Analysis of Two Public-Key Encryptions based on Lattice Problems

Jinsu Kim[i†]

[†]Faculty of mathematics, Naval Academy, Gyungnam, 51704 Republic of Korea

Summary
A study on lightweight public key cryptography is one of the important task for cloud computing and IoT environment. Recently, with the advance in quantum computing, many people in various fields are preparing their information systems to be secure for quantum attacks. In this background, we propose and analyze two public-key encryption schemes based on AGCD and LWE in order to see their possibility as lightweight PKE. We apply existing attacks of AGCD and LWE more precisely and concretely. Finally, we show how to choose parameters of the schemes under the consideration of their decryption correctness and security against the proposed attacks. We expect this work would be a post stone for designing lightweight public-key cryptosystem resistant in quantum world.

Key words:
Public-key Encryption, LWE, AGCD, lightweight

1. Introduction

Data communication network enlargement with improvement of computing power and development of cloud computing make ubiquitous world. This enables a variety of service through resource limited and wireless devices such as RFID, USN.

However there exist some vulnerabilities for massive data transmission. Cryptographic solutions are needed to solve the problem, however, almost existing cryptographic primitives are hard to apply directly to them. While the devices used in a service have only limited computation power and the network has limitations on its bandwidth. For these reasons, one need lightweight cryptography which is applicable in limited computing environment. It is clear lightweight cryptography tries to minimize the impact of security and privacy protection on the performance and cost of devices. On the other hand, there is the risk of breaking the security by using minimized cryptographic primitives and protocols. Thus finding the right trade-off between security and cost is therefore important.

In this circumstance, one of the main advantages attributed to symmetric key cryptography is that it is cheaper to implement than public key cryptography. So there have been studies about block ciphers, and hash functions. On the other hand, lightweight public key cryptography as well as symmetric key cryptography have been also studied extensively for its usefulness. It has a key management advantage, and many functionalities like identity based encryption, homomorphic encryption, oblivious transfer, anonymous authentication and signatures, etc.

The studies of lightweight public key cryptography have conducted mainly in three ways. The first is an efficient implementation of existing primitives that is considered as secure, and the next is designing new primitives from new mathematical hard problems in non-commutative group, lattice, polynomial ring, etc. The last is studying about public key encryption schemes that is suitable for low bandwidth environment.

Lattice-based cryptography is gaining more interest due to its security against quantum computers, and its worst case security guarantee. However, the efficiency problem remains. Seen in this light, recent advances in fully homomorphic encryption either improves the efficiency of previous schemes, or proposes a new scheme with better efficiency. In this paper, we propose public-key encryption schemes can be seen as public-key version of FHE schemes, CS[7] and BGV[19]. We consider the existing lattice based attacks more precisely and propose a novel attack strategy on these schemes for smaller size of parameters. From that, we examine the possibility of such schemes as a lightweight public key encryption.

2. Preliminaries

We provide a background on the ACD, LWE problem and recall the CS, BGV fully homomorphic encryption schemes. We also give some basics about lattice and basis reduction in order to explain the attacks of the schemes. We will use (boldface) lower-case letter $\mathbf{a}, \mathbf{b}$ or c, d to denote column vectors, and upper-case letters A, B for matrices. When constructing matrices with vectors, we use $(a, \cdots, b)$ for horizontal concatenation. The product symbol $\cdot$ will be used for both dot products of two vectors, and for matrix product, to be interpreted case by case properly. When speaking of the norm of a vector $\boldsymbol{v}$ over the residue ring $\mathbb{Z}_q$ of $\mathbb{Z}$ modulo q, we mean the shortest norm among the equivalence class of $\boldsymbol{v} \in \mathbb{Z}_q^n$ in $\mathbb{Z}^n$.

