# On SIS-problem-based random Feistel ciphers and its statistical evaluation of resistance against differential cryptanalysis

Yu Morishima, *Member, IEEE,* Masahiro Kaminaga, *Member, IEEE,*

***Abstract*—Provable security based on a robust mathematical framework is the gold standard for security evaluation in cryptography. Several provable secure cryptosystems have been studied for public key cryptography. However, provably secure symmetric-key cryptography has received little attention. Although there are known provably secure symmetric-key cryptosystems based on the hardness of factorization and discrete logarithm problems, they are not only slower than conventional block ciphers but can also be broken by quantum computers.**

**Our study aims to tackle this latter problem by proposing a new provably secure Feistel cipher using collision resistant hash functions based on a Short Integer Solution problem (SIS). Even if cipher primitives are resistant to quantum algorithms, it is crucial to determine whether the cipher is resilient to differential cryptanalysis, a fundamental and powerful attack against symmetric-key cryptosystems.**

**In this paper, we demonstrate that the proposed cipher family is secure against differential cryptanalysis by deriving an upper bound on the maximum differential probability. In addition, we demonstrate the potential success of differential cryptanalysis for short block sizes and statistically evaluate the average resistance of cipher instances based on differential characteristic probabilities. This method approximates the S-box output using a folded two-dimensional normal distribution and employs a generalized extreme value distribution. This evaluation method is first introduced in this paper and serves as the basis for studying the differential characteristics of lattice matrices and the number of secure rounds. This study is foundational research on differential cryptanalysis against block ciphers using a lattice matrix based on SIS.**

***Index Terms*—Feistel cipher, Short integer solution problem, Differential cryptanalysis.**

## I. Introduction

ADVANCES in quantum computing technology have raised concerns about the security of conventional cryptographic systems, and research on cryptography resistant to attacks using quantum computing, that is, post-quantum cryptography, is actively being conducted. The increasing significance of cryptographic systems with mathematically provable security is a response to progress made in quantum computing. Such security, called provable security, is an essential property in the design of modern cryptography, as it ensures that security against specific attacks can be guaranteed through mathematical proofs. Although public key cryptography has been studied extensively as a provable secure cipher, symmetric-key cryptography has received little attention. Since there are provable secure constructions of symmetric-key cryptography that rely on the computational hardness of problems such as RSA and discrete logarithms, these systems suffer from slower processing speeds than conventional block ciphers. Furthermore, they are susceptible to being broken by quantum computers. To address the latter issue, our aim is to explore the construction of symmetric-key cryptography with provable security in the post-quantum era.

Yu Morishima and Masahiro Kaminaga are with Tohoku Gakuin University, Japan. e-mail: morishima@mail.tohoku-gakuin.ac.jp

Cryptographic systems with provable security are based on the computational hardness of mathematical problems. Lattice cryptography, which relies on hard lattice problems, is considered to be a candidate for post-quantum cryptography. Lattice cryptography began with Ajtai's seminal paper [1], and the use of hard problems on lattices makes it possible to solve hard problems in the worst case. He showed that it is possible to construct a one-way function with average computational hardness from hard problems. Micciancio extended these results to develop a hash function that exhibits collision resistance [2].

Learning with Errors (LWE) and Short Integer Solution problem (SIS) are known as the main lattice problems that form the basis of lattice cryptography. LWE and SIS have a duality [3]. If the solution vector in the SIS is identified with the error vector in the LWE, the two are reduced to the Closest Vector Problems (CVP) of the same class [4]. SIS is used for hash function construction [5] and digital signatures [6], and LWE is used for public key and homomorphic encryption [7] [8]. A configuration using LWE has been cited as an example for applying the lattice problem to symmetric-key cryptography, and many configurations using LWE have been considered in the existing research. On the other hand, studies on SIS have received little attention. However, SIS does not require precise design of the error distribution in LWE and is simple to implement, making it suitable for theoretical analysis.

Pseudorandom functions are regarded as effective tools for the design of symmetric-key cryptosystems. The Goldreich-Goldwasser-Micali (GGM) method [9] and the synthesizer technique [10] are both established methods for constructing provably secure ciphers through pseudorandom functions. Although the GGM is a theoretically useful method, its higher circuit complexity makes it less desirable. This is because the number of computations required for GGM increases proportionally with the input length. This is because the GGM has a length-doubling property. By contrast, the synthesizer enables more efficient parallel processing. A variant of the

synthesizer that incorporates the LWE through Learning with Rounding (LWR) as a primitive has been proposed [11], which, despite its benefits, faces challenges related to the synchronous execution of parallel processes and increased communication overhead. As an extension of this research, a further refined version of the synthesizer has been proposed [12], which enhances efficiency but requires substantially larger key sizes. While these are essential theoretical results, constructing symmetric-key cryptosystems based on SIS without these trivial constructions remains an open problem.

This paper proposes a new Feistel cipher using a hash function family based on SIS as S-boxes (lattice-based Feistel cipher, LBF for short), and evaluates its security against differential cryptanalysis. By evaluating the maximum differential probability of the round function, we show that the proposed cipher provides provable security against differential cryptanalysis. Even in instances where provable security is established, assessing the typical security of specific instances of LBF for practical applications remains imperative. Typical security, which refers to the security expected on average, of LBF instances is demonstrated through comprehensive numerical simulations replicating real-world scenarios. We use an approximate model of the S-box in our analysis and simulation to verify the security against differential cryptanalysis from theoretical and practical perspectives.

The remainder of this paper is organized as follows. Section 2 describes the definition of hard lattice problems, collision resistant hash function, differential cryptanalysis for Feistel ciphers and block ciphers, and the trinity theorem in extreme value statistics, which are necessary to describe the results. Section 3 describes the configuration of the LBF. In Section 4, we present the main result (Theorem 4) of this study, and the upper bound of the output differential of the LBF family decays exponentially with the block size under appropriate conditions. Section 5 provides an example of applying differential cryptanalysis to LBF instances with small block sizes. Furthermore, we perform a Monte Carlo simulation to evaluate the average property of the LBF family against differential cryptanalysis. In this simulation, we approximate the S-box output difference using a folded two-dimensional normal distribution, use a generalized extreme value distribution to verify practical security, calculate the LBF block size, and clarify the relationship between the number of rounds.

## II. Preliminaries

### A. Lattice Problems

A lattice is a set of all integer linear combinations of $n$ linearly independent column vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$. The lattice $\mathcal{L}(\mathbf{B})$ generated by these vectors can be represented by matrix $\mathbf{B} = \begin{pmatrix} \boldsymbol{b}_1 & \boldsymbol{b}_2 & \cdots & \boldsymbol{b}_n \end{pmatrix}$ as follows:

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{B}\boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{Z}^n\}, \tag{1}$$

where $\boldsymbol{x}$ denotes a column vector. In the following, vectors are assumed to be column vectors, and $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ denotes the integers modulo $q$. The successive minima of the lattice are defined as follows.

**Definition 1.** (Successive Minima) The successive minima $\lambda_1, \ldots, \lambda_n$ of the rank $n$ lattice $\mathcal{L}$ are defined as follows: The $i$-th minimum $\lambda_i(\mathcal{L})$ is

$$\lambda_i(\mathcal{L}) = \inf\{r \mid \dim(\mathrm{span}(\mathcal{L} \cap B(r))) \geq i\}. \tag{2}$$

Here, we denote the closed ball of centered at the origin and radius $r$ as $B(r)$.

Lattice problems can be used in cryptography to discuss computational hardness and security. For example, the Closest Vector Problem (CVP), which finds a vector in $\mathcal{L}(\mathbf{B})$ closest to a given target vector $\boldsymbol{t} \notin \mathcal{L}(\mathbf{B})$, and the Shortest Vector Problem (SVP), which finds the shortest nonzero vector in $\mathcal{L}(\mathbf{B})$. The Shortest Independent Vectors Problem (SIVP) is another example of a lattice problem, with its computational hardness stemming from the difficulty of identifying a set of linearly independent vectors.

The lattice problems serve as the foundation for constructing strong ciphers. By using the technique of reducing worst case to average case hardness, we can build a cipher that exhibits strong resistance to attacks on average. SIS and LWE are exemplary problems that demonstrate such average resilience. The following provides a formal description of lattice problems relevant to this paper.

**Definition 2.** (SIS) Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a real number $\beta \geq 1$, find a nonzero integer vector $\boldsymbol{x} \in \mathbb{Z}^m$ such that $\mathbf{A}\boldsymbol{x} = \mathbf{0} \in \mathbb{Z}_q^n$ and $\|x\| \leq \beta$.

**Definition 3.** (SVP) Given a lattice $\mathcal{L}(\mathbf{A})$, find the shortest nonzero vector $\boldsymbol{v}$ in $\mathcal{L}(\mathbf{A})$. The parameter $\gamma$ in the "$\gamma$-approximate SVP"(SVP$_\gamma$ for short) refers to the approximation factor, where the algorithm finds a vector $\boldsymbol{v}$ such that $\|\boldsymbol{v}\| \leq \gamma\lambda_1$, where $\lambda_1$ is the norm of the shortest nonzero vector in $\mathcal{L}(\mathbf{A})$.

$\gamma$ in SVP$_\gamma$ is a function of rank $n$ of the lattice matrix. $\gamma = \sqrt{n}$ is called the Minkowski's bound, and SVP is known to have a nonzero solution. The LLL lattice reduction algorithm [13] can solve SVP$_\gamma$ where $\gamma = 2^{(n-1)/4}$ in polynomial time. If there is no algorithm to solve the SVP in probabilistic polynomial time, the SIS cannot be solved in probabilistic polynomial time either [1].

**Definition 4.** (GapSVP$_\gamma$) Given an $n$-dimensional lattice basis $\mathbf{B}$ and $d$ is a rational number, determine whether $\lambda_1(\mathcal{L}) \leq d$ or $\lambda_1(\mathcal{L}) > \gamma(n)d$. If neither condition is satisfied, then any output is acceptable.

**Definition 5.** (SIVP$_\gamma$) Given a lattice $\mathcal{L}$ of rank $n$, find $n$ linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ such that $\max_i \|\boldsymbol{v}_i\| \leq \gamma\lambda_n(\mathcal{L})$.

### B. Collision Resistant Hash Function Family

Ajtai proposed a hash function family based on a computationally hard problem on a random lattice.

