2020

An Automatic Analysis Approach Toward Indistinguishability of Sampling on the LWE Problem

Shuaishuai Zhu
the College of Cryptography Engineering, Engineering University of People’s Armed Police, Xi’an 710086, China.

Yiliang Han
the College of Cryptography Engineering, Engineering University of People’s Armed Police, Xi’an 710086, China.

Xiaoyuan Yang
the Key Laboratory of Network and Information Security under the People’s Armed Police, Engineering University of People’s Armed Police, Xi’an 710086, China.

Follow this and additional works at: https://tsinghuauniversitypress.researchcommons.org/tsinghua-science-and-technology

Part of the Computer Sciences Commons, and the Electrical and Computer Engineering Commons

Recommended Citation
Shuaishuai Zhu, Yiliang Han, Xiaoyuan Yang. An Automatic Analysis Approach Toward Indistinguishability of Sampling on the LWE Problem. Tsinghua Science and Technology 2020, 25(05): 553-563.
An Automatic Analysis Approach Toward Indistinguishability of Sampling on the LWE Problem

Shuaishuai Zhu, Yiliang Han*, and Xiaoyuan Yang

Abstract: Learning With Errors (LWE) is one of the Non-Polynomial (NP)-hard problems applied in cryptographic primitives against quantum attacks. However, the security and efficiency of schemes based on LWE are closely affected by the error sampling algorithms. The existing pseudo-random sampling methods potentially have security leaks that can fundamentally influence the security levels of previous cryptographic primitives. Given that these primitives are proved semantically secure, directly deducing the influences caused by leaks of sampling algorithms may be difficult. Thus, we attempt to use the attack model based on automatic learning system to identify and evaluate the practical security level of a cryptographic primitive that is semantically proved secure in indistinguishable security models. In this paper, we first analyzed the existing major sampling algorithms in terms of their security and efficiency. Then, concentrating on the Indistinguishability under Chosen-Plaintext Attack (IND-CPA) security model, we realized the new attack model based on the automatic learning system. The experimental data demonstrates that the sampling algorithms perform a key role in LWE-based schemes with significant disturbance of the attack advantages, which may potentially compromise security considerably. Moreover, our attack model is achievable with acceptable time and memory costs.

Key words: lattice-based cryptography; learning with errors; security model; Non-Polynomial (NP)-hard problems

1 Background

With breakthroughs in modern computing power, especially the development of quantum computers, cryptography built on conventional hard problems, such as reduction of large numbers and discrete logistic problem, is potentially challenged in terms of security strength. Many hard problems in number theory are no longer complex enough in primitive design facing the quantum algorithms. Thus, post-quantum cryptography is already an emerging field[1,2].

In Post-Quantum Cryptographic (PQC) primitives, the Non-Polynomial (NP)-hard problems in lattice theory are applied in many schemes to construct basic trapdoor functions[3–8], and traditional analysis methodologies have been deployed to qualitatively evaluate PQC schemes, such as side-channel attack[9], flow analysis[10], and message leakage attack[11]. Among all the lattice hard problems, Learning With Errors (LWE) is the most widely and easily applied in the design of Public-Key Encryption (PKE), Identity-Based Encryption (IBE), and Key Encapsulation Mechanism (KEM) protocols. In Refs. [5, 12], LWE is proved to be an NP-complete problem, thus making LWE-based schemes semantically secure against quantum attack models. Another lattice hard problem applied in cryptographic schemes is the Small Integer Solution (SIS), which is a dual problem of LWE. In this paper, we focus on the sampling problem of LWE, including the generation of error vector...
The availability indicates that a chosen error vector comes from instances with or without trapdoors\cite{5}.

**Availability.** The availability indicates that a chosen error vector is a random point that is accurate enough to fit the point on the curve of probability density function.

**Efficiency.** The sampling process should be efficient enough to synchronize the execution of cipher algorithms. A main system bottleneck of the previous LWE schemes is its low efficiency in sampling vectors in lattice space.

The security of an LWE primitive depends on the hardness of decoding the LWE problem masked with error factors. In the realization of the details, the security basis is largely rooted in the indistinguishability and availability of sampling from lattice space. However, in the evaluation routines of semantic security for the existing LWE schemes, the security consideration of sampling components is usually avoided by ideal sampling assumption. In the era of artificial intelligence, the sampling results may be easily identified and cracked without following the above basic properties.

The basic steps of sampling in lattice is defined by an ideal distribution on lattice, such as discrete Gaussian, from which random points are chosen to fit the point on the curve of probability density function. Unfortunately, only a few systematically methods comply with the above properties\cite{13-17}. Rejection sampling\cite{15, 18} is a primitive way of sampling points on a given curve by applying partitioning and testing. Peikert\cite{17} presented inversion sampling and parallel sampling mode to improve sampling efficiency. In Refs. \cite{16, 19}, a dichotomy algorithm that combines rejection and inversion of samples is designed. In Ref. \cite{13}, Buchmann et al. proposed a discrete ziggurat algorithm that aimed to achieve time-memory maximum optimization. Roy et al.\cite{20} designed an Field Programmable Gate Array (FPGA) circuit model based on the Knuth-Yao algorithm, which is an efficient stream generator of random bits. However, its memory consumption is worse than that of the ziggurat algorithm.