Manuscript received November 5, 2019
Manuscript revised November 20, 2019

2.1 Lattice

Lattice is a discrete subgroup of $\mathbb{R}^n$ or a free $\mathbb{Z}$- module. For a set of linearly independent vertors in $\mathbb{R}^n$, say $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_m\}$, a lattice L is defined as the set of all integer combination of $\boldsymbol{b}_i$'s:

$$L = L(B) = \{Bx : B = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_m) \in \mathbb{R}^{n\times m}, x \in \mathbb{Z}^n\}$$

The set of vectors $\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_m\}$, B are called a basis, basis matrix of L respectively. If n = m, the lattice L is said to be a full rank lattice. Just like bases for vector spaces, lattice bases are not unique. Two bases matrices B_1 and B_2 describe the same lattice, if and only if $B_2 = B_1U$, where U is a unimodular matrix, i.e. $det(U) = 1, U \in \mathbb{Z}^{n\times m}$.
One can define the determinant of L as follows, since a lattice L is completely determined by a basis matrix B, and invariant under the choice of the lattice basis,

$$\det(L) := \sqrt{\det(B^tB)}.$$

$det\big(L(B)\big)$ is equal to the volume of the fundamental parallelepiped,

$$P(B) = \{Bx \mid x \in \mathbb{R}^n, \forall i : 0 \le x_i \le 1\}$$

All base of L span the same $\mathbb{R}$-vector subspace of $\mathbb{R}^n$ which we denote by $Span\big(L(B)\big)$ or $Span(B)$. The dimension of $Span(L)$ over $\mathbb{R}$ is equal to the dimension of L. We say that L is a sublattice of a lattice Ω in $\mathbb{R}^n$ if $L \subseteq \Omega$ and if both have the same dimension. In particular, all integral lattice L(i.e. $L \in \mathbb{Z}^n$) is a sublattice of $\overline{L} = \mathrm{Span}(L) \cap \mathbb{Z}^n$. Usually, L is called complete lattice. We define the orthogonal lattice to be $L^\perp := \mathrm{Span}(L)^\perp \cap \mathbb{Z}^n$. Thus, $L^\perp$ is a complete lattice in $\mathbb{Z}^n$ with dimension $n - m$. The already known fact is that $(L^\perp)^\perp = \overline{L}$, and $\det((L^\perp)^\perp) = \det(L^\perp) = \det\big(\overline{L}\big)$. The dual lattice L^* of a lattice L is the set of all vectors $\boldsymbol{y} \in \mathbb{R}^n$ such that $\boldsymbol{y} \cdot \boldsymbol{x} \in \mathbb{Z}$ for all $x \in L$. Given a basis matrix B of L, we can compute the basis matrix B^* of L^* via $B^* = (B^{-1})^t$. Hence $det(L^*) = 1/\det(L)$ .The length of the shortest vector of a lattice $L(B)$ is denoted $\lambda_1\big(L(B)\big)$. More generally, the successive minima (i.e. second and following shortest vectors, linearly independent from the previous minima) are denoted as $\lambda_i\big(L(B)\big)$ for $i = 1, \dots, m$. There exist several bounds and estimations for the length of the shortest lattice vector. In particular, Minkowski's 1st theorem says that

$$\lambda_1\big(L(B)\big) \le \sqrt{m}\big(detL(B)\big)^{1/m}.$$

For a random lattice, the Gaussian heuristic states that

$$\lambda_1\big(L(B)\big) \approx \sqrt{\frac{m}{2\pi e}}\, det\big(L(B)\big)^{1/m}.$$

The Gaussian heuristic only gives an estimation of the length of the shortest vector of a lattice. Note that we follow the notion of a random lattice in [5]. The lattices are following type:
We recall the Gram-Schmidt orthogonalization in linear algebra. This algorithm is closely related with lattice and basis reduction. The transformed orthogonal basis is very helpful when examining lattices. The Gram-Schmidt algorithm makes an orthogonal basis $\{\boldsymbol{b}_1^*, \dots, \boldsymbol{b}_m^*\}$ iteratively as follows:

$$b_i^* = b_i - \textstyle\sum_{j<i} \mu_{i,j}\, b_j^* \quad \text{where} \quad \mu_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}.$$

One can easily compute its determinant as $det\big(L(B)\big) = \prod_i \|b_i^*\|$. This algorithm is related to the i. QR-decomposition B = Q · R with Q an orthonormal matrix and R upper-triangular. The matrix Q can be obtained trivially from the Gram-Schmidt orthogonalization by normalizing the columns of B.
The goal of lattice reduction algorithms is to find a good basis for a given lattice. A basis is considered good, when the basis vectors are almost orthogonal and correspond approximately to the successive minima of the lattice.

