基于容错学习的属性基加密方案的具体安全性分析

赵 建* 高海英 胡 斌
(解放军信息工程大学 郑州 450001)

摘 要：为了能全面研究基于容错学习(LWE)的属性基加密(ABE)方案的安全性，考察其抵抗现有攻击手段的能力，在综合考虑格上算法和方案噪声扩张对参数的限制后，利用已有的解决LWE的算法及其可用程序模块，该文提出了针对基于LWE的ABE方案的具体安全性分析方法。该方法可以极快地给出满足方案限制要求的具体参数及方案达到的安全等级，此外，在给定安全等级的条件下，该方法可以给出相应的具体参数值。最后，利用该方法分析了4个典型的基于LWE的属性基加密方案的具体安全性。实验数据表明，满足一定安全等级的基于LWE的属性基方案的参数尺寸过大，还无法应用到实际中。

关键词：属性基加密方案；具体安全性；容错学习
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)08-1779-08
DOI: 10.11999/JEIT180824

Analysis Method for Concrete Security of Attribute-based Encryption Based on Learning With Errors

ZHAO Jian GAO Haiying HU Bin
(*The PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: In order to comprehensively study the security of the Attribute-Based Encryption (ABE) scheme based on Learning With Errors (LWE) and test its ability to resist existing attacks, an analysis method for concrete security of ABE based on LWE is proposed. After consideration of the parameter restrictions caused by algorithms on lattices and noise expansion, this method applies the existing algorithms to solving LWE and the available program modules, and it can quickly provide the specific parameters that satisfy the scheme and estimate the corresponding security level. In addition, it can output the specific parameters that satisfy the pre-given security level. Finally, four existing typical schemes are analyzed by this method. Experiments show that the parameters are too large to be applied to practical applications.

Key words: Attribute-Based Encryption (ABE); Concrete security; Learning With Errors (LWE)

1 引言

2005年Sahai等人[1]提出了属性基加密体制(Attribute-Based Encryption, ABE)的概念。在该加密体制中，用户的身份用一系列描述性的属性表示，同时添加了一个灵活的访问结构，访问控制策略由访问结构的位置来决定，当用户的属性满足指定的访问结构时才能解密。1996年，Ajtai[2]首次将格(lattice)应用到密码学领域。基于格的密码系统很难被量子计算机攻破，具有较高的安全性。之后，文献[3]提出格上的容错学习(Learning With Errors, LWE)问题，并且证明该问题具有最坏情况下的困难性。在2010年，Lyubashevsky等人[4]首次提出环上容错学习问题(Learning With Errors over Ring, R-LWE)的概念，并将R-LWE问题的困难性规约到理想格上的近似最短向量问题。

在现有的基于格的ABE方案中，一般会给出安全性证明，即将方案的安全性规约到区分LWE(或R-LWE)上，能通过安全性证明的ABE方案，本文称其具有理论安全性。而本文主要研究基于LWE问题的ABE方案的具体安全性，即研究该类方案抵抗现有攻击手段的能力。实际上，方案的安全性由多个参数共同决定，如果参数规模过小，方案的安全性不能得到有效的保证；如果参数规模过大，又会导致密钥和密文规模过大，从而降低方案

收稿日期：2018-08-22；改回日期：2019-01-23；网络出版：2019-02-15
*通信作者： 赵建 back_zj@126.com
基金项目：国家自然科学基金(61702548, 61601515)，河南省基础与前沿技术课题(162300410192)
Foundation Items: The National Natural Science Foundation of China (61702548, 61601515), The Fundamental and Frontier Technology Research of Henan Province (162300410192)

的实现效率。那么在实际应用中构建一个具体的基于格的ABE方案时，如何选取合适的参数才能取得适当的安全性呢?目前，还没有针对基于格的ABE方案的具体安全性的普适性分析方法，而本文的主要研究目的就是为了解决这个问题。

为了解决上述问题，需要掌握现有的针对格上LWE问题的攻击算法。文献[5–7]对现有解决格上LWE(R-LWE)实例的算法进行了详细的研究和讨论。其中，文献[5]总结分析了现有的解决LWE实例的算法，并利用Sage软件编写了估算各类算法解决一个LWE实例所需时间复杂度的程序。

一般可以用参数n, q, α来刻画一个LWE实例。首先考虑参数n, q, α内部之间的关系，主要包括3点：(1)为了ABE方案能够正确解密，参数要满足由噪声扩张导致的限制函数；(2)方案的设计过程中，需要调用格上的采样算法，而这些采样算法对参数也有一定限制；(3)参数能否保证LWE问题的基本安全性。一般用安全参数λ来定义方案的具体安全性。在已知的各类解决LWE实例的算法中，分别给出了利用已有参数估算该算法时间复杂度的函数，本文利用该函数构建参数n, q, α和方案安全参数λ之间的关系设计了基于LWE问题的属性基加密方案具体安全性的分析方法。

