doi:10.11959/j.issn.1000-436x.2017077

环上基于属性的全同态加密体制设计

郑永辉[1,2]，康元基[3]，顾纯祥[1,2]，董辉[3]

(1. 信息工程大学，河南 郑州 450002；2. 数学工程与先进计算国家重点实验室，江苏 无锡 214125；
3. 中国人民解放军 66136 部队，北京 100043)

摘 要：全同态加密在云计算的数据和隐私安全领域有重要应用，但现有全同态加密体制普遍存在密钥、密文尺寸偏大的弊端，严重制约其实用性。为此，以环上容错学习问题为基础，提出环上重编码体制与基于属性加密体制，并与全同态加密体制结合，构造基于属性的全同态加密体制，该体制无需公钥证书，可实现对加密数据细粒度访问控制，与已有同类成果相比，大大缩短了密钥与密文尺寸。

关键词：RLWE 问题；重编码；基于属性加密；全同态加密

中图分类号：TP309 **文献标识码**：A

Attribute-based fully homomorphic encryption scheme over rings

ZHENG Yong-hui[1,2], KANG Yuan-ji[3], GU Chun-xiang[1,2], DONG Hui[3]

(1.Information Engineering University, Zhengzhou 450002, China;
2.State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi 214125, China;
3. 66136 Troop of PLA, Beijing 100043, China)

Abstract: The fully homomorphic encryption has important applications in the area of data security and privacy security of cloud computing, but the size of secret keys and ciphertext in most of current homomorphic encryption schemes were too large, which restricted its practical. To improve these drawbacks, a recoding scheme and a attribute-based encryption scheme based on learning with errors problem over rings were provided, then a attribute-based fully homomorphic encryption was constructed. The new scheme overcame the above mentioned drawbacks, because it did't need public key certificate, meanwhile, it can achieve the fine-grained access control to the ciphertext. Compared with similar results, proposed method decreases the size of keys and ciphertext greatly.

Key words: RLWE problem, recode, attribute-based encryption, fully homomorphic encryption

1 引言

全同态加密是近些年来广受关注的新型加密技术，除具备一般公钥加密体制的功能外，还可以在不解密的条件下，实现密文任意运算，以达到明文做相同运算的效果，故其在解决云计算中隐私保护与数据保护的矛盾有重要意义，在数据库加密、医疗数据加密等方面也有重要应用。全同态加密的思想在 1978 年由 Rivest 等[1]提出，但直到 2009 年，才由 Gentry[2]在其博士论文中提出第一个真正意义上的全同态加密体制（以下简称 FHE 体制），之后，围绕 Gentry 提出的方法，人们构造出许多类似的 FHE 体制[3~5]。

使用 Gentry 方法构造体制时，由于许多依赖的问题难解性并未得到证明，人们对这类体制的安全性存在质疑。2011 年，Brakerski 等[6,7]提出了基于 LWE[8]与 RLWE[9]问题的体制（以下简称 LWE 体制与 RLWE 体制），这 2 类问题难解性都得到了严格

收稿日期：2016-03-07；**修回日期**：2017-02-23

基金项目：河南省科技创新杰出青年基金资助项目（No.134100510002）；河南省基础与前沿技术研究基金资助项目（No.142300410002）；数学工程与先进计算国家重点实验室开放基金资助项目

Foundation Items: The Province Foundation for Science Innovation Distinguished Young Scholars of Henan Province (No.134100510002), Henan Province Foundation and Advanced Technology Study (No.142300410002), State Key Laboratory of Mathematical Engineering and Advanced Computing Open Foundation

证明，并且相比使用 Gentry 方法构造的体制，解密算法计算复杂度大大降低。2012 年，Brakerski 等[10]又提出了密钥转换与模转换等一系列技术，进一步降低此类体制的计算复杂度。然而，目前的 FHE 体制依然存在密钥、密文尺寸过大的问题，严重制约 FHE 体制的实际应用。

基于属性加密体制[11,12]（以下简称 ABE 体制）是基于身份加密体制[13]（以下简称 IBE 体制）的延伸，不仅拥有 IBE 体制无需公钥证书，避免证书相关计算的优点，还可以实现对加密数据的细粒访问控制，适用于分布式环境下解密方不固定的条件，解密方只要与加密方属性集合的交集大于某个门限值即可解密。2013 年，Sergey 等[14]提出了基于 LWE 问题的 two-to-one raecoding（简写为 TOR）体制，并依此进一步提出 ABE 体制，同年，Gentry 等[15]指出该体制可通过一系列处理，转变为基于属性的全同态加密体制（以下简称 ABFHE 体制）。

相比 LWE 体制，RLWE 体制在许多加密应用中具备独特优势：令 n 为安全参数，q 为体制模数，RLWE 体制中的乘法一次可以得到 n 个伪随机等式，而 LWE 体制中需要 $m=n\mathrm{lb}q$ 个抽样才能达到相同安全性；环上运算可以使用快速傅里叶变换提高效率。由于构造简单，便于理解，目前，许多 RLWE 体制使用的是分圆多项式次数为 2 的幂环，文献[9,10]中的体制都以此类环为代数结构，但此类环分布稀疏，并且不具备实现 SIMD 技术等提高效率手段的性质，因此，本文将使用分圆多项式次数任意的环，这类环分布紧密，构造体制时效率最多可提高一倍，而且可使用 SIMD 技术提高加解密效率，但这类环上数学分析较少，近些年来，只有 Vadim 等[16]提出的分析方法及一些定理。

文献[17]提出任意分圆环上的 FHE 体制，此体制可以使用 Gentry 方法构造 ABFHE 体制，因此本文以文献[17]中 FHE 体制与文献[15]中 ABE 体制（以下简称 GVW 体制）为基础，首先利用 RLWE 问题构造环上编码，实现 2 种重编码方法与环上对称加密方法，构造以任意分圆环为代数结构的 TOR 体制，并以此为基础提出基于 RLWE 问题的 ABE 体制，证明这 2 个体制的正确性，利用基于游戏序列的方法证明它们的选择明文攻击（CPA，chosen-plaintext attack）安全性，并与文献[14]中的对应体制进行效率对比分析。进一步地，证明环上 ABE 体制与 FHE 体制结合为 ABFHE 体制的转换定理，将本文提出的 ABE 体制与文献[17]的 FHE 体制结合为 ABFHE 体制，相比文献[15]的 ABFHE 体制，本文体制无论在公私钥尺寸还是密文尺寸都大大缩小。

2 预备知识

2.1 符号定义

对于 $\mathbb{R}^n$ 及 $\mathbb{C}^n$ 上向量 $\boldsymbol{x}$，2-范数为 $\|\boldsymbol{x}\|_2=\left(\sum_i|x_i|^2\right)^{\frac{1}{2}}$，无穷范数为 $\|\boldsymbol{x}\|_\infty=\max_i|x_i|$，令 $\mathbb{Z}_m^*$ 为小于 m 且与 m 互质的正整数集合，$\varphi(\cdot)$ 为欧拉函数，$\lceil\cdot\rceil$ 与 $\lfloor\cdot\rfloor$ 分别表示向上取整与向下取整，$[\cdot]$ 表示四舍五入，$[\![a]\!]_q$ 在 $|a|<\frac{q}{4}$ 取值为 0，否则取 1；令 $negl(n)$ 表示关于 n 的可忽略函数，$poly(n)$ 表示关于 n 的多项式函数。

