PAPER Special Section on Cryptography and Information Security

On the Complexity of the LWR-Solving BKW Algorithm*

Hiroki OKADA[†a)], **Atsushi TAKAYASU**[††], ***Nonmembers***, **Kazuhide FUKUSHIMA**[†], **Shinsaku KIYOMOTO**[†], ***and*** **Tsuyoshi TAKAGI**[††], ***Members***

SUMMARY The Blum-Kalai-Wasserman algorithm (BKW) is an algorithm for solving the learning parity with noise problem, which was then adapted for solving the learning with errors problem (LWE) by Albrecht et al. Duc et al. applied BKW also to the learning with rounding problem (LWR). The number of blocks is a parameter of BKW. By optimizing the number of blocks, we can minimize the time complexity of BKW. However, Duc et al. did not derive the optimal number of blocks theoretically, but they searched for it numerically. Duc et al. also showed that the required number of samples for BKW for solving LWE can be dramatically decreased using Lyubashevsky's idea. However, it is not shown that his idea is also applicable to LWR. In this paper, we theoretically derive the asymptotically optimal number of blocks, and then analyze the minimum asymptotic time complexity of the algorithm. We also show that Lyubashevsky's idea can be applied to LWR-solving BKW, under a heuristic assumption that is regularly used in the analysis of LPN-solving BKW. Furthermore, we derive an equation that relates the Gaussian parameter σ of LWE and the modulus p of LWR. When σ and p satisfy the equation, the asymptotic time complexity of BKW to solve LWE and LWR are the same.

key words: *lattice, learning with errors, learning with rounding, Blum-Kalai-Wasserman algorithm*

1. Introduction

Background.

The National Institute of Standards and Technology (NIST) initiated post-quantum cryptography (PQC) standardization [2] in December 2016. In the list of first-round candidates, there are several learning with errors problem (LWE) based schemes such as [3]–[7], and learning with rounding problem (LWR) based schemes such as [8]–[11]. Subsequently, NIST announced 26 second-round candidates selected from the 69 first-round candidates in January 2019. LWE-based [3]–[5] and LWR-based [10], [12] schemes still remain on the second-round candidate list. Therefore, studies on the algorithms for solving LWE and LWR are important for design and security analysis of post-quantum cryptosystems.

LWE, which is an extension of the learning parity with noise problem (LPN), is introduced by Regev [13]. An adversary of LWE receives samples $(\boldsymbol{a}_j, \langle \boldsymbol{a}_j, \boldsymbol{s} \rangle + e_j) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ $(j = 1, 2, \dots)$ from the oracle of LWE, where $\boldsymbol{a}_j$ is a uniformly random vector in $\mathbb{Z}_q^n$, $\boldsymbol{s}$ is a fixed secret vector in $\mathbb{Z}_q^n$, and $e_j \in \mathbb{Z}_q$ is a noise (usually, a discrete Gaussian noise). The goal of the adversary is to recover secret vector $\boldsymbol{s}$. LPN has a fixed modulus $q = 2$ and the noise follows the Bernoulli distribution. Regev [13] presents a reduction from worst-case lattice problems to the average-case LWE.

We can classify algorithms for solving LWE into two families. The first family uses lattice reduction techniques, which have been extensively studied [14]–[16]. The expected complexity of these algorithms is often considered when parameters for LWE-based schemes are discussed, such as in [17]. The second family is tailor-made for LPN and LWE without lattice reduction, which includes the main subject of this paper: the Blum-Kalai-Wasserman algorithm (BKW) [18]. BKW can be described as a "block-wise" and addition-only variant of the standard Gaussian elimination. First, we separate the vector $\boldsymbol{a}_j \in \mathbb{Z}_q^n$ into a blocks: We can write $\boldsymbol{a}_j = (\boldsymbol{a}_{j,1} \| \boldsymbol{a}_{j,2} \| \dots \| \boldsymbol{a}_{j,a})$, where $\boldsymbol{a}_{j,1}, \dots, \boldsymbol{a}_{j,a} \in \mathbb{Z}_q^{\frac{n}{a}}$, and then, by adding the samples together like the Gaussian elimination, we obtain "reduced" samples $\boldsymbol{a}'_j = (\boldsymbol{a}'_{j,1} \| \boldsymbol{0} \| \dots \| \boldsymbol{0})$. As reported in [19], improved variants of BKW such as [20], [21] are some of the asymptotically fastest algorithms. Although some algorithms [22] based on lattice reduction outperform these BKW-like algorithms for some parameter-sets (q, σ), it allows a heuristic [19].

LWR is proposed by Banerjee et al. [23] with its reduction from LWE. We can consider LWR as a deterministic variant of LWE in which the noise additions are replaced with deterministic rounding operations. An adversary of LWR receives samples $(\boldsymbol{a}_j, \lceil \frac{p}{q} \langle \boldsymbol{a}_j, \boldsymbol{s} \rangle \rfloor) \in \mathbb{Z}_q^n \times \mathbb{Z}_p$ $(j = 1, 2, \dots)$ from the LWR oracle, where p is a rounding modulus such that $p < q$. Compared with LWE-based cryptographic schemes, LWR-based schemes can be simply implemented because they replace the rich Gaussian error sampling process of the LWE-based schemes with the rounding operations (which can be simply implemented by rounding off the lower-order bits). LWR was initially applied to low-depth pseudorandom functions [23], [24], and there have been a number of applications, e.g., lossy trapdoor functions [25], public-key cryptosystems [10], [12] and key exchange protocol [9].

However, few studies have examined the complexity of

Manuscript received March 18, 2019.
Manuscript revised July 1, 2019.

[†]The authors are with KDDI Research, Inc., Fujimino-shi, 356-8502 Japan.
[††]The authors are with The University of Tokyo, Tokyo, 113-8654 Japan.

*A preliminary version of this paper was presented in [1] at ICISC 2018. This full version provides a technical contribution over [1] in Sect. 4.

a) E-mail: ir-okada@kddi-research.jp

DOI: 10.1587/transfun.2019CIP0022

LWR, while the complexity of LWE has been extensively studied. The complexity of LWR is often estimated by adopting the LWE-solving algorithms to LWR. Albrecht et al. [17] estimate the cost of running primal and dual lattice attacks, which is based on lattice reduction techniques, against lattice-based schemes including LWE-based and LWR-based schemes in the list of the first-round submissions for the NIST PQC. They consider that the cost of lattice attacks for LWE and LWR are the same when the equation $\sigma = \frac{q}{2\sqrt{3}p}$ holds, as considered in [8], [10]. This equation is simply derived by comparing the variance of the Gaussian noise of LWE and the "rounding error" of LWR. Note that the equation, which relates the hardness of LWR and LWE, is limited to attacks based on lattice reduction techniques, and it is not shown that the conversion equation can be applied for BKW.

Previous Works. BKW initially targeted LPN, and its time complexity is sub-exponential in $2^{O(n/\log n)}$. Albrecht et al. [26] expanded it to solve LWE whose time complexity is $q^{O(n/\log n)}$. Duc et al. [27] improved Albrecht et al.'s BKW and also introduced its variant for LWR, which was the first algorithmic analysis of LWR. They showed that the time complexity of the LWR-solving algorithm is $q^{O(n/\log n)}$ when the number of blocks is $a = O(\log n)$. However, they did not show that this choice of a is optimal; thus the minimum time complexity of the algorithm is not shown.

Furthermore, Duc et al. applied Lyubashevsky's idea [28] to LWE and showed that the minimum required number of samples using his method is $n^{1+(\log q+1)/\log n}$, at the expense of increasing the size of the noise. However, they did not show that Lyubashevsky's idea can also be applied to LWR.

After BKW proposed by Albrecht et al., new variants of BKW [20], [21], [29], [30] for solving the *small-secret* LWE, whose secret vector $\boldsymbol{s}$ is extremely small (e.g. $\boldsymbol{s} \in \{0,1\}^n$), have been proposed. These algorithms can be applied to the general LWE, whose secret vector $\boldsymbol{s}$ is uniform in $\mathbb{Z}_q^n$, by transforming the general LWE to *small-secret* LWE problem with a technique called *secret-error switching*, and it is shown that some of these algorithms [20], [21] solve the general LWE problem faster. However, it is not shown that these new types of BKW can be applied to LWR. In order to apply the *secret-error switching* technique to LWR, we need to convert LWR samples into LWE samples with uniform error by substituting the LWR samples $(\boldsymbol{a}_j, \lceil \frac{p}{q}\langle \boldsymbol{a}_j, \boldsymbol{s}\rangle \rfloor)$ with $(\boldsymbol{a}_j, \frac{q}{p}\lceil \frac{p}{q}\langle \boldsymbol{a}_j, \boldsymbol{s}\rangle \rfloor)$, and solving this converted LWR with their algorithm is out of reach, as mentioned in [21]. On the other hand, Duc et al.'s LWR-solving BKW does not need to convert LWR samples into LWE samples; the algorithm is tailor-made for solving LWR.

Our Contribution. Our work mainly targets the asymptotic complexity for solving the LWR problem, rather than for specific LWR instances with the parameters used in NIST PQC candidates.

