doi:10.11959/j.issn.1000-436x.2016258

基于 RLWE 的密钥策略属性加密体制

孙泽栋[1,2]，祝跃飞[1,2]，顾纯祥[1,2]，郑永辉[1,2]
（1. 解放军信息工程大学，河南 郑州 450001；2. 数学工程与先进计算国家重点实验室，江苏 无锡 214125）

摘 要：在 Brakerski 等提出的基于 LWE 问题的属性加密体制基础上，提出了一个基于 RLWE 问题的属性加密体制。相比基于 LWE 问题的属性加密体制，该体制效率更高、密钥尺寸更小。在 RLWE 的安全性假设下，该体制支持长度不受限制的属性和半适应性安全。最后设计了一个编译器，利用该编译器可以将满足要求的属性加密体制转化为基于属性的全同态加密体制。

关键词：格密码；RLWE；基于属性加密；基于属性全同态加密
中图分类号：TP309.7 **文献标识码**：A

RLWE-based key-policy ABE scheme

SUN Ze-dong[1,2], ZHU Yue-fei[1,2], GU Chun-xiang[1,2], ZHENG Yong-hui[1,2]
(1. PLA Information Engineering University, Zhengzhou 450001, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi 214125, China)

Abstract: Based on the attribute-based encryption(ABE) scheme which was proposed by Brakerski and constructed on the LWE problem, a RLWE-based key-policy ABE scheme was presented. Efficiency and key size of this scheme overtakes old ones which are based on the LWE problem. Under the RLWE assumption, this scheme supports attributes of unbounded length and semi-adaptive security. Moreover, a compiler was constructed and could compile ABE scheme that meets its demand into an attribute-based fully homomorphic encryption (ABFHE) scheme.

Key words: lattice cryptography, RLWE, attribute-based encryption, attribute-based fully homomorphic encryption

1 引言

随着互联网和分布式计算技术的迅速发展，越来越多的数据资源，特别是一些像个人信息、私人邮件这样的敏感数据开始在网上存储、分享和使用，这就对数据的访问控制策略提出了新的要求，不仅要控制数据的共享范围，还要保证数据在通信过程中的机密性。在这些方面，基于属性加密（ABE, attribute-based encryption）能够发挥很大的作用。

2005 年，Sahai 等[1]提出了一种称为 Fuzzy IBE 新型的基于身份加密体制，基于属性加密的概念由此而产生。从此，ABE 成为了密码学领域一件强有力的工具。在一个 ABE 体制中，数据提供者需要提供谓词，当且仅当他们的属性满足谓词的要求时，用户可以进行解密。2006 年，Goyal 等[2]提出了 2 种形式的 ABE：key-policy ABE 和 ciphertext-policy ABE，二者分别将一组属性与一个秘密密钥和一个密文相关联。

至今，在基于不同的假设和不同的应用场景构建高效和安全的 ABE 方案方面已经取得了很大进展。但是，最初大多数 ABE 体制都基于椭圆曲线上的双线性映射，这并不能抵抗量子密码分析。出于安全考虑，密码学家们不得不基于其他假设构造

收稿日期：2016-08-25
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: Henan Science and Technology Innovation Outstanding Youth Fund (No.134100510002), Research on Basic and Advanced Technology of Henan Province (No.142300410002), State Key Laboratory of Mathematical Engineering and Advanced Computing Open-End Fund

ABE 体制，并发现基于格的 ABE 体制可以避免这种安全漏洞。

实际上，由于许多加密方案的安全分析可以转化为格上困难问题的求解，格理论第一次在密码学领域中出现，扮演的是密码分析工具的角色。1996 年，Aitai[3]的开创性工作给出了格上 average-case 问题向 worst-case 问题的规约。一年后，首个基于格的加密体制 Ajtai-Dwork[4]体制诞生。除了在安全性方面的优良特性之外，由于运算通常都是线性的，基于格的密码体制更加高效和简单。Regev[5]在 2005 年提出了 LWE 问题，并证明了解决 average-case 情况下的该问题与（量子条件下）解决 worst-case 情况下的标准格上困难问题困难性相当。随后，LWE 问题成为许多加密体制的基石，例如基于身份加密[6]和基于属性加密[7]。然而，由于固有的乘法开销，基于 LWE 问题的加密体制效率较差。旨在解决 LWE 问题效率低的问题，在 2010 年，Lyubashevsky 等[8]引入了 RLWE 问题。RLWE 问题是 LWE 问题的一个代数变体，同样具有很强的安全性保证。较之于 LWE 问题，基于 RLWE 问题的加密体制效率更高，密钥尺寸更小。因此，基于此构建诸如文献[8]中的公钥密码系统具有广阔的前景。

Boneh 等[9]在 2014 年基于 LWE 问题构建了第一个 key-policy ABE 方案。然而，它只支持有限长度属性和选择性安全。为了克服上述 2 个缺点，2016 年，Brakerski 和 Vaikuntanathan[10]构建了基于 LWE 问题的 key-policy ABE 方案，其支持无限属性长度和半自适应安全性。由于 Brakerski 的方案是基于 LWE 问题的，它在效率和密钥大小方面存在缺陷。鉴于 RLWE 的良好性质，在一定程度上，基于 RLWE 问题重构 Brakerski 的方案可以克服上述 2 个缺点，使 ABE 方案更加实用。为了重构 ABE 方案，需要在环上重新设计“gadget matrix”，陷门和同态运算，而考虑到 LWE 和 RLWE 之间的结构差异，这并不是一个容易的工作。

