Hindawi
Security and Communication Networks
Volume 2018, Article ID 4957045, 9 pages
https://doi.org/10.1155/2018/4957045

Research Article

Cryptanalysis of Compact-LWE and Related Lightweight Public Key Encryption

Dianyan Xiao [1] **and Yang Yu** [2]

[1] *Institute for Advanced Study, Tsinghua University, Beijing 100084, China*
[2] *Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*

Correspondence should be addressed to Yang Yu; y-yl3@mails.tsinghua.edu.cn

Received 15 December 2017; Revised 14 January 2018; Accepted 28 January 2018; Published 11 March 2018

Academic Editor: Ilsun You

In the emerging Internet of Things (IoT), lightweight public key cryptography plays an essential role in security and privacy protection. With the approach of quantum computing era, it is important to design and evaluate lightweight quantum-resistant cryptographic algorithms applicable to IoT. LWE-based cryptography is a widely used and well-studied family of postquantum cryptographic constructions whose hardness is based on worst-case lattice problems. To make LWE friendly to resource-constrained IoT devices, a variant of LWE, named Compact-LWE, was proposed and used to design lightweight cryptographic schemes. In this paper, we study the so-called Compact-LWE problem and clarify that under certain parameter settings it can be solved in polynomial time. As a consequence, our result leads to a practical attack against an instantiated scheme based on Compact-LWE proposed by Liu et al. in 2017.

1. Introduction

The Internet is changing from a network of conventional computers to a network of smart objects, that is, "things," including vehicles, electronics, implantable medical devices, and sensors. The trend of Internet of Things (IoT) makes the Internet more ubiquitous, but it simultaneously brings a series of challenges, such as monitoring [1], communication [2], and management [3]. Among all these challenges, security [4–6] is currently listed as a top concern. As the theoretical basis, cryptographic algorithms play a key role in achieving data confidentiality and integrity, authentication, and other security needs in IoT.

Currently, RSA and ECC cryptosystems have been implemented efficiently on resource-constrained devices [7, 8], which provides desirable security for IoT applications. However, these public key schemes are based on integer factorization or discrete logarithms, which are fragile under quantum cryptanalysis. To defense quantum attacks, NIST has launched the postquantum cryptography standardization. Lattice-based cryptography is viewed as a very promising postquantum alternative to classical cryptography due to its strong security guarantee, great performance and powerful functionality. It is becoming increasingly important to design and evaluate practical schemes based on well-studied lattice problems.

The *Learning With Errors* (LWE) problem, introduced by Regev [9], is one of the most popular lattice problems for cryptographic applications [10–13]. An LWE instance consists of a random matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ and a vector $\mathbf{b} = \mathbf{As} + \mathbf{e} \bmod q$, where the secret $\mathbf{s} \in \mathbb{Z}_q^n$ and the error $\mathbf{e} \in \mathbb{Z}^m$ are sampled from a certain distribution. The decision LWE problem is to distinguish the distribution of LWE instances from the uniform distribution over $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, while the search version is to recover the secret $\mathbf{s}$ from LWE instances. In [9], the average-case LWE is proved as hard as certain worst-case lattice problems, which provides a solid theoretical grounding for LWE-based schemes.

However, LWE-based schemes are usually not efficient in practice. It seems infeasible to apply regular LWE-based cryptographic constructions to IoT directly, due to the constrained computing environments of smart devices. Thus it is critical to refine existing algorithms or develop new LWE-based cryptographic schemes for security protection using limited resources. So far, there are mainly two optimization

strategies: (1) introducing extra algebraic structures and (2) reducing the sizes of matrix or vector elements. Following the first one, some LWE variants, such as Ring-LWE [14] and Module-LWE [15], were developed and led to many practical schemes [16–18] and efficient implementations [19, 20]. Following the second strategy, some variants were proposed as well, including LWE with short secret or error [21–23] and LWE with compact matrix [24, 25]. Then, related cryptanalyses [26–29] provided concrete security estimations for the schemes based on these variants.

A recent instantiation of LWE-based encryption scheme with particularly aggressive parameter was proposed by Liu et al. [25] and presented as an invited talk at ACISP 2017 conference. The scheme is based on the so-called Compact-LWE and designed especially for resource-constrained IoT devices. As shown by experimental results, the scheme indeed achieves an excellent performance on small IoT devices. Subsequently, Bootle and Tibouchi gave a cryptanalysis of this scheme [29] by recovering the nonce in the encryption process with the help of lattice embedding technique. They pointed out that the security level was much lower than [25] claimed.

We took an insight into the Compact-LWE problem, an LWE variant with the random $\mathbf{A}$ selected from a small range, and discovered that two q-ary lattices defined by $\mathbf{A}$ have reduced bases of special patterns. We proved that the Compact-LWE problem can be solved in polynomial time under certain parameters, which is applied to analyze two concrete lightweight public key schemes proposed in [24, 25], respectively. We failed to attack the scheme of [24] due to its moderate parameters and successfully recovered plaintexts with 100% probability and within a very short time for the encryption scheme in [25]. Compared with the attack against the scheme of [25] in [29], our attack follows a different method and can be used to analyze general cryptographic constructions based on this kind of LWE variant.

The article is organized as follows. In Section 2, we recall some notations and basic facts used in our discussion. In Section 3, we introduce Compact-LWE and present our analysis. We describe a concrete attack against related Compact-LWE-based schemes in Section 4 and conclude in Section 5.

2. Preliminaries

2.1. Notations. For any positive integer q, we identify $\mathbb{Z}_q$ with the set $\{0, \ldots, q-1\}$. We denote by $[x]_q$ the remainder of x divided by q in $\mathbb{Z}_q$ and by $[x]_q$ the remainder in $\{-\lceil q/2\rceil, \ldots, q-1-\lceil q/2\rceil\}$. Let $\langle\cdot,\cdot\rangle$ and $\|\cdot\|$ be the Euclidean inner product and norm, respectively. The elements of $\mathbb{R}^m$ are viewed as column vectors. For any point $\mathbf{t} \in \mathbb{R}^m$ and $r > 0$, we denote by $\mathcal{B}_m(\mathbf{t}, r)$ the m-dimensional ball of radius r centered at $\mathbf{t}$.

2.2. Probability and Statistics. Let χ be a distribution over a discrete domain E. We write $X \hookleftarrow \chi$ to represent the random variable X that is sampled from the distribution χ. For a finite domain E, we denote by $U(E)$ the uniform distribution over E.

A function $f(n)$ is *negligible*, if $f(n) = o(n^{-c})$ for every fixed constant c. We generally denote by $\mathrm{negl}(n)$ as a negligible function with respect to n. We say that a probability is *overwhelming* if it is $1 - \mathrm{negl}(n)$, and a probability is *nonnegligible* if it is $\omega(n^{-c})$ for some constant c.

Definition 1. Given a distribution χ over $\mathbb{Q}^m$, we say that χ is (α, β)-confidence with respect to λ, if $\Pr[\|X\| \geq \alpha] \leq \mathrm{negl}(\lambda)$ and $\Pr[\|X\| \leq \beta] \geq 1/\mathrm{poly}(\lambda)$ for $X \hookleftarrow \chi$.

The parameter α describes an overwhelming confidence interval for χ with respect to λ, while β describes a nonnegligible confidence interval.