2.2 格基础与分圆域（环）

$\mathbb{C}^n$ 上的格可定义为 $\mathbb{C}^n$ 的离散加法子群，是由 n 个线性无关向量 $\boldsymbol{B}=\{b_i\}\subset\mathbb{C}^n$ 的所有整系数线性组合构成的集合，即 $\Lambda=\Lambda(\boldsymbol{B})=\left\{\sum_i a_ib_i:a_i\in\mathbb{Z}\right\}$，对于 $s>0$，定义高斯函数 $\rho_s(\boldsymbol{x})=\exp\left(-\frac{\pi\|\boldsymbol{x}\|_2^2}{s^2}\right)$，归一化可得连续高斯分布。对 $\mathbb{C}^n$ 中的向量 $\boldsymbol{x}$，可定义格陪集 $\Lambda+\boldsymbol{x}$ 上离散高斯分布 $D_{\Lambda+\boldsymbol{x},s}(\boldsymbol{x})=\frac{\rho_s(\boldsymbol{x})}{\rho_s(\Lambda+\boldsymbol{x})}$。

取正整数 m，在有理数域中加入 m 次本原单位根 ζ_m 得到的 $K=\mathbb{Q}(\zeta_m)$ 称为 m 次分圆域，在整数中加入 ζ_m 得到的 $R=\mathbb{Z}(\zeta_m)$ 称为 m 次分圆环。K 中有 n 个自同构 σ_i，其保持 $\mathbb{Q}$ 中元素不变，将 ζ_m 映射为 ζ_m^i，定义标准映射 $\sigma(a)=(\sigma_i(a))_{i\in\mathbb{Z}_m^*}$，其中，$a\in K$，定义迹函数 $\mathrm{Tr}:K\to\mathbb{Q}$ 为 $\mathrm{Tr}(a)=\sum_i\sigma_i(a)$，定义 $R^\vee=\{a\in K:\mathrm{Tr}(aR)\subseteq\mathbb{Z}\}$ 为分圆环 R 的对偶环，R 与其对偶环有以下定理。

定理 1[16] 对于分圆环 R 及其对偶 $R^\vee$，存在 $t\in R$，使 $R^\vee=t^{-1}R$。

2.3 RLWE 问题与环上陷门

首先定义一个分布，对于 $s\in R_q^\vee$（或 $R^\vee$）和 $\mathbb{R}(\zeta_m)$ 上连续高斯分布 ψ，RLWE 分布 $A_{s,\psi}$ 定义如下，均匀随机选择 $a\leftarrow R_q$，$e\leftarrow\psi$，则形为 $(a,b=as+e\bmod qR^\vee)$ 的二元组构成的分布称为

RLWE 分布。而判定性 RLWE（简称为 DRLWE）问题定义如下。

定义 1　$\mathrm{DRLWE}_{q,\psi}$ 问题是要以不可忽略的优势区分以下 2 个分布：第一个为从 RLWE 分布 $A_{s,\psi}$ 中随机抽样；第二个为 $R^\vee\left(\dfrac{\mathbb{R}(\zeta_m)}{qR^\vee}\right)$ 上同等数目的均匀随机抽样。

关于 DRLWE 问题的困难性有如下定理。

定理 2[16]　令参数如 2.2 节描述，令 $\alpha = poly(n)$，$q = poly(n)$，并且 $q = 1 \bmod m$，使 $\alpha q \geqslant \omega(\sqrt{\mathrm{lb}n})$，给定抽样数为 l，若存在解决 $\mathrm{DRLWE}_{q,\psi}$ 的算法，那么就存在算法可以解决 K 中理想格上的近似因子为 $\widetilde{O}\left(\dfrac{\sqrt{n}}{\alpha}\right)$ 的最短向量问题，其中，ψ 为离散高斯分布 $D_{\mathbb{R}(\zeta_m),s}$，$s = \dfrac{\alpha q (nl)^{\frac{1}{4}}}{[\mathrm{lb}(nl)]^{\frac{1}{4}}}$。

在实际情况中，通常使用离散高斯分布代替连续高斯分布，因此，需要将连续高斯分布离散化，令 $\|\|$ 表示从连续高斯分布转变为对应离散高斯分布，令 $\chi = \|p\psi\|_{\omega + pR^\vee}$ 表示从连续高斯分布 $p\psi$ 离散到格陪集 $\omega + pR^\vee$ 上的离散高斯分布，具体离散化方法见文献[16]，关于 $\mathrm{DRLWE}_{q,\chi}$ 的难度有如下定理。

定理 3　令 p 和 q 互质，若存在解决 $\mathrm{DRLWE}_{q,\psi}$ 问题在给定 l 个抽样时的算法，那么就存在解决 $\mathrm{DRLWE}_{q,\chi}$ 在给定 $l-1$ 个抽样时的算法。

本文体制构造公私钥对时，需要文献[17]中的 SampleR 算法，该算法的主要功能是利用陷门得到格陪集上符合离散高斯分布的一系列点。首先定义 2 个格：对于矩阵 $\boldsymbol{A} \in R_q^{m \times n}$，$\Lambda^\perp(\boldsymbol{A}) = \{\boldsymbol{x} \in R^n : \boldsymbol{A}\boldsymbol{x} = 0 \bmod qR\}$ 与 $\mathcal{L}^\perp(\boldsymbol{A}) = \{\boldsymbol{y} \in \mathbb{Z}^n : \boldsymbol{A}\boldsymbol{y} = 0 \bmod q\}$，$\mathcal{L}^\perp(\boldsymbol{A})$ 的“好”基（指这组基构成的矩阵奇异值较小）可由文献[18]的方法生成，关于这 2 个格的基有如下定理。

定理 4[16]　若 $\boldsymbol{B}$ 是 $\mathcal{L}^\perp(\boldsymbol{A})$ 的一组好基，$\boldsymbol{b}$ 是 R 的一组基，那么 $\boldsymbol{B} \otimes \boldsymbol{b}^{\mathrm{T}}$ 是 $\Lambda^\perp(\boldsymbol{A})$ 的一组好基。

2.4　全同态加密体制

一个全同态加密体制 FHE 包含 4 个算法：密钥生成算法 KeyGen、加密 Enc、解密 Dec 和密文同态运算算法 Eval，前 3 个与一般公钥体制类似，Eval 算法为密文对应代数结构上的运算，详细定义见文献[2]。

本文第 4 节构造体制时，需要文献[17]中的 AE 体制，该体制是使用近似特征向量构造的 FHE 体制，是构造无需运算密钥的 IBFHE 体制与 ABFHE 体制的基础。AE 体制同样分为密钥生成算法、加密算法、解密算法、密文同态运算算法，与其他 FHE 体制相比，AE 体制采用近似特征向量的等式进行解密，关系简单，因此无需运算密钥。另外在该体制描述中，定义了本文中会用到的 4 个函数：BitDecomp 函数及其逆函数、Flatten 函数和 Powersof2 函数。

2.5　基于属性的加密

本文 ABE 体制是以电路为基础，与一个电路 C 和比特串 ind 相关联，电路中每个门与一个输出节点、2 个输入节点（或更多）相关联，电路 C 的输入节点数与串 ind 长度相等，当 $C(ind) = 1$ 时才能正确解密。

一个 ABE 体制分为 3 个算法：密钥生成算法 KeyGen、加密算法 Enc 和解密算法 Dec。而 ABFHE 体制分为 4 个算法，前 3 个与 ABE 体制相同，第 4 个为密文同态运算算法 Eval，详细的定义及安全性定义可参见文献[12]。