本文的组织结构如下：第2节中介绍基础知识；第3节给出具体安全性的分析方法；第4节对多个方案的具体安全性进行分析；第5节总结全文。

2 基础知识

2.1 符号与基本定义

由于方案中使用的符号较多，首先简单说明文中涉及的符号定义，具体如表1所示。特别地，文中将$\log_2$简记为log。

由于篇幅限制，格、矩阵范数和LWE的定义这里不再给出，具体定义可以参考文献[8]。

2.2 格上的采样算法

设n, m为整数，q为素数。有如下3个多项式时间的算法：

表 1 符号定义

符号	意义	符号	意义
d	整数值	$\mathbb{Z}_q$	模q的剩余类环
$\boldsymbol{a}$	列向量$\boldsymbol{a}$	$\mathbb{Z}^{n\times m}$	$n\times m$整数矩阵集合
$\boldsymbol{A}$	矩阵$\boldsymbol{A}$	$\lceil q/2\rceil$	大于$q/2$的最小整数
$\boldsymbol{A}^{\mathrm{T}}$	矩阵$\boldsymbol{A}$的转置	$\lfloor q/2\rfloor$	小于$q/2$的最大整数
$\boldsymbol{A}\|\boldsymbol{B}$	矩阵$\boldsymbol{A}$和矩阵$\boldsymbol{B}$合并	$\Theta(n)$	渐进精确界记号
$\mathbb{Z}$	整数域	$\omega(n)$	非渐进紧下界记号
$\mathbb{R}$	实数域	$O(n)$	渐进上界记号

算法1[9] $\mathbf{TrapGen}(1^n, 1^m, q)\rightarrow(\boldsymbol{A}, \boldsymbol{T}_{\boldsymbol{A}})$

对于$m=\Theta(n\log q)$，输出满秩矩阵$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和格$\Lambda_q^{\perp}(\boldsymbol{A})$的基$\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}^{m\times m}$，其中矩阵$\boldsymbol{A}$接近随机分布，$||\tilde{\boldsymbol{T}}_{\boldsymbol{A}}||=O(\sqrt{n\log q})$，称$\boldsymbol{T}_{\boldsymbol{A}}$是矩阵$\boldsymbol{A}$的陷门矩阵。

算法2[10] $\mathbf{SampleD}(\boldsymbol{A}, \boldsymbol{T}_{\boldsymbol{A}}, \boldsymbol{U}, \sigma)\rightarrow\boldsymbol{X}$

在$\sigma=||\tilde{\boldsymbol{T}}_{\boldsymbol{A}}||\cdot\omega(\sqrt{\log m})$的情况下，输出一个取自分布$D_{\Lambda_q^{\boldsymbol{U}}(\boldsymbol{A}),\sigma}$的随机取样矩阵$\boldsymbol{X}\in\mathbb{Z}^{m\times k}$。

算法3[8] $\mathbf{RightSample}(\boldsymbol{A}, \boldsymbol{T}_{\boldsymbol{A}}, \boldsymbol{B}, \boldsymbol{P}, \sigma)\rightarrow\boldsymbol{K}$

输入满秩矩阵$\boldsymbol{A}, \boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$、格$\Lambda_q^{\perp}(\boldsymbol{A})$的基$\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$、一个随机矩阵$\boldsymbol{P}\in\mathbb{Z}_q^{n\times(h+n)}$和高斯参数$\sigma=||\tilde{\boldsymbol{T}}_{\boldsymbol{A}}||\cdot\omega(\sqrt{\log 2m})$。算法输出一个矩阵$\boldsymbol{K}\in\mathbb{Z}_q^{2m\times(h+n)}$使$(\boldsymbol{A}|\boldsymbol{B})\boldsymbol{K}=\boldsymbol{P}$成立。

2.3 LWE实例解法介绍

文献[5]总结了3种解决LWE实例的算法思路，下面分别进行简单的介绍。

第1种思路是有界距离解码(Bounded Distance Decoding, BDD)算法。给定m个取样$(\boldsymbol{w}_i, v_i)_{i\in[m]}$组成的$(\boldsymbol{W}, \boldsymbol{v}=\boldsymbol{W}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e})$，已知$\boldsymbol{e}$取自高斯分布，所以$\boldsymbol{v}$可以看作是在格点$\boldsymbol{W}^{\mathrm{T}}\boldsymbol{s}$的有界距离以内的点。由此，可以把LWE实例当作一个格上的BDD问题实例，即给定1个格的基，1个目标向量和目标向量至格的距离界限，找到1个与目标向量在距离界限之内的格向量。实际上，格点$\boldsymbol{W}^{\mathrm{T}}\boldsymbol{s}$就是上述BDD问题的解，再利用线性代数知识恢复向量$\boldsymbol{s}$，由此可解决搜索LWE问题。利用这种思路的解法简称为解码(Dec)算法。

