Adventures in Crypto Dark Matter: Attacks, Fixes and Analysis for Weak Pseudorandom Function Candidates

Jung Hee Cheon[1], Wonhee Cho[1], Jeong Han Kim[2], and Jiseung Kim[2]

[1] Seoul National University, Republic of Korea.
{jhcheon,wony0404}@snu.ac.kr
[2] School of Computational Sciences, Korea Institute for Advanced Study,
Seoul 02455, Korea
{jhkim,jiseungkim}@kias.re.kr

Abstract. A weak pseudorandom function (weak PRF) is one of the most important cryptographic primitives for its efficiency although it has lower security than a standard PRF.

Recently, Boneh et al. (TCC'18) introduced two types of new weak PRF candidates, called a basic Mod-2/Mod-3 and alternative Mod-2/Mod-3 weak PRF. They both use the mixture of linear computations defined on different small moduli to satisfy conceptual simplicity, low complexity (depth-2 ACC^0) and MPC friendliness. In fact, the new candidates are conjectured to be exponentially secure against any adversary that allows exponentially many samples, and a basic Mod-2/Mod-3 weak PRF is the only candidate that satisfies all above features. However, none of direct attacks which focus on a basic and alternative Mod-2/Mod-3 weak PRFs uses their own structures.

In this paper, we investigate weak PRFs in three perspectives; attacks, fixes, and a new analysis to support the hardness conjecture of weak PRFs. We first propose direct attacks for an alternative Mod-2/Mod-3 weak PRF and a basic Mod-2/Mod-3 weak PRF when a circulant matrix is used as a secret key.

For an alternative Mod-2/Mod-3 weak PRF, we prove that the adversary's advantage is at least $2^{-0.105n}$, where n is the size of input space of weak PRF. Similarly, we show that the advantage of our heuristic attack to the weak PRF with a circulant matrix key is larger than $2^{-0.21n}$, which is contrary to previous expectation that 'a structured secret key' does not affect the security of a weak PRF. Thus, for optimistic parameter choice $n = 2\lambda$ for the security parameter λ, parameters should be increased to preserve λ-bit security when an adversary obtains exponentially many samples.

Next, we provide a simple method for repairing two weak PRFs affected by our attack while preserving the depth-2 ACC^0 circuit complexity and parameters.

Moreover, we provide an observation and a new analysis to support the exponential hardness conjecture of a basic Mod-2/Mod-3 weak PRF when a secret key is uniformly sampled from $\{0,1\}^{m\times n}$.

Keywords: Cryptanalysis, weak PRF

1 Introduction

A pseudorandom function (PRF) proposed by Goldreich, Goldwasser and Micali [GGM86] is a keyed function which looks like a true random function. PRFs have been widely used as building blocks to construct several cryptographic primitives such as HMAC, digital signature and indistinguishability obfuscation [Gol86, BCK96, App14, Bel15, ABSV15, BR17].

Weak PRFs, which satisfy weaker security and higher efficiency than PRFs, are keyed functions whose input-output behaviors are indistinguishable from those of random functions when adversaries are limited to observing outputs mapped by randomly sampled inputs. Many cryptographic primitives and applications are built from weak PRFs because of the its efficiency [DN02, MS07, Pie09, DKPW12, LM13, ASA17, BHI$^+$20].

To construct more efficient weak PRFs, simple constructions are emphasized to minimize circuit complexity and depth. Akavia *et al.* proposed a simple construction of weak PRFs which satisfies depth-3 ACC^0 circuit complexity with quasi-polynomial security [ABG$^+$14].

As line of works, Boneh *et al.* (TCC'18) proposed simple weak PRF candidates by mixing linear computations on different moduli [BIP$^+$18]. Motivated by a paper [ABG$^+$14], they provided a weak PRF which satisfies the following properties: conceptually simple structure, low complexity (depth-2 ACC^0 circuit complexity) and MPC-friendliness. In particular, new candidates are the unique depth-2 weak PRFs conjectured to satisfy the exponential hardness beyond the polynomial hardness. Moreover, they provided two types of parameters: optimistic and conservative. A conservative parameter is set to be secure against attacks for LPN problem, but it does not seem to be applicable to weak PRFs. Thus, an optimistic choice was additionally proposed.

We now briefly describe constructions of Mod-2/Mod-3 weak PRFs in [BIP$^+$18]. For each Mod-2/Mod-3 weak PRF, a function $\mathcal{F} : \mathbb{Z}_2^n \times \mathbb{Z}_2^{m\times n} \to \mathbb{Z}_3$ with an input $\mathbf{x} \in \{0,1\}^n$ is defined as follows. (For details, see the construction 3.1)

- Basic Mod-2/Mod-3:
  For a "random" secret key $\mathbf{A} \in \mathbb{Z}_2^{m\times n}$, $\mathcal{F}(\mathbf{x}, \mathbf{A}) = \mathsf{map}(\mathbf{A} \cdot \mathbf{x})$, where map is a function from $\{0,1\}^m$ to $\mathbb{Z}_3$ mapping a binary vector $\mathbf{y} = (y_j)$ to an integer $\sum_{j=1}^m y_j \bmod 3$.[1]
- Circulant Mod-2/Mod-3:[2]
  Take $m = n$. Then, it is exactly the same as a basic Mod-2/Mod-3 except $\mathbf{A}$ is a circulant matrix.

[1] For well-definedness, $\mathbf{A} \cdot \mathbf{x}$ is interpreted as a binary vector.

[2] In the original paper [BIP$^+$18], they used a Toeplitz matrix or a block-circulant matrix as a secret key of weak PRF for its efficiency. However, in this paper, we only deal with a case that a secret key of weak PRF is a circulant matrix which is exactly the same as block-circulant matrix in original paper. Indeed, they said that block-circulant matrix can be represented by a single vector'.

