Computer Science and Application 计算机科学与应用, 2018, 8(4), 503-511
Published Online April 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.84056

Hans汉斯

Attribute-Based Fully Homomorphic Encryption Based LWR

Xinglan Zhang, Yushun Lu*

Department of Information, Beijing University of Technology, Beijing
Email: *lu_hbnd@163.com

Received: Apr. 4th, 2018; accepted: Apr. 21st, 2018; published: Apr. 28th, 2018

Abstract

For the current fully-homomorphic encryption scheme based on LWE (Learn With Errors) structure, Gaussian function sampling and public key size are generally needed. This paper adopts the efficient LWR (Learning With Rounding) to replace the traditional LWE scheme and proposes key-policy-attribute-based full-homomorphic encryption (LWR-ABFHE) scheme for end-to-end data protection in multi-users cloud environments. The LWR-ABFHE scheme proposed in this paper can perform homomorphic computing while performing fine-grained access to encrypted data, and achieve the effect of handling monotonic access structures on a set of authorization attributes without sacrificing the computational power of homomorphic encryption. In this paper, the IND-CPA security of the proposed scheme under LWR assumption is proved.

Keywords

LWR, LWE, Attribute-Based Encryption, Fully Homomorphic Encryption, Monotonic Access Structure

一种基于LWR的属性全同态加密方案

张兴兰，卢玉顺*

北京工业大学，信息学部，北京
Email: *lu_hbnd@163.com

收稿日期：2018年4月4日；录用日期：2018年4月21日；发布日期：2018年4月28日

摘　要

针对目前基于LWE (Learn With Errors)构造的全同态加密方案普遍需要高斯函数抽样以及公钥尺寸过

*通讯作者。

文章引用: 张兴兰, 卢玉顺. 一种基于 LWR 的属性全同态加密方案[J]. 计算机科学与应用, 2018, 8(4): 503-511.
DOI: 10.12677/csa.2018.84056

大等问题，本文采用高效的LWR (Learning With Rounding)替换传统的LWE方案，提出了多用户云环境中提供端到端数据保护的基于密钥策略－属性的全同态加密(LWR-ABFHE)方案。本文提出的LWR-ABFHE方案能够在对加密数据进行细粒度访问的同时执行同态计算，并且在不牺牲同态加密的计算能力情况下，达到在一组授权属性上处理单调访问结构的效果。本文在LWR假设下，证明了LWR-ABFHE方案在选择明文攻击下的安全性。

关键词

LWR，LWE，基于属性，全同态加密，单调访问结构

1. 引言

随着互联网的快速发展和云计算的普及，人们对数据隐私越来越重视。针对如何保证用户数据的私密性产生了很多加密方案，其中全同态加密占据主流的研究地位。全同态加密(FHE)是一种特殊的加密方案，可以解决云计算、电子商务等安全问题，因为它允许第三方对加密数据进行任何操作，而无需预先解密。2009 年 Craig Gentry [1]实现了第一个全同态加密(FHE)方案，其允许对加密的密文数据执行任何加法和乘法的功能。

自 Gentry 实现第一个全同态加密方案后，FHE 方案逐渐成为了研究的热点，至今产生了各种相关的实现及优化。当前研究全同态加密的主流方案是基于 LWE 困难问题的安全性假设。因为 LWE 问题理论上可以量子规约到格上的求解 SIVP 困难问题和 GapSVP 困难问题，因此认为基于 LWE 的全同态加密方案具有牢固的安全性保证。2011 年 Brakerski 等[2] [3]提出基于 LWE 问题构造全同态加密方案的思想，方案利用“重线性化”技术实现密文之间的同态运算，但是同态过程需要用到额外的运算公钥 evk，导致密文运算复杂而且效率低下；2012 年 Brakerski 等人[4]基于 LWE 又提出了模不变的全同态方案，省略了模交换技术的消耗，但是该方案在保证安全性的前提下，模数 q 的取值很大，导致了较高的复杂度；2013 年，Gentry [5]在 Crypto 国际会议中提出利用近似特征向量方法构造全同态加密方案。该方案的优势是密文之间乘积不会导致维数的膨胀，消除了秘钥交换技术。但是密文的同态计算由向量转换为矩阵之间的加法和乘法，计算复杂；文献[6] [7]分别提出利用多键和舍弃自举技术等方案在一定程度上改进了全同态方案的效率，但是这些方案基于 LWE 问题都需要高斯噪声抽样，时间开销很大，计算上也存在瓶颈。所以消除高斯噪声带来的高昂实际代价很有必要，Bogdanov [8]和 Costache [9]提出的 LWR 方案是 LWE 问题的变体，安全性与 LWE 问题一样困难，而且 LWR 问题消除了高斯函数抽样，显著提高了计算效率。