一般来讲，ABE 方案不支持对加密数据的计算，而这正是全同态加密（FHE）旨在解决的问题。2013 年，Gentry 等[11]提出了一个可以将任何满足某些性质的基于 LWE 问题的 IBE 体制转化为 IBFHE 的编译器。进一步地，他们还修改了这个编译器，使其能够实现转化 ABE 方案为 ABFHE 方案，并对文献[12]中的 ABE 体制进行了转化。然而，由于文献[12]中的 ABE 体制具有某些特殊性质，这个编译器并不通用。因此，设计一个通用的 ABFHE 编译器是有意义的，而 Gentry 的 IBFHE 编译器无疑给了研究者极大的启发。

本文基于 RLWE 问题，构建了一个 key-policy ABE 体制。该体制支持长度不受限制的属性和半自适应安全性。此外，由于基于 RLWE 问题，该体制比以往体制效率更高，密钥尺寸更小。最后，本文构造了一个编译器，利用该编译器可以将满足要求的属性加密体制转化为一个基于属性全同态加密体制。

2 预备知识

2.1 RLWE 问题

2010 年，Lyubaskevsky 等[8]提出了 RLWE 问题，同时，将该问题的困难性规约到多项式环理想格中近似最短向量问题（SVP）。

基于后期体制的效率问题，本文只考虑特殊的任意分圆环。具体定义如下。

定义 1 判别性 RLWE 问题假设。对于安全参数 λ，令 $f(x)=x^d+1$，其中，$d=d(\lambda)$ 是 2 的方幂，令 $q=q(\lambda)\geqslant 2$ 为一个整数。令 $R=\frac{Z[x]}{f(x)}$，R_q 是 R 上的一个分布。$\mathrm{RDLWE}_{d,q,\chi}$ 问题是指对下面 2 种分布进行区分：1) (a_i,b_i) 随机均匀取自 R_q^2；2) 首先均匀随机选取 $s\leftarrow R_q$，然后随机均匀选取 $a_i\leftarrow R_q$ 和 $e_i\leftarrow\chi$ 并计算 $b_i=a_is+e_i$，最终得到 $(a_i,b_i)\in R_q^2$。$\mathrm{RDLWE}_{d,q,\chi}$ 假设是指 $\mathrm{RDLWE}_{d,q,\chi}$ 问题中的 2 种分布是不可区分的。

一般来讲，噪音分布 χ 通常为高斯分布。

2.2 密钥策略的属性加密体制

定义 2 密钥策略的属性加密（KP-ABE）。一个密钥策略的属性加密体制通常由 ABE.Params、ABE.Enc、ABE.Keygen、ABE.Dec 这几个概率多项式时间算法构成。

1) ABE.Params(1^λ)的输入为安全参数 λ，输出为主密钥 msk 和一个公共参数的集合 pp。

2) ABE.Enc(μ,x)的输入为公共参数集合 pp，取自消息空间 $M=M_\lambda$ 中的一个消息 μ 以及属性 $x\in\{0,1\}^*$，输出为密文 $ct\in\{0,1\}^*$。

3) ABE.Keygen(f)的输入为主密钥 msk 和一个函数 $f\in F_\lambda$，输出为私钥 sk_f。

4) ABE.Dec(sk_f, x, ct)的输入为私钥sk_f，属性$x \in \{0,1\}^*$，密文$ct \in \{0,1\}^*$，输出为一个消息$\mu' \in M$。

定义 3　Negated Policy[10]。为了使方案更加简洁，规定在$f(x)=0$时 ABE 方案可以进行解密，在安全性游戏过程中进行询问时，要求$f(x^*)=1$。

定义 4　KP-ABE 的正确性。如果一个 KP-ABE 体制满足下列条件，则认为它是正确的。

$\{f_\lambda \in F_\lambda\}_\lambda$和$\{x_\lambda \in \{0,1\}^*\}_\lambda$分别为函数序列和属性序列，对于输入尺寸为$|x_\lambda|$的函数$f$，$f_\lambda(x_\lambda)=0$对于所有的$\lambda$成立。对于所有前述的序列和任意的序列$\{m_\lambda \in M_\lambda\}_\lambda$

$$\Pr[\text{ABE.Dec}_{pp}(sk_f, x, ct) \neq \mu] = negl(\lambda)$$

其中，$(msk, pp) = \text{ABE.Params}(1^\lambda)$，$ct = \text{ABE.Enc}_{pp}(\mu, x)$，$sk_f = \text{ABE.Kyegen}_{msk}(f)$。

定义 5　KP-ABE 的安全性。一个 KP-ABE 体制的安全性通过下述的游戏序列来刻画。

1) challenger 利用算法 ABE.Params(1^λ)生成(msk, pp)并将 pp 发送给 adversary。

2) adversary 通过向 challenger 发送函数f_i进行任意次数的密钥询问。收到函数f_i后，challenger 生成$sk_i = \text{ABE.Keygen}_{msk}(f_i)$并把$sk_i$发送给 adversary。

