김일성종합대학학보
(자연과학)
주체106(2017)년 제63권 제9호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 63 No. 9 JUCHE106(2017).

오유있는 학습문제에 기초한 한가지 격자암호체계에 대한 연구

리룡철, 김철은

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

《정보통신부문에서는 첨단암호기술을 개발리용하여 통신하부구조의 보안준위를 높임으로써 적들의 해킹과 도청을 철저히 막으며 통신의 안전성과 신뢰성을 확고히 담보하여야 합니다.》

앞으로 량자콤퓨터가 정보처리에 널리 리용되면 RSA암호나 타원곡선암호와 같이 현재 널리 리용되고있는 암호체계는 더이상 쓸수 없게 된다.[2] 이로부터 세계적으로 량자콤퓨터로도 풀수 없는 새로운 암호에 대한 연구가 심화되고있으며 특히 격자암호가 광범히 연구되고있다.

론문에서는 평등우연분포를 리용하여 정의된 오유있는 학습(LWE: Learning With Errors)문제에 기초하여 알고리듬적으로 보다 효률적이고 안전한 격자암호체계의 한가지 구성방법을 제기하고 그 안전성을 증명한다.

선행연구[1]에서 제기된 풀기 어려운 문제로 알려진 LWE문제에 기초한 격자암호체계는 량자콤퓨터를 리용한 공격에 안전하다는 우점이 있지만 열쇠길이가 매우 크다는 결함으로 하여 실용화되지 못하였다.

선행연구[2]에서는 선행연구[1]에서의 암호체계보다 열쇠길이가 더 짧으면서 보다 안전한 격자암호체계를 제기하였다. 이 암호체계는 선행연구들에서 제기된 추상적인 암호체계를 실용화한것인데 다른 격자암호체계들보다 공간효률성이 더 좋다.

그러나 선행연구[2]를 비롯한 일련의 연구들에서 제기된 LWE문제에 기초한 격자암호체계들은 이전의 체계들에 비하여 공간효률성에 있어서나 안전성에 있어서 많이 갱신되였지만 오유분포가 리산가우스분포에 따른다는 가정에 기초하고있기때문에 그것들을 알고리듬으로 실현하자면 품이 많이 든다는 약점을 가지고있다.

선행연구[3]에서는 리산가우스분포대신에 {0, 1}에서의 평등분포를 오유분포로 리용하여도 적당한 제한조건을 주면 LWE문제의 난도가 보장된다는것을 증명하였다.

선행연구들에서 제기된 격자암호체계들에서 알고리듬적으로 보다 실현하기 쉬운 평등분포를 오유분포로 리용하지 못한 리유는 표본개수 m이 충분히 클 때에는 Arora-Ge의 방법[4]으로 $\boldsymbol{Z}_t$ $(t \in \boldsymbol{Z}^+)$에서의 평등분포를 오유분포로 리용한 LWE문제를 풀수 있기때문이였다.

한편 선행연구[3]에서는 일정한 제한조건밑에서 평등분포를 오유분포로 가지는 LWE문제의 복잡성을 증명하였으나 설정된 제한조건의 특성으로 하여 아직까지 그것에 기초한 격자암호체계가 나오지 못하고있다.

우리는 평등분포를 오유분포로 가지는 LWE문제에 기초한 한가지 격자암호체계를 제기한다.

$f(x):=\frac{\rho_s(x)}{\int_{\boldsymbol{R}^n}\rho_s(z)dz}=\frac{\rho_s(x)}{s^n}$, $\rho_s(x)=\exp\left(-\pi\frac{\|x\|^2}{s^2}\right)$ 과 같은 밀도함수를 가지는 분포를 $\boldsymbol{R}^n$ 우에서 파라메터 s 를 가지는 가우스분포라고 한다.

잉여격자 $\boldsymbol{c}+L\subset\boldsymbol{R}^n$ 과 파라메터 $s>0$ 에 대하여 리산가우스(확률)분포 $D_{\boldsymbol{c}+L,\,s}$ 는 $D_{\boldsymbol{c}+L,\,s}\sim\begin{cases}\rho_s(\boldsymbol{x}), & \boldsymbol{x}\in\boldsymbol{c}+L\\ 0, & \boldsymbol{x}\notin\boldsymbol{c}+L\end{cases}$ 을 만족시키는 분포이다. 리산가우스분포는 평활파라메터 s 를 가진다. 이것은 매 잉여류 $\boldsymbol{c}+L$ 들의 가우스질량 $\rho_s(\boldsymbol{c}+L):=\sum_{\boldsymbol{x}\in\boldsymbol{c}+L}\rho_s(\boldsymbol{x})$ 들이 얼마간의 상대오유까지 허용하면서 거의 같아질 때의 가장 작은 정의파라메터로 볼수 있다.