In this paper, we analyzed the previous dominant sampling methods and proposed a novel framework to evaluate the mentioned three properties. In the framework, learning systems based on Support Vector Machine (SVM), Logistic Regression (LR), and deep learning models are designed and trained to decide whether a sample is associated with a trapdoor. The proposed framework can be applied in deciding which sampling algorithm is better in handling the indistinguishability of samples.

The rest of this paper is arranged as follows: Necessary preliminaries are listed in Section 2. The statistical attack model is constructed in Section 3 as our main contribution. Supplementary data are demonstrated and analyzed in Section 4 to evaluate the attack framework. We draw our conclusion in the last section.

## 2 Preliminary

### 2.1 Notation

Let $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ denote the integer, real, and complex number fields, respectively. We use the notation $b_i$ to denote a vector or the $i$-th coordinate of $b$ according to our requirements. On different norms of vectors, we note $||v||_1 = \sum_i |v_i|$, $||v||_2 = \sqrt{\sum v_i^2}$, and $||v||_\infty = \max |v_i|$. For an integer lattice $L$, $\lambda^2(L)$ denotes the 2-norm of the shortest non-zero vector in $L$. $\mathcal{D}_{c,c}$ denotes a discrete Gaussian with a mean vector $c$. $\Psi_{q,n}$ denotes a noise distribution bounded by a system modulo $q$ and a security parameter $n$.

### 2.2 Definition

**Definition 1.** Let $B = [b_1 | b_2 | \ldots | b_n]$ be an $n \times n$ matrix, in which $b_1^T, b_2^T, \ldots, b_n^T \in \mathbb{R}^n$ are linearly independent vectors. Then, the $n$-dimensional lattice generated by $B$ is the following vector set:

$$\Lambda = \mathcal{L}(B) = \{ y \in \mathbb{R}^m, \text{s.t. } \exists s \in \mathbb{Z}^m, y = Bs = \sum_{i=1}^n s_ib_i \}. $$

The rank of $\mathcal{L}(B)$ is $n$, indicating that $\mathcal{L}(B)$ contains all linear combinations of $b_1^T, b_2^T, \ldots, b_n^T$.

**Definition 2.** A $(\mathbb{Z}_q, n, \mathcal{D})$-LWE problem defined on a discrete Gaussian distribution $\mathcal{D}$ over $\mathcal{L}$ is the access to

controlled by a fixed trapdoor. Without any exception, a necessary component is vector sampling in lattice space. Previous works show that the properties of sampling algorithms have major influences on time complexity, storage complexity, and overall security.

A sampling algorithm in LWE satisfies the following three basic characters:

**Indistinguishability.** In an LWE sampling algorithm with the same initial parameters, two instances $I_1$ and $I_2$ with respective outcomes $e_1$ and $e_2$ exist, thus making it difficult to decide which outcome is from $I_1$. This character can ensure the dependency of each sampling. In the realization of ciphers, indistinguishability indicates the hardness of deciding whether the error vector comes from instances with or without trapdoors\cite{5}.
a challenge oracle \(\mathcal{O}\), which is either a pseudo-random oracle \(\mathcal{O}_p\) or a truly random oracle \(\mathcal{O}_t\). \(\mathcal{O}_p\) and \(\mathcal{O}_t\) are defined as follows:

\(\mathcal{O}_p\) generates a value \((u_i, v_i) = (u_i, u_i^T s + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\), where \(s\) is a uniformly random vector in \(\mathbb{Z}_q^n\), \(u_i\) are randomly selected vectors in \(D_{c,s}\), and \(e_i \in \mathbb{Z}_q\) are fresh noise samples in \(\Psi_{q,n}\).

\(\mathcal{O}_t\) generates a truly uniform random sample from \(\mathbb{Z}_q^n \times \mathbb{Z}_q\).

Then, the decisional LWE problem is to distinguish the source oracle of the outputs, and the computational LWE problem is to recover \(s\) from \((u_i, v_i)\).

**Definition 3.** An LWE-based PKE scheme consists of four polynomial time algorithms: \((\mathcal{D}, \mathcal{P}) \leftarrow \text{init}(n, q), (A, T_A) \leftarrow \text{keyGen}(\mathcal{D}, \mathcal{P}, s_i) \leftarrow \text{Enc}(\mathcal{A}, m_i, \mathcal{D}), \text{and } m_i \leftarrow \text{Dec}(T_A, c_i)\).

