김일성종합대학학보 주체109(2020)년
수 학 제66권 제3호

쌍대환이 없는 다항식환우에서의 오유동반학습문제의 계산복잡성

방미연, 김철은

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《이미 일정한 토대가 있고 전망이 확고한 연구대상들에 힘을 넣어 세계패권을 쥐며 그 성과를 확대하는 방법으로 과학기술을 빨리 발전시켜야 합니다.》

론문에서는 량자콤퓨터로도 풀기 어려운것으로 알려진 격자기반공개열쇠암호의 안전성기초로 널리 연구되고있는 옹근수결수다항식환의 몇가지 잉여환우에서의 오유동반학습문제의 계산복잡성을 연구하였다. 이러한 환우에서의 오유동반학습문제를 간단히 RLWE (Ring-learning with error)문제라고 부른다.

선행연구[1]에서는 한가지 RLWE(Ring-LWE)문제를 처음으로 정식화하였으나 그 문제의 정식화에는 환 R의 쌍대환을 포함하고있는것으로 하여 추가적인 표준뭍기과정을 요구한다. 그로부터 2의 제곱째 원분수환우에서의 RLWE문제의 계산복잡성을 론의하고 그에 기초한 여러가지 암호체계를 내놓았다. 이때까지 많은 암호체계들이 기초하고있는 특수한 2의 제곱째 원분다항식환의 리용은 열쇠길이와 기타 파라메터들이 2배로 늘어나는 결함을 가지고있다. 선행연구[5]에서는 RLWE문제가 2의 제곱째 원분수환이 아닌 다른 형태의 환에 기초할 때 완전효률성이 더 높아진다는것을 보여주었다. 선행연구[4]에서는 임의의 원분수환우의 RLWE문제의 계산복잡성을 론의하였지만 문제의 정식화에서 쌍대환을 제거하지 못하였다.

PLWE문제(Polynomial Ring Learning With Error)[5]는 RLWE문제의 변종으로서 기초하고있는 환이 옹근수결수다항식환의 한가지 잉여환(또는 다항식환)이다.

선행연구[3]에서는 한가지 선형넘기기를 리용하여 RLWE문제의 정식화에서 쌍대환 $R^\vee$을 제거한 PLWE문제로 전환시킬수 있다는것을 보여주었다. 그러나 론문에서 론의된 계산문제의 곤난성에 기초한 암호체계는 옹근수결수다항식환에 대하여 R의 특수한 확장환인 경우 즉 원분다항식의 차수가 2^k 혹은 $2^k p^i$, $2^k p^i q^j$ (p, q :씨수) 인 경우만을 제외하고는 그 잡음의 크기가 전환과정에 얼마나 커지는가에 대한 웃한계를 주지 못한것으로 하여 실용화하기 어렵다. 선행연구[6]에서는 결수들이 모듈수 q와 서로 소인 임의의 모니크다항식들에 대한 PLWE문제의 곤난성을 가정하고 MP-LWE(Middle product-LWE) 문제의 곤난성을 증명하였으며 그에 기초한 암호체계를 구성하였다. 그러므로 2의 제곱째 원분다항식환이 아닌 다른 모양의 환에 기초한 PLWE문제를 연구하는것이 필요하다.

론문에서는 2의 제곱째 원분다항식환에 기초하지 않은 옹근수결수다항식환의 몇가지 잉여환에서의 PLWE문제의 곤난성을 론의한다.

론문에서 다음과 같은 기호들을 받아들인다.

K: 수체, O_K: 수체 K의 대수적옹근수환, $K_{\mathbf{R}} := K \otimes_{\mathbf{Q}} \mathbf{R}$

$R^\vee$: 환 R의 쌍대환, $R_q = R/qR$, $R_q[x] = R[x]/qR[x]$

$a \leftarrow \varphi$: 분포 φ에 따르는 우연량의 표본값을 선택

$a \leftarrow A$: 모임 A에서 원소 a를 임의로 선택

$a \leftarrow U(A)$: 모임 A에서 원소 a를 평등분포에 따라 선택

ξ_m: 단위원소의 원시 m제곱뿌리, $\Phi_m(x) \in \mathbf{Q}[x]$: m째 원분다항식

$$\theta_m(x) = \begin{cases} x^{m-1} - 1, & m\text{이 홀수일 때} \\ x^{m/2} + 1, & m\text{이 짝수일 때} \end{cases}$$