2.2 Lattice Reduction

BKZ(Blockwise Korkine-Zolotarev) is a reduction algorithm for lattices that outputs BKZ reduced basis. It has been introduced by Schnorr and Euchner[2]. It finds $\boldsymbol{b}_i^*$ with small norm in β dimensional lattice at each round. Note that, in terms of Q · R decomposition, the goal of lattice reduction is the same with finding small diagonal coefficients $\|\boldsymbol{b}_i^*\|$'s in R. The quality of the basis that is achieved by BKZ reduction depends on the block-size β. Increasing β means an improvement in the basis quality. However, it is known that BKZ algorithm for β > 30 with nontrivial dimensions does not terminate in reasonable time[11]. The BKZ reduction algorithm can be seen as a block-wise version of HKZ reduction. Thus one can see the quality of the output basis is between that of LLL and HKZ reduction.
In 2011, Chen and Nguyen proposed a modification of BKZ using recent progress on lattice enumeration, called BKZ-2.0[18], [17]. This state-of-the-art implementation incorporates the latest improvements of lattice basis reduction[10]. In particular, it use a enumeration technique called extreme pruning in [10]. This enables the BKZ-2.0 algorithm is able to reduce a basis of lattices with much higher block sizes in reasonable time. In particular, these improvements allow to consider block-size β > 50.
Chen and Nguyen also proposed an efficient simulation algorithm of BKZ-2.0 that can be used in high dimensions with large block-sizes β > 50. The simulation algorithm takes as input the Gram- Schmidt norms of an LLL-reduced basis, a block-size $\beta \in \{50, \dots, m\}$ and a number N of rounds, and outputs a prediction for the Gram-Schmidt norms after N rounds of BKZ reduction. This makes it much

easier to heuristically explain the behavior of BKZ-2.0 in practice and the root Hermite factor even for block sizes that we might not be able to run in practice. A sage(python) implementation of this simulation algorithm has been made available by the authors in [17]. For more details about BKZ, and BKZ 2.0, see [18], [17].

In [5], van de Pol and Smart propose an idea that computes the root hermite factor of lattices in 2λ, and [16] improves the approach. They use the reduction cost formula of [18], [17],

$$cost(N,\beta) \leq N \times (m-\beta) \times cost(Enumeration\ in\ \beta) + O(1)$$

to estimate the cost of BKZ-2.0N,β (in terms of the number of nodes visited) on an basis of m- dimensional lattice, and to generate secure parameters. Specifically speaking, for a given security parameter λ and a dimension m, they derive the smallest root Hermite factor δ(m, λ) on an m-dimensional lattice achievable using BKZ-2.0 by an adversary limited to a computational cost. This means that for all β and N, we need to have N × (m − β)× cost(Enumeration in dimension β) ≤ 2λ. Thus, for each β and using the enumeration costs in [18], [17], one obtains an upper bound N_{max} on the number of BKZ-2.0 rounds with block-size β that an adversary bounded as above can afford to run. This yields a root Hermite factor δ(m, λ) for this specific block-size β. By taking the minimum value over all block-sizes, one obtains the minimal root Hermite factor β achievable in dimension m for the security parameter λ using BKZ-2.0.

3. Analysis of PKE's

3.1 The RLWE-based PKE

First, we briefly introduce notation for stating the Ring-LWE-based FHE scheme BGV, and formulate the Ring Learning with Errors(RLWE) Problem. Let d be a positive integer and let $\Phi_d(x) \in \mathbb{Z}[x]$ be the $d-th$ cyclotomic polynomial. Let $R = \mathbb{Z}[x]/(\Phi_d(x))$. The elements of R are polynomials with integer coefficients of degree less than $n = \varphi(d)$. For any polynomial $a = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, let $\|a\|_\infty = max\{|a|: 0 \leq i \leq n\}$ be the infinity norm of a. When multiplying elements of R, the norm of the product grows at most with a factor $\xi = sup\{\|ab\|_\infty / \|a\|_\infty \|b\|_\infty : a, b \in R\}$, the so-called expansion factor. For an integer modulus $q > 0$, define $R_q = R/qR$. Denote by $[\ ]_q$ reduction modulo q into the interval $(-q/2, q/2]$ of an integer or integer polynomial (coefficient wise). Let χ_{key} and χ_{err} be two discrete, bounded probability distributions on R. In practical instantiations, the distribution χ_{err} is typically a truncated discrete Gaussian distribution that is statistically close to a discrete Gaussian. The distribution χ_{key} is chosen to be a very narrow distribution, sometimes even such that the coefficients of the sampled elements are in the set $\{-1, 0, 1\}$. We denote the bounds corresponding to these distributions by B_{key} and B_{err}, respectively. This means that $|e|_\infty < B_{err}$ for $e \leftarrow \chi_{err}$ and $|s|_\infty < B_{key}$ for $s \leftarrow B_{key}$. Now we can define the Ring-LWE distribution on $R_q \times R_q$ as follows: sample $a \leftarrow R_q$ uniformly at random, $s \leftarrow \chi_{key}$ and $e \leftarrow \chi_{err}$, and output $(a, [as + e]_q)$. Next, we formulate a version of the Ring-LWE problem that applies to the schemes BGV considered in this paper.