A basic indistinguishability under Chosen-Plaintext Attack (IND-CPA) instance for one-bit message encryption involves the following steps[5]:

1. \((s, B) \leftarrow \text{Keygen}(n, q): \text{Let } \sigma = \sqrt{n} \log^2 n (1/(q \sqrt{2\pi})). \text{ Then, for } s \in \mathbb{Z}_q^n, A = \{a_1, a_2, \ldots, a_n\} \text{ is chosen, in which } a_i \in D_{c,s} \text{ and } e_i \in \Psi_{q}. \text{ Let } B = b_1, b_2, \ldots, b_n, \text{ in which } b_i = \{a_i, s\} + e_i\).
2. \(c \leftarrow \text{Enc}(m, B): \text{Let } c = \left(\sum_{i \in S} a_i, \sum_{i \in S} b_i + m[q/2]\right), \text{ in which } S \text{ is a subset of } 2^{\{0, 1\}}\).
3. \(m \leftarrow \text{Dec}(c, s): \text{For } c = (c_0, c_1), \text{ if } |c_1, s\rangle - |q/2\rangle > |c_1, s\rangle, \text{ the algorithm outputs } m = 0; \text{ else } m = 1\).

**Definition 4.** An indistinguishability game is defined by the following interactions between a challenger \(\mathcal{C}\) and an adversary \(\mathcal{A}\):

- **System initialization.** \(\mathcal{C}\) initiates a decryption oracle with a set of public parameters \(PP = (n, q)\) and sends \(PP\) to \(\mathcal{A}\).

- **Phase 1.** \(\mathcal{A}\) issues \(N\) queries of the plaintext of \(\{c_i\}\) that is adaptively chosen to decrypt. \(\mathcal{C}\) answers the queries with coordinate plaintext \(\{m_i\}\).

- **Challenge.** \(\mathcal{A}\) chooses two challenge messages \(\{m_0, m_1\}\) and sends them to \(\mathcal{C}\). \(\mathcal{C}\) flips a coin and randomly picks a number \(i \in \{0, 1\}\). Then, \(\mathcal{C}\) encrypts \(m_i\) and sends the ciphertext back to \(\mathcal{A}\).

- **Phase 2.** \(\mathcal{A}\) repeats Phase 1 with the knowledge acquired during previous phases.

- **Guess.** \(\mathcal{A}\) outputs a value \(j \in \{0, 1\}\), if \(j = i\), \(\mathcal{A}\) wins the game.

In the above interactive game, an adaptively indistinguishability game under Chosen-Ciphertext Attack (IND-CCA2) is defined. If Phase 2 is closed, then the game is reduced to an IND-CCA game. When the adversary can only access an encryption oracle in Phase 1, then the game reduces to an IND-CPA game. Each type of game can semantically define a security model for LWE-based public key cryptographic primitives.

**Definition 5.** For any polynomial time attacker \(\mathcal{A}\), the cryptographic primitive based on LWE \(S_{\mathcal{A}}^{(q, n, D)}\)-LWE achieves semantical security in a \((\mathbb{Z}_q, n, D)\)-LWE indistinguishable security model, if \(\mathcal{A}\) wins the indistinguishability game with negligible probability.

### 2.3 Assumption and corollary

**Heuristic 1**[21]. For an integer lattice, a constant \(c > 0\) exists such that the ball of radius \(\lambda(2)\) contains at least \(2^c\) points of \(L\). With coordinates renormalized, these points are independently and uniformly distributed in the unit ball.

**Lemma 1**[22, 23]. For any \(q = \text{poly}(n)\) and \(m \geq 5n \log q, n \in \mathbb{Z}^+\), a polynomial time algorithm TrapGen\((q, n)\) exists, which can uniformly generate a random matrix \(A \in \mathbb{Z}_q^{n \times m}\) and a trapdoor matrix \(T_A \in \mathbb{Z}_q^{m \times m}\) satisfying \(||T_A|| \leq O(n \log q)^{1/2}\).

**Lemma 2**[22]. For any \(q \geq 2\), a random matrix \(A \in \mathbb{Z}_q^{n \times n}\), and a trapdoor matrix \(T_A \in \mathbb{Z}_q^{n \times n}\) of lattice \(\Lambda_q^n(A)\):

1. A polynomial time algorithm SampleGaussian\((A, T_A, \sigma, c)\) exists, which returns an error vector \(e \in \Lambda_q^n(A)\) that closely satisfies the discrete Gaussian distribution \(D_{A, \sigma, c}\), in which \(\sigma \geq ||T_A|| \omega((\log n)^{1/2})\) and \(c \in \mathbb{R}^n\).

2. A polynomial time algorithm SamplePre\((A, T_A, u, c)\) exists, which returns an error vector \(e \in \Lambda_q^n(A)\) that closely satisfies \(D_{A, \sigma, c}\) and \(Ac = u \mod q\).

### 2.4 Discrete ziggurat sampling algorithm

The key idea of the ziggurat sampling algorithm is to divide the \(x \geq 0\) part of the area below the Gaussian probability density function \(f(x)\) into \(m\) rectangles with the same area. Then, the coordinate \(x\) is sampled with the following steps:

1. The down-right point \((x_i, y_i)\) of each rectangle is recorded, in which \(x_{m-1} < x_{m-2} < \cdots < x_0\) and \(y_{m-1} > y_{m-2} > \cdots > y_0\).

2. The \(i\)-th rectangle is selected, in which \(i\) is a random integer that satisfies \(1 \leq i < m - 1\).

3. A random number \(x'\) is generated within \([0, x_i]\). If \(x' \leq x_{i+1}\), then \(x'\) is accepted, or else \(x'\) is rejected.