**Definition 6.** (Ajtai's hash function family [1]) For $m > n\log_2 q$, Ajtai's hash function family $f$ is defined as

$$f(\boldsymbol{x}) = \mathbf{A}\boldsymbol{x} \bmod q, \tag{3}$$

where $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is uniformly selected at random and $\boldsymbol{x} \in \{0,1\}^m$.

This function has the parameters $n, m, q \in \mathbb{Z}^+$, where $m$ and $q$ are defined as functions of $n$. By considering the appropriate parameters and lattice problems, we can evaluate the computational hardness of this hash function. Ajtai demonstrated that this function can be a one-way hash function. These results indicate that the various computational hardness aspects of this function can be reduced to the average computational hardness of SIS. The average case hardness in lattice problems refers to the difficulty in solving these problems when the input is randomly sampled. The worst case hardness addresses the difficulty of solving the most challenging instances of lattice problems. There are many results regarding the selection of parameters and problems. The worst case hardness can be reduced within factor $\mathcal{O}(\beta\sqrt{n})$ to the average hardness of the SIS with $\beta$ for $q \leq \beta\omega(\sqrt{n \log n})$ [14], [15], where $h(n) = \omega(g(n))$ implies that for any constant $c > 0$, $h(n)$ will eventually exceed $c \cdot g(n)$ as $n$ increases.

Micciancio demonstrated that taking advantage of the computational hardness of SIS makes it possible to construct a family of collision resistant hash functions.

**Theorem 1.** (Collision reistant hash function family [2]) For any sufficiently large polynomial $q$, if there exists no polynomial time algorithm for solving SIVP$_\gamma$ with $\gamma = \mathcal{O}(n)$, which is almost linear in the rank of the lattice, then the hash function family defined in (3) is collision resistant.

Here, a large polynomial can be, for instance, chosen as $n^3$ or $2^n$. For more detailed discussion, please refer to [16]. It is well known that the collision resistance can also be derived using GapSVP$_\gamma$ instead of SIVP$_\gamma$.

The worst case computational hardness of SIVP$_\gamma$ with $\gamma = \mathcal{O}(n)$ is reduced to SIS average computational hardness with $q = \Omega(n^2)$, $\beta = \mathcal{O}(\sqrt{m})$, $m \approx n \log q$ where $h(n) = \Omega(g(n))$ if there are constants $c > 0$ and $n_0$ such that $0 \leq c \cdot g(n) \leq h(n)$ for all $n \geq n_0$. This indicates that $g(n)$ is a lower bound on $h(n)$.

The fact that $f(\boldsymbol{x})$ is a collision resistant hash function implies that the probability $p(m)$ for finding a pair $\boldsymbol{x}, \boldsymbol{x}'(\boldsymbol{x} \neq \boldsymbol{x}')$ such that $\mathbf{A}\boldsymbol{x} = \mathbf{A}\boldsymbol{x}'$ can be proven to be negligible with respect to $m$ using a probabilistic polynomial time algorithm. In this context, negligible implies that $p(m)$ is satisfied $p(m) \leq 1/\text{poly}(m)$ for sufficiently large $m$ and any positive polynomial poly$(\cdot)$ To construct a concrete hash function, it is necessary to specify $q$, $m$, and $n$, and following reference [2], we choose $q = 2^n$ and $m = 2n^2$ as reasonable values.

### C. Feistel Cipher

A Feistel cipher is a global structure for building block ciphers, like DES [17]. First, the input data is divided into halves $\boldsymbol{L}_0$ and $\boldsymbol{R}_0$, and $\boldsymbol{L}_0$ is scrambled by $F$ which is a nonlinear function of the input half data and round key $\boldsymbol{K}_1$ and EXORed with $\boldsymbol{R}_0$. The ciphertext is generated by executing the same round operation $N$ times with round keys $\boldsymbol{K}_1, \boldsymbol{K}_2, \cdots, \boldsymbol{K}_N$(see Fig.1).

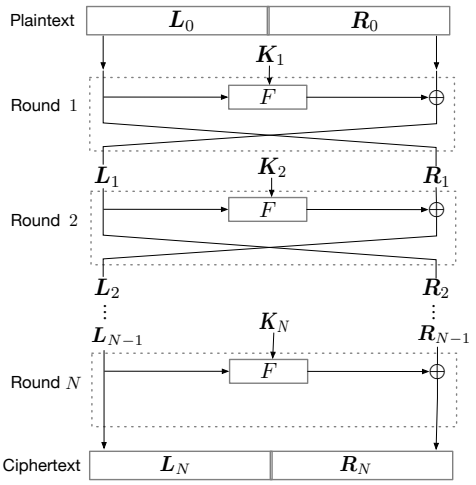


Fig. 1. Feistel cipher.

The $F$ function determines the strength of the Feistel cipher. Using the Luby-Rackoff construction with a pseudorandom function family, a class of block ciphers that is secure against chosen plaintext attacks and known plaintext attacks can be constructed. It is known that a family of pseudorandom functions can be constructed using a hash function with one-way property [18]. One-wayness and collision resistance are different concepts in computational complexity theory. However, the requirements for relaxed collision resistance are known to be harder than the one-wayness [19]. Therefore, a secure Feistel cipher can be constructed by using a collision resistant hash function.

### D. Differential Cryptanalysis

Differential cryptanalysis is a chosen plaintext attack, a practical attack method against block ciphers [20]. Differential cryptanalysis uses the input plaintext pair $\boldsymbol{X}, \boldsymbol{X}'$ and their difference $\Delta\boldsymbol{X} = \boldsymbol{X} \oplus \boldsymbol{X}' \neq \mathbf{0}$. When the attacker can control the pairs, the round key is extracted by observing the bias of the difference $\Delta\boldsymbol{Y} = \boldsymbol{Y} \oplus \boldsymbol{Y}'$ of the output pair $\boldsymbol{Y}, \boldsymbol{Y}'$.

The number of plaintext and ciphertext pairs required for a successful differential cryptanalysis attack is proportional to the reciprocal probability of $\Delta\boldsymbol{Y}$ for the input difference $\Delta\boldsymbol{X}$. Therefore, the higher the probability of $\Delta\boldsymbol{Y}$ is, the easier the attack will be successful, and the more uniformly distributed the probability of $\Delta\boldsymbol{Y}$, the more difficult the attack will be. In other words, the security of a block cipher against differential cryptanalysis is evaluated by the maximum value of the probability of $\Delta\boldsymbol{Y}$, and the plaintext input difference $\Delta\boldsymbol{X}$ in $N$ rounds. The maximum value $P_N$ of the probability of the ciphertext output difference $\Delta\boldsymbol{Y}$ is defined by

$$P_N = \max_{\Delta\boldsymbol{X} \neq \mathbf{0}, \Delta\boldsymbol{Y}} P(\Delta\boldsymbol{Y}|\Delta\boldsymbol{X}), \tag{4}$$

where $P(\Delta\boldsymbol{Y}|\Delta\boldsymbol{X})$ denotes the conditional probability of event $\Delta\boldsymbol{Y}$ occurring for a given $\Delta\boldsymbol{X}$. (4) is called the maximum differential probability.

### E. Extreme value distributions

Extreme value distributions describe the limiting distributions for the minimum or maximum independent random variables from the same distribution. $X_1, \ldots, X_n, \ldots$ be a sequence of independent and identically distributed random variables with a cumulative distribution function $F(x)$ and let $M_n = \max\{X_1, \ldots, X_n\}$ denote the maximum. The distribution of the maximum is given by $P(M_n \leq x) = P(X_1 \leq x) \cdots P(X_n \leq x) = F(x)^n$. We do not see the distribution of $M_n$ for an unknown $F$, but as $n \to \infty$, we can find its limit distribution. The limit cumulative distribution function $G(x)$ of the extreme distribution is described by the generalized extreme value (GEV) distribution [21]:

$$G(x) = \exp\left\{-\left[1+\xi\left(\frac{x-\mu}{\sigma}\right)\right]^{-\frac{1}{\xi}}\right\}, \tag{5}$$

defined on $\{x : 1+\xi(x-\mu)/\sigma > 0\}$, where $\mu \in \mathbb{R}$, $\sigma > 0$ and $\xi \in \mathbb{R}$. This distribution has three parameters: $\mu$ represents location, $\sigma$ scale, and $\xi$ shape. Among these, depending on the value of shape parameter $\xi$, it can be divided into the three distributions corresponding to Gumbel (Type I) at $\xi = 0$, Fréchet (Type II) at $\xi > 0$, and Weibull (Type III) at $\xi < 0$. An asymptotic result is obtained by following the extreme value trinity theorem.

**Theorem 2.** (The extreme value trinity theorem) There exist sequences of constants $a_n > 0$ and $b_n \in \mathbb{R}$ such that for $M_n^* = (M_n - b_n)/a_n$, $P(M_n^* \leq x) \to G(x)$ as $n \to \infty$.

We will represent the distribution of the maximum differential probability of the output of S-boxes in GEV.

## III. Lattice Based Feistel Cipher

A method using GGM [9] or a synthesizer [10] is known to construct a function family with pseudorandomness from a family of hash functions with one-wayness. However, these methods require processing delays due to circuit depth and repetitive processing in implementation; therefore, another approach is desirable. In this study, we propose a strategy based on Feistel construction. Since the Feistel cipher can always decrypt any $F$ function, it is possible to construct a block cipher using a family of hash functions that is as good as the $F$ function. This study presents the construction of a lattice-based Feistel cipher (LBF) using a family of hash functions as the $F$ function. Fig. 2 shows the structure of the LBF round function. After $m$-bits input, the plaintext $\boldsymbol{X}$ is divided into $m/2$-bits $\boldsymbol{L}_0$ and $\boldsymbol{R}_0$ and input to the first-round function. This process repeats $N$ rounds to generate the ciphertext $\boldsymbol{Y}$.

The $F$ function in the round function consists of an expansion permutation $E$, EXOR with the round key $\boldsymbol{K}_i$, and the S-box. The extended permutation $E$ concatenates the bit strings represented by $||$, which corresponds to the expansion permutation in DES [20]. Here, $E$ has a simple structure, and while it may appear overly simplistic compared to DES, there is no need to complicate $E$ because $\mathbf{A}$ is random in LBF.