3　环上 TOR 体制

由于环上采样和运算的高效性，本文利用 TOR 体制的思想，以分圆环作为基础代数结构构造环上 TOR 体制（简记为 RTOR 体制）并证明其正确性和安全性。

3.1　体制描述

令 $R = \mathbb{Z}(\zeta_m)$ 为 m 次分圆环，令 $n = \varphi(m)$，q 为 RLWE 中的模数，d 为 RTOR 体制的重编码深度，ψ 为 $\mathbb{R}(\zeta_m)$ 上连续高斯分布，$D_{R,r}$ 表示 R 上以 r 为参数的一般离散高斯分布，令 $\chi = \|q\psi\|_{qR^\vee}$，$k \leqslant l \leqslant poly(n)$，$\chi$ 中的高斯参数定义为 s，由文献[16]及文献[12]可知，s 由下式决定。

$$s \geqslant \frac{\omega(\sqrt{\mathrm{lb}n})(nl)^{\frac{1}{4}}}{[\mathrm{lb}(nl)]^{\frac{1}{4}}}$$

因此，取 $s = O(\sqrt{nl})$，并且令 $r = s$，χ 的界定义为 $B = s\sqrt{nl} = O(nl)$，为满足体制正确性，取 $q = |t|O(nl)^{2d+1}$。

RTOR 体制共分为 7 个部分：密钥生成算法 RTOR.KeyGen、编码算法 RTOR.Encode、重编码密钥生成算法 RTOR.RecodeKeyGen、无私钥重编码密钥生成算法 RTOR.NSRecodeKeyGen、重编码算法 RTOR.Recode、对称加密算法 RTOR.Enc 和对称解密算法 RTOR.Dec。

1) RTOR.KeyGen：利用定理 3 生成矩阵 $\boldsymbol{A}\in R_q^{k\times l}$ 与对应陷门 $\boldsymbol{T}\in R^{l\times l}$，令公钥为 $\boldsymbol{pk}=\boldsymbol{A}$，私钥为 $\boldsymbol{sk}=\boldsymbol{T}$。

2) RTOR.Encode($\boldsymbol{pk},\boldsymbol{u}$)：$\boldsymbol{u}$ 为构造编码时需要的输入，从 χ^k 中均匀随机采样可得，故 $\boldsymbol{u}\in(R_q^{\vee})^k$，取 $\boldsymbol{e}\leftarrow\chi^l$，故 $\boldsymbol{e}\in(R_q^{\vee})^l$，输出编码 $\boldsymbol{y}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{u}+\boldsymbol{e}\in(R_q^{\vee})^l$。

3) RTOR.RecodeKeyGen($\boldsymbol{pk}_0,\boldsymbol{pk}_1,\boldsymbol{pk}_{\mathrm{res}},\boldsymbol{sk}_b$)：该算法以公钥 $\boldsymbol{pk}_0$、$\boldsymbol{pk}_1$ 和任意一个公钥所对应的私钥 $\boldsymbol{sk}_b$（其中，$b\in\{0,1\}$）以及重编码后的公钥 $\boldsymbol{pk}_{\mathrm{res}}$ 为输入，输出为完成重编码所需重编码密钥 $\boldsymbol{E}_{0,1}^{\mathrm{res}}$，令 $\boldsymbol{pk}_0=\boldsymbol{A}_0,\boldsymbol{pk}_1=\boldsymbol{A}_1,\boldsymbol{sk}_b=\boldsymbol{T}_b,\boldsymbol{pk}_{\mathrm{res}}=\boldsymbol{A}_{\mathrm{res}}$，计算过程如下：在 $D_{R,r}$ 上取矩阵 $\boldsymbol{E}_b\in R^{l\times l}$，即矩阵中每一项都取自 $D_{R,r}$；计算 $\boldsymbol{U}=\boldsymbol{A}_{\mathrm{res}}-\boldsymbol{A}_b\boldsymbol{E}_b$；令 $\boldsymbol{U}=\boldsymbol{A}_{1-b}\boldsymbol{E}_{1-b}$，利用 SampleR 算法及陷门 $\boldsymbol{T}$ 可计算 $\boldsymbol{E}_{1-b}\in R^{l\times l}$。可得重编码密钥

$$\boldsymbol{E}_{0,1}^{\mathrm{res}}=\begin{bmatrix}\boldsymbol{E}_0\\ \boldsymbol{E}_1\end{bmatrix}\in R^{2l\times l}$$

可以看到，$\boldsymbol{A}_{res}-\boldsymbol{A}_b\boldsymbol{E}_b=\boldsymbol{U}=\boldsymbol{A}_{1-b}\boldsymbol{E}_{1-b}$，故可得 $\boldsymbol{A}_{\mathrm{res}}=\boldsymbol{A}_0\boldsymbol{E}_0+\boldsymbol{A}_1\boldsymbol{E}_1=\left[\boldsymbol{A}_0\middle\|\boldsymbol{A}_1\right]\boldsymbol{E}_{0,1}^{\mathrm{res}}$。

4) RTOR.NSRecodeKeyGen ($\boldsymbol{pk}_0,\boldsymbol{pk}_1$)：令 $\boldsymbol{pk}_0=\boldsymbol{A}_0,\boldsymbol{pk}_1=\boldsymbol{A}_1$，首先从 $D_{R,r}$ 上取矩阵 $\boldsymbol{E}_{0,1}^{\mathrm{res}'}\in R^{2l\times l}$，令 $\boldsymbol{A}'_{\mathrm{res}}=[\boldsymbol{A}_0\|\boldsymbol{A}_1]\cdot\boldsymbol{E}_{0,1}^{\mathrm{res}'}$，输出公钥 $\boldsymbol{pk}_{\mathrm{res}}=\boldsymbol{A}'_{\mathrm{res}}$ 和重编码密钥 $\boldsymbol{E}_{0,1}^{\mathrm{res}'}$。

5) RTOR.Recode($\boldsymbol{E}_{0,1}^{\mathrm{res}},\boldsymbol{y}_1,\boldsymbol{y}_2$)：利用 $\boldsymbol{E}_{0,1}^{\mathrm{res}}$ 对 $\boldsymbol{y}_1$、$\boldsymbol{y}_2$ 进行重编码可得 $\boldsymbol{y}_{\mathrm{res}}=\left(\left[\boldsymbol{y}_0^{\mathrm{T}}\middle\|\boldsymbol{y}_1^{\mathrm{T}}\right]\boldsymbol{E}_{0,1}^{\mathrm{res}}\right)^{\mathrm{T}}$。

6) RTOR.Enc($\boldsymbol{y},\boldsymbol{\mu}$)：输入为一个编码 $\boldsymbol{y}\in(R_q^{\vee})^l$ 和明文 $\boldsymbol{\mu}\in(R_2)^l$，输出密文为

$$\boldsymbol{c}=\boldsymbol{y}+\boldsymbol{t}^{-1}\left\lfloor\frac{q}{2}\right\rfloor\boldsymbol{\mu}\ \bmod q$$

7) RTOR.Dec($\boldsymbol{c},\boldsymbol{y}'$)：输入为一个编码 $\boldsymbol{y}'\in(R_q^{\vee})^l$ 和密文 $\boldsymbol{c}\in(R_q^{\vee})^l$，输出为 $\boldsymbol{\mu}=\llbracket(\boldsymbol{c}-\boldsymbol{y}')\cdot\boldsymbol{t}\rrbracket_q$。

3.2 正确性分析

由于对称加解密过程中仅用到环上加法运算，故可将每个环上元素看成 $\mathbb{Z}^n$ 上向量，那么明文 $\boldsymbol{\mu}\in(R_2)^l$ 可看作 $\{0,1\}^{nl}$ 上的向量，记作 $\boldsymbol{\mu}'$，取编码 $\boldsymbol{y}_0=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{u}+\boldsymbol{e}_0,\boldsymbol{y}_1=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{u}+\boldsymbol{e}_1$，类似地，可将 $\boldsymbol{ty}_0$、$\boldsymbol{ty}_1$、$\boldsymbol{te}_0$、$\boldsymbol{te}_1$ 看作 $\mathbb{Z}_q^{nl}$ 上的向量，分别记作 $\boldsymbol{y}'_0$、$\boldsymbol{y}'_1$、$\boldsymbol{e}'_0$、$\boldsymbol{e}'_1$。由文献[14]对 TOR 体制的分析可知，RTOR 体制的正确性分为以下 3 个部分。

