작은 비밀 벡터에 대한 Sparse LWE 보안성 분석 연구

김신, 노재상, 김도혁*, 신동준*
한양대학교, 월넛

{thegimsin, darkelzm, dohyuk1000, djshin}@hanyang.ac.kr,

*{dohyuk1000, djshin}@walllnut.com

A Security Analysis of Sparse LWE with Small Secret Vectors

Sin Kim, Jaesang Noh, Dohyuk Kim*, and Dong-Joon Shin*
Hanyang Univ., *waLLLnut Co., Ltd., Seoul, Korea

요 약

본 논문은 작은 비밀 벡터를 갖는 sparse LWE 의 보안성을 평가하기 위해 행렬의 희소성을 활용한 uSVP 임베딩 기법을 제안하며 BKZ 알고리즘 기반의 보안성 분석을 수행한다. 제안 기법은 0 이 아닌 원소가 존재하는 부분공간 차원을 사용해 격자 기저의 차원을 축소하고, 가우시안 휴리스틱을 통해 각 매개변수 조합에서 공격 성공에 필요한 모듈러스를 추정한다.

Ⅰ. 서론

동형 암호는 암호화된 데이터 위에서 직접 연산을 수행할 수 있도록 하며[1], 계산 효율성을 위해 비밀 벡터의 성분이 작아지도록 주로 이진 또는 삼진 분포를 사용한 샘플링을 자주 사용한다[2]. Sparse learning with error (LWE)는 기존 LWE 난이도 가정을 보존하면서 공개 행렬 A의 각 행을 k개의 0 이 아닌 원소로만 구성하는 희소(sparse) 행렬로 바꿔 저장 공간과 계산 비용을 동시에 절감한다. 이로 인해 연산의 속도가 큰 폭으로 향상되며 동형 암호에서 지연(latency)을 줄이고 연산 속도를 높일 수 있다[3]. 하지만 작은 비밀 벡터를 사용하는 Sparse LWE 가 안전한지는 아직까지 명확히 규명되지 않고 있다.

본 논문에서는 작은 비밀 벡터를 가진 sparse LWE 문제에 대한 보안성을 분석하기 위해 희소 구조를 활용한 uSVP 임베딩 기법을 제안하고 BKZ 알고리즘 기반의 보안성 분석을 수행한다. 기존 임베딩 기법의 경우 LWE 차원 n 에 대해서 $(n+2)$ 차원 기저를 구축하여 uSVP 문제로 환원했지만, 제안된 임베딩 기법은 희소 구조를 활용해 실제 0 이 아닌 원소가 존재하는 k 차원 부분 공간만을 추출하여 $(k+2)$ 차원 기저 기반 uSVP 문제로 환원한다. 이후 BKZ 격자 감소 알고리즘과 가우시안 휴리스틱(Gaussian heuristic)을 적용하여 임베딩된 격자 상에서 최단 벡터 탐색 성능을 평가하고, 이를 바탕으로 다양한 매개변수 조합에서 공격 성공에 필요한 최소 모듈러스를 추정한다.

Ⅱ. LWE 문제와 sparse LWE 문제

각 원소가 $\mathbb{Z}_q$ 에서 균등하게 샘플링 된 공개 행렬 $A \in \mathbb{Z}_q^{m\times n}$ 에 대해서 비밀 벡터 $\mathbf{s} \in \mathbb{Z}_q^n$ 와 오류 벡터 $\mathbf{e}_i \in \mathbb{Z}_q^m$ 로 $\mathbf{b} = \mathbf{As} + \mathbf{e} \bmod q$ 를 구한다. 여기서 정수 n 과 m 은 각각 LWE 차원과 LWE 샘플 수이고 q 는 소수 모듈러스이다. 그러면 LWE 문제는 $(\mathbf{A}, \mathbf{b})$ 로부터 비밀 벡터 $\mathbf{s}$ 를 찾는 문제를 말한다. 구체적으로, 탐색 LWE(search-LWE)문제는 특정 LWE 분포에 의해 생성된 $(\mathbf{a}_i, \mathbf{b}_i)$ 쌍들이 주어지면, 비밀벡터 $\mathbf{s}$를 찾아내는 문제이다. 여기서 $\mathbf{a}_i \in \mathbb{Z}_q^n$는 $\mathbf{A}$의 행 벡터이고 $(\mathbf{a}_i, \mathbf{b}_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + \mathbf{e}_i) \bmod q\ (i = 1, \dots, m)$ 이다. 본 논문에서는 쌍 $(\mathbf{a}, \mathbf{b})$ 를 LWE 샘플로 정의한다. 결정 LWE(decision-LWE) 문제는 $(\mathbf{a}_i, \mathbf{b}_i)$ 쌍들이 주어지면, 이 쌍들이 특정한 LWE 분포로부터 생성된 샘플인지, $\mathbb{Z}_q^n \times \mathbb{Z}_q$에서 무작위로 생성된 샘플인지 구별하는 문제이다.