为了支持多用户需求，到目前为止所回顾的所有方案都受到这样的事实的影响，即对同态加密方案的引入扩展对计算能力具有负面影响。Xiao 等人方案[10]和 Lopez 方案[11]均通过密钥代理或 CSP 服务器来实现额外的密钥转换过程。同时，Gentry 方案[5]和 Clear-Mc Goldrick 方案[12]能够提供对用户属性进行加密的细粒度控制访问。然而，Gentry 方案[5]和 Clear Mc Goldrick 方案[12]仅允许用相同属性加密的数据执行计算，因此无法支持多用户设置下的同态加密。尽管 Clear-Mc Goldrick 方案[13]能够支持多属性计算，但是它们的方案继承了 Lopez 方案[11]的性能瓶颈。本文提出的方案与现有的工作[5] [11] [12] [13] [14]之间的主要区别是三个方面。首先，利用 LWR 问题构造基于属性的全同态加密方案，不仅消除

了高斯噪声抽样和运算秘钥，而且公钥尺寸更加小，具有更加高效的计算效率。其次，与现有的 ABHE 方案[5] [12] [13] [14]相比，它们仅将其访问结构视为单一属性[5] [12]；或者使用单个属性来表示一组“子属性”[13]；所提出的方案使用 LSSS 矩阵(G，p)在一组属性上表示单调访问结构。最后，所提出的 LWR-ABFHE 方案不是将同态加密和 ABE 方案直接融合成单个密文，而是将密文分解为两个子分量。第一个分量用公钥 PK 对数据进行加密；而第二个组件包含一组授权属性 U。同态评估只涉及第一个组件。同时，第二个组件用于细化加密数据的访问控制。用户的秘密密钥 SK 通过一组授权属性与单调访问结构 A 关联。单调访问结构中的每个授权属性 A_i 都拥有密钥 SK 的有效份额。因此，当且仅当 $A_i \in A$ 时，才能正确解密加密数据。另外，为了防止多个用户之间的共谋攻击，所提出的 LWR-ABFHE 方案扩展了密钥随机化技术[15] [16]，以使用户的秘密密钥失效，其中多个用户不能将他们的属性集中在一起并重建一个有效的密钥。

2. 预备知识

本文中用粗体小写字母表示向量，例如 r；向量的第 i 个分量用 r[i]表示；向量均以列向量形式表示，向量转置用 r^{T} 表示；$\lceil \bullet \rfloor$ 表示向上取整，$\lceil \bullet \rfloor$ 表示四舍五入取整；向量范数 $\|x\|_{\infty}^{can}$ 表示所有向量元素绝对值中的最大值。文中对数 log 默认底是 2，向量加法和乘法运算均在模 q 或者模 p 意义下进行。

2.1. LWE 和 LWR 问题

定义 1. (LWE 问题)选取整数 n 和 $q \geq 2$，对于选定的向量 $\mathbf{s} \in Z_q^n$ 和随机均匀选择的向量 $\mathbf{a} \leftarrow Z_q^n$，输出 $\left(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e\right) \in Z_q^{n+1}$，其中 e 是服从离散高斯分布的噪音向量。LWE 问题的本质就是从上述 LWE 函数生成的独立样本中恢复向量 $\mathbf{s}$。

定理 1. (LWE 问题难解性假设)选取整数 n，$m \leq poly(n)$ 令 $\alpha = \alpha(n) \in (0,1)$ 和素数 $q = q(n)$ 满足条件 $q > \frac{2\sqrt{n}}{\alpha}$。如果存在一个攻击者 A 能够在多项式时间内破解 $\mathrm{LWE}_{n,m,q,\chi}$ 问题，则存在一个以 $O\left(\frac{n}{\alpha}\right)$ 为近似因子的有效算法求解格上的 GapSVP 问题。

定义 2. (LWR 问题)选取整数 n，q 和 p，并且满足 $n \geq 1$ 以及 $q \geq p$，定义 LWR 问题(带舍入学习)如下：对向量 $\mathbf{s} \in Z_q^n$，均匀随机选取 $\mathbf{a} \leftarrow Z_q^n$，输出 $\left(\mathbf{a}, \lceil \langle \mathbf{a}, \mathbf{s} \rangle \rfloor_p\right) \in Z_q^n \times Z_p$。$\mathrm{LWR}_{n,q,p}$ 问题的本质是区分若干抽样 (a_i, b_i) 与等量的均匀抽样 $(c_i, d_i) \in Z_q^n \times Z_p$。

定理 2. 假设χ是任意 Z_q 上 B 有界分布的 LWR 问题取样，而且χ可以有效的取样。令 $B < q/2p$.则对于求解任一分布上 $\mathrm{s} \in Z_q^n$ 的 LWR 问题，我们认为困难程度等价于求解相同分布上 $\mathrm{s} \in Z_q^n$ 的 LWE 问题。

