}_1,\boldsymbol{c}_2)\in\mathbb{Z}_q^{2m}\times\mathbb{Z}_q$构造方法如上，否则随机选取均匀分布的矩阵 $\boldsymbol{C}^*\in U(\mathbb{Z}_q^{2m}\times\mathbb{Z}_q)$，将 $\boldsymbol{C}^*$ 发送给攻击者 $\mathcal{A}$.

第 2 阶段询问. 和第 1 阶段询问一样，带有一些限制.

猜测. 询问过后，攻击者 $\mathcal{A}$ 给出一个猜想 $\beta'\in\{0,1\}$，这里 $\beta'=1$ 意味着攻击者 $\mathcal{A}$ 正在与 Game2 交互，仿真者 $\mathcal{S}$ 回答 LWE 挑战的猜测 $\delta'=\beta'$，这里 $\delta'=1$ 意味着上述实例 $(\boldsymbol{w}_i,v_i)(1\leqslant i\leqslant m+1)$ 服从 LWE 分布，否则 $\delta'=0$ 表示实例服从随机均匀分布.

如果实例化过程中预言机 $\mathcal{O}$ 输出的分布来自 $\mathcal{O}_s$，那么密文 $\boldsymbol{C}^*$ 的分布与 Game2 中分布相同. 原因如下：第一，$\boldsymbol{F}_{id^*}=(\boldsymbol{A}_0|\boldsymbol{A}_0\boldsymbol{R}^*)$；第二，令 $\boldsymbol{c}_1'=\boldsymbol{A}_0^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e}_x$，那么密文第 1 部分 $\boldsymbol{c}_1^*=(\hat{\boldsymbol{c}}_1'|\boldsymbol{R}^{*\mathrm{T}}\cdot\boldsymbol{c}_1')=\boldsymbol{F}_{id}^{\mathrm{T}}\boldsymbol{s}+(\boldsymbol{e}_x|\boldsymbol{R}^{*\mathrm{T}}\boldsymbol{e}_x)$；第 2 部分 $\boldsymbol{c}_2^*=v_{m+1}+M\lfloor q/2\rfloor=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}+x+M\lfloor q/2\rfloor$，这 2 部分都与 Game2 中挑战密文的分布相同.

如果实例化过程中预言机 $\mathcal{O}$ 输出的分布来自 $\mathcal{O}_\$$，那么根据引理 2，$\boldsymbol{c}_1''=\boldsymbol{R}^{*\mathrm{T}}\cdot\boldsymbol{c}_1'$ 也是服从均匀分布的，所以整个密文在统计上仍服从随机均匀分布，而在 Game3 中，密文 $\boldsymbol{C}=(\boldsymbol{c}_1,\boldsymbol{c}_2)\in\mathbb{Z}_q^{2m}\times\mathbb{Z}_q$取于随机均匀分布.

以上完成了对仿真者 $\mathcal{S}$ 的描述，可以看出如果 $\mathcal{A}$ 能够以不可忽略的优势区分 Game2 和 Game3，那么仿真者 $\mathcal{S}$ 能够以绝对的优势解决判定性 LWE 问题.

通过以上 4 个等价游戏，将方案的安全性归约为判定性 LWE 困难假设. 根据定理 1，方案达到了语义安全.

解密一致性证明. 利用反证法证明方案的解密一致性. 假设攻击者 $\mathcal{A}$ 找到 2 组解密份额 $S=\{\theta_1,\theta_2,\cdots,\theta_k\}$和 $S'=\{\theta_1',\theta_2',\cdots,\theta_k'\}$，他们在身份 id^* 和 TVK_{id^*} 下都是合法的份额，且来自 t 个不同解密服务器，那就意味着在拉格朗日插值计算过程中，他们的序号即 x 坐标是相同的，但是 y 坐标是不同的，最终重构出 2 个不同的多项式(常数项一定是不同的).

这就与定理 5 产生了矛盾.

因此，$Adv_{\mathcal{A},k,N}^{\mathrm{CD\text{-}ID}}(\Lambda)=0$，上述方案是满足解密一致性的，因此方案满足 IND-sID-CPA 安全. 证毕.

4.3 效率比较

目前，基于格上困难问题构造的门限解密方案主要有文献[13,15]，这 2 个方案都是基于 LWE 困难问题构造的，且都满足非交互性，但是从构造方法、安全性和效率方面有所差异. 将这些类似方案进行比较，具体如表 1 所示. 可公开验证性是指解密份额是否满足可公开验证性；密钥份额是指每个解密服务器获得的密钥份额，其长度单位为 $\log q$ 位，密文长度是指加密 1 位明文后生成的密文长度，单位为 $\log q$ 位；计算量中的乘法运算指的是 $\mathbb{Z}_q$ 上 2 个整数相乘，采用 Mul 表示；指数运算是指离散对数群上生成元的指数计算，采用 Exp 表示. Hash 表示一次 Hash 运算，Sign 表示一次签名运算.