3) adversary 发送属性x^*和一对消息m_0, m_1给 challenger，challenger 取样得到$b \in \{0,1\}$并计算挑战密文$ct^* = \text{ABE.Enc}_{pp}(m_b, x)$然后将$ct^*$发送给 adversary。

4) adversary 重复进行第二步中的任意多次密钥询问。

5) adversary 输出$\tilde{b} \in \{0,1\}$。

6) 用 legal 表示 adversary 所有的密钥询问结果都为$f_i(x^*)=1$的情况。如果为 legal，则游戏的输出为$b' = \tilde{b}$；反之，则b'为一个随机比特。

在此游戏中，adversary 的优势为$|\Pr[b'=b] - \frac{1}{2}|$。

上述游戏称为 ABE 体制的适应性安全游戏，在半适应性安全游戏中，adversary 在第 2)步之前向 challenger 发送属性x^*。

如果在一个 ABE 体制的适应性（半适应性）安全游戏中，任意一个概率多项式时间的 adversary 的优势都是可以忽略不计的，则称该 ABE 体制是适应性（半适应性）安全的。

2.3　伪随机函数

定义 6　一个伪随机函数族 PRF 由 2 个概率多项式时间算法 PRF.Gen 和 PRF.Eval 构成。其中，PRF.Gen(1^λ)的输入为安全参数λ，输出为种子$\sigma \in \{0,1\}^\eta$（其中，$\eta = \eta_\lambda$为长度）；PRF.Eval(σ, x)的输入为种子$\sigma \in \{0,1\}^\eta$和$x \in \{0,1\}^*$，输出为$y \in \{0,1\}$。

伪随机函数族 PRF 是安全的，则对每一个多项式时间 adversary A，下式成立。

$$|\Pr[A^{PRF.Eval(\sigma,\cdot)}(1^\lambda)=1] - \Pr[A^{O(\cdot)}(1^\lambda)=1]| = negl(\lambda)$$

其中，$\sigma = PRF.Gen(1^\lambda)$，$O$ 是一个随机谕示。

3　基于 RLWE 的密钥策略属性加密体制描述

在 Brakerski 和 Vaikuntanathan 的 KP-ABE 体制[10]的启发下，本文基于 RLWE 问题构造了一个新的 KP-ABE 体制，该体制支持长度不受限制的属性和半适应的安全性。首先，本文对 gadget matrix，陷门和电路运算进行了一些改进，使之能够满足环上的运算。其次，基于 RLWE 问题给出了体制的构造细节。最后，证明了该体制的正确性和安全性。

3.1　gadget matrix

令“gadget matrix”$\boldsymbol{G} = (1, x, \cdots, x^{n-1}) \in R_q^n$，映射$\boldsymbol{G}^{-1}: R_q^m \to R_q^{n\times m}$把输入向量的每一个分量$a \in R_q$转化为一个列向量，该列向量实际为幂基表示的系数。对于所有的$\boldsymbol{A} \in R_q^m$，都有$\boldsymbol{G} \cdot \boldsymbol{G}^{-1}(\boldsymbol{A}) = \boldsymbol{A}$。

3.2　陷门

$n, m, q \in N$，矩阵$\boldsymbol{A} \in R_q^m$，对于所有的$V \in R_q^{m'}$，令$\boldsymbol{A}_\tau^{-1}(V)$服从高斯分布$D_{R^m,\tau}^{m'}$且满足$\boldsymbol{A} \cdot \boldsymbol{A}_\tau^{-1}(V) = V$的随机变量。$\boldsymbol{A}$的一个$\tau-$陷门是一个对于任意的$V$在时间$poly(n, m, m', q)$内从分布$\boldsymbol{A}_\tau^{-1}(V)$中采样的算法。本文用$\boldsymbol{A}_\tau^{-1}$来表示$\boldsymbol{A}$的$\tau-$陷门。

对于陷门的性质，Ajtai、Gentry、Peikert 等已经进行了深入研究，结合本文体制设计需求，总结为如下引理。

引理 1　陷门性质[4,6,13~15]如下。

1) 给定$\boldsymbol{A}_\tau^{-1}$，对于任意的$\tau' \geqslant \tau$能够得到$\boldsymbol{A}_{\tau'}^{-1}$；

2) 给定$\boldsymbol{A}_\tau^{-1}$，对于任意的$\boldsymbol{B}$能够得到$[\boldsymbol{A} \| \boldsymbol{B}]_\tau^{-1}$和$[\boldsymbol{B} \| \boldsymbol{A}]_\tau^{-1}$；

3) 对所有的$\boldsymbol{A} \in R_q^m$和$\boldsymbol{T} \in R_q^{m\times n}$，对于$\tau = O(m \| \boldsymbol{T} \|_\infty)$能得到$[\boldsymbol{A}\boldsymbol{T} + \boldsymbol{G} \| \boldsymbol{A}]_\tau^{-1}$；

4) 存在一个有效的算法 TrapEmbed($1^n, q$)能够

输出 $(\boldsymbol{A}, \boldsymbol{A}_{\tau_0}^{-1})$，其中，对于某个 $m = O(n\log q)$，$\boldsymbol{A} \in R_q^m$ 是 2^{-n} 均匀的，$\tau_0 = O(\sqrt{n\log q \log n})$。