第2种思路是短向量解法(Short Integer Solutions, SIS)。给定取样$(\boldsymbol{W}, \boldsymbol{v})$，利用由$\boldsymbol{W}$生成的对偶格$\Lambda_q^{\perp}(\boldsymbol{W})$中找到的短向量$\boldsymbol{b}$就可区分取样$(\boldsymbol{W}, \boldsymbol{v})$，其中格$\Lambda_q^{\perp}(\boldsymbol{W})=\{\boldsymbol{x}\in\mathbb{Z}_q^m, \text{ s.t. } \boldsymbol{W}\boldsymbol{x}=\boldsymbol{0}\,(\bmod q)\}$。计算$\langle\boldsymbol{b}, \boldsymbol{v}\rangle$，如果$(\boldsymbol{W}, \boldsymbol{v})$取自$\mathcal{O}_{\mathrm{s}}$，由格$\Lambda_q^{\perp}(\boldsymbol{W})$的定义，有$\langle\boldsymbol{b}, \boldsymbol{v}\rangle=\langle\boldsymbol{b}, \boldsymbol{W}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e}\rangle=\langle\boldsymbol{b}, \boldsymbol{e}\rangle$，则$\langle\boldsymbol{b}, \boldsymbol{v}\rangle$满足高斯分布；如果$(\boldsymbol{W}, \boldsymbol{v})$取自$\mathcal{O}_{\bar{\mathrm{s}}}$，$\langle\boldsymbol{b}, \boldsymbol{v}\rangle$满足随机分布。因此，如果能成功区分$\langle\boldsymbol{b}, \boldsymbol{v}\rangle$满足的分布，就能够有效地解决区分LWE问题。利用该思路的常见算法主要有格基规约算法、Blum-Kalai-Wasserman(BKW)算法和唯一最短向量(unique Shortest Vector Problem, uSVP)算法。

第3种思路是直接查找向量$\boldsymbol{s}$。通过找到合适的向量$\boldsymbol{s}$使得$||\boldsymbol{e}||=||\boldsymbol{v}-\boldsymbol{W}^{\mathrm{T}}\boldsymbol{s}||$足够小，这样就可以直接解决搜索LWE问题。利用该思路的算法主要有穷举搜索算法，文献[11]中提出了一种中间相遇(Meet In The Middle, MITM)算法，可以在一定程度上提升穷举搜索算法效率。

3　具体安全性分析方法

安全等级是衡量一个密码算法的通用评判标准，如果已知最好的攻击可以在2^n次操作内解决某个密码算法，那么这个密码算法可以称为拥有“n位的安全等级”。基于LWE的加密方案的整体安全性由安全等级λ来刻画，对于某选定的LWE算法，其计算时间与算法攻击优势ϵ之比等于2^{λ}[12]。如表2给出了密码算法的安全级别。

表 2　密码算法的安全级别

安全等级(2^n)	40	64	80	128	192	256
安全级别	薄弱(weak)	传统(legacy)	基准(baseline)	标准(standard)	较高(high)	超高(ultra)

一个LWE实例可以用参数n, q, α来刻画，在给出具体安全性分析方法前，首先从以下几点考虑参数内部关系。

(1) 参数之间的关系是否满足ABE方案涉及的格上采样算法的限制条件：在一个基于LWE的ABE方案中，主要参数有$n, m, \sigma, l, \alpha, q, \mathcal{X}_{\max}$等，可以根据方案调用的格上采样算法的参数要求，找到参数内部关系，即找到$m = m(n, q)$, $\sigma = \sigma(n, q)$, $\alpha = \alpha(n, q)$和$\mathcal{X}_{\max} = \mathcal{X}_{\max}(n, q)$。

(2) 参数之间的关系是否满足ABE方案正确解密所要求的限制条件：为了保证方案解密的正确性，会有限制噪声增长的判别式$\mathrm{Dis}(\cdot)$。将找到的参数关系代入具体判别式即可得到判别式$\mathrm{Dis}(n, q)$，再利用该判别式判断找到的参数是否满足方案要求。

(3) 参数之间的关系是否满足LWE问题的基本安全性。

最后，再考虑选定的参数是否能保证LWE问题的基本安全性，如将GapSVP问题规约到LWE问题[3]的参数要求，本文将该类判别式记为$\mathrm{fun}(n, q)$。

注：ABE方案均要求q为素数，因此还需要素性检测函数$\mathrm{pri}(\cdot)$。此外，记号AF(指代多个变量参数，如属性个数l、电路最大深度d等)作为额外变量因素进行单独讨论。

然后再考虑参数与ABE方案的安全等级之间的关系，文献[5,11,13,14]分别讨论了在2.3节中介绍的解决LWE实例的算法，并给出了与参数n, q, α及优势ϵ相关的计算时间复杂度的函数。因此，本文考虑采用MITM, BKW, Dual(格基规约算法)，Dec和uSVP5种典型算法，并分别计算针对固定参数的算法运行时间，选取其中的运算时间最小值作为本文设定参数的决定值。

在给定LWE实例的参数条件下，文献[5]给出了一个在Sage软件上运行的可以估算上述算法运行时间的模块，即可以实现各文献中关于计算时间复杂度函数的程序。实际上，在设计本文的分析方法时，可以直接利用函数来估算时间复杂度，但有些算法涉及的参数较多，作者在编写这个模块时根据经验对很多参数进行了一定的取舍，以保证结果接近实际运行时间。因此出于简便性的考虑，本文利用这个模块计算时间复杂度。

Sage模块输入参数n, q, α，输出时间rop(rop表示环操作(ring operation)次数)和算法优势ϵ(有些算法的优势已经预先选定)，由此可计算各个算法的安全等级。最后取其中的最小值计为最低安全等级λ。因此本文记输入为n, q, α，输出为最低安全等级λ的模块为$\lambda = \mathrm{es}(n, q, \alpha)$。