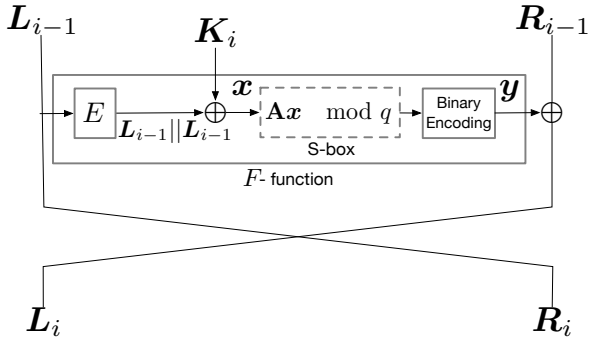


Fig. 2. Round function of LBF.

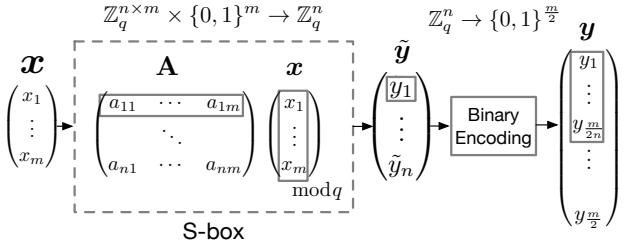


Fig. 3. S-box and binary encoding of LBF.

The hash function family $f(\boldsymbol{x})$ composed of (3), is used for the S-box (Fig. 3). For the input $\boldsymbol{x} \in \{0,1\}^m$ to the S-box, the output $\tilde{\boldsymbol{y}} \in \mathbb{Z}_q^n$ of $f(\boldsymbol{x})$, and by encoding $\tilde{y}_i \in \mathbb{Z}_q$ of $\tilde{\boldsymbol{y}}$ into a binary expression for each of $i = 1, 2, \ldots, n$ and concatenating it, the S-box output $\boldsymbol{y} \in \{0,1\}^{\frac{m}{2}}$ is obtained. The selection of round keys is arbitrary, as long as the period is long enough to assume that they are uniformly distributed.

While pseudorandom functions can be constructed from one-way functions, collision resistant functions are employed in the LBF. This is due to the fact that even one-way functions might lead to the leakage of round key information if a collision occurs. Consider when a pair of inputs to an S-box, $\boldsymbol{x}$ and $\boldsymbol{x}'$ (where $\boldsymbol{x} \neq \boldsymbol{x}'$), results in $\mathbf{A}\boldsymbol{x} = \mathbf{A}\boldsymbol{x}'$. Let the input to the round function be $\boldsymbol{L} = \boldsymbol{L}_j||\boldsymbol{L}_j$ and let the input pair of $\boldsymbol{L}$ be $\boldsymbol{L}'$. In this case, for the $i$-th bit of the vectors $\boldsymbol{z}$ and $\boldsymbol{w}$, the EXOR operation satisfies $z_i \oplus w_i = z_i + w_i - z_i w_i$. Here, we obtain the followings for the input pair $\boldsymbol{x}$ and $\boldsymbol{x}'$,

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{K} \oplus \boldsymbol{L} && (6)\\ \boldsymbol{x}' &= \boldsymbol{K} \oplus \boldsymbol{L}' && (7)\\ \mathbf{A}(\boldsymbol{x} - \boldsymbol{x}') &= \mathbf{0}. && (8) \end{aligned}$$

Thus, for the $i$-th bit of $\boldsymbol{x} - \boldsymbol{x}'$, we derive

$$\begin{aligned} x_i - x_i' &= k_i \oplus L_i - k_i \oplus L_i' && (9)\\ &= (L_i - L_i')(1 - k_i) = 0. && (10) \end{aligned}$$

If $L_i - L_i' \neq 0$, we can determine $k_i = 1$. Therefore, a secure Feistel cipher can be constructed by using a collision resistant hash function.

When the hash function family used in the S-box is collision resistant, the probability of finding a pair of inputs such that $\mathbf{A}\boldsymbol{x} = \mathbf{A}\boldsymbol{x}'$ is negligible. With the LBF constructed in this manner, the hash function that is difficult to inverse

is used as a large S-box, which makes it difficult to apply differential cryptanalysis. Moreover, this design allows flexible construction of ciphers with different block sizes in a single structure.

## IV. Differential Cryptanalysis of LBF

In this section, we evaluate the security of LBF against differential cryptanalysis. In block ciphers with a Feistel structure, the maximum differential probability indicates the security of the entire system, even if the number of rounds is two or more. We can find the maximum differential probability by brute-force search if the number of rounds or block size is small. However, an brute-force search is unrealistic due to the large block size and many rounds used in practical systems, thus we require an theoretical study of the maximum differential probability; the following Theorem 3 shown in [22] is the basis for the theoretical estimation of differential probabilities.

**Theorem 3.** In Feistel cipher, when the round keys are uniformly and independently selected, an upper bound of the maximum differential probability $P_N$ when $N \geq 4$ is given by the following using the maximum differential probability $P_{\max}$ of one round:

$$P_N \leq 2P_{\max}^2. \tag{11}$$

(11) means that the security against differential cryptanalysis can be evaluated using the maximum differential probability of the round function.

Below, we evaluate the maximum differential probability $P_{\max}$ of the round function of the LBF. Regarding the input $\boldsymbol{X} \in \{0,1\}^m$ and output $\boldsymbol{Y} \in \{0,1\}^m$ of a round function, if $\boldsymbol{X} = \boldsymbol{X}_L || \boldsymbol{X}_R$ and $\boldsymbol{Y} = \boldsymbol{Y}_L || \boldsymbol{Y}_R$ are blocks divided into $m/2$-bits, the following holds between the input difference $\Delta\boldsymbol{X}$ and the output difference $\Delta\boldsymbol{Y}$ of the round function:

$$\begin{aligned} \Delta\boldsymbol{Y} &= \Delta\boldsymbol{Y}_L || \Delta\boldsymbol{Y}_R \\ &= \Delta\boldsymbol{y} \oplus \Delta\boldsymbol{X}_R || \Delta\boldsymbol{X}_L, \end{aligned} \tag{12}$$

where $\Delta\boldsymbol{y} \in \{0,1\}^{\frac{m}{2}}$ is the output difference of the S-box (see Fig.3). Since $\Delta\boldsymbol{Y}_R = \Delta\boldsymbol{X}_L$ and the attacker can control the input difference, maximizing the probability of $\Delta\boldsymbol{Y}_L$ maximizes the probability of $\Delta\boldsymbol{Y}$. Note that since the maximum probability of $\Delta\boldsymbol{Y}_L$ is independent of $\Delta\boldsymbol{X}_R$, the maximum probability of $\Delta\boldsymbol{Y}_L$ is determined by $\Delta\boldsymbol{y}$. If the round key $\boldsymbol{K}_i \in \{0,1\}^m$ can be regarded as a uniform random, the S-box input $\boldsymbol{x}$ can also be regarded as a uniform one. Therefore, the maximum probability of $\Delta\boldsymbol{Y}_L$ is determined by the input difference $\Delta\boldsymbol{x}$ of the S-box and output difference $\Delta\boldsymbol{y}$ of the S-box. Furthermore, if the binary encoding of the S-box output $\tilde{\boldsymbol{y}}$ is a bijection, that is, the parameter is chosen such that $m = 2n\log_2 q$ holds, then $\boldsymbol{y}$ and $\tilde{\boldsymbol{y}}$ correspond one-to-one. In this case, $P_{\max}$ can be represented using the maximum differential probability of the S-box as follows:

$$P_{\max} = \max_{\Delta\boldsymbol{x}\neq\boldsymbol{0},\Delta\boldsymbol{y}} P(\Delta\boldsymbol{y}|\Delta\boldsymbol{x},\mathbf{A}), \tag{13}$$

where $P(\Delta\boldsymbol{y}|\Delta\boldsymbol{x},\mathbf{A})$ denotes the conditional probability of event $\Delta\boldsymbol{y}$ occurring for given $\Delta\boldsymbol{x}$ and $\mathbf{A}$.

In the following, the maximum differential probability of the S-box output of the LBF is theoretically derived. It is well known that the sum of uniformly distributed variables tends to a normal distribution. However, an exact distribution of the sum of discrete uniform distributions, when folded by modulo-$q$, cannot be directly derived. First, we present the following lemma for the uniform random variable used to construct the hash function to derive the S-box output difference distribution.

**Lemma 1.** Let $a_i$ for $i = 1, 2, \ldots, n$ be independent and identically distributed random variables that obey a discrete uniform distribution over $\mathbb{Z}_q$. Then, the value of $s_q$, as defined by the following, obeys a discrete uniform distribution over $\mathbb{Z}_q^n$.

$$s_q = \sum_{i=1}^{n} a_i \bmod q. \tag{14}$$

*Proof.* Consider $n$-tuple $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)$ of independent uniform random variables $a_l \in \mathbb{Z}_q (l = 1, 2, \cdots, n)$. Since $\boldsymbol{a}$ is uniformly distributed over $\mathbb{Z}_q$, to find $P(s_q = k)$, it is sufficient to find the number of $\boldsymbol{a}$ such that

$$s := \sum_{l=1}^{n} a_l = k + iq, \tag{15}$$

where $i = 0, 1, \cdots, \lfloor \frac{n(q-1)-k}{i} \rfloor$. Therefore we have

$$\sum_{l=1}^{n-1} a_l = k + iq - a_n. \tag{16}$$

The left-hand side of (16) takes the value of $\{0, 1, \cdots, (n-1)(q-1)\}$, and the value of $a_n$ is uniquely determined for $(n-1)$-tuple $(a_1, a_2, \cdots, a_{n-1})$, which (16) holds.

Subsequently, $\boldsymbol{a}$ for which (16) holds exists as $q^{n-1}$ for given $k$, $q$, so that $P(s_q = k) = \frac{q^{n-1}}{q^n} = \frac{1}{q}$. □

Lemma 1 leads to the following theorem regarding the distribution of the S-box output pairs.

**Theorem 4.** For a given $\Delta\boldsymbol{x} \in \{0,1\}^m$, let the input pairs be $\boldsymbol{x}$, $\boldsymbol{x}' \in \{0,1\}^m$, and let the output pairs of the S-box be, $\boldsymbol{y}$, $\boldsymbol{y}' \in \{0,1\}^{\frac{m}{2}}$. If $\mathbf{A}$ obeys a discrete uniform distribution over $\mathbb{Z}_q^{n\times m}$ and $m$ is equal to $n\log_2 q$, then the probability that the output pair $\boldsymbol{y}$, $\boldsymbol{y}'$ is obtained from a given $\Delta\boldsymbol{x}$ obeys a uniform distribution over $\{0,1\}^{\frac{m}{2}} \times \{0,1\}^{\frac{m}{2}}$.