$\mathbf{Q}(\xi_m)$: m째 원분체, 차수는 $\phi(m)$ (오일러함수), $\mathbf{Z}[\xi_m]$: $\mathbf{Q}(\xi_m)$의 대수적옹근수환

$f(n) = w(g(n))$: $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = \infty$가 성립한다는것을 의미, $poly(n)$: n에 관한 다항식함수

정의 1[3] 모임 L이 $\mathbf{R}^n$의 부분모임으로서 더하기부분군이고 리산적일 때 n차원격자라고 부른다. 그리고 격자 L이 유한개의 1차독립인 벡토르단 $\boldsymbol{B}$에 의해 생성될 때 $\boldsymbol{B}$를 격자 L의 토대라고 부른다.

정의 2[2] $\mathbf{R}^n$우에서 정의된 함수 $\rho_s(\boldsymbol{x}) := \exp(-\pi \| \boldsymbol{x} \|^2 / s^2)$에 대하여

$$f(\boldsymbol{x}) := \rho_s(\boldsymbol{x}) / \int_{\mathbf{R}^n} \rho_s(\boldsymbol{z}) d\boldsymbol{z} = \rho_s(\boldsymbol{x}) / s^n$$

모양으로 표시되는 밀도함수를 가지는 분포를 련속가우스분포라고 부르고 ψ_s^n으로 표시한다.

정의 3[2] n차원격자 L의 토대 $\boldsymbol{B}$가 주어졌을 때 이 토대에 관하여 $\| \boldsymbol{v} \| \leq \gamma(n) \cdot \lambda_1(L)$로 되는 령이 아닌 벡토르 $\boldsymbol{v} \in L$을 찾는 문제를 근사최단벡토르문제 간단히 ASVP_γ문제라고 부른다. 여기서 $\gamma(n)$은 근사도, $\lambda_1(L) := \min\limits_{\boldsymbol{v} \in L \setminus \{0\}} \| \boldsymbol{v} \|$이다.

정의 4[4] $s \in R_q^\vee$와 $K_{\mathbf{R}}$우에서의 오유분포 ψ가 주어졌을 때 $R_q \times K_{\mathbf{R}}/qR^\vee$ 우의 벡토르쌍 $(a,\ b = a \cdot s + e \bmod qR^\vee)$ ($a \leftarrow U(R_q)$, $e \leftarrow \psi$)를 우연량으로 취하는 분포를 RLWE분포라고 부르고 $A_{s,\psi}$라고 표기한다.

정의 5[4] $q(\geq 2)$가 옹근수, $\boldsymbol{\psi}$가 $K_{\mathbf{R}}$우에서의 분포족이라고 할 때 $R = O_K$에서의 RLWE문제 즉 $s \in R_q^\vee$와 $\psi \in \boldsymbol{\psi}$에 따라 주어지는 분포 $A_{s,\psi}$에 따르는 임의의 개수의 1차독립인 벡토르쌍 $(a_i,\ b_i)$들이 주어질 때 s를 찾는 문제를 탐색형환오유동반학습문제라고 부른다.

정의 6[4] $s \leftarrow U(R_q^\vee)$에 대하여 주어지는 분포 $A_{s,\psi}$에 따라 뽑은 1차독립인 벡토르쌍들과 같은 수의 $R_q \times K_{\mathbf{R}}/qR^\vee$ 우에서의 평등분포에 따라 뽑은 1차독립인 벡토르쌍들을 구별하는 문제를 판정형환오유동반학습문제라고 부른다.

정의 5와 6에서 정의된 문제들을 통털어 환오유동반학습문제라고 부르고 다같이 $\mathrm{RLWE}_{q,\psi}$라고 표기한다.