The Ring-Learning With Errors Problem is the problem to distinguish with non-negligible probability between independent samples $(a_i, [a_i s + e_i]_q)$ from the Ring-LWE distribution and the same number of independent samples (a_i, b_i) from the uniform distribution on $R_q \times R_q$.

We consider here a simple version of original scheme which has no multiplication and based on ring LWE problem. Here, we assume d is a power of 2. Thus $n = d/2$.

- BGV.ParamsGen(λ): Given the security parameter λ, determine $q, d = 2n, N, \chi$ providing security λ and decryption correctness. Output (q, d, N, χ). Note that q, d, χ is the modulus, degree, error distribution on R_q respectively, and the error distribution is the same with key distribution.
- BGV.KeyGen(q, d, N, χ): Sample $t \leftarrow \chi$. Then $sk = (1, t)^t \in R_q^2$. Sample $b \leftarrow R_q^N$, $e \leftarrow \chi^N$. Compute $u = tb + 2e = (tb_1 + 2e_1, \cdots, tb_N + 2e_N)^t$. Then pk $= A = (u - b)$. Note that $A \cdot sk = (u - b)\binom{1}{t} = u - tb = 2e$.
- BGV.Encrypt(A, m): Given a message $m \in \{0, 1\}$, sample $r \leftarrow R_2^N$ uniformly random, and outputs the ciphertext $c = (m, 0) + A^t r \in R_q^2$.
- BGV.Decrypt(sk, c): Decrypt a ciphertext c by $m = [[c \cdot sk]_q]_2$.

We consider the distinguishing attack against RLWE in order to set parameters. In the following, we denote by $0 < \epsilon < 1$ the advantage of adversary to distinguish an RLWE instance $(a, b = a \cdot s + e) \in R_q^2$ from a uniform random instance $(a, u) \in R_q^2$. For any $a \in R_q$, we define $\Lambda_q(a)$ by $\Lambda_q(a) = \{y \in R_q : \exists z \in R, y = a \cdot z\ mod\ q\}$. The distinguishing attack consists in finding a small vector $v \in q\Lambda_q(a)^\times = \left(\Lambda_q(a)\right)^\perp$. Then, for all $y \in \Lambda_q(a), v \cdot y = 0\ mod\ q$. To distinguish whether a given pair (a, u) was sampled according to the RLWE distribution or the uniform distribution, one tests whether the inner product $v \cdot u$ is 'close' to 0 modulo q. (i.e. whether $|v \cdot u| < q/4$) or not. Indeed, when u is uniformly distributed in