*Proof.* For a given input pair $(\boldsymbol{x}, \boldsymbol{x}') \in \{0,1\}^m \times \{0,1\}^m$, let $\Delta\boldsymbol{x} = \boldsymbol{x} \oplus \boldsymbol{x}' \in \{0,1\}^m$. Letting the $i$-th row of the row vector $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n$ of $\mathbf{A}$ be $\boldsymbol{a}_i = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{im} \end{pmatrix}$, the output pair $(\tilde{y}_i, \tilde{y}_i') \in \mathbb{Z}_q \times \mathbb{Z}_q$ of $f(\boldsymbol{x})$ corresponding to $\boldsymbol{a}_i$ can be represented as follows:

$$\tilde{y}_i = \boldsymbol{a}_i\boldsymbol{x} \bmod q \tag{17}$$

$$\tilde{y}_i' = \boldsymbol{a}_i(\boldsymbol{x} \oplus \Delta\boldsymbol{x}) \bmod q. \tag{18}$$

Here, the $k$-th bit of $\Delta\boldsymbol{x}$ is represented as $\Delta x_k$ and the set of indices where the bit is 0 or 1 is defined as follows:

$$\Delta\mathbb{I}_0 = \{k \mid \Delta x_k = 0 \ (k = 1, 2, \cdots, m)\} \tag{19}$$

$$\Delta\mathbb{I}_1 = \{k \mid \Delta x_k = 1 \ (k = 1, 2, \cdots, m)\}. \tag{20}$$

Using the set of indices $\Delta\mathbb{I}_0$, $\Delta\mathbb{I}_1$ and the $k$-th bit $x_k$ of $\boldsymbol{x}$, $\tilde{y}_i$ and $\tilde{y}'_i$ can be represented as follows:

$$\tilde{y}_i = \sum_{k\in\Delta\mathbb{I}_0} a_{ik}x_k + \sum_{k\in\Delta\mathbb{I}_1} a_{ik}x_k \mod q \quad (21)$$

$$\tilde{y}'_i = \sum_{k\in\Delta\mathbb{I}_0} a_{ik}x_k + \sum_{k\in\Delta\mathbb{I}_1} a_{ik}(x_k \oplus 1) \mod q. \quad (22)$$

Since the elements of $\boldsymbol{a}_i$ are random variables that obey the uniform distribution over $\mathbb{Z}_q$, the first terms of (21) and (22) can be represented as random variables $u$ that obey a discrete uniform distribution over $\mathbb{Z}_q$ from Lemma 1. Also, the second term in (21) is the sum of $a_{ik}$ for $k$ such that $x_k = 1$, and the second term of (22) is the sum of $a_{ik}$ for $k$ such that $x_k = 0$, and since $a_{ik}$ in (1) and (2) do not overlap, their sums are mutually independent.

From Lemma 1, each sum is an independent random variable $v$, $w$ that obey uniform distribution over $\mathbb{Z}_q$. $\tilde{y}_i$, $\tilde{y}'_i$ can be represented in the following form using independent random variables $u$, $v$, and $w$ that obey discrete uniform distribution over $\mathbb{Z}_q$ as follows:

$$\tilde{y}_i = u + v \mod q \quad (23)$$

$$\tilde{y}'_i = u + w \mod q. \quad (24)$$

Since $v$, $w$, and $u$ are independent, $\tilde{y}_i, \tilde{y}'_i$ are independent and uniformly distributed random variables over $\mathbb{Z}_q$.

As each row of the matrix $\mathbf{A}$ is independent, each row of the outputs $\tilde{\boldsymbol{y}}$ and $\tilde{\boldsymbol{y}}'$ of the S-box are also independent. Therefore, the random variables $(\tilde{\boldsymbol{y}}, \tilde{\boldsymbol{y}}')$ obey uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q^n$. Considering that the binary encoding $\mathbb{Z}_q^n \times \mathbb{Z}_q^n \to \{0,1\}^{\frac{m}{2}} \times \{0,1\}^{\frac{m}{2}}$ is a bijection for $m = n\log_2 q$, the S-box output pair $(\tilde{\boldsymbol{y}}, \tilde{\boldsymbol{y}}')$ is also a random variable that obeys a uniform distribution over $\{0,1\}^{\frac{m}{2}} \times \{0,1\}^{\frac{m}{2}}$. □

Therefore, if the binary encoding of the LBF is a bijection, the difference of output $\Delta\boldsymbol{y} = \boldsymbol{y} \oplus \boldsymbol{y}'$ obeys the uniform distribution over $\{0,1\}^{\frac{m}{2}}$, then $P_{\max} = 1/2^{\frac{m}{2}}$.

This result and Theorem 5 lead to the estimate of $N$ round maximum differential probability $P_N$ given by

$$P_N \le 2P_{\max}^2 = \frac{1}{2^{m-1}}. \quad (25)$$

This result shows that since the lower bound of the maximum differential probability is $1/2^m$, $P_N$ is at most twice the lower bound.

## V. Statistical analysis of differential cryptanalysis on LBF instances

In the evaluation of cryptography, it is important to analyze a family of functions, but it is also necessary to examine specific instances for practical applications. In this study, we evaluate the typical security of LBF instances against differential cryptanalysis, where typical security refers to the security expected on average when focusing on individual instances in the family. We examine the specific instances and analyze the average properties within the LBF family. In addition, we use extreme value theory by GEV for the approximate model of the S-box to theoretically estimate the maximum differential characteristic probability and the practically secure number of rounds.

### A. Differential cryptanalysis works well against LBF with small block sizes

The LBF family uses secure primitives with a collision resistance. However, even secure primitives in block ciphers can be vulnerable to differential cryptanalysis. Therefore, it is essential to evaluate their security. We conducted simulations to examine whether LBF is vulnerable to attacks by differential cryptanalysis, focusing on cases with short block sizes. First, to eliminate the uncertainty caused by the random selection and examine the characteristics, we perform a computer simulation of differential cryptanalysis for the block size for which the candidate keys can be brute-force searched. When differential cryptanalysis is attempted on a Feistel cipher, the input difference $\Delta\boldsymbol{X}$ of the plaintexts is controlled, and the round key is estimated based on the output difference $\Delta\boldsymbol{Y}$ of the ciphertexts. For example, if the number of rounds is $N = 1$, the key can be obtained by the following procedure [23].

1) For the selected $\Delta\boldsymbol{X}$, select a pair of plaintext input pairs $\boldsymbol{X}, \boldsymbol{X}' = \boldsymbol{X} \oplus \Delta\boldsymbol{X}$ and find $\Delta\boldsymbol{Y}$.
2) Select a pair of input pairs $\boldsymbol{x}, \boldsymbol{x}'$ to the S-box such that input difference of the plaintext is $\Delta\boldsymbol{X}$, and determine $\Delta\boldsymbol{Y}$.
3) For the pairs $\boldsymbol{X}, \boldsymbol{X}', \Delta\boldsymbol{Y}$ obtained in 1) and the pairs $\boldsymbol{x}, \boldsymbol{x}', \Delta\boldsymbol{Y}$ obtained in 2), where $\Delta\boldsymbol{Y}$ is identical, the candidate key $\hat{\boldsymbol{K}}_1$ is derived from the relations $\boldsymbol{x} = \boldsymbol{L}_0 \parallel \boldsymbol{L}_0 \oplus \boldsymbol{K}_1$ and $\boldsymbol{X} = \boldsymbol{L}_0 \parallel \boldsymbol{R}_0$, and add it to the list of candidate keys.

The above procedure is repeated for multiple $\Delta\boldsymbol{X}$ to narrow down the keys. If the candidate keys can be searched for every $\boldsymbol{X}$and $\boldsymbol{x}$, the candidate keys can be narrowed down by taking the intersection of the candidate keys for each $\Delta\boldsymbol{X}$. If the number of rounds is $N = 3$, the candidate keys can be estimated using the same procedure by modifying the relation between the input and output differences to be used. If the input block size $m$ is large, searching for all the candidates becomes difficult. Therefore, modifying the candidate keys to estimate them from several randomly selected input pairs is necessary.

In the simulation, one instance on $\mathbb{Z}_q^{n\times m}$ that is a full rank matrix is chosen at random as $\mathbf{A}$ of the S-box, and a round key is searched for an instance of LBF for the selected $\mathbf{A}$ according to the differential cryptanalysis procedure described above. For the LBF with parameters $(n, m, q) = (2, 8, 4)$ and $(4, 32, 16)$, we searched for candidate keys by differential cryptanalysis and found that the correct round key can be identified in a few hours in both cases where the number of rounds $N = 1$ and 3.

Table I shows the results of how the number of key candidates decreases for each instance of randomly generated $\mathbf{A}$ with $m = 32$ and $N = 3$ as the number of input differences increases from 1 to 3. The table shows the minimum, maximum, mean, and median number of key candidates for 100 instances. With only one difference, approximately one million possible keys can be found. However, with two differences, the number of possible keys decreases significantly to around

TABLE I
STATISTICAL RESULTS OF THE NUMBER OF KEY CANDIDATES PER NUMBER OF DIFFERENCE USED.

| # of difference | Minimum | Maximum | Mean | Median |
|---|---|---|---|---|
| 1 | 587880 | 8388608 | 1203716.30 | 1051008 |
| 2 | 126 | 4132 | 397.61 | 274 |
| 3 | 1 | 5 | 1.33 | 1 |

TABLE II
LINEAR REGRESSION PARAMETERS FOR $y = c + dx$ REGARDING THE REDUCTION IN KEY CANDIDATES FOR THE NUMBER OF INPUT DIFFERENCES.

| Coefficient | Estimate | Std. Error | $t$-value | $Pr(>\|t\|)$ |
|---|---|---|---|---|
| $c$ | 29.35747 | 0.16927 | 173.4 | $<$ 2e-16 |
| $d$ | -9.89946 | 0.07836 | -126.3 | $<$ 2e-16 |

a few hundred. With three differences, most instances are able to identify the correct key.

The results are shown in Table II, where we performed a linear regression $y = c + dx$ on the base-2 logarithm of the number of key candidates in the simulation. In the estimation, the $R^2$ value is 0.9817, indicating a good fit of the regression equation to the results. With each additional difference, the number of candidates decreases to approximately $1/2^d \approx 1/1000$, corresponding to 9.9-bits.