- Alternative Mod-2/Mod-3:
  Set $m = 1$. $\mathcal{F}(\mathbf{x}, \mathbf{k}) = (\langle \mathbf{k}, \mathbf{x} \rangle \bmod 2 + \langle \mathbf{k}, \mathbf{x} \rangle \bmod 3) \bmod 2$ for a random secret key $\mathbf{k} \in \{0, 1\}^n$.

However, there is no direct or concrete attack for weak PRFs using their own structures. Therefore, further cryptanalyses or security proofs should be required to break or support their conjectures and concrete security.

1.1 This work

In this paper, we investigate Mod-2/Mod-3 weak PRFs in three perspectives; attacks, fixes and a new analysis to support the hardness conjecture of Mod-2/Mod-3 weak PRFs.

Attacks. Our concrete attacks mainly concentrate on two weak PRFs; an alternative and a circulant Mod-2/Mod-3 weak PRFs. As a result, we show that the advantage of an alternative Mod-2/Mod-3 weak PRF is $2^{-0.105n}$ with the size of input space n. It is computed as the conditional probability of input vectors given that outputs are 'zero'. Similarly, we provide a heuristic attack with an advantage $2^{-0.21n}$ and experimental results of a circulant weak PRF. This result is contrary to previous prediction that parameters will not be much affected by the structure of a key. Our attacks are the first attacks using structure of Mod-2/Mod-3 weak PRFs. Indeed, we first observe interesting features of certain secret keys of weak PRFs, and statistically attack them using these features. As an example, a circulant matrix always preserves the number of nonzero entries h in each column, so $(1, ..., 1)$ is a left-eigenvector of a circulant matrix with an eigenvalue h.

Mod-2/Mod-3 weak PRFs			
Parameter Choices		Alternative	Circulant Key
[BIP+18]	Optimistic	-	256
	Conservative	384	384
Ours	$\log(T/\epsilon^2)$-bit security	610	305
	$\log(T/\epsilon)$-bit security	1220	610

Table 1: Changes of concrete parameters for 128-bit security to prevent our attacks with $m = n$. [‡]

[‡] We take concrete parameters according to guidance of a paper [MW18]. For decision primitives, they recommended $\lambda = \log_2(T/\epsilon^2)$ rather than $\lambda = \log_2(T/\epsilon)$, with a cost T and an advantage ϵ. The latter is also widely used in crypto community. We include both results in table 1. However, we mainly deal with the measure $\lambda = \log_2(T/\epsilon^2)$ in this paper.

Our attacks mainly exploit conditional probabilities based on structures of weak PRFs to distinguish weak PRF samples from uniform samples. More specifically, an adversary model to attack an alternative Mod-2/Mod-3 weak PRF computes $\Pr[x_i = 0 \mid \mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0 \bmod 2]$ for input $\mathbf{x} = (x_j) \in \{0,1\}^n$. If the probability for some x_i is far from $1/2$ by $\frac{1}{2^{0.105n}}$, we conclude that pairs of inputs and outputs follow a distribution of an alternative weak PRF, not a uniform distribution. As a result, this simple attack satisfies interesting features.

- Support a full parallel computing: when δ processors are given, the total time complexity decreases from T_{total} to $T_{total}/\delta + O(\delta)$
- Require only $O(n)$ memory space because calculating an average does not need to store samples.
- Simply extend to Mod-p/Mod-q weak PRFs for any primes p and q: For an alternative Mod-p/Mod-q, we show that the bigger pq is, the more powerful our attack is. For example, an alternative and a circulant Mod-3/Mod-5 weak PRFs should be set as $n = 4000$ and $n = 2000$, respectively, for 128-bit security under measure T/ϵ^2.

Fixes. We suggest simple variants of weak PRFs to be secure against our attacks while preserving a depth of original weak PRFs and circuit class complexity ACC^0.

For an alternative case, our attack heavily relies on the number of nonzero entries in the secret key $\mathbf{k}$, so we easily present a new alternative candidate to force the hamming weights of $\mathbf{k}$. For instance, if we use the secret key with 310 nonzero entries, then it is secure against the statistical attack. Moreover, an adversary cannot search $\mathbf{k}$ by brute-force attack since $\binom{384}{310} \gg 2^{200}$.

On the other hand, for repairing a circulant Mod-2/Mod-3 weak PRF, we use two different vectors $\mathbf{a}$ and $\mathbf{b}$ to construct a secure circulant Mod-2/Mod-3 weak PRF. Exploiting two secret vectors, we generate a new secret key $\mathbf{B}$ such that for $1 \le i \le n/2$, i-th row of $\mathbf{B}$ is rotation of the vector $\mathbf{a}$, and for $n/2 < j \le n$, j-th row vector is rotation of the vector $\mathbf{b}$. Then, the fixed Mod-2/Mod-3 weak PRF with the secret key $\mathbf{B}$ is secure against our attack since a combination of two vectors can remove a structured weakness of circulant matrix that the number of nonzero entries in column vector is always the same. In other words, vector of ones $(1, \cdots, 1)$ is not a left-eigenvector of $\mathbf{B}$ anymore. Moreover, we heuristically confirm that combining two vector strategy is an appropriate approach for small n. Indeed, experimental results show that the advantage of fixed candidate is larger than $2^{-0.5n}$, which means that it achieves 128-bit security against all known attacks under without a parameter blow-up. The size of PRF key of the fixed candidate is still smaller than that of random key, and it preserves depth-2 ACC^0 circuits and current parameter n.

Observation. Our analysis points out a statistical weakness from structures of weak PRF candidates. For a fixed circulant case, we observe that the structured chaos of secret key might be a crucial factor for the security of weak PRF. As stated earlier, when we use two secret vectors to generate a secret key $\mathbf{B}$ with several rotations, it is secure against all known attacks. Rotations of two vectors make it hard to find rules of $\mathbf{B}$ while reducing key size, and the security of a weak PRF with $\mathbf{B}$ might be almost the same for a random key under current attacks.

