Project 1

Xiyue Su

1 R and Z_n

Implemented as **FromRtoZn()** and **FromZntoR()**.

2

2.1 Ideal Lattice

(Task 2a)We'll first prove that I is a full-rank lattice.

Suppose the quadratic ring $R = \frac{Z[x_1,x_2,\cdots,x_r]}{x_1^2-p_1,x_2^2-p_2,\cdots,x_r^2-p_r}$. We keep other notations same as in section 1.1, $e = (e_1, \cdots, e_r) \in \{0,1\}^r$, and define $\alpha_e = \alpha_1^{e_1}\alpha_2^{e_2}\cdots\alpha_r^{e_r}$. Since I is isomorphic to the corresponding ideal lattice L_I, so if we can prove I is n-dimensional, L_I is correspondingly a full-rank lattice. Now that R is isomorphic to Z_n and I is a subspace of R, so the rank of I is at most n. So it suffices to find n linearly independent vectors, i.e.

for $\forall\gamma \neq 0$, $I = R\gamma$ has n linearly independent vectors. In fact, we'll prove that $\forall\gamma \neq 0$, the n vectors $\{\alpha^{(0,\cdots,0,0)}\gamma, \alpha^{(0,\cdots,0,1)}\gamma, \cdots, \alpha^{(1,\cdots,1,1)}\gamma\}$ are linear independent. Considering the linear combinations of these n vectors $\sum_{e\in\{0,1\}^r} a_e \cdot \alpha^e\gamma, a_e \in I$, if

$$\sum_{e\in\{0,1\}^r} a_e \cdot \alpha^e\gamma = \gamma \cdot \sum_{e\in\{0,1\}^r} a_e \cdot \alpha^e = 0 \tag{1}$$

then $\sum_{e\in\{0,1\}}^r a_e \cdot \alpha^e = 0$(we assume that $\gamma \neq 0$ first), therefore $\forall e, a_e = 0$. Here we apply a formally unproved lemma: for $\alpha, \beta \in R$, if $\alpha \cdot \beta = 0$, we'll have $\alpha = 0$ or $\beta = 0$. It's safe to say the lemma stands, because intuitively, the multiplication of two non-zero elements $a_0 + a_1\sqrt{p_1} + a_2\sqrt{p_2} + a_3\sqrt{p_1p_2}$ and $b_0 + b_1\sqrt{p_1} + b_2\sqrt{p_2} + b_3\sqrt{p_1p_2}$ is also non-zero. Furthermore, the rank of an ideal lattice is the degree of the ideal. Then we have a finite degree : $Rank(L_I) = N(I) = \#(R/I)$.

Example: For a 2-dimensional lattice $L \in Z^2$

$$\begin{pmatrix} 0 & 5 \\ 3 & 0 \end{pmatrix} \tag{2}$$

Its corresponding $I = \{3x+5y\alpha | x, y \in Z\}$ is not an ideal, since $\alpha \in R$, while $\alpha(3x + 5y\alpha) \notin I$. It's not an ideal, hence L is not an ideal lattice.

2.2 Norm

Implemented as **Nrm()**.

3

Implemented as **Keygen()**, **Encrypt()** and **Decrypt()**.

4

4.1 Frequency

r	failure times	failure frequency(%)
3	656	6.56
4	14	1.40
5	0	0.00
6	0	0.00

Security issues: finding a decryption failure affects the security, because ciphertexts that produce multiple decryption failures can be used to break the security. If decryption fails, it's probable that some coefficients of $cZ(\gamma)$ are much larger than $q/2$. Actually once multiple failures are found, the attacker can reveal some relevance between the ciphertexts and the secret keys from this. The secret key can be recovered, and the distribution of plaintext will not seem uniform, breaking the IND-CPA security. In all, the adversary can infer some information about the secret keys via decryption failures.

4.2 Additively Homomorphic

First we'll prove that it is additively homomorphic encryption with $Decrypt(C_1 + C_2 \pmod q) = M_1 \oplus M_2$.

We first encrypt two plaintexts M_1,M_2, namely $C_1' := \phi(M_1 + 2\rho_1)$, $C_2' := \phi(M_2 + 2\rho_2)$. By setting $\rho_3 = \rho_1 + \rho_2$. Considering the homomorphism of $\phi : R \to F_q$, we have $C_1' + C_2' := \phi(M_1 + 2\rho_1) + \phi(M_1 + 2\rho_1) = \phi(M_1 + 2\rho_1 + M_2 + 2\rho_2) = \phi(M_1 + M_2 + 2\rho_3)$. Considering we take modulo 2 of ciphertexts during encryption, we have $D(C_1' + C_2' \pmod q) = D(C_1' + C_2') = (M_1 + M_2 + 2\rho_3) \pmod 2 = M_1 \oplus M_2$. So it's indeed 'additively homomorphic'.