2.3. Lattices. A *lattice* $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^m$ and generated by a set of linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$, that is, $\mathcal{L} = \{\sum_{i=1}^n x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \text{ for any } i\}$. We call $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m\times n}$ a *basis* of $\mathcal{L}$ and write $\mathcal{L}$ as $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ or $\mathcal{L}(\mathbf{B})$. The integer n is called the *rank* of $\mathcal{L}$. For any unimodular matrix $\mathbf{U} \in \mathbb{Z}^{n\times n}$, $\mathbf{BU}$ is also a basis of $\mathcal{L}$. The *span* of $\mathcal{L}$, denoted by $\mathrm{span}(\mathcal{L})$, is the linear space spanned by its basis. The first minimum of a lattice $\mathcal{L}$ is defined as $\lambda_1(\mathcal{L}) := \min_{\mathbf{v}\in\mathcal{L}\setminus\{\mathbf{0}\}}\|\mathbf{v}\|$.

We denote by $\mathbf{B}^* = (\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$ the *Gram-Schmidt orthogonalization* of $\mathbf{B}$ where $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$ and $\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^*\rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^*\rangle$. The *volume* of $\mathcal{L}$ is defined as $\mathrm{vol}(\mathcal{L}) = \prod_{i=1}^n \|\mathbf{b}_i^*\|$ that is an invariant of $\mathcal{L}$ and independent of the choice of the basis.

The *dual* lattice of $\mathcal{L}$ is $\mathcal{L}^* := \{\mathbf{y} \in \mathrm{span}(\mathcal{L}) \mid \langle \mathbf{x}, \mathbf{y}\rangle \in \mathbb{Z}, \forall \mathbf{x} \in \mathcal{L}\}$. If $\mathbf{B}$ is a basis of $\mathcal{L}$, it is known that $\mathbf{D} = \mathbf{B}(\mathbf{B}^T\mathbf{B})^{-T}$ is a basis of $\mathcal{L}^*$. Furthermore, we have the following relation between the Gram-Schmidt orthogonalization of a basis and its dual.

Lemma 2. *Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an ordered basis of lattice $\mathcal{L}$ and $(\mathbf{d}_1, \ldots, \mathbf{d}_n)$ be its dual basis in reverse order (i.e., $\langle \mathbf{d}_i, \mathbf{b}_j\rangle = \delta_{i,n+1-j}$ where $\delta_{i,j}$ denotes Kronecker delta). Then $\mathbf{d}_i^* = \mathbf{b}_{n+1-i}^*/\|\mathbf{b}_{n+1-i}^*\|^2$ for $i = 1, \ldots, n$.*

Given a lattice $\mathcal{L}$ and a "reasonable" subset K of $\mathrm{span}(\mathcal{L})$, *Gaussian heuristic* says that the number of points in $K \cap \mathcal{L}$ is approximately $\mathrm{vol}(K)/\mathrm{vol}(\mathcal{L})$. From Gaussian heuristic, we would expect that $\lambda_1(\mathcal{L}) \approx \mathrm{vol}(\mathcal{L})^{1/n}\cdot \mathrm{GH}(n)$ where $\mathrm{GH}(n) = \mathrm{vol}(\mathcal{B}_n(\mathbf{0}, 1))^{-1/n} \approx \sqrt{n/2\pi e}$.

Lattice reduction is a powerful tool for cryptanalysis. LLL, invented by Lenstra et al. [30], is the first polynomial time lattice reduction algorithm. We now recall this classical reduction. For a detailed introduction, we refer to [31].

Definition 3 (LLL reduced basis). A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is a δ-LLL reduced basis with $\delta \in (1/2, 1)$ if the following conditions hold:

(1) Size Reduced: $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq n$.

(2) Lovász Condition: $\delta\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_{i+1}^* + \mu_{i+1,i}\mathbf{b}_i^*\|$ for $1 \leq i < n$.

Then we immediately get the following property of LLL reduced bases.

Lemma 4. *Let* $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ *be a* δ*-LLL reduced basis. For any* $1 \le j < i \le n$*, then*

$$\left\|\mathbf{b}_i^*\right\| \ge \gamma^{j-i} \left\|\mathbf{b}_j^*\right\|, \tag{1}$$

where $\gamma = 1/\sqrt{\delta^2 - 1/4}$.

3. Compact-LWE and Its Weak Instances

In this section, we will introduce an LWE variant named Compact-LWE and report on an attack against certain Compact-LWE instances. A formal definition of Compact-LWE is given as follows.

Definition 5. Let q, m, n, b be positive integers and χ be a distribution over $\mathbb{Z}^m$. Given $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, the Compact-LWE$_{q,m,n,b,\chi}$ problem is to recover $\mathbf{s}$ from $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q)$ where $\mathbf{A} \hookleftarrow U(\mathbb{Z}_b^{m\times n})$ and $\mathbf{e} \hookleftarrow \chi$.

Compared with classical LWE, the sizes of elements of $\mathbf{A}$, namely b, can be less than the modulus q. Thanks to this modification, Compact-LWE-based schemes are of smaller public key sizes and better efficiency than original LWE-based schemes. Thus Compact-LWE seems friendly to lightweight cryptography and constrained devices.

3.1. Structures of q-Ary Lattices in Compact-LWE. We introduce two m-dimensional q-ary lattices which are widely used in the cryptanalysis of LWE. The first lattice, denoted by $\mathscr{L}_q(\mathbf{A})$, is generated by the columns of $\mathbf{A}$ and $q\cdot\mathbf{I}_m$ and defined as

$$\begin{aligned}&\mathscr{L}_q(\mathbf{A})\\ &\quad\coloneqq \left\{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{x} = \mathbf{A}\mathbf{y} \bmod q \text{ for some } \mathbf{y} \in \mathbb{Z}^n\right\},\end{aligned} \tag{2}$$

The second lattice $\mathscr{L}_q^\perp(\mathbf{A})$ is formed by all integer vectors "orthogonal" (modulo q) to the columns of $\mathbf{A}$, which is

$$\mathscr{L}_q^\perp(\mathbf{A}) \coloneqq \left\{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{A}^T\mathbf{x} = \mathbf{0} \bmod q\right\}. \tag{3}$$

As shown in [10], these two lattices are duals scaled by a factor:

$$\mathscr{L}_q^\perp(\mathbf{A}) = q \cdot \mathscr{L}_q(\mathbf{A})^*. \tag{4}$$

By running LLL algorithm with input $(\mathbf{A} \mid q\cdot\mathbf{I}_m)$, one can obtain a basis of $\mathscr{L}_q(\mathbf{A})$. For $\mathbf{A}$ in the compact setting, the LLL reduced basis is of a special structure.

Lemma 6. *Let* $\mathbf{A} \in \mathbb{Z}_b^{m\times n}$ *where* $m \ge n + 2\pi e$ *and* $b \le q^{(m-n)/m}/\sqrt{m}$*. Let* $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$ *be the basis of* $\mathscr{L}_q(\mathbf{A})$ *obtained by running LLL with parameter* δ *on* $(\mathbf{A} \mid q\cdot\mathbf{I}_m)$*. Under Gaussian heuristic, then, for* $\gamma = 1/\sqrt{\delta^2 - 1/4}$*,*

(1) $\mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \mathscr{L}(\mathbf{A})$ *and* $\|\mathbf{b}_i^*\| \le b\sqrt{m}$ *for* $1 \le i \le n$*;*

(2) $\|\mathbf{b}_i^*\| > q\gamma^{n-i+1}(b\sqrt{m})^{-n/(m-n)}$ *for* $n+1 \le i \le m$.