4. \(y' \in [y_{i-1}, y_i]\) is randomly generated. If \(y' + y_{i-1} \leq f(x')\), sampling from the Gaussian distribution
is equivalent to choosing \( x' \); otherwise, Step 2 is performed.

In the discrete field, the approach is identical except with the addition of the following steps to round up to the nearest integers:

1. The area of each rectangle is defined as \((1 + x_i)y_i(y_i - y_{i-1})\), in which \(x_i\) is rounded up to the nearest integer.

2. Let \( y_m = x_0 = 0 \) and \( x_m = t\sigma \), in which \(t\) and \(\sigma\) are the upper bound and variance of the Gaussian distribution, respectively. For all the \(m\) rectangles, we set the same area \(S\). Then, the coordinates are computed with the following iterations:

   \[
   y_{m-1} = S/(1 + x_m),
   x_{m-1} = f^{-1}(y_{m-1}).
   \]

   For \(1 < i < m - 1\),

   \[
   y_i = y_{i+1} + S/(1 + x_{i+1}),
   x_i = f^{-1}(y_i),
   y_0 = y_1 + S/(1 + x_1).
   \]

3. An \(\omega\in\mathbb{Z}^+\) is randomly selected, then \(y'\) is uniformly sampled from \([0,1,\ldots,\omega-1]\). Let \(\bar{y} = \hat{h}_i y'\), in which \(\hat{h}_i\) is the height of the \(i\)-th rectangle and \(\hat{h}_i = y_{i-1} - y_i\). Finally, the algorithm outputs \(\bar{y}\) as a sample.

### 2.5 Other sampling algorithms

**Central limitation method.** Let \(k\) be a uniformly distributed variable: \(k \sim U(0,1)\). Then the variable \(X = \sum_{k=1}^{12} U(k) - 6\) approximately complies with a standard normal distribution if enough \(k\) samples are generated.

**Box-Muller algorithm.** Let \(U_1 \) and \(U_2\) be uniformly distributed variables from independent sample sources, \(X\) and \(Y\) are generated as two independent variables with a normal distribution:

\[
X = \sqrt{-2\ln U_1 \cos(2\pi U_2)},
Y = \sqrt{-2\ln U_1 \sin(2\pi U_2)}.
\]

### 2.6 Automatic learning system

The commonly applied learning frameworks of integer vector-type data are SVM\([24,25]\), LR\([26,27]\), and Convolutional Neural Network (CNN)\([28-30]\), along with their variables. They have superior advantages in extracting the pattern of characters by learning the relationships of different norms of vectors. Given that these automatic learning systems are applied as basic tools in our attack model, their data processing details are not discussed in this paper.

### 3 Statistical Attack

#### 3.1 Inspiration

All the cryptographic primitives based on trapdoor technology usually reduce their hardness to hard problems to achieve a semantic security level in well-defined security models. To the best of our knowledge, some PKE schemes\([3,4,7,22]\) based on LWE and Ring-LWE (RLWE) are proved to be CPA secure in the standard security model, and recently, IBE schemes of CCA secure level\([6,7]\) (and Hierarchical-IBE (HIBE)\([22]\)) appeared in the selective Identity (ID) security model. In the above schemes, the proof of indistinguishability is based on the assumption of ideal sampling. In this section, we take a close look at the process of sampling and analyze the potential influence of sampling algorithms on the semantic reduction in the security proof. Given that the methodology is identical for all the indistinguishability game of LWE, we focus on the IND-CPA security model only, which is a basic and weak security model. If Public Key Cryptography (PKC) schemes under IND-CPA model with the problem of restricted power is proven to be not secure, then the attack results will hold in other strong secure models.

#### 3.2 Attack

In this section, we first initiate an instance of indistinguishability game over LWE-based PKE mentioned in Definition 3 of Section 2.

**System initialization.** \(\mathcal{C}\) fixes an encryption oracle with a set of public parameters \(\mathbb{PP}^* \leftarrow (A = \{a_0, a_1, \ldots, a_n\} \in \mathbb{Z}^{n\times n}, B = \{b_0, b_1, \ldots, b_n\} \in \mathbb{Z}^{n\times n}, \sigma = 1/\sqrt{(\log n)^2}, q \in \mathbb{Z}^\mathbb{N}, \epsilon = 0\), a trapdoor vector \(s \in \mathbb{Z}^n\), and noise vector \(e_i \sim N(c, \sigma/\sqrt{2\pi})\), and sends \(\mathbb{PP}^*\) to \(A\).

**Query phase.** \(A\) issues \(N\) queries of the ciphertexts \(m \in \{0, 1\}\) that are adaptively chosen to encrypt. \(\mathcal{C}\) computes \(c = (\sum_{i\in S} a_i, \sum_{i\in S} b_i + m[q/2]),\) in which \(S\) is a subset of \(2^A.B\). For any chosen \(\epsilon > 0\), \(|S| = (1 + \epsilon)(1 + n)\log q\). Finally, \(\mathcal{C}\) answers the queries with coordinate ciphertexts \(c\). Simultaneously, \(A\) constructs and updates two databases \(O_0\) and \(O_1\), in which \((m = 0, c_m) \in O_0\) and \((m = 1, c_1) \in O_1\). The quantity complexity of \(O_0\) and \(O_1\) is bounded by the attack power of \(A\) or by the time of guess phase issued by \(A\).