New Analysis to Support the Hardness Conjecture. Our observation may imply that the structured chaos of secret key is critical factor to prevent from our attack. Therefore, if a random matrix sampled from the $\{0,1\}^{m\times n}$ is used for weak PRF as a secret key, it might be secure against statistical adversaries containing our models. As one of bases of the observation, the advantage of our attacks for fixed schemes is exponentially decreased to the number of extra secret vectors.

To support that our observation would hold true, we provide another analysis of a basic Mod-2/Mod-3 weak PRF based on algorithms for solving the k-xor problem that is already well known for its hardness. For example, we show that the advantage of a basic Mod-2/Mod-3 weak PRF is larger than $2^{-0.60m}$ if we can find three vectors $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \{0,1\}^n$ such that $\mathbf{x}+\mathbf{y}+\mathbf{z} = \mathbf{0} \in \mathbb{Z}_2^n$.

However, since they are uniformly sampled from $\mathbb{Z}_2^n$, finding such vectors is the same as solving the 3-xor problem, well known for the computational hardness problem. Indeed, it takes exponential time and space $O(2^{n/2})$. [3] Moreover, even if an adversary can access to an oracle to solve the 3-xor problem in polynomial time, our attack requires exponentially many samples due to the adversary's advantage. Thus, a new analysis would give a ground to support our observation of how large m can prevent statistical adversaries.

Open Problems. We leave some open problems.

- A direct attack for a basic Mod-2/Mod-3 can break current parameters $n = m = 256$ for 128-bit security.
- A concrete attack when adversaries of weak PRFs are limited to get polynomially many samples.
- Proves or disproves for the hardness conjectures.

Organization. We describe preliminaries about definitions of PRF and weak PRF, and some circuit complexities and results of k-xor problem in Section 2. We explicitly describe the constructions of weak PRF candidates in Section 3, and provide cryptanalyses of an alternative Mod-2/Mod-3 weak PRF and a circulant weak PRF in Section 4, respectively. In Section 5, we give a method to fix an alternative and a circulant Mod-2/Mod-3 weak PRFs. We additionally provide a new analysis of a basic construction based on the k-xor problem.

2 Preliminaries

2.1 Notations

Matrices and vectors are written as bold capital letters, and bold lower-case letters respectively. Moreover, we assume that vectors are column form in this paper, and i-th component of $\mathbf{x}$ will be denoted by x_i. The transpose of matrix or

[3] If we find roots of $k(\geq 5)$-xor problem, the advantage induced by them is drastically smaller than 2^{-m} although time complexity of k-xor problem is reduced to $O(2^{n/(k-1)})$.

vector is denoted by $\mathbf{A}^T$ or $\mathbf{x}^T$. Moreover, we denote an inner product between two vectors $\mathbf{x}$ and $\mathbf{y}$ by $\langle \mathbf{x}, \mathbf{y} \rangle$. A square matrix $\mathbf{A}$ is called a circulant matrix generated a base vector $\mathbf{a} = (a_i)$ such that $\mathbf{A} = \sum_{i=1}^{n} a_i \cdot \mathbf{P}^{i-1}$ for a permutation matrix $\mathbf{P}$ given by

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

$\mathbf{I}_n$ is the n-dimensional identity matrix. Also, we denote the n-dimensional vector that all entries are zero by $\mathbf{0}^n$, and similarly, $\mathbf{1}^n$ is a vector that all entries are one. For the convenience of notation, we sometimes omit the subscript if it does not lead to any confusion.

For any positive integer n, $[n]$ is denoted by the set of integers $\{1, 2, \cdots, n\}$. All elements in $\mathbb{Z}_q$ are represented by integers in range $[0, q)$ for any positive integer q. For a vector $\mathbf{x}$, we use a notation $[\mathbf{x}]_q$ to denote an 'entrywise' modulo q. *i.e*, $[\mathbf{x}]_q = ([x_i]_q)$ for $\mathbf{x} = (x_i)$. Let S be a finite set. Then, $s \overset{\$}{\leftarrow} S$ is denoted by uniformly sampled from the set S.

Definition 2.1 (Pseudorandom function (PRF) in [BIP+18]) *Let λ be the security parameter. A $(t(\lambda), \epsilon(\lambda))$-pseudorandom function family (PRF) is a collection of functions $\mathcal{F}_\lambda : \mathcal{X}_\lambda \times \mathcal{K}_\lambda \to \mathcal{Y}_\lambda$ with a domain $\mathcal{X}_\lambda$, a key space $\mathcal{K}_\lambda$ and an output space $\mathcal{Y}_\lambda$ such that for any adversary running time in $t(\lambda)$, it holds that*

$$\left| \Pr[\mathcal{A}^{\mathcal{F}_\lambda(\cdot,k)}(1^\lambda) = 1] - \Pr[\mathcal{A}^{f_\lambda(\cdot)}(1^\lambda) = 1] \right| \leq \epsilon(\lambda),$$

where $k \overset{\$}{\leftarrow} \mathcal{K}_\lambda$,and $f_\lambda \overset{\$}{\leftarrow} \mathsf{Funs}[\mathcal{X}_\lambda, \mathcal{Y}_\lambda]$.

In this paper, PRF is sometimes called strong PRF to make a difference with below weak PRF. The main difference between strong PRF and weak PRF is that an adversary is limited to obtaining randomly chosen input vectors.