综合上述分析，设计了基于LWE问题的ABE方案具体安全性的分析方法。下面给出具体安全性分析方法1，该方法可以找到合适的参数，并估算方案的安全等级。

(1) 固定额外变量AF；

(2) 由格上采样算法要求，找到$m = m(n, q)$, $\sigma = \sigma(n, q)$, $\alpha = \alpha(n, q)$和$\mathcal{X}_{\max} = \mathcal{X}_{\max}(n, q)$；

(3) 利用方案判别式$\mathrm{Dis}(\cdot)$得到$\mathrm{Dis}(n, q)$；

(4) 从$n = 2^i (i = 7)$开始，到$i = 13$；

(5) 从$q = 1$开始；

(6) 由$\mathrm{pri}(q)$判断q是否为素数，否，执行$q++$，返回(6)；若是则执行；

(7) 判断$\mathrm{Dis}(n, q)$是否成立，否，执行$q++$，返回(6)；若成立，执行；

(8) 判断$\mathrm{fun}(n, q)$是否成立，否，执行$q++$，返回(6)；若成立，执行；

(9) 计算$\alpha = \alpha(n, q)$，并输出$\lambda = \mathrm{es}(n, q, \alpha)$，返回(4)。

注：在(4)中，考虑到实际应用中参数n的大小，可以选取i从7～13。实际上n的范围可以根据需要进行调节。在(5)中，可以适当提升q的初始值，以提升程序的实现效率。在(8)中，若q足够大时，$\mathrm{fun}(n, q)$仍不能成立，可以返回(4)。

再根据表2中特定安全等级λ'考虑如何为方案选取合适的参数。只需上述方法做简单的更改即可得到分析方法2：

(1) 由格上采样算法要求，找到$m = m(n, q)$,

$\sigma=\sigma(n,q)$, $\alpha=\alpha(n,q)$和$\mathcal{X}_{\max}=\mathcal{X}_{\max}(n,q)$；

(2) 利用方案判别式Dis$(\cdot)$得到Dis(n,q)；

(3) 循环AF中参数从最小值到所需大小；

(4) 从$n=1$开始；

(5) 从$q=1$开始；

(6) 由pri(q)判断q是否为素数，否，执行$q++$，返回(6)；若是则执行；

(7) 判断Dis(n,q)是否成立，否，执行$q++$，返回(6)；若成立，执行；

(8) 判断fun(n,q)是否成立，否，执行$q++$，返回(6)；若成立，执行；

(9) 计算$\alpha=\alpha(n,q)$，并输出$\lambda=\mathrm{es}(n,q,\alpha)$，返回(4)；

(10) 判断$\lambda\approx\lambda'$，否，则返回(4)；若成立，输出n,m,q,α并返回(3)。

4 方案具体安全性分析

4.1 基于格的支持电路结构的属性基加密方案具体安全性分析

为了便于理解第3节给出的具体安全性分析方法，本节利用分析方法1和方法2分析文献[15]中的方案，并详细分析各步中的实验数据结果。

4.1.1 方案简述

文献[15]给出的ABE方案由如下4个算法组成：

算法1 **Setup**$(1^\lambda,l,d)\to(\mathrm{PP},\mathrm{MSK})$：算法输入安全参数$\lambda$，电路输入个数$l$和电路的最大深度$d$(电路根节点记作第0层)。利用**TrapGen**算法生成部分公参矩阵和主密钥，最后输出公钥$\mathrm{PP}=\{\{\boldsymbol{A}_i^0\in\mathbb{Z}_q^{n\times m},\boldsymbol{A}_i^1\in\mathbb{Z}_q^{n\times m}\}_{i\in[l]},\boldsymbol{D}\in\mathbb{Z}_q^{n\times m}\}$和主密钥$\mathrm{MSK}=\{\boldsymbol{T}_i^0\in\mathbb{Z}_q^{m\times m},\boldsymbol{T}_i^1\in\mathbb{Z}_q^{m\times m}\}_{i\in[l]}$。

算法2 **Enc**$(\mathrm{PP},\boldsymbol{x},\boldsymbol{m})\to\mathrm{CT}$：算法输入PP，属性集合$\boldsymbol{x}=(x_1,x_2,\cdots,x_l)\in\{0,1\}^l$，明文消息$\boldsymbol{m}\in\{0,1\}^m$。输出密文$\boldsymbol{c}_i=(\boldsymbol{A}_i^{x_i})^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e}_i \mod q$和$\boldsymbol{c}=\boldsymbol{D}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{e}+\boldsymbol{m}\cdot\lfloor q/2\rfloor \mod q$，其中$\boldsymbol{e}_i$, $\boldsymbol{e}$是取自离散高斯分布的噪声向量。

算法3 **KeyGen**$(\mathrm{MSK},f)\to\mathrm{SK}_f$：算法输入主密钥MSK和电路访问结构$f$。定义节点$\omega\in[l+1,l+r]$有两个子节点$u_1(\omega)$和$u_2(\omega)$。