Proof. Let $\phi : \mathbb{Z}^m/\mathscr{L}_q^\perp(\mathbf{A}) \to \mathbb{Z}_q^n$ be the homomorphism mapping $\mathbf{v} + \mathscr{L}_q^\perp(\mathbf{A})$ to $\mathbf{A}^T\mathbf{v} \bmod q$. It can be verified that ϕ is injective, then we have

$$\mathrm{vol}\left(\mathscr{L}_q^\perp(\mathbf{A})\right) \le q^n. \tag{5}$$

Together with (4), it follows that

$$\mathrm{vol}\left(\mathscr{L}_q(\mathbf{A})\right) \ge q^{m-n}. \tag{6}$$

Let $\boldsymbol{\pi}_{\mathbf{A}}(\cdot)$ denote the projection to the orthogonal complement of span$(\mathbf{A})$. Considering the projected lattice $\mathscr{L}'$ generated by $\boldsymbol{\pi}_{\mathbf{A}}(q\cdot\mathbf{I}_m)$, the dimension of $\mathscr{L}'$ is $(m-n)$. Combined with (6), we have

$$\mathrm{vol}\left(\mathscr{L}'\right) \ge \frac{\mathrm{vol}\left(\mathscr{L}_q(\mathbf{A})\right)}{\mathrm{vol}\left(\mathscr{L}(\mathbf{A})\right)} \ge \frac{q^{m-n}}{\mathrm{vol}\left(\mathscr{L}(\mathbf{A})\right)}. \tag{7}$$

Since $\mathrm{vol}(\mathscr{L}(\mathbf{A})) = \prod_{i=1}^n \|\mathbf{a}_i^*\| \le \prod_{i=1}^n \|\mathbf{a}_i\| \le (b\sqrt{m})^n$, it follows that

$$\mathrm{vol}\left(\mathscr{L}'\right) \ge \frac{q^{m-n}}{(b\sqrt{m})^n}. \tag{8}$$

By Gaussian heuristic, we have that

$$\begin{aligned}\lambda_1\left(\mathscr{L}'\right) &\approx \sqrt{\frac{m-n}{2\pi e}} \cdot \left(\mathrm{vol}\left(\mathscr{L}'\right)\right)^{1/(m-n)}\\ &\ge q \cdot (b\sqrt{m})^{-n/(m-n)}.\end{aligned} \tag{9}$$

A straightforward computation leads to that $\lambda_1(\mathscr{L}') \ge b\sqrt{m} \ge \max_{i=1}^n \|\mathbf{a}_i^*\|$. It is known that the maximum of the Gram-Schmidt norms would never increase in LLL algorithm. Thus, Lovász condition always holds for the nth and $(n+1)$th vectors during LLL, which means that these two vectors would never be swapped. In other words, running LLL on $(\mathbf{A} \mid q\cdot\mathbf{I}_m)$ is equivalent to running LLL on $\mathbf{A}$ and $\boldsymbol{\pi}_{\mathbf{A}}(q\cdot\mathbf{I}_m)$, respectively. Consequently, we have $\mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \mathscr{L}(\mathbf{A})$ and $\|\mathbf{b}_i^*\| \le \max_{i=1}^n \|\mathbf{a}_i^*\| \le b\sqrt{m}$ for $1 \le i \le n$.

For the second inequality, Lemma 4 yields that

$$\left\|\mathbf{b}_{n+i}^*\right\| \ge \left\|\mathbf{b}_{n+1}^*\right\| \gamma^{1-i} > q\gamma^{1-i}(b\sqrt{m})^{-n/(m-n)}, \tag{10}$$

because $\|\mathbf{b}_{n+1}^*\| \ge \lambda_1(\mathscr{L}')$. We now complete the proof. □

Remark 7. Experimental results coincide with Lemma 6. Under parameter settings $(q, m, n) = (2^{20}, 300, 120)$, we generated 20 instances for each b ranging from 2 to 2^{18}. Figure 1 illustrates the average profile of $\mathbf{B}$, where the first n $\mathbf{b}_i^*$'s are relatively short when b is small. We notice that the slope of $\{\log_2\|\mathbf{b}_i^*\|\}_{i=n+1}^m$ is less than the theoretical bound $\log_2\gamma \approx 0.2172$, which can be explained by the better performance of LLL in practice than the theoretical prediction. Figure 2 shows the gap between $\|\mathbf{b}_{n+1}^*\|$ and $\|\mathbf{b}_n^*\|$, which is narrowing as b increases. It is worth noting that when $b < q^{m/(m-n)}/\sqrt{m}$ (the bound in Lemma 6 marked by the dashed line), the gap is quite significant.

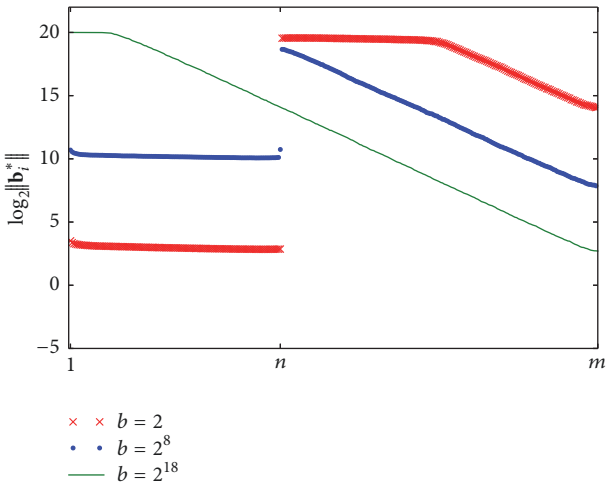

Figure 1: Experimental measure of $\{\log_2\|\mathbf{b}_i^*\|\}_{i=1}^m$ for different b.

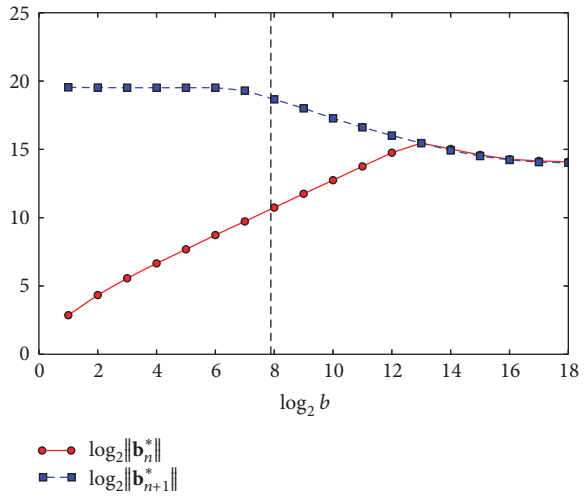

Figure 2: Experimental measure of the gap between $\log_2\|\mathbf{b}_n^*\|$ and $\log_2\|\mathbf{b}_{n+1}^*\|$.

Lemma 8. *Let $m \geq n + 2\pi e$ and $b \leq q^{(m-n)/m}/\sqrt{m}$. Let $\mathbf{A} \in \mathbb{Z}_b^{m\times n}$ and $\delta \in (1/2, 1)$. There exists a basis of $\mathcal{L}_q^\perp(\mathbf{A})$, denoted by $\mathbf{D} = (\mathbf{d}_1, \ldots, \mathbf{d}_m)$, satisfying the following conditions under Gaussian heuristic:*

(1) $\mathcal{L}(\mathbf{d}_1, \ldots, \mathbf{d}_{m-n}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{x}^T\mathbf{A} = \mathbf{0}\}$,

(2) $\|\mathbf{d}_i\| \leq \sqrt{(i+3)/4}\cdot\gamma^{m-n}(b\sqrt{m})^{n/(m-n)}$ *for* $1 \leq i \leq m-n$,

(3) $\|\mathbf{d}_i\| \geq \sqrt{n/2\pi e}(q/b\sqrt{m})$ *for* $m - n + 1 \leq i \leq m$,

where $\gamma = 1/\sqrt{\delta^2 - 1/4}$. This basis can be obtained in polynomial time.