In Sect. 3, we first review Duc et al.'s LWR-solving BKW, and then derive the time complexity in a simpler form. Subsequently, we theoretically derive the optimal choice of the number of blocks a that asymptotically minimize the time complexity, while Duc et al. searched numerically for the optimal a in [27]]. Thus, an entirely theoretical analysis of the time complexity of the algorithm is shown in this paper: We show that the minimum time complexity of BKW is $t = q^{O(n/\log n)}$ and the required number of samples is $m = q^{O(n/\log n)}$. We also confirm that the derived parameter is accurately optimal by showing the results of some concrete instances of LWR, and that they fit the results given by Duc et al.

In Sect. 3.4, we derive a conversion equation between the Gaussian parameter σ in LWE and the rounding modulus p in LWR, by comparing the time complexity of BKW for LWE and LWR: We show that the time complexity of BKW to solve LWE and that to solve LWR are the same when σ and p satisfy equation $\sigma = \frac{q}{2\sqrt{3}p}$. This equation coincides with the equation derived from the complexity analysis of the attacks based on lattice reduction techniques. Thus, our result means that the equation is applicable also for complexity analysis based on BKW.

In Sect. 4, we apply Lyubashevsky's idea (hereinafter called *sample amplification*) to the LWR problem, and show that the minimum required number of samples for LWR-solving BKW with sample amplification is $m = O(n \log q)$, while it is shown that the LWR-solving BKW requires $m = q^{O(n/\log n)}$ samples in Sect. 3. This result means that the LWR-solving BKW algorithm is also applicable in a practical situation where we can obtain only a polynomial-size number of LWR samples, using the sample amplification technique.

2. Preliminaries

Notations.

We denote the logarithm of base 2 and the natural logarithm as $\log(\cdot)$ and $\ln(\cdot)$, respectively. We denote the imaginary unit as i, and a real part of $x \in \mathbb{C}$ as $\mathrm{Re}(x)$. We let $\lceil \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$ be the rounding function that rounds to the closest integer (in the case of equality, we take the floor). We define $\theta_q := e^{\frac{2\pi i}{q}}$ and also $\theta_p := e^{\frac{2\pi i}{p}}$. We write vectors in bold. By $\boldsymbol{a}_j$ we denote the j-th vector of the list of vectors. We denote a partial vector of a vector $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ by $\boldsymbol{a}_{(k,l)} := (a_k, a_{k+1}, \ldots, a_l)$, where $1 \le k \le l \le n$. By $(\boldsymbol{a}\|\boldsymbol{b})$ we denote the concatenation of two vectors $\boldsymbol{a}$ and $\boldsymbol{b}$. We denote the Hamming weight of the vector $\boldsymbol{x}$ by $\mathrm{Hw}(\boldsymbol{x})$. We denote by $\langle \cdot, \cdot \rangle$ the usual dot product of two vectors, and we define $\langle \cdot, \cdot \rangle_q := \langle \cdot, \cdot \rangle \pmod q$. We denote the empty set by $\emptyset$. We write $\boldsymbol{s} \xleftarrow{U} \mathcal{S}$ to denote the process of sampling $\boldsymbol{s}$ uniformly at random over $\mathcal{S}$, and we write $e \leftarrow \chi$ to denote the process of sampling e according to a probability distribution χ.

2.1 LWE and LWR

LWE oracle and LWE are defined as follows.

Definition 1 (LWE oracle). *Let n, q be positive integers.*

Learning with Error (LWE) oracle $\mathsf{LWE}_{s,\chi}$ for a fixed vector $s \in \mathbb{Z}_q^n$ and probability distribution χ over $\mathbb{Z}_q$ is an oracle returning $\left\{(a, c) \,\middle|\, c = \langle a, s\rangle + e \bmod q,\ a \xleftarrow{U} \mathbb{Z}_q^n,\ e \leftarrow \chi\right\}$.

For the distribution of noise χ, variants of the Gaussian distribution that is discretized into $\mathbb{Z}_q$ are used. In this paper, we consider two types of Gaussian distributions that are considered in [27]; the *rounded Gaussian distribution* $\bar{\Psi}_{\sigma,q}$ and the *discrete Gaussian distribution* $D_{\sigma,q}$. The probability mass function of $\bar{\Psi}_{\sigma,q}$ for integer x in the interval $]-\frac{q}{2}, \frac{q}{2}]$, is given by $\Pr[x \leftarrow \bar{\Psi}_{\sigma,q}] = \int_{x-\frac{1}{2}}^{x+\frac{1}{2}} g(\theta; q, \sigma)d\theta$, where $g(\theta; q, \sigma) := \sum_{l=-\infty}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(\theta+lq)^2}{2\sigma^2}}$, for $\theta \in \left]-\frac{q}{2}, \frac{q}{2}\right]$. The probability mass function of $D_{\sigma,q}$ is, for x an integer in $]-\frac{q}{2}, \frac{q}{2}]$, $\Pr[x \leftarrow D_{\sigma,q}] = e^{-\frac{x^2}{2\sigma^2}} / \sum_{y\in]-\frac{q}{2},\frac{q}{2}]} e^{-\frac{y^2}{2\sigma^2}}$.

Definition 2 (LWE problem)**.** *LWE is the problem of recovering the hidden secret s given m samples $(a_j, c_j) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ $(j = 1, 2, \ldots, m)$ received from $\mathsf{LWE}_{s,\chi}$.*

LWE oracle and LWE, which are the main focus of this paper, are defined as follows.

Definition 3 (LWR oracle)**.** *Let n, q be natural numbers. Learning with Rounding (LWR) oracle $\mathsf{LWR}_{s,p}$ for a hidden vector $s \in \mathbb{Z}_q^n$ and rounding modulus p is an oracle returning* $\left\{(a, c) \,\middle|\, c = \left\lceil \frac{p}{q}\langle a, s\rangle_q \right\rfloor,\ a \xleftarrow{U} \mathbb{Z}_q^n\right\}$.

Definition 4 (LWR problem)**.** *LWR is the problem of recovering the hidden secret s given m samples $(a_j, c_j) \in \mathbb{Z}_q^k \times \mathbb{Z}_q$ $(j = 1, 2, \ldots, m)$ received from $\mathsf{LWR}_{s,p}$.*

The rounding calculation in the LWR sample generates a "rounding error," which is similar to the Gaussian noise added in the LWE sample. Duc et al. proved that "rounding error" follows a uniform distribution, in Lemma 19 in [27].

Lemma 5 (Lemma 19. in [27])**.** *Let n and $p \geq 2$ be positive integers, $q > p$ be prime. Let (a, c) be a random sample from an LWR oracle $\mathsf{LWR}_{s,p}$. Then, the "rounding error," given by*

$$\xi = \frac{p}{q}\langle a, s\rangle_q - c, \tag{1}$$

follows the uniform distribution in a discrete subset of $[-\frac{1}{2}, \frac{1}{2}]$ with mean zero. Furthermore, the characteristic function of ξ, for $t \in \mathbb{R}_{\neq 0}$, is

$$\phi_\xi(t) := E[e^{\pm it\xi}] = \frac{\sin(\frac{t}{2})}{q \sin(\frac{t}{2q})}. \tag{2}$$

Banerjee et al., showed a reduction from LWE to LWR, in the paper [23] in which they first introduced LWR. Alwen et al. [25] also showed a reduction without the super-polynomial parameters, but it limits the number of samples that the LWR oracle allows the adversary to receive.

2.2 Duc et al.'s BKW for LWR

We recall Duc et al.'s BKW to solve LWR. BKW consists of three stages: 1) Sample reduction, 2) Hypothesis testing, and 3) Back substitution. For simplicity, we consider only the case that the number of blocks a and the block length b satisfy $ab = n$.

Stage 1: Sample reduction. We receive m samples $\{(a_j, c_j)\}_{j=1}^m$ from LWR oracle $\mathsf{LWR}_{s,p}$, and represent the set of samples as $\mathcal{S} := \{(a_j, c_j)\}_{j=1}^m$. We separate the vector $a_j \in \mathbb{Z}_q^n$ into a blocks whose length are b: We can write $a_j = (a_{j(1,b)} \| a_{j(b+1,2b)} \| \ldots \| a_{j((a-1)b+1,ab)})$. In Stage 1, our goal is to produce samples whose elements are all zero except for the first block, with the addition or subtraction of pairs of samples. For $l = 0$, we extract a sample (a, c) from $\mathcal{S}$, and search another sample (a', c') such that $(a \pm a')_{((a-1)b+1,ab)} = \mathbf{0}$, then we store the sample $(a \pm a', c \pm c')$ in the temporary set $\mathcal{S}'$. If a sample (a, c) already holds $a_{((a-1)b+1,ab)} = \mathbf{0}$, we directly store it in $\mathcal{S}'$. If we cannot find the sample (a', c') such that $(a \pm a')_{((a-1)b+1,ab)} = \mathbf{0}$, we store the sample (a, c) in $\mathcal{T}_0$. After we finish extracting samples and empty the set $\mathcal{S}$, we renew $\mathcal{S} \leftarrow \mathcal{S}'$ and move on to the next step for $l = 1$. In this manner, we recursively generate the sets $\mathcal{T}_l$ for $0 \leq l \leq a - 2$, and then we set $\mathcal{T}_{a-1} \leftarrow \mathcal{S}$ in the end. Note that the samples (a, c) in $\mathcal{T}_l$ hold $a_{((a-l)b+1,ab)} = \mathbf{0}$ (except for $l = 0$). In particular, the samples (a, c) in $\mathcal{T}_{a-1}$ hold $a_{(b+1,ab)} = \mathbf{0}$. We may think of the reduced samples in T_{a-1} as the set of samples of the b-dimensional LWR, although the variance of their noise is larger than those of the original samples. Hereinafter, the samples in $\mathcal{T}_l$ are termed "reduced samples," and represent $\mathcal{T}_l = \{(\overline{a}_j^l, \overline{c}_j^l)\}_{j=1}^{m_l}$, where $m_l := \#\mathcal{T}_l$. Note that the maximum number of samples whose $(a - l)$-th block cannot vanish is $\frac{q^b-1}{2}$, and the minimum (worst) number of reduced samples in $\mathcal{T}_{a-1}$ (i.e. minimum value of m_{a-1}) is

