数理解析研究所講究録
1489巻 2006年 43-49

Multi-Bit Cryptosystems based on Lattice Problems (Extended Abstract)

草川 恵太* Keita Xagawa
河内 亮周* Akinori Kawachi
田中 圭介* Keisuke Tanaka

Abstract— We propose multi-bit versions of several single-bit cryptosystems based on lattice problems, the error-free version of the Ajtai-Dwork cryptosystem by Goldreich, Goldwasser, and Halevi [CRYPTO '97], the Regev cryptosystems [STOC 2003 and STOC 2005], and the Ajtai cryptosystem [STOC 2005]. Based on a common structure amongst them, we develop a generic technique for constructing their multi-bit versions without increase in the size of ciphertexts. By analyzing the trade-off between the decryption error and the hardness of underlying lattice problems, it is shown that our multi-bit versions encrypt $O(\log n)$-bit plaintexts into ciphertexts of the same length as the original ones with the reasonable sacrifices of the hardness of the underlying lattice problems. Our technique also provides a new algebraic property *pseudo-homomorphism* of the lattice-based cryptosystems.

Keywords: Multi-bit public-key cryptosystems, Lattice problems, Pseudo-homomorphism.

1 Introduction

Background. The lattice-based cryptosystems have been well-studied since Ajtai's seminal result [1] on a connection between the worst-case and the average-case hardness of a certain class of lattice problems. Ajtai and Dwork constructed lattice-based public-key cryptosystems using this connection [3]. Following their results, a number of lattice-based cryptosystems have been proposed in the last decade [6, 5, 16, 2, 17].

We can roughly classify the lattice-based cryptosystems into two classes by whether they have the security proofs based on hard lattice problems or not. The cryptosystems in the first class do not have security proofs to hard lattice problems, but have efficiency on the size of keys and of ciphertexts and the speed of encryption and decryption procedures. For example, the GGH cryptosystem [7] and NTRU [9] are efficient multi-bit cryptosystems using lattice-related problems. However, it is unknown whether their security is guaranteed by well-known hard lattice problems such as uSVP, SVP and SIVP. Actually, several cryptanalysis were reported for cryptosystems in this class [13].

On the other hand, the cryptosystems in the second class have security proofs based on well-known hard lattice problems [3, 16, 17]. The security of these cryptosystems can be guaranteed by the worst-case complexity of certain lattice problems, that is, if it is hard to solve the lattice problems in the worst case, then the adversaries cannot efficiently distinguish between ciphertexts even on average. This attractive property is also studied from a theoretical point of view [1, 12]. However, they generally have longer keys and ciphertexts than the cryptosystems in the first class. The Ajtai-Dwork cryptosystem is already analyzed with practical security parameters in [14] due to the large size of the public key.

Several researchers recently have considered efficient lattice-based cryptosystems with the connections between their security and computationally hard problems.

For example, Regev constructed an efficient lattice-based cryptosystem with short keys [17]. The security is based on the worst-case hardness of certain approximation problems of SVP and SIVP for quantum polynomial-time algorithms, that is, the security is based on the assumption that any quantum polynomial-time algorithm cannot solve certain lattice problems. Ajtai also constructed an efficient lattice-based cryptosystem with short keys by using a compact representation for a special case of uSVP [2]. The security is based on the average-case hardness of a certain Diophantine approximation problem. It is unknown whether the security can be reduced its worst-case hardness or not.

Our Contribution. We continue to study efficient lattice-based cryptosystems with security proofs based on well-known hard lattice problems or other secure cryptosystems. In particular, we focus on the size of plaintexts encrypted by the cryptosystems in the second class. To the best of the authors' knowledge, all those in the second class are single-bit cryptosystems. We therefore obtain more efficient lattice-based cryptosystems with security proofs if we succeed to con-

* Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan. {xagawa5, kawachi, keisuke}@is.titech.ac.jp. Supported in part by NTT Information Sharing Platform Laboratories and Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 16092206.

struct their multi-bit versions without increase in the size of ciphertexts.

In this paper, we consider multi-bit versions of the improved Ajtai-Dwork cryptosystem proposed by Goldreich, Goldwasser, and Halevi [6], the Regev cryptosystems proposed in 2003 [16] and in 2005 [17], and the Ajtai cryptosystem [2]. Based on a common structure amongst them, we develop a generic technique for constructing their multi-bit versions without increase in the size of ciphertexts.

To apply our technique to constructions of the multi-bit versions, we need to consider trade-offs between decryption errors and hardness of underlying lattice problems. By analyzing the trade-offs for each of the cryptosystems in detail, it is shown that our multi-bit versions encrypt $O(\log n)$-bit plaintexts into ciphertexts of the same length as the original ones with reasonable sacrifices of the hardness of the underlying lattice problems.

The ciphertexts of our multi-bit version are distributed in the same ciphertext space, theoretically represented with real numbers, as the original cryptosystem. To represent the real numbers in their ciphertexts, we have to round their fractional parts with certain precision. The size of ciphertexts then increases if we process the numbers with high precision. We stress that our technique does not need higher precision than the original cryptosystems, i.e., we take the same precision in our multi-bit versions as that of the original ones.

See Table 1 for the cryptosystems studied in this paper. We call the cryptosystems proposed in [6, 16, 17, 2] $\mathrm{AD}_{\mathrm{GGH}}$, R03, R05, and A05, respectively. We also call the corresponding multi-bit versions $\mathrm{mAD}_{\mathrm{GGH}}$, mR03, mR05, and mA05.