정의 7[7] 임의로 주어진 잉여다항식 f와 비밀벡토르 $s \in R_q$에 대하여 $a \leftarrow U(R_q)$, $e \leftarrow \psi$, $e \in R[x]/\langle f(x) \rangle$일 때 $R_q \times R_q[x]/\langle f(x) \rangle$ 우의 벡토르쌍 $(a,\ a \cdot s + e \bmod qR)$들의 분포를 PLWE분포라고 부르고 $\mathrm{RLWE}_{q,\psi}^f(s)$로 표기한다.

정의 8[7] 임의로 선택한 잉여다항식 f와 $s \in R_q$ (모든 벡토르쌍에 대하여 고정)에

대하여 주어진 분포 $\mathrm{RLWE}_{q,\psi}^{f}$ 에 따르는 m 개의 1차독립인 벡토르쌍 $(a_i,\ b_i)$ 가 주어질 때 s 를 찾는 문제를 탐색형 PLWE^{f} 문제라고 한다.

정의 9[7] 임의로 주어진 잉여다항식 f 에 대하여 평등분포 또는 우연적으로 선택한 $s\in R_q$ 에 관한 분포 $\mathrm{RLWE}_{q,\psi}^{f}(s)$ 에 따라 선택되는 m 개의 1차독립인 벡토르쌍 $(a_i,\ b_i)$ 들이 주어질 때 그것들이 어느 분포에 따르는가를 판정하는 문제를 판정형 PLWE^{f} 문제라고 부른다. 정의 8과 9에서 정의된 문제들을 통털어 PLWE문제라고 부른다.

1. 잉여다항식이 $\Phi_{2^k}(x^m)$ 인 PLWE문제의 계산복잡성

정리 1 m 이 웅근수, $n=\varphi(m),\ K=\mathbf{Q}(\xi_m),\ R=\mathbf{Z}(\xi_m),\ R_q=R/qR,\ R^{\vee}=\dfrac{1}{\Phi'_m(\xi_m)}\mathbf{Z}[\xi_m]$, α 는 $\alpha=\alpha(n)>0$ 이고 $\alpha<\sqrt{\log n/n}$ 인 실수, q 는 $q=q(n)\geq 2$ 이고 $\alpha q>w(\sqrt{\log n})$ 이 성립하는 씨수라고 하자. 이때 $R_q\times K_{\mathbf{R}}/qR^{\vee}$ 에서 평등분포에 따라 뽑은 k개의 벡토르쌍들과 k 개의 벡토르쌍 $(a_i,\ a_iw+e_i \bmod qR^{\vee})\in R_q\times K_{\mathbf{R}}/qR^{\vee}$, $1\leq i\leq k$ 를 $1/(poly(n))$ 의 확률로 구별하는 $poly(n)$ 시간알고리듬이 있다면 환 $\mathbf{Z}[\xi_m]$ 의 임의의 이데알에서 근사도 $\gamma=\widetilde{O}(\sqrt{n}/\alpha)$ 의 ASVP_{γ} 문제를 푸는 $O(q\cdot poly(n))$ 시간량자알고리듬이 존재한다. 여기서 $a_i\leftarrow U(R_q)$, $U(R^{\vee}/qR^{\vee})$, $e_i\leftarrow\psi_s^n$, $e_i\in K_{\mathbf{R}}$, $s=\alpha q(nk/(\log(nk)))^{1/4}$ 이다.

따름 $m=2^t\ (t\in\mathbf{N}),\ K=R[x]/\langle\Phi_m(x)\rangle,\ n=\varphi(m),\ R=\mathbf{Z}[x]/\langle\Phi_m(x)\rangle$, $R_q=\mathbf{Z}_q[x]/\langle\Phi_m(x)\rangle$, α 를 $\alpha\in(0,\ 1)$, $\alpha<\sqrt{\log n/n}$ 인 실수, q 를 $q=q(n)\geq 2$ 이고 $q\equiv 1(\bmod m)$, $\alpha q>w(\sqrt{\log n})$ 인 씨수라고 하자. 만일 $R_q\times K/qR$ 에서 평등분포에 따라 뽑은 k 개의 벡토르쌍들과 k 개의 벡토르쌍 $(a_i,\ a_iw+e_i \bmod qR)\in R_q\times K/qR$, $1\leq i\leq k$ (여기서 $a_i,\ w\leftarrow U(R_q)$, $e_i\leftarrow\psi_s^n$, $e_i\in R[x]/\langle\Phi_m(x)\rangle$, $s=\alpha q\sqrt{n}\left(\dfrac{nk}{\log(nk)}\right)^{1/4}$ 로 정의)를 $\dfrac{1}{poly(n)}$ 의 확률로 구별하는 $poly(n)$ 시간알고리듬이 있다면 환 $\mathbf{Z}[\xi_m]$ 의 임의의 이데알에서 근사도 $\gamma=\widetilde{O}(\sqrt{n}/\alpha)$ 의 ASVP_{γ} 문제를 푸는 $O(q\cdot poly(n))$ 시간량자알고리듬이 존재한다.