3.3 电路运算

$n, q \in N$，$\boldsymbol{C}_1, \cdots, \boldsymbol{C}_l \in R_q^n$，$\vec{\boldsymbol{C}} = [\boldsymbol{C}_1 \| \cdots \| \boldsymbol{C}_l]$。$f$ 是一个级数为 d 的布尔电路：$\{0,1\}^l \to \{0,1\}$，并且假设 f 只由 NAND 门构成。定义 $\boldsymbol{C}_f = \mathrm{Eval}(f, \vec{\boldsymbol{C}})$，其中，$\boldsymbol{C}_1, \cdots, \boldsymbol{C}_l$ 作为电路的输入。对于电路 f 中的每个线路 w，令 u, v 为它的上层输入并且定义 $\boldsymbol{C}_w = \boldsymbol{G} - \boldsymbol{C}_u \cdot \boldsymbol{G}^{-1}(\boldsymbol{C}_v)$。$\boldsymbol{C}_f$ 为最终输出的矩阵。

对于 $\boldsymbol{C}_f = Eval(f, \vec{\boldsymbol{C}})$，有 $\boldsymbol{C}_f - f(x)\boldsymbol{G} = (\vec{\boldsymbol{C}} - x\vec{\boldsymbol{G}})H_{f,x,\vec{\boldsymbol{C}}}$ 对于满足 $\|\boldsymbol{H}_{f,x,\vec{\boldsymbol{C}}}\| \leqslant (n+1)^d$ 的矩阵 $\boldsymbol{H}_{f,x,\vec{\boldsymbol{C}}}$，其中，$x\vec{\boldsymbol{G}} = [x_1\boldsymbol{G} \| \cdots \| x_l\boldsymbol{G}]$。特别地，如果 $\boldsymbol{C}_i = \boldsymbol{A}\boldsymbol{R}_i + x_i\boldsymbol{G}$（例如 $\vec{\boldsymbol{C}} = \boldsymbol{A}\vec{\boldsymbol{R}} + x\vec{\boldsymbol{G}}$，$\vec{\boldsymbol{R}} = [\boldsymbol{R}_1 \| \cdots \| \boldsymbol{R}_l]$），则有 $\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_f + f(x)\boldsymbol{G}$ 对于 $\boldsymbol{R}_f = \vec{\boldsymbol{R}}\boldsymbol{H}_{f,x,\vec{\boldsymbol{C}}}$（$\boldsymbol{H}$ 与 $\vec{\boldsymbol{R}}$ 相互独立）。

在给出具体的属性加密体制之前，首先定义如下 2 种电路。

定义 7 级数有限电路。级数至多为 d 的电路用 P_d 来表示，对于 $d = d(\lambda)$ 集合族 $\{P_{d,\lambda}\}_\lambda$ 表示级数至多为 $d(\lambda)$ 的布尔电路集合 $P_{d,\lambda}$ 的全体。

定义 8 比特比对电路。对于 $v \in N$，$x \in \{0,1\}^*$ 和 $|x| \leqslant 2^v$，定义比特比对电路 $BitCheck_{v,x} : [2^v] \times [2^v] \times \{0,1\} \to \{0,1\}$，其中，$BitCheck_{v,x}(l,i,b) = 1$ 当且仅当 $|x| = l$ 且 $x_i = b$。显然 $BitCheck_{v,x}$ 可以由级数为 $O(\log|x|) = O(v)$ 的布尔电路表出。

3.4 详细描述

令 $v = v(\lambda)$，oldABE = (oldABE.Params, oldABE.Enc, oldABE.Keygen, oldABE.Dec)为一个选择性安全的 KP-ABE 体制，且其函数集为 $\{\{BitCheck_{v(\lambda),x} : |x| \leqslant 2^v\}\}_\lambda$（$v$ 的具体定义如上所述）。需要注意的是，该 KP-ABE 只需要支持长度有限的属性。令 PRF 为一组伪随机函数的集合，令 $\eta = \eta_\lambda$ 为种子长度（λ 为安全参数）。令 d_{prf} 为 $\mathrm{PRF.Eval}(\sigma, x)$ 的级数，其中，$|x| = v$（有定义则可知 $d_{prf} = poly(\lambda)$）。

下面本文给出基于 RLWE 的密钥策略属性加密体制的具体细节。鉴于要事先给定电路的多项式函数的级数上界，故初始参数为安全参数和该级数上界。

1) ABE.Params$(1^\lambda, 1^d)$：为了能够支持 P_d（定义 7），初始化环节的输入为 $(1^\lambda, 1^{d(\lambda)})$。$\lambda$ 为安全参数，d 为电路级数上界且为 λ 的多项式函数。在此过程中，首先根据定理 2 设置 RDLWE 问题的参数 q、χ、B 且保证 $\frac{q}{B} \geqslant (N+1)^{2(d+d_{prf})} 2^{3v}$。其次取 B'-swallowing and $\tilde{B}$-bounded 分布 $\tilde{\chi}$，文献[10]给出了具体的选取方法）。