Definition 2.2 (Weak PRF) *Let λ be the security parameter. A function $\mathcal{F}_\lambda : \mathcal{X}_\lambda \times \mathcal{K}_\lambda \to \mathcal{Y}_\lambda$ with a domain $\mathcal{X}_\lambda$, a key space $\mathcal{K}_\lambda$ and an output space $\mathcal{Y}_\lambda$ is called (ℓ, t, ϵ)-weak PRF if for any adversary running time in $t(\lambda)$, it holds that*

$$\{(\mathbf{x}_i, \mathcal{F}_\lambda(\mathbf{x}_i, k))\}_{i \in [\ell]} \approx_\epsilon \{(\mathbf{x}_i, y_i)\}_{i \in [\ell]}$$

where a key $k \overset{\$}{\leftarrow} \mathcal{K}_\lambda$, $\mathbf{x}_i \overset{\$}{\leftarrow} \{0,1\}^n$, and $y_i \overset{\$}{\leftarrow} \mathcal{Y}_\lambda$. We denote $\approx_\epsilon$ by the advantage of any adversary is smaller than ϵ.

To deal with the circuit class, we borrow some definitions from the paper [BIP+18].

Definition 2.3 (in [BIP+18]) *For any integer m, the MOD_m gate outputs 1 if m divides the sum of its inputs, and 0 others.*

Definition 2.4 (Circuit Class ACC^0 in [BIP+18]) *For integers $m_1, \cdots, m_k > 1$, $\mathsf{ACC}^0[m_1, \cdots, m_k]$ is the set of languages $\mathcal{L}$ decided by some circuit family $\{C_n\}_{n \in \mathbb{N}}$ with constant depth, polynomial size, and consisting of unbounded fan-in AND, OR, NOT and $\mathsf{MOD}_{m_1}, \cdots, \mathsf{MOD}_{m_k}$ gates. Moreover, ACC^0 is denoted by the class of all languages that is in $\mathsf{ACC}^0[m_1, \cdots, m_k]$ for some $k \geq 0$ and integers $m_1, \cdots, m_k > 1$.*

2.2 Generalized Birthday Problem (k-xor Problem)

In this section, we briefly review the results of generalized birthday problem.

Problem 2.5 (Generalized Birthday Problem (k-xor Problem)) Given k lists $L_1, \cdots, L_k$ of elements independently sampled from $\{0,1\}^n$, find vectors $\mathbf{x}_1 \in L_1,\ \mathbf{x}_2 \in L_2, \cdots \mathbf{x}_k \in L_k$ such that

$$\mathbf{x}_1 + \mathbf{x}_2 + \cdots \mathbf{x}_k = \mathbf{0} \bmod 2$$

If $\prod_{i=1}^{k} |L_i|$ is much larger than 2^n, then there exists a solution of the problem, but it is hard to efficiently find such a solution. Wagner [Wag02] proposed an algorithm to solve the k-xor problem, which requires $O(k \cdot 2^{n/(1+\lfloor \log_2 k \rfloor)})$ time and space using lists of size $O(2^{n/(1+\lfloor \log_2 k \rfloor)})$. Moreover, there exist algorithms for solving k-xor problems [Ber07, BLN+09, NS15, DDKS19, Din19]. Moreover, there exists a more efficient algorithm for solving the generalized birthday problem under the quantum computing [NPS20].

3 Construction of weak PRF Candidates

In this section, we briefly review how to construct weak PRF candidates proposed by Boneh *et al.* [BIP+18]. All constructions consist of linear computations on different moduli, which look simple and efficient.

3.1 Mod-2/Mod-3 weak PRF Candidate

In this section, we provide a basic construction of Mod-2/Mod-3 weak PRF candidate. Mod-2/Mod-3 weak PRFs are easily extended to Mod-p/Mod-q constructions for arbitrary primes p and q.

Construction 3.1 (A basic Mod-2/Mod-3 weak PRF) For the security parameter λ, a weak PRF candidate is a collection of functions $\mathcal{F}_\lambda : \{0,1\}^n \times \{0,1\}^{m \times n} \to \mathbb{Z}_3$ with a domain $\{0,1\}^n$, a key space $\{0,1\}^{m \times n}$ and an output space $\mathbb{Z}_3$. For a fixed key $\mathbf{A} \in \{0,1\}^{m \times n}$, we use a notation $\mathcal{F}_{\mathbf{A}} : \{0,1\}^n \to \mathbb{Z}_3$ which defines as follows.

1. Computes $\mathbf{y} = [\mathbf{A} \cdot \mathbf{x}]_2$
2. Outputs $\mathsf{map}(\mathbf{y})$, where map is a function from $\{0,1\}^m$ to $\mathbb{Z}_3$ which maps a binary vector $\mathbf{y} = (y_j)$ to an integer $\sum_{j=1}^{m} y_j \bmod 3$.

Thus, we summarize $\mathcal{F}_{\mathbf{A}}(\mathbf{x}) = \mathsf{map}([\mathbf{A}\cdot\mathbf{x}]_2)$. This simple construction induced by mixed linear computations on different moduli might be secure against previous attacks. Moreover, authors showed that a low-degree polynomial (rational function) approximation of map is hard, and standard learning algorithms cannot break this constructions. Moreover, a conjecture 3.2 is proposed.

Conjecture 3.2 (Exponential Hardness of Mod-2/Mod-3 weak PRF) Let λ be the security parameter. Then, there exist constants $c_1, c_2, c_3, c_4 > 0$ such that for $n = c_1\lambda, m = c_2\lambda$, $\ell = 2^{c_3\lambda}$, and $t = 2^{\lambda}$, a function family $\{\mathcal{F}_\lambda\}$ defined as Mod-2/Mod-3 construction is an (ℓ, t, ϵ)-weak PRF for $\epsilon = 2^{-c_4\lambda}$.

Remark 3.3 For improved efficiency of Mod-2/Mod-3 weak PRFs in real applications, a structured key $\mathbf{A}$ is used, not a random key from $\{0,1\}^{m\times n}$. Thus we expect the key size can be reduced when $\mathbf{A}$ is a block-circulant matrix or Toeplitz matrix. [4] Roughly speaking, a random key $\mathbf{A}$ requires mn key size, but the key size of a structured key $\mathbf{A}$ is $m+n$, much smaller than mn. A basic Mod-2/Mod-3 weak PRF with a circulant secret key $\mathbf{A}$ is called a circulant Mod-2/Mod-3 weak PRF.