1) 对于 $i\in[0,d]$，定义集合 $Y_{\boldsymbol{A},\boldsymbol{u},i}=\{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{u}+\boldsymbol{e}:\|\boldsymbol{e}\|_\infty\leqslant(2nls\sqrt{nl})^iB\}$，在 $i=0$ 时有 $\|\boldsymbol{e}\|_\infty\leqslant B$，故 $\Pr[\mathrm{Encode}(\boldsymbol{A},\boldsymbol{u})\in Y_{\boldsymbol{A},\boldsymbol{u},0}]=1$，并且由 $Y_{\boldsymbol{A},\boldsymbol{u},i}$ 的定义可知一定有 $Y_{\boldsymbol{A},\boldsymbol{u},0}\subseteq Y_{\boldsymbol{A},\boldsymbol{u},1}\subseteq\ldots\subseteq Y_{\boldsymbol{A},\boldsymbol{u},d}$。

2) 由 q、B、s 的取法有 $\|\boldsymbol{y}'_0-\boldsymbol{y}'_1\|_\infty=\|\boldsymbol{e}'_0-\boldsymbol{e}'_1\|_\infty\leqslant 2|\boldsymbol{t}|B(2nls\sqrt{nl})^d<\frac{q}{4}$，故编码 $\boldsymbol{ty}_0,\boldsymbol{ty}_1$ 之间的差异不会影响解密正确性，即 $\mathrm{Dec}(\boldsymbol{y}_0,\mathrm{Enc}(\boldsymbol{y}_1,\boldsymbol{\mu}))=\boldsymbol{\mu}$。

3) 对 $\boldsymbol{A}_2,\boldsymbol{A}_3\in R_q^{k\times l}$，$i_2,i_3\in\{0,1,\cdots,d-1\}$，取 $\boldsymbol{y}_2\in Y_{\boldsymbol{A}_2,\boldsymbol{u},i_2},\boldsymbol{y}_3\in Y_{\boldsymbol{A}_3,\boldsymbol{u},i_3}$，不失一般地令 $\boldsymbol{y}_2=\boldsymbol{A}_2^{\mathrm{T}}\boldsymbol{u}+\boldsymbol{e}_2$，$\boldsymbol{y}_3=\boldsymbol{A}_3^{\mathrm{T}}\boldsymbol{u}+\boldsymbol{e}_3,\|\boldsymbol{e}_2\|_\infty\leqslant(2nls\sqrt{nl})^{i_2}B,\quad\|\boldsymbol{e}_3\|_\infty\leqslant(2nls\cdot\sqrt{nl})^{i_3}B$，那么由 Recode 算法可计算 $\boldsymbol{y}_{\mathrm{res}}$ 为

$$\begin{aligned}\boldsymbol{y}_{\mathrm{res}}^{\mathrm{T}}&=[\boldsymbol{y}_2^{\mathrm{T}}\|\boldsymbol{y}_3^{\mathrm{T}}]\boldsymbol{E}_{2,3}^{\mathrm{res}}\\&=[\boldsymbol{u}^{\mathrm{T}}\boldsymbol{A}_2+\boldsymbol{e}_2^{\mathrm{T}}\|\boldsymbol{u}^{\mathrm{T}}\boldsymbol{A}_3+\boldsymbol{e}_3^{\mathrm{T}}]\boldsymbol{E}_{2,3}^{\mathrm{res}}\\&=\boldsymbol{u}^{\mathrm{T}}[\boldsymbol{A}_2\|\boldsymbol{A}_3]\boldsymbol{E}_{2,3}^{\mathrm{res}}+[\boldsymbol{e}_2^{\mathrm{T}}\|\boldsymbol{e}_3^{\mathrm{T}}]\boldsymbol{E}_{2,3}^{\mathrm{res}}\\&=\boldsymbol{u}^{\mathrm{T}}\boldsymbol{A}_{\mathrm{res}}+\boldsymbol{e}_{\mathrm{res}}\end{aligned}$$

其中，令 $\boldsymbol{e}_{\mathrm{res}}=[\boldsymbol{e}_2^{\mathrm{T}}\|\boldsymbol{e}_3^{\mathrm{T}}]\boldsymbol{E}_{2,3}^{\mathrm{res}}$，那么就有

$$\begin{aligned}\|\boldsymbol{e}_{\mathrm{res}}\|_\infty&\leqslant l\left\|\boldsymbol{E}_{2,3}^{res}\right\|_\infty(\|\boldsymbol{e}_2\|_\infty+\|\boldsymbol{e}_3\|_\infty)\\&\leqslant nlr\sqrt{nl}B((2nls\sqrt{nl})^{i_2}+(2nls\sqrt{nl})^{i_3})\\&\leqslant(2nls\sqrt{nl})^{\max(i_2,i_3)+1}B\end{aligned}$$

综合以上 3 个部分证明，RTOR 的正确性得证。

3.3 安全性分析

关于 RTOR 体制的安全性有如下定理。

定理 5 设系统参数如体制描述中所述，那么 RTOR 体制是 IND-CPA 安全的。

证明 定理证明采用基于游戏序列的证明方法，符号表示与体制描述中相同，令 $Adv_{\mathrm{Game}i}[\mathcal{A}]$ 表示攻击者 $\mathcal{A}$ 在 Game i 中的优势。

Game 0：Game 0 为标准的 IND-CPA 游戏：挑战者 $\mathcal{C}$ 依次调用 Encode 算法及 RecodeKeyGen 算法或 NSRecodeKeyGen 算法生成编码 $\boldsymbol{y}_{\mathrm{res}}$，并选择挑战明文 $\boldsymbol{\mu}_0^*$、$\boldsymbol{\mu}_1^*$，$\mathcal{C}$ 从中随机选择 $\boldsymbol{\mu}_a^*$ 并加密得到挑战

密文 $\boldsymbol{c}$，$\mathcal{A}$ 猜测 $\boldsymbol{c}$ 对应的明文为 $\boldsymbol{\mu}_a$，为简化公式，记 $P(\boldsymbol{y},\boldsymbol{\mu}_b^*)=\Pr[\mathcal{A}(\mathrm{RTOR.Enc}(\boldsymbol{y},\boldsymbol{\mu}_b^*))]$，那么 $\mathcal{A}$ 的优势记为

$$Adv_{\mathrm{CPA}}[\mathcal{A}]=|P(\boldsymbol{y},\boldsymbol{\mu}_0^*)-P(\boldsymbol{y},\boldsymbol{\mu}_1^*)| \tag{1}$$

Game 1：令 Game 1 中采用 RecodeKeyGen 算法来生成重编码密钥，那么 Game 1 相比 Game 0 的区别在于 $\boldsymbol{E}_{1-b}\in R^{l\times l}$ 采样自 $D_{R,r}$，这时 RecodeKeyGen 算法与 NSRecodeKeyGen 算法相同，由文献[16] 2.4.2 节的分析可知，SampleR 算法的结果与 $D_{R,r}$ 的统计距离在 $negl(n)$ 以内，故使用 $\boldsymbol{sk}_0$ 和 $\boldsymbol{sk}_1$ 生成的重编码密钥之间的统计距离在 $2negl(n)$ 以内，并且有

$$\left|Adv_{\mathrm{Game1}}[\mathcal{A}]-Adv_{\mathrm{CPA}}[\mathcal{A}]\right|\leqslant negl(n) \tag{2}$$