$$m' = m - (a - 1)\frac{q^b - 1}{2}. \tag{3}$$

Stage 2: Hypothesis testing. For simplicity, we explain Stage 2 and Stage 3 only for $l = a - 1$[†]. For simplicity of notation, we define a b-dimensional vector $\overline{a}_j := (\overline{a}_j^{a-1})_{(1,b)}$, and denote $\overline{c}_j := \overline{c}_j^{a-1}$. The goal of this stage is to estimate the first b elements of s, denoted as $s_{(1,b)}$. We define the function $f(y) := \sum_{j=1}^{m'} \mathbb{1}_{\{\overline{a}_j = y\}} \theta_p^{\overline{c}_j}$, where $y \in \mathbb{Z}_q^b$, $\theta_p := e^{\frac{2\pi i}{p}}$, and $\mathbb{1}_{\{\overline{a}_j = y\}}$ is 1 when $\overline{a}_j = y$ is true and 0 otherwise. The discrete Fourier transform of f is

$$\hat{f}(z) := \sum_{y\in\mathbb{Z}_q^b} f(y)\theta_q^{-\langle y,z\rangle} = \sum_{j=1}^{m'} \theta_p^{-(\frac{p}{q}\langle \overline{a}_j, z\rangle - \overline{c}_j)}. \tag{4}$$

Then, we search the max $\mathrm{Re}(\hat{f}(z))$, and output $s_{(1,b)} =$

[†]In Sect. 3.1, we consider only the time complexity to recover $s_{(1,b)}$ because the whole time complexity of the algorithm is at most a positive constant multiple of it.

$\mathrm{argmax}_z \mathrm{Re}(\hat{f}(z))$. We explain how the output estimates the secret vector. We define the "rounding error" of the reduced samples $\{(\overline{\boldsymbol{a}}_j, \overline{c}_j)\}_{j=1}^{m'}$ by $\overline{\xi}_j := \frac{p}{q}\langle \overline{\boldsymbol{a}}_j, \boldsymbol{s}_{(1,b)}\rangle - \overline{c}_j$, as like (1). Recall that the $\overline{\boldsymbol{a}}_j$ is produced by $a-1$ times of the "tree-like" addition of the original samples in the process of Stage 1, i.e. $\overline{\boldsymbol{a}}_j$ is the sum of the 2^{a-1} original samples, thus we can write $\overline{\boldsymbol{a}}_j = (\boldsymbol{a}_{j,1} \pm \boldsymbol{a}_{j,2} \pm \cdots \pm \boldsymbol{a}_{j,2^{a-1}})_{(1,b)}$, where $\boldsymbol{a}_{j,1}, \ldots, \boldsymbol{a}_{j,2^{a-1}}$ are the original samples. Similarly, we can write $\overline{c}_j = c_{j,1} \pm c_{j,2} \pm \cdots \pm c_{j,2^{a-1}}$, and obtain $\overline{\xi}_j = \frac{p}{q}\langle \boldsymbol{a}_{j,1} \pm \boldsymbol{a}_{j,2} \pm \cdots \pm \boldsymbol{a}_{j,2^{a-1}}, \boldsymbol{s}\rangle - (c_{j,1} \pm c_{j,2} \pm \cdots \pm c_{j,2^{a-1}}) = \sum_{k=1}^{2^{a-1}} \frac{p}{q}\langle \boldsymbol{a}_{j,k}, \boldsymbol{s}\rangle - c_{j,k} = \sum_{k=1}^{2^{a-1}} \xi_{j,k}$, where the $\xi_{j,k}$ are independent rounding errors from original samples. From the above equation and (4), when $z = \boldsymbol{s}_{(1,b)}$, we obtain $\hat{f}(\boldsymbol{s}_{(1,b)}) = \sum_{j=1}^{m'} \theta_p^{-(\sum_{k=1}^{2^{a-1}} \xi_{j,k})}$. On the other hand, when $z \neq \boldsymbol{s}_{(1,b)}$, $\frac{p}{q}\langle \overline{\boldsymbol{a}}_j, z\rangle - \overline{c}_j$ distribute uniformly in $]0, p]$.

Thus, when we select an appropriate value of parameter a such that the sum of the rounding errors $\sum_{k=1}^{2^{a-1}} \xi_{j,k}$ does not grow too large, $\mathrm{Re}(\hat{f}(\boldsymbol{s}))$ is so much larger than $\mathrm{Re}(\hat{f}(z))$ that the hypothesis test succeeds with high probability.

Stage 3: Back substitution. Using the obtained $\boldsymbol{s}_{(1,b)}$, update the sets $\mathcal{T}_l$ by zeroing-out b elements in each sample: Replace all $(\boldsymbol{a}, c) \in \mathcal{T}_{l'}$ for $0 \le l' < a-1$ with $(\boldsymbol{a}', c')$, where $\boldsymbol{a}' = (\boldsymbol{0} \| \boldsymbol{a}_{(b+1,n)}) \in \mathbb{Z}_q^n$, $c' = c - \frac{p}{q}\langle \boldsymbol{a}_{(1,b)}, \boldsymbol{s}_{(1,b)}\rangle_q \in \mathbb{Z}_p$. Then back to Stage 2 to obtain $\boldsymbol{s}_{(b+1,2b)}$.

Repeating a rounds of Stages 2 to 3, we estimate $\boldsymbol{s}_{(1,b)}$, $\boldsymbol{s}_{(b+1,2b)}$, $\ldots$, $\boldsymbol{s}_{(a(b-1)+1,ab)}$, and obtain $\boldsymbol{s} = (\boldsymbol{s}_{(1,b)} \| \boldsymbol{s}_{(b+1,2b)} \| \ldots \| \boldsymbol{s}_{((a-1)b+1,ab)})$.

3. Our Analysis of BKW

We derive the minimum time complexity and the minimum number of required samples, by optimizing the number of blocks a which is a parameter of BKW. As with Duc et al., we consider only the case that the block length b satisfy $n = ab$, for simplicity. Therefore, the block length b is determined by the number of blocks a, as $b = \frac{n}{a}$. Note that the complexity of BKW for the general case, where $n = (a-1)\cdot b + n'$ and $n' < b$, is asymptotically the same with that for the case where $ab = n$. We always consider q to be a prime, and $q > p > 4$ because we need the condition to prove Lemma 7.

In Sect. 3.1, we analyze the time complexity of BKW for solving LWR, using a as a parameter. Then, we derive the optimal value of a that asymptotically minimizes the asymptotic time complexity in Sect. 3.2. We confirm that the optimal value of a minimizes the time complexity of the algorithm in Sect. 3.3, by calculating the concrete time complexity of BKW for several LWR instances. Furthermore, in Sect. 3.4, we derive an equation that relates σ of LWE and p of LWR. When σ and p satisfy the equation, the asymptotic time complexity of BKW to solve LWE and LWR are the same.

3.1 Complexity

We analyze the time complexity and the required number of samples to solve LWR. We asymptotically analyze the time complexity and make it in a simple form so that we can theoretically derive the optimal number of blocks a in Sect. 3.2. We first refer to Lemma 6 (Theorem 23. in [27]), which is the analysis of the minimum number of samples needed to solve LWR.

Lemma 6 (Theorem 23. in [27])**.** *We define the probability that the algorithm cannot recover the correct answer* $\epsilon := \Pr\left[\mathrm{argmax}_z \mathrm{Re}\left(\hat{f}(z)\right) \neq \boldsymbol{s}_{(1,b)}\right]$*. Then, the number of samples required to solve* LWR *with oracle* $\mathsf{LWR}_{s,p}$ *is*

$$m^{\mathsf{LWR}} = \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left((R_{q,p})^{2^{a-1}} - (3/p)^{2^{a-1}}\right)^{-2} + (a-1)\frac{q^{\frac{n}{a}}-1}{2}, \tag{5}$$

where $R_{q,p} := \frac{\sin\left(\frac{\pi}{p}\right)}{q\sin\left(\frac{\pi}{pq}\right)}$.

Note that $R_{q,p}$ is derived based on the characteristic function of the "rounding error" given in (2): $R_{q,p} = \phi_\xi(\frac{2\pi}{p})$ holds. As discussed later, this m^{LWR} in (5) is the main term of the time complexity of the algorithm.

In the following Lemma 7, we analyze the asymptotic behavior of the complicated part of the m^{LWR}. We describe it in a simpler form in order to enable the analysis of the minimum time complexity, which is given later in Sect. 3.2. Note that we use the error rate of the LWR sample $\alpha_{\mathrm{lwr}} := \frac{1}{p}\sqrt{\frac{\pi}{6}}$ [8] to describe the time complexity for simplicity of notation.