Our generic technique also provides a new algebraic property *pseudo-homomorphism* such that the sum of ciphertexts of two plaintexts x_1 and x_2 is equal to a variant of a ciphertext of $x_1 + x_2$ that can be decrypted by the private key of the multi-bit version. We present the pseudo-homomorphic property of $\mathrm{mAD}_{\mathrm{GGH}}$, mR03, mR05, and (a slightly modified version of) mA05.

We surely obtain a multi-bit cryptosystem simply by concatenating the ciphertexts of a single-bit cryptosystem if we concede the increase in the size of ciphertexts. However, this simple modification does not provides such an algebraic property. Therefore, we can claim that our technique contributes the new algebraic property of the lattice-based cryptosystems.

Many number-theoretic and algebraic cryptosystems are known to have a homomorphic property of cryptosystems, which is useful for cryptographic applications such as voting protocol. On the contrary, as far as we know, there are no other (e.g., combinatorial) cryptosystems with such an algebraic property except for our new cryptosystems so far.

Main Idea for Multi-Bit Constructions and Their Security. We can actually find the following common structure amongst the single-bit cryptosystems $\mathrm{AD}_{\mathrm{GGH}}$, R03, R05, and A05: Their ciphertexts of 0 are basically distributed according to a periodic Gaussian distribution and those of 1 are also distributed according to another periodic Gaussian distribution whose peaks are shifted to the middle of the period. We thus embed two periodic Gaussian distributions into the ciphertext space such that their peaks appear alternatively and regularly.

Our technique is based on a generalization of this structure. More precisely, we regularly embed *multiple* periodic Gaussian distributions into the ciphertext space rather than only two ones. Embedding p periodic Gaussian distributions as shown in this figure, the ciphertexts for a plaintext $i \in \{0, \ldots, p-1\}$ are distributed according the i-th periodic Gaussian distribution. This cyclic structure enables us not only to improve the efficiency of the cryptosystems but also to guarantee their security.

If we embed too many periodic Gaussian distributions, the decryption errors increase due to overlaps amongst the distributions. We can then decrease the decryption errors by reducing their variance. However, it is known that smaller variance generally provides less security in cryptosystems based on such Gaussian distributions, as commented in [6]. We therefore have to analyze the trade-offs in our multi-bit versions between the decryption errors and their security, which depend on their own structures of the cryptosystems.

Once we analyze their trade-offs, we can apply a common strategy based on the cyclic structure to the security proofs. The security of the original cryptosystems basically depends on the indistinguishability between a certain periodic Gaussian distribution Φ and a uniform distribution U since it is shown in their security proofs that we can construct an efficient algorithm for a certain hard lattice problem by employing an efficient distinguisher between Φ and U. The goal is thus to construct the distinguisher from an adversary against the multi-bit version.

We first assume that there exist two periodic Gaussian distributions Φ_i and Φ_j corresponding to two kinds of ciphertexts in our multi-bit version and an efficient adversary for distinguishing between Φ_i and Φ_j with its public key. By the hybrid argument, the adversary can distinguish either between Φ_i and U or between Φ_j and U. We now suppose that it can distinguish between Φ_i and U. Note that we can slide Φ_i to Φ_0 corresponding to ciphertexts of 0 even if we do not know the private key by the cyclic property of the ciphertexts. Thus, we obtain an efficient distinguisher between Φ_0 and U. Φ_0 is in fact a variance-reduced version of the periodic Gaussian distribution Φ used in

	Ajtai-Dwork		Regev'03	
cryptosystem	AD_{GGH} [6]	mAD_{GGH}	R03 [16]	mR03
security	$O(n^{11})$-uSVP	$O(n^{11+r})$-uSVP	$\tilde{O}(n^{1.5})$-uSVP	$\tilde{O}(n^{1.5+r})$-uSVP
size of public key	$O(n^5 \log n)$	$O(n^5 \log n)$	$O(n^4)$	$O(n^4)$
size of private key	$O(n^2)$	$O(n^2)$	$O(n^2)$	$O(n^2)$
size of plaintext	1	$O(\log n)$	1	$O(\log n)$
size of ciphertext	$O(n^2 \log n)$	$O(n^2 \log n)$	$O(n^2)$	$O(n^2)$
rounding precision	2^{-n}	2^{-n}	2^{-8n^2}	2^{-8n^2}
	Regev'05		Ajtai	
cryptosystem	R05 [17]	mR05	A05 [2]	mA05
security	$SVP_{\tilde{O}(n^{1.5})}$	$SVP_{\tilde{O}(n^{1.5+r})}$	(Special uSVP)	A05
size of public key	$O(n^2 \log^2 n)$	$O(n^2 \log^2 n)$	$O(n^2 \log n)$	$O(n^2 \log n)$
size of private key	$O(n \log n)$	$O(n \log n)$	$O(n \log n)$	$O(n \log n)$
size of plaintext	1	$O(\log n)$	1	$O(\log n)$
size of ciphertext	$O(n \log n)$	$O(n \log n)$	$O(n \log n)$	$O(n \log n)$
rounding precision	2^{-n}	2^{-n}	$1/n$	$1/n$

Table 1: summary. ($r > 0$ is any constant and $\tilde{O}(f(n))$ means $O(f(n)\,\mathrm{poly}(\log n))$.)

the original cryptosystem. We can still reduce the indistinguishability between such a version Φ_0 and U to a lattice problem with a slight loss of its hardness. We can therefore guarantee the security of our multi-bit versions similarly to the original ones.