Then, \(A\) simulates a guess oracle \(O_{O_0, O_1}\) supervised by \(O_0\) and \(O_1\) with the following steps:

1. All the samples from \(O_0\) and \(O_1\) are divided into
An Automatic Analysis Approach Toward Indistinguishability of Sampling on the LWE Problem

The oracle guess is rejected with the confidence $O_g$. Output a value $b$.

Let $C$ be the mean variable of the sample sets of $O_0$ and $O_1$, then $\bar{X} = n Am + (e_1 + e_2 + \cdots + e_n) \sim N(n Am, \frac{\sigma^2}{n})$. For any $m_1, i \in \{0, 1\}$, we have

$$\bar{X}_i = Am_i + (e_1 + e_2 + \cdots + e_n) \frac{1}{n}$$

and then statistically,

$$\bar{X}_i \sim N(\lambda m_1, \frac{\sigma^2}{n}).$$

Next, we only need to evaluate the parameters $\lambda m_1$, $\frac{\sigma^2}{n}$ by constructing and analyzing the two sample databases built during the query phases of the CPA game. Under the assumption of Heuristic 1, the probability of successfully distinguishing $O_0$ and $O_1$ is negligible, but with the involvement of the realized sampling algorithms with a fixed routine, such as ziggurat sampling algorithm, the noise samples potentially show uncontrolled patterns compared with the ideal Gaussian distributions. From the view of detailed sampling algorithm, we can draw the following series of conclusions to identify pseudo-random samples from true random samples.

**Theorem 1.** On the sample sets $O_0$ and $O_1$, $< A + \frac{\hat{c}}{m_i}, \frac{\sigma^2}{n} >$ satisfies non-bias evaluation and standard error consistency.

**Proof.** Considering the process of sampling from vertex coordinates and true random sources, we compute the limitation of $A + \frac{\hat{c}}{m_i}$ following the heuristic of discrete Gaussian distribution:

$$\lim_{|O_1| \to \infty} E(\frac{\hat{c}}{m_i}) = \lim_{|O_1| \to \infty} E(A) + \lim_{|O_1| \to \infty} E(\frac{\hat{c}}{m_i}) = \Gamma(1 + n/2) |O_1|^{1/n} + \frac{1}{\sqrt{\pi}}.$$

So that for any positive $\epsilon$, we have

$$\lim_{|O_1| \to \infty} P \left\{ \left| A + \frac{\hat{c}}{m_i} - E(A) \right| < \epsilon \right\} =$$

$$\lim_{|O_1| \to \infty} P \left\{ E \left( \frac{\hat{c}}{m_i} \right) < \epsilon \right\} =$$

$$P \left\{ E \left( \frac{\hat{c}}{m_i} \right) < \epsilon \right\} = 1.$$

Also, let $D = S \left( A + \frac{\hat{c}}{m_i} \right)$ be the mean standard error. Then a positive $\epsilon'$ that holds the following requirement exists:

$$\lim_{|O_1| \to \infty} P \left\{ \left| D - \frac{\sigma^2}{n} \right| < \epsilon' \right\} = 1.$$

Then, according to statistical evaluation theory, there exists parameters $A + \frac{\hat{c}}{m_i}, \frac{\sigma^2}{n}$, thus making the partial sample sets $O_0$ and $O_1$ statistically consistent with the LWE vector space. Then, we explain what kind of sample sets are learnable by the following theorem:

$\Lambda$ simulates $k$ guesses toward $O_{00}, O_{11}$ with $m_l, c_1 \in O_0 \cup O_1$, in which $i \in \{0, 1\}$. For an accuracy $\lambda$, the following two hypotheses are made by $\Lambda$:

**H0.** The oracle guess is accepted with the confidence of $\lambda$.

**H1.** The oracle guess is rejected with the confidence of $\lambda$.

Then, the oracle is checked to see whether $P_{O_{00}, O_{11}} (H0) > \lambda$ holds in the simulation. If H1 holds with $k$ requests toward the oracle, $\Lambda$ goes on to make more queries to update $O_0$ and $O_1$.

**Challenge.** $\Lambda$ chooses two challenge messages $m_0$ and $m_1$, and sends them to $C$. $C$ flips a coin and randomly picks a number $i \in \{0, 1\}$. Then $C$ encrypts $m_i$ and sends the ciphertext $c_i$ back to $\Lambda$.

**Guess.** $\Lambda$ outputs a value $j \in \{0, 1\}$, if $j = i$, $\Lambda$ wins the game.

The advantage for $\Lambda$ to win the game is computed as

$$Adv_{\Lambda}^{IND-CPA} = P(\Lambda | M(k \rightarrow 1)) - 1/2.$$
**Theorem 2.** The sample sets \( O_0 \) and \( O_1 \) are learnable, if a traceable pattern expressed by \( \theta \) exists, which covers the outputs in the sampling algorithms.