而后，生成一个矩阵陷门对 $(\boldsymbol{A}, \boldsymbol{A}_{\tau_0}^{-1}) = \mathrm{TrapEmbed}(1^n, q)$（引理 1），取 $\boldsymbol{u} \xleftarrow{\$} R_q$，取向量列 $\boldsymbol{B}_1, \cdots, \boldsymbol{B}_\eta \xleftarrow{\$} R_q^n$，令 $\vec{\boldsymbol{B}} = [\boldsymbol{B}_1 \| \cdots \| \boldsymbol{B}_\eta]$。

生成 oldABE 的初始参数：$(\mathrm{oldABE}msk, \mathrm{oldABE}pp) = \mathrm{oldABE.Params}(1^\lambda)$。

生成一个 PRF 的种子：$\sigma = \mathrm{PRF.Gen}(1^\lambda)$。

最终，令 $msk = (\boldsymbol{A}_\tau^{-1}, \mathrm{oldABE}msk, \sigma)$，$pp = (\boldsymbol{A}, \vec{\boldsymbol{B}}, \mathrm{oldABE}pp)$。

2) $\mathrm{ABE.Enc}_{pp}(\mu, x)$：输入为 $u \in \{0,1\}$，$x \in \{0,1\}^*$。令 $l = |x|$ 表示属性长度。对于所有的 $i \in [l]$，生成 $\boldsymbol{C}_i = \mathrm{Eval}(\mathrm{PRF.Eval}(\bullet, i), \vec{\boldsymbol{B}})$，其中，$\mathrm{PRF.Eval}(\bullet, i)$ 为输入为种子 σ，输出为 $\mathrm{PRF.Eval}(\sigma, i)$ 的电路。

取 $\boldsymbol{s} \xleftarrow{\$} R_q$，$\boldsymbol{e} \xleftarrow{\$} \chi^m$，$\boldsymbol{e}' \xleftarrow{\$} \chi$，令

$$\boldsymbol{c}_0^{\mathrm{T}} = \boldsymbol{s}^{\mathrm{T}}[\boldsymbol{A} \| \boldsymbol{v}] + [\boldsymbol{e}^{\mathrm{T}} \| \boldsymbol{e}'] + \mu\left\lceil \frac{q}{2} \right\rceil [\boldsymbol{0}^{\mathrm{T}} \| \boldsymbol{1}]$$

对于所有的 $i \in [l]$，取一个噪音向量 $\tilde{\boldsymbol{e}}_i \xleftarrow{\$} \tilde{\chi}^n$ 并计算

$$\boldsymbol{c}_{i,x_i \oplus \beta}^{\mathrm{T}} = \boldsymbol{s}(\boldsymbol{C}_i - (\boldsymbol{x}_i \oplus \boldsymbol{\beta})\boldsymbol{G}) + \tilde{\boldsymbol{e}}_i$$

而后，将向量 $\boldsymbol{c}_{i,\beta}$ 用 oldABE 加密

$$\psi_{i,\beta} = \mathrm{oldABE.Enc}((l, i, \beta), \boldsymbol{c}_{i,x_i \oplus \beta})$$

最终密文为 $ct = (\boldsymbol{c}_0, (\psi_{i,\beta})_{i \in [l], \beta \in \{0,1\}})$。

3) $\mathrm{ABE.Keygen}_{msk}(f)$：$f$ 是一个满足映射 $\{0,1\}^l \to \{0,1\}$ 的电路。在生成密钥之前，需要注意的是根据 negated policy（定义 3），当 $f(x) = 0$ 时 sk_f 方可进行解密。

对于所有的 i，定义 $\Delta_i = \mathrm{PRF.Eval}(\sigma, i)$ 并令 $\Delta_{\leqslant l} = \Delta_1 \cdots \Delta_l$ 为长度无限的串 Δ 的 l-前缀。

生成 oldABE 的密钥：$\text{oldABE}sk_l = \text{oldABE.Keygen}_{\text{oldABEmsk}}(\text{BitCheck}_{v,\Delta_{\leqslant l}})$。定义 $f_\Delta : \{0,1\}^l \to \{0,1\}$ 为 $f_\Delta(x) = f(x \oplus \Delta_{\leqslant l})$。

对于所有的 $i \in [l]$，生成 $C_i = \text{Eval}(\text{PRF.Eval}(\cdot, i), \vec{\boldsymbol{B}})$，令 $\vec{\boldsymbol{C}} = [\boldsymbol{C}_1 \| \cdots \| \boldsymbol{C}_l]$，$\boldsymbol{C}_f = \text{Eval}(f_\Delta, \vec{\boldsymbol{C}})$，$\boldsymbol{r}_f = [\boldsymbol{C}_f \| \boldsymbol{A}]_\tau^{-1}(v)$，$\boldsymbol{t}_f = [-\boldsymbol{r}_f^{\mathrm{T}} \| \boldsymbol{1}]^{\mathrm{T}}$，由其性质可得 $[\boldsymbol{C}_f \| \boldsymbol{A} \| \boldsymbol{v}] \cdot \boldsymbol{t}_f = 0$。