R_q, $v \cdot u$ is statistically close to the uniform distribution. However, when (a,u) is an RLWE sample, i.e. there exists $s \in R_q$ and $e \leftarrow \chi_{err}$ such that $u = a \cdot s + e$, we have $v \cdot u = v \cdot e \bmod q$, which is essentially a sample from a Gaussian (reduced modulo q) with standard deviation $|v| \cdot \sigma_{err}$. Now when this parameter is not much larger than q, $v \cdot e$ can be distinguished from uniform with advantage $\exp(-\pi\tau^2)$ with $\tau = |v| \cdot \sigma_{err}/q$. It is unknown how to exploit the ring structure of RLWE to improve lattice reduction ¥cite{CN11}. Therefore, we embed our RLWE instance into an LWE lattice. Next we apply the distinguishing attack against LWE and the result can be used to distinguish the RLWE instance from uniform. Define an LWE matrix $A \in Z_q^{m \times n}$ associated to a as the matrix whose first n lines are the coefficient vectors of x^i for $i = 0, \ldots, n-1$ and the $m - n$ last lines are small linear combinations of the first n lines. Here m must be larger than $k := \frac{n \log q}{\log q - \log 4B - \lambda/n}$ from the uniqueness of LWE problem. Denote the LWE lattice $\Lambda_q(A) = \{y \in Z^m : \exists z \in Z^n, y = Az \bmod q\}$. Now, we use lattice basis reduction in order to find such a short vector $v \in q\Lambda_q(A)^{\times}$. An optimal use of BKZ-2.0 would allow us to recover a vector v such that $|v| = \gamma(m)^m q^{n/m}$ because $\det\left(q\Lambda_q(A)^{\times}\right) = q^n$. Therefore, to keep the advantage of the BKZ-2.0-adversary small enough, we need to have $\exp(-\pi\tau^2) = \exp\left(-\pi\left(\gamma(m)^m q^{n/m}\sigma_{err}/q\right)^2\right) \leq \epsilon$, i.e. $\gamma(m)^m q^{(n/m)-1}\sigma_{err} > \sqrt{-log(\epsilon)/\pi}$. Define $\alpha = \sqrt{-log(\epsilon)/\pi}$. To ensure security for all $m > n$, we obtain the condition $\log_2(q) \leq \min 1_{m>k} \frac{m^2 \log_2(\gamma(m)) + m \log_2(\sigma/\alpha)}{m-n}$. Let us fix the security parameter λ. Following the experiment described in Section 3.2, one can recover the minimal root Hermite factor $\gamma(m)$ for all $m > n$. Therefore, given a target distinguishing advantage ϵ, a dimension n and an error distribution χ_{err}, one can derive the maximal possible value for $\log_2(q)$.

Let's consider the decryption algorithm to check noise term in ciphertext. The message is decrypted by $m = \left[[c \cdot sk]_q\right]_2 = [m + 2e \cdot r]_2$. Thus if $\|2e \cdot r\|_\infty$ is sufficiently small then the decrypted message may be correct. More precisely, if $\|2e \cdot r\|_\infty < q/2$, then $[m + 2e \cdot r]_q = m + 2e \cdot r$. We know $\|2e \cdot r\|_\infty = \|2\sum e_i r_i\|_\infty \leq 2N\xi\|e_i\|_\infty\|r_i\|_\infty \leq 2NnB_\chi$, since $e_i \leftarrow \chi, r_i \leftarrow R_2, \xi \leq n$. Thus we get a constraint about decryption correctness which is $2NnBx < \frac{q}{2}$. In [19], they propose some choices for the value N. It suffices $N > 2\log q$ from [13], or (when q is prime) $N = \log\left(q \cdot \lambda^{\omega(1)}\right)$[19]. Here, we take $N = 2\log q$.

In BGV, it is common to fix the value of σ in advance, and hence the only parameters one can play with are q and n. On one hand we would like q to be large so as to allow correct decryption, but a large q implies low security. Therefore we choose q, n as small as possible holding the correctness and security. Let $\chi = D_{Z^n,\sigma}$ be the spherical discrete gaussian distribution with mean 0 standard deviation σ with probability density function $f(x) = \frac{1}{\alpha} e^{-\pi|x|^2/\sigma^2}$ where $\alpha = \sum_{x \in Z^n} e^{-\pi\|x\|^2/\sigma^2}$. Then all (error) samples are B-bounded with very high probability for $B = 6\sigma$. See for details, [6]. We set $\sigma = 8$ as like [16] which is come from experimental result. Then the error bound $2NnBx$ is less than $2(2\log q)n48$ which must be less than $\frac{q}{2}$. Hence, we get $96n < q/\log q$ which gives a lower bound for $log\, q$. Finally, we get $n = 512, log\, q = 20, \sigma = 8$ for $\lambda = 80$ bit security from the distinguishing attack(max log q), and decryption correctness(min log q).