**Proof.** We assume the vector set \( B = \{b_0, b_1, \ldots, b_n\} \) and \( e_i \) sampled from discrete Gaussian distribution contain energy, as demonstrated by \( ||v||^2 \) for each \( v \). Without losing any generality in any learning system, we consider the neural network structure, in which \( \theta \) is the weight of neural connections. If \( b_i \in O_0 \cup O_1 \), then the energy input by \( B \) is computed as

\[
E(B, h) = -(a^T \cdot B + b^T \cdot h + B \cdot \theta \cdot h),
\]

in which \((a, b, h) \in \{0, 1\}^n\) are the state parameters of the neural network. Then, we construct the joint probability distribution function:

\[
P(B, h) = \frac{1}{Q} e^{-E(B, h)},
\]

\[
Q = \sum_{B, h} e^{-E(B, h)}.
\]

According to Theorem 1, a complete evaluation of \( i \in \{0, 1\} \) can be obtained from \( O_0 \) and \( O_1 \). Therefore, we can evaluate \( \hat{i} \) in the following conventional statistical learning model:

\[
(B, i) \xrightarrow{P(h|(B, i), \theta)} h \xrightarrow{P((B, i)|h, \theta)} \hat{i},
\]

in which \( P(h|(B, i), \theta) \) and \( P(i|h, \theta) \) are computed as follows:

\[
P(h|(B, i), \theta) = \frac{1}{Q_B} \cdot e^{b^T \cdot h + B \cdot w \cdot h},
\]

\[
Q_B = P(B) \cdot Q,
\]

\[
P((B, i)|h, \theta) = \frac{1}{Q_h} \cdot e^{a^T \cdot B + B \cdot w \cdot h},
\]

\[
Q_h = P(h) \cdot Q.
\]

Then, we can construct an optimization function with the cross-entropy model:

\[
\arg\max \{ J(\hat{\theta}) \} = \max \left\{ \sum_{j=1}^{N} \log P(b_j) \right\} = \max \left\{ \sum_{j=1}^{N} \log \sum_{B, h} e^{-E(b_j, h)} \right\} - N \log \sum_{B, h} e^{-E(B, h)},
\]

which can be optimized by solving the partial dispersal differential equations on each batch of input according to the analysis in Ref. [5]. For \( k = (|O_0| + |O_1|)/N \) chosen in the learning phase, an optimized accuracy \( \lambda_k = P(B, i|h, \theta) \) exists, in which the guess oracle outputs \( \hat{i} \) as the learning result.

**Theorem 3.** On the sample sets \( O_0 \) and \( O_1 \) from sampling algorithm \( SA \), which outputs \( s_{(0)} = Am + \epsilon(0) \) and \( s_{(1)} = Am + \epsilon(1) \), a decision model \( M \) exists to decide the value of \( i \) with non-negligible probability of accuracy, if \( O_{O_0, O_1} \) outputs \( \hat{i} \) with the distinguishable accuracy of non-negligible probability of accuracy.

**Proof.** If \( O_{O_0, O_1} \) outputs \( \hat{i} \) with distinguishable accuracy of non-negligible probability \( \epsilon \), then \( \mathcal{A} \) can gain the \( \epsilon \)-advantage over \((O_0, O_1)\) from the learning phase by launching \( k \) rounds of challenge simulation with the oracle. In the challenge phase, \( \mathcal{A} \) outputs a guess with the output of \( O_{O_0, O_1} \). According to the completeness of \(|O_0| \) and \(|O_1| \), if \( \epsilon \) is significantly non-negligible, then in the one-time real challenge with \( C \), the advantage of \( \mathcal{A} \) is

\[
\text{Adv}_{\mathcal{A}}^{\text{IND-CPA}} = P\{H_0|M(k = (|O_0| + |O_1|)/N)\} - \frac{1}{2} = \frac{P(H_0, k = (|O_0| + |O_1|)/N)}{\epsilon} - \frac{1}{2},
\]

in which \( \mu \) indicates the optimized mapping of the parameter \( \lambda_k \). If \( \lambda_k \) is non-negligible, then the above advantage is non-negligible.

**4 Data**

In this section, we instantiate the IND-CPA game defined in Section 3 to test the availability and performance of the attack framework between \( C \) and \( \mathcal{A} \).

**4.1 Configuration**

To fully evaluate the performance of our distinguishing model, we realize an instance of the IND-CPA game, in which the adversary \( \mathcal{A} \) launches attacks by constructing a guess oracle with a learning system. We design a series of comparative tests to demonstrate the effectiveness of the attack approach, including the frameworks of accuracy, computing costs, and the parameter optimization. Our computing platform includes: (1) the adversary: ThinkCentre with Intel Core i5@2.7 GHz, 4 GB DDR4 RAM and 1 Gbit/s; 1 TB storage, and 1 Gbit/s ethernet; (2) the challenger: Lenovo X230 with Intel Core i5@2.4 GHz, 4 GB DDR4 RAM, and 1 Gbit/s ethernet.