Game 2：Game 2 与 Game1 的区别在于编码 $\boldsymbol{y}$ 的生成方式，Game 2 中直接从 $(R_q^\vee)^l$ 均匀随机选取，由定理 2 可知

$$\left|Adv_{\mathrm{Game2}}[\mathcal{A}]-Adv_{\mathrm{Game1}}[\mathcal{A}]\right|\leqslant negl(n) \tag{3}$$

Game 3：Game 3 中，对称加密体制的密文不再由加密算法生成，而是从 $(R_q^\vee)^l$ 从均匀随机选取，由于密钥 $\boldsymbol{y}$ 为 $(R_q^\vee)^l$ 上均匀随机选取，以及 $\boldsymbol{c}=\boldsymbol{y}+\boldsymbol{t}^{-1}\left\lfloor\frac{q}{2}\right\rfloor\boldsymbol{\mu} \bmod q$，故有

$$\left|Adv_{\mathrm{Game3}}[\mathcal{A}]-Adv_{\mathrm{Game2}}[\mathcal{A}]\right|\leqslant negl(n) \tag{4}$$

至此，Game 3 中挑战者所给出的密钥、密文都服从均匀分布，且与目标密文之间完全独立，RecodeKeyGen 算法中无论选取哪个私钥都与 NSRecodeKeyGen 算法相同，故 $\mathcal{A}$ 在 Game 3 中能取得的优势为 0，即

$$Adv_{\mathrm{Game3}}[\mathcal{A}]=0 \tag{5}$$

结合式(1)~式(5)，有

$$\left|Adv_{\mathrm{CPA}}[\mathcal{A}]\right|\leqslant 3negl(n)$$

因此，$Adv_{\mathrm{CPA}}[\mathcal{A}]$ 可忽略，故 RTOR 是 IND-CPA 安全的。证毕。

3.4　效率分析与对比

与 TOR 体制相比，RTOR 体制以 RLWE 问题为基础，因此，重编码复杂度与重编码密钥有较大改善，并且 Encode 算法中的公钥更短。为使 2 种体制安全性相同，取 TOR 与 RTOR 体制的安全参数 $n=256$，对于 RTOR 体制来说，$t=n=256$，取 $k=4,l=8,d=4$，故取 $q=\left|t\right|(nl)^{2d+1}=2^{107}$，在对称加密算法中，明文大小为 $nl=2\ 048$；对于 TOR 体制来说，$n=256$，同样取 $d=4$，那么可得 $q=n(dn^2)^d\,\mathrm{lb}((dn^2)^d)\approx 2^{80}$，$m=n\mathrm{lb}q=20\ 480$，明文大小为 20 480 bit，为 RTOR 体制中的 10 倍，故在表 1 中统一为加密 2 048 bit 时的参数。由于 RTOR 中的运算为环上运算，将其直接看作整数运算（这里仅为对比方便，否则效率很难比较，实际上，视为整数运算会降低 RTOR 体制的效率，因为环上乘法可使用快速傅里叶变换）。

在利用 TOR 以及 RTOR 体制构造基于属性的体制时，需要生成多个公私钥对，反复利用 Encode 算法生成编码，并调用多次 RecodeKeyGen 算法来生成最后对称加密时所使用的密钥，故 RTOR 体制的改进有较大意义。表 1 为 TOR 体制与 RTOR 体制在公钥尺寸、重编码钥尺寸和重编码复杂度上的对比。

表 1　　TOR 与 RTOR 的对比

参数	TOR	RTOR
n	256	256
$\mathrm{lb}q$	80	107
d	4	4
公钥尺寸	40 MB	856 KB
重编码密钥尺寸	6.25 GB	3.34 MB
重编码复杂度	8.39×10^7 次乘	8.39×10^6 次乘
	8.39×10^7 次加	8.42×10^6 次加

4　环上 ABFHE 体制

本节首先提出环上 ABE 体制，同样利用环上运算的高效性设计以分圆环作为基础代数结构的体制，并证明其安全性与证明性，接着证明环上 FHE 体制与 ABE 体制结合为 ABFHE 体制的转换定理，设计出具备属性加密优势的全同态加密体制，缩短密钥和密文尺寸，最后对体制的效率进行对比分析。

4.1　环上 ABE 体制

令 C 为深度为 d 的布尔电路 $\{0,1\}^\lambda\to\{0,1\}$，$|C|$ 为该电路中所有节点数，λ 为整个电路的输入个数。那么环上 ABE 体制（以下简记为 RABE 体制）分为 5 个部分：密钥生成算法 RABE.KeyGen、重编码密钥生成算法 RABE.ReKeyGen、加密算法 RABE.Enc、解密算法 RABE.Dec、重编码算法 RABE.SinRecode。

1) RABE.KeyGen：首先生成均匀随机矩阵

$\boldsymbol{A}_{0,1}\in R_q^{k\times 1}$ 以及矩阵集合 $\{\boldsymbol{A}_{i,b}\in R_q^{k\times l}: i\in[1,\lambda],\ b\in\{0,1\}\}$，利用定理 4 生成每个矩阵对应陷门 $\boldsymbol{T}_{i,b}\in R^{l\times l}$，令公钥 $\boldsymbol{mpk}=(\boldsymbol{A}_{0,1},\{\boldsymbol{A}_{i,b}\},\lambda,d)$，主私钥 $\boldsymbol{msk}=\{\boldsymbol{T}_{i,b}\}$。

2) RABE.RekeyGen($\boldsymbol{msk},ind$)：将 $\boldsymbol{A}_{0,1}$ 与 C 的输出相关联，将 $\boldsymbol{A}_{i,b}$ 与 C 的第 i 个输入相关联，对于 C 中节点 z 以及标识位 a，其中，$z\in[\lambda+1,|C|-1]$，$a\in\{0,1\}$，生成均匀随机矩阵 $\boldsymbol{A}_{z,a}\in R_q^{k\times l}$，并利用定理 4 生成对应陷门 $\boldsymbol{T}_{z,a}\in R^{l\times l}$；取电路中门 $g=(u,v,w)$，其中，令节点 u、v 为 g 的输入，节点 w 为 g 的输出，令 $\boldsymbol{A}_{u,b}$、$\boldsymbol{A}_{v,c}$ 分别与节点 u、v 相关联，利用 RTOR.RecodeKeyGen 算法可生成 g 对应的 $\boldsymbol{E}_{u_b,v_c}^{w}$，即 $\boldsymbol{E}_{u_b,v_c}^{w}$ 可完成从 $\boldsymbol{A}_{u,b}$、$\boldsymbol{A}_{v,c}$ 到 $\boldsymbol{A}_{w,g_w(b,c)}$ 的转换，令与电路 C 相关私钥为 $\boldsymbol{sk}_C=\{\boldsymbol{E}_{u_b,v_c}^{w}: w\in[\lambda+1,|C|]\}$，其中，$b,c\in\{0,1\}$。

3) RABE.Enc($\boldsymbol{mpk},ind\in\{0,1\}^{\lambda},\boldsymbol{\mu}\in R_2$)：首先令 $\boldsymbol{A}_{ind}=\boldsymbol{A}_{1,ind_1}\|\cdots\|\boldsymbol{A}_{\lambda,ind_\lambda}\in R^{k\times\lambda l}$，$\boldsymbol{A}'_{ind}=\boldsymbol{A}_{0,1}\|\boldsymbol{A}_{ind}\in R^{k\times(\lambda l+1)}$，在 χ^k 上选取 $\boldsymbol{u}\in(R_q^{\vee})^k$，并令 $\boldsymbol{y}=\boldsymbol{A}_{0,1}^{\mathrm{T}}\cdot\boldsymbol{u}$，接着构造向量 $\boldsymbol{\mu}'\in R_q^{\lambda l+1}$，令其第一项为 $\left\lfloor\frac{q}{2}\right\rfloor\boldsymbol{\mu}\in R_q$，其余项皆为环上零元素，在 $\chi^{\lambda l}$ 上选取 $\boldsymbol{e}\in(R_q^{\vee})^{\lambda l+1}$，令密文为 $\boldsymbol{ct}_{ind}=\boldsymbol{u}\boldsymbol{A}'_{ind}+\boldsymbol{e}+\boldsymbol{\mu}'$。