2.2. 访问控制相关概念

定义 3. (单调访问结构)：令 $U = \{u_1, u_2, \cdots, u_n\}$ 表示一组属性。如果对于任意的 B、C 满足条件 $B \in \mathbf{A}$ 并且 $B \subseteq C$，意味着 $C \in \mathbf{A}$，则集合 $\mathbf{A} \subseteq U$ 是单调的。单调访问结构是 $\{u_1, u_2, \cdots, u_n\}$ 的非空子集的单调集合 A。A 中的集合称为授权集合，而不在 A 中的集合称为未授权集合。

一般来说，在 CP-ABE 方案中有三种方法来表示布尔公式，访问树和线性秘密共享方案(LSSS)。在本文中，访问策略是基于 LSSS 方法构建的，因为已经证明 LSSS 能够表达任何单调访问结构[17]。接下来，LSSS 方案定义如下。

定义 4. 线性秘密共享方案(Linear Secret-Sharing Schemes (LSSS))：由访问策略形成的线性秘密共享矩阵的每一行对应一个属性值，即行向量与属性值形成一一映射的关系。如果满足以下两个性质，则在 $U = \{u_1, u_2, \cdots, u_n\}$ 集合上的秘密共享方案Π称为线性的(通过 R_q)：

1) 每个属性的共享秘钥是在 R_q 上形成的一个向量；

2) 存在Π的秘密共享矩阵，表示为矩阵 $G \in R_q^{n\times m}$，其中行标签 $p(i) \in U$，$\forall i \in [n]$，给定一个秘密分享列向量 $\mathbf{v} = (s, r_2, \cdots, r_m)$，其中 $s \in R_q$ 是要共享的秘钥并且随机选择 $r_2, \cdots, r_m \leftarrow R_q$，$Gv$ 表示根据Π的 n 个共享秘钥的向量。共享 $\delta_i = (Gv)_i$，即内积 $G_i \cdot v$ 属于属性 $p(i)$，其中 p 是从 $\{1, \cdots, n\}$ 到 U 的函数。

LSSS 享有如下的线性重构性质[7]。假设Π是一个代表访问机构 **A** 的 LSSS 方案。设 $C \in \mathbf{A}$ 是一个授权的集合，并且 $I \subset \{1, 2, \cdots, n\}$ 被定义为 $I = \{i : p(i) \in C\}$。存在常数 $\{w_i \in R_q\}_{i\in I}$，使得 δ_i 是依据Π的秘钥 SK 的有效分享，那么 $\sum_{i\in I} \delta_i w_i = s$。此外，这些常数 w_i 可以以共享生成矩阵 **G** 的大小在多项式时间内找到。对于任何未授权的集合，不存在这样的常数。在本文中，LSSS 矩阵 (G, p) 将用于表示与用户密钥相关的访问结构。

2.3. 密文策略基于属性的加密(CP-ABE)

定义 5. 基于密文策略属性的加密方案由以下四种算法组成：

$Setup(\lambda, U)$：设置算法将安全参数λ和属性 U 的全局作为输入。它输出公共参数 PP 和主密钥 MSK。

$Encrypt(PP, M, \mathrm{D})$：加密算法采用公共参数 PP，明文消息 M 和包含全部属性的 U 上的访问结构 D 作为输入。该算法对明文消息 M 进行加密并输出密文 CT，使得只有符合条件的用户拥有满足访问结构的一组属性才能够解密该消息。

$KeyGen(MSK, A)$：密钥生成算法使用主密钥 MSK 和描述密钥的一组属性 A。它输出一个对应于属性 A 的私钥 SK。

$Decrypt(PP, CT, SK)$：解密算法采用公开参数 PP，由访问结构 **D** 组成的密文 CT 和属性集合 A 的私钥 SK。如果属性集合 A 满足访问结构 **D** 使得 $A \in \mathbf{D}$，那么算法输出消息 M，否则输出一个解密失败符号 $\perp$。

3. 利用 LWR 构建基于关键策略属性的全同态加密方案

本章节首先构造高效的基于 LWR 的属性全同态加密方案(以下简称 LWR-ABFHE 方案)。在所提出的方案中，访问策略被构建在密文中，并且用户的私钥与一组属性相关联。这随后允许在不知道实际用户数的情况下加密数据。当且仅当其私钥满足加密数据中的访问策略时，新用户才能访问加密数据。接下来，提出的 LWR-ABFHE 方案被正式定义如下。

3.1. LWR-ABFHE 方案构造

本节提出的 LWR-ABFHE 方案由 LWR-ABFHE. Setup (初始化)、LWR-ABFHE. Key Gen (秘钥生成)、LWR-ABFHE.Enc (加密)、LWR-ABFHE. Dec (解密)和 LWR-ABFHE. Evaluate (同态评估)四部分组成。