LWE문제는 파라메터로서 웅근수 n 과 q, 웅근수모임 $\boldsymbol{Z}$ 우의 오유분포 χ 를 가진다. 여기서 오유분포 χ 는 보통 면적이 αq $(\alpha<1)$ 인 리산가우스분포에 따르는데 이때 α 를 상대오유률이라고 부른다.

정의 1 [1](LWE분포) 비밀값이라고 부르는 벡토르 $\boldsymbol{s}\in\boldsymbol{Z}_q^n$ 에 대하여 $\boldsymbol{Z}_q^n\times\boldsymbol{Z}_q$ 우에서 평등우연적으로 $\boldsymbol{a}\in\boldsymbol{Z}_q^n$ 을 취하고 $e\leftarrow\chi$ 를 선택하면서 $(\boldsymbol{a},\ b)$ 를 출력하여 표본화되는 분포 $A_{\boldsymbol{s},\,\chi}$ 를 LWE분포라고 부른다. 여기서 $b=\langle\boldsymbol{s},\ \boldsymbol{a}\rangle+e \bmod q$ 이다.

LWE문제는 두가지 부류 즉 LWE분포로부터 여러개의 표본들이 주어졌을 때 비밀값을 찾는 문제(탐색－LWE문제)와 LWE분포표본들과 평등우연표본들이 주어졌을 때 어느것이 LWE분포표본들인가를 결정하는 문제(판정－LWE문제)로 나누어진다.

정의 2 평등우연비밀값 $\boldsymbol{s}\in\boldsymbol{Z}_q^n$ 에 대한 LWE분포 $A_{\boldsymbol{s},\,\chi}$ 로부터 m개의 독립표본들 $(\boldsymbol{a}_i,\ b_i)\in\boldsymbol{Z}_q^n\times\boldsymbol{Z}_q$ 가 주어졌을 때 $\boldsymbol{s}$ 를 찾는 문제를 탐색－LWE문제라고 한다.

정의 3 평등우연비밀값 $\boldsymbol{s}\in\boldsymbol{Z}_q^n$ 에 대한 LWE분포 $A_{\boldsymbol{s},\,\chi}$ 와 평등분포에서 뽑은 m개의 표본들이 주어졌을 때 어느것이 LWE분포 $A_{\boldsymbol{s},\,\chi}$ 의 표본이고 어느것이 평등분포의 표본인가를 결정하는 문제를 판정－LWE문제라고 한다.

대표적인 격자암호체계들에 대하여 보자.

Regev의 암호체계 선행연구[1]에서는 LWE문제에 기초한 다음과 같은 격자암호체계를 내놓았다.

① 비밀열쇠는 평등우연적인 LWE비밀값 $\boldsymbol{s}\in\boldsymbol{Z}_q^n$ 이며 공개열쇠는 LWE분포 $A_{\boldsymbol{s},\,\chi}$ 로부터 뽑은 $m\approx(n+1)\log q$ 개정도의 벡토르 $(\overline{\boldsymbol{a}}_i,\ b_i=\langle\boldsymbol{s},\ \overline{\boldsymbol{a}}_i\rangle)\in\boldsymbol{Z}_q^{n+1}$ 들이다.

행렬로 표시하면 공개열쇠는 $\boldsymbol{A}=\begin{bmatrix}\overline{\boldsymbol{A}}\\ \boldsymbol{b}^t\end{bmatrix}\in\boldsymbol{Z}_q^{(n+1)\times n}$ 과 같다.

이때 $\boldsymbol{b}^t=\boldsymbol{s}^t\cdot\overline{\boldsymbol{A}}+\boldsymbol{e}^t \bmod q$ 이다.(사용자가 여러명인 경우 인증기관이 $\overline{\boldsymbol{A}}$ 를 모든 사용자들에게 배포하여 공유하게 함으로써 공개열쇠크기를 $\boldsymbol{b}^t$ 로 줄인다.)

정의에 의하여 $(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{A}=\boldsymbol{e}^t\approx\boldsymbol{0} \bmod q$ 가 성립된다. 여기서 오유분포 χ 는 리산가우

스분포이다.