Pseudo-Homomorphism in Multi-Bit Versions. The regular embedding of the periodic Gaussian distributions also gives our multi-bit cryptosystems the algebraic property *pseudo-homomorphism*. Recall that a Gaussian distribution has the following reproducing property: For two random variables X_1 and X_2 according to $N(m_1, s_1^2)$ and $N(m_2, s_2^2)$, where $N(m, s^2)$ is a Gaussian distribution with mean m and standard deviation s, the distribution of $X_1 + X_2$ is equal to $N(m_1 + m_2, s_1^2 + s_2^2)$. This property implies that the sum of two ciphertexts (i.e., the sum of two periodic Gaussian distributions) becomes a variant of a ciphertext (i.e., a periodic Gaussian distribution with larger variance). This sum can be moreover decrypted into the sum of two plaintexts with the private key of the multi-bit version, and has the indistinguishability based on the security of the multi-bit version.

Definitions. The security parameter n is given by dimension of a lattice in the lattice problems on which security of the cryptosystems are based. Let $\lceil x \rfloor$ be the closest integer to $x \in \mathbb{R}$ (if there are two such integers, we choose the smaller.) and $\mathrm{frc}(x) = |x - \lceil x \rfloor|$ for $x \in \mathbb{R}$, i.e., $\mathrm{frc}(x)$ is the distance from x to the closest integer. We define $x \bmod y$ as $x - \lfloor x/y \rfloor y$ for $x, y \in \mathbb{R}$.

The length of a vector $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$, denoted by $\|\mathbf{x}\|$, is $\sqrt{\sum_{i=1}^n x_i^2}$. The inner product of two vectors $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$ and $\mathbf{y} = (y_1, \ldots, y_n)^T \in \mathbb{R}^n$, denoted by $\langle \mathbf{x}, \mathbf{y} \rangle$, is $\sum_{i=1}^n x_i y_i$.

A function $f(n)$ is called negligible for sufficiently large n if $\lim_{n\to\infty} n^c f(n) = 0$ for any constant $c > 0$. We similarly call $f(n)$ a non-negligible function if there exists a constant $c > 0$ such that $f(n) > n^{-c}$ for sufficiently large n. Also, a probability is called exponentially close to 1 when it is at least $1 - 2^{-\Omega(n)}$. We represent a real number by rounding its fractional part. If the fractional part of $x \in \mathbb{R}$ is represented with m bits, the rounded number $\bar{x}$ has the precision of $1/2^l$, i.e., we have $|x - \bar{x}| \le 1/2^l$.

We say that an algorithm distinguishes between two distributions if the gap between the acceptance probabilities for their samples is non-negligible.

A Gaussian distribution $N(m, s^2)$ with mean m and standard derivation s is a distribution on $\mathbb{R}$ defined by the density function $\nu(l) = \frac{1}{\sqrt{2\pi}s}\exp\left(-\frac{(l-m)^2}{2s^2}\right)$. We actually make use of many variants of the Gaussian distribution. So, we will define such variants when required.

A lattice in $\mathbb{R}^n$ is the set $L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{\sum_{i=1}^n \alpha_i \mathbf{b}_i : \alpha_i \in \mathbb{Z}\right\}$ of all integral combinations of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. The sequence of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called a *basis* of a lattice L. For clarity of notations, we represent a basis by the matrix $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n\times n}$. For any basis $\mathbf{B}$, we define the *fundamental parallelepiped* $\mathcal{P}(\mathbf{B}) = \{\sum_{i=1}^n \alpha_i \mathbf{b}_i : 0 \le \alpha_i < 1\}$. The vector $\mathbf{x} \in \mathbb{R}^n$ reduced modulo the parallelepiped $\mathcal{P}(\mathbf{B})$, denoted by $\mathbf{x} \bmod \mathcal{P}(\mathbf{B})$, is the unique vector $\mathbf{y} \in \mathcal{P}(\mathbf{B})$ such that $\mathbf{y} - \mathbf{x} \in L(\mathbf{B})$.

The dual lattice L^* of a lattice L is the set $L^* = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}$. If L is generated by basis $\mathbf{B}$, then $(\mathbf{B}^T)^{-1}$ is a basis for the dual lattice, where $\mathbf{B}^T$ is the transpose of $\mathbf{B}$. For more details, see the textbook by Goldwasser and Micciancio [11].

Organization. The rest of this paper is organized as follows. We propose our multi-bit versions from Sections 2 to 5. Because of the lack of space, we omit the description of mR05 and mA05. In Section 2 and **??**, we first review intuitions, protocols and performance of the original single-bit cryptosystems. We omit the proofs for their decryption errors, security, pseudo-homomorphisms.

2 A Multi-Bit Version of the Ajtai-Dwork Cryptosystem

In this section, we consider the improved variant given by Goldreich, Goldwasser, and Halevi [6] instead of the original Ajtai-Dwork cryptosystem [3].