LWR-ABFHE.Setup$(\lambda, \mathbf{U}, k) \to (PP, MSK)$：设置算法将输入：安全参数$\lambda$，全部属性 $U = \{u_1, u_2, \cdots, u_n\}$ 以及系统中参与计算的用户数量 k。选择一个足够大的素数 q 使得 $q = 1 \bmod (2\lambda)$，以及一个较小的正整数 p，使得 $\gcd(p, q) = 1$。设 $f(x) = (x^d + 1)$，其中 d 是 2 的次幂。令 $R_q = Z_q[x] / \langle f(x) \rangle$ 是整数多项式 $f(x)$ 和 q 模的环。选择一个均匀随机的主密钥 $K_0 \leftarrow R_q$ 和选择 t 个随机元素 $a_t \leftarrow R_q$ (下标 t 表示第 t 个元素)，计算 t 个 $PK_t = \lceil a_t \cdot K_0 \rfloor_p \in R_p$。接下来针对 U 中的每个属性 $\{u_1, u_2, \cdots, u_n\}$，选择一对均匀随机元素 $(K_i, K_i^{-1}) \leftarrow R_q$，其中 K_i^{-1} 是 R_q 下 SK_i 的倒数。计算 $PK_i = \lceil K_i \rfloor_p \in R_p$，最后，输出如下公共参数 PP 和主密钥 MSK。

$$PP = \left\{a, PK_0, \{PK_i\}_{i=1}^n\right\}$$

$$MSK=\left\{K_0,\left\{K_i\right\}_{i=1}^{n},\left\{K_i^{-1}\right\}_{i=1}^{n}\right\}$$

LWR-ABFHE.KeyGen$\left(PP,MSK,D\right)\to\left(SK_D\right)$：秘钥生成算法将公共参数 PP，一个主私钥 MSK 和一个在属性 U 范围内的访问结构 D 作为输入。它首先将访问结构 D 转换成 LSSS 矩阵$\left(G,p\right)$，其中矩阵 $G\in R_q^{n\times m}$，行标签 $p\left(i\right)\in U$，$\forall i\in\left[n\right]$。然后，通过生成一个向量 $\mathbf{v}$ 来分配主密钥 MSK 的有效部分 s，使得 $\mathbf{v}=\left(s,r_2,\cdots,r_m\right)$，其中 $r_2,\cdots,r_m\leftarrow R_q$ 是随机选择的。Gv 表示根据访问结构 D 上线性秘密共享方案Π的秘钥 s 的 n 个份额的向量。$\delta_i=G_i\cdot v\in R_q$，其中 G_i 表示矩阵 G 第 i 行的向量。下一步选择一个均匀随机数α和其对应的倒数 α^{-1} 使得 $\alpha,\alpha^{-1}\leftarrow R_q$。该算法输出与 $\left(G,p\right)$ 的描述相关联的用户的秘密密钥 $SK_D=\left(SK_0,SK_i\right)$，其中：

$$SK_0=K_0\cdot\alpha^{-1}\in R_q$$

$$SK_i=\alpha\cdot K_i^{-1}\cdot\delta_i\in R_q,\forall i\in A$$

LWR-ABFHE.Encrypt$\left(M_1,\cdots,M_t,PP,A\right)\to\left(CT_1,\cdots,CT_t\right)$：加密算法采用主公钥参数 PP，要加密的明文消息 $M\in\left\{0,1\right\}$ 以及一个授权属性集 A 作为输入。选取 t 个均匀随机的数 $r_t\in\left\{0,1\right\}$，令 $\triangle p=\left\lfloor\frac{q_1}{p}\right\rfloor$，其中 q_1 是明文模量，即 $\triangle p=\frac{q_1}{p}-\varepsilon_{q1}$，$0\le\varepsilon_{q1}\le1$，接下来计算密文。输出如下形式的密文 $CT_t=\left(C_t^0,C_t^i\right)$，其中：

$$C_t^0=PK_0\cdot r_t+\triangle p\cdot M_t\in R_p$$

$$C_t^i=a_t\cdot PK_i\cdot r_t\in R_q$$

LWR-ABFHE.Evaluate$\left(PP,F,C_1^0,\cdots,C_t^0\right)\to F\left(C_1^0,\cdots,C_t^0\right)$：同态评估算法采用公开参数 PP，多项式时间计算函数 F 和密文 $C_1^0,\cdots,C_t^0$ 的第一分量作为输入。它在密文空间输出计算结果，使得 $C_t^{0*}=F\left(C_1^0,\cdots,C_t^0\right)$。