Lemma 7. *Let* $\alpha_{\mathrm{lwr}} := \frac{1}{p}\sqrt{\frac{\pi}{6}}$*. When* $q > p > 4$*, we have*

$$\left((R_{q,p})^{2^{a-1}} - (3/p)^{2^{a-1}}\right)^{-2} = e^{\pi\alpha_{\mathrm{lwr}}^2 2^a} + O\left(\frac{1}{p^2q^2}\right). \tag{6}$$

Proof. When $q > p > 4$, we obtain $R_{q,p} = \frac{\frac{p}{\pi}\sin\left(\frac{\pi}{p}\right)}{\frac{pq}{\pi}\sin\left(\frac{\pi}{pq}\right)} \ge \frac{p}{\pi}\sin\left(\frac{\pi}{p}\right)$. Since $\frac{p}{\pi}\sin\left(\frac{\pi}{p}\right)$ is monotonically increasing when $p > 4$, we obtain $R_{q,p} > \frac{4}{\pi}\sin\left(\frac{\pi}{4}\right) \simeq 0.9003$, and $R_{q,p} > 3/p$. Let $x = (R_{q,p})^{2^{a-1}}$ and $y = (3/p)^{2^{a-1}}$, then we have $\frac{y}{x} < 1$. Using Taylor expansion, we obtain $(x-y)^{-2} = \frac{1}{x^2}\left(1 + O(\frac{y}{x})\right)$. Therefore, we obtain $\left((R_{q,p})^{2^{a-1}} - (3/p)^{2^{a-1}}\right)^{-2} = (R_{q,p})^{-2^a} + O\left(\frac{1}{p^{2^{a-1}}}\right)$. Using Taylor expansion, we obtain $R_{q,p} = 1 - \frac{\pi^2}{6p^2} + O\left(\frac{1}{p^2q^2}\right) = 1 - \pi\alpha_{\mathrm{lwr}}^2 + O\left(\frac{1}{p^2q^2}\right)$, and $R_{q,p} - e^{-\pi\alpha_{\mathrm{lwr}}^2} = O\left(\frac{1}{p^2q^2}\right)$. Consequently, from this equation, we obtain $\left(R_{q,p}\right)^{-2^a} = e^{\pi\alpha_{\mathrm{lwr}}^2 2^a} + O\left(\frac{1}{p^2q^2}\right)$. Thus, we have (6). □

We can now derive the number of required samples and the time complexity of the algorithm.

Theorem 8. *Let* n *and* $p > 4$ *be positive integers,* $q > p$ *be a prime, and* a *be a natural number. Fix* $\epsilon \in (0, 1)$.

When at least $m^{\mathsf{LWR}} = \mathrm{poly}(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}, q^{\frac{n}{a}})$ *samples are given by* LWR *oracle* $\mathsf{LWR}_{s,p}$*, the time complexity of BKW to recover secret* $\boldsymbol{s}$ *with a probability of at least* $1-\epsilon$ *is* $t^{\mathsf{LWR}} = \mathrm{poly}(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}, q^{\frac{n}{a}})$*, where* $\alpha_{\mathrm{lwr}} = \frac{1}{p}\sqrt{\frac{\pi}{6}}$.

Proof. From Lemma 6 and Lemma 7, the number of required samples to solve LWR is

$$m^{\mathsf{LWR}} = \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a} + O\left(\frac{1}{p^2q^2}\right)\right) + (a-1)\frac{q^{\frac{n}{a}}-1}{2}. \tag{7}$$

Recall that the number of the "reduced" samples we obtain after Stage 1 is $m' = m^{\mathsf{LWR}} - (a-1)\frac{q^{\frac{n}{a}}-1}{2} = \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a} + O\left(\frac{1}{p^2q^2}\right)\right)$, which is defined in (3).

In Stage 1, since we apply the addition for $O(m^{\mathsf{LWR}})$ samples in $\mathbb{Z}_q^n$ for $a-1$ times, the time complexity is $t_1 = O(anm^{\mathsf{LWR}})$. In Stage 2, we first calculate $f(\boldsymbol{y}) := \sum_{j=1}^{m'} \mathbb{1}_{\{\overline{\boldsymbol{a}}_j=\boldsymbol{y}\}}\theta_p^{\bar{c}_j}$, for all $\boldsymbol{y} \in \mathbb{Z}_q^b$. Since we need only to calculate $f(\boldsymbol{y})$ for $\boldsymbol{y} \in \{\overline{\boldsymbol{a}}_j\}_{j=1}^{m'}$, the time complexity for calculating $f(\boldsymbol{y})$ is $O(m') = O(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}(\frac{n}{a})\ln q)$. After that, we compute the DFT of f, the complexity of which is $O(q^{\frac{n}{a}}(\frac{n}{a})\ln q)$. Finally, we search max $\hat{f}(\boldsymbol{z})$ defined in (4) for all $\boldsymbol{z} \in \mathbb{Z}_q^{\frac{n}{a}}$, the time complexity of which is $O(q^{\frac{n}{a}}\frac{n}{a})$. Thus, the time complexity of Stage 2 is $t_2 = O(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}(\frac{n}{a})\ln q) + O(q^{\frac{n}{a}}(\frac{n}{a})\ln q)$. In Stage 3, since we update all samples stored in $\mathcal{T}_{l'}$ (the total number of these samples is $m^{\mathsf{LWR}} - m'$) with inner product calculation of the vectors in $\mathbb{Z}_q^{\frac{n}{a}}$, and the time complexity is $t_3 = O((m^{\mathsf{LWR}} - m')\frac{n}{a}) = O(q^{\frac{n}{a}}\frac{n}{a})$. Therefore, the time complexity of BKW is $t^{\mathsf{LWR}} = t_1 + t_2 + t_3 = O(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}(\frac{n}{a})\ln q) + O(q^{\frac{n}{a}}(\frac{n}{a})\ln q) = \mathrm{poly}(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}, q^{\frac{n}{a}})$. □

3.2 Optimization

We analyze the optimal choice for input parameter a to asymptotically minimize the asymptotic time complexity of BKW to solve LWR. Furthermore, we analyze the minimum time complexity.

Theorem 9 (Optimal choice of a)**.** *The optimal parameter* a *that asymptotically minimizes the asymptotic time complexity of the algorithm to solve* LWR *is*

$$a = \left\lfloor \frac{1}{\ln 2} W\left(\frac{n\ln q\ln 2}{\pi\alpha_{\mathrm{lwr}}^2}\right)\right\rfloor \tag{8}$$

where W *is Lambert W function [31].*

Proof. From Theorem 8, we obtain the time complexity $t = O(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}(\frac{n}{a})\ln q) + O(q^{\frac{n}{a}}(\frac{n}{a})\ln q)$. Note that $e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}$ monotonically increases and $q^{\frac{n}{a}}$ monotonically decreases, as a increases. Therefore, the time complexity is asymptotically minimized[†] when a satisfies

$$e^{\pi\alpha_{\mathrm{lwr}}^2 2^a} = q^{\frac{n}{a}}. \tag{9}$$

From (9), by simple arithmetic, we obtain $(\ln 2)ae^{(\ln 2)a} = \frac{n\ln q\ln 2}{\pi\alpha_{\mathrm{lwr}}^2}$. To solve this equation in terms of a, we use the Lambert W function, which satisfies $W(ze^z) = z$. We obtain $W((\ln 2)ae^{(\ln 2)a}) = (\ln 2)a$, and (8). □

Since the Lambert function $W(x)$ has an asymptotic form as $W(x) = \ln(x) - \ln(\ln(x)) + o(1)$, we can evaluate $a = \frac{1}{\ln 2}\left(\ln\left(\frac{n\ln q\ln 2}{\pi\alpha_{\mathrm{lwr}}^2}\right) - \ln\ln\left(\frac{n\ln q\ln 2}{\pi\alpha_{\mathrm{lwr}}^2}\right)\right) + o(1)$. Furthermore, when we consider q to be at most exponential of n (this range of q includes most of q used in LWE cryptosystems), we obtain $\log q = O(n)$, and $a = O(\log n)$. Using this value, (9), and Theorem 8, we obtain the corollary below.

Corollary 10 (Minimum time complexity)**.** *Let* n *and* $q > p > 4$ *be prime numbers. Let* $a = \left\lfloor \frac{1}{\ln 2} W\left(\frac{n\ln q\ln 2}{\pi\alpha_{\mathrm{lwr}}^2}\right)\right\rfloor$*, where* $\alpha_{\mathrm{lwr}} = \frac{1}{p}\sqrt{\frac{\pi}{6}}$*. Fix* $\epsilon \in (0,1)$*. When at least* $q^{O(n/\log n)}$ *samples are given by* LWR *oracle* $\mathsf{LWR}_{s,p}$*, the time complexity of BKW to recover secret* $\boldsymbol{s}$ *with a probability of at least* $1-\epsilon$ *is* $q^{O(n/\log n)}$.