4) RABE.Dec($\boldsymbol{sk}_C,ind,\boldsymbol{ct}_{ind}$)：计算 $C(ind)$，若 $C(ind)=0$，解密算法终止；否则，执行算法 RABE.SinRecode($\boldsymbol{sk}_C,ind$)得到向量 $\boldsymbol{h}\in R_q^{\lambda l}$，使 $\boldsymbol{A}_{ind}\boldsymbol{h}=\boldsymbol{A}_{0,1}\bmod q$ 成立，令子密钥 $\boldsymbol{h}'=(1,-\boldsymbol{h})\in R_q^{\lambda l+1}$，计算 $\boldsymbol{\mu}=\left[\!\left[\langle\boldsymbol{ct}_{ind},\boldsymbol{h}'\rangle\right]\!\right]_q\in R_2$。

5) RABE.SinRecode(sk_C,ind)：将 C 看作 π 级电路 $L_0,\cdots,L_\pi$，其中，$\pi\leqslant\lambda$，L_0 为电路输入级，L_π 为电路输出级；利用 $\boldsymbol{sk}_C$ 可计算 $\boldsymbol{A}_{0,1}$ 与 $\boldsymbol{A}_{u,b}$、$\boldsymbol{A}_{v,c}$ 之间的重编码密钥 $\boldsymbol{E}_{u_b,v_c}^{w}$，其中，$u,v\in L_{\pi-1},b,c\in\{0,1\}$，对所有级数为 $i\in[0,\pi-2]$ 的节点做类似递归计算，最终可得到 $\boldsymbol{A}_{0,1}$ 与输入级中所有节点的编码关系，即通过上述计算可得到 $\boldsymbol{h}\in R_q^{\lambda l}$，使 $\boldsymbol{A}_{ind}\boldsymbol{h}=\boldsymbol{A}_{0,1}\bmod q$。

4.2 RABE 体制的正确性与安全性

正确性：解密算法的输出为

$$\begin{aligned}\left[\!\left[\langle\boldsymbol{ct}_{ind},\boldsymbol{h}'\rangle\right]\!\right]_q&=\left[\!\left[\langle\boldsymbol{u}\boldsymbol{A}'_{ind}+\boldsymbol{e}+\boldsymbol{\mu}',(1,-\boldsymbol{h})\rangle\right]\!\right]_q\\&=\left[\!\left[\boldsymbol{u}\left[\boldsymbol{A}_{0,1}\|\boldsymbol{A}_{ind}\right](1,-\boldsymbol{h})+\langle\boldsymbol{e}+\boldsymbol{\mu}',(1,-\boldsymbol{h})\rangle\right]\!\right]_q\\&=\left[\!\left[\langle\boldsymbol{e}+\boldsymbol{\mu}',(1,-\boldsymbol{h})\rangle\right]\!\right]_q\\&=\left[\!\left[\langle\boldsymbol{e},\boldsymbol{h}'\rangle+\left\lfloor\frac{q}{2}\right\rfloor\boldsymbol{\mu}\right]\!\right]_q\\&=\boldsymbol{\mu}\end{aligned}$$

由于 $\boldsymbol{e}$ 取自高斯分布，故 $\langle\boldsymbol{e},\boldsymbol{h}'\rangle$ 不会影响解密结果。

关于体制安全性有以下定理。

定理 6 若 RTOR 体制是 IND-CPA 安全的，那么 RABE 体制具备 IND-selective-CPA 安全性。

证明 证明分为 2 个部分，首先构造替代算法，用以构造后续证明中的攻击者；接着采用基于游戏序列的证明方法完成证明。

1) 替代算法

选定挑战 ind，替代算法的目的是在不知道私钥的情况下回复私钥查询，算法包括 2 个部分：密钥生成算法 RABE.KeyGen*和加密算法 RABE.Enc*。

①RABE.KeyGen*(ind,C)：与 RABE.KeyGen 类似，生成均匀随机的矩阵集合 $\{\boldsymbol{A}_{i,1-ind_i}\in R_q^{k\times l}: i\in[1,\lambda]\}$ 与矩阵 $\boldsymbol{A}_{0,0}\in R_q^{k\times 1}$，令这些矩阵对应陷门为 $\{\boldsymbol{T}_{i,1-ind_i}\in R^{l\times l}: i\in[1,\lambda]\}$，对于节点 $w'\in[\lambda+1,|C|-1]$，令 $ind_{w'}=b^*$，同样可生成 $\{\boldsymbol{A}_{w',1-b^*}\in R_q^{k\times l}: i\in[1,\lambda]\}$ 与对应陷门 $\{\boldsymbol{T}_{w',1-b^*}\in R^{l\times l}: i\in[1,\lambda]\}$；对于节点 $w\in[\lambda+1,|C|]$，门 $g=(u,v,w)$，其中，u、v 为该门输入，令 u、v 的标识位分别为 b^*、c^*，那么 $d^*=g_w(b^*,c^*)$ 为 w 的标识位，故已知 $\boldsymbol{T}_{u,1-b^*}$ 与 $\boldsymbol{T}_{v,1-c^*}$。利用 RTOR.NSRecodeKeyGen($\boldsymbol{A}_{u,b^*},\boldsymbol{A}_{v,c^*}$)生成 $\boldsymbol{A}_{w,d^*}$ 与重编码密钥 $\boldsymbol{E}_{u_{b^*},v_{c^*}}^{w}$，接着调用 3 次 RecodeKeyGen 算法，令参数为($\boldsymbol{A}_{u,1-b^*},\boldsymbol{A}_{v,c^*},\boldsymbol{T}_{u,1-b^*}$，$\boldsymbol{A}_{w,g_w(1-b^*,c^*)}$)可生成 $\boldsymbol{E}_{u_{1-b^*},v_{c^*}}^{w}$，参数为 ($\boldsymbol{A}_{u,b^*},\boldsymbol{A}_{v,1-c^*}$，$\boldsymbol{T}_{v,1-c^*}$，$\boldsymbol{A}_{w,g_w(b^*,1-c^*)}$)生成 $\boldsymbol{E}_{u_{b^*},v_{1-c^*}}^{w}$，参数为($\boldsymbol{A}_{u,1-b^*}$，$\boldsymbol{A}_{v,1-c^*},\boldsymbol{T}_{u,1-b^*},\boldsymbol{A}_{w,g_w(1-b^*,1-c^*)}$) 生成 $\boldsymbol{E}_{u_{1-b^*},v_{1-c^*}}^{w}$。可以看到，$\boldsymbol{E}_{u_{1-b^*},v_{c^*}}^{w}$ 与 $\boldsymbol{E}_{u_{1-b^*},v_{1-c^*}}^{w}$ 在 RABE.KeyGen 与 RABE.KeyGen*算法中生成方式相同。

②RABE.Enc*($ind,\boldsymbol{\mu},\boldsymbol{mpk}$)：构造加密时所用 $\boldsymbol{A}_{ind}=\boldsymbol{A}_{1,1-ind_1}\|\cdots\|\boldsymbol{A}_{\lambda,1-ind_\lambda}$，与矩阵 $\boldsymbol{A}'_{ind}=\boldsymbol{A}_{0,0}\|\boldsymbol{A}_{ind}$，在 χ^k 取 $\boldsymbol{u}\in(R_q^{\vee})^k$，令 $\boldsymbol{y}=\boldsymbol{A}_{0,1}^{\mathrm{T}}\boldsymbol{u}$，构造向量 $\boldsymbol{\mu}'\in R_q^{\lambda l+1}$，令其第一项为 $\left\lfloor\frac{q}{2}\right\rfloor\boldsymbol{\mu}\in R_q$，其余项皆为