LWR-ABFHE.Decrypt$\left(SK_D,C_t^0,C_t^i\right)\to\left(M^*or\perp\right)$：解密算法将密文空间中的计算结果 $C_t^{0*}=F\left(C_1^0,\cdots,C_t^0\right)=F\left(M_1,\cdots,M_t\right)$。利用 LSSS 的线性重构算法计算一组常量，如果等式 $\sum_{i\in I}\delta_i w_i=s$ 成立，接下来计算 $M^*=\frac{1}{\triangle p}\left(C_t^0-SK_0\sum_{i\in I}SK_i\cdot w_i\cdot C_t^i\right)$，并将计算结果输出到明文空间中使得 $M=\lceil M^*\rfloor\bmod p$，否则输出解密失败符号 $\perp$。

3.2. 正确性分析

设 $\triangle k=\lceil K_i\rfloor_p-\frac{p}{q}K_i$，$\triangle k1=\lceil a_t\cdot K_0\rfloor_p-\frac{p}{q}a_t\cdot K_0$，由解密公式得出解密算法的正确性分析：

$$\begin{aligned}M^*&=\frac{1}{\triangle p}\left(C_t^0-SK_0\sum_{i\in I}SK_i\cdot w_i\cdot C_t^i\right)\\&=\frac{1}{\triangle p}\left(C_t^0-SK_0\sum_{i\in I}\alpha\cdot K_i^{-1}\cdot\delta_i\cdot w_i\cdot C_t^i\right)\\&=\frac{1}{\triangle p}\left(C_t^0-SK_0\sum_{i\in I}\alpha\cdot K_i^{-1}\cdot s\cdot C_t^i\right)\\&=\frac{1}{\triangle p}\left(C_t^0-SK_0\sum_{i\in I}\alpha\cdot K_i^{-1}\cdot s\cdot a_t\cdot PK_i\cdot r_t\right)\\&=\frac{1}{\triangle p}\left(\left(PK_0\cdot r_t\cdot s+\triangle p\cdot M_t\right)-SK_0\sum_{i\in I}\alpha\cdot K_i^{-1}\cdot s\cdot a_t\cdot PK_i\cdot r\right)\end{aligned}$$

$$
\begin{aligned}
&=\frac{1}{\triangle p}\left(\left(\lceil a_t\cdot K_0\rfloor_p\cdot r_t\cdot s+\triangle p\cdot M_t\right)-K_0\cdot\alpha^{-1}\sum_{i\in I}\alpha\cdot K_i^{-1}\cdot s\cdot a_t\cdot\lceil K_i\rfloor_p\cdot r_t\right)\\
&=M_t+\frac{1}{\triangle p}\left(\lceil a_t\cdot K_0\rfloor_p\cdot r_t\cdot s-K_0\cdot\sum_{i\in I}K_i^{-1}\cdot s\cdot a_t\cdot\lceil K_i\rfloor_p\cdot r_t\right)\\
&=M_t+\frac{1}{\triangle p}\left(\left(\frac{p}{q}a_t\cdot K_0+\triangle k1\right)\cdot r_t\cdot s-\sum_{i\in I}K_i^{-1}\cdot s\cdot a_t\cdot\left(\frac{p}{q}K_i+\triangle k\right)\cdot r_t\right)\\
&=M_t+\frac{1}{\triangle p}\left(\left(\frac{p}{q}a_t\cdot K_0+\triangle k1\right)\cdot r_t\cdot s-\sum_{i\in I}\left(\frac{p}{q}\cdot s\cdot a_t\cdot r_t+K_i^{-1}\cdot s\cdot a_t\cdot\triangle k\cdot r_t\right)\right)\\
&=M_t+\frac{1}{\triangle p}\left(\triangle k1\cdot r_t\cdot s-\sum_{i\in I}K_i^{-1}\cdot s\cdot a_t\cdot\triangle k\cdot r_t\right)\\
&\le M_t+\frac{\triangle k1}{\triangle p}-\frac{\triangle k}{\triangle p}=M_t+\frac{\triangle k1-\triangle k}{\triangle p}
\end{aligned}
$$

因为 $r_t\in\{0,1\}$，$0<\triangle k,\triangle k1<\frac{1}{2}$，由以上公式可知当$\lceil\frac{\triangle k1-\triangle k}{\triangle p}\rfloor=0$时，解密公式$M=\lceil M^*\rfloor \bmod p$可以正确求出 M。显然，$\triangle k1-\triangle k$ 的误差范围在$\frac{\triangle p}{2}$以内时，可以保密解密的正确性。故当满足$\left\|\triangle k1-\triangle k\right\|_\infty^{can}\le\triangle p/(2\cdot c_m)$，$c_m$表示环常数，详细解释见文献[9]。

同态运算包括同态加法和同态乘法运算，同态计算过程只计算密文的第一个分量，密文第二个分量用来区分该密文属性是否在信任区间。设C_1^0和C_2^0是两个新鲜密文的第一部分，即$C_1^0=PK_1\cdot r_1+\triangle p\cdot M_1$，$C_2^0=PK_2\cdot r_2+\triangle p\cdot M_2$。