Sparse LWE 문제는 기존 LWE 문제에서 공개 행렬 $\mathbf{A}$에 희소성(sparsity)을 도입하여 연산 효율성을 개선한 문제이다. 여기서 희소성은 $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$의 각 행이 k개의 0 이 아닌 원소를 포함함을 의미하며 $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$의 각 0 이 아닌 항은 $\mathbb{F}_q^*$에서 균등하게 샘플링된다. 희소성 k에 따라서 계수 행렬 $\mathbf{A}$ 의 저장 크기는 $\frac{n}{k}$배 작아지며 곱셈 속도는 $\frac{n}{k}$배 향상된다. Jain et al. [3]은 적절한 k와 차원 확장을 통해 sparse LWE 가 기존 LWE 와 대체로 동등한 격자 난이도를 유지함을 보였으며, 이를 바탕으로 실용적 보안성을 확보할 수 있음을 제시하였다.

Ⅲ. LWE 에서 uSVP 로의 환원

1) LWE 에서 BDD 로의 환원

비밀 벡터의 norm 이 작다고 가정하면, LWE 문제를 Bounded Distance Decoding(BDD) 문제로 변환할 수 있다. 구체적으로, 기저(basis) 행렬 $\mathbf{B}$를 가지는 격자 $\mathcal{L}(\mathbf{B})$와 목표 벡터 $\mathbf{t}$가 주어졌을 때, $\mathbf{t}$와 $\mathcal{L}(\mathbf{B})$ 사이의 거리가 λ_1의 배수로 상한 제한되어 있을 경우 이때 BDD 문제는 $\mathbf{t}$에 가까운 격자 벡터 $v \in \mathcal{L}(\boldsymbol{B})$를 찾는 것이다.

$$\mathbf{B}_0 = \begin{pmatrix} q & \mathbf{a}_i \\ \mathbf{0}_{m\times 1} & \mathbf{I}_{n\times n} \end{pmatrix}. \quad (1)$$

$\mathbf{As}+\mathbf{e}=\mathbf{b} \bmod q$는 정수 상의 식 $\mathbf{b}=\mathbf{As}+\mathbf{e}+q\cdot\mathbf{c}$로 쓸 수 있으며 이때 $\mathbf{c}\in\mathbb{Z}^m$ 이다. 따라서 격자 $\mathcal{L}(\mathbf{B_0})$는 다음 벡터를 포함한다.

$$\mathbf{B}_0\begin{pmatrix}-\mathbf{c}\\-\mathbf{s}\end{pmatrix}=\begin{pmatrix}-\mathbf{a}_i\cdot\mathbf{s}-q\cdot\mathbf{c}\\-\mathbf{s}\end{pmatrix}=\begin{pmatrix}-\mathbf{b}_i+\mathbf{e}_i\\-\mathbf{s}\end{pmatrix}. \quad (2)$$

따라서 $\mathbf{B}_0$로 생성된 격자에서 목표 벡터 $\mathbf{t}=\begin{pmatrix}\mathbf{b}_i\\\mathbf{0}\end{pmatrix}$에 대해 BDD 문제를 해결하면 작은 벡터 $\begin{pmatrix}-\mathbf{e}_i\\\mathbf{s}\end{pmatrix}$를 얻을 수 있으며, 이를 통해 비밀 벡터 $\mathbf{s}$를 복원할 수 있다.