最终得到密钥 $sk_f = (f, \Delta_{\leqslant l}, \text{oldABE}sk_l, \boldsymbol{t}_f)$。

4) ABE.Dec(sk_f, x, ct)：首先利用 oldABEsk_l 计算

$$c_{i,x_i \oplus \Delta_i} = \text{oldABE.Dec}(\text{oldABEsk}_l, \psi_{i,\Delta_i}, (l, i, \Delta_i))$$

而后得到

$$\boldsymbol{c}^{\mathrm{T}}_{x \oplus \Delta \leqslant l} = [\boldsymbol{c}^{\mathrm{T}}_{1,x_1 \oplus \Delta_1} \| \cdots \| \boldsymbol{c}^{\mathrm{T}}_{l,x_l \oplus \Delta_l}]$$

再次计算 $\boldsymbol{C}_i = \text{Eval}(\text{PRF.Eval}(\cdot, i), \vec{\boldsymbol{B}})$，$\vec{\boldsymbol{C}} = [\boldsymbol{C}_1 \| \cdots \| \boldsymbol{C}_l]$ 和 $\boldsymbol{C}_f = \text{Eval}(f_\Delta, \vec{\boldsymbol{C}})$。

计算 $\boldsymbol{H} = \boldsymbol{H}_{f\Delta, x \oplus \Delta_{\leqslant l}, \vec{\boldsymbol{C}}}$ 且由前述可知 $f_\Delta(x \oplus \Delta_{\leqslant l}) = f(x) = 0$ 故有

$$(\vec{\boldsymbol{C}} - (x \oplus \Delta_{\leqslant l})\vec{\boldsymbol{G}})\boldsymbol{H} = \boldsymbol{C}_f - f_\Delta(x \oplus \Delta_{\leqslant l})\boldsymbol{G} = \boldsymbol{C}_f$$

最终，计算 $\tilde{\mu} = [\boldsymbol{c}_f^{\mathrm{T}} \| \boldsymbol{c}_0^{\mathrm{T}}] \cdot \boldsymbol{t}_f$ 并输出 $\mu' = 0$ 如果 $\left|\tilde{\mu}\right| < \frac{q}{4}$，输出 $\mu' = 1$ 如果 $\left|\tilde{\mu}\right| \geqslant \frac{q}{4}$。

3.4.1 正确性

定理 1　当参数如体制中所要求的恰当选取时，本文基于 RLWE 的 KP-ABE 体制是安全的。

证明　由上面给出的 ABE.Dec(sk_f, x, ct) 可以得到

$$\tilde{\mu} = [\boldsymbol{c}_f^{\mathrm{T}} \| \boldsymbol{c}_0^{\mathrm{T}}] \cdot \boldsymbol{t}_f = [\tilde{\boldsymbol{e}}\boldsymbol{H} \| \boldsymbol{e}^{\mathrm{T}} \| \boldsymbol{e}'] \cdot \boldsymbol{t}_f + \mu \left\lceil \frac{q}{2} \right\rceil$$

因此，只要 $|[\tilde{\boldsymbol{e}}\boldsymbol{H} \| \boldsymbol{e}^{\mathrm{T}} \| \boldsymbol{e}'] \cdot t_f|$ 限定在 $\frac{q}{4}$ 以内便能够进行正确的解密。由离散高斯分布的性质可知，

$$|[\tilde{\boldsymbol{e}}\boldsymbol{H} \| \boldsymbol{e}^{\mathrm{T}} \| \boldsymbol{e}'] \cdot \boldsymbol{t}_f| \leqslant \boldsymbol{B}(n+1)^{2(d+d_{prf})} 2^{2v} \cdot poly(n, \log q)$$

由于在 ABE.Params$(1^\lambda, 1^d)$ 中，令 $\frac{q}{B} \geqslant (N+1)^{2(d+d_{prf})} 2^{3v}$，故解密的正确性可以保证。

3.4.2 安全性

定理 2　假设 PRF 是一族安全可靠的伪随机函数（定义 3），假设对于函数集合 $\text{BitCheck}_{v,x}$（定义 8，其中，$v = v(\lambda)$），oldABE 是一个选择性安全的 ABE 体制，则在 $\text{RDLWE}_{n,q,\chi}$ 假设下，该 ABE 体制是半适应性安全的。

证明　下面通过一系列混合来规约证明该体制的安全性。

用 Adv[$\boldsymbol{A}$]表示 adversary 在安全性游戏中的优势。

Hybrid $\boldsymbol{H}_0$：该 Hybrid 与定义 5 中相同，故 $\text{Adv}_{\boldsymbol{H}_0}[\boldsymbol{A}] = \text{Adv}[\boldsymbol{A}]$。

Hybrid $\boldsymbol{H}_1$：在此 Hybrid 中，改变串 Δ 的构成。在 Hybrid $\boldsymbol{H}_0$ 中，$x_i^* \oplus \Delta_i = \text{PRF}(i)$，但在该 Hybrid 中，需要知道 x^* 来计算串 Δ。因此，在进行此 Hybrid 时，challenger 在回应密钥询问前要事先知道 x^*，而这与半适应性安全性相符，故有

$$|\text{Adv}_{\boldsymbol{H}_1}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_0}[\boldsymbol{A}]| = \text{negl}(\lambda)$$