环上零元素，在 $\chi^{\lambda l}$ 上选取噪声向量 $\boldsymbol{e}\in(R_q^{\vee})^{\lambda l+1}$，令 $\boldsymbol{ct}_{ind}=\boldsymbol{u}\boldsymbol{A}'_{ind}+\boldsymbol{e}+\boldsymbol{\mu}'$ 为密文。

2) 基于游戏序列的证明

令 $Adv_{\text{Game}i}[\mathcal{A}]$ 表示攻击者 $\mathcal{A}$ 在 Game i 中的优势，并且 $\mathcal{A}$ 有 Q 次喻示访问权限条件。

Game 0：Game 0 即不做任何改变的原体制。

Game *i*：$i\in[1,Q]$：Game i 与 Game 0 相比，区别在于，在挑战者回复前 i−1 个密钥查询时使用 RABE.KeyGen* 算法，其余查询仍然使用 RABE.KeyGen 算法，对于第 i 次密钥查询 C_i，定义子游戏如下。

Game *i.j*：$j\in[\lambda+1,|C_i|]$：挑战者利用 RABE. KeyGen*算法生成 $(\boldsymbol{A}_{j,d^*},\boldsymbol{E}^{j}_{u_{b^*},v_{c^*}})$，其中，$u$、$v$ 表示输出为 j 的门的输入节点；接着生成 $\boldsymbol{E}^{j}_{u_{b^*},v_{1-c^*}}$，另外 2 个密钥 $\boldsymbol{E}^{j}_{u_{1-b^*},v_{c^*}}$、$\boldsymbol{E}^{j}_{u_{1-b^*},v_{1-c^*}}$ 在 RABE.KeyGen* 与 RABE. KeyGen 算法中生成方式相同，由 RTOR 体制安全性证明的 Game 1 的分析可知，这些重编码密钥之前的距离为 n 的可忽略函数，故挑战者已经将从 RABE.KeyGen 算法生成的重编码密钥集合 $\left\{\boldsymbol{E}^{j}_{u_b,v_c}:b\in\{0,1\},c\in\{0,1\}\right\}$ 转化为从 RABE.KeyGen* 算法生成，由 RTOR 体制安全性证明中 Game 1 中分析可知有

$$Adv_{\text{Game}i.j}[\mathcal{A}]-Adv_{\text{Game}i.(j+1)}[\mathcal{A}]\leqslant negl(n)$$

这时在 Game Q 中，挑战者使用 RABE.KeyGen*回复所有密钥查询，并可利用 RABE.Enc 生成挑战密文，那么有

$$Adv_{\text{Game}Q}[\mathcal{A}]-Adv_{\text{Game}0}[\mathcal{A}]<(|C|-\lambda)Qnegl(n)$$

Game $Q+1$：Game $Q+1$ 相比 Game Q 的区别在于挑战者使用 RABE.Enc*生成挑战密文，并且令 $\boldsymbol{y}$ 从 $R_q^{\vee}$ 中均匀随机选取，到此，显然可以构造针对 RTOR 体制的攻击者 $\mathcal{B}$，由 RTOR 体制的安全性证明可知 $\mathcal{B}$ 在 RTOR 体制中的优势 $Adv_{\text{RTOR}}[\mathcal{B}]\leqslant 3negl(n)$，那么有

$$\left|Adv_{\text{Game}(Q+1)}[\mathcal{A}]-Adv_{\text{Game}Q}[\mathcal{A}]\right|\leqslant Adv_{\text{RTOR}}[\mathcal{B}]$$

并且，由 RTOR 体制安全性分析的 Game 3 可知，$\mathcal{A}$ 在 Game $Q+1$ 中的优势为

$$\left|Adv_{\text{Game}(Q+1)}[\mathcal{A}]\right|\leqslant negl(n)$$

综合上面 4 式可得

$$\left|Adv_{\text{Game}0}[\mathcal{A}]\right|\leqslant((|C|-\lambda)Q+4)negl(n)$$

因此，在 RTOR 体制具备 IND-CPA 安全性的前提下，RABE 体制具备 IND-selective-CPA 安全性，证毕。

4.3　RABE 体制向 ABFHE 体制的转化

本节介绍一个将 RABE 体制转化为 ABFHE 体制的方法，此方法是文献[15]中转化定理在环上的变体。

定理 7　若一个 RABE 体制满足以下 3 条性质：1)令密钥为 $\boldsymbol{sk}_C$，子密钥和密文分别为 $\boldsymbol{h}'$ 和 $\boldsymbol{ct}_{ind}$，那么 $\boldsymbol{h}'$ 的第一项为 1；2)若 $\boldsymbol{ct}'_{ind}$ 为 0 的密文，那么 $\langle\boldsymbol{ct}'_{ind},\boldsymbol{h}'\rangle=0\bmod qR^{\vee}$；3)0 的密文与 $(R_q^{\vee})^{\lambda l+1}$ 上均匀分布不可区分，那么该 RABE 体制就可转化为 ABFHE 体制。

证明　ABFHE 体制使用 RABE 体制的密钥生成算法，令 $\ell'=\lceil\text{lb}q\rceil,N=\ell'(\lambda l+1)$，为加密 $\boldsymbol{\mu}\in\{0,1\}$，加密者利用 RABE 的加密算法生成 N 个 0 的密文，令 $\boldsymbol{C}'_{ind}$ 为 $N(\lambda l+1)$ 的矩阵，它的行由这些密文组成，令 $\boldsymbol{C}_{ind}=\text{Flatten}(\boldsymbol{\mu}\boldsymbol{I}_N+\text{BitDecomp}(\boldsymbol{C}'_{ind}))$，其中，$\boldsymbol{I}_N$ 为 N 阶单位矩阵，定义 $\boldsymbol{v}_{ind}=\text{Powersof2}(\boldsymbol{h}')$，解密时就可利用 AE 体制的解密算法得到 $\boldsymbol{\mu}$，同态运算与 AE 体制相同。

显然解密是正确的，因为 $\boldsymbol{C}_{ind}\boldsymbol{v}_{ind}=\boldsymbol{\mu}\boldsymbol{v}_{ind}+\boldsymbol{C}'_{ind}\boldsymbol{h}'=\boldsymbol{\mu}\boldsymbol{v}_{ind}\bmod qR^{\vee}$，由于性质 2)，故 $\boldsymbol{C}'_{ind}\boldsymbol{h}'=0\bmod qR^{\vee}$，因此，解密正确；另外，若存在攻击者可以区分 $\boldsymbol{C}'_{ind}$ 与 $(R_q^{\vee})^{N\times(\lambda l+1)}$ 上的均匀矩阵，则根据性质 3)，该攻击者也有能力以不可忽略的优势解决 DRLWE 问题，即证明了该体制安全性。证毕。

由于 RABE 体制显然满足定理中的 3 条性质，故可通过此方法转化为 ABFHE。该体制共分为以下 5 个部分。

1) Setup：调用 RABE.Setup 生成参数、主公私钥对(***mpk***, ***msk***)。

2) KeyGen(***msk***, *ind*)：令属性标识为 ***ind***，调用 RABE.KeyGen 生成与电路 C 相关的私钥 $\boldsymbol{sk}_c$ 以及重编码密钥。