2) BDD 에서 uSVP 로의 환원

BDD 문제는 Kannan 의 임베딩 기법[4]을 이용하여 uSVP 문제로 환원할 수 있다. 이를 위해 식 (2)에 한 행과 한 열을 추가하여 구성된 기저 행렬 $\mathbf{B}_1$을 고려한다.

$$\mathbf{B}_1=\begin{pmatrix}\mathbf{B}_0 & \mathbf{t}\\ \mathbf{0} & 1\end{pmatrix}=\begin{pmatrix}q & \mathbf{a}_i & \mathbf{b}_i\\ \mathbf{0}_{n\times1} & \mathbf{I}_{n\times n} & \mathbf{0}_{n\times1}\\ 0 & \mathbf{0}_{1\times n} & 1\end{pmatrix}\in\mathbb{F}_q^{(n+2)\times(n+2)}. \quad (3)$$

행렬 $\mathbf{B}_1$의 열들로 생성된 격자는 다음과 같은 유일한 최단 벡터를 포함한다.

$$\mathbf{B}_1\begin{pmatrix}-\mathbf{c}\\-\mathbf{s}\\1\end{pmatrix}=\begin{pmatrix}\mathbf{e}_i\\-\mathbf{s}\\1\end{pmatrix}\in\mathbb{F}_q^{(n+2)}. \quad (4)$$

sparse LWE 에서는 $\mathbf{a}_i'$은 전체 차원 n 대신 k개의 0 이 아닌 원소만 추출하여 구성된 행 벡터이며 $\mathbf{a}_i'$과 이에 대응하는 축소 비밀 벡터인 $\mathbf{s}'$을 이용하여 식 (3)이 아래와 같이 크기가 $(n+2)\times(n+2)$에서 $(k+2)\times(k+2)$로 축소되면, uSVP 문제로의 임베딩 과정에서 저장 공간과 계산 비용이 크게 감소된다.

$$\mathbf{B}=\begin{pmatrix}q & \mathbf{a}_i' & \mathbf{b}_i\\ \mathbf{0}_{k\times1} & \mathbf{I}_{k\times k} & \mathbf{0}_{k\times1}\\ 0 & \mathbf{0}_{1\times k} & 1\end{pmatrix}\in\mathbb{F}_q^{(k+2)\times(k+2)}. \quad (5)$$

$$\mathbf{B}\begin{pmatrix}-\mathbf{c}\\-\mathbf{s}'\\1\end{pmatrix}=\begin{pmatrix}\mathbf{e}_i\\-\mathbf{s}'\\1\end{pmatrix}\in\mathbb{F}_q^{(k+2)}. \quad (6)$$

격자 내에서 λ_1과 λ_2 사이의 간격이 충분히 크다고 가정하면, BKZ 와 같은 격자 축소 알고리즘을 사용하여 유일한 최단 벡터를 구할 수 있다. $\lambda_1(\mathbf{B})$ 벡터는 $\mathcal{L}(\mathbf{B})$ 격자의 최단 벡터이므로, 격자의 첫번째 최소값 λ_1 을 expected norm 으로 근사한다. 이때 σ_e와 σ_s는 각각 비밀 벡터와 오류 벡터가 따르는 이산 가우시안 분포 χ_{σ_e} 및 χ_{σ_s} 의 표준 편차를 나타낸다.

$$\lambda_1(\mathbf{B})\approx\sqrt{\sigma_e^2+\sigma_s^2k+1}. \quad (7)$$

두번째 최소값 λ_2 를 동일한 차원을 갖는 임의의 격자의 첫번째 최소값과 유사하다고 가정하며 가우시안 휴리스틱을 이용하여 다음과 같이 추정한다.

$$\lambda_2(\mathbf{B})\approx\sqrt{\frac{k+2}{2\pi e}}\cdot q^{\frac{1}{k+2}}. \quad (8)$$

τ_β 는 BKZ 와 같은 격자 축소 알고리즘을 적용했을 때 유일한 최단 벡터를 구하기 위해 필요한 보정 계수이며 $\tau_\beta>0$이다. δ_β^{k+2}는 root Hermite factor 로 BKZ 를 한 블록 크기 β로 설정하였을 때 차원 d인 격자에서 첫번째 최소값 $\|v_1\|=\delta_\beta^d\cdot\det(\mathcal{L})^{1/d}$ 로 근사되는 휴리스틱 상수이다. 유일한 최단 벡터를 찾을 수 있는 조건은 다음과 같다.

$$\frac{\lambda_2(\boldsymbol{B})}{\lambda_1(\boldsymbol{B})}\geq\tau_\beta\delta_\beta^{k+2}. \quad (9)$$

식 (9)에 식 (7)과 (8)을 대입하면 식 (10)을 얻게 된다.