3.2 The AGCD-based PKE

The approximate common divisor problem(AGCD) is to find the "approximate" common divisor p when elements $a_1 = pq_1 + r_1, \ldots, a_m = pq_m + r_m$ with "small" errors r_i are given. The original formulation of this problem was stated by Howgrave-Graham [9], who gave algorithms based on continued fractions and lattices for solving the case when one receives one exact multiple $a_1 = pq$ and one "noisy" multiple $a_2 = pq_1 + r_1$, and the case when one receives two "noisy" approximate multiples $a_1 = pq_1 + r_1, a_2 = pq_2 + r_2$. This problem was extended to many samples by van Dijk, Gentry, Halevi, and Vaikuntanathan [8], who used it as a hardness assumption underlying the construction of a fully homomorphic encryption scheme DGHV. Since then, similar assumptions have been used to construct many fully homomorphic encryption schemes as well as candidate multilinear maps.

The scheme is a variant of the DGHV encryption scheme that embeds the plaintext message in the most significant bit modulo p of an AGCD sample: a ciphertext c corresponding to a plaintext m is of the form $c = qp + \lfloor p/2 \rceil m + r$. we consider here a simple version of original scheme which has no multiplication.

- CS.ParamsGen(λ): Given the security parameter λ, determine γ, η, ρ and $X, \chi_{key}, \chi_{err}$ providing security λ and decryption correctness. Output $(X, \chi_{key}, \chi_{err})$. Note that γ, η, ρ is the bit-size of X (ciphertext), p (secret key), r (error or noise) respectively.
- CS.KeyGen($X, \chi_{key}, \chi_{err}$): Sample $p \leftarrow \chi_{key}$. For $0 \leq i \leq \tau$, sample $r_i \leftarrow \chi_{err}, q_i \leftarrow Z \cap [0, X/p)$, and compute $x_i = pq_i + r_i$. Relabel so that x_0 is the largest, x_1 has an odd $\lfloor x_1/p \rceil$, and restart if

we cannot find such an x_1. Output $(pk, sk) = ((x_0, x_1, \dots, x_\tau), p)$.

CS.Encrypt($(x_0, x_1, \dots, x_\tau), m$): Given a message $m \in \{0,1\}$, uniformly sample a subset $S \subseteq \{1, 2, \dots, \tau\}$, and output the ciphertext $c = [\sum_{i \in S} x_i + \lfloor x_1/2 \rceil m]_{x_0}$.
CS.Decrypt(p, c): Decrypt a ciphertext c by $m = [\lfloor 2c/p \rceil]_2$.
We consider the orthogonal lattice attack using Nguyen and Stern's Orthogonal Lattice[8]. The goal of the attack is to find p when $x_i = pq_i + r_i$ for $0 \le i \le n$ (or $x = (x_0, \dots, x_n)$) is given. Thus we consider the lattices generated by x and q, r which denote L_x, and $L_{q,r}$. The idea of the attack is to reduce $L_x^\perp$ to recover these $n-1$ vectors of $L_{q,r}^\perp$, from which we can recover r, and hence p. A framework of the attack is as follows:

Compute a BKZ reduced basis $\{b_0, \cdots, b_{n-1}\}$ of $L_x^\perp$ from x.
If $|b_i|$ is sufficiently small, $\{b_0, \cdots, b_{n-2}\} \subseteq L_{q,r}^\perp$. Thus $\{b_0, \cdots, b_{n-2}\}$ is a (BKZ reduced) basis of $L_{q,r}^\perp$
Compute a basis $\{d_1, d_2\}$ of $\left(L_{q,r}^\perp\right)^\perp = \overline{L_{q,r}} \subseteq L_{q,r}$ from $\{b_0, \cdots, b_{n-2}\}$ in step 2.
Compute Lagrange-Gaussian reduced basis of $\left(L_{q,r}^\perp\right)^\perp$. If$\left(L_{q,r}\right) = \left(L_{q,r}^\perp\right)^\perp = \overline{L_{q,r}}$ and r is the shortest vector in $L_{q,r}$, we can find r, so p. Otherwise further works are needed.
Note that there exist an algorithm for computing $L^\perp$ from L. One can refer to an efficient algorithm for that in appendix. In step 2, an attacker must take $n > \frac{\gamma}{\eta - \rho}$. More precisely, let's consider the length of the shortest vector v_0 in $L_x^\perp - L_{q,r}^\perp$.
We see that if $|b_i| < |v_0|$, then $b_i \in L_{q,r}^\perp$ when $|v_0| > \lambda_i\left(L_{q,r}^\perp\right) \approx \cdots \approx \lambda_{n-1}\left(L_{q,r}^\perp\right)$. On the other hand, $\det\left(L_{q,r}^\perp\right)|v_0| \ge \det(L_x^\perp)$, so
$|v_0| \ge \frac{\det(L_x^\perp)}{\det(L_{q,r}^\perp)} = \frac{\det(\overline{L_x})}{\det(\overline{L_{q,r}})} \approx \frac{|x|}{|q||r|} \approx \frac{2^r}{2^{r-\eta}2^\rho} = 2^{\eta-\rho}$.