These results show that when the block size $m$ and the number of rounds $N$ are small, the round key of the LBF can be identified using only a few input and output difference pairs by using differential analysis. As observed here, differential cryptanalysis is practical when the block size and number of rounds are small. Therefore, it is necessary to determine block sizes and the number of rounds that differential cryptanalysis cannot solve.

### B. Number of secure rounds

It is crucial to select a sufficiently large block size and number of rounds when designing block ciphers to ensure the required level of security. In this study, we analyze differential characteristics for randomly selected instances of $\mathbf{A}$ and statistically evaluate the number of secure rounds.

In general, Feistel ciphers attack by differential cryptanalysis becomes more difficult as the number of rounds increases. However, the processing time increases proportionately to the number of rounds, so studying the trade-off between security and the number of rounds is necessary. It is known that efficient differential cryptanalysis against Feistel ciphers with several small S-boxes and many rounds by tracking active S-boxes. However, this attack cannot apply directly to LBF because it has a single S-box.

Another approach to the security evaluation of block ciphers with many rounds is differential characteristic probability, which estimates the differential probability of $N$ rounds using the product of the differential probabilities for each round [20].

**Definition 7.** Suppose the input difference to the round function in the $j$-th round is $\Delta \boldsymbol{X}_{j-1}$, the output difference is $\Delta \boldsymbol{X}_j$, and the conditional probability of the output difference for a given the input difference is $P(\Delta \boldsymbol{X}_j | \Delta \boldsymbol{X}_{j-1})$. Then,

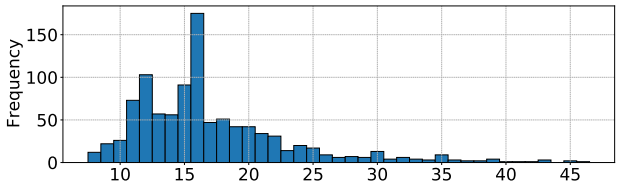


Fig. 4. Number of rounds to achieve $P_{c,N} \leq 2^{-m}$.

the differential characteristic probability $P_{c,N}$ for $N$ rounds is defined by

$$P_{c,N} = \prod_{j=1}^{N} P(\Delta \boldsymbol{X}_j | \Delta \boldsymbol{X}_{j-1}), \tag{26}$$

where $\Delta \boldsymbol{X}_0 = \Delta \boldsymbol{X} \neq \mathbf{0}$.

For each round, the combination of realized values of the input difference $\Delta \boldsymbol{X}_{j-1}$ is called a *path*, and the differential characteristic probability is obtained by searching for the path that maximizes $P_{c,N}$.

When the differential characteristic probability satisfies $P_{c,N} \leq 2^{-m}$, the cipher is considered to be "practically secure" against differential cryptanalysis [24]. The smallest such $N$ is the number of rounds the cipher is secure against differential cryptanalysis. For block ciphers satisfying $P_{c,N} \leq 2^{-m}$, an attacker needs plaintext greater than or equal to all possible plaintext patterns to decrypt the cipher with differential cryptanalysis. The practically secure lower bound of $N(\mathbf{A}) = \min\{N \mid P_{c,N} \leq 2^{-m}\}$ is determined only by $\mathbf{A}$. We find the distribution of $N(\mathbf{A})$ by computing the differential characteristic probability for uniformly random $\mathbf{A}$. For an LBF with the parameter $(n, m, q) = (2, 8, 4)$ and fixed round keys, we generate 1000 instances of $\mathbf{A}$ of full rank and determine $N(\mathbf{A})$.

Fig. 4 depicts the distribution of $N(\mathbf{A})$ obtained by the Monte Carlo simulation. The minimum value of $N(\mathbf{A})$ is 8, the maximum value is 46, and the average is 17.08. The results confirm that the number of secure rounds varies, corresponding to each instance.

In this simulation, it was confirmed that there exists a bad instance where the output difference is the same for any round key $\boldsymbol{K}_j$ and input difference $\Delta \boldsymbol{X}_{j-1}$. In fact, for example,

$$\begin{pmatrix} 2 & 1 & 2 & 0 & 1 & 3 & 0 & 2 \\ 0 & 2 & 1 & 1 & 2 & 3 & 3 & 3 \end{pmatrix}$$

is a bad instance in which the output difference is fixed. In this case, with $\Delta \boldsymbol{X}_{j-1}$ represented as the binary sequence 11000100 and $\boldsymbol{K}_j$ as 11110000, $\Delta \boldsymbol{X}_j$ is always 10111100. In the simulation, such bad instances are excluded from generating instances for LBF.

In the following, we determine the probability that such a bad instance occurs. Since the rows of $\mathbf{A}$ are independent, the characteristics of a bad instance can be considered separately for each row of $\mathbf{A}$. Let $\Delta \tilde{y}_i$ be the output difference after binary encoding for the pair $\tilde{y}_i, \tilde{y}'_i$ of the S-box output corresponding to $i$-th row $\boldsymbol{a}_i$ of $\mathbf{A}$. $\mathbf{A}$ is a bad instance if $\Delta \tilde{y}_1, \Delta \tilde{y}_2, \cdots \Delta \tilde{y}_n$ are all fixed together.

The probability $P_{\mathbf{A}}$ that $\mathbf{A}$ becomes a bad instance can be expressed as $P_{\mathbf{A}} = P_{\boldsymbol{a}_i}^n$ using the probability $P_{\boldsymbol{a}_i}$ that $\boldsymbol{a}_i$ becomes a bad instance. The necessary and sufficient condition for $\boldsymbol{a}_i$ to be a bad instance is to satisfy all of the following (P1), (P2), and (P3).

- (P1) Given a input difference $\Delta \boldsymbol{X}_{j-1}$ and the round key $\boldsymbol{K}_j$, the output difference $\Delta \tilde{y}_i$ is uniquely determined for all combinations of round input pairs $\boldsymbol{X}$ and $\boldsymbol{X}'$
- (P2) (P1) holds for any input differences $\Delta \boldsymbol{X}_{j-1}$
- (P3) (P1) holds for any round keys $\boldsymbol{K}_j$.

Let $\mathbb{A}_{P1\cap P2\cap P3}$ be the set of $\boldsymbol{a}_i$ satisfying all these conditions and $\mathbb{A}$ be the set of all instances $\mathbf{A}$. Then $P_{\boldsymbol{a}_i}$ is given by the proportion of bad instances in the whole instance, i.e.,

$$P_{\boldsymbol{a}_i} = \frac{|\mathbb{A}_{P1\cap P2\cap P3}|}{|\mathbb{A}|}, \tag{27}$$

where $|S|$ is the cardinality of set $S$.

Counting the elements of $\mathbb{A}_{P1\cap P2\cap P3}$ directly is difficult because the number of elements increases exponentially for $n$. Then, we determine the upper bound of $P_{\boldsymbol{a}_i}$. To obtain this estimate, consider the set $\mathbb{A}_{P1'\cap P2'\cap P3'}$, which satisfies all the conditions (P1'), (P2'), and (P3') obtained by relaxing the conditions of (P1), (P2), and (P3).

- (P1') Given a input difference $\Delta \boldsymbol{X}_{j-1}$ and the round key $\boldsymbol{K}_j$, the output difference $\Delta \tilde{y}_i$ is uniquely determined for all $N_x \in \{1, 2, \cdots, 2^m\}$ combinations of round input pairs $\boldsymbol{X}$ and $\boldsymbol{X}'$.
- (P2') (P1') holds for all $N_d \in \{1, 2, \cdots, 2^m\}$ input differences $\Delta \boldsymbol{X}_{j-1}$.
- (P3') (P1') holds for all $N_k \in \{1, 2, \cdots, 2^m\}$ round keys $\boldsymbol{K}_j$.

Namely, (P1), (P2), and (P3) are conditions that the output differences are uniquely determined for every input pair $\boldsymbol{X}, \boldsymbol{X}'$, every input differences $\Delta \boldsymbol{X}_{j-1}$, and all round keys $\boldsymbol{K}_j$. On the other hand, (P1'), (P2'), and (P3') are relaxed conditions such that the output difference is uniquely determined for $N_x$ input pairs $\boldsymbol{X}, \boldsymbol{X}'$, $N_d$ input differences $\Delta \boldsymbol{X}_{j-1}$, and $N_k$ round keys $\boldsymbol{K}_j$. Then, since $\mathbb{A}_{P1\cap P2\cap P3} \subseteq \mathbb{A}_{P1'\cap P2'\cap P3'}$ we have

$$P_{\boldsymbol{a}_i} = \frac{|\mathbb{A}_{P1\cap P2\cap P3}|}{|\mathbb{A}|} \leq \frac{|\mathbb{A}_{P1'\cap P2'\cap P3'}|}{|\mathbb{A}|}. \tag{28}$$

The right-hand side of (28) approaches $P_{\boldsymbol{a}_i}$ as $N_x$, $N_d$, and $N_k$ are larger. However, it becomes difficult to search for candidates of bad instances when the block size $m$ is too large.

Here, we evaluate the upper bound for the simplest case of $N_d = 1$. The input difference $\Delta \boldsymbol{X}_{j-1}$ can be chosen arbitrarily on conditions (P1'), (P2'), (P3'). We select an input difference where only the first $l$-bits are set to 1. In this way, it is possible to reduce the number of candidates of input pairs $\boldsymbol{X}$, $\boldsymbol{X}'$, round keys $\boldsymbol{K}_j$, and $\boldsymbol{a}_i$ to be verified.

Under these conditions, it is sufficient to explore inputs $\boldsymbol{X}$ where the first $l$-bits are $b_k \in \{0, 1\} (k = 1, 2, \cdots, l)$ and the remaining bits are 0. For (P1'), there are $N_x = 2^l$ possible input pairs to verify whether they produce a unique output difference. Since the input difference is fixed to a single setting, $N_d$ is 1 in (P2'). Likewise, for (P3'), it is sufficient to consider $N_k = 2^{2l}$ key candidates corresponding to the first $l$-bits expanded through the permutation $E$.