3.3 Concrete Analysis

Table 1 shows the concrete time complexity of BKW. We denote the time complexity of the LWR-solving BKW by C^{LWR}. Then, similar to Theorem 17 in [27], we obtain

$$C^{\mathsf{LWR}} = \frac{1}{4}(a-2)(a-1)\left(\frac{2n}{a}+1\right)(q^{\frac{n}{a}}-1) + nq^{\frac{n}{a}}\log(q) + \sum_{j=0}^{a-1} m'^{\mathsf{LWR}}_{j,\epsilon}\left(\frac{a-1-j}{2}(n+2)+2\right), \tag{10}$$

where $m'^{\mathsf{LWR}}_{j,\epsilon} := \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left(R_{q,p}^{2^{a-1-j}} - (3/p)^{2^{a-1-j}}\right)^{-2}$. We use the same parameters n, q and p as in Table 2 in [27]: For type (a), $q = \mathrm{nextprime}(\lceil(2\sigma n)^3\rceil)$, $p = \mathrm{nextprime}(\lceil\sqrt[3]{q}\rceil)$ and for type (b), $p = 13$, $q = \mathrm{nextprime}(\lceil 2\sigma np\rceil)$, where $\sigma = \frac{n^2}{\sqrt{2\pi n}(\log(n))^2}$. These parameters are selected based on Corollary 4.2 in [25]. Type (a) parameters maximize the efficiency, and type (b) parameters minimize the modulus to error ratio (q/σ). Note that we also ignored the constraint on the number of samples m as Duc et al. did. We set $a = \left\lfloor \frac{1}{\ln 2} W\left(\frac{n\ln q\ln 2}{\pi\alpha_{\mathrm{lwr}}^2}\right)\right\rfloor$ and calculate m^{LWR} and C^{LWR} in (5) and (10), respectively. We also set $\epsilon = 0.01$ in Table 1,

[†]Let $\tilde{a}$ satisfies $e^{\pi\alpha_{\mathrm{lwr}}^2 2^{\tilde{a}}} = q^{n/\tilde{a}}$, and Let $t_{\tilde{a}}$ be the time complexity with $a = \tilde{a}$, namely $t_{\tilde{a}} = O(e^{\pi\alpha_{\mathrm{lwr}}^2 2^{\tilde{a}}}(\frac{n}{\tilde{a}})\ln q)$. If we set $a > \tilde{a}$, then we obtain $t_a = O(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}(\frac{n}{a})\ln q)$, and $t_a > t_{\tilde{a}}$ since $e^{\pi\alpha_{\mathrm{lwr}}^2 2^a} > e^{\pi\alpha_{\mathrm{lwr}}^2 2^{\tilde{a}}}$. If we set $a < \tilde{a}$, then we obtain $t = O(q^{\frac{n}{a}}(\frac{n}{a})\ln q)$, and $t_a > t_{\tilde{a}}$ since $q^{\frac{n}{a}} > q^{n/\tilde{a}}$. Therefore, $\tilde{a}$ is asymptotically optimal.

Table 1 Time and sample complexity for the LWR-solving BKW.

	LWR instance: type (a)					LWR instance: type (b)				
n	q	p	a	$\log(C^{\mathsf{LWR}})$	$\log(m^{\mathsf{LWR}})$	q	p	a	$\log(C^{\mathsf{LWR}})$	$\log(m^{\mathsf{LWR}})$
32	6318667	191	19*	51.00	42.70	2411	13	11*	44.53	37.00
40	23166277	293	20*	60.66	52.18	3709	13	11*	53.24	45.44
64	383056211	733	24† (23)	92.70† (92.10)	83.08† (82.80)	9461	13	12*	81.48	72.92
80	1492443083	1151	25*	110.82	101.11	14867	13	12*	103.76	94.86
96	4587061889	1663	26*	132.17	122.15	21611	13	12*	126.83	117.66
112	11942217841	2287	28*	148.00	137.68	29717	13	13*	140.08	130.63
128	27498355153	3023	29*	167.44	156.88	39241	13	13*	162.50	152.84

* : optimal value. † : not optimal value. The optimal values are shown in parenthesis.

in accordance with the setting given in Table 2 of [27]. In Table 1, we can observe that our choice of the number of blocks a asymptotically (but almost exactly) minimizes the time complexity of the algorithm.

3.4 Relation between LWE and LWR

We compare the time complexity of BKW to solve LWE and LWR, and then derive a relation between p in LWR and σ in LWE. We showed that the time complexity of BKW to solve LWR is $\mathrm{poly}(e^{\pi\alpha_{\mathrm{lwr}}^2 2^a}, q^{\frac{n}{a}})$ in Theorem 8. On the other hand, based on Theorem 16 in [27], Kaminakaya et al. [32] analyzed the time complexity of BKW to solve LWE, and showed that the complexity is $\mathrm{poly}(e^{\pi\alpha_{\mathrm{lwe}}^2 2^a}, q^{\frac{n}{a}})$, where $\alpha_{\mathrm{lwe}} := \frac{\sqrt{2\pi}\sigma}{q}$. We describe the result later in Lemma 12 and refer to the proof given in [32]. As a preparation, we refer to Theorem 16 in [27], which shows the number of samples required to solve LWE:

Lemma 11 (Theorem 16. in [27]). *Let* $\epsilon := \Pr\left[\mathrm{argmax}_{\boldsymbol{z}} \mathrm{Re}\left(\hat{f}(\boldsymbol{z})\right) \neq \boldsymbol{s}_{(1,b)}\right]$ *be the probability that the algorithm does not recover the correct answer. Then, the number of samples required to solve LWE with oracle* $\mathsf{LWE}_{s,\chi}$ *is* $m^{\mathsf{LWE}} = \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)(R_{q,\sigma,\chi})^{-2^a} + (a-1)\frac{q^{\frac{n}{a}}-1}{2}$, *where*

$$R_{q,\sigma,\chi} = \begin{cases} \frac{q}{\pi}\sin\left(\frac{\pi}{q}\right)e^{-2\pi^2\sigma^2/q^2} & \text{when } \chi = \bar{\Psi}_{q,\sigma}, \\ 1 - \frac{2\pi^2\sigma^2}{q^2} & \text{when } \chi = D_{q,\sigma}. \end{cases}$$

We can show the time complexity of BKW for LWE based on this Lemma:

Lemma 12 ([32]). *Let a and b be natural numbers such that $ab = n$. There is an algorithm to solve LWE whose oracle is $\mathsf{LWE}_{s,\chi}$, with the number of samples $m = \mathrm{poly}(e^{\pi\alpha_{\mathrm{lwe}}^2 2^a}, q^{\frac{n}{a}})$, and the time complexity $t = \mathrm{poly}(e^{\pi\alpha_{\mathrm{lwe}}^2 2^a}, q^{\frac{n}{a}})$, where $\alpha_{\mathrm{lwe}} := \frac{\sqrt{2\pi}\sigma}{q}$, both when $\chi = D_{\sigma,q}$ and $\chi = \bar{\Psi}_{\sigma,q}$.*

Proof. Here, we refer the proof given in [32]. Similar to the proof of Theorem 8, using Lemma 11, we can prove that there is an algorithm to solve LWE whose oracle is $\mathsf{LWE}_{s,\chi}$, with number of samples $m = \mathrm{poly}(\left(R_{q,\sigma,\chi}\right)^{-2^a}, q^{\frac{n}{a}})$, and time complexity $t = \mathrm{poly}(\left(R_{q,\sigma,\chi}\right)^{-2^a}, q^{\frac{n}{a}})$. Thus, we need only prove that $R_{q,\sigma,\chi} = O(e^{-\pi\alpha_{\mathrm{lwe}}^2})$ holds, both when $\chi = \bar{\Psi}_{\sigma,q}$ and when $\chi = D_{\sigma,q}$. When $\chi = \bar{\Psi}_{\sigma,q}$, since $\sin\left(\frac{\pi}{q}\right) < \frac{\pi}{q}$, we obtain $R_{q,\sigma,\chi} < e^{-2\pi^2\sigma^2/q^2} = e^{-\pi\alpha_{\mathrm{lwe}}^2}$, which means $R_{q,\sigma,\chi} = O(e^{-\pi\alpha_{\mathrm{lwe}}^2})$. When $\chi = D_{\sigma,q}$, using Taylor expansion, we obtain $R_{q,\sigma,\chi} - e^{-\pi\alpha_{\mathrm{lwe}}^2} = 1 - \pi\alpha_{\mathrm{lwe}}^2 - e^{-\pi\alpha_{\mathrm{lwe}}^2} = -\frac{\alpha_{\mathrm{lwe}}^4}{2} + O(\alpha_{\mathrm{lwe}}^6)$, thus we obtain $R_{q,\sigma,\chi} = e^{-\pi\alpha_{\mathrm{lwe}}^2} + O(\alpha_{\mathrm{lwe}}^4)$. □

We can now derive the relation between the parameters of LWE and LWR.