The Improved Ajtai-Dwork Cryptosystem. Let $N = n^n = 2^{n \log n}$ and $m = n^3$. We define an n-dimensional hypercube C and an n-dimensional ball B_r as $C = \{\mathbf{x} \in \mathbb{R}^n : 0 \leq x_i < N, i = 1, \ldots, n\}$ and $B_r = \{\mathbf{x} \in \mathbb{R}^n : \|x\| \leq n^{-r}/4\}$ for any constant $r \geq 7$, respectively. For $\mathbf{u} \in \mathbb{R}^n$ and an integer i we define an hyperplane H_i as $H_i = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{u} \rangle = i\}$.

Roughly speaking, the improved Ajtai-Dwork cryptosystem encrypts 0 into a vector close to hidden $(n-1)$-dimensional hyperplanes $H_0, H_1, H_2, \cdots$ for a normal vector $\mathbf{u}$ of H_0 and 1 into their intermediate hyperplanes $H_0 + \mathbf{u}/(2\|\mathbf{u}\|^2), H_1 + \mathbf{u}/(2\|\mathbf{u}\|^2), \cdots$. Then, the private key is the normal vector $\mathbf{u}$. These distributions of ciphertexts can be obtained from its public key, which consists of samples of vectors on the hidden hyperplanes and information i_1 for shifting a vector on the hyperplanes to one on the intermediate ones. If we know the normal vector, we can reduce the n-dimensional space to on the 1-dimensional space along the normal vector. Then, we can easily find whether a ciphertext distributed around the hidden hyperplanes or the intermediate ones.

We now describe the protocol of $\mathrm{AD_{GGH}}$ as follows. Our description slightly generalizes the original one by introducing a parameter r, which control the variance of the distributions of a perturbation since we need to estimate a trade-off between the security and the size of plaintexts in our multi-bit version.

Key Generation: We choose $\mathbf{u}$ uniformly at random from the n-dimensional unit ball. Repeating the following procedure m times, we sample m vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$: (1) We choose $\mathbf{a}_i$ from $\{\mathbf{x} \in C : \langle \mathbf{x}, \mathbf{u} \rangle \in \mathbf{Z}\}$ uniformly at random, (2) choose $\mathbf{b}_1, \ldots, \mathbf{b}_n$ from B_r uniformly at random, (3) and output $\mathbf{v}_i = \mathbf{a}_i + \sum_{j=1}^n \mathbf{b}_j$ as a sample. We then take the minimum index i_0 satisfying that the width of $\mathcal{P}(\mathbf{v}_{i_0+1}, \ldots, \mathbf{v}_{i_0+n})$ is at least $n^{-2}N$, where width of a parallelpiped $\mathcal{P}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is defined as length of an edge of the minimum hypercube contained in $\mathcal{P}(\mathbf{x}_1, \ldots \mathbf{x}_n)$, i.e., $\min_{i=1,\ldots,n} \mathrm{Dist}(\mathbf{x}_1, \mathrm{span}(\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \ldots, \mathbf{x}_n))$ for a distance function $\mathrm{Dist}(\cdot, \cdot)$ between a vector and an $(n-1)$-dimensional hyperplane.

Now let $\mathbf{w}_j = \mathbf{v}_{i_0+j}$ for every $j \in \{1, \ldots, n\}$. Also, let $V = (\mathbf{v}_1, \ldots, \mathbf{v}_m)$ and $W = (\mathbf{w}_1, \ldots, \mathbf{w}_n)$. We also choose an index i_1 uniformly at random from $\{i : \langle \mathbf{a}_i, \mathbf{u} \rangle \text{ is odd}\}$. Note that there are such indices i_0 and i_1 with probability $1 - o(1)$. If they do not exist, we perform this procedure again. Then, the private key is $\mathbf{u}$ and the public key is (V, W, i_1).

Encryption: Let S be a subset of $\{0,1\}^m$ chosen uniformly at random. We encrypt a plaintext $\sigma \in \{0, 1\}$ to $\mathbf{x} = \frac{\sigma}{2}\mathbf{v}_{i_1} + \sum_{i \in S} \mathbf{v}_i \bmod \mathcal{P}(W)$.

Decryption: Let $\mathbf{x} \in \mathcal{P}(W)$ be a received ciphertext. We decrypt $\mathbf{x}$ to 0 if $\mathrm{frc}(\langle \mathbf{x}, \mathbf{u} \rangle) \leq 1/4$ and to 1 otherwise.

Carefully reading the results in [3, 6] and using the results in [4], we obtain the following theorem on the cryptosystem $\mathrm{AD_{GGH}}$.

Theorem 2.1 ([6]). *The cryptosystem* $\mathrm{AD_{GGH}}$ *encrypts a 1-bit plaintext into a $O(n^2 \log n)$-bit ciphertext with no decryption errors. The security of* $\mathrm{AD_{GGH}}$ *is based on the worst case of $O(n^{r+4})$-uSVP for $r \geq 7$. The size of the public key is $O(n^5 \log n)$ and the size of the private key is $O(n^2)$.*

Our Multi-bit Cryptosystem. We now describe the multi-bit version $\mathrm{mAD_{GGH}}$ of $\mathrm{AD_{GGH}}$. Let p be a prime such that $p \leq 2n^{r-7}$. In $\mathrm{mAD_{GGH}}$, we can encrypt a plaintext of $\log p$ bits into a ciphertext of the same size as one of $\mathrm{AD_{GGH}}$. The strategy of our construction basically follows the argument in Section 1.