Table 1 The Comparison to Related Works

表 1 相关工作比较

Schemes	Security Model	Security Level	Publicly Verifiable	Partition Object and Its Distribution	Length of Key Share	Length of Ciphertext	Encryption Calculations	Decryption Calculations	Share Verification Calculations
Ref[13]	Random Oracle	IND-sID-CPA	Yes	User's private key/ Gaussian distribution	n	$m+1$	$(n+1)n\times$ Mul$+1\times$ Sign	$n\times$Mul$+$ $C_{N-1}'\times$Hash $+1\times$Exp	$(n+1)\times$ $1\times$Exp$+$ $(n+1)\times$Mul
Ref[15]	Random Oracle	IND-sID-CCA	No	User's private key and noise/Gaussian distribution	$m+n$	$n+1$	$(m+1)n\times$ Mul	$n\times$Mul	0
Our Scheme	Standard	IND-sID-CPA	Yes	Public vector/ Uniform distribution	$2m$	$2m+1$	$(2m+1)n\times$ Mul	$2m\times$Mul$+$ $C_{N-1}'\times$Hash $+1\times$Exp	$(2m+1)\times$Exp $+(2m+1)\times$ Mul

5 总 结

本文利用格上陷门产生函数、左右采样基、Shamir 秘密分享等技术构造了一种 IND-sID-CPA 安全的 IBTD 方案,并基于离散对数困难问题来实现可公开验证性.同现存格上基于身份的门限加密方案相比,本文是对满足均匀分布的向量进行分割,通过私钥份额和解密份额之间的同态性来保证方案的正确性,同时方案的证明过程在标准模型下完成.

参 考 文 献

[1] Shamir A. How to share a secret [J]. Communications of the ACM, 2011, 22(22): 612-613

[2] Blakley G R. Safeguarding cryptographic keys [C] //Proc of Int Workshop on Managing Requirements Knowledge (AFIPS). Piscataway, NJ: IEEE, 1979: 313-317

[3] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [C] //Proc of the Annual Int Cryptology Conf. Berlin: Springer, 2001: 213-229

[4] Boneh D, Boyen X, Halevi S. Chosen ciphertext secure public key threshold encryption without random oracles [C] //Proc of the Cryptographers' Track at the RSA Conf. Berlin: Springer, 2006: 226-243

[5] Baek J, Zheng Yuliang. Identity-based threshold decryption [C] //Proc of the Int Workshop on Public Key Cryptography. Berlin: Springer, 2004: 262-276

[6] Chai Zhenchuan, Cao Zhenfu, Lu Rongxing. ID-based threshold decryption without random oracles and its application in key escrow [C] //Proc of the Int Conf on Information Security. New York: ACM, 2004: 119-124

[7] Libert B, Quisquater J J. Efficient revocation and threshold pairing based cryptosystems [C] //Proc of the 22nd Annual Symp on Principles of Distributed Computing. New York: ACM, 2003: 163-171

[8] Zhang Pingyuan, Jiang Han, Cai Jie, et al. Recent advances in lattice-based cryptography [J]. Journal of Computer Research and Development, 2017, 54(10): 2121-2129 (in Chinese)
(张平原, 蒋瀚, 蔡杰, 等. 格密码技术近期研究进展[J]. 计算机研究与发展, 2017, 54(10): 2121-2129)

[9] Bendlin R, Damgård I. Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2010: 201-218

[10] Regev O. On lattices, learning with errors, random linear codes, and cryptography [C] //Proc of the 37th Annual ACM Symp on Theory of Computing. New York: ACM, 2005: 84-93

[11] Xie Xiang, Xue Rui, Zhang Rui. Efficient threshold encryption from lossy trapdoor functions [C] //Proc of the 4th Int Workshop on Post-Quantum Cryptography. Berlin: Springer, 2011: 163-178

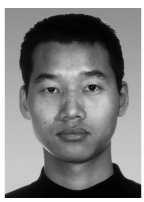
[12] Singh K, Rangan C P, Banerjee A K. Lattice based efficient threshold public key encryption scheme [J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2013, 4(4): 93-107

[13] Singh K, Rangan C P, Banerjee A K. Lattice-based identity-based resplittable threshold public key encryption scheme [J]. International Journal of Computer Mathematics, 2016, 93(2): 289-307

[14] Agrawal S, Boyen X, Vaikuntanathan V, et al. Fuzzy identity based encryption from lattices [EB/OL]. [2018-06-10]. http://eprint.iacr.org/2011/414.pdf

[15] Kuchta V, Markowitch O. Identity-based threshold encryption on lattices with application to searchable encryption [C] //Proc of the 6th Int Conf on Applications and Techniques in Information Security. Berlin: Springer, 2016: 117-129

[16] Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model [C] //Proc of the Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 553-572



Wu Liqiang, Born in 1986. MSc, lecturer. His main research interests include cryptosystems based on lattices and provable security theory.

Yang Xiaoyuan, born in 1959. PhD, professor and PhD supervisor. His main research interests include cryptography and network security.

Zhang Minqing, born in 1967. PhD, professor. Her main research interests include network security and information hiding.