No, we cannot add up infinitely. Suppose if we have $C_1 + C_2 + \cdots + C_n$ with an incredibly large n, then $(C_1 + C_2 + \cdots + C_n - kq)Z(\gamma) = (f_1 + f_2 + \cdots + f_n - kZ(\gamma))q + (c_1 + c_2 + \cdots + c_n)Z(\gamma)$; recall that in section 3.1 we must keep $(c_1 + c_2 + \cdots + c_n)Z(\gamma)$ much smaller than $q/2$, which implies that we cannot have infinite ciphertext additions.

4.3 Choice of a_i

To simplify, let's start with one replacement of a_i to $-a_i$, $1 \leq i \leq r$, namely $(\gamma') = (q, \alpha_1 - a_1, \alpha_2 - a_2, ..., \alpha_i + a_i, \alpha_r - a_r)$. Therefore, leading to a new ideal $\phi' : R \to F_q$, we'll have $\phi'(c) = \phi(c) - 2a_i x = \phi(c + 2\rho') = \phi(M + 2(\rho + \rho'))$, where x is a value consisting of other $(r-1)$ a_js, $1 \leq j \leq r, j \neq i$. So the sign flipping of a_i is contained in the change of ρ.

In decryption, we take a modulo 2 of the ciphertexts to remove the effects of ρ as well as the additional $-2a_i x$ brought by the change of a_i. Thus these 2^r ideals of norm q does not change values of decryption.

5

5.1 Estimation

We'll make a rough estimation of the norm q first. Considering we select γ at random, our expected volume should be around $\gamma \leftarrow [\pm B_1/2]^n$. Its expected length should be around $Length(\gamma) = \frac{B_1}{2}(\sqrt{1 + p_1^2 + p_2^2 + \cdots + p_1^2 p_2^2 \cdots p_r^2})$. Therefore, our expected norm of the lattice is $q = Norm(L_\gamma) = Norm(\gamma) \approx (n\frac{B_1}{2}) \cdots (n\frac{B_1}{2}) \cdot (1 + p_1^n + p_2^n + \cdots + p_1^n p_2^n \cdots p_r^n) = (\frac{B_1}{2}n)^n \cdot (1 + p_1^n + p_2^n + \cdots + p_1^n p_2^n \cdots p_r^n)$.

As we have the shortest vector $||\gamma|| = \frac{B_1}{2}(\sqrt{1 + p_1^2 + p_2^2 + \cdots + p_1^2 p_2^2 \cdots p_r^2}) \leq \sqrt{\frac{n}{e\pi}} \cdot \frac{nB_1}{2} \sqrt[n]{(1 + p_1^n + p_2^n + \cdots + p_1^n p_2^n \cdots p_r^n)}$, γ is among the shortest vectors in L_γ.

5.2 qLattice

Implemented as **qLattice()**.

5.3 Frequency

Implemented as **Task5c()**.

r	success times	success frequency(%)
3	7719	77.19
4	990	99.00
5	100	100.00
6	10	100.00

5.4 Coefficients of γ

As we mentioned in 2.2, every ideals with a norm q arises in this way. Since there are 2^r ideals of norm q in all, a new γ with some flipped signs must fall on one of these 2^r ideals where some a_i change their signs. Recall in 4.3 that the change of a_i does not affect the decryption result, so flipping signs in γ won't change it either.

5.5 Other Short Vectors

Other few short vectors include ($\alpha_1\gamma$, $\alpha_2\gamma$,$\cdots$,$\alpha_r\gamma$). Their lengths are at most $p_i \cdot ||\gamma||$, so they are likely to be part of the LLL basis.

6 Relation to Knapsack

It's actually related to the Knapsack problem. The n weights are actually the $a^e = a_1^{e_1} a_2^{a_2} \cdots a_r^{e_r}, e \in \{0,1\}^r$, and the sum should be C.