Concrete Parameters. They proposed two types of parameters; optimized and conservative choices. The conservative choice, $m = n = 384$, is set to be robust against the BKW attack for LPN problem. However, the BKW attack does not seem to apply to this candidate, the optimized parameter, $m = n = 2\lambda = 256$, is also suggested to obtain 128-bit security.

3.2 Alternative Mod-2/Mod-3 Weak PRF Candidate

An alternative weak PRF is additionally proposed to obtain higher efficiency in two-party secure computation setting.

Construction 3.4 (Alternative Mod-2/Mod-3 weak PRF) For a secret key $\mathbf{k} \in \{0,1\}^n$, an alternative Mod-2/Mod-3 weak PRF is defined that for any input $\mathbf{x} \in \{0,1\}^n$,

$$\mathcal{F}(\mathbf{k},\mathbf{x}) = \langle \mathbf{k},\mathbf{x}\rangle \bmod 2 + \langle \mathbf{k},\mathbf{x}\rangle \bmod 3 \bmod 2.$$

For simplicity, we use a notation $\mathcal{F}_{\mathbf{k}}(\mathbf{x})$ instead of $\mathcal{F}(\mathbf{k},\mathbf{x})$ on a key $\mathbf{k} \in \{0,1\}^n$.

Concrete Parameters. Similar to a basic Mod-2/Mod-3 weak PRF, they consider all known attacks to claim the security of alternative's. Moreover, it resembles an LPN instance with a deterministic noise rate 1/3, so parameters are set as $m = n = 384$. For more details, see the original paper [BIP+18].

[4] In the original paper, authors mentioned that 'block-circulant matrix' can be represented by a single vector. Thus, a block-circulant matrix is the same as a circulant matrix in this paper.

4 Cryptanalysis of weak PRF candidates

We now introduce our analysis on two weak PRF candidates; an alternative Mod-2/Mod-3 and a circulant Mod-2/Mod-3 weak PRFs. These attacks are also applicable to an alternative and a circulant Mod-p/Mod-q weak PRF for arbitrary primes p and q.

4.1 Cryptanalysis of an alternative Mod-2/Mod-3 weak PRF

We briefly recall the construction of alternative Mod-2/Mod-3 weak PRF with the secret key $\mathbf{k} \in \{0,1\}^n$

$$\mathcal{F}_{\mathbf{k}}(\mathbf{x}) = (\langle \mathbf{k}, \mathbf{x} \rangle \bmod 2 + \langle \mathbf{k}, \mathbf{x} \rangle \bmod 3) \bmod 2.$$

We simply observe that $\mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0 \bmod 2$ if and only if $\langle \mathbf{k}, \mathbf{x} \rangle = 0, 1, 2 \bmod 6$. Then, our attack of alternative Mod-2/Mod-3 weak PRF is very simple. After an adversary collects $\ell = c_1 \cdot 2^{0.21n}$ samples whose output is 0 for some constant c_1, computes a conditional probability $\Pr[x_j = 0 \mid \mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0 \bmod 2]$ for each index $j \in [n]$. If there exists an index j such that it is apart from $1/2$ by $\frac{1}{2^{0.105n}}$, we conclude that an adversary has alternative Mod-2/Mod-3 weak PRF samples.

In order to provide a formal analysis, let h be the hamming weight of the secret key vector $\mathbf{k} \in \{0,1\}^n$. For the sake of explanation, suppose that the first h elements of $\mathbf{k}$ are all 1, and the others are zero. Then, we observe that

$$\langle \mathbf{k}, \mathbf{x} \rangle = x_1 + \cdots + x_h.$$

Note that a value x_i with $i > h$ has no effect on a result $\langle \mathbf{k}, \mathbf{x} \rangle$ since k_i is zero. So now, we only consider x_i for $i \in [h]$. For all $j \in [h]$, the conditional probability of x_j given by $\mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0 \bmod 2$ is that

$$\begin{aligned}
\Pr[x_j = 0 \mid \mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0 \bmod 2] &= \frac{\sum_{k=0}^{\lfloor \frac{h-1}{6} \rfloor} \binom{h-1}{6k} + \binom{h-1}{6k+1} + \binom{h-1}{6k+2}}{\sum_{k=0}^{\lfloor \frac{h}{6} \rfloor} \binom{h}{6k} + \binom{h}{1+6k} + \binom{h}{2+6k}} \\
&= \frac{1}{2} + \frac{(w^5 i\sqrt{3})^{h-1} \cdot w^4 + (-wi\sqrt{3})^{h-1} \cdot w^2}{3 \cdot 2^h + 2w^5 \cdot (w^5 i\sqrt{3})^h + 2w \cdot (-wi\sqrt{3})^h}
\end{aligned}$$

where w is 6-th root of unity, $\frac{1+\sqrt{3}i}{2}$. The proofs of following lemmas only require straightforward (but tedious) computations, so we skip the proofs.

Lemma 4.1 *Let h be the hamming weight of the secret key $\mathbf{k}$. For all $i \in [h]$,*

$$\Pr[x_i = 0 \mid \mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0 \bmod 2] = \begin{cases}
\frac{1}{2} - \frac{(i\sqrt{3})^h}{3 \cdot 2^h + 2 \cdot (i\sqrt{3})^h} & h = 6k \\
\frac{1}{2} - \frac{(i\sqrt{3})^{h-1}}{3 \cdot 2^h + 6 \cdot (i\sqrt{3})^{h-1}} & h = 6k+1 \\
\frac{1}{2} & h = 6k+2 \\
\frac{1}{2} + \frac{3(i\sqrt{3})^{h-3}}{3 \cdot 2^h + 18 \cdot (i\sqrt{3})^{h-3}} & h = 6k+3 \\
\frac{1}{2} + \frac{9(i\sqrt{3})^{h-4}}{3 \cdot 2^h + 18 \cdot (i\sqrt{3})^{h-4}} & h = 6k+4 \\
\frac{1}{2} + \frac{18(i\sqrt{3})^{h-5}}{3 \cdot 2^h} & h = 6k+5
\end{cases}$$

Since the simple attack does not work if $h \equiv 2 \bmod 6$, another adversary is required. A new adversary computes a conditional probability of $x_i = x_j = 0$ with $i \neq j$ given by $\mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0$. Then, we obtain the below lemma.