Corollary 13. *The time complexity of BKW to solve LWE over $\mathbb{Z}_q^n$ with Gaussian parameter σ and that to solve LWR over $\mathbb{Z}_q^n$ with rounding modulus p are asymptotically the same, when q, p and σ satisfy*

$$\sigma = \frac{q}{2\sqrt{3}p}. \tag{11}$$

Proof. The time complexity of BKW to solve LWE and LWR are given in Theorem 8 and Lemma 12, respectively. Solving the equation $\pi\alpha_{\mathrm{lwe}} = \pi\alpha_{\mathrm{lwr}}$ for σ, we obtain (11). □

3.5 Application to Variants of LWR

Most of LWE-based [3], [5] or LWR-based [10], [12] schemes are based on the ring variants of LWE or LWR, which are Ring-LWE (RLWE) [33], Module-LWE (MLWE) [34], Ring-LWR (RLWR) [23] and Module-LWR (MLWR) [10], [12]. In RLWE, polynomials s, a_i, and e_i are sampled from a ring $\mathcal{R}_q := \mathbb{Z}_q/\phi$ for some polynomial ϕ of degree n, e.g. $\phi = X^n + 1$. Given a list of RLWE samples $(a_i, a_i \cdot s + e_i)_{i=1}^m$, Search-RLWE is to recover s and Decision-RLWE is to distinguish the list of samples from a list uniformly sampled from $\mathcal{R}_q \times \mathcal{R}_q$. MLWE is a problem which generalizes RLWE. In MLWE, polynomial vectors $\boldsymbol{a}_i$, $\boldsymbol{s}$, and polynomials e_i are drawn from $\mathcal{R}_q^k$ and $\mathcal{R}_q$ respectively. Search-MLWE is to recover $\boldsymbol{s}$ from a list of MLWE samples $(\boldsymbol{a}_i, <\langle \boldsymbol{a}_i, \boldsymbol{s}\rangle + e_i)_{i=1}^m$. Decision-MLWE is to distinguish the list of samples from a list uniformly sampled from $\mathcal{R}_q^k \times \mathcal{R}_q$. In Search-RLWR and Decision-RLWR, a list of RLWR samples $(a_i, \lceil \frac{p}{q} a_i \cdot s \rfloor + e_i)_{i=1}^m \in \mathcal{R}_q \times \mathcal{R}_p$ is given, where $\lceil \cdot \rfloor$ is the function that rounds the coefficients of an input polynomial to the nearest integer. In Search-MLWR and Decision-MLWR, a list of MLWR samples $(\boldsymbol{a}_i, \lceil \frac{p}{q}\langle \boldsymbol{a}_i \cdot \boldsymbol{s}\rangle \rfloor + e_i)_{i=1}^m \in \mathcal{R}_q^k \times \mathcal{R}_p$,

The complexity of RLWE, MLWE, RLWR and MLWR

are evaluated by interpreting those ring elements as integer vectors, in [17]: They convert those variants to LWE or LWR. Specifically, let us consider the case when we are given RLWE sample $(a, b = a \cdot s + e) \in \mathcal{R}_q \times \mathcal{R}_q$ with $\phi = X^n + 1$, as an example. Let us denote $a := \sum_{i=0}^{n-1} \overline{a}_i X^i$, $b := \sum_{i=0}^{n-1} \overline{b}_i X^i$, $s := \sum_{i=0}^{n-1} \overline{s}_i X^{-i}$, $e := \sum_{i=0}^{n-1} \overline{e}_i X^i$, $\overline{\boldsymbol{a}} = (\overline{a}_0, \ldots, \overline{a}_{n-1})$, and $\overline{\boldsymbol{s}} = (\overline{s}_0, \ldots, \overline{s}_{n-1})$. Then, we notice that $\overline{b}_0 = \langle \overline{\boldsymbol{a}}, \overline{\boldsymbol{s}} \rangle + e_0$, and $(\overline{\boldsymbol{a}}, \overline{b}_0) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ is an LWE sample. Using this simple conversion, the bit security of all the LWE, LWR and NTRU based schemes is estimated. In the same way as this, using the conversion, the BKW algorithm is also simply applicable to the ring variants. Thus, our analysis of the BKW algorithm can also be applied to RLWR and MLWR if we can obtain sufficiently many samples.

4. Using Fewer Samples

We apply the *sample amplification* idea introduced by Lyubashevsky [28] to the LWR-solving BKW, and we show that the required number of samples of BKW can be decreased to polynomial size, increasing the size of the rounding error in LWR samples,

4.1 Sample Amplification Technique

We show how to apply the sample amplification idea to LWR-solving BKW. We define a variant LWR oracle $\mathsf{LWR}'_{\boldsymbol{s},p,\chi}$, which regards the rounding error as a stochastic variable. And then, we obtain Corollary 15.

Definition 14. *Let n, q be natural numbers. LWR oracle $\mathsf{LWR}'_{\boldsymbol{s},p,\chi}$ for a fixed vector $\boldsymbol{s} \in \mathbb{Z}_q^n$ is an oracle returning $\left\{(\boldsymbol{a}, c) = \left(\boldsymbol{a}, \frac{p}{q}\langle \boldsymbol{a}_j, \boldsymbol{s}\rangle_q + \xi\right) \middle| \boldsymbol{a} \xleftarrow{U} \mathbb{Z}_q^n,\ \xi \leftarrow \chi\right\}$, where χ is defined by its characteristic function*

$$\phi_\chi(t) = \mathbb{E}\left[e^{it\xi}\right] = \frac{\sin\left(\frac{t}{2}\right)}{q \sin\left(\frac{t}{2q}\right)}. \tag{12}$$

Corollary 15. *An algorithm that can solve LWR with the oracle $\mathsf{LWR}'_{\boldsymbol{s},p,\chi}$, can also solve LWR with the oracle $\mathsf{LWR}_{\boldsymbol{s},p}$.*

Proof. Suppose we received samples $(\boldsymbol{a}, c) = \left(\boldsymbol{a}, \left\lceil \frac{p}{q}\langle \boldsymbol{a}_j, \boldsymbol{s}\rangle_q \right\rfloor\right)$ from $\mathsf{LWR}_{\boldsymbol{s},p}$. Let us define $\overline{\xi} = \left\lceil \frac{p}{q}\langle \boldsymbol{a}, \boldsymbol{s}\rangle_q \right\rfloor - \frac{p}{q}\langle \boldsymbol{a}, \boldsymbol{s}\rangle_q$, and denote the distribution of $\overline{\xi}$ by $\overline{\chi}$. From Lemma 19 in [27], we can show that the characteristic function of $\overline{\chi}$ is the same as (12). □

In the rest of this section, we consider the algorithm for solving a variant of LWR with $\mathsf{LWR}'_{\boldsymbol{s},p,\chi}$.

Theorem 16 (Sample amplification)**.** *Let $w \in \mathbb{N}$, and $\beta \in \mathbb{R}$ ($\beta > 1$). When we obtain $m = wq^{\beta n/w}$ samples from $\mathsf{LWR}'_{\boldsymbol{s},p,\chi}$, we can generate an arbitrary number of samples of $\mathsf{LWR}'_{\boldsymbol{s},p,\chi_w}$, where χ_w is the distribution whose characteristic function is $\phi_{\chi_w}(t) = \mathbb{E}\left[e^{it\xi}\right] = \left(\frac{\sin\left(\frac{t}{2}\right)}{q \sin\left(\frac{t}{2q}\right)}\right)^w$.*

Proof. We show that the *amplified* samples obtained with sample amplification and the original samples are statistically indistinguishable, in a way similar to Lemma 17 in [32]. For m samples $(\boldsymbol{a}_j, c_j)$ obtained from $\mathsf{LWR}_{\boldsymbol{s},p}$, we define

$$\begin{cases} h_A(\boldsymbol{x}) = & \sum_{j\in\{j|x_j=1\}} \boldsymbol{a}_j \pmod q \\ h_c(\boldsymbol{x}) = & \sum_{j\in\{j|x_j=1\}} c_j \pmod p. \end{cases} \tag{13}$$

For $j = 1, \ldots, M$, we sample $x_j \xleftarrow{U} \{x \in \{0,1\}^m \mid \mathrm{Hw}(x) = w\}$, and generate an *amplified* sample $(\hat{\boldsymbol{a}}_j, \hat{c}_j) = (h_A(\boldsymbol{x}_j), h_c(\boldsymbol{x}_j))$. We define the set of m original samples as $\mathcal{S} := \{(\boldsymbol{a}_j, c_j)\}_{j=1}^m$, and the set of M *amplified* samples as $\hat{\mathcal{S}} := \{(\hat{\boldsymbol{a}}_j, \hat{c}_j)\}_{j=1}^M$. Let us define predicate g, which outputs 1 when BKW solves LWR correctly with a given set of samples and outputs 0 otherwise. Then, in a way similar to Lemma 17 in [32], we obtain $\left|\Pr[g(\hat{\mathcal{S}}) = 1] - \Pr[g(\mathcal{S}) = 1]\right| \le Mq^{-\frac{(\beta-1)n}{2}}$. Thus, when we define the value of β such that $\lim_{n\to\infty} Mq^{-\frac{(\beta-1)n}{2}} = 0$ (at least $\beta > 1$), we obtain $\lim_{n\to\infty} \left|\Pr[g(\hat{\mathcal{S}}) = 1] - \Pr[g(\mathcal{S}) = 1]\right| = 0$.