同态加法：
$$
\begin{aligned}
C_{add}&=F\left(C_1^0+C_2^0\right)=\left(PK_1\cdot r_1+\triangle p\cdot M_1\right)+\left(PK_2\cdot r_2+\triangle p\cdot M_2\right)\\
&=\triangle p\cdot\left(M_1+M_2\right)+PK_1\cdot r_1+PK_2\cdot r_2
\end{aligned}
$$

同态乘法：
$$
\begin{aligned}
\mathbf{C}_{mult}&=F\left(C_1^0\cdot C_2^0\right)=\frac{1}{\triangle p}\left(PK_1\cdot r_1+\triangle p\cdot M_1\right)\cdot\left(PK_2\cdot r_2+\triangle p\cdot M_2\right)\\
&=\frac{1}{\triangle p}\left(\triangle p^2\cdot M_1\cdot M_2+PK_1\cdot PK_2\cdot r_1r_2+\triangle p\cdot\left(M_1\cdot PK_2\cdot r_2+M_2\cdot PK_1\cdot r_1\right)\right)\\
&=\triangle p\cdot\left(M_1\cdot M_2\right)+PK_2\cdot r_2\cdot\frac{M_1}{\triangle p}+PK_1\cdot r_1\cdot\frac{M_2}{\triangle p}+\frac{\left(PK_1\cdot r_1\right)\cdot\left(PK_2\cdot r_2\right)}{\triangle p}
\end{aligned}
$$

通过以上同态加法和同态乘法计算公式不难看出评估密文和新鲜密文形式一致，设C_1^0和C_2^0的计算误差分别为$\triangle k_1$、$\triangle k_2$，则同态加法后的密文误差为$\triangle k_{add}=\triangle k_1+\triangle k_2$，因为$\left\|\triangle k_1+\triangle k_2\right\|_\infty^{\text{can}}\le\left\|\triangle k_1\right\|_\infty^{\text{can}}+\left\|\triangle k_2\right\|_\infty^{\text{can}}$，则同态加法可以正确计算。设同态乘法的计算误差为$\triangle k_{mult}$，$\delta=\frac{\left(PK_1\cdot r_1\right)\cdot\left(PK_2\cdot r_2\right)}{\triangle p}$，则对于同态乘法的噪音分析如下：
$$
\begin{aligned}
\left\|\triangle k_{mult}\right\|_\infty^{can}&\le\left\|\varepsilon_{q1}\cdot M_1\cdot M_2\right\|_\infty^{can}+\left\|\triangle k_1\cdot M_1\right\|_\infty^{can}+\left\|\triangle k_2\cdot M_2\right\|_\infty^{can}+\left\|\delta\right\|_\infty^{can}\\
&\le 4\cdot p^2\cdot\phi(m)/3+6\cdot\left(B+B'\right)\cdot p\cdot\sqrt{\phi(m)/12}+B_\delta=F\left(B,B'\right)
\end{aligned}
$$
。其中 B(或者 B')表示$\triangle k_1$(或者$\triangle k_2$)的标准范数的上界，那么$\triangle k_{mult}$的分类范数本质上增长为$p\cdot B\cdot B'/\triangle p$。我们通过函数$F\left(B,B'\right)$绑定了$\triangle k_{mult}$的规范形式。所以当满足$\left\|\triangle k_{mult}\right\|_\infty^{can}\le F\left(B,B'\right)$，可以保证同态乘法计算的正确性。

加密数据的细粒度访问控制：加密数据的访问控制由密文的第二部分C_t^i实现。满足访问结构 **D** 的秘钥SK_D的任何加密数据集 **A** 的超集能够恢复计算结果。如果一个属性子集 S 在访问结构 **D** 中，所有包含 S 作为子集的属性集合也是访问结构中的一部分。例如，一个访问结构为$\mathrm{D}=\{a_1\cap a_2\}$，如果集合

$S=\{a_1,a_2\}$ 满足访问结构 D，则 $A=\{a_1,a_2,a_3\}$ 也满足访问结构 D。

3.3. 安全性分析

本文提出的 LWR-ABFHE 方案的安全性是基于 Ring-LWR 问题的困难硬度构建起来的。本节证明了 LWR-ABFHE 方案满足 IND-ID-CPA(选择明文和选择 id 攻击下的不可区分安全)安全。证明如下：

定理 3. 如果 LWR 问题求解困难假设成立，则上节提出的 LWR-ABFHE 方案满足 IND-ID-CPA(选择明文和选择 id 攻击下的不可区分安全)安全。