Key Generation: The key generation procedure is the almost same as $\mathrm{AD_{GGH}}$. We choose an index i_1' uniformly at random from $\{i : x_i \not\equiv 0 \bmod p\}$ instead of i_1 in the original key generation procedure. Note that there is such a k with probability $1 - (1/p)^m = 1 - o(1)$. Then, the private key is $(\mathbf{u}, k)$ and the public key is (V, W, i_1').

Encryption: Let S be a uniformly random subset of $\{0, 1\}^m$. We encrypt $\sigma \in \{0, \ldots, p-1\}$ to $\mathbf{x} = \frac{\sigma}{p}\mathbf{v}_{i_1'} + \sum_{i \in S} \mathbf{v}_i \bmod \mathcal{P}(W)$.

Decryption: We decrypt a received ciphertext $\mathbf{x} \in \mathcal{P}(W)$ to $\lceil p \langle \mathbf{x}, \mathbf{u} \rangle \rfloor k^{-1} \bmod p$, where k^{-1} is the inverse of k in $\mathbf{Z}_p$.

Note that we can correctly decrypt the ciphertexts since the number p of plaintexts is prime.

We obtain the following theorem on the size of plaintexts and the security of our multi-bit version $\mathrm{mAD_{GGH}}$.

Theorem 2.2 (multi-bit version). *Let $r \geq 7$ be a integer and let p be a prime such that $2 \leq p(n) \leq 2n^{r-7}$. The cryptosystem* $\mathrm{mAD_{GGH}}$ *encrypts a $\lfloor \log p(n) + 1 \rfloor$-bit plaintext into an $O(n^2 \log n)$-bit ciphertext without decryption errors. The security of* $\mathrm{mAD_{GGH}}$ *is based on the worst case of $O(n^{r+4})$-uSVP. The size of the public key is the same as the original one. The size of the private key is $O(\log p)$ plus the original one.*

Finally, we present a pseudo-homomorphic property of our cryptosystem $\mathrm{mAD_{GGH}}$. Let E_m be the encryption function of $\mathrm{mAD_{GGH}}$.

Theorem 2.3 (pseudo-homomorphism). *Let $r \geq 7$ be any constant. Also, let p be a prime and let κ be an integer such that $\kappa p \leq n^{r-7}$. For any κ plaintexts $\sigma_1, \ldots, \sigma_\kappa$ $(0 \leq \sigma_i \leq p-1)$, we can decrypt the sum of κ ciphertexts $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i) \bmod \mathcal{P}(W)$ into $\sum_{i=1}^{\kappa} \sigma_i \bmod p$ without decryption error. Moreover, if there exist two sequences of plaintexts $(\sigma_1, \ldots, \sigma_\kappa)$ and $(\sigma'_1, \ldots, \sigma'_\kappa)$, and a polynomial-time algorithm that distinguishes between $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i) \bmod \mathcal{P}(W)$ and $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma'_i) \bmod \mathcal{P}(W)$ with its public key, then there exists a polynomial-time algorithm that solves $O(n^{r+4})$-uSVP in the worst case with non-negligible probability.*

3 A Multi-Bit Version of the Regev'03 Cryptosystem

The Regev'03 Cryptosystem. In this section, we consider the Regev cryptosystem R03 proposed in [16]. Roughly speaking, the ciphertexts of 0 and 1 approximately corresponds to two periodic Gaussian distributions in R03. We now denote the distributions of the ciphertexts of 0 and 1 as Φ_0 and Φ_1, respectively. Note that every peaks in Φ_1 are regularly located in the middle of two peaks in Φ_0. A parameter h is approximately equal to the number of peaks in Φ_0, and a private key d, obtained from h, corresponds to length of the period. A public key is of the form $(a_1, \ldots, a_m, i_0)$, where $a_1, \ldots, a_m$ are samples from Φ_0 to make a ciphertext of 0 by summing up randomly chosen elements from the samples and a certain index $i_0 \in \{1, \ldots, m\}$ is used to shift a ciphertext of 0 to that of 1 by adding $a_{i_0}/2$ to a ciphertext of 0. One can easily see that we can distinguish between Φ_0 and Φ_1 with d. It however seems hard to distinguish them only with polynomially many samples of Φ_0 and i_0. Actually, it is shown in [16] that breaking R03 is at least as hard as the worst case of a certain uSVP.

In what follows, we precisely describe the original R03. We begin with the definition of a folded Gaussian distribution Ψ_α whose density function is $\Psi_\alpha(l) = \sum_{k \in \mathbb{Z}} \frac{1}{\alpha} \exp\left(-\pi \frac{(l-k)^2}{\alpha^2}\right)$. This distribution is obtained by "folding" a Gaussian distribution $N(0, \alpha^2/(2\pi))$ on $\mathbb{R}$ into the interval $[-1/2, 1/2)$. Note that this folded Gaussian distribution is equivalent with the fractional part of $N(0, \alpha^2/(2\pi))$. Based on this distribution, R03 makes use of a periodic distribution $\Phi_{h,\alpha}$ defined by the following density function: $\Phi_{h,\alpha}(l) = \Psi_\alpha(lh \bmod 1)$. We can sample values according to this distribution by using samples from Φ_α, as shown in [16]: (1) We sample $x \in \{0, \ldots, \lceil h \rceil\}$ uniformly at random and then (2) sample y according to Ψ_α. (3) If $0 \leq (x+y)/h < 1$, we then take the value as a sample. Otherwise, we repeat (1) and (2).