Heuristically, if q, r were random,
$\lambda_1\left(L_{q,r}^\perp\right) \approx \cdots \approx \lambda_{n-1}\left(L_{q,r}^\perp\right) \approx \sqrt{n-1}\det\left(L_{q,r}^\perp\right)^{\frac{1}{n-1}} \approx 2^{\frac{r+\rho-\eta}{n-1}}$.
Finally it suffice
$\lambda_1\left(L_{q,r}^\perp\right) \approx \cdots \approx \lambda_{n-1}\left(L_{q,r}^\perp\right) \approx 2^{\frac{r+\rho-\eta}{n-1}} < \frac{|x|}{|q|r|} \approx 2^{\eta-\rho}$
for the constrains, because
$$2^{\frac{r+\rho-\eta}{n-1}} < 2^{\eta-\rho} \Leftrightarrow \frac{r+\rho-\eta}{n-1} < \eta - \rho \Leftrightarrow n > \frac{r}{\eta-\rho}$$
Note that attacker can choose arbitrary n. However if n is large, lattice reduction algorithm may not be able to recover the desired short vectors.

Now, we need $|b_i| \ge 2^{\eta-\rho}$ to prevent the attack for all $n > \frac{\gamma}{\eta-\rho}$. It suffices $|b_i| \ge |b_0| = \delta(n,\lambda)^n \det(L_x^\perp)^{\frac{1}{n}} = \delta(n,\lambda)^n 2^{\frac{\gamma}{n}} \ge 2^{\eta-\rho}$ for all $n > \frac{\gamma}{\eta-\rho}$.
Let $n > \frac{\gamma}{\eta-\rho} \ge opt$. Then for $\lambda = 80$, It suffices

$$\delta(n,\lambda)^n 2^{\frac{\gamma}{n}} = 2^{n\log\delta(n,80)}2^{\frac{\gamma}{n}} \ge 2^{\sqrt{\gamma\log\delta(n,80)}} \ge 2^{\sqrt{\gamma\log\delta(opt,80)}} \ge 2^{\eta-\rho}$$

We get $\sqrt{\gamma\log\delta(opt,80)} \ge \eta - \rho$ from above inequality. Finally we get following two constrains that are related with parameter.

$$\gamma \ge \frac{1}{\log\delta(opt,80)}\frac{(\eta-\rho)^2}{4}, \gamma \ge (\eta-\rho)opt$$

All fresh ciphertext c has an inherent noise term, which is $r \in Z$ where $c \bmod p = \lfloor p/2 \rceil + r$. If $|r|$ is small enough, then decryption works correctly. More precisely, ¥cite{CS15} shows that this is the case if $log(8\tau + 2) < \eta - \rho$.
All of the constrains about parameter for a PKE version of CS scheme is following:
$\rho \ge \lambda$(error exhaustive search)
- $\gamma - \eta \ge \lambda$(q exhaustive search)
- $\gamma \ge \frac{1}{\log\delta(opt,80)}\frac{(\eta-\rho)^2}{4}, \gamma \ge (\eta-\rho)opt$ (Orthogonal Lattice Attack)
- $\eta - \rho > \log(8\tau + 2)$
- $\tau \ge r + 2\lambda - 2$(IND-CPA security)

First, we find the value opt such that $\frac{1}{\log\delta(opt,80)}\frac{(\eta-\rho)^2}{4} \approx (\eta-\rho)opt$ by using BKZ$-$\$2.0\$ simulation algorithm. We find thh value $opt = 370$. Next, we compute the smallest γ, η, τ that satisfies the constraints with $\varrho = \lambda = 80$, $opt = 370$. After some calculation, we can set the parameters as $\gamma = 5923, \eta = 96, \tau = 6081$.