$$q\geq\left(\tau_\beta\delta_\beta^{k+2}\sqrt{\frac{2\pi e(\sigma_e^2+\sigma_s^2k+1)}{k+2}}\right)^{k+2}. \quad (10)$$

IV. 보안성 분석

본 실험에서는 sparse LWE 보안성을 평가하기 위해 다음과 같은 파라미터 설정 하에 수행되었다. 희소성 $k=20,30,40$으로 설정하였으며, 모듈러스 q는 $\log_2 q\in[20,100]$ 구간을 균등 분할하여 탐색하였다. BKZ 알고리즘의 블록 크기 β 는 $2,2+\frac{k}{5},2+\frac{2k}{5},2+\frac{3k}{5},2+\frac{4k}{5}$로 변화시키며 각각 10,000 회 반복 실험을 수행하였다. 비밀 벡터와 오차 벡터의 분포는 모두 삼진 분포로 샘플링 하였으며 q 은 추정된 모듈러스 값이며 q^* 는 실제 모듈러스 값을 의미한다. 각 실험을 통해 주어진 (k,q,β) 조합에 대해 공격 성공률을 산출하고, sparse LWE 매개변수 변화가 공격 성능에 미치는 영향을 분석한다.

1) 희소성 $k=20$일 때 보안성 분석

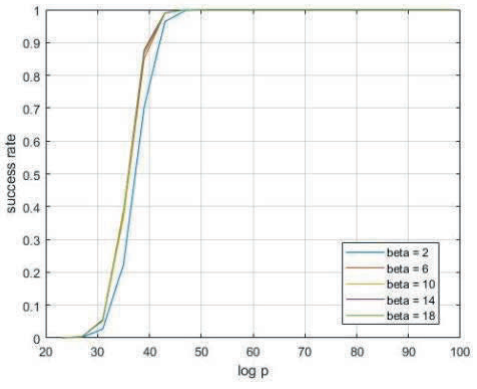

그림 1. $k=20$일 때 BKZ 블록 크기 β에 따른 sparse LWE 공격 성능.

β	2	6	10	14	18
δ_β^{k+2}	1.021	1.017	1.016	1.014	1.014
τ_β	1.16	1.16	1.04	1.04	0.98
q	46.8240	44.0830	39.9301	38.5543	36.6682
q^*	47	47	43	43	43

표 1. $k=20$일 때 각 β별 δ_β^{k+2}, τ_β, 추정치 q 및 실제 성공 최소 q^*

$k=20$ 실험에서 $\beta=2$ 인 경우 성공률이 $\log_2 q\approx45$ 구간에서 급격히 상승하였고 실제 성공 최소 모듈러스 $q^*\approx47$ 이상으로 나타났다. β 를 순차적으로 증가시키자 q^* 는 점차 감소하였다. 한편, q^*는 휴리스틱 예측 값 q와 유사한

감소 추세를 보이며 휴리스틱 모델이 실제 실험 결과를 비교적 정확히 반영함을 확인하였다.

2) 희소성 $k = 30$일 때 보안성 분석

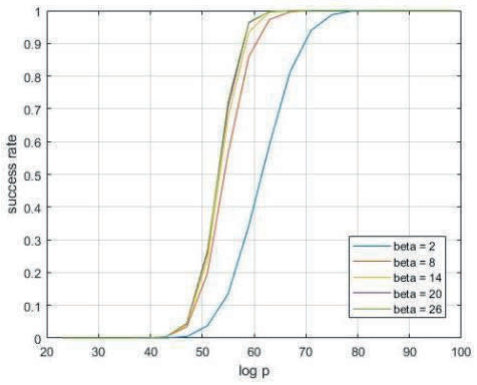

그림 2. $k = 30$일 때 BKZ 블록 크기 β에 따른 sparse LWE 공격 성능.

β	2	6	10	14	18
δ_β^{k+2}	1.021	1.016	1.014	1.013	1.013
τ_β	1.16	1.04	1.04	0.98	0.95
q	77.7021	65.4083	62.4974	58.2964	56.8610
q^*	79	67	63	63	63

표 2. $k = 30$일 때 각 β별 δ_β^{k+2}, τ_β, 추정치 q 및 실제 성공 최소 q^*

$k = 30$ 실험에서 $\beta = 2$인 경우 성공률이 $\log_2 q \approx 55$ 부근에서 크게 상승하였고, 실제 성공 최소 모듈러스 $q^* \approx 79$ 이상으로 나타났다. β를 순차적으로 늘려갈 수록 q^*는 감소하였다. 이와 함께 q도 점차 낮아져 휴리스틱 기반 예측이 실제 실험 결과와 잘 일치함을 확인하였다.