(1) 分别计算$\boldsymbol{L}_\omega^{a,b}\leftarrow\mathbf{RightSample}(\boldsymbol{A}_{u_1(\omega)}^a|\boldsymbol{A}_{u_2(\omega)}^b,\boldsymbol{T}_{u_1(\omega)}^a,\boldsymbol{A}_\omega^{g(a,b)},\sigma)$和$\boldsymbol{L}_H\leftarrow\mathbf{SampleD}(\boldsymbol{A}_{l+r}^1,\boldsymbol{T}_{l+r}^1,\boldsymbol{D},\sigma)$。

(2) 输出密钥$\mathrm{SK}_f=\{\boldsymbol{K}_H=\boldsymbol{L}_H\in\mathbb{Z}_q^{m\times m},\{\boldsymbol{K}_\omega=\boldsymbol{L}_\omega^{a,b}\in\mathbb{Z}^{2m\times m}\}_{l+1\le\omega\le l+r}\}$。

算法4 **Dec**$(\mathrm{SK}_f,\mathrm{CT})\to\boldsymbol{m}$：算法输入密钥$\mathrm{SK}_f$和密文CT。如果用户属性集合$\boldsymbol{x}$满足访问结构$f$，则输出消息$\boldsymbol{m}$。

4.1.2 方案安全参数具体分析结果

下面给出文献[15]中方案的参数要求，如引理1所示。

引理1 在文献[15]的方案中，参数需满足如式(1)所示关系。

$$\left.\begin{aligned}&m=\lceil 2n\log q\rceil,\sigma=\sqrt{2m}\cdot\log m\\&\alpha=2\sqrt{\pi m}\cdot\log m/q\\&\mathcal{X}_{\max}=q\alpha\sqrt{m}\log m+\sqrt{m}/2\end{aligned}\right\}\tag{1}$$

同时，为了保证方案的正确性，上述参数还需要满足判别式Dis$(\cdot)$

$$2\left(\sigma\cdot\sqrt{2m}\right)^{d+1}\cdot\mathcal{X}_{\max}\le q/4\tag{2}$$

其中，参数d表示电路深度并作为额外变量AF。

证明 在方案算法1中调用了格上的算法**TrapGen**，算法**TrapGen**要求$m=\Theta(n\log q)$，实验中选取$m=m(n,q)$: $m=\lceil 2n\log q\rceil$。

在方案算法3中，方案调用了算法**SampleD**和算法**RightSample**，算法**SampleD**要求$\sigma=||\tilde{\boldsymbol{T}}_{\boldsymbol{A}}||\cdot\omega(\sqrt{\log m})$，算法**RightSample**要求$\sigma=||\tilde{\boldsymbol{T}}_{\boldsymbol{A}}||\cdot\omega(\sqrt{\log 2m})$。在该方案中，实验选择$\sigma=||\tilde{\boldsymbol{T}}_{\boldsymbol{A}}||\cdot\omega(\sqrt{\log 2m})=O(\sqrt{n\log q})\cdot\omega(\sqrt{\log 2m})$($||\tilde{\boldsymbol{T}}_{\boldsymbol{A}}||$由算法**SampleD**可得)。可以取$\sigma\ge 2\sqrt{m/2}\cdot\log m=\sqrt{2m}\cdot\log m$，实验选择$\sigma=\sigma(m)$: $\sigma=\sqrt{2m}\cdot\log m$。

在离散高斯分布中，$\sigma=\alpha q/\sqrt{2\pi}$表示标准差，根据$\sigma$定义，有$\alpha=\alpha(m,q)$: $\alpha=2\sqrt{\pi m}\cdot\log m/q$。

$\mathcal{X}_{\max}$是指特定分布X(一般使用离散高斯分布)中所有向量l_2范数的上确界，即在分布$\mathcal{X}$中任取一个向量$\boldsymbol{e}$，都有$||\boldsymbol{e}||\le\mathcal{X}_{\max}$成立。实验取$\mathcal{X}_{\max}=\mathcal{X}_{\max}(m,\alpha,q)$: $\mathcal{X}_{\max}=q\alpha\sqrt{m}\log m+\sqrt{m}/2$。此时有$||\boldsymbol{e}||\le\mathcal{X}_{\max}$成立，该结论用到了引理2。

再根据方案[15]中对方案正确性的分析，当且仅当方案参数满足判别式Dis$(\cdot)$: $2(\sigma\cdot\sqrt{2m})^{d+1}\cdot\mathcal{X}_{\max}\le q/4$时，用户才能够正确解密。由前式关系可以轻易得到判别式Dis(n,q)。

引理2[8] 现有模数q，向量$\boldsymbol{y}\in\mathbb{Z}^m$和$\boldsymbol{e}$取自分布$\mathcal{X}(\overline{\Psi}_\alpha{}^m)$，则$|\boldsymbol{y}^{\mathrm{T}}\boldsymbol{e}|$作为区间$[0,q-1]$中的整数以极大的优势满足

$$|\boldsymbol{y}^{\mathrm{T}}\boldsymbol{e}|\le||\boldsymbol{e}||q\alpha\omega(\sqrt{\log m})+||\boldsymbol{e}||\sqrt{m}/2\tag{3}$$

此外，作为一种特殊情况，任取$e\leftarrow\mathcal{X}$有$|e|\le q\alpha\omega(\sqrt{\log m})+1/2$。