证明：下面我们通过下述随机预言模型游戏进行。令 $\mathrm{Adv}_{\mathrm{Gamei}}[\mathrm{A}]$ 表示攻击者 A 在游戏 Gamei 中的优势，B 表示挑战者。

Game 0：这是一个关于我们 LWR-ABFHE 方案的标准 IND-CPA 游戏。依次通过下列步骤来刻画。

1) 初始化阶段：给出一个大小为 u 的属性集 U，B 声明他希望受到挑战的访问结构 A^* 并向 A 公布他的意向。

2) B 利用 LWR-ABFHE.Setup$(\lambda,\mathbf{U},k)$ 算法生成 (PP,MSK)，并且将 PP 发送给 A。

3) A 向 B 发送属性列表 $B^*=\{B_1^*,B_2^*,\cdots,B_j^*\}$ 的私钥查询，其中对于所有的 i 都有 $B^*\neq A^*$。B 通过秘钥生成算法 LWR-ABFHE.KeyGen(PP,MSK,D) 生成 SK_D，并且发送给 A。

4) A 发送属性 B^* 和一对消息 M_0、M_1 给 B，B 随机产生在访问结构 A^* 的密文 CT。然后将 CT 发送给 A。

5) A 重复进行第三步中的任意多次秘钥询问。

6) A 输出 $M'\in\{0,1\}$。B 接收到 A 对于密文 CT 的猜测 CT'，如果 $CT=CT'$，则成功；否则输出一个随机比特。在这个游戏中，A 的优势是 $\left|\Pr[CT=CT']-\frac{1}{2}\right|$。

Game 1：与 Game 0 不同的是，Game 1 改变了 Setup 算法，B 随机均匀构造 $\left(K1_i,K1_i^{-1}\right)\leftarrow R_q$，由 LWR 问题的困难性知 $\left(K1_i,K1_i^{-1}\right)$ 和 $\left(K_i,K_i^{-1}\right)$ 是统计上不能区分的，因此攻击者 A 在 Game 1 中的优势为 $\left|\mathrm{Adv}_{\mathrm{Game0}}(\mathrm{A})-\mathrm{Adv}_{\mathrm{Game1}}(\mathrm{A})\right|\le negl(\lambda)$。

Game 2：与 Game 1 不同的是，Game 2 改变了 KeyGen 算法中随机数α和其对应倒数α^{-1}的生成方式，因为 R_q 上均匀随机选取到的α及α^{-1}在统计意义上是不可区分的，则

$\left|\mathrm{Adv}_{\mathrm{Game1}}(\mathrm{A})-\mathrm{Adv}_{\mathrm{Game2}}(\mathrm{A})\right|\le negl(\lambda)$。并且因为选值是随机均匀的，所以 $\mathrm{Adv}_{\mathrm{Game2}}(\mathrm{A})=\frac{1}{2}$。

综上所述，我们可以计算出 Game 0 中攻击者 A 获胜的概率为：

$$\mathrm{Adv}_{\mathrm{Game0}}(\mathrm{A})=\left|\Pr(0)-\frac{1}{2}\right|\le\sum_{i=0,1}\left|\Pr(i)-\Pr(i+1)\right|+\left|\Pr(2)-\frac{1}{2}\right|\le negl(\lambda)$$

所以，LWR-ABFHE 全同态加密方案满足 IND-ID-CPA 安全，定理 3 得证。

4. 效率分析与对比

当数据接收方的属性列表满 L 足访问控制策略 W 时，接收方利用获得的用户私钥 SK_L，可以成功运行解密算法，从而获得数据的明文信息。下面从两个方面验证计算的正确性：

本文提出了基于 Ring-LWR 问题硬度的 LWR-ABFHE 方案的构建。为了支持多用户云环境下的端到端数据保护，本文将基于属性的加密方案扩展为同态加密方案。所提出的 LWR-ABFHE 方案能够在对加密数据进行细粒度访问控制的同时执行计算。在访问结构方面，所提出的 LWR-ABFHE 方案非常灵活，

Table 1. Comparison of efficiency analysis
表 1. 效率分析对比

方案	公钥尺寸	私钥尺寸	密文尺寸	基于困难问题
AB-GSW 方案	$2n(n+1)\log^2 q$	$(n+1)\lceil \log q \rceil^2$	$(n+1)^2\lceil \log q \rceil^3$	LWE
本文方案	$\log^2 d^3$	$\log^2 d^2$	$m\log p$	LWR

能够通过一组授权属性处理单调访问结构。在加密方面，所提出的 LWR-ABFHE 方案将密文分解为两个子分量，这进而改进了同态加密的计算能力。第一个组件承载用同态加密方案加密的数据;而第二个组件则负责通过使用基于属性的加密方案提供加密数据的细粒度访问。因此，能够扩展同态加密方案以支持多用户环境而不影响同态加密的计算能力。所提出的方案在 Ring-LWR 硬度的选择性设置模型下是安全的。