3) 희소성 $k = 40$일 때 보안성 분석

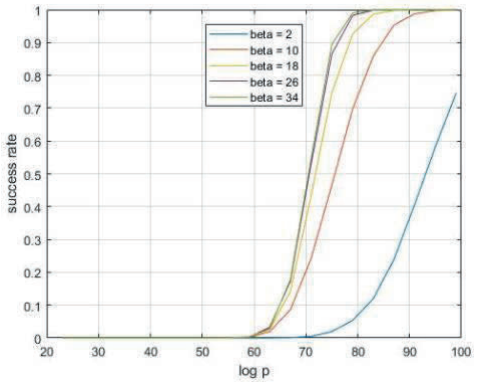

그림 3. $k = 40$일 때 BKZ 블록 크기 β에 따른 sparse LWE 공격 성능.

β	2	6	10	14	18
δ_β^{k+2}	1.021	1.016	1.014	1.013	1.012
τ_β	1.16	1.04	0.98	0.95	0.93
q	114.5768	97.1898	86.8514	82.4565	78.6537
q^*	–	95	87	83	79

표 3. $k = 40$일 때 각 β별 δ_β^{k+2}, τ_β, 추정치 q 및 실제 성공 최소 q^*

$k = 40$ 실험에서 $\beta = 2$ 인 경우 성공률이 $\log_2 q \approx 80$ 이상에서 급격히 상승하였으며, q^*를 측정할 수 없었다. 그러나 β를 증가시키자 q^*은 점차 감소하였고 이에 대응하는 휴리스틱 예측 값 q 역시 동일한 감소 경향을 보였으며 q^*과 1~2 수준의 오차 범위를 유지하였다.

실험 결과 BKZ 블록 크기 β가 커질수록 공격 성공에 필요한 q^*가 감소하였다. 이는 β 증가에 따라 δ_β^{k+2}가 개선되어 임베딩된 최단 벡터 보다 효과적으로 분리해낼 수 있기 때문이다. 또한 희소성 k가 커질 수록 동일한 β 에서 요구되는 q^*도 함께 증가하였는데 이는 k 증가가 임베딩된 기저의 차원을 확장시켜 격자 축소 난이도를 높이기 때문이다. 한편, 휴리스틱 모델을 기반으로 산출된 q와 실제 성공 최소 모듈러스 q^*은 모두 유사한 감소 추세를 보여 휴리스틱 기반 예측이 sparse LWE 공격 성능 분석에 유효함을 확인하였다.

V. 결론

본 논문에서는 작은 비밀 벡터를 가진 sparse LWE 문제에 대한 보안성 분석을 위해 희소 구조를 활용한 uSVP 임베딩 기법을 제안하며 BKZ 알고리즘 기반의 보안성 분석을 제시한다. 공개 행렬의 희소성을 활용해 부분 공간으로 축소하여 기저를 구성한 뒤, BKZ 알고리즘과 가우시안 휴리스틱을 통해 임베딩 된 격자에서 최단 벡터를 탐색한다. 실험 통해 작은 비밀 벡터를 가진 sparse LWE 공격에서 최소 모듈러스를 정량적 분석을 하였고 실용적 매개변수에 관련된 이론적 모델을 제시하였다. 본 연구 결과는 동형 암호 등에서 sparse LWE 매개변수 설정 시 실용적 보안성과 효율성을 고려하는 데 지침이 될 것이다.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.RS-2024-00409492).

참 고 문 헌

[1] M. Albrecht, M. Chase, H. Chen, et al. “Homomorphic encryption security standard,” In MICRO, 2021.

[2] D. Micciancio and C. Peikert, “Hardness of SIS and LWE with small parameters,” CRYPTO 2013, vol. 8042, pp. 21–39, 2013.

[3] A. Jain, H. Lin, and S. Saha, “A Systematic Study of Sparse LWE,” CRYPTO 2024, vol. 14922, pp. 210–245, 2024.

[4] R. Kannan, “Minkowski’s convex body theorem and integer programming,” Math. Oper. Res. 12, vol. 3, pp. 415–440, 1987.