② 암호화는 공개열쇠의 우연적인 렬벡토르들의 부분합벡토르의 마지막성분에 통보문비트 μ를 적당히 부호화하여 더하는 방법으로 1개 비트씩 진행한다. 즉 평등우연적으로 $\boldsymbol{x}\in\{0,\ 1\}^m$을 취한 다음 암호문 $\boldsymbol{c}=\boldsymbol{A}\cdot\boldsymbol{x}+\left(\boldsymbol{0},\ \mu\cdot\left\lfloor\frac{q}{2}\right\rfloor\right)^t\in\boldsymbol{Z}_q^{n+1}$을 출력한다.

③ 복호화는 비밀열쇠 $\boldsymbol{s}$를 리용하여 다음과 같이 진행된다.

$$(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{c}=(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{A}\cdot\boldsymbol{x}+\mu\cdot\left\lfloor\frac{q}{2}\right\rfloor=\boldsymbol{e}^t\cdot\boldsymbol{x}+\mu\cdot\left\lfloor\frac{q}{2}\right\rfloor\approx\mu\cdot\left\lfloor\frac{q}{2}\right\rfloor\ \bmod\ q$$

계산결과가 0에 가까우면 0, $\left\lfloor\frac{q}{2}\right\rfloor$에 가까우면 1을 복호화결과로 출력한다.

Lindner와 Peikert의 암호체계 선행연구[2]에서 제기한 암호체계에서는 웅근수모듈수 $q\geq 2$, 웅근수차원수 $n_1,\ n_2\geq 1$과 같은 파라메터들이 리용된다. 이 차원수들은 암호체계가 기초하고있는 LWE문제들과 관련된다.

열쇠생성과 암호화에 리용되는것은 가우스분포파라메터들 $\boldsymbol{s}_k$와 $\boldsymbol{s}_e$, 통보문자모 $\sum$(실례로 $\sum=\{0,\ 1\}$), 통보문길이 $l\geq 1$이다. 또한 통보문자모의 기호에 대하여 오유럭값을 리용하는 단순한 부호화함수 encode: $\Sigma\to\boldsymbol{Z}_q$, 복호화함수 decode: $\boldsymbol{Z}_q\to\Sigma$가 리용된다. 여기서 $t\geq 1$이 충분히 클 때 임의의 웅근수 $e\in[-t,\ t)$에 대하여 다음과 같다.

$$\text{decode}(\text{encode}(\mu)+e\ \bmod\ q)=\mu$$

우리는 평등분포를 오유분포로 하는 LWE문제에 기초하여 선행연구[1]에서 제기한 LWE격자암호체계에 비하여 열쇠길이가 보다 짧고 알고리듬적으로 보다 효률적인 새로운 격자암호체계를 제기한다.

열쇠생성 $\overline{\boldsymbol{A}}\in\boldsymbol{Z}_q^{n\times m}$ ($m\approx n(1+\alpha),\ \alpha>0$)이 평등우연적으로 뽑은 행렬이라고 하고 오유분포 χ가 $\{0,\ 1\}$에서의 평등분포라고 하자.

이때 비밀열쇠는 매 성분을 오유분포 χ에서 표본화한 n차원벡토르 $\boldsymbol{s}\in\{0,\ 1\}^n$이며 공개열쇠는 $\boldsymbol{A}=\begin{bmatrix}\overline{\boldsymbol{A}}\\ \boldsymbol{b}^t\end{bmatrix}\in\boldsymbol{Z}_q^{(n+1)\times m}$과 같다. 여기서 $\boldsymbol{b}^t=\boldsymbol{s}^t\overline{\boldsymbol{A}}+\boldsymbol{e}^t\in\boldsymbol{Z}_q^m$이며 $\boldsymbol{e}$는 매 성분이 χ에서 독립적으로 표본화된 m차원벡토르이다.

이때 $(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{A}=\boldsymbol{e}^t\approx\boldsymbol{0}\ \bmod q$가 성립된다는것을 알수 있다.

암호화 암호화와 복호화는 1개 비트 $\mu\in\{0,\ 1\}$씩 진행한다.

평등우연벡토르 $\boldsymbol{r}\in\{0,\ 1\}^m$을 취하고 다음과 같은 계산을 진행하여 암호문을 출력한다.

$$\boldsymbol{c}=\boldsymbol{A}\cdot\boldsymbol{r}+\left(\boldsymbol{0},\ \mu\cdot\left\lfloor\frac{q}{2}\right\rfloor\right)^t+(\boldsymbol{0},\ e')^t\in\boldsymbol{Z}_q^{n+1},\ e'\leftarrow\chi$$

복호화 복호화는 비밀열쇠 s를 리용하여 다음과 같이 진행한다.