Proof. Let $\mathbf{B} = (\mathbf{B}_1 \mid \mathbf{B}_2)$ be the LLL reduced basis of $\mathcal{L}_q(\mathbf{A})$ defined in Lemma 6 where $\mathcal{L}(\mathbf{B}_1) = \mathcal{L}(\mathbf{A})$. Let $\mathbf{U}$ be a matrix such that $\mathbf{U}^T\mathbf{B} = q\mathbf{I}_m$. Then, from (4), $\mathbf{U}$ is a basis of $\mathcal{L}_q^\perp(\mathbf{A})$. Let $\mathbf{U} = (\mathbf{U}_1 \mid \mathbf{U}_2) = (\mathbf{u}_m, \ldots, \mathbf{u}_1)$ where $\mathbf{U}_1 \in \mathbb{Z}^{m\times n}$.

Let $\mathcal{L}^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{x}^T\mathbf{A} = \mathbf{0}\}$. We claim that $\mathcal{L}(\mathbf{U}_2) = \mathcal{L}^\perp(\mathbf{A})$. It is easy to observe that $\mathcal{L}^\perp(\mathbf{A}) = \mathcal{L}^\perp(\mathbf{B}_1)$ where $\mathcal{L}^\perp(\mathbf{B}_1) = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{x}^T\mathbf{B}_1 = \mathbf{0}\}$. On one hand, we have $\mathcal{L}(\mathbf{U}_2) \subseteq \mathcal{L}^\perp(\mathbf{B}_1)$ since $\mathbf{U}_2^T\mathbf{B}_1 = \mathbf{0}$. On the other hand, for arbitrary $\mathbf{v} \in \mathcal{L}^\perp(\mathbf{B}_1) \subseteq \mathcal{L}_q^\perp(\mathbf{A})$, there exists a unique vector pair $(\mathbf{z}_1, \mathbf{z}_2)$ such that $\mathbf{v} = \mathbf{U}_1\mathbf{z}_1 + \mathbf{U}_2\mathbf{z}_2$. Since $\mathbf{U}_1^T\mathbf{B}_1 = q\mathbf{I}_n$, we have $\mathbf{v}^T\mathbf{B}_1 = q\mathbf{z}_1^T = \mathbf{0}$ and then $\mathbf{v} \in \mathcal{L}(\mathbf{U}_2)$. Therefore, it holds that $\mathcal{L}(\mathbf{U}_2) = \mathcal{L}^\perp(\mathbf{A})$.

We run size reduction algorithm on $(\mathbf{u}_1, \ldots, \mathbf{u}_m)$ (vectors of $\mathbf{U}$ in reverse order) and obtain a new basis of $\mathcal{L}_q^\perp(\mathbf{A})$, denoted by $\mathbf{D} = (\mathbf{d}_1, \ldots, \mathbf{d}_m)$. Size reduction can be done within polynomial time; thus it suffices to prove the last two conditions hold for $\mathbf{D}$. From Lemmas 2 and 6, we have that, for $i = 1, \ldots, m - n$,

$$\|\mathbf{d}_i^*\| = \|\mathbf{u}_i^*\| = \frac{q}{\|\mathbf{b}_{m+1-i}^*\|} \leq \gamma^{m-n-i}\left(b\sqrt{m}\right)^{n/(m-n)}, \tag{11}$$

and then

$$\begin{aligned}\|\mathbf{d}_i\| &\leq \sqrt{\|\mathbf{d}_i^*\|^2 + \frac{1}{4}\sum_{j=1}^{i-1}\|\mathbf{d}_j^*\|^2} \\ &\leq \sqrt{\frac{i+3}{4}}\gamma^{m-n}\left(b\sqrt{m}\right)^{n/(m-n)}.\end{aligned} \tag{12}$$

Let $\mathcal{L}'' = \mathcal{L}(\boldsymbol{\pi}_{m-n}(\mathbf{d}_{m-n+1}), \ldots, \boldsymbol{\pi}_{m-n}(\mathbf{d}_m))$ where $\boldsymbol{\pi}_{m-n}(\cdot)$ is the projection to the orthogonal complement of $\mathrm{span}(\mathbf{d}_1, \ldots, \mathbf{d}_{m-n})$. Observing that $\mathrm{vol}(\mathcal{L}_q(\mathbf{A}))\mathrm{vol}(\mathcal{L}_q^\perp(\mathbf{A})) = q^m$ and $\|\mathbf{d}_i^*\| = q/\|\mathbf{b}_{m+1-i}^*\|$ for $i \leq m - n$, together with Lemma 6, we have

$$\mathrm{vol}\left(\mathcal{L}''\right) = \frac{\mathrm{vol}\left(\mathcal{L}_q^\perp(\mathbf{A})\right)}{\prod_{i=1}^{m-n}\|\mathbf{d}_i^*\|} = \frac{q^n}{\prod_{i=1}^{n}\|\mathbf{b}_i^*\|} \geq \frac{q^n}{\left(b\sqrt{m}\right)^n}. \tag{13}$$

On the basis of Gaussian heuristic, we conclude that, for $m - n + 1 \leq i \leq m$,

$$\|\mathbf{d}_i\| \geq \|\boldsymbol{\pi}_{m-n}(\mathbf{d}_i)\| \geq \lambda_1\left(\mathcal{L}''\right) \geq \sqrt{\frac{n}{2\pi e}}\frac{q}{b\sqrt{m}}. \tag{14}$$

We now complete the proof. □

Remark 9. We ran experiments under parameters $(q, m, n) = (2^{20}, 300, 120)$ and tested 20 instances for each b ranging from 2 to 2^{18}. Figure 3 provides a geometric intuition of $\mathbf{D}$. There also exists a large gap between $\|\mathbf{d}_{m-n}\|$ and $\|\mathbf{d}_{m-n+1}\|$ when b is small. As illustrated in Figure 4, the gap between $\|\mathbf{d}_{m-n}\|$ and $\|\mathbf{d}_{m-n+1}\|$ is shrinking as b grows. However, when $b < q^{m-n/m}/\sqrt{m}$ (marked by the dashed line), the length of $\mathbf{d}_{m-n}$ is far less than q.

3.2. Attack Against Weak Compact-LWE Instances. Figure 1 illustrates a staircase-shaped profile of the basis of $\mathcal{L}_q(\mathbf{A})$. Exploiting this feature, we can prove that it is possible to efficiently recover a candidate error whose norm is close to that of the original error for certain parameters. The following lemma will be used in the later discussion.