정리 2[7] $\mathbf{Z}[x]$ 의 모니크다항식 f 에 대하여 만일 $\mathrm{PLWE}_{q,D_{\alpha q}}^{f}$ 문제가 주어진 $k+n-1$ 개의 벡토르쌍들에 대하여 풀기 힘들다면 $\mathrm{PLWE}_{q,D}^{f(x)}$ 문제도 k 개의 벡토르쌍들에 대하여 풀기 힘들다.

정리 3 $l=2^t m\ (t,\ m\in\mathbf{N})$, $K=R[x]/(\Phi_{2^t}(x^m))$, $R=\mathbf{Z}[x]/(\Phi_{2^t}(x^m))$, $R_q=\mathrm{R}/qR$, $n=\varphi(2^t)=2^{t-1},\ K'=R[x]/\langle\Phi_{2^t}(x)\rangle,\ R'=\mathbf{Z}[x]/\langle\Phi_{2^t}(x)\rangle,\ R'_q=\mathbf{Z}_q[x]/\langle\Phi_{2^t}(x)\rangle$ 이고 α 가 $\alpha\in(0,\ 1)$, $\alpha<\sqrt{\log n/n}$ 인 실수, q 는 $q=q(n)\geq 2$, $q\equiv 1(\bmod m)$, $\alpha q>w(\sqrt{\log n})$ 인 씨수라고 하자.

만일 $R_q\times K/qR$ 에서 평등분포에 따라 뽑은 k 개의 벡토르쌍들과 k 개의 벡토르쌍 $(a_i,\ a_iw+e_i \bmod qR)\in R_q\times K/qR$, $1\leq i\leq k$ (여기서 $w=T(w'_0,\ w'_1,\ w'_2,\ w'_{m-1})$, $a_i=T(\widetilde{a}_0,\ \widetilde{a}_1,$

$\widetilde{a}_2, \cdots, \widetilde{a}_{m-1})$, $s=\alpha q\sqrt{n}\left(\frac{n(k+m-1)}{\log(n(k+m-1))}\right)^{1/4}$ 이고 $0\le j\le m-1$ 에 대하여 $w'_j \leftarrow U(R'_q)$, $\widetilde{a}_j \leftarrow U(R'_q)$, $\widetilde{e}_j \leftarrow \psi_s^n$, $\widetilde{e}_j \in \mathbf{Q}[x]/\langle \Phi_{2^t}(x^m)\rangle (=K')$ 이며 넘기기 $T:(R[x]/\langle \Phi_{2^k}(x)\rangle)^m \to R[x]/\langle \Phi_{2^k}(x^m)\rangle$ 는 $T(g_0, g_1, \cdots, g_{m-1})=\sum_{j=0}^{m-1} x^j g_j(x^m)$ 으로 정의)를 $1/poly(n)$ 의 확률로 구별하는 $poly(n)$ 시간알고리듬이 있다면 환 R 의 임의의 이데알에서 근사도 $\gamma=\widetilde{O}(\sqrt{n}/\alpha)$ 의 ASVP_γ 문제를 푸는 $O(q\cdot poly(n))$ 시간량자알고리듬이 존재한다.