The bad instance is not determined by the elements $a_{i\frac{m}{2}-l}a_{i\frac{m}{2}-l+1}\cdots a_{i\frac{m}{2}}$, $a_{im-l}a_{im-l+1}\cdots a_{im}$of $\boldsymbol{a}_i$, which are multiplied with input bits that are fixed to 0. As a result, if the candidates of $\boldsymbol{a}_i$ are determined to be bad using this method, subsequent $2^{m-2l}$ instances following the first $l$ elements are treated as bad instances. Note that the larger the value of $l$, the greater the number of combinations that need to be explored, which also makes the calculation more difficult. For the case where $l = 1$, the output pair is fixed to be either $\{(0, a_{i1} + a_{i\frac{m}{2}+1}), (a_{i1} + a_{i\frac{m}{2}+1}, 0)\}$ or $\{(a_{i1}, a_{i\frac{m}{2}+1}), (a_{i\frac{m}{2}+1}, a_{i1})\}$ depending on the key. This configuration yields a $P_{\boldsymbol{a}_i} = 1$. Therefore, we evaluate $P_{\boldsymbol{a}_i}$ for $l = 2$, which is computationally feasible, and evaluate $P_{\mathbf{A}}$ using the upper bound $P_{\mathbf{A}} \leq P_{\boldsymbol{a}_i}^n$.

TABLE III
EVALUATION OF $P_{\mathbf{A}}$.

| $n$ | Block size $m$ | $P_{\boldsymbol{a}_i}^n$ ( $l = 2$ ) |
|---|---|---|
| 2 | 8 | $5.62500\times10^{-01}$ |
| 3 | 18 | $7.50847\times10^{-02}$ |
| 4 | 32 | $2.50116\times10^{-03}$ |
| 5 | 50 | $2.09182\times10^{-05}$ |
| 6 | 72 | $4.56045\times10^{-08}$ |
| 7 | 98 | $2.66528\times10^{-11}$ |

Table III shows the results obtained by the upper bound of $P_{\mathbf{A}}$ from (28) through a brute-force search, which shows that when $\mathbf{A}$ is chosen uniformly at random, the probability that it becomes a bad instance decays exponentially with increasing block size. For further verification, we performed Monte Carlo simulations to determine whether a uniformly randomly selected $\mathbf{A}$ is a bad instance. However, we could not find a bad instance among 100 million instances of $\mathbf{A}$ for $n = 3$. For $n \geq 4$, the total set of $\mathbf{A}$ is too large, which makes Monte Carlo simulations difficult. Since the upper bound in (28) is a loose estimate, the probability that a bad instance occurs is expected to be much smaller than this upper bound for an increase in $n$.

### C. Average properties on S-box Output Differential

Based on the previous discussion, this section studies the average characteristics of LBF instances. In an ideal S-box, the distribution of the output pairs obeys a uniform distribution. An ideal maximum difference characteristic is that the maximum output difference is small, and the probability of the output difference asymptotically obeys a uniform distribution.

It is difficult to demonstrate directly that the distribution of the maximum differential probability of the LBF approaches a uniform distribution. By using a method based on the generalized extreme value distribution, we propose that the distribution of maximum differential probability of the LBF asymptotically approaches that of an ideal distribution.

We approximate the distribution of the output pairs of the LBF S-box by a folded two-dimensional normal distribution and show that the average output characteristics of the LBF approach the ideal uniform distribution using a generalized

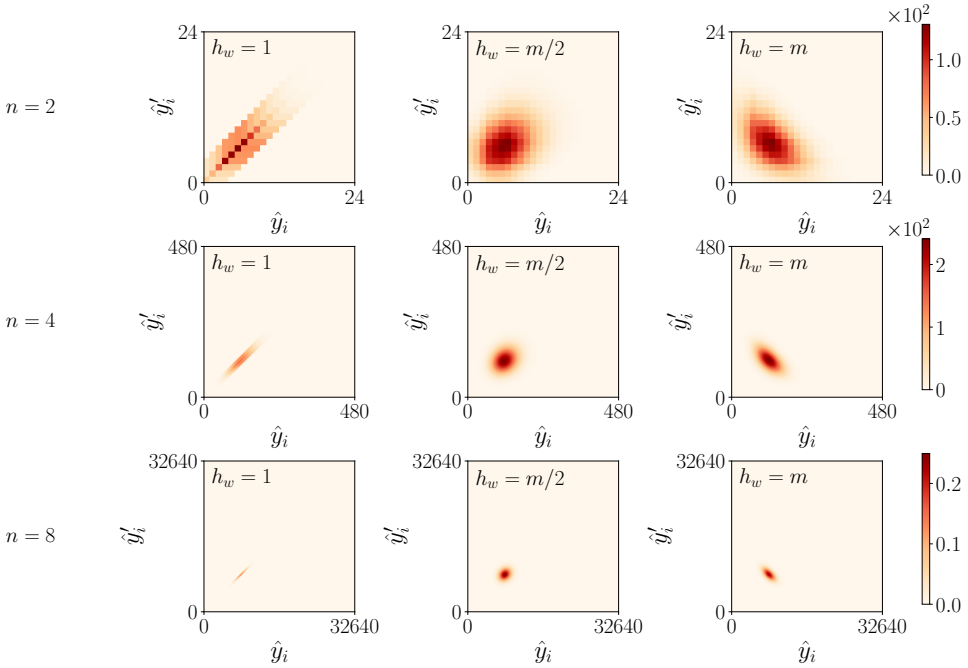


Fig. 5. Emprical distribution of $(\hat{y}_i, \hat{y}'_i)$.

extreme value distribution. When selecting an instance of $\mathbf{A}$, each row $\boldsymbol{a}_i \in \mathbb{Z}_q^m (i = 1, 2, \cdots, n)$ is independent, so the distribution of S-box output differences is a joint distribution of the distributions for each row.

First, for the S-box input pair $\boldsymbol{x}$, $\boldsymbol{x}'$ and $\mathcal{J}_{m,q} = \{0, 1, \cdots, m(q-1)\}$, define the S-box output pair $(\hat{y}_i, \hat{y_i}') \in \mathcal{J}_{m,q} \times \mathcal{J}_{m,q}$ as follows:

$$\hat{y}_i = \boldsymbol{a}_i \boldsymbol{x}, \tag{29}$$
$$\hat{y}'_i = \boldsymbol{a}_i \boldsymbol{x}'. \tag{30}$$

Fig. 5 shows the empirical distribution of output pairs $(\hat{y}_i, \hat{y}'_i)$ for randomly generated instances of $\boldsymbol{a}_i$ by the Monte Carlo simulation. Note that the empirical distribution depends on the input difference, but since the components of $\boldsymbol{a}_i$ are selected independently, we only need to consider the Hamming weight $h_w$ of the input difference to obtain the empirical distribution. In the Fig. 5, the top, middle, and bottom rows correspond to $n = 2$, 4, and 8, respectively. From left to right across the columns, the figures correspond to the Hamming weights $h_w = 1$, $m/2$, and $m$ (where $m$ is the block size).

For the cases where $n = 2$, 4, and 8, the empirical distribution was obtained for 100000 instances under each condition, and the frequency was averaged for each instance. In this simulation, the empirical distribution of input $\boldsymbol{x}$ was created using all inputs for $n = 2$. In the case $n = 4$ and 8, the empirical distribution was obtained using 1000000 inputs selected uniformly at random with a fixed input difference $\Delta\boldsymbol{x}$ and a pair of inputs $\boldsymbol{x}' = \boldsymbol{x} \oplus \Delta\boldsymbol{x}$.

Since components of $\boldsymbol{a}_i$ are independent and obey a discrete uniform distribution, the output, which is the sum of them, is close to a normal distribution. It can be seen that as $n$ increases from 2 to 8, the distribution is close to the two-dimensional normal distribution, especially when $h_w = m/2$. Moreover, as the parameter $n$ increases, the number of random variables that obey the uniform distribution increases, so we expect that the distribution is approximately close to the normal distribution.

As $n$ increases, the range of values for $(\hat{y}_i, \hat{y}_i{}')$ grows exponentially, but the concentration ellipse becomes smaller, and regions far from the ellipse become rare events. Consequently, the data becomes zero-inflated categorical data. Such data can destabilize the $\chi^2$ value in chi-square tests, making the uniformity test difficult [25]. Therefore, in the following, the joint distribution of the output pairs $(\hat{y}_i, \hat{y}'_i)$ is approximated by a two-dimensional normal distribution. This method is a standard approach for representing bivariate distributions with correlations. By using a folded two-dimensional normal distribution by modulo-$q$ and the GEV, we demonstrate that the maximum differential probability asymptotically approaches that of an ideal S-box.

First, the distribution of the vector $\hat{\boldsymbol{y}} = (\hat{y}_i, \hat{y}'_i)$ representing the output pair is modeled as a two-dimensional normal distribution as follows:

$$p(\hat{\boldsymbol{y}}) = \frac{1}{\sqrt{2\pi}^2 \sqrt{|\boldsymbol{\Sigma}|}} \exp\left(-\frac{1}{2}(\hat{\boldsymbol{y}} - \boldsymbol{\mu})^\top \boldsymbol{\Sigma}^{-1} (\hat{\boldsymbol{y}} - \boldsymbol{\mu})\right) \tag{31}$$

$$\boldsymbol{\mu} = \begin{pmatrix} \mu, & \mu \end{pmatrix} \tag{32}$$
$$\boldsymbol{\Sigma} = \begin{pmatrix} \sigma^2 & \sigma^2 - \Delta \\ \sigma^2 - \Delta & \sigma^2 \end{pmatrix} \tag{33}$$
$$\mu = \frac{m}{4}(q-1) \tag{34}$$

$$\sigma^2 = \frac{m(q-1)}{4}\left(\frac{2q-1}{3} + \frac{m^2(q-1)(m-1)}{16}\right) \tag{35}$$
$$\Delta = \frac{1}{12}(2q-1)(q-1)h_w(\Delta\boldsymbol{x}), \tag{36}$$

where $\boldsymbol{\mu}$ is the mean vector, $\boldsymbol{\Sigma}$ is the covariance matrix, and $h_w(\Delta \boldsymbol{x})$ is the Hamming weight of the input difference (see Appendix).

Next, we obtain the distribution folded by modulo-$q$, which models the distribution of S-box output pairs. By evaluating the maximum probability of this distribution, that is, the frequency of the mode, we can estimate the bias in the differential probability. When a one-dimensional normal distribution is folded by modulo-$q$, it asymptotically becomes a uniform distribution with a sufficiently small partition width [26]. On the other hand, this result can be applied to a multidimensional normal distribution if each dimension is independent. However, it is not easy to extend this result directly because the variables in our approximate model are correlated.