Lemma 10. *Let $\mathcal{L} \subseteq \mathbb{R}^m$ be a lattice of rank n and $\mathbf{B}$ be a basis of $\mathcal{L}$. Let $\mathbf{t} \in \mathbb{R}^m$ and $\mathrm{dist}(\mathbf{t}, \mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}}\|\mathbf{t} - \mathbf{v}\|$. If*

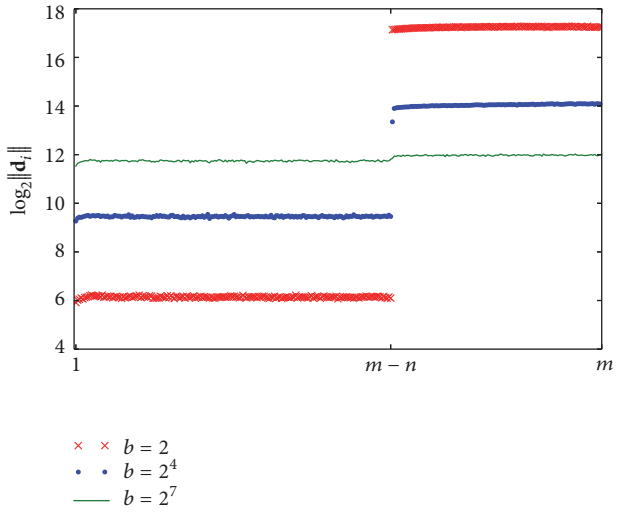

Figure 3: Experimental measure of $\{\log_2\|\mathbf{d}_i\|\}_{i=1}^m$ for different b.

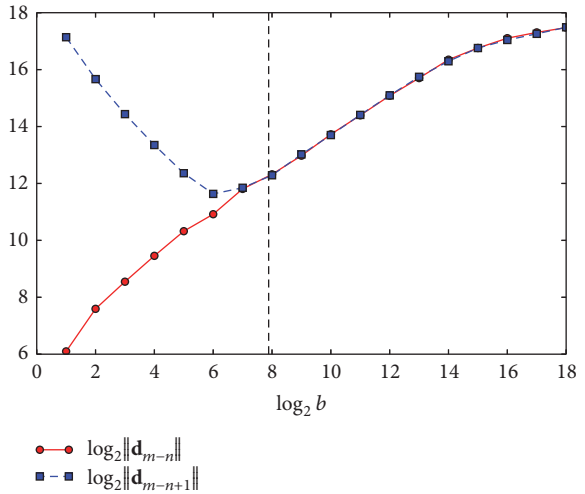

Figure 4: Experimental measure of the gap between $\log_2\|\mathbf{d}_{m-n}\|$ and $\log_2\|\mathbf{d}_{m-n+1}\|$.

$\mathrm{dist}(\mathbf{t}, \mathscr{L}) \le r < (1/2)\min_{i=1}^n\|\mathbf{b}_i^*\|$, *then there exists a unique vector in* $\mathscr{B}(\mathbf{t}, r) \cap \mathscr{L}$.

Proof. We denote by $\mathbf{v} = \sum_{i=1}^n v_i\mathbf{b}_i$ the vector output by Babai's nearest plane algorithm [32] on the lattice $\mathscr{L}$ and target vector $\mathbf{t}$. Assume, by contradiction, that $\mathbf{v}' \neq \mathbf{v}$ is another vector in $\mathbf{B}(\mathbf{t}, r) \cap \mathscr{L}$ and $\mathbf{v}' = \sum_{i=1}^n v_i'\mathbf{b}_i$. Let k be the largest index such that $v_k \neq v_k'$. According to the process of Babai's algorithm, we conclude that

$$\left\|\mathbf{v}' - \mathbf{t}\right\| \ge \frac{1}{2}\left\|\mathbf{b}_k^*\right\| > r, \tag{15}$$

which implies a contradiction. □

Next we demonstrate a class of provably weak instances of Compact-LWE and also an attack aiming at them.

Theorem 11. *Let* q, m, n, b, r *be positive integers satisfying* $b \le q^{(m-n)/m}/\sqrt{m}$ *and* $(\sqrt{mn}/2)b < r \le (q/2)\gamma^{n-m+1}(b\sqrt{m})^{-n/(m-n)}$ *where* $\gamma = 1/\sqrt{\delta^2 - 1/4}$ *for* $\delta \in (1/2, 1)$ *and a constant* $c > 0$. *Let* χ *be a* $(r, (1/2)\sqrt{4r^2 - mnb^2})$*-confidence distribution. Under Gaussian heuristic, there exists a probabilistic polynomial time algorithm solving Compact-LWE*$_{q,m,n,b,\chi}$.

Proof. Given a random sample $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e} \bmod q)$, we can obtain a basis of $\mathscr{L}_q(\mathbf{A})$, denoted by $\mathbf{B}$, by applying LLL algorithm with parameter δ on $(\mathbf{A} \mid q\mathbf{I}_m)$. Exploiting Babai's algorithm on $\mathscr{L}_q(\mathbf{A})$ and target vector $\mathbf{b}$, we get a pair of solution $(\mathbf{s}', \mathbf{e}')$. We are to prove that $(\mathbf{s}', \mathbf{e}')$ is legal for Compact-LWE, that is, $\|\mathbf{e}'\| \le r$, with nonnegligible probability.

From Lemma 6, we get that $r < (1/2)\|\mathbf{b}_i^*\|$ for $n+1 \le i \le m$. We denote by $\boldsymbol{\pi}_n(\cdot)$ the projection to the orthogonal complement of $\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Let $\mathscr{L}' = \boldsymbol{\pi}_n(\mathscr{L})$ and $\mathbf{b}' = \boldsymbol{\pi}_n(\mathbf{b})$. Lemma 10 shows that there exists a unique vector in $\mathscr{B}(\mathbf{b}', r) \cap \mathscr{L}'$, namely, $\boldsymbol{\pi}_n(\mathbf{e}) = \boldsymbol{\pi}_n(\mathbf{e}')$. Then we have

$$\begin{aligned}\left\|\mathbf{e}'\right\|^2 &= \left\|\mathbf{e}' - \boldsymbol{\pi}_n\left(\mathbf{e}'\right)\right\|^2 + \left\|\boldsymbol{\pi}_n\left(\mathbf{e}'\right)\right\|^2 \\ &\le \frac{1}{4}\sum_{i=1}^n\left\|\mathbf{b}_i^*\right\|^2 + \|\mathbf{e}\|^2 \le \frac{mnb^2}{4} + \|\mathbf{e}\|^2.\end{aligned} \tag{16}$$

Since χ is $(r, (1/2)\sqrt{4r^2 - mnb^2})$-confidence, it implies that $\|\mathbf{e}\| \le (1/2)\sqrt{4r^2 - mnb^2}$ with nonnegligible probability. Thus the probability of $\|\mathbf{e}'\| \le r$ is nonnegligible. □

Remark 12. In such weak instances, it can be verified that

$$q > \sqrt{n} \cdot \gamma^{m-n-1}\left(b\sqrt{m}\right)^{m/(m-n)}, \tag{17}$$

and thus parameters are overstretched [33, 34]. The inequalities given in Lemma 6 follow the worst-case result of LLL, but LLL behaves much better in practice. Hence our attack may apply to more Compact-LWE instances. Moreover, note that, for usual LWE distribution χ such as discrete Gaussian, it is easy to set α, β such that χ is (α, β)-confidence.

4. Attack against Compact-LWE-Based Schemes

In this section, our analysis of Section 3 is applied to attack concrete Compact-LWE-based lightweight encryption schemes. We successfully recover the plaintexts in IoT-oriented public key encryption proposed by Liu et al. in [25] following a totally different way with [29]. However, we fail to give an effective cryptanalysis of the binary LWE-based lightweight encryption in [24].