5. Conclusion

We propose and analyze a public key encryption version of two fully homomorphic encryption schemes BGV and CS scheme. We apply the existing lattice based attacks more precisely on the schemes, and we set parameters of these scheme with considering decryption correctness and IND-CPA security. When $\lambda = 80$, Our analysis shows that the key size and ciphertext size of AGCD based PKE is 4.29MB and 5,923bit, respectively. On the other hand, the key size and ciphertext size of RLWE based PKE is 1,080bit and 10,260bit, respectively. The ciphertext size of CS scheme is less than that of BGV approximately 1/2. On the other hand, the public key size of CS scheme is too large relatively. Thus it is necessary some optimization for that.

Implementation of the schemes with optimization remains for estimating their speed.

References

[1] C. Peikert, A. Sahai. B. Applebaum, D. Cash. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In CRYPTO, volume 5677 of LNCS, pages 595–618. Springer, 2009.

[2] M. Euchner, C. P. Schnorr. lattice basis reduction: improved practical algorithms and solving subset sum problems. In H. Hand- schuh and M. A. Hasan, editors, Mathematical programming, volume 66, pages 181–199, 1994.

[3] A. Meyer. D. Goldstein. On the equidistribution of hecke p oints. In Forum Math, volume 15, page 165189, 2003.

[4] C. Gentry. Fully homomorphic encryption using ideal lattices. In STOC, pages 169–178, 2009.

[5] N. Smart. J. van de Pol. Estimating key sizes for high dimensional lattice-based systems. In Stam, pages 290–303, 2013.

[6] J. Loftus. M. Naehrig, JW. Bos, K. Lauter. Improved security for a ring-based fully homomorphic encryption scheme. In Stam, pages 45–64, 2013.

[7] D. Steleh, JH. Cheon. Fully Homomorphic Encryption over the Integers Revisited. In Advances in Cryptology - EUROCRYPT 2015. Springer-Verlag, 2015.

[8] S. Halevi, V. Vaikuntanathan, M. van Dijk, C. Gentry. Fully homomorphic encryption over the integers. In EUROCRYPT, LNCS, pages 24–43. Springer, 2010.

[9] N. Howgrave-Graham. Approximate integer common divisors. In Cryptography and Lattice, pages 51–66, 2001.

[10] O. Regev, N. Gama, Phong Q. Nguyen. Lattice enumeration using extreme pruning. In EUROCRYPT, LNCS. Springer, 2010.

[11] O. Regev, N. Gama, P. Nguyen. Lattice enumeration using extreme pruning. In EUROCRYPT, LNCS. Springer, 2010.P. N. Nicolas Gama. Predicting lattice reduction. In EUROCRYPT, volume 4965 of LNCS, pages 31–51. Springer, 2008

[12] J. Stern. P. Nguyen. Merkle-hellman revisited: a cryptanalysis of the qu-vanstone cryptosystem based on group factor- izations. In Proceeding of Crypto 97, volume 1294 of LNCS, pages 198–212. Springer, 1997.

[13] O. Regev. On lattices, learning with errors, random linear co des, and cryptography. In STOC, LNCS, pages 84–93, 2005

[14] C. Peikert, R. Lindner. Better key sizes (and attacks) for lwe-based encryption. In A. Kiayias, editor, CT-RSA, volume 6558 of LNCS, pages 319–339. Springer, 2011

[15] M. Dertouzos, R. Rivest, L. Adleman. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pages 169–180, 1978.

[16] M. Naehrig, T, Lepoint. a comparison of the homomorphic encryption schemes FV and YASHE. In Innovations in Theoretical Computer Science(ITCS'12), 2014.

[17] P. Nguyen, Y. Chen. BKZ 2.0: Better lattice security estimates. Full version.

[18] P. N. Yuanmi Chen. BKZ 2.0: Better lattice security estimates. In ASIACRYPT, LNCS, pages 1–20. Springer, 2011.

[19] V. Vaikuntanathan, Z. Brakerski, Craig Gentry. Fully homomorphic encryption without bootstrapping. In Innovations in Theoretical Computer Science(ITCS'12), 2012.

Jinsu Kim received the B.S. M.S. and D.S. degrees in Mathematical Science from Seoul National University in 2008, 2012 and 2018, respectively. He now with naval academy in Republic of Korea.