本文的 LWR-IBFHE 方案比传统的基于 LWE 问题构造的全同态加密方案具有更小的公、私钥尺寸和密文尺寸。而且消除了加密过程 LWE 进行高斯函数抽样的高昂时间开销，具有更快的高效的加解密效率。表 1 中列出了和文献[5] (以下简称 AB-GSW 方案)在同态计算电路的深度为 d 时的效率对比，其中 $m=O(n\log q)$， $p \geq m^{\frac{3}{2}d+1}\omega\left(\log^{2d} m\right)$ 并且 $q \geq 2mpB$ 。

5. 结语

近年来基于容错学习的全同态加密方案是研究的热点，但这类方案隐含的公钥尺寸过大和代价高昂的高斯噪声抽样，成为影响其效率的瓶颈。在本文中，我们基于 R-LWR 问题的困难性构造了一个更有效的 LWR-ABFHE 方案，并且演示了如何利用基于 LSSS 方案的单调访问结构编码密文以及密文的同态计算。带舍入学习问题的构造在保证安全性的基础上也降低了公钥尺寸，取得更快的计算效率。下一步工作将致力于研究非单调访问结构的访问策略构造全同态加密方案，以达到更高的效率和实现更广泛的应用场景。

基金项目

国家自然科学基金(10007016201201)。

参考文献

[1] Gentry, C. (2009) A Fully Homomorphic Encryption Scheme. Stanford University.

[2] Brakerski, Z. and Vaikuntanathan, V. (2011) Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. Cryptology Conference. Springer, Berlin, Heidelberg, 505-524. https://doi.org/10.1007/978-3-642-22792-9_29

[3] Brakerski, Z. and Vaikuntanathan, V. (2011) Efficient Fully Homomorphic Encryption from (Standard) LWE. *Foundations of Computer Science*, *IEEE*, 97-106.

[4] Brakerski, Z. (2012) Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. *Lecture Notes in Computer Science*, **7417**, 868-886. https://doi.org/10.1007/978-3-642-32009-5_50

[5] Gentry, C., Sahai, A. and Waters, B. (2013) Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. Advances in Cryptology - CRYPTO 2013. Springer Berlin Heidelberg, 75-92.

[6] Clear, M. and Mcgoldrick, C. (2015) Multi-Identity and Multi-Key Leveled FHE from Learning with Errors. Advances in Cryptology - CRYPTO 2015. Springer Berlin Heidelberg, 630-656.

[7] Brakerski, Z., Gentry, C. and Vaikuntanathan, V. (2014) (Leveled) Fully Homomorphic Encryption without Bootstrapping. *ACM Transactions on Computation Theory*, **6**, 1-36. https://doi.org/10.1145/2633600

[8] Bogdanov, A., Guo, S., Masny, D., *et al*. (2016) On the Hardness of Learning with Rounding over Small Modulus.

Proceedings, *Part I*, *of the* 13*th International Conference on Theory of Cryptography*, **9562**, Springer-Verlag New York, Inc., 209-224.

[9] Costache, A. and Smart, N.P. Homomorphic Encryption without Gaussian Noise. https://eprint.iacr.org/2017/163.pdf

[10] Fang, F., Li, B., Lu, X., *et al*. (2016) (Deterministic) Hierarchical Identity-Based Encryption from Learning with Rounding over Small Modulus. 907-912.

[11] Xiao, L., Bastani, O. and Yen, I.L. (2012) An Efficient Homomorphic Encryption Protocol for Multi-User Systems. IACR Cryptology ePrint Archive, 193.

[12] Clear, M. and Mcgoldrick, C. (2015) Policy-Based Non-Interactive Outsourcing of Computation Using Multikey FHE and CP-ABE. *International Conference on Security and Cryptography*, *IEEE*, 1-9.

[13] Clear, M. and Mcgoldrick, C. (2014) Bootstrappable Identity-Based Fully Homomorphic Encryption. Cryptology and Network Security. Springer International Publishing, 1-19.

[14] Tromer, E. and Vaikuntanathan, V. (2012) On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption. *Forty-Fourth ACM Symposium on Theory of Computing*, *ACM*, 1219-1234.

[15] Goyal, V., Pandey, O., Sahai, A., *et al*. (2006) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. *ACM Conference on Computer and Communications Security*, *ACM*, 89-98.

[16] Koo, D., Hur, J. and Yoon, H. (2013) Secure and Efficient Data Retrieval over Encrypted Data Using Attribute-Based Encryption in Cloud Storage. *Computers & Electrical Engineering*, **39**, 34-46. https://doi.org/10.1016/j.compeleceng.2012.11.002

[17] Beimel, A. (1996) Secure Schemes for Secret Sharing and Key Distribution. *International Journal of Pure & Applied Mathematics*.