4.1. Liu et al.'s Compact-LWE-Based Scheme. Firstly, we briefly recall the public key encryption in [25]. The scheme is

specified by a tuple of public parameters (q, n, m, t, w, b) satisfying

$$\begin{aligned} n + 1 < m < n^2, \\ 2\log_2 b < n < b, \\ (2b\log_2 b + 2) \cdot b < q. \end{aligned} \tag{18}$$

We list below three main algorithms: key generation **Gen**, encryption **Enc**$(\cdot)$, and decryption **Dec**$(\cdot)$.

(i) **Gen**: sample $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, and choose sk, r, p from $\mathbb{Z}_q$ satisfying

$$\begin{aligned} t \le p, \\ b < r, \\ sk\,(t-1) + wrp < q, \end{aligned} \tag{19}$$

and sk, p, q are pairwise coprime. Sample $\mathbf{A} \hookleftarrow U(\mathbb{Z}_b^{m\times n})$ and $\mathbf{e} \hookleftarrow U(\mathbb{Z}_r^m)$. Let $sk_q^{-1} \in \mathbb{Z}_q$ such that $sk \cdot sk_q^{-1} = 1 \bmod q$. Output $\mathbf{SK} = (\mathbf{s}, sk, r, p)$ as the secret key and $\mathbf{PK} = (\mathbf{A}, \mathbf{pk} = \mathbf{As} - sk_q^{-1} \cdot p \cdot \mathbf{e} \bmod q)$ as the public key.

(ii) **Enc**$(v \in \mathbb{Z}_t, \mathbf{PK})$: uniformly and independently sample $i_1, \ldots, i_w \hookleftarrow U(\mathbb{Z}_m)$, and calculate $\mathbf{c}' = \sum_{j=1}^{w} (\mathbf{a}_{i_j}, pk_{i_j}) \bmod q$ where $(\mathbf{a}_i, pk_i)$ is the ith row of $\mathbf{PK}$. Let $\mathbf{c}' = (\mathbf{a}, pk)$, output $\mathbf{c} = (\mathbf{a}, v - pk \bmod q)$ as the ciphertext.

(iii) **Dec**$(\mathbf{c} = (\mathbf{a}, x), \mathbf{SK})$: calculate $c = \langle \mathbf{a}, \mathbf{s} \rangle + x \bmod q$ and then calculate $skv = sk \cdot c \bmod q$. Let sk_p^{-1} be the multiplicative inverse of sk modulo p. Output the plaintext $v = [sk_p^{-1} \cdot skv]_p$.

In [25], the authors also proposed concrete parameters to instantiate the scheme. The parameters are listed as follows:

(i) Public parameters: $(q, n, m, t, w, b) = (2^{32}, 13, 74, 2^{16}, 86, 16)$

(ii) Secret parameters: $(sk, p, r) = (2x+1, t+2y+1, \le (q-1-sk\cdot(t-1))/(w\cdot p))$ where $(x, y) \in [0, 50]\times[0, 500]$ or $[0, 500] \times [0, 50]$.

4.2. Attack against Liu et al.'s Scheme. According to the average profile of bases shown in Lemmas 6 and 8 under the parameters $(q, m, n, b) = (2^{32}, 74, 13, 16)$ (see Figures 5 and 6) as suggested in [25], it seems that Liu et al.'s scheme is fragile. We propose a new attack against Liu et al.'s scheme with the help of our analysis towards Compact-LWE in Section 3.

Our attack consists of two steps: *guessing the mask coefficient* (sk, p) and *recovering the plaintext*. In the first step, one can almost determine the pair (sk, p) (sometimes together with several possible candidate pairs) by enumerating and checking. In the second step, combined with (sk, p), one can calculate a pair of legal solution $(\mathbf{s}', \mathbf{e}')$ to the Compact-LWE problem and recover the plaintext as well. Now we are to show the details of our attack.

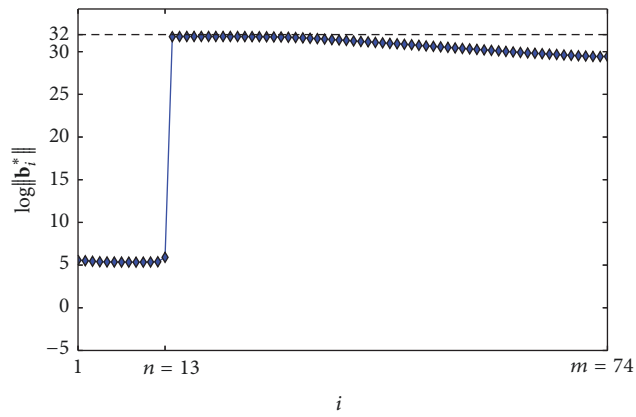

Figure 5: Experimental measure of $\{\log_2 \|\mathbf{b}_i^*\|\}_{i=1}^m$.

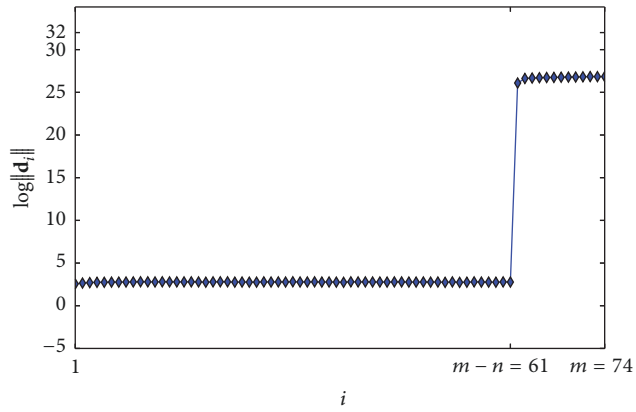

Figure 6: Experimental measure of $\{\log_2 \|\mathbf{d}_i\|\}_{i=1}^m$.

Step 1 (guessing the mask coefficient (sk, p)). Firstly, we prove that it is possible to recover efficiently the secret parameters sk and p only from the public key $\mathbf{PK} = (\mathbf{A}, \mathbf{pk})$.

Let $\mathbf{D} = (\mathbf{d}_1, \ldots, \mathbf{d}_n)$ be a basis of $\mathcal{L}_q^{\perp}(\mathbf{A})$ as described in Lemma 4 with $\delta = \sqrt{0.99}$. Let $p_q^{-1} \in \mathbb{Z}$ such that $p_q^{-1} \cdot p = 1 \bmod q$; then we have that

$$sk \cdot p_q^{-1} \cdot \langle \mathbf{d}_i, \mathbf{pk} \rangle = -\langle \mathbf{d}_i, \mathbf{e} \rangle \bmod q. \tag{20}$$

Since $\|\mathbf{e}\| \le r\sqrt{m} \le (q - 1 - sk \cdot (t-1))/(w \cdot p)\sqrt{m}$ and $\|\mathbf{d}_i\|$ is also small when $1 \le i \le m - n$, a routine computation yields that $|\langle \mathbf{d}_i, \mathbf{e} \rangle| \le \|\mathbf{d}_i\| \cdot \|\mathbf{e}\| < q/2$ under the parameter setting suggested in [25]. Then it holds that

$$\begin{aligned} \left| \left[sk \cdot p_q^{-1} \cdot \langle \mathbf{d}_i, \mathbf{pk} \rangle \right]_q \right| &= \left| \langle \mathbf{d}_i, \mathbf{e} \rangle \right| \\ &\le \frac{q - 1 - sk \cdot (t-1)}{w \cdot p} \sqrt{m} \cdot \|\mathbf{d}_i\|, \end{aligned} \tag{21}$$

for $i = 1, \ldots, m-n$. We try all possible pairs $(sk, p) \in \{2x+1 \mid x \in [0, 50] \cap \mathbb{Z}\} \times \{t + 2y + 1 \mid y \in [0, 500] \cap \mathbb{Z}\}$ and check inequality (21) for $\mathbf{d}_1, \ldots, \mathbf{d}_{m-n}$, respectively; then (sk, p) is viewed as a candidate when it holds for all $i = 1, \ldots, m - n$.