Lemma 4.2 *Let h be the hamming weight of the secret key $\mathbf{k}$. If $i, j \in [h]$ and $h \equiv 2 \bmod 6$,*

$$\Pr[x_i = 0, x_j = 0 \mid \mathcal{F}_{\mathbf{k}}(\mathbf{x}) = 0 \bmod 2] = \frac{\sum_{k=0}^{\lfloor \frac{h-2}{6} \rfloor} \binom{h-2}{6k} + \binom{h-2}{1+6k} + \binom{h-1}{2+6k}}{\sum_{k=0}^{\lfloor \frac{h}{6} \rfloor} \binom{h}{6k} + \binom{h}{1+6k} + \binom{h}{2+6k}}$$
$$= \frac{1}{4} - \frac{(i\sqrt{3})^{h-2}}{3 \cdot 2^h + 12(i\sqrt{3})^{h-2}}$$

According to lemma 4.1, 4.2, the advantage of an alternative Mod-2/Mod-3 weak PRF is larger than $c_h \cdot \left(\frac{\sqrt{3}}{2}\right)^h \approx \frac{1}{2^{0.21h}}$. Moreover, since $\mathbf{k}$ is chosen uniformly from the set $\{0,1\}^n$, we assume that h is $\frac{n}{2}$ without loss of generality. Thus, the advantage is larger than $\frac{1}{2^{0.105n}}$. As a result, to preserve 128-bit security, a parameter n should increase from 384 to 610 or 1220 under the measure $\frac{T}{\epsilon^2}$ or $\frac{T}{\epsilon}$ with a cost T and an advantage ϵ.

Remark 4.3 Our attack is easily extended to an alternative Mod-p/Mod-q weak PRF for arbitrary primes p and q. Following the our proof, the adversary's advantage of an alternative Mod-p/Mod-q is larger than $c_h \cdot \left|\frac{w_{pq}+1}{2}\right|^h \approx \left(\cos\left(\frac{\pi}{pq}\right)\right)^h$ where w_{pq} is pq-th root of unity. Therefore, the bigger pq is, the more powerful our attack is. For example, the advantage of an alternative Mod-3/Mod-5 weak PRF is larger than $\left(\cos\left(\frac{\pi}{15}\right)\right)^h \approx \frac{1}{2^{0.032h}}$, so n should be increased to 4000 for the 128-bit security under a measure T/ϵ^2 if $h = n/2$.

Remark 4.4 Since our attack just computes conditional probabilities, there exist interesting features.

- Full parallel computations are allowed. Hence, if there are δ processors, total time complexity is reduced from $O(2^{0.21n})$ to $O(2^{0.21n}/\delta) + O(\delta)$.
- An adversary does not need to store many weak PRF samples. Thus, Our attack is a space efficient algorithm. It requires only $O(n)$ space even though our attack needs a lot of samples.

Remark 4.5 An alternative construction can be reinterpreted by operations on mod 6 space. However, an input space of this construction is only $\{0,1\}^n$, not a full space $\mathbb{Z}_6^n$. This might be a statistical weakness of alternative weak PRF.

4.2 Cryptanalysis of A Circulant Mod-2/Mod-3 Weak PRF

As stated in Remark 3.3, structured keys are widely used to provide higher efficiency. In this section, we provide a heuristic analysis of a circulant Mod-

2/Mod-3 weak PRF candidate.[5] Before analysis, we present several observations of a circulant Mod-2/Mod-3 weak PRF.

Let $\mathbf{A} \in \{0,1\}^{n\times n}$ be a circulant matrix used in a Mod-2/Mod-3 weak PRF as a secret key and h be the hamming weights of a vector $\mathbf{a}$ which generates $\mathbf{A}$. Then, we observe that

- $\mathbf{1}^T \cdot \mathbf{A} = h(1, \cdots, 1)$
- $\mathbf{1}^T \cdot \mathbf{A} \cdot \mathbf{x} = h \cdot h_{\mathbf{x}}$ where $h_{\mathbf{x}}$ is the number of 1's in an input $\mathbf{x}$
- $\mathbf{1}^T \cdot [\mathbf{A} \cdot \mathbf{x}]_2 \equiv h \cdot h_{\mathbf{x}} \bmod 2$
- If $h_{\mathbf{x}}$ is even, then the number of 1's in $[\mathbf{A} \cdot \mathbf{x}]_2$ is also even.

Therefore, $[\mathbf{A} \cdot \mathbf{x}]_2$ preserves the parity of $\mathbf{x}$ if $h_{\mathbf{x}}$ is even. This is a key observation of our heuristic analysis. Moreover, if $[\mathbf{A} \cdot \mathbf{x}]_2$ is component-wise independent, then we can compute $\Pr[\mathcal{F}_{\mathbf{A}}(\mathbf{x}) \equiv 0 \bmod 3 \mid h_{\mathbf{x}} \text{ is even}]$ and $\Pr[\mathcal{F}_{\mathbf{A}}(\mathbf{x}) \equiv 2 \bmod 3 \mid h_{\mathbf{x}} \text{ is even}]$ according to Lemmas 4.6 and 4.7. Thus, we show that an adversary's advantage is larger than $c_n \cdot \left(\frac{\sqrt{3}}{2}\right)^n \approx \frac{1}{2^{0.21n}}$.