Let $N = 2^{8n^2}$, $m = c_0 n^2$ for a sufficiently large constant c_0, and $\gamma(n) = \omega(n\sqrt{\log n})$, specifying the size of the ciphertext space, the size of the public keys, and the variance of the folded Gaussian distribution, respectively. In this section, we require precision of $1/2^{8n^2} = 1/N$ for rounding real numbers.

Key Generataion: Let $H = \{h \in [\sqrt{N}, 2\sqrt{N}) : \mathrm{frc}(h) < 1/(16m)\}$. We choose $h \in H$ uniformly at random and set $d = N/h$. The private key is the number d. Choosing $\alpha \in [2/\gamma(n), (2\sqrt{2})/\gamma(n))$, we sample m values $z_1, \ldots, z_m$ from the distribution $\Phi_{h,\alpha}$, where $z_i = (x_i + y_i)/h$ $(i = 1, \ldots, m)$ according to the above sampling procedure. Let $a_i = \lceil N z_i \rceil$ for every $i \in \{1, \ldots, m\}$. Note that we have an index i_0 such that x_{i_0} is odd with a probability exponentially close to 1. Then, the public key is $(a_1, \ldots, a_m, i_0)$.

Encryption: We choose a uniformly random subset S of $\{1, \ldots, m\}$. The ciphertext is $\sum_{i \in S} a_i \bmod N$ if the plaintext is 0, and $(\sum_{i \in S} a_i + \lfloor a_{i_0}/2 \rfloor) \bmod N$ if it is 1.

Decryption: We decrypt a received ciphertext $w \in \{0, \ldots, N-1\}$ to 0 if $\mathrm{frc}(w/d) < 1/4$ and to 1 otherwise.

Summarizing the results in [16] on the size of plaintexts, ciphertexts, and keys, the decryption errors, and the security of R03, Regev proved the following theorem.

Theorem 3.1 ([16]). *The cryptosystem R03 encrypts a 1-bit plaintext into an $8n^3$-bit ciphertext with decryption error probability at most $2^{-\Omega(\gamma^2(n)/m)} + 2^{-\Omega(n)}$. The security of R03 is based on the worst case of $O(\gamma(n)\sqrt{n})$-uSVP. The size of the public key is $O(n^4)$ and the size of the private key is $O(n^2)$.*

Our Multi-bit Cryptosystem. We next propose a multi-bit version mR03 of the cryptosystem R03. Let p be a prime such that $2 \leq p \leq n^r$ and $\delta(n) = \omega(n^{1+r}\sqrt{\log n})$ for any constant $r > 0$, where the parameter r controls the trade-off between the decryption errors (or the size of plaintext space) and the hardness of underlying lattice problems. Our cryptosystem mR03 can encrypt one of p plaintexts in $\{0, \ldots, p-1\}$ into a ciphertext of the same size as one of R03.

As mentioned above, R03 relates the ciphertexts to two periodic Gaussian distributions Φ_0 and Φ_1 such that each of them has one peak in a period of length d. Our construction follows the argument in Section 1. The idea of our cryptosystem is embedding of p periodic Gaussian distributions $\Phi_0, \ldots, \Phi_{p-1}$ corresponding to the plaintexts $\{0, \ldots, p-1\}$ into the same period of length d. We also adjust the parameter α, which affects the variance of the Gaussian distributions, to bound the decryption errors. Note that $\mathrm{frc}(h)$ also affects the decryption errors. Therefore, adjusting the set H simultaneously with α, we have to reduce the decryption errors by $\mathrm{frc}(h)$.

Based on the above idea, we describe our cryptosystem mR03 as follows.

Key Generation: Let $H_r = \{h \in [\sqrt{N}, 2\sqrt{N}) : \mathrm{frc}(h) < 1/(8n^r m)\}$. We choose $h \in H_r$ uniformly at random and set $d = N/h$. Choosing $\alpha \in [2/\delta(n), (2\sqrt{2})/\delta(n))$, we sample m values $z_1, \ldots, z_m$ from the distribution $\Phi_{h,\alpha}$, where $z_i = (x_i + y_i)/h$ $(i = 1, \ldots, m)$ according to the above sampling procedure. Let $a_i = \lceil N z_i \rceil$ for every $i \in \{1, \ldots, m\}$. Additionally, we choose an index i'_0 uniformly at random from $\{i : x_i \not\equiv 0 \bmod p\}$. Then, we compute $k \equiv x_{i'_0} \bmod p$. The private key is (d, k) and the public key is $(a_1, \ldots, a_m, i'_0)$.
Encryption: Let $\sigma \in \{0, \ldots, p-1\}$ be a plaintext. We choose a uniformly random subset S of $\{1, \ldots, m\}$. The ciphertext is $\left(\sum_{i \in S} a_i + \left\lceil \sigma a_{i'_0}/p \right\rfloor\right) \bmod N$.
Decryption: For a received ciphertext $w \in \{0, \ldots, N-1\}$, we compute $\tau = w/d \bmod 1$. We decrypt the ciphertext w to $\lceil p\tau \rfloor k^{-1} \bmod p$, where k^{-1} is the inverse of k in $\mathbf{Z}_p$.