Algorithms are coded based on Keras running on Anaconda 3.7 (64 bit) with initial parameters listed in Table 1. Uniformly random vectors are sampled with fplll library.

**4.2 Result**

Given that the automatic cryptographic analysis based on learning theory is still a new research field, no comparable results in indistinguishable security attacks...
Table 1 Initial parameter list.

| Parameter | Initial value |
|-----------|---------------|
| $n$       | $[60, 80]$    |
| $q$       | $2n^2$        |
| $N$       | $[80, q^n] \in \mathbb{Z}^+$ |
| $|O_0|$    | $[1, 2^{\sqrt{2n} \log n}] \in \mathbb{Z}^+$ |
| $|O_1|$    | $[1, 2^{\sqrt{2n} \log n}] \in \mathbb{Z}^+$ |
| $a$       | $1$           |
| $b$       | $1$           |
| $|k|$      | $1024$        |
| $w$       | $[0, 1] \in \mathbb{R}^+$ |

Table 2 Results in accuracy test.

| Model of oracle | $k$ | $N \times 10^5$ | Best advantage |
|-----------------|-----|-----------------|----------------|
| Semantic advantage | NULL | $2^{\sqrt{n} - 1}n$ | Negligible |
| SVM             | $1$ | $1.15$ | $0.122$ |
| CNN             | $80$ | $2.90$ | $0.260$ |
| LR              | $80$ | $2.00$ | $0.093$ |

Table 3 Results of the accuracy test in the CNN-based oracle.

| Model of oracle | $k$ | $n$ | Best advantage |
|-----------------|-----|-----|----------------|
| Ideal pseudo-random | NULL | $[60, 80]$ | Negligible |
| Ziggurat        | $80$ | $60$ | $0.140$ |
| CLT             | $80$ | $60$ | $0.260$ |
| Box-Muller      | $80$ | $60$ | $0.230$ |

likely to be Gaussian types of samples, according to the assumption of CLT. Also, the sample sets from CLT contain less isolated points, which may be accumulated as a significant character in CNN. The process of Box-Muller sampling consists of three fitting curves with uniformly distributed variables. As a result, more features are extracted from the above process than in ziggurat.

Computation costs. A major challenge in effectively simulating the attack game is the time and resource costs for the adversary. Theoretically, for a vector space of $n = 60$, the total points may reach at least $\det(L_{n=60}) = q^{60}$ according to the Gaussian heuristic. We assume the samples obtained for tests accurately match the probability density function curve, so that a standard sample set can be available in the learning oracle according to Theorem 1. Even if the scale of samples is small, the learning system will work, as long as the model parameters stably demonstrate their boundaries. We evaluate the time and memory costs from the angles of sampling algorithms and learning systems, respectively, as shown in Figs. 1–4.
The performance of learning systems varies significantly in achieving a stable state. Figure 1 shows that SVM and LR converge much faster than CNN with the same amount of ciphertext samples, while CNN demonstrates the best converging stability. Despite the natural character of learning systems, such as learning on batch strategy and local optimization strategy, CNN consumes more time and samples to reach the same training level. However, better accuracy is achieved when CNN is used to process more samples. Thus, a higher advantage will be achieved when more powerful resources are offered for the CNN-based learning oracle.

Compared with the variance of $\theta$ coordinating with sampling algorithms in Fig. 2, all the subjects show a significant consistency in achieving optimized stable boundaries. Only the Box-Muller sampling needs more time and queries to reach the same optimization level.

As we expected, the dynamic memory cost of the adversary caused by the learning oracles varies significantly, as shown in Fig. 3, especially for the CNN-based learning oracle. The main reason for this situation is its small-batch learning strategy, which guarantees an accumulation of abstracted characters in high dimension. Also, the dynamic memory cost increases sharply as more queries are added in the oracle. The dynamic storage cost may be less important in the attack, but its scale partially decides the time efficiency of data processing for the adversary. From the result in Fig. 4, the increase rate of the dynamic storage cost is approximately linear to the query processing. However, the CNN model contains a multiple-layer matrix to express the characters of previous samples, thus reserving more storage for the matrix, and dynamic storage cost increases steadily as the matrix transforms from a sparse one to a normal one in the learning procedure.

**Parameter tune.** Assuming that each round of the IND game is statistically independent, the final advantage of a learning oracle is decided by several factors, including sampling algorithms, learning systems, and initial parameters. With fixed parameters of $k$ and $n$, we evaluated the influences of the first two factors. In this part, we explore the optimized advantage of the adversary by searching and tuning the space of $k$ and $n$. The optimized results are demonstrated in Table 4. The best advantage in Table 4 basically reflects the performance of each parameter combination of learning oracle in the IND game. CLT sampling evidently has the maximum advantage for the attacker, followed by the Box-Muller algorithm. The sampling algorithms partially leak a large amount of discriminative information of the ciphertexts, which verifies the assumption at the beginning of this paper. Also, the results in Table 4 indicate that the performance of different learning systems varies tremendously, especially for the case of CNN, which shows an advantage in processing large-scale samples. Given the
outstanding performance of CNN, the costs of memory, storage, and CPU clocks are much higher.