Hybrid $\boldsymbol{H}_2$：在此 Hybrid 中，改变矩阵 $\vec{\boldsymbol{B}}$ 的生成方式。由于 $\vec{\boldsymbol{B}} = \boldsymbol{A}\vec{\boldsymbol{R}} + \sigma\vec{\boldsymbol{G}}$，根据陷门 $\boldsymbol{A}_\tau^{-1}$ 的性质且陷门已知，故有

$$|\text{Adv}_{\boldsymbol{H}_2}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_1}[\boldsymbol{A}]| = \text{negl}(\lambda)$$

Hybrid $\boldsymbol{H}_3$：在此 Hybrid 中，改变矩阵 $\boldsymbol{A}$ 的生成方式，均匀随机的从 R_q^m 上选取，而不是用算法 $\text{TrapEmbed}(1^n, q)$ 生成。因为 $\text{TrapEmbed}(1^n, q)$ 生成的 $\boldsymbol{A}$ 在统计意义上与从 R_q^m 上均匀随机选取得到的 $\boldsymbol{A}$ 不可区分，故有

$$|\text{Adv}_{\boldsymbol{H}_3}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_2}[\boldsymbol{A}]| = \text{negl}(\lambda)$$

Hybrid $\boldsymbol{H}_4$：在此 Hybrid 中，改变挑战密文运算过程中向量 $\boldsymbol{b}$ 和 $\boldsymbol{b}'$ 的生成方式，由 $\text{RDLWE}_{d,q,\chi}$ 假设可知

$$|\text{Adv}_{\boldsymbol{H}_4}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_3}[\boldsymbol{A}]| = \text{negl}(\lambda)$$

此外，由于 $\boldsymbol{b}'$ 是均匀随机的，且在计算过程中被 μ 的值混淆，故有

$$\text{Adv}_{\boldsymbol{H}_4}[\boldsymbol{A}] = \frac{1}{2}$$

综上所述有

$$|\text{Adv}[\boldsymbol{A}] - \frac{1}{2}| \leqslant |\text{Adv}_{\boldsymbol{H}_1}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_0}[\boldsymbol{A}]| + |\text{Adv}_{\boldsymbol{H}_2}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_1}[\boldsymbol{A}]| + |\text{Adv}_{\boldsymbol{H}_3}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_2}[\boldsymbol{A}]| + |\text{Adv}_{\boldsymbol{H}_4}[\boldsymbol{A}] - \text{Adv}_{\boldsymbol{H}_3}[\boldsymbol{A}]| = \text{negl}(\lambda)$$

体制的安全性得证。

3.4.3 效率

由于 RLWE 的优良性质，本文的 KP-ABE 体制在效率方面具有较好的性质。相比 Brakerski 和

Vaikuntanathan 基于 LWE 问题的 KP-ABE 体制[9]，本文体制将“gadget matrix” 由 Z_q 上 $n\times N(N=n\lceil\log q\rceil)$ 的矩阵转化为 R_q 上 $1\times n$ 的矩阵，并将 $\boldsymbol{A},\boldsymbol{B}_1,\cdots,\boldsymbol{B}_\eta,\boldsymbol{C}_1,\cdots,\boldsymbol{C}_l$ 这些 Z_q 上 $n\times N(N=n\lceil\log q\rceil)$ 的矩阵转化为 R_q 上 $1\times n$ 的矩阵。这些转化不仅减小了密钥和密文的尺寸，同时，有效地降低了体制的计算复杂度，而密钥尺寸过大一直以来都限制着 ABE 体制的实用性。此外，基于 RLWE 问题，环上多项式之间的乘法可以通过快速傅里叶变换来实现，这也会大大提升本文体制的效率和实用性。表 1 对本文 KP-ABE 体制和 BV 体制（参考文献[10]）的效率进行了对比。

表 1 效率对比

体制	加密复杂度	解密复杂度
BV	$O(n^3)$ 次乘法 $O(n)$次加法	$O(n^4)$ 次乘法 $O(n)$次加法
本文	$O(n)$次乘法 $O(n)$次加法	$O(n^2)$ 次乘法 $O(n)$次加法

表 2 密钥尺寸对比

体制	公钥尺寸	私钥尺寸
BV	$O(n^2)$	$O(n^2)$
本文	$O(n)$	$O(n)$

4 基于属性全同态加密体制

定义 9 基于属性全同态加密：一个基于属性全同态加密体制较之于属性加密体制会增加一个 Eval 算法。Eval 算法与某一个函数族 F 相关联。对于任意的 $f\in F$，$c\leftarrow\text{Eval}(mpk,x,f,c_1,\cdots,c_t)$ 表示在同一属性 x 标识下，对 f 作用在 $\{c_i\leftarrow\text{Enc}(\text{MPK},x,\mu_i)\}$ 上的结果的同态运算。

基于属性全同态加密体制的正确性[15]：对于任意的私钥 $sk_y\leftarrow\text{KeyGen}(msk,y)$ ($y\in\{0,1\}^k$)，对任意的 t 以及任意基于属性串 $x\in\{0,1\}^l$ 的密文 $\{c_i\leftarrow\text{Enc}(\text{MPK},x,\mu_i):i\in[t]\}$，在满足 $R(x,y)=1$ 时，对于任意的 t-ary 函数 $f\in F$，$c\leftarrow\text{Eval}(\text{MPK},x,f,c_1,\cdots,c_t)$ 满足 $\text{Dec}(sk_y,c)=f(\mu_1,\cdots,\mu_t)$。