However, unfortunately, no one could be sure that components of $[\mathbf{A} \cdot \mathbf{x}]_2$ behave independently of each other since $\mathbf{A}$ is a circulant matrix. Therefore, we will give experimental results to support that the above conditional probabilities are almost the same as results of Lemmas 4.6 and 4.7, where lemmas are assumed to be independency of each component. (See experimental results 4.8.)

From now, we give an analysis under the assumption that a vector is component-wise independent. To avoid confusion, we newly define a random variable Y as follows. Let Y be a multivariate random variable that follows a distribution on $\{0,1\}^n$ that each entry is independently and uniformly sampled from $\{0,1\}$. Then, the conditional probability of $\mathbf{1}^T \cdot \mathbf{y} = 0 \bmod 3$ given that $\mathbf{y}$ is uniformly sampled from Y and $h_{\mathbf{y}}$ is even is

$$\begin{aligned}
&\Pr[\mathbf{1}^T \cdot \mathbf{y} = 0 \bmod 3 |\ \mathbf{y} \xleftarrow{\$} Y, h_{\mathbf{y}} \text{ is even}]\\
&= \frac{\sum_{k=0}^{\lfloor \frac{n}{6} \rfloor} \binom{n}{6k}}{\sum_{k=0}^{\lfloor \frac{n}{6} \rfloor} \binom{n}{6k} + \binom{n}{2+6k} + \binom{n}{4+6k}} = \frac{\sum_{k=0}^{5} (1+w^k)^n}{6 \cdot 2^{n-1}}\\
&= \frac{1}{3} + \frac{w^{2n}((-i\sqrt{3})^n + (-1)^n) + w^{4n}((i\sqrt{3})^n + (-1)^n)}{6 \cdot 2^{n-1}}
\end{aligned}$$

where w is 6-th root of unity, $\frac{1+i\sqrt{3}}{2}$. Similar to above section, a straightforward computation leads us following lemmas.

Lemma 4.6 *Let Y be a multivariate random variable that follows a distribution on $\{0,1\}^n$ that each entry is independently and uniformly sampled from $\{0,1\}$. Then, the conditional probability of $\mathbf{1}^T \cdot \mathbf{y} = 0 \bmod 3$ given that $\mathbf{y}$ is uniformly*

[5] As stated in Section 1, a circulant matrix is exactly the same a block-circulant in [BIP$^+$18]

sampled from Y and $h_{\mathbf{y}}$ is even is that

$$\Pr[\mathbf{1}^T \cdot \mathbf{y} = 0 \bmod 3 |\ \mathbf{y} \overset{\$}{\leftarrow} Y, h_{\mathbf{y}} \textit{ is even}] = \begin{cases} \frac{1}{3} + \frac{2(i\sqrt{3})^n + 2(-1)^n}{6 \cdot 2^{n-1}} & n = 6k \\ \frac{1}{3} + \frac{3(i\sqrt{3})^{n-1} + (-1)^{n+1}}{6 \cdot 2^{n-1}} & n = 6k+1 \\ \frac{1}{3} - \frac{(i\sqrt{3})^n + (-1)^n}{6 \cdot 2^{n-1}} & n = 6k+2 \\ \frac{1}{3} + \frac{2(-1)^n}{6 \cdot 2^{n-1}} & n = 6k+3 \\ \frac{1}{3} - \frac{(i\sqrt{3})^n + (-1)^n}{6 \cdot 2^{n-1}} & n = 6k+4 \\ \frac{1}{3} - \frac{3(i\sqrt{3})^{n-1} + (-1)^n}{6 \cdot 2^{n-1}} & n = 6k+5 \end{cases}$$

If $n \equiv 3 \bmod 6$, we require an extra analysis to point out a weakness of circulant Mod-2/Mod-3 weak PRF. However, we easily overcome this situation by computing a new conditional probability stated in below lemma.

Lemma 4.7 *Let Y be a random variable defined on Lemma 4.6. If n is $6k+3$, then we have that*

$$\begin{aligned} &\Pr[\mathbf{1}^T \cdot \mathbf{y} = 2 \bmod 3 |\ \mathbf{y} \overset{\$}{\leftarrow} Y, h_{\mathbf{y}} \textit{ is even}] \\ &= \frac{\sum_{k=0}^{\lfloor \frac{n}{6} \rfloor} \binom{n}{6k+2}}{\sum_{k=0}^{\lfloor \frac{n}{6} \rfloor} \binom{n}{6k} + \binom{n}{2+6k} + \binom{n}{4+6k}} \\ &= \frac{1}{3} + \frac{w^{2n+4}((-i\sqrt{3})^n + (-1)^n) + w^{4n+2}((i\sqrt{3})^n + (-1)^n)}{6 \cdot 2^{n-1}} \\ &= \frac{1}{3} - \frac{3(-i\sqrt{3})^{n-1} + (-1)^n}{6 \cdot 2^{n-1}} \end{aligned}$$

To support our expectation, we implement experiments in accordance with

1. Sample a random vector $\mathbf{a}$ from $\{0,1\}^n$.
2. Construct a circulant matrix $\mathbf{A}$ using the sampled vector $\mathbf{a}$.[6]
3. Compute $\mathcal{F}_{\mathbf{A}}(\mathbf{x})$ for sufficiently many $\mathbf{x}$'s.
4. Compute a conditional probability like above two lemmas.
5. Go to 1 again.

Experiments 4.8 We provide experimental results to support that $\Pr[\mathcal{F}_{\mathbf{A}}(\mathbf{x}) \equiv 0 \bmod 3 \mid h_{\mathbf{x}}$ is even$]$ and $\Pr[\mathcal{F}_{\mathbf{A}}(\mathbf{x}) \equiv 2 \bmod 3 \mid h_{\mathbf{x}}$ is even$]$ are almost the same as results of Lemmas 4.6 and 4.7.