In the following, we use Monte Carlo simulation to obtain the empirical distribution of the random variables $(\tilde{y}_i, \tilde{y}'_i)$, which are the output pairs $(\hat{y}_i, \hat{y}'_i)$ folded by modulo-$q$. Observing the frequency of the mode of this empirical distribution, we determine the empirical frequency distribution of mode. By fitting the GEV to the empirical frequency distribution of the mode, we can estimate the maximum density of the S-box output pair.

$N_s$ random output pairs that obey (31) are generated in the simulation. These random variable values are folded by modulo-$q$ to obtain the empirical distribution of $(\tilde{y}_i, \tilde{y}'_i)$, and its frequency of the mode. This process is repeated $N_m$ times to obtain the empirical frequency distribution. The parameters of the GEV were obtained by maximum likelihood estimation. We employed the ismev package of R to estimate the parameters [27]. Additionally, since the ideal S-box output pairs $(\tilde{y}_i, \tilde{y}'_i)$ obey a uniform distribution over $\mathbb{Z}_q \times \mathbb{Z}_q$, we compare its distribution with that of the output given by (31) using Monte Carlo simulation.

In the Fig. 6, the top, middle, and bottom rows correspond to $n = 2$, 4, and 8, respectively. The sample size of the output pair is $N_s = 1000000$, the sample size of the frequency is $N_m = 100000$, and the Hamming weights of input differences are $h_w = 1, m/2$, and $m$. Fig. 6 shows the probability density function of the GEV with the estimated parameters, and Table IV–VI shows the estimated parameters. From results, for $n = 2$, only the distribution for $h_w = 1$ (dash-dotted line) deviates from the others ($h_w = 4, 8$) and from the uniform case. For $n = 4$, the distribution for $h_w = 1$ is slightly offset from the others. For $n = 8$, all the distributions are almost identical, confirming that the deviation decreases as $n$ increases. We also confirmed that the distribution of $n = 2$ and $h_w = 1$ differs from other distributions. However, this discrepancy becomes smaller for larger $n = 4, 8$, and the larger $n$, the closer the distribution estimated by the normal distribution approximation becomes to that estimated by the uniform distribution.

Tables IV–VI show the estimated GEV parameters, location $\mu$, scale $\sigma$, shape $\xi$, and their standard errors ($SE_\mu$, $SE_\sigma$, $SE_\xi$) obtained by the maximum likelihood estimation. These estimated parameters show that the larger $n$ is, the more asymptotic the normal distribution approximation result is to the uniform distribution characteristic, which is an ideal S-box. Considering the obtained standard error, if one examines

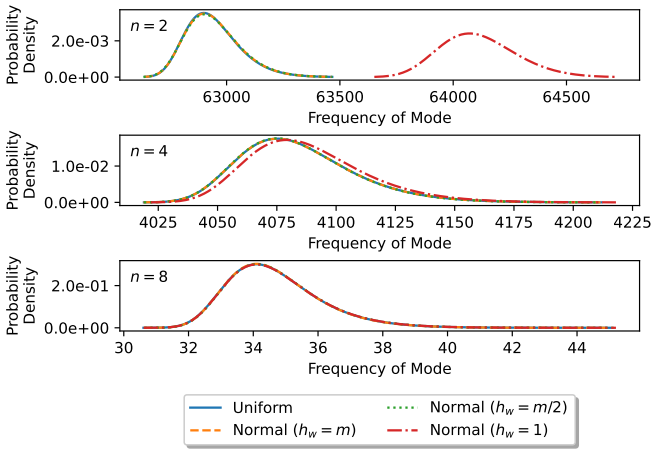


Fig. 6. Estimated frequency distribution of mode.

the one-sided 95% confidence interval, the shape parameter is sufficiently less than zero, suggesting that the distribution of the output pair $(\tilde{y}_i, \tilde{y}'_i)$ of the S-box modeled by the normal distribution approximation obeys the Weibull distribution.

TABLE IV
ESTIMATED PARAMETER ($n = 2$).

| | Uniform | Normal ($h_w = m$) | Normal ($h_w = m/2$) | Normal ($h_w = 1$) |
|---|---|---|---|---|
| $\mu$ | 62889.9804 | 62891.2570 | 62891.1632 | 64044.1023 |
| $SE_\mu$ | 0.366293 | 0.368066 | 0.371648 | 0.518169 |
| $\sigma$ | 104.3645 | 105.4014 | 106.7196 | 155.1743 |
| $SE_\sigma$ | 0.258920 | 0.263640 | 0.270961 | 0.353453 |
| $\xi$ | -0.086671 | -0.092448 | -0.094775 | -0.167586 |
| $SE_\xi$ | 0.002037 | 0.002018 | 0.002064 | 0.000806 |

TABLE V
ESTIMATED PARAMETER ($n = 4$).

| | Uniform | Normal ($h_w = 1$) | Normal ($h_w = m/2$) | Normal ($h_w = m$) |
|---|---|---|---|---|
| $\mu$ | 4073.5561 | 4073.4771 | 4073.4372 | 4077.5444 |
| $SE_\mu$ | 0.073623 | 0.073703 | 0.073359 | 0.075155 |
| $\sigma$ | 21.039072 | 21.061516 | 20.952711 | 21.469652 |
| $SE_\sigma$ | 0.052006 | 0.051980 | 0.051752 | 0.053072 |
| $\xi$ | -0.077223 | -0.078088 | -0.078389 | -0.078177 |
| $SE_\xi$ | 0.001978 | 0.001971 | 0.001984 | 0.001981 |

TABLE VI
ESTIMATED PARAMETER ($n = 8$).

| | Uniform | Normal ($h_w = 1$) | Normal ($h_w = m/2$) | Normal ($h_w = m$) |
|---|---|---|---|---|
| $\mu$ | 34.0361 | 34.0343 | 34.0496 | 34.0439 |
| $SE_\mu$ | 0.004282 | 0.004259 | 0.004283 | 0.004301 |
| $\sigma$ | 1.222491 | 1.214973 | 1.220174 | 1.226664 |
| $SE_\sigma$ | 0.003036 | 0.003020 | 0.003043 | 0.003054 |
| $\xi$ | -0.049566 | -0.051149 | -0.047329 | -0.046985 |
| $SE_\xi$ | 0.001993 | 0.002010 | 0.002040 | 0.002016 |

From the mode of the probability distribution of the S-box output pairs $(\tilde{y}_i, \tilde{y}'_i)$ obtained in this way, we can estimate the maximum differential probability of the LBF in the $N$ round. Let $c(\tilde{\boldsymbol{y}}, \tilde{\boldsymbol{y}}')$ be the number of occurrences of the output pair $(\tilde{\boldsymbol{y}}, \tilde{\boldsymbol{y}}') \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n$ of the S-box. The maximum differential

probability $P_{\max}$ of the S-box is as follows:

$$P_{\max} = \max_{\Delta\tilde{\boldsymbol{y}}} P(\Delta\tilde{\boldsymbol{y}}) = \max_{\Delta\tilde{\boldsymbol{y}}} \sum_{(\tilde{\boldsymbol{y}},\tilde{\boldsymbol{y}}')s.t.\tilde{\boldsymbol{y}}\oplus\tilde{\boldsymbol{y}}'=\Delta\tilde{\boldsymbol{y}}} \frac{c(\tilde{\boldsymbol{y}},\tilde{\boldsymbol{y}}')}{2^m}, \tag{37}$$

where $\Delta\tilde{\boldsymbol{y}}$ is a formal notation representing the EXOR of $\tilde{\boldsymbol{y}}$ and $\tilde{\boldsymbol{y}}'$ after binary encoding, which represented as $\Delta\tilde{\boldsymbol{y}} = \tilde{\boldsymbol{y}} \oplus \tilde{\boldsymbol{y}}'$. From the independence of each row in $\mathbf{A}$, this can be rewritten in the following form:

$$P_{\max} = \left( \max_{\Delta\tilde{y}_i} \sum_{(\tilde{y}_i,\tilde{y}_i')s.t.\tilde{y}_i\oplus\tilde{y}_i'=\Delta\tilde{y}_i} \frac{c(\tilde{y}_i,\tilde{y}_i')}{q^2} \right)^n, \tag{38}$$

where $c(\tilde{y}_i, \tilde{y}_i')$ is the number of occurrences of the output pair $(\tilde{y}_i, \tilde{y}_i')$, and $\tilde{y}_i \oplus \tilde{y}_i' = \Delta\tilde{y}_i$ represents the EXOR after binary encoding. Then, there are $q$ output pairs $(\tilde{y}_i, \tilde{y}_i')$ whose output differences are $\Delta\tilde{y}_i$, and it is found that the upper bound of (38) can be evaluated using the frequency of the mode $N_g$ for the number of occurrences $c(\tilde{y}_i, \tilde{y}_i')$ and $N_s$:

$$P_{\max} = \left( \max_{\Delta\tilde{y}_i} \sum_{(\tilde{y}_i,\tilde{y}_i')s.t.\tilde{y}_i\oplus\tilde{y}_i'=\Delta\tilde{y}_i} \frac{c(\tilde{y}_i,\tilde{y}_i')}{q^2} \right)^n \leq \left( q\frac{N_g}{N_s} \right)^n. \tag{39}$$

The upper bound of the maximum differential characteristic probability of $N$ rounds can be obtained as the power of $N$, and the number of rounds $N$ satisfying the practically secure criterion can be estimated by determining the smallest $N$ satisfying the following:

$$\left( \frac{qN_g}{N_s} \right)^{nN} \leq 2^{-m}. \tag{40}$$

For $N_s > qN_g$, the following can be derived

$$N \geq \frac{m}{\log_2 \frac{N_s}{qN_g}}. \tag{41}$$

According to the estimation of the number of rounds by (41), $N$ required is maximized by the largest $N_g$. Since $(-\infty, \mu - \frac{\sigma}{\xi}]$ is supported on the negative axis for the GEV shape parameter $\xi < 0$, we consider $N_g = \mu - \frac{\sigma}{\xi}$, which has the largest mode, to estimate the upper bound on the number of rounds required. For $n = 2$, a large value of $N_g$ results in $N_s < qN_g$, making it impossible to evalue the number of rounds. However, for $n = 4$, $N = 16$, and for $n = 8$, $N = 6$, the upper bound of the required number of rounds can be estimated. To the best of the authors' knowledge, there have been no examples of theoretical evaluation of secure rounds focusing on its probability distribution. As a result, the fact that this approach yields specific number of secure rounds is particularly noteworthy.