再根据规约LWE问题的困难性，当满足关系式fun(n,q): $\alpha q>2\sqrt{n}$时，可以将GapSVP问题规约到LWE问题[3]，由引理1中α的定义，关系式

$\alpha q > 2\sqrt{n}$已经满足。

利用引理1的结论得到分析方法1的第(2)步和第(3)步，且由第(2)步设置的参数大小知第(7)步的判别式一直成立。

找到参数间的关系后，下面开始估算确定参数条件下方案的安全等级。在具体实验中，先固定额外变量AF。表3给出了分析方法1第(4)步中的一个循环的实验结果，即在固定$d=1, n=64$时参数和最低安全等级的关系，表3中数据抽样展示了比较有代表性的结果(当$q \approx n^c$时，c是一个常数)。分析方法1在第(5)步中尝试不同的q，由判别式Dis(·)形式可知，总能找到足够大的q使得参数满足式Dis(·)。

表3说明在固定电路深度d和参数n后，单纯地增大q对提升安全等级的影响不大，但会极大地降低方案的实现效率。

表4展示了分析方法1总的实验结果。表4说明扩大参数n可以有效地提升方案的安全等级，n值超过1275时，方案安全等级提升速度很快。

最后，利用分析方法2来讨论在达到方案基准安全等级$\lambda' \approx 80$时电路深度d与方案参数的关系。表5给出了方案在达到基准安全等级$\lambda' \approx 80$时方案可以设置的参数，表中实验数据表明电路深度会极大地影响方案参数的设置，当电路深度超过16时，参数n达到5位数的级别。

表 3　d, n=64时参数和最低安全等级λ的关系

c	q	$\log q \approx$	m	Dis(·)?	λ
8	281474976710677	48	6144	否	–
11	73786976294838206459	66	8448	是	30.6
16	79228162514264337593543950319	96	12288	是	31.1
32	627710173538668076383578942320766641610235544446403451 3029	192	24576	是	32.0
64	394020061963944792122790401001436138050797392704654466679482934042457217 7149721061141426625488491564080662799030704 7	384	48727	是	32.9

表 4　d= 1时参数和最低安全等级λ的关系

n	c	q	$\log q \approx$	m	Dis(·)?	α	λ
128	8	72057594037927931	56	14336	否	–	–
	10	1180591620717411303449	70	17920	是	6.01e–18	31.8
512	7	9223372036854775783	63	64512	否	–	–
	8	4722366482869645213711	72	73728	是	3.30e–18	35.1
1024	7	1180591620717411303449	70	143360	否	–	–
	8	1208925819614629174706189	80	163840	是	2.10e–20	60.1
1275	7	5477360094305419921879	72	184146	否	–	–
	8	6983634120239410400390599	83	210452	是	4.11e–21	81.3
4096	6	4722366482869645213711	72	589824	否	–	–
	7	1934281311383406679529 8819	84	688128	是	2.95e–21	636.7

表 5　达到基准安全等级$\lambda' \approx 80$时方案的参数

d	n	$\log q \approx$	m	α
1	1275	82.5	210452	4.11e–21
2	1375	104.3	286694	1.42e–27
4	2925	161.2	943015	2.04e–44
8	5500	285.8	3143580	1.27e–81
16	11000	537.0	1181490	6.32e–157

4.1.3　方案数据量

考虑方案的实用性时，就不得不考虑方案的数据量大小。以下是文献[15]中方案的公钥、主密钥、密文和密钥的数据量。

公钥

$$(2l+1)(n\times m)\lceil\log q\rceil \le (2\times 2^d+1)(n\times m)\lceil\log q\rceil = (2^{d+1}+1)(2n^2\log q)\lceil\log q\rceil \tag{4}$$

主密钥

$$2l(m\times m)\lceil\log q\rceil \le 2\times 2^d(m\times m)\lceil\log q\rceil = 2^{d+1}(4n^2\log^2 q)\lceil\log q\rceil \tag{5}$$

密文

$$(l+1)m\lceil\log q\rceil \le (2^d+1)m\lceil\log q\rceil = (2^d+1)(2n\log q)\lceil\log q\rceil \tag{6}$$

密钥

$$\begin{aligned}&((m\times m)+r(2m\times m))\lceil\log q\rceil\\&<((m\times m)+2^d(2m\times m))\lceil\log q\rceil\\&=(1+2^{d+1})4n^2\log^2 q\lceil\log q\rceil\end{aligned}\tag{7}$$

电路的最大深度d(根节点计为第0层)决定了电路中的最大输入个数l，这里取$l=2^d$。利用表5的数据(安全级别达到80)可以得到方案公钥、主密钥、密文和密钥的最大数据量，具体如表6。

表 6 方案数据量大小(GB)

d	公钥	主密钥	密文	密钥
1	12.96	1719.55	0.006098	2138.19
2	43.39	8044.95	0.017530	9050.57
4	1716.67	536681.89	0.302340	553453.20
8	295332.43	168482949.37	26.900739	168812017.63
16	1064847265.92	1143637238342.29	48402.517727	1143645963601.98