먼저 $(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{c}=(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{A}\cdot\boldsymbol{r}+\mu\cdot\left\lfloor\frac{q}{2}\right\rfloor+e'=\ \mu\cdot\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}^t\cdot\boldsymbol{r}+e'$를 계산한 다음 결과가 $\left\lfloor\frac{q}{2}\right\rfloor$보다 작으면 0, 같거나 크면 1을 출력한다.

평문을 l개 비트씩 암호화하기 위하여서는 암호체계를 다음과 같이 구성하면 된다.

비밀열쇠를 행렬의 매 성분들이 χ에서 독립적으로 표본화된 $\boldsymbol{S}\in\chi^{n\times l}$로, 공개열쇠를

$$\boldsymbol{A}=\begin{bmatrix}\overline{\boldsymbol{A}}\\ \boldsymbol{B}^t\end{bmatrix}\in\boldsymbol{Z}_q^{(n+l)\times m}$$

으로 설정한다. 여기서 $\boldsymbol{B}^t=\boldsymbol{S}^t\overline{\boldsymbol{A}}+\boldsymbol{E}^t\in\boldsymbol{Z}_q^{m\times l}$ 이며 $\boldsymbol{E}\in\chi^{l\times m}$ 은 행렬들의 매 성분들을 χ에서 독립적으로 표본화한 오유행렬이다.[5]

론문에서 제기된 암호체계는 선행연구[1]에서 제기한 암호체계에서 표본개수 $m\approx(n+1)\log q$ 를 $m\approx n(1+\alpha)$ $(\alpha>0)$ 개로 줄이고 대신에 선행연구[2]에서 제기한 착상을 리용하여 암호문에 오유항을 더 첨가함으로써 체계의 안전성을 높이였다.

다음으로 암호체계의 정확성과 안전성에 대하여 론의하자.

정리 1 론문에서 제기된 암호체계의 복호화과정은 파라메터들이 조건 $q>2m+2$ 를 만족시킬 때 정확히 진행된다.

증명 암호체계의 정의로부터 다음식들이 성립된다.

$$(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{c}=\mu\cdot\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}^t\cdot\boldsymbol{r}+e',\ \ 0\le\boldsymbol{e}^t\cdot\boldsymbol{r}\le m,\ \ 0\le e'\le 1$$

따라서 $\mu=0$ 일 때 $0\le(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{c}\le m+1$, $\mu=1$ 일 때 $\left\lfloor\frac{q}{2}\right\rfloor\le(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{c}\le\left\lfloor\frac{q}{2}\right\rfloor+m+1$ 이다.

한편 암호체계의 복호화과정이 정확히 진행되자면 $\mu=0$ 일 때 $0\le(-\boldsymbol{s}^t,1)\cdot\boldsymbol{c}<\left\lfloor\frac{q}{2}\right\rfloor$ 가 성립되여야 하며 $\mu=1$일 때 $\left\lfloor\frac{q}{2}\right\rfloor\le(-\boldsymbol{s}^t,\ 1)\cdot\boldsymbol{c}$ 가 성립되여야 한다.

따라서 $m+1<\left\lfloor\frac{q}{2}\right\rfloor\le\frac{q}{2}$ 와 $\left\lfloor\frac{q}{2}\right\rfloor\le\left\lfloor\frac{q}{2}\right\rfloor+m+1$ 이 성립되여야 한다. 즉 제안된 암호체계는 $q>2m+2$ 일 때 확률 1로 암호문을 정확히 복호화한다.(증명끝)

정리 2 론문에서 제기한 암호체계는 그것이 기초하고있는 LWE문제의 난도가 담보되는 조건에서 CPA－안전하다.

증명 CPA공격자가 평문 μ에 대하여 최대로 알아낸것들이 다 평등우연적인것과 구별불가능하다는것을 밝히면 충분하다.

공격자가 암호체계에 대하여 볼수 있는것은 $(\boldsymbol{A},\ \boldsymbol{c})$ 뿐이다.

그러므로 $(\boldsymbol{A},\ \boldsymbol{c})$ 가 평등우연적인것과 구별불가능하다는것을 밝히면 된다. 여기서 $\boldsymbol{A}=\begin{bmatrix}\overline{\boldsymbol{A}}\\ \boldsymbol{b}^t\end{bmatrix}$는 공개열쇠이며 $\boldsymbol{c}\leftarrow\mathrm{Enc}(\boldsymbol{A},\ \mu)$ 은 암호문이다.