## VI. Conclusion

In this paper, we constructed a Feistel cipher using a hash function based on the computational hardness of the SIS as a lattice problem and evaluated its security. To evaluate the robustness of the constructed cipher against differential cryptanalysis, we derived a theoretical upper bound on the maximum differential probability and determined the number of secure rounds corresponding to each block size $m$.

We also examined the typical security of the LBF instances. Through statistical analysis of the bias in the S-box output and using the GEV to determine the number of secure rounds, we were able to provide concrete insights. The results show that for block sizes of 32 and 128, the required number of secure rounds are 16 and 6, respectively. These findings demonstrate that LBF can be constructed to be secure against differential cryptanalysis.

Since our method involves simulations to obtain empirical distributions, applying it to scenarios where $n$ exceeds 8 is difficult. This is mainly due to the need for increased samples, which require significant computational resources. Additional research is needed to develop alternative approaches that do not rely on simulations. In addition to considering the resistance of differential cryptanalysis, the application of linear cryptanalysis to LBF requires further study.

## Acknowledgments

JSPS KAKENHI Grant Number 20K11817 supported the second author Masahiro Kaminaga's work on this paper.

## Appendix A
## Folded two-dimensional normal distribution approximation of S-box output

Approximating the distribution of $(\hat{y}_i, \hat{y}_i')$ in (29), (30) by folded two-dimensional normal distribution. The mean $\boldsymbol{\mu}$ of $(\hat{y}_i, \hat{y}_i')$ is obtained as follows:

$$\begin{aligned} E_{\boldsymbol{x}}[E_{\boldsymbol{a_i}}[\hat{y}_i]] &= E_{\boldsymbol{x}}[E_{\boldsymbol{a}_i}[\boldsymbol{a}_i\boldsymbol{x}]] \\ &= E_{\boldsymbol{x}}\left[\frac{q-1}{2}\sum_{k=1}^{m} x_k\right] \\ &= \frac{m}{4}(q-1) \end{aligned}$$

$$\begin{aligned} E_{\boldsymbol{x}}[E_{\boldsymbol{a_j}}[\hat{y}_i]] &= E_{\boldsymbol{x}}[E_{\boldsymbol{a}_i}[\boldsymbol{a}_i(\boldsymbol{x}\oplus\Delta\boldsymbol{x})]] \\ &= E_{\boldsymbol{x}}\left[\frac{q-1}{2}\sum_{k=1}^{m}(x_k + \Delta x_k - 2x_k\Delta x_k)\right] \\ &= \frac{m}{4}(q-1). \end{aligned}$$

Letting $\mu = \frac{m}{4}(q-1)$, the mean $\boldsymbol{\mu}$ is given by

$$\boldsymbol{\mu} = (\mu, \mu).$$

The diagonal elements of the covariance matrix $\boldsymbol{\Sigma}$ are obtained as follows:

$$\begin{aligned} &E_{\boldsymbol{x}}[E_{\boldsymbol{a}_i}[(\hat{y}_i - \mu)^2]] \\ &= E_{\boldsymbol{x}}[E_{\boldsymbol{a_i}}[(\boldsymbol{a}_i\boldsymbol{x})^2]] - \mu^2 \\ &= E_{\boldsymbol{x}}\left[\frac{(2q-1)(q-1)}{6}(\sum_{k=1}^{m} x_k^2) + \mu^2\sum_{k\neq l}^{m} x_k x_l\right] - \mu^2 \\ &= \frac{m(q-1)}{4}\left(\frac{2q-1}{3} + \frac{m^2(q-1)(m-1)}{16}\right) \end{aligned}$$

$$
\begin{aligned}
&E_{\boldsymbol{x}}[E_{\boldsymbol{a}_i}[(\hat{y}_i' - \mu)^2]] \\
&= E_{\boldsymbol{x}}[E_{\boldsymbol{a}_i}[(\boldsymbol{a}_i(\boldsymbol{x} \oplus \Delta\boldsymbol{x}))^2]] - \mu^2 \\
&= E_{\boldsymbol{x}}\left[\frac{(2q-1)(q-1)}{6}\left(\sum_{k=1}^{m}(x_k \oplus \Delta x_k)^2\right)\right. \\
&\quad \left. + \mu^2 \sum_{k \neq l}^{m}(x_k \oplus \Delta x_k)(x_l \oplus \Delta x_l)\right] - \mu^2 \\
&= \frac{m(q-1)}{4}\left(\frac{2q-1}{3} + \frac{m^2(q-1)(m-1)}{16}\right).
\end{aligned}
$$

Thus, we let $\sigma^2 = \frac{m(q-1)}{4}\left(\frac{2q-1}{3} + \frac{m^2(q-1)(m-1)}{16}\right)$ and we have the covariance

$$
\begin{aligned}
&E_{\boldsymbol{x}}[E_{\boldsymbol{a}_i}[(\hat{y}_i - \mu)(\hat{y}_i' - \mu)]] \\
&= E_{\boldsymbol{x}}[E_{\boldsymbol{a}_i}[(\boldsymbol{a}_i\boldsymbol{x})(\boldsymbol{a}_i(\boldsymbol{x} \oplus \Delta\boldsymbol{x}))]] - \mu^2 \\
&= \sigma^2 - \frac{(2q-1)(q-1)h_w(\Delta\boldsymbol{x})}{12}.
\end{aligned}
$$

For convenience, we let $\Delta = \frac{(2q-1)(q-1)h_w(\Delta\boldsymbol{x})}{12}$ and the covariance matrix $\boldsymbol{\Sigma}$ is given by

$$
\boldsymbol{\Sigma} = \begin{pmatrix} \sigma^2 & \sigma^2 - \Delta \\ \sigma^2 - \Delta & \sigma^2 \end{pmatrix}. \tag{42}
$$

## REFERENCES


[1] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, July 1996, pp. 99–108.

[2] P. Q. Nguyen and B. Vallee, Eds., *The LLL Algorithm: Survey and Applications*. Berlin, Germany: Springer, December 2009.

[3] O. Regev, "The learning with errors problem (invited survey)," in *Proceedings of 2010 IEEE 25th Annual Conference on Computational Complexity*, June 2010, pp. 191–204.

[4] D. Micciancio, "(invited talk) duality in lattice based cryptography," in *Proceedings of 13th International Conference on Practice and Theory in Public Key Cryptography*, May 2010.

[5] O. Goldreich, S. Goldwasser, and S. Halevi, *Collision-Free Hashing from Lattice Problems*, O. Goldreich, Ed. Berlin, Heidelberg: Springer, August 2011.

[6] K. Kajita, G. Ohtake, K. Ogawa, K. Nuida, and T. Takagi, "Short lattice signature scheme with tighter reduction under Ring-SIS assumption," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E106.A, no. 3, pp. 228–240, March 2023.

[7] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, September 2009.

[8] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *Proceedings of 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*. IEEE, October 2011, pp. 97–106.

[9] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *Journal of the ACM*, vol. 33, no. 4, pp. 792–807, August 1986.

[10] M. Naor and O. Reingold, "Synthesizers and their application to the parallel construction of Pseudo-Random functions," *Journal of Computer and System Sciences*, vol. 58, no. 2, pp. 336–375, April 1999.

[11] A. Banerjee, "New constructions of cryptographic pseudorandom functions," Ph.D. dissertation, Georgia Institute of Technology, August 2015.

[12] H. Montgomery, "More efficient lattice prfs from keyed pseudorandom synthesizers," in *Proceedings of Progress in Cryptology – INDOCRYPT 2018*, D. Chakraborty and T. Iwata, Eds. Cham: Springer, December 2018, pp. 190–211.

[13] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, December 1982.

[14] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing – STOC'08*. New York, NY, USA: Association for Computing Machinery, May 2008, p. 197–206.

[15] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with small parameters," in *Proceedings of Advances in Cryptology – CRYPTO 2013*. Springer Berlin Heidelberg, August 2013, pp. 21–39.

[16] D. Micciancio and O. Regev, "Worst - case to average - case reductions based on gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

[17] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 373–386, April 1988.

[18] J. HÅstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM Journal on Computing*, vol. 28, no. 4, pp. 1364–1396, January 1999.

[19] N. Bitansky, I. Haitner, I. Komargodski, and E. Yogev, "Distributional collision resistance beyond one-way functions," in *Proceedings of Advances in Cryptology – EUROCRYPT 2019*. Cham: Springer International Publishing, April 2019, pp. 667–695.

[20] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, pp. 3–72, January 1991.

[21] S. Coles, *An Introduction to Statistical Modeling of Extreme Values*. Springer London, August 2001.

[22] K. Nyberg and L. R. Knudsen, "Provable security against a differential attack," *Journal of Cryptology*, vol. 8, pp. 27–37, December 1995.

[23] D. R. Stinson, *Cryptography: theory and practice*. Boca Raton, Florida, U.S.A.: CRC Press, March 1995.

[24] L. R. Knudsen, *Practically secure Feistel ciphers. In: Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 1994.

[25] A. Agresti, *Categorical Data Analysis*. John Wiley & Sons, 2012.

[26] T. Suzuki and M. Kaminaga, "A true random number generator method embedded in wireless communication systems," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E103.A, no. 4, pp. 686–694, April 2020.

[27] O. S. functions written by Janet E. Heffernan with R port and R. documentation provided by Alec G. Stephenson., *ismev: An Introduction to Statistical Modeling of Extreme Values*, 2018, r package version 1.42. [Online]. Available: https://CRAN.R-project.org/package=ismev



**Yu Morishima** (Member, IEEE) received his B.S., M.S., and Ph.D. degrees in Engineering from Osaka City University in 2009, 2011, and 2014, respectively. From 2014 to 2018, he served as an Assistant Professor and from 2018 to 2019 as a Lecturer at National Institute of Technology, Suzuka College. Since 2019, he has been a Lecturer at Tohoku Gakuin University. His research interests include error correcting codes, information theory, wireless communication, and cryptography.

**Masahiro Kaminaga** (member, IEEE) received a B.S. degree in 1991 from Tokyo University of Science, a M.S. in 1993 from Kyoto University, and a Ph.D. in 2003 from Osaka University, all in mathematics. He was an instructor at Tokyo Denki University from 1994 to 1998 and a researcher at the Central Research Laboratory, HITACHI Ltd., from 1998 to 2004. In 2004, he joined the engineering faculty at Tohoku Gakuin University as a lecturer. Since 2011, he has been a Professor in the Department of Electrical Engineering and Information Technology. His research interests include spectral theory, mathematical physics, and cryptography.