We omit the proof of the decryption errors since it can be done by a quite similar analysis to [6]. We also omit the security proof since the reduction is similar as the one of $\mathrm{mAD_{GGH}}$. The performance of our cryptosystem mR03 is summarized as follows.

Theorem 3.2 (multi-bit version). *For any constant $r > 0$, let $\delta(n) = \omega(n^{1+r}\sqrt{\log n})$ and let $p(n)$ be a prime such that $2 \le p(n) \le n^r$. The cryptosystem* mR03 *encrypts a $\lfloor \log p(n) \rfloor$-bit plaintext into an $8n^3$-bit ciphertext with decryption error probability at most $2^{-\Omega(\delta^2(n)/(n^{2r}m))} + 2^{-\Omega(n)}$. The security of* mR03 *is based on the worst case of $O(\delta(n)\sqrt{n})$-uSVP. The size of a public key is the same as that of the original one. The size of a private key is $\lceil \log p(n) \rceil$ plus that of the original one.*

Finally, we present a pseudo-homomorphic property of our cryptosystem mR03. Let E_{m} be the encryption function of mR03.

Theorem 3.3 (pseudo-homomorphism). *Let $\delta(n) = \omega(n^{1+r}\sqrt{\log n})$. Also let $p(n)$ be a prime and κ an integer such that $\kappa p \le n^r$ for any constant $r > 0$. For any κ plaintexts $\sigma_1, \ldots, \sigma_\kappa$ $(0 \le \sigma_i \le p-1)$, we can decrypt the sum of κ ciphertexts $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i) \bmod N$ into $\sum_{i=1}^{\kappa} \sigma_i \bmod p$ with decryption error probability at most $2^{-\Omega((\delta(n))^2/n^{2r}m)}$. Moreover, if there exist two sequences of plaintexts $(\sigma_1, \ldots, \sigma_\kappa)$ and $(\sigma'_1, \ldots, \sigma'_\kappa)$, and a polynomial-time algorithm that distinguishes between $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i) \bmod N$ and $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma'_i) \bmod N$ with its public key, then there exists a polynomial-time algorithm that solves $O(\delta(n)\sqrt{n})$-uSVP in the worst case with non-negligible probability.*

4 A Multi-Bit Version of the Regev'05 Cryptosystem

The cryptosystem R05 proposed in 2005 [17] is also constructed by using a variant of Gaussian distributions. Let $m = 5(n+1)(2\log n + 1) = \Theta(n \log n)$ and $q(n) \in [n^2, 2n^2]$ be a prime. Let $r \in (0,1)$ be any constant, which controls the trade-off between the size of plaintext space and the hardness of underlying lattice problems, and p be an integer such that $p \le n^r = o(n)$, which is the size of the plaintext space in mR05. mR05 can encrypt a plaintext in $\{0, \ldots, p-1\}$ into a ciphertext of the same size as R05. We introduce a parameter $\beta = \beta(n) = o(1/(n^{0.5+r}\log n))$ to control the distribution. The parameter $\beta(n)$ must satisfy $\beta(n)q(n) > 2\sqrt{n}$.

As mentioned in Section 1, we omit the description of R05 and mR05. We only stated the performance and pseudo-homomorphic property of mR05. The performance of our cryptosystem mR05 is summarized as follows.

Theorem 4.1 (multi-bit version). *Let $p = p(n)$ be an integer such that $p(n) \le n^r$ for any constant $0 < r < 1$. The cryptosystem* mR05 *encrypts a $\lfloor \log p(n) \rfloor$-bit plaintext into an $(n+1)\lceil \log q \rceil$-bit ciphertext with decryption error probability at most $2^{-\Omega(1/(m\beta^2(n)n^{2r}))} + 2^{-\Omega(n)}$. The security of* mR05 *is based on the worst case of $\mathrm{SVP}_{\tilde{O}(n/\beta(n))}$ and $\mathrm{SIVP}_{\tilde{O}(n/\beta(n))}$ for quantum polynomial-time algorithms. The size of the public key and private key is the same as that of the original one.*

We present a pseudo-homomorphic property of our cryptosystem mR05. Let E_{m} be the encryption function of mR05.

Theorem 4.2 (pseudo-homomorphism). *Let $p(n)$ and κ be integers such that $\kappa p \le n^r$ for any constant $0 < r < 1$. For any κ plaintexts $\sigma_1, \ldots, \sigma_\kappa$ $(0 \le \sigma_i \le p-1)$, we can decrypt the sum of κ ciphertexts $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i)$ into $\sum_{i=1}^{\kappa} \sigma_i \bmod p$ with decryption error probability at most $2^{-\Omega(1/(m\beta^2(n)n^{2r}))}$, where the addition is defined over $\mathbf{Z}_q^n \times \mathbf{Z}_q$. Moreover, if there exist two sequences of plaintexts $(\sigma_1, \ldots, \sigma_\kappa)$ and $(\sigma'_1, \ldots, \sigma'_\kappa)$, and a polynomial-time algorithm that distinguishes between $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i)$ and $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma'_i)$ with its public key, then there exists a polynomial-time quantum algorithm that solves $\mathrm{SVP}_{\tilde{O}(n/\beta(n))}$ and $\mathrm{SIVP}_{\tilde{O}(n/\beta(n))}$ in the worst case with non-negligible probability.*

5 A Multi-Bit Version of the Ajtai Cryptosystem

Let $F = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ be a basis of a certain lattice which is given in [2]. We also denote by $U_{\mathcal{P}(F)}$ the uniform distribution on $\mathcal{P}(F)$. We suppose that $\eta(n) = \omega(\sqrt{\log n})$ is a parameter to control a trade-off between decryption errors and size of plaintexts. Let $r > 0$ be any constant, which controls the trade-off between the size of plaintext space and the hardness of underlying lattice problems. Let a prime p be the size of plaintext space such that $p < n^{r/6}/(8\eta(n))$. As mentioned in Section 1, we omit the description of A05 and mA05. We only stated the performance of mA05 and the pseudo-homomorphic property of mA05′. The performance of our cryptosystem mA05 is summarized as follows.