지금까지 밝혀진 여러 문제들간의 관계를 도식으로 나타내면 다음과 같다.

$$\mathrm{ASVP}_\gamma \prec_p^q \mathrm{PLWE}^{\Phi_{2^t}(x)} \prec_p^q \mathrm{PLWE}^{\Phi_{2^t}(x^m)}$$

여기서 $\prec_p^q$ 는 량자다항식귀착을 의미한다.

2. 잉여다항식이 $\Phi_{p^k}(x^m)$ 형태인 다항식환에 기초한 PLWE문제의 계산복잡성

선행연구[3]에서는 $f(x)\mapsto f(x) \bmod \Phi_m(x)$ 로 정의되는 넘기기 $\mathbf{Z}[x]/\langle\theta_m(x)\rangle \to \mathbf{Z}[x]/\langle\Phi_m(x)\rangle$ 에 의하여 $\mathbf{Z}[x]/\langle\theta_m(x)\rangle$ 에서 가우스분포에 따라 뽑은 오유다항식을 원분환 $\mathbf{Z}[x]/\langle\Phi_m(x)\rangle$ 에로 넘겨도 다항식이 가우스분포에 따른다는것을 증명하였다.

정리 4[3] m 이 자연수, $R_q=\mathbf{Z}_q[x]/\Phi_m$, q 는 $q\equiv 1 (\bmod\ m)$ 인 씨수, α 는 $\alpha\in(0,\ 1)$ 이고 $\alpha q>w(\sqrt{\log m})$ 인 실수, $m'=\begin{cases} m, & m:\text{홀수} \\ \dfrac{m}{2}, & m:\text{짝수} \end{cases}$ 라고 하자. 만일 $R_q\times R_q$ 에서 평등분포에 따라 뽑은 k 개의 벡토르쌍들과 k 개의 벡토르쌍 $(a_i,\ a_i w+e_i)\in R_q\times R_q$, $1\le i\le k$ (여기서 $a_i, w\leftarrow R_q$, $e'_i\in\mathbf{Q}[x]/\theta_m$, $e'_i\leftarrow\psi_s^{m'}$, $e_i=\lceil e'_i \bmod \Phi_m \rceil$, $s=\sqrt{m'}\alpha q\left(\frac{\phi(m)k}{\log(\phi(m)k)}\right)^{1/4}$)를 $1/poly(m)$ 의 확률로 구별하는 $poly(m)$ 시간알고리듬이 있다면 환 $\mathbf{Z}[\xi_m]$ 의 임의의 이데알에서 근사도가 $\gamma=\widetilde{O}(\sqrt{m}/\alpha)$ 인 ASVP_γ 문제를 푸는 $O(q\cdot poly(m))$ 시간량자알고리듬이 존재한다. 정리 4로부터 다음의 따름을 얻는다.

따름 p 는 2가 아닌 씨수, $R_q=\mathbf{Z}_q[x]/\langle\Phi_p(x)\rangle$, q 는 $q\equiv 1 (\bmod\ p)$ 인 씨수, α 는 $\alpha\in(0,\ 1)$ 이고 $\alpha q>w(\sqrt{\log p})$ 인 실수라고 하자. 만일 $R_q\times R_q$ 에서 평등분포에 따라 뽑은 k 개의 벡토르쌍들과 k 개의 벡토르쌍 $(a_i,\ a_i w+e_i)\in R_q\times R_q$, $1\le i\le k$ (여기서 $a_i,\ w\leftarrow U(R_q)$, $e'_i\in\mathbf{Q}[x]/\langle\theta_p(x)\rangle$, $e'_i\leftarrow\psi_s^p$, $e_i=\lfloor e'_i \bmod \Phi_p \rceil$, $s=\sqrt{p}\alpha q\left(\frac{\phi(p)k}{\log(\phi(p)k)}\right)^{1/4}$)를 $1/poly(p)$ 의 확률로 구별하면 환 $\mathbf{Z}[\xi_p]$ 의 임의의 이데알에서 근사도 $\gamma=\widetilde{O}(\sqrt{p}/\alpha)$ 의 ASVP_γ 문제를 푸는 $O(q\cdot poly(p))$ 시간량자알고리듬이 존재한다.