Next, we derive the characteristic function of χ_w. From (13), we obtain $\hat{c}_j = \sum_{j\in\{j|x_j=1\}} \left(\frac{p}{q}\langle \boldsymbol{a}_j, \boldsymbol{s}\rangle_q + \xi_j\right) = \frac{p}{q}\langle \hat{\boldsymbol{a}}_j, \boldsymbol{s}\rangle_q + \sum_{j\in\{j|x_j=1\}} \xi_j \pmod p$. We define $\hat{\xi}_j := \sum_{j\in\{j|x_j=1\}} \xi_j$. Because ξ_j and $\xi_{j'}$ ($j \neq j'$) are i.i.d, from (12), we obtain $\phi_{\chi_w}(t) := \mathbb{E}\left[e^{it\hat{\xi}}\right] = \prod_{j\in\{j|x_j=1\}} \mathbb{E}\left[e^{it\xi_j}\right] = \left(\frac{\sin\left(\frac{t}{2}\right)}{q \sin\left(\frac{t}{2q}\right)}\right)^w$. □

Independence Heuristic. In order to use the *amplified samples* as input of LWR-solving BKW, we assume a heuristic, which is often used in the analysis of BKW-type algorithms for solving LPN [35]–[37]. While BKW needs original samples to be statistically independent of each other, sums of samples (e.g. *amplified* samples) are obviously stochastically dependent of each other. However, in [38], it has been shown that the dependence between sums of 2 LPN samples, which are the counterpart of simplified samples with $w = 2$, merely affect the asymptotic time complexity of the LPN solving algorithm. Moreover, the authors of [39] proposed a variant of LPN-solving BKW with improved memory complexity under the heuristic that sums of $w(> 2)$ LPN samples also merely affects the asymptotic time complexity of the LPN-solving BKW algorithm. They has also presented precise experimental results that verify the heuristic in the paper. Similar to their heuristic, we assume that the dependency of the amplified LWR samples for $w \ge 2$ merely affects the asymptotic time complexity of the LWR-solving BKW.

4.2 Complexity

We analyze the time complexity and the required number of *original* samples for solving LWR with the sample amplification, in a way similar to Theorem 8.

Theorem 17. *Let a and b be natural numbers such that*

Table 2 Time and sample complexity for the LWR-solving BKW with sample amplification.

			without sample amplification (from Table 1)			*with* sample amplification		
n	q	p	a	$\log(C^{\mathsf{LWR}})$	$\log(m^{\mathsf{LWR}})$	a	$\log(C^{\mathsf{LWR-amp}})$	$\log(m^{\mathsf{LWR-amp}})$
32	6318667	191	19*	51.00	42.70	10*	83.60	7.91
40	23166277	293	20*	60.66	52.18	11*	99.51	8.21
64	383056211	733	24† (23)	92.70† (92.10)	83.08† (82.80)	13*	151.94	8.84
80	1492443083	1151	25*	110.82	101.11	14*	186.20	9.13
96	4587061889	1663	26*	132.17	122.15	15*	217.88	9.36
112	11942217841	2287	28*	148.00	137.68	16*	247.16	9.56
128	27498355153	3023	29*	167.44	156.88	17*	274.27	9.72

* : optimal value. † : not optimal value. The optimal values are shown in parentheses.

ab $= n$. *Let* $w \in \mathbb{N}$, *and* $\beta(>1) \in \mathbb{R}$. *Fix* $\epsilon \in (0,1)$. *Then, under the Independence Heuristic, when at least* $m = wq^{\beta n/w}$ *samples are given by* LWR *oracle* $\mathsf{LWR}_{s,p}$, *the time complexity of BKW with sample amplification to recover secret* $\mathbf{s}$ *with a probability of at least* $1-\epsilon$ *is* $t = \mathrm{poly}(q^{\frac{n}{a}}, \exp(\alpha_{\mathrm{lwr}}^2 w 2^a))$ *where* $\alpha_{\mathrm{lwr}} = \frac{1}{p}\sqrt{\frac{\pi}{6}}$.

Proof. We derive the required number of *amplified* samples which we denote by $\hat{M}$ for solving LWR with sample amplification, under the Independence Heuristic. This can be derived by replacing $R_{q,p}$ in (5) with $R_{q,p,w} := \phi_{\chi_w}\left(\frac{2\pi}{p}\right)$. Thus, we obtain $\hat{M} = \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left((R_{q,p,w})^{2^{a-1}} - (3/p)^{2^{a-1}}\right)^{-2} + (a-1)^{\frac{q^{\frac{n}{a}}-1}{2}}$, Similarly to Lemma 7, we can show that $\hat{M} = \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left(e^{\pi w\alpha_{\mathrm{lwr}}^2 2^a} + O\left(\frac{1}{p^2q^2}\right)\right) + (a-1)\frac{q^{\frac{n}{a}}-1}{2}$. The rest of the proof follows that of Theorem 8, by replacing m^{LWR} in (7) with this $\hat{M}$, and we can show that the time complexity of BKW with sample amplification is $t = O(e^{\pi w\alpha_{\mathrm{lwr}}^2 2^a}(\frac{n}{a})\ln q) + O(q^{\frac{n}{a}}(\frac{n}{a})\ln q) = \mathrm{poly}(e^{\pi w\alpha_{\mathrm{lwr}}^2 2^a}, q^{\frac{n}{a}})$. □

4.3 Optimization

As in Sect. 3.2, we derive the optimal value of the parameter a that minimizes the asymptotic time complexity of the BKW algorithm with sample amplification. In a similar way to derive (8), we can show that the optimal value of a to minimize the time complexity of BKW with *sample amplification* is

$$a = \left\lfloor \frac{1}{\ln 2} W\left(\frac{n\ln q \ln 2}{\pi w \alpha_{\mathrm{lwr}}^2}\right)\right\rfloor. \tag{14}$$

Next, we minimize the required number of samples, regarding w as a parameter. Since $m = wq^{\beta n/w}$, and $\frac{\partial m}{\partial w} = \frac{q^{\beta n/w}(w-\beta n\log q)}{w}$, when choose $w = \tilde{w} := \beta n \ln q$, we obtain $m = \tilde{m} := e\beta n \ln q$, which is the minimum. Inserting $w = \tilde{w}$ into (14), we obtain $\tilde{a} = \left\lfloor \frac{1}{\ln 2} W\left(\frac{\ln 2}{\pi\beta\alpha_{\mathrm{lwr}}^2}\right)\right\rfloor$. When α_{lwr}^2 is small enough, we can evaluate

$$\tilde{a}' \simeq \left\lfloor \frac{1}{\ln 2}\left(\ln\left(\frac{\ln 2}{\beta\alpha_{\mathrm{lwr}}^2}\right) - \ln\ln\left(\frac{\ln 2}{\beta\alpha_{\mathrm{lwr}}^2}\right)\right)\right\rfloor. \tag{15}$$

To summarize, we obtain the following corollary:

Corollary 18. *Let* a *and* b *be natural numbers such that* $ab = n$. *Fix* $\epsilon \in (0,1)$, *and* $\beta \geq 2$. *Then, under the Independence Heuristic, when at least* $m = \tilde{m} = e\beta n \ln q$ *samples are given by* LWR *oracle* $\mathsf{LWR}_{s,p}$, *the time complexity of BKW with sample amplification to recover secret* $\mathbf{s}$ *with a probability of at least* $1-\epsilon$ *is* $t = q^{O(n/\tilde{a})}$, *where* $\alpha_{\mathrm{lwr}} = \frac{1}{p}\sqrt{\frac{\pi}{6}}$, *and* $\tilde{a}'$ *is defined as in* (15).

4.4 Concrete Analysis

Table 2 shows the concrete time complexity of the LWR-solving BKW algorithm with our sample amplification technique, in the case where we use a minimum number $\tilde{m} = e\beta n \ln q$ of the LWR samples. We set $\beta = 2$ for this table. We denote the time and the sample complexity of the LWR-solving BKW by $C^{\mathsf{LWR-amp}}$ and $m^{\mathsf{LWR-amp}}$, respectively. Similar to Sect. 3.3, we can obtain

$$\begin{aligned} C^{\mathsf{LWR-amp}} &= \frac{1}{4}(a-2)(a-1)\left(\frac{2n}{a}+1\right)(q^{\frac{n}{a}}-1) \\ &\quad + nq^{\frac{n}{a}}\log(q) \\ &\quad + \sum_{j=0}^{a-1} m'^{\mathsf{LWR-amp}}_{j,\epsilon}\left(\frac{a-1-j}{2}(n+2)+2\right), \end{aligned} \tag{16}$$

where $m'^{\mathsf{LWR-amp}}_{j,\epsilon} := \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left(R_{q,p,w}^{2^{a-1-j}} - (3/p)^{2^{a-1-j}}\right)^{-2}$. This can be derived by replacing the $R_{q,p}$ in $m'^{\mathsf{LWR}}_{j,\epsilon} = \frac{8n}{a}\ln\left(\frac{q}{\epsilon}\right)\left(R_{q,p}^{2^{a-1-j}} - (3/p)^{2^{a-1-j}}\right)^{-2}$ with $R_{q,p,w}$. We use the type (a) parameters which are also used in Table 1. We also set $\epsilon = 0.01$, in accordance with the setting given in the table. In Table 2 we reproduce the optimal parameter a, the time and sample complexity of the LWR solving BKW *without* sample amplification from Table 1, for readability purposes. From Table 2 we can observe that our choice of the number of blocks a for BKW with sample amplification, which is derived in (14), minimizes the time complexity of the algorithm. We can observe that, at the expense of increasing the time complexity, the sample amplification technique significantly reduces sample complexity to polynomial size ($\tilde{m} = 2en\ln q$).

5. Conclusion

We analyzed the time complexity of BKW for LWR

and theoretically derived the optimal number of blocks a that asymptotically (but almost completely) minimizes the time complexity of the algorithm, while Duc et al. [27] numerically searched for the optimal value of a. We derived the relation between the parameters of LWE and LWR with the same time complexity of BKW, which is $\sigma = \frac{q}{2\sqrt{3}p}$. This equation coincides with the equation derived by the complexity analysis of the lattice attacks: We showed that the conversion equation also holds on the complexity analysis of BKW. We also showed that the sample amplification method is applicable to LWR-solving BKW under the *Independence Heuristic*, and analyzed that the minimum required number of samples for LWR-solving BKW with sample amplification is $O(n \log q)$.