Experiments indicate that this step can indeed determine the unique correct (sk, p) at most times, and output a few

Table 1: Experimental results.

Parameter	Time for Step 1	Time for Step 2	Time for attack	Determining unique (sk, p)	Success rate
ParaA	0.61 s	1.94 s	2.55 s	67%	100%
ParaB	0.60 s	1.86 s	2.46 s	71%	100%

Table 2: Experimental results for optimized attack.

Parameter	Time for Step 1	Time for Step 2	Time for attack	Success rate
ParaA	0.57 s	1.14 s	1.71 s	100%
ParaB	0.57 s	1.14 s	1.71 s	100%

candidates (including the correct pair) of the form $(\lambda \cdot sk, p)$ for small factor λ at other times. Therefore, by guessing sk and p, we can actually remove the secret scaling factor and transform **PK** into a standard Compact-LWE sample.

Step 2 (recovering the plaintext). After the previous step, we obtain one or more (sk, p) pairs. Next, we are to show how to recover the plaintext combined with the ciphertext.

Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$ be the basis of $\mathscr{L}_q(\mathbf{A})$ described in Lemma 6. Given a candidate pair of the mask coefficient $(sk', p') = (\lambda \cdot sk, p)$ where λ is small, let $\mathbf{pk}' = sk' \cdot p_q^{-1} \cdot \mathbf{pk} \bmod q$. Running Babai's algorithm on $\mathscr{L}_q(\mathbf{A})$ and target vector $\mathbf{pk}'$, we obtain $\mathbf{v}' \in \mathscr{L}_q(\mathbf{A})$ and let $\mathbf{e}' = \mathbf{v}' - \mathbf{pk}'$. We observe that the distance from $\mathbf{pk}'$ to $\mathscr{L}_q(\mathbf{A})$ is at most $\|\lambda \cdot \mathbf{e}\|$, and $\|\lambda \cdot \mathbf{e}\| \le \lambda \cdot r\sqrt{m} < (1/2)\|\mathbf{b}_i^*\|$ for $n+1 \le i \le m$. Following a similar argument of (16) in Theorem 11, we know that

$$\left\|\mathbf{e}'\right\|^2 \le \|\lambda \cdot \mathbf{e}\|^2 + \frac{n}{4}\max_{1\le i\le n}\left\|\mathbf{b}_i^*\right\|^2 \le \left(\lambda^2 r^2 + \frac{n}{4}b^2\right)m. \quad (22)$$

Let $\mathbf{s}' \in \mathbb{Z}_q^m$ such that $\mathbf{v}' = sk' \cdot p_q^{-1}\mathbf{A}\mathbf{s}' \bmod q$, then $\mathbf{pk} = \mathbf{A}\mathbf{s}' - sk_q'^{-1} \cdot p' \cdot \mathbf{e}' \bmod q$ where $sk_q'^{-1} \cdot sk_q' = 1 \bmod q$. Exploiting the substitute secret key $(sk', p', \mathbf{s}', \mathbf{e}')$, we can decrypt the ciphertext $\mathbf{c} = (\mathbf{a}, x)$ as follows:

(1) Calculate $c' = [\langle \mathbf{a}, \mathbf{s}' \rangle + x]_q$.

(2) Calculate $skv' = \lfloor sk' \cdot c' \rceil_q$.

(3) Return $v' = [sk_p'^{-1} \cdot skv']_p$ where $sk_p'^{-1} \cdot sk' = 1 \bmod p$.

We now explain why the ciphertext can be decrypted correctly by above algorithm. It can be checked that $sk' \cdot c' = sk' \cdot v + p' \sum_{j=1}^{w} e'_{i_j} \bmod q$. Noticing that $\|\mathbf{e}'\|$ is well-bounded and some coordinates e'_i of $\mathbf{e}'$ could be negative, we may assert that $sk' \cdot v + p' \sum_{j=1}^{w} e'_{i_j} \in (-q/2, q/2)$ with a high probability. Thus the term $sk' \cdot v + p' \sum_{j=1}^{w} e'_{i_j}$ can be recovered (as skv') correctly, which implies that v' is the plaintext.

Experiments show that the plaintext can indeed be recovered, even if $(sk', p') = (\lambda \cdot sk, p)$ for some $\lambda \ne 1$. When λ is large, the norm of $\mathbf{e}'$ may exceed the upper bound $r\sqrt{m}$, which implies that (sk', p') is a wrong guess. Therefore, we may eliminate some wrong guesses of (sk', p') further in this step. Moreover, one may also try more middle terms such as $skv' = \lfloor sk' \cdot c' \rceil_q, \lfloor sk' \cdot c' \rceil_q \pm q$ during the "decryption" to ensure that the correct value of $sk' \cdot v + p' \sum_{j=1}^{w} e'_{i_j}$ is not missed. However, from our experimental results, we observe that trying only one $skv' = \lfloor sk' \cdot c' \rceil_q$ is enough to recover the plaintext in practice.

Experimental Results. We implemented our attack using the NTL library [35]. All experiments were run on a single core of a 3.40 GHz Core i7-4930K PC.

We follow the parameter setting suggested in [25]: the public parameters $(q, n, m, t, w, b) = (2^{32}, 13, 74, 2^{16}, 86, 16)$ and the secret parameters $(sk, p) = (2x + 1, t + 2y + 1)$. We denote the cases $(x, y) \in [0, 50] \times [0, 500]$ and $[0, 500] \times [0, 50]$ by **ParaA** and **ParaB**, respectively. For **ParaA** and **ParaB**, we respectively generated 100 random instances and calculated the ciphertexts of 100 random messages for each instance. Then we ran the attack on these 10000 ciphertexts. Experimental results are given in Table 1.

As mentioned before, we may obtain several (sk', p') pairs in Step 1. In fact, it suffices to take use of the pair with the minimal sk' to recover the plaintext. This observation leads to an optimization of the attack: one may search (sk', p') in increasing (dictionary) order and move to Step 2 once a candidate is found. Experimental results for optimized attack are given in Table 2.

Comparison with Bootle and Tibouchi's Attack. We note that Bootle and Tibouchi also proposed a practical attack [29] against Liu et al.'s encryption scheme. They deployed the technique of embedding lattices to compute the nonce sequence $i_1, \ldots, i_w$ in encryption process $\mathbf{Enc}(\cdot)$, while we start from a different angle and recover a substitutable tuple of private keys $(sk', p', \mathbf{s}', \mathbf{e}')$. We hold the view that the insecurity of Liu et al.'s scheme is not only a result of the small value of n as claimed in [29], but also the overstretched magnitude relation between the modulus q and parameters b, m, and n, which is clarified in Theorem 11.

4.3. Attack against Galbraith's Scheme. In [24], Galbraith proposed a class of LWE-based encryption for constrained devices with more compact parameters; that is, the public matrix $\mathbf{A}$ is binary. We tried to attack Galbraith's scheme exploiting short vectors of $\mathscr{L}_q^{\perp}(\mathbf{A})$ as described before, but it was ineffective even for the parameters totally broken in [27]. That is because the modulus q in Galbraith's scheme is not so

overstretched. However, the binary public matrix and encryption nonce may still be problematic as suggested in [27].