表6中的实验数据表明该方案距实际应用还有一定距离，如在电路深度$d=1$时，方案只有密文量较小，需要传输的密钥量和公钥量太大，但方案1次可以加密210452 bit的数据，是其优势之一。但在电路深度扩大时，密钥量和公钥量会极速扩大，如在$d=1$和$d=16$时相比，明文数据量提升了只有大约5倍，但公钥量提升了大约82164140倍，密钥量提升了大约534913921倍。

4.2 典型ABE方案的具体安全性分析

根据上节对方案的参数分析步骤，本文分别对文献[9,16,17]中的方案进行了分析。

类似于引理1，在文献[9]中，设置$m=\lceil 2n\log q\rceil$，$\sigma=\sqrt{5}(2m+1)\cdot\log m$，$\alpha=\sqrt{10\pi}(2m+1)\cdot\log m/q$ 和$\mathcal{X}_{\max}=q\alpha\sqrt{m}\log m+\sqrt{m}/2$，判别式Dis$(\cdot)$为$1+2m\sigma(\alpha_F+1)<q/4\mathcal{X}_{\max}$，其中$\alpha_F(n)=(\beta(m))^d\cdot 20\sqrt{m}$, $\beta(m)=2(p^k-1)m/(p-1)$(或$\beta(m)=2km$，这里取二者的最大值)，$p<q$表示电路中乘法门输入的上限，k表示电路门的输入个数，d表示电路深度。本文将参数d,k和p作为额外变量AF。

在文献[16]中，设置$m=\lceil 1+\log q\rceil^2$，$\sigma=\sqrt{nm\log q}\log^2 m$，$\alpha=\sqrt{2nm\pi\log q}\log^2 m/q$和$\mathcal{X}_{\max}=q\alpha\sqrt{n}\log n+\sqrt{n}/2$，判别式Dis$(\cdot)$为$q\geq 4(2Y^2(d+1)nm^2\sigma\mathcal{X}_{\max}t+Yx_0)$，其中参数$Y=(r!)^2$, r表示属性个数，$d=r$表示虚拟属性个数，t为一常数，$x_0<\mathcal{X}_{\max}$。本文将参数r作为额外变量AF。

在文献[17]中，设置$m=6\lceil(n+1)\log q+\log^2 n\rceil$, $\sigma=m\cdot\log m$, $\alpha=(m\cdot\log m\cdot\sqrt{m}(20\sqrt{m}+1)(l+1)((2l)!)^4\cdot m)^{-1}$和$\mathcal{X}_{\max}=q\alpha\log m+1/2$，判断式Dis$(\cdot)$为$\sigma q\alpha\sqrt{m}(s_R+1)(l+1)((l+d)!)^4\cdot m+\sigma m(s_R+1)(l+1)((l+d)!)^4<q/5$，其中$s_R\leq 20\sqrt{m}$，虚拟参数个数$d=l$, l表示参数个数，s表示高斯参数σ。本文将参数l作为额外变量AF。

利用分析方法1研究各方案中参数和最低安全等级λ的关系，结果如表7所示。

在表7额外变量因素AF中，文献[9]分别固定电路深度$d=1$，门输入最大个数$k=2$和输入上限$p=10$，文献[16]方案中固定总属性个数$r=2$，文献[17]中固定属性个数$l=3$。表6数据表明在$n=128$时，3个方案达到的安全等级是很接近的，但当n逐渐增大时，文献[16]安全等级增长最快，文献[17]增长速度最慢。考虑到文献[9]的访问结构是算术电路，而文献[16,17]均为门限结构，所以文献[16,17]的数据较有比较意义。

下面给出在如上固定额外变量因素AF的条件下，各方案在达到基准安全等级$\lambda'\approx 80$时参数的大小。

表8数据表明在达到基准安全等级时，文献[16]参数n和m值较[17]有优势，但q值更大。

最后利用表8的数据可以得到方案公钥、密文和密钥的最大数据量，具体如表9。表9数据表明在达到基准安全等级时，文献[16]与文献[17]相比，密钥量和密文量扩大了10倍左右，但公钥量缩减了300多倍。相较之下，文献[16]有更高的实际应用价值。

经过对上述多个方案的分析，可以看到现有基于LWE的ABE方案的参数的大小距离实际应用都有较大的差距。类似地，根据文献[8]的分析结果，现有的基于格的全同态加密方案在达到一定安全等级的情况下，参数规模也非常大，并不能满足实际应用的需求。

5 结束语

本文对基于LWE的ABE方案的具体安全性进

表 7　方案中参数和最低安全等级λ的关系

方案	AF	n	$\log q \approx$	m	α	λ
文献[9]	$d=1$	128	103	26368	4.28e–25	32.5
	$k=2$	1024	120	245760	3.71e–29	40.6
	$p=10$	4096	132	1081344	4.46e–32	335.3
文献[16]	$r=2$	128	93	8836	4.46e–22	31.9
		1024	102	10609	2.94e–24	50.3
		4096	108	11881	1.03e–25	511.2
文献[17]	$l=3$	128	87	67632	2.91e–28	31.7
		1024	96	591000	3.48e–31	37.8
		4096	101	2483646	4.18e–33	185.8