정리 5 $l = p^t m$ (p 는 2가 아닌 씨수, t, $m \in \mathbf{N}$), $K = R[x]/\langle \Phi_{p^t}(x^m) \rangle$, $R = \mathbf{Z}[x]/\langle \Phi_{p^t}(x^m) \rangle$, $R_q = R/qR$, $n = \varphi(p^t) = p^{t-1}$, $K' = R[x]/\langle \Phi_{p^t}(x) \rangle$, $R' = \mathbf{Z}[x]/\langle \Phi_{p^t}(x) \rangle$, $R'_q = \mathbf{Z}_q[x]/\langle \Phi_{p^t}(x) \rangle$, q 는 $q = q(n) \geq 2$ 이고 $q \equiv 1 (\mathrm{mod}\, p^t m)$ 인 씨수, α 는 $\alpha \in (0,\ 1)$ 이고 $\alpha q > w(\sqrt{\log l})$ 이 성립하는 실수라고 하자. 만일 $R_q \times R_q$ 에서 평등우연적으로 뽑은 k 개의 벡토르쌍들과 k 개의 벡토르쌍 $(a_i,\ a_i w + e_i \bmod qR) \in R_q \times R_q$, $1 \leq i \leq k$ (여기서 $w = T(w'_0,\ w'_1,\ w'_2,\ w'_{m-1})$, $a_i = T(\widetilde{a}_0,\ \widetilde{a}_1,\ \widetilde{a}_2,\ \cdots,\ \widetilde{a}_{m-1})$, $e_i = T(\widetilde{e}_0,\ \widetilde{e}_1,\ \widetilde{e}_2,\ \widetilde{e}_{m-1})$, $s = \alpha q \sqrt{p^t} \left(\dfrac{n(k+m-1)}{\log(n(k+m-1))} \right)^{1/4}$ 이고 $0 \leq j \leq m-1$ 에 대하여 $w'_j \leftarrow U(R'_q)$, $\widetilde{a}_j \leftarrow U(R'_q)$, $\widetilde{e}_j = \lfloor e'_j \bmod \Phi_{p^t} \rfloor$, $e'_i \in \mathbf{Q}[x]/\langle \theta_{p^t}(x) \rangle$ 이며 넘기기 T 는 정리 2에서와 같음)를 $\dfrac{1}{poly(l)}$ 의 확률로 구별하는 $poly(l)$ 시간알고리듬이 있다면 환 R 의 임의의 이데알에서 근사도가 $\gamma = \widetilde{O}(\sqrt{n}/\alpha)$ 인 근사최단벡토르문제 ASVP_γ 를 푸는 $O(q \cdot poly(n))$ 시간량자알고리듬이 존재한다.

참 고 문 헌

[1] V. Lyubashevsky et al.; EUROCRYPT 2010 (LNCS 6110), Springer, 1～23, 2010.
[2] C. Peikert; IACR Cryptology ePrint Archive: Report 2015/939, 1～90, 2015.
[3] L. Ducas et al.; In: PKC 2012 (LNCS 7293), Springer, 34～51, 2012.
[4] V. Lyubashevsky et al.; In: EUROCRYPT 2013 (LNCS 7881), Springer, 35～54, 2013.
[5] Z. Brakerski et al.; In: CRYPTO 2011 (LNCS 6841), Springer, 505～524, 2011.
[6] M. Rosca et al.; In: CRYPTO 2017-III (LNCS 10403), Springer, 283～297, 2017.
[7] M. Bolboceanu; IACR Cryptology ePrint Archive: Report 2018/1035, 1～6, 2018.

주체109(2020)년 3월 15일 원고접수

On the Hardness of Learning with Error Problems over the Polynomial Rings without the Dual Rings

Pang Mi Yon, *Kim Chol Un*

For the polynomial rings of the form $\mathbf{Z}[x]/\langle \Phi_{p^k}(x^m) \rangle$ which has no the dual ring, we give a quantum reduction from the approximate shortest vector problems (ASVP) for the ideals in the corresponding rings to the polynomial learning with errors(LWE) problem over the polynomial rings without the dual ring.

Keyword: post-quantum cryptography