5. Conclusion

In this paper, we target the variant of LWE called Compact-LWE which may be applied to design IoT-oriented lightweight cryptography. We give an explicit analysis of Compact-LWE and point out some weak instances with extreme compactness and overstretched moduli. As an application of our results, we propose a practical attack against the lightweight public key scheme in [25]. Consequently, we claim that the security estimation in [25] is incorrect.

The fragility of the scheme in [25] comes not only from its small parameters but also from the weak hardness of Compact-LWE. It would be interesting to generally figure out a theoretical hardness relation between Compact-LWE and other lattice problems.

Compact-LWE may be still of some interest under refined parameters. We leave to future work the issues of tradeoff between efficiency and security, in particular the practical parameter selections achieving given security levels for IoT devices.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors thank Léo Ducas and Professor Xiaoyun Wang for helpful discussions and comments. This research was supported by the National Key Research and Development Program of China (Project no. 2017YFA0303903), 973 National Program on Key Basic Research Project of China (Project no. 2013CB834205), and National Natural Science Foundation of China (no. 61502269).

References

[1] I. Kotenko, I. Saenko, and A. Kushnerevich, "Parallel big data processing system for security monitoring in internet of things networks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 8, no. 4, pp. 60–74, 2017.

[2] R. Sanchez-Iborra, J. S. Gómez, J. Santa et al., "Integrating LP-WAN communications within the vehicular ecosystem," *Journal of Internet Services and Information Security*, vol. 7, no. 4, pp. 45–56, 2017.

[3] G. Pau, M. Collotta, S. Tirrito, and R. Caponetto, "An innovative approach for the management of cross-coupling interference in street lighting networks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 8, no. 2, pp. 44–63, 2017.

[4] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[5] V. Desnitsky, D. Levshun, A. Chechulin, and I. Kotenko, "Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 7, no. 2, pp. 60–80, 2016.

[6] S. Aram, R. A. Shirvani, E. Pasero, and M. F. Chouikha, "Implantable medical devices; networking security survey," *Journal of Internet Services and Information Security*, vol. 6, no. 3, pp. 40–60, 2016.

[7] H. Seo, Z. Liu, J. Großschädl, and H. Kim, "Efficient arithmetic on ARM-NEON and its application for high-speed RSA implementation," *Security and Communication Networks*, vol. 9, no. 18, pp. 5401–5411, 2016.

[8] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 237–248, 2017.

[9] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, STOC 2005*, pp. 84–93, Baltimore, MD, USA, 2005.

[10] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pp. 197–206, ACM, Victoria, British Columbia, Canada, 2008.

[11] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011*, pp. 97–106, USA, October 2011.

[12] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," in *Proceedings of the 45th Annual ACM Symposium on Theory of Computing, STOC 2013*, pp. 545–554, June 2013.

[13] M. S. Rahman, A. Basu, and S. Kiyomoto, "Decentralized ciphertext-policy attribute-based encryption: a post-quantum construction," *Journal of Internet Services and Information Security*, vol. 7, no. 3, pp. 1–16, 2017.

[14] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proceedings of the Advances in Cryptology—EUROCRYPT 2010*, vol. 6110 of *Lecture Notes in Comput. Sci.*, pp. 1–23, Springer, French Riviera, France, 2010.

[15] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.

[16] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS – Dilithium: Digital signatures from module lattices," in *Cryptology ePrint Archive*, 2017, Report 2017/633, http://eprint.iacr.org/2017/633.

[17] J. Bos, L. Ducas, E. Kiltz et al., "CRYSTALS – Kyber: a cca-secure module-lattice-based kem," in *Cryptology ePrint Archive*, 2017, Report 2017/634, http://eprint.iacr.org/2017/634.

[18] E. Alkim, L. Ducas, T. P, P. Schwabe, and T. Pöppelmann, "Post-quantum key exchange—a new hope," in *Proceedings of the 25th USENIX Security Symposium*, vol. 16, pp. 327–343, 2016, https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim.

[19] Z. Liu, H. Seo, S. S. Roy, J. Großschädl, H. Kim, and I. Verbauwhede, "Efficient ring-LWE encryption on 8-bit AVR processors," *CHES*, vol. 9293, pp. 663–682, 2015.

[20] Z. Liu, R. Azarderakhsh, H. Kim, and H. Seo, "Efficient Software Implementation of Ring-LWE Encryption on IoT Processors," *IEEE Transactions on Computers*, 2017.

[21] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann, "Practical lattice-based cryptography: a signature scheme for embedded systems," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012*, vol. 7428, pp. 530–547.

[22] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with small parameters," in *Proceedings of the Advances in Cryptology—CRYPTO 2013. Part I*, vol. 8042 of *Lecture Notes in Comput. Sci.*, pp. 21–39, Springer, Santa Barbara, CA, USA, 2013.

[23] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, "Classical hardness of learning with errors," in *Proceedings of the 45th Annual ACM Symposium on Theory of Computing, STOC 2013*, pp. 575–584, USA, June 2013.

[24] S. D. Galbraith, "Space-efficient variants of cryptosystems based on learning with errors," 2013, https://www.math.auckland.ac.nz/~sgal018/compact-LWE.pdf.

[25] D. Liu, N. Li, J. Kim, and S. Nepal, "Compact-LWE: Enabling practically lightweight public key encryption for leveled IoT device authentication," in *Cryptology ePrint Archive*, 2017, Report 2017/685, http://eprint.iacr.org/2017/685.

[26] S. Bai and S. D. Galbraith, "Lattice decoding attacks on binary LWE," *ACISP*, vol. 8544, pp. 322–337, 2014.

[27] G. Herold and A. May, "LP solutions of vectorial integer subset sums - cryptanalysis of Galbraith's binary matrix LWE," in *Proceedings of the Public-key cryptography—PKC 2017. PART I*, vol. 10174 of *Lecture Notes in Comput. Sci.*, pp. 3–15, Springer, Amsterdam, The Netherlands, 2017.

[28] E. Kirshanova, A. May, and F. Wiemer, "Parallel implementation of BDD enumeration for LWE," *ACNS*, vol. 9696, pp. 580–591, 2016.

[29] J. Bootle and M. Tibouchi, "Cryptanalysis of Compact-LWE," in *Cryptology ePrint Archive*, 2017, Report 2017/742, http://eprint.iacr.org/2017/742.

[30] A. K. Lenstra, J. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, 1982.

[31] P. Q. Nguyen and B. Vallée, *The LLL algorithm: Survey and applications*, Springer, 2010.

[32] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem," in *STACS*, vol. 182 of *Lecture Notes in Comput. Sci.*, pp. 13–20, Springer, Saarbrücken, Germany, 1985.

[33] M. Albrecht, S. Bai, and L. Ducas, "A subfield lattice attack on overstretched NTRU assumptions: cryptanalysis of some FHE and graded encoding schemes," in *Proceedings of the Advances in Cryptology—CRYPTO 2016. Part I*, vol. 9814 of *Lecture Notes in Comput. Sci.*, pp. 153–178, Springer, Santa Barbara, CA, USA, 2016.

[34] P. Kirchner and P.-A. Fouque, "Revisiting lattice attacks on overstretched NTRU parameters," in *Proceedings of the Advances in Cryptology—EUROCRYPT 2017. Part I*, vol. 10210 of *Lecture Notes in Comput. Sci.*, pp. 3–26, Springer, Paris, France, 2017.

[35] V. Shoup, "NTL: A library for doing number theory," http://www.shoup.net.