ABFHE 体制的安全性与 ABE 体制相似，只是 Eval 算法可能会被 adversary 在实施攻击的过程中利用。

4.1 同态运算

在给出 ABFHE “编译器”的构造之前，首先给出本文 ABFHE 体制同态运算的定义。

1) 倍乘(c,α)。用一个常数 $\alpha\in R_q$ 来乘以一个密文 c，输出结果为 αc，即密文 c 的每个分量都乘以 α，由此可知错误也变为原来的 α 倍。

2) 加(c_1,c_2)。密文 c_1,c_2 相加，只需要将 2 个密文对应的矩阵进行相加即可。需要注意的是 2 个不同的密文错误取自同一个分布。

3) 乘(c_1,c_2)。密文 c_1,c_2 相乘首先要确保二者进行过相同次数的乘法，而且新生成密文的错误取决于原始错误。

显然对于任意一个函数 $f\in F$，都可以被上述 3 种运算进行刻画。因此，只要确保这 3 种运算实现同态性便可以将 ABE 体制转化为一个 ABFHE 体制。

受 Gentry[15]等启发，本文构造了一个编译器。满足该编译器要求的 ABE 体制都可以转化为一个 ABFHE 体制，具体见如下定理。

定理 3 具有如下性质的 ABE 体制能够转化为一个相应的 ABFHE 体制。

性质 1 密文和解密密钥向量：用 $\boldsymbol{y}$ 来表示一个谓词，解密密钥 $sk_{x,y}$，对于某个 m 密文 $c_x\in R_q^m$。$sk_{x,y}$ 的第一个系数为 1。

性质 2 点积：如果 c_x 是加密零向量后得到的密文，那么 $c_x sk_{x,y}$ 值接近零向量。

性质 3 安全性：加密零向量后得到的密文与 R_q 上均匀随机选取的向量不可区分。

如上所述，本文的 ABE 体制及其同态运算满足定理中列出的 3 条性质。因此，本文的 ABE 体制可以转化为一个 ABFHE 体制。

5 结束语

本文基于 RLWE 问题构造了一个 KP-ABE 体制，该体制支持长度不受限制的属性和半适应性安全，且较之以往的基于 LWE 问题的 KP-ABE 体制，具有更高的效率和更短的密钥尺寸。此外，本文最后构造了一个实现从 ABE 体制向 ABFHE 体制转化的编译器，利用该编译器能够将本文中的 ABE 体制转化为一个 ABFHE 体制。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// Interna-

tional Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2005:457-473.

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, 2006:89-98.

[3] AJTAI M. Generating hard instances of lattice problems (extended abstract)[C]//The 28th Annual ACM Symposium on Theory of Computing. ACM, 1996:99-108.

[4] AJTAI M, DWORK C. A public-key cryptosystem with worst-case/average-case equivalence[C]//STOC, ACM, 1997: 184-193.

[5] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2005, 56(6):84-93.

[6] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//40th ACM Symp. on Theory of Computing (STOC), Victoria, British Columbia, Canada, 2008: 197-206.

[7] BOYEN X. Attribute-based functional encryption on lattices[C]//TCC 2013. LNCS 7785, 2013: 122-142.

[8] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings [C]//Eurocrypt 2010. LNCS 6110, 2010: 1-23.

[9] DAN B, GENTRY C, GORBUNOV S, et al. Fully key-homomorphic encryption, arithmetic circuit abe and compact garbled circuits[M]// Advances in Cryptology-EUROCRYPT 2014. Springer Berlin Heidelberg, 2014:533-556.

[10] BRAKERSKI Z, VAIKUNTANATHAN V. Circuit-ABE from LWE: unbounded attributes and semi-adaptive security[EB/OL]. http://eprint.iacr.org/2016/118.pdf, 2016.7.15.

[11] 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.

[12] SERGEY G, VINOD V, HOETECK W. Attribute-based encryption for circuits[C]//STOC. 2013: 545-554.

[13] LYUBASHEVSKY V, PEIKERT C, REGEV O. A toolkit for ring-lwe cryptography[M]//Advances in Cryptology-Eurocrypt 2013. Springer Berlin Heidelberg, 2013: 35-54.

[14] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[M]// Advances in Cryptology-Eurocrypt 2012. Springer Berlin Heidelberg, 2012: 700-718.

[15] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees or how to delegate a lattice basis[J]. Journal of Cryptology, 2012, 25(4): 523-552.

作者简介：

孙泽栋（1992-），男，山东淄博人，解放军信息工程大学硕士生，主要研究方向为全同态加密、基于属性加密。

祝跃飞（1962-），男，浙江杭州人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为密码学、信息安全。

顾纯祥（1976-），男，安徽霍山人，博士，解放军信息工程大学副教授、硕士生导师，主要研究方向为密码学、网络与信息安全。

郑永辉（1976-），男，江西乐平人，博士，解放军信息工程大学讲师，主要研究方向为密码学、网络与信息安全。