우선 론문에서 제기한 암호체계가 기초하고있는 LWE문제의 난도가 담보된다는 가정으로부터 공개열쇠의 매 렬벡토르들이 평등우연적인것인가 아니면 LWE분포에서 취한 표본들인가를 구별할수 없다는 사실이 나오므로 공개열쇠 $\boldsymbol{A}=\begin{bmatrix}\overline{\boldsymbol{A}}\\ \boldsymbol{b}^t\end{bmatrix}$는 평등우연적인것과 구별불가능하다.

다음으로 $(\boldsymbol{A}, \boldsymbol{c})$ 도 평등우연적인것과 구별불가능하다.

$\boldsymbol{c} = \boldsymbol{A}\cdot\boldsymbol{r} + \left(\boldsymbol{0},\ \mu\cdot\left\lfloor\frac{q}{2}\right\rfloor\right)^t + (\boldsymbol{0},\ e')^t$ 인데 $\boldsymbol{r}$, e' 는 평등우연이고 $\boldsymbol{A}$ 는 평등우연적인것과 구별불가능하다고 볼수 있으므로 암호문 $\boldsymbol{c}$ 는 $\boldsymbol{A}$ 의 매 렬벡토르들과 독립적으로 평등우연적인것과 구별불가능하며 따라서 $(\boldsymbol{A}, \boldsymbol{c})$ 도 평등우연적인것과 구별불가능하다.

따라서 론문에서 제기한 암호체계는 그것이 기초하고있는 LWE문제의 난도가 보장되는 조건에서 CPA－안전하다.(증명끝)

다음으로 암호체계의 기초로 되는 LWE문제의 난도에 대하여 보기로 하자.

정리 3[2] n 과 $m = n\cdot\left(1+\Omega\left(\frac{1}{\log n}\right)\right)$ 이 웅근수이고 $q \geq n^{O(1)}$ 이 충분히 큰 모듈수라고 하면 n, m, q 를 파라메터로 가지고 $\{0, 1\}^m$ 에서의 독립평등분포를 오유분포로 가지는 LWE문제는 최소한 $\Theta(n/\log n)$ 차원격자우에서 $\gamma = \widetilde{O}(\sqrt{n}\cdot q)$ 내의 근사도를 가지는 최악의 경우의 근사격자문제들만큼 어렵다.

정리 4 론문에서 제기한 암호체계가 기초하고있는 LWE문제는 최소한 $\Theta(n/\log n)$ 차원격자우에서 $\gamma = \widetilde{O}(\sqrt{n}\cdot q)$ 내의 근사도를 가지는 최악의 경우의 근사격자문제들만큼 어렵다. 여기서 $\widetilde{O}(f(n))$ 은 $O(\log^c n\cdot f(n))$ 의 간략표시이다. c는 고정된 상수이다.

증명 론문에서 제기한 암호체계가 기초하고있는 LWE문제는 오유분포가 $\{0, 1\}^m$ 에서의 독립평등분포이며 표본수는 $m \approx n(1+c)$ 이고 모듈수는 $q > 2m+2$ 이다.$(c > 0)$

이때 $n(1+c) = n\cdot\left(1+\Omega\left(\frac{1}{\log n}\right)\right)$ 이 성립된다.

왜냐하면 $\exists n' > 0,\ \forall n > n'$ 일 때 $c \geq \frac{1}{\log n}$ 이므로 $\Omega\left(\frac{1}{\log n}\right) = c$ 이기때문이다.

또한 $q \geq n^{O(1)}$ 이 성립된다.

왜냐하면 $q > 2m+2 > 2n > n = n^{O(1)}$ 이기때문이다.

따라서 론문에서 제기한 암호체계가 기초하고있는 LWE문제는 정리 3의 전제조건을 만족시키므로 최소한 $\Theta(n/\log n)$ 차원격자우에서 $\gamma = \widetilde{O}(\sqrt{n}\cdot q)$ 내의 근사도를 가지는 최악의 경우의 근사격자문제들만큼 어렵다.(증명끝)

참 고 문 헌

[1] O. Regev; J. ACM, 56, 6, 1, 2005.

[2] R. Lindner et al.; Better Key Sizes for LWE-based Encryption, CT-RSA, 319～339, 2011.

[3] D. Micciancio et al.; Hardness of SIS and LWE with Small Parameters, CRYPTO, 21～39, 2013.

[4] S. Arora et al.; Lecture Notes in Computer Science, Springer, 403～415, 2011.

주체106(2017)년 5월 5일 원고접수

A Lattice Cryptosystem based on the LWE Problem

Ri Ryong Chol, Kim Chol Un

We propose a construction of a lattice cryptosystem based on LWE problem defined using uniform error distribution, which is more efficient and secure algorithmically, and prove its security.

Key word: lattice cryptosystem