5 Conclusion and Future Work

Cryptosystem based on LWE is widely accepted as an important post-quantum primitive with a concrete security foundation in ideal instances. But the randomness and security of ciphertexts and mid-variables in the cryptosystem largely depend on the sampling algorithms to offer trapdoor vectors that are indistinguishable from true random noise. We perform a tactic security evaluation to detect the influences caused by sampling. The evaluation is mainly an experimental simulation of the semantic attack game that appeared in previous coordinate LWE cryptosystems. In the instance of our attack game, a distinguishing oracle based on automatic learning system is first applied to automatically perform global learning toward the queried samples. A major advantage is the potential leakage extracted and detected by the learning system without the need to construct a complex analysis model. Also, the attack routine is universal in analyzing noise-bounded encryption schemes and solving bounded code problems as long as enough samples are available.

Given that the analysis of a sematic attack model is conventionally performed in semantic theory frameworks, our experimental analysis is the first attempt to apply machine learning theory. Hence, the theoretical foundation is not sufficiently concrete. Meanwhile, the details of the oracle construction are uncontrollable during the learning phase. In future work, we will focus on these two problems and strengthen the theoretical support for our attack framework. We foresee a new perspective trend in cryptographic analysis based on artificial intelligence and other interactive evolving models. Thus, our automatic analysis of LWE-based cryptosystem is a useful and meaningful attempt in the field.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 61572521 and U1636114), the National Key Project of Research and Development Plan (No. 2017YFB0802000), the Innovative Research Team Project of Engineering University of PAP (No. KYTD201805), and the Fundamental Research Project of Engineering University of PAP (No. WJY201910).

References

[1] NIST CSRC of Information Technology Laboratory. Post-quantum cryptography round 2 submissions, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions, 2019.
[2] J. H. Liu, Y. Yu, J. W. Jia, S. J. Wang, P. R. Fan, H. Z. Wang, and H. G. Zhang. Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks. Tsinghua Science and Technology, vol. 24, no. 5, pp. 575–584, 2019
[3] J. H. Cheon, K. Han, J. Kim, C. Lee, and Y. Son. A practical post-quantum public-key cryptosystem based on spLWE, in Proc. 19th Int. Conf. Information Security and Cryptology, Seoul, Korea, 2016, pp. 51–74.
[4] D. Dachman-Soled, H. J. Gong, M. Kulkarni, and A. Shahverdi, On the leakage resilience of ideal-lattice based public key encryption, IACR Cryptology ePrint Archive, Report 2017/1127, 2017.
[5] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, Journal of the ACM, vol. 56, no. 6, p. 34, 2009.
[6] O. Regev, The learning with errors problem (invited survey), in Proc. 2010 IEEE 25th Annul. Conf. Computational Complexity, Cambridge, MA, USA, 2010, pp. 191–204.
[7] D. D. Zhang, J. Li, B. Li, X. H. Lu, H. Y. Xue, D. D. Jia, and Y. M. Liu, Deterministic identity-based encryption from lattice-based programmable hash functions with high min-entropy, Cryptology ePrint Archive, Report 2019/051, 2019.
[8] J. Zhang, Y. Yu, S. Q. Fan, and Z. F. Zhang. Improved lattice-based CCA2-secure PKE in the standard model, Cryptology ePrint Archive, Report 2019/149, 2019.
[9] M. Tang, M. X. Luo, J. F. Zhou, Z. Yang, Z. P. Guo, F. Yan, and L. Liu, Side-channel attacks in a real scenario, Tsinghua Science and Technology, vol. 23, no. 5, pp. 586–598, 2018.
[10] C. Sun, Z. S. Fei, D. Jia, C. Z. Cao, and X. Y. Wang. Secure transmission scheme for parallel relay channels based on polar coding, Tsinghua Science and Technology, vol. 23, no. 3, pp. 357–365, 2018.
Shuaishuai Zhu received the master’s degree in cryptography from Engineering University of People’s Armed Police in 2011. He is now a PhD candidate and assistant professor in Engineering University of People’s Armed Police. His main research interests include cryptanalysis and information security. Since 2014, he has been working on designing and analyzing of post-quantum cryptographic primitives, including lattice-based schemes LWE schemes and their applications in network secure protocols.

Yiliang Han received the PhD degree in computer science and technology from Xi’an Jiaotong University in 2013. He is a professor, PhD supervisor, and deputy dean in Engineering University of People’s Armed Police. His research work mainly includes cyberspace security, cryptography, and privacy protection. In recent five years, he has presided over two national nature foundation projects in post-quantum cryptography and three military theoretical projects in big data security protection.
Xiaoyuan Yang received the master’s degree in mathematics from Xidian University in 1984. He is a professor and PhD supervisor in Engineering University of People’s Armed Police, and the winner of national outstanding teacher award and military academy talent cultivation award. His main research interests include information security and cryptology. He has presided over 70 national and military research projects during his outstanding academic career, including National “863” Program. Currently, his work mainly focuses on full homomorphic encryption and other post-quantum algorithm developments.