References

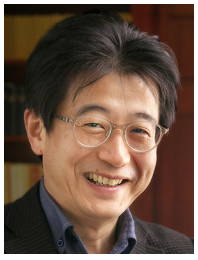
[1] H. Okada, A. Takayasu, K. Fukushima, S. Kiyomoto, and T. Takagi, "On the complexity of the LWR-solving BKW algorithm," ICISC 2018, pp.196–214, 2019.
[2] National Institute of Standards and Technology, "Post-quantum cryptography," https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. Accessed: Feb. 27, 2019.
[3] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS — Kyber: A CCA-secure module-lattice-based KEM," EuroS&P 2018, pp.353–367, 2018.
[4] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo: Take off the ring! practical, quantum-secure key exchange from LWE," CCS 2016, pp.1006–1018, 2016.
[5] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange — A new hope," USENIX Security Symposium, pp.327–343, 2016.
[6] R.E. Bansarkhani, "LARA — A design concept for lattice-based encryption," Cryptology ePrint Archive, Report 2017/049, 2017.
[7] M.R. Albrecht, E. Orsini, K.G. Paterson, G. Peer, and N.P. Smart, "Tightly secure Ring-LWE based key encapsulation with short ciphertexts," ESORICS 2017, pp.29–46, 2017.
[8] J.H. Cheon, D. Kim, J. Lee, and Y. Song, "Lizard: Cut off the tail! a practical post-quantum public-key encryption from LWE and LWR," SCN 2018, pp.160–177, 2018.
[9] Z. Jin and Y. Zhao, "Optimal key consensus in presence of noise," CoRR, vol.abs/1611.06150, 2016.
[10] J.P. D'Anvers, A. Karmakar, S.S. Roy, and F. Vercauteren, "Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM," AFRICACRYPT 2018, pp.282–305, 2018.
[11] H. Baan, S. Bhattacharya, O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, and Z. Zhang, "Round2: KEM and PKE based on GLWR," Cryptology ePrint Archive, Report 2017/1183, 2017.
[12] H. Baan, S. Bhattacharya, S. Fluhrer, O. Garcia-Morchon, T. Laarhoven, R. Rietman, M.J.O. Saarinen, L. Tolhuizen, and Z. Zhang, "Round5: Compact and fast post-quantum public-key encryption," Cryptology ePrint Archive, Report 2019/090, 2019.
[13] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, vol.56, no.6, pp.34:1–34:40, 2009.
[14] A. Becker, N. Gama, and A. Joux, "A sieve algorithm based on overlattices," LMS J. Comput. Math., vol.17, no.A, pp.49–70, 2014.
[15] Y. Chen and P.Q. Nguyen, "BKZ 2.0: Better lattice security estimates," ASIACRYPT 2011, pp.1–20, 2011.
[16] N. Gama, P.Q. Nguyen, and O. Regev, "Lattice enumeration using extreme pruning," EUROCRYPT 2010, pp.257–278, 2010.
[17] M.R. Albrecht, B.R. Curtis, A. Deo, A. Davidson, R. Player, E.W. Postlethwaite, F. Virdia, and T. Wunderer, "Estimate all the {LWE, NTRU} schemes!," SCN 2018, pp.351–367, 2018.
[18] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," J. ACM, vol.50, no.4, pp.506–519, 2003.
[19] G. Herold, E. Kirshanova, and A. May, "On the asymptotic complexity of solving LWE," Des. Codes Cryptogr., vol.86, no.1, pp.55–83, 2018.
[20] Q. Guo, T. Johansson, and P. Stankovski, "Coded-BKW: Solving LWE using lattice codes," CRYPTO 2015, pp.23–42, 2015.
[21] P. Kirchner and P.A. Fouque, "An improved BKW algorithm for LWE with applications to cryptography and lattices," CRYPTO 2015, pp.43–62, 2015.
[22] T. Laarhoven, "Sieving for shortest vectors in lattices using angular locality-sensitive hashing," CRYPTO 2015, pp.3–22, 2015.
[23] A. Banerjee, C. Peikert, and A. Rosen, "Pseudorandom functions and lattices," EUROCRYPT 2012, pp.719–737, 2012.
[24] D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan, "Key homomorphic PRFs and their applications," CRYPTO 2013, pp.410–428, 2013.
[25] J. Alwen, S. Krenn, K. Pietrzak, and D. Wichs, "Learning with rounding, revisited," CRYPTO 2013, pp.57–74, 2013.
[26] M.R. Albrecht, C. Cid, J.C. Faugère, R. Fitzpatrick, and L. Perret, "On the complexity of the BKW algorithm on LWE," Des. Codes Cryptogr., vol.74, no.2, pp.325–354, 2015.
[27] A. Duc, F. Tramèr, and S. Vaudenay, "Better algorithms for LWE and LWR," EUROCRYPT 2015, pp.173–202, 2015.
[28] V. Lyubashevsky, "The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem," Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques, pp.378–389, 2005.
[29] Q. Guo, T. Johansson, E. Mårtensson, and P. Stankovski, "Coded-BKW with sieving," ASIACRYPT 2017, pp.323–346, 2017.
[30] M.R. Albrecht, J.C. Faugère, R. Fitzpatrick, and L. Perret, "Lazy modulus switching for the BKW algorithm on LWE," PKC 2014, pp.429–445, 2014.
[31] R.M. Corless, G.H. Gonnet, D.E. Hare, D.J. Jeffrey, and D.E. Knuth, "On the Lambert W function," Adv. Comput. Math., vol.5, no.1, pp.329–359, 1996.
[32] K. Kaminakaya, N. Kunihiro, and A. Takayasu, "BKW algorithm for solving LWE problem," Symposium on Cryptography and Information Security, SCIS 2016, IEICE, 2016 (in Japanese).
[33] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," EUROCRYPT 2010, pp.1–23, 2010.
[34] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," Des. Codes Cryptogr., vol.75, no.3, pp.565–599, June 2015.
[35] S. Bogos, F. Tramér, and S. Vaudenay, "On solving LPN using BKW and variants," Cryptogr. Commun., vol.8, no.3, pp.331–369, 2016.
[36] S. Bogos and S. Vaudenay, "Optimization of LPN solving algorithms," ASIACRYPT 2016, pp.703–728, 2016.
[37] B. Zhang, L. Jiao, and M. Wang, "Faster algorithms for solving LPN," EUROCRYPT 2016, pp.168–195, 2016.
[38] S. Devadas, L. Ren, and H. Xiao, "On iterative collision search for LPN and subset sum," Theory of Cryptography, pp.729–746, 2017.
[39] A. Esser, F. Heuer, R. Kübler, A. May, and C. Sohler, "Dissection-BKW," CRYPTO 2018, pp.638–666, 2018.

Hiroki Okada received his B.E. and M.E. in applied mathematics and physics from Kyoto University, Japan, in 2014 and 2016, respectively. He joined KDDI in 2016 and has been engaged in research on lattice-based cryptography and homomorphic encryption. He is currently an associate research engineer at the Information Security Laboratory of KDDI Research, Inc.

Atsushi Takayasu received his B.E. in mathematical engineering and information physics from the University of Tokyo in 2012, M.S. and Ph.D. in complexity science and engineering from the University of Tokyo in 2014 and 2017. He was a JSPS Research Fellow (DC1) during his Ph.D. course. He is currently an assistant professor in the Graduate School of Information Science and Technology at the University of Tokyo, a Collaborative Researcher in National Institute of Advanced Industrial Science and Technology. He received Best Student Paper Award in ACISP 2016. His research interest includes cryptography and information security.

Kazuhide Fukushima received his M.E. in Information Engineering from Kyushu University, Japan, in 2004. He joined KDDI and has been engaged in the research on post-quantum cryptography, cryptographic protocols, and identification technologies. He is currently a research manager at the Information Security Laboratory of KDDI Research, Inc. He received his Doctorate in Engineering from Kyushu University in 2009. He received the IEICE Young Engineer Award in 2012. He is a member of the Information Processing Society of Japan.

Shinsaku Kiyomoto received his B.E. in engineering sciences and his M.E. in Material Science from Tsukuba University, Japan, in 1998 and 2000, respectively. He joined KDD (now KDDI) and has been engaged in research on stream ciphers, cryptographic protocols, and mobile security. He is currently a senior researcher at the Information Security Laboratory of KDDI Research, Inc. He was a visiting researcher of the Information Security Group, Royal Holloway University of London from 2008 to 2009. He received his doctorate in engineering from Kyushu University in 2006. He received the IEICE Young Engineer Award in 2004 and Distinguished Contributions Awards in 2011. He is a member of IEICE and JPS.



Tsuyoshi Takagi received the B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively. He was engaged in research on network security at NTT Laboratories from 1995 to 2001. He received the PhD from the Technical University of Darmstadt in 2001. He was an Assistant Professor in the Department of Science at Technical University of Darmstadt until 2005. He is currently a Professor in the Graduate School of Information Science and Technology at University of Tokyo and in the Institute of Mathematics for Industry at Kyushu University. His current research interests are information security and cryptography. He received DOCOMO Mobile Science Award in 2013, IEICE Achievement Award in 2013, and JSPS Prize in 2014. Dr. Takagi was a Program Chair of the 7th International Conference on Post-Quantum Cryptography, PQCrypto 2016.