表 8　方案达到基准安全等级$\lambda' \approx 80$时方案的参数

方案	n	$\log q \approx$	m	α
文献[9]	1750	125	437500	2.16e–30
文献[16]	1380	104	11024	8.86e–25
文献[17]	2500	99	1486359	2.03e–32

表 9　方案数据量大小(GB)

方案	公钥	密文	密钥
文献[9]	44.5652	0.0255	5570.6550
文献[16]	1.1012	1.8354	1.4683
文献[17]	342.6093	0.1370	0.2056

行了分析研究。文中提出两个分析方法：分析方法1可以高效地给出满足ABE方案限制要求的参数，并能估算出该具体参数对应的ABE方案的安全等；分析方法2在给定安全等级的条件下，可以给出满足该安全等级的具体参数值。对多个方案实验的数据表明，满足一定安全等级的基于LWE的ABE方案的参数尺寸过大，还无法应用到实际中。下一步工作就是考虑如何降低方案中的噪声扩张程度，扩大参数的选择范围。

参 考 文 献

[1] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[2] AJTAI M. Generating hard instances of lattice problems (extended abstract)[C]. The 28th Annual ACM Symposium on Theory of Computing, Philadelphia, Pennsylvania, USA, 1996: 99–108. doi: 10.1145/237814.237838.

[3] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]. The 37th Symposium on Theory of Computing, Baltimore, USA, 2005: 84–93. doi: 10.1145/1060590.1060603.

[4] LYUBASHEVSKY V, PEIKERT C, and REGEV O. On ideal lattices and learning with errors over rings[J]. *Journal of the ACM*, 2010, 60(6): 43. doi: 10.1145/2535925.

[5] ALBRECHT M R, PLAYER R, and SCOTT S. On the concrete hardness of learning with Errors[J]. *Journal of Mathematical Cryptology*, 2015, 9(3): 169–203. doi: 10.1515/jmc-2015-0016.

[6] BECKER A, DUCAS L, GAMA N, *et al*. New directions in nearest neighbor searching with applications to lattice sieving[C]. The Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, Arlington, Virginia, 2016: 10–24. doi: 10.1137/1.9781611974331.ch2.

[7] SCHNEIDER M. Sieving for shortest vectors in ideal lattices[C]. The 6th International Conference on Cryptology in Africa, Cairo, Egypt, 2013: 375–391. doi: 10.1007/978-3-642-38553-7_22.

[8] AGRAWAL S, BONEH D, and BOYEN X. Efficient lattice (H)IBE in the standard model[C]. The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, France, 2010: 553–572. doi: 10.1007/978-3-642-13190-5_28.

[9] BONEH D, NIKOLAENKO V, and SEGEV G. Attribute-based encryption for arithmetic circuits[EB/OL]. http://eprint.iacr.org/2013/669, 2013.

[10] CHEN Yuanmi and NGUYEN P Q. BKZ 2.0: Better lattice security estimates[C]. The 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, 2011: 1–20. doi: 10.1007/978-3-642-25385-0_1.

[11] BAI Shi and GALBRAITH S D. Lattice decoding attacks on binary LWE[C]. The 19th Australasian Conference on Information Security and Privacy, Wollongong, NSW, Australia, 2014: 322–337. doi: 10.1007/978-3-319-08344-5_21.

[12] PAAR C and PELZL J. Understanding Cryptography: A Textbook for Students and Practitioners[M]. Berlin Heidelberg: Springer, 2010: 156.

[13] LINDNER R and PEIKERT C. Better key sizes (and attacks) for LWE-based encryption[C]. The Cryptographers' Track at the RSA Conference 2011 Topics in Cryptology, San Francisco, USA, 2011: 319–339. doi: 10.1007/978-3-642-19074-2_21.

[14] ALBRECHT M R, CID C, FAUGèRE J, *et al*. On the complexity of the BKW algorithm on LWE[J]. *Designs, Codes and Cryptography*, 2015, 74(2): 325–354. doi: 10.1007/s10623-013-9864-x.

[15] ZHAO Jian, GAO Haiying, and ZHANG Junqi. Attribute-based encryption for circuits on lattices[J]. *Tsinghua Science and Technology*, 2014, 19(5): 463–469. doi: 10.3969/j.issn.1007-0214.2014.05.005.

[16] 赵建, 高海英, 胡斌. 基于理想格的高效密文策略属性基加密方案[J]. 电子与信息学报, 2018, 40(7): 1652–1660. doi: 10.11999/JEIT170863.

ZHAO Jian, GAO Haiying, and HU Bin. An efficient ciphertext-policy attribute-based encryption on ideal lattices[J]. *Journal of Electronics & Information Technology*, 2018, 40(7): 1652–1660. doi: 10.11999/JEIT170863.

[17] ZHANG Jiang, ZHANG Zhenfeng, and GE Aijun. Ciphertext policy attribute-based encryption from lattices[C]. The 7th ACM Symposium on Information, Computer and Communications Security, Seoul, Korea, 2012: 16–17. doi: 10.1145/2414456.2414464.

赵 建：男，1989年生，博士生，研究方向为公钥密码的设计与分析.

高海英：女，1978年生，教授，博士生导师，研究方向为密码算法的设计与分析.

胡 斌：男，1971年生，教授，博士生导师，研究方向为密码算法的设计与分析.