3) Enc(***mpk***, *ind*, $\boldsymbol{\mu}$)：令 $\ell'=\lceil\text{lb}q\rceil,N=\ell'(\lambda l+1)$，为加密 $\boldsymbol{\mu}\in\{0,1\}$，加密者调用 RABE.Enc 生成 N 个 0 的密文，令 $\boldsymbol{C}'_{ind}$ 为 $N(\lambda l+1)$ 的矩阵，它的行由这些密文组成，令 $\boldsymbol{C}_{ind}=\text{Flatten}(\boldsymbol{\mu}\cdot\boldsymbol{I}_N+\text{BitDecomp}(\boldsymbol{C}'_{ind}))$，其中，$\boldsymbol{I}_N$ 为 N 阶单位矩阵。

4) Dec($\boldsymbol{C}_{ind}$, $\boldsymbol{sk}_{ind}$)：调用 AE.Dec($\boldsymbol{C}_{ind}$, $\boldsymbol{sk}_{ind}$)恢复明文 $\boldsymbol{\mu}$。

5) Eval(C_1, C_2)：调用 AE.Evaluate(C_1, C_2)实现密文的同态加法和同态乘法运算。

4.4 效率分析与对比

本节首先对比 RABE 与 GVW 体制的效率，再对比本文 ABFHE（以下简称 RABFHE 体制）与文献[15]中 ABFHE 体制（以下简称 GSW 体制）的效率。

RABE 体制与 GVW 体制相比，使用 RLWE 问题代替 LWE 问题设计体制，因此会大大降低公钥尺寸与密文尺寸，另外运算复杂度也有所降低，表 2 给出了 2 种体制在相同安全条件下的效率分析与对比。

表 2 GVW 与 RABE 的对比

参数	GVW	RABE
n	256	256
lb q	80	107
公钥尺寸	320 MB	6.79 MB
密文尺寸	640 KB	883 KB
ReKeyGen 算法复杂度	5.04×10^8 次乘 5.04×10^8 次加	5.04×10^7 次乘 5.06×10^7 次加
是否可使用 SIMD 技术	否	是

表 2 中数据具体说明如下，令 2 种体制的安全参数都为 $n=256$，RABE 体制的参数选取与 RTOR 体制类似，根据 3.4 节的分析，同样取 $t=n=256$, $k=4, l=8, d=4$，故可得 $q=|t|(nl)^{2d+1}=2^{107}$，明文比特数为 $nl=2\ 048$，同时由于 $d=4$，故可令 $\lambda=4$，那么这时 $|C|=10$；对于 GVW 体制来说，$n=256, d=4, \lambda=4, q\approx2^{80}, m=20\ 480$，明文是 RABE 体制的 10 倍，因此，表 2 中统一为加密 2 048 bit 时的参数。由于 2 种体制加密时使用的是简单的向量加法与环上加法，因此复杂度相当。而 ReKeyGen 算法中由于生成较多的重编码密钥，并且需要大量重编码运算，因此，该算法在整个加密进程中对效率影响较大，故表 2 比较了 2 种体制的 ReKeyGen 算法复杂度，表中数据并未考虑 SampleR 算法带来的影响，这是由于 SampleR 算法与整数上采样算法复杂度相当。另外，与 3.4 节的分析相同，RABE 体制可使用快速傅里叶变换进一步提高环上运算的效率，由文献[17]的分析可知，RABE 体制还可使用 SIMD 技术分割明文空间，实现并行加密，进一步提升加解密效率。

接下来，比较 RABFHE 与 GSW 体制的效率。RABFHE 体制相比 GSW 体制，同样使用 RLWE 问题代替 LWE 问题，参数设置与上文 RABE 体制、GVW 体制的讨论相同，因此，RABFHE 体制中，$\ell'=\lceil \mathrm{lb}q \rceil=107$，$N=\ell'(\lambda l+1)=3\ 531$，而 GSW 体制中，$\ell'=81$，$N=6\ 553\ 680$。表 3 给出 2 种体制在此条件下的效率对比。

表 3 GSW 与 RABFHE 的对比

参数	GSW	RABFHE
n	256	256
ℓ'	81	107
N	6 553 680	3 531
公钥尺寸	320 MB	6.79 MB
私钥尺寸	6.33 MB	883 KB
密文尺寸	22.26 GB	2.97 GB

5 结束语

随着云计算的高速发展，数据与隐私保护的重要性日益凸显，因此，全同态加密等新型加密技术得到广泛关注。但其公私钥尺寸与密文尺寸过大的问题始终难以解决。本文以环上容错学习问题为基础，设计基于属性的全同态加密体制，首先，环上运算效率较高，可有效减小公私钥与密文尺寸；其次，其具备基于身份加密无需公钥证书，避免其相关计算带来的巨大开销；最后，该体制具备解密灵活、可对密文进行细粒度访问控制的优势，可有效为云端共享数据提供访问控制。

参考文献：

[1] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[2] GENTRY C. Fully homomorphic encryption using ideal lattices[C]// STOC, 2009, 9: 169-178.

[3] DUK M V, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[C]//The 29th Annual Eurocrypt Conference. Riviera, French, 2010:24-43.

[4] SMART N P, VERCAUTEREN F. Fully homomorp-hic encryption with relatively small key and cipher-ext sizes[C]//The 13th International Conference on Practive and Theory in Public Key Cryptography(PKC2010). Paris, France, 2010:420-443.

[5] GENTRY C, HALEVI S. Implementing gentry's fully homomorphic encryption scheme[C]//EUROCRYP-T, Lecture Notes in Computer Science. 2011:129-148.

[6] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[J]. SIAM Journal on Computing, 2014, 43(2): 831-871.

[7] BRAKERSKI Z, VAIKUNTANATHAN V. Fully homomorphic en-

cryption from ring-LWE and security for key dependent messages[M]. Advances in Cryptology CRYPTO 2011. Springer Berlin Heidelberg, 2011: 505-524.

[8] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 34.

[9] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM (JACM), 2013, 60(6): 43.

[10] BRAKERSKI Z, Gentry C, VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping[C]//The 3rd Innovations in Theoretical Computer Science Conference. ACM, 2012: 309-325.

[11] SAHAI A, WATERS B. Fuzzy identity-based encryption[M]. Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457-473.

[12] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006: 89-98.

[13] SHAMIR A. Identity-based cryptosystems and signa-ture schemes[C]// Advances in Cryptology. Springer Berlin Heidelberg, 1985: 47-53.

[14] GORBUNOY S, VAIKUNTANATHAN V, WEE H. Attribute-based encryption for circuits[J]. Journal of the ACM (JACM), 2015, 62(6): 45.

[15] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based[M]. Advances in Cryptology–CRYPTO 2013. Springer Berlin Heidelberg, 2013: 75-92.

[16] LYUBASHEVSKY V, PEIKERT C, REGEV O. A toolkit for ring-LWE cryptography[M]. Advances in Cryptology–EUROCRYPT 2013. Springer Berlin Heidelberg, 2013: 35-54.

[17] KANG Y J, GU C X, ZHENG Y H, et al. Identity-based fully homomorphism encryption from eigenvector[J]. Journal of Software, doi:10.13328/j.cnki.jos.004991.

[18] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//The 40th Annual ACM Symposium on Theory of Computing. ACM, 2008: 197-206.

作者简介：

郑永辉（1976-），男，江西乐平人，博士，信息工程大学讲师，主要研究方向为密码学。

康元基（1992-），男，辽宁凤城人，66136 部队助理工程师，主要研究方向为全同态加密。

顾纯祥（1976-），男，安徽霍山人，博士，信息工程大学副教授，主要研究方向为密码学。

董辉（1982-），男，河北丰南人，66136 部队工程师，主要研究方向为模拟计算。