The encryption looks like $A(M+2\rho) = C \pmod q$, where A is $(1, a_1, a_2, \cdots, a_1 a_2 \cdots a_r)$. Considering that the value of M and ρ is really small, we can regard them as a knapsack problem, given $a_1, a_2, \cdots, a_r$ and the ciphertext C, from this lattice

$$\begin{pmatrix} 1 & 0 & \cdots & 1 & \pmod q \\ 0 & 1 & \cdots & a_1 & \pmod q \\ \vdots & \vdots & & \vdots & \\ 0 & \cdots & 1 & a_1 a_2 \cdots a_r & \pmod q \\ 0 & 0 & \cdots & C & \end{pmatrix} \tag{3}$$

It's easy to see that vector $D := (M+2\rho, 0)$ is in the lattice with a length not greater than $3\sqrt{n}$. One thing to notice: q is very large, so other vectors(except for the first row) with non-zero last component must have much larger lengths than vector D. However, the first row is always the shortest vector for now. One possible solution : if we delete the first row, we'll have a small error introduced by the first component with $|M' - M| < 3$. Therefore, we want to calculate the first component of M by this small error in C and add a vector $(0, 0, \cdots, q)$ as the modulo operation, renew this lattice:

$$\begin{pmatrix} 0 & 0 & \cdots & q \\ 0 & 1 & \cdots & a_1 \\ \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & a_1 a_2 \cdots a_r \\ 1 & 0 & \cdots & C \end{pmatrix} \tag{4}$$

Hence the attacker can use the shortest vector γ' to recover the whole message without recovering the private keys.

Solution: the attack is simple. First we generate an above-mentioned lattice, and its shortest vector γ' is likely to be $(M + 2\rho)$(There is an exception for the first column, which can be calculated from the first and last column). Taking modulo 2 will lead to the corresponding M. Our attack is thus successful.

The solution is implemented as **qLatticeDecrypt()**.

7

7.1 Construction of Lattice

Here, we use a lattice to make the approximation of a Pell's equation. Considering $(c + d\alpha)$ is approximately $\frac{1}{B}$, we have to make sure that $cpB^2 + d\alpha B^2 \approx B^2\alpha(c + d\alpha)$.

So we consider a lattice basis, whose shortest vector v being $(dpB^2+c\alpha B^2, d\alpha)$.

$$\begin{pmatrix} pB^2 & \alpha \\ \alpha B^2 & 0 \end{pmatrix} \tag{5}$$

It's easy to prove that $|c + d\alpha| < \frac{2}{\sqrt{\pi}B} < \frac{4}{\pi d}$. From the Hermite Bound we know that, $|dpB^2 + c\alpha B^2| < ||v||^2 < \frac{2}{\pi e}(det(L))^{\frac{1}{2}} = \frac{2}{\pi e}(\alpha B)$, so we have $|c + d\alpha| < \frac{2}{\pi e \alpha B^2}(\alpha B) = \frac{2}{\pi e B} < \frac{2}{\sqrt{\pi}B}$. On the other hand, the length of second component of the shortest vector v is also smaller than that of v, therefore we have $|d\alpha| < ||v|| < \frac{2}{\pi e}(\alpha B)$. Suppose $c < 0$ and $d > 0$ for simplicity, we can get the second inequality with $d < \frac{2}{\pi e}B < \frac{2}{\sqrt{\pi}}B$.

Now we prove the Norm of $c + d\alpha$ is also bounded by p. We can derive two bounds for both c and d respectively, $|c| < \frac{2}{\sqrt{\pi}}(\frac{1}{B} + B\sqrt{p})$ and $d < \frac{2}{\sqrt{\pi}}B$. So, norm of $c + d\alpha$ is:

$$\begin{aligned} |Norm(c + d\alpha)| = |(c + d\alpha)(c - d\alpha)| &< \frac{2}{\sqrt{\pi}B}|c - d\alpha| \leq \frac{2}{\sqrt{\pi}B}(|c| + |d\alpha|) \\ &< \frac{2}{\sqrt{\pi}B}[(\frac{1}{B} + B\sqrt{p}) + \frac{2B}{\sqrt{\pi}}\sqrt{p}] \\ = \frac{4}{\pi}(2\sqrt{p} + \frac{1}{B^2}) &< \frac{4}{\pi}(2\sqrt{p} + 4) = \frac{8(\sqrt{p} + 2)}{\pi} \end{aligned} \tag{6}$$

7.2 Some Unit

Implemented as **SomeUnit()**.

8

8.1 Smallest Unit

Implemented as **SmallestUnit()**.

References

[1] Nguyen P Q. Hermite's constant and lattice algorithms[M]//The LLL Algorithm. Springer, Berlin, Heidelberg, 2009: 19-69.

[2] D'Anvers J P, Guo Q, Johansson T, et al. Decryption failure attacks on IND-CCA secure lattice-based schemes[C]//IACR International Workshop on Public Key Cryptography. Springer, Cham, 2019: 565-598.