Theorem 5.1 (multi-bit version). *The cryptosystem* mA05 *encrypts a* $\lfloor \log p(n) \rfloor$*-bit plaintext into an* $O(n \log n)$*-bit ciphertext with decryption error probability at most* $2^{-\Omega(\eta^2(n))}$*, where* $p < n^{r/6}/(8\eta(n))$*. The size of the public key is the same as that of the original one. The size of the private key is* $\lceil \log p \rceil$ *plus that of the original one.*

We next discuss the pseudo-homomorphic property of mA05. We consider a modified version mA05′ of our multi-bit mA05 is the same cryptosystem as mA05 except that the precision is $2^{-n \log n}$ for its ciphertexts instead of $1/n$. This modified version mA05′ actually has the pseudo-homomorphism. We denote by E_{m} the encryption function of mA05′.

Theorem 5.2 (pseudo-homomorphism). *Let* p *be a prime and* κ *be an integer such that* $\kappa p < n^{r/6}/(8\eta(n))$ *for any constant* $r > 0$*. We can decrypt the sum of* κ *ciphertexts* $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i) \bmod \mathcal{P}(F)$ *into* $\sum_{i=1}^{\kappa} \sigma_i \bmod p$ *with decryption error probability at most* $2^{-\Omega(\eta^2(n))}$*. Moreover, if there exist two sequences of plaintexts* $(\sigma_1, \ldots, \sigma_\kappa)$ *and* $(\sigma'_1, \ldots, \sigma'_\kappa)$*, and a polynomial-time algorithm that distinguishes between* $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma_i) \bmod \mathcal{P}(F)$ *and* $\sum_{i=1}^{\kappa} E_{\mathrm{m}}(\sigma'_i) \bmod \mathcal{P}(F)$ *with its public key, then there exists a polynomial-time algorithm that distinguishes between* $E_{\mathrm{m}}(0)$ *of* mA05′ *and* $U_{\mathcal{P}(F)}$ *with the same public key.*

References

[1] M. Ajtai. "Generating hard instances of lattice problems (extended abstract)". In *STOC '96*, pages 99–108, 1996.

[2] M. Ajtai. "Representing hard lattices with $O(n \log n)$ bits". In *STOC 2005*, pages 94–103, 2005.

[3] M. Ajtai and C. Dwork. "A public-key cryptosystem with worst-case/average-case equivalence". In *STOC '97*, pages 284–293, 1997. See also ECCC TR96-065.

[4] J.-Y. Cai. "A new transference theorem in the geometry of numbers and new bounds for Ajtai's connection factor". *Discrete Applied Mathematics*, 126(1):9–31, 2003.

[5] J.-Y. Cai and T. W. Cusick. "A lattice-based public-key cryptosystem". *Information and Computation*, 151(1-2):17–31, 1999.

[6] O. Goldreich, S. Goldwasser, and S. Halevi. "Eliminating decryption errors in the Ajtai-Dwork cryptosystem". In *CRYPTO '97*, LNCS 1294, pages 105–111, 1997. See also ECCC TR97-018.

[7] O. Goldreich, S. Goldwasser, and S. Halevi. "Public-key cryptosystems from lattice reduction problems". In *CRYPTO '97*, LNCS 1294, pages 112–131, 1997.

[8] S. Goldwasser and D. Kharchenko. "Proof of plaintext knowledge for the Ajtai-Dwork cryptosystem". In *TCC 2005*, LNCS 3378, pages 529–555, 2005.

[9] J. Hoffstein, J. Pipher, and J. H. Silverman. "NTRU: A ring-based public key cryptosystem". In *ANTS-III*, LNCS 1423, pages 267–288, 1998.

[10] D. Micciancio. "Improving lattice based cryptosystems using the Hermite normal form". In *CaLC 2001*, LNCS 2146, pages 126–145, 2001.

[11] D. Micciancio and S. Goldwasesr *Complexity of lattice problems: a cryptographic perspective*. Kluwer, 2002.

[12] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. In *FOCS 2004*, pages 372–381, 2004.

[13] Phong Q. Nguyen. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97. In *CRYPTO '99*, pages 288–304, 1999.

[14] Phong Q. Nguyen and Jacques Stern. Cryptanalysis of the Ajtai-Dwork cryptosystem. In *CRYPTO '98*, pages 223–242, 1998.

[15] S.-H. Paeng, B. E. Jung, and K. C. Ha. "A lattice based public key cryptosystem using polynomial representations". In *PKC 2003*, LNCS 2567, pages 292–308, 2003.

[16] O. Regev. "New lattice-based cryptographic constructions". In *STOC 2003*, pages 407–416, 2003.

[17] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In *STOC 2005*, pages 84–93, 2005.