In figure 3, we first regard (logarithms of) averages of the above conditional probabilities for several n, as blue points. Then, we draw a trend line from them. The (logarithm) trend line is $0.2038n + 0.4537$ similar to $2^{-0.21n}$ induced by our computations.

We also conducted several experiments for a fixed n. For cases $n \leq 18$, we ran experiments for all possible base vectors to show that our experiments are not lucky cases. As the same reason, 128 random base vectors were used to support our heuristic assumptions for $n = 32, 40$ and 50.

[6] We call $\mathbf{a}$ a base vector.

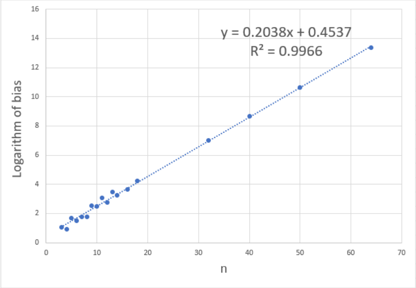
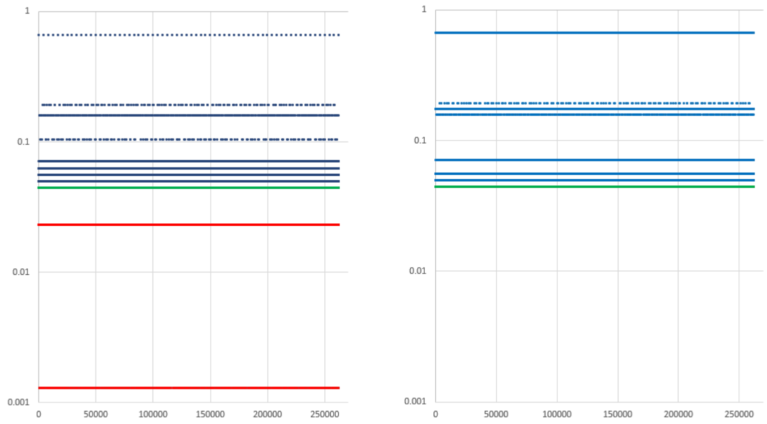


Fig. 1: Averages of (logarithm) biases according to n and its trend line.

During experiments, we observed some irregular points outside of our expectations. For example, under a case $n = 2^{18}$, there are $3.2\% = (8422/2^{18})$ base vectors that our assumption is invalid even though the analysis does not depend on the form of $\mathbf{A}$. Indeed, the value of red points drawn irregular cases in figure 2a is much smaller than that of the green points that follow our prediction. However, for these cases, we gathered $\mathbf{x}$'s with odd $h_{\mathbf{x}}$. Then, we observe that the maximum value M of $\{M_{\alpha,\beta}\}_{\alpha \in \{0,2\}, \beta \in \{\text{odd, even}\}}$, where $M_{\alpha,\beta}$ is defined as (1), is far from 1/3 by at least $\frac{1}{2^{0.21n}}$ in figure 2b, which supports that our attacks success regardless of the base vector $\mathbf{a}$.

$$M_{\alpha,\beta} := \left| \Pr[\mathcal{F}_{\mathbf{A}}(\mathbf{x}) \equiv \alpha \bmod 3 \mid h_{\mathbf{x}} \text{ is } \beta] - \frac{1}{3} \right| \tag{1}$$



(a) Log-size of $\max\{M_{*,\text{even}}\}$ according to all $\mathbf{a}$.

(b) Log-size of M according to all $\mathbf{a}$.

Fig. 2: Experimental results of all base vectors in $\{0,1\}^n$ with $n = 2^{18}$.

The x-axis is the decimal representation of the all base vectors. Note that every binary vector with the length n can be represented by an integer $\leq 2^n$.

Remark 4.9 The above mentioned remarks 4.3 and 4.4 are also satisfied with a circulant Mod-p/Mod-q weak PRF. As an example, we observe that the advantage of a circulant Mod-3/Mod-5 weak PRF is larger than $\left(\cos\left(\frac{\pi}{15}\right)\right)^n \approx \frac{1}{2^{0.032n}}$ from the same computation, so n should be increased to 2000 for the 128-bit security under a measure $T/\epsilon^2 = 2^\lambda$.

5 Analysis of Weak PRF to Support the Exponential Hardness

Previous attacks point out a statistical weakness if a secret key can be represented by a single vector. To avoid he weakness, a dimension of an input space n, should be increased.

In this section, we give an evidence to support that the conjecture of exponential hardness of a Mod-2/Mod-3 weak PRF, by fixing weak PRFs from a simple observation and presenting a new result that followed our observation.

5.1 How to Fix a weakness of Mod-2/Mod-3 weak PRFs

In this section, we suggest modified weak PRF candidates to prevent our statistical attacks while preserving low depth and its circuit complexity. Thus, we think that fixed weak PRFs are still MPC friendliness. Since our attacks use the biases of conditional probabilities, if a bias of the probability becomes smaller, our attacks become weaker.

An alternative Mod-2/Mod-3 weak PRF. We are easily able to fix an alternative Mod-2/Mod-3 weak PRF since our attack heavily depends on the hamming weights of the secret key $\mathbf{k}$. More specifically, under the current parameter $n = 384$, when we set the hamming weights $h = 310$ that is larger than $n/2$, it is secure against our statistical attacks. Moreover, this simple variant is secure against all known attacks presented by the original paper since they does not consider the hamming weights of the secret vector. Also, it is robust against brute-force attack for finding the secret key because of $\log_2 \binom{384}{310} \gg 200$. Thus, the fixed scheme preserves the depth-2 ACC^0 circuit complexity and current parameters.

A circulant Mod-2/Mod-3 weak PRF. Our strategy is to break a weak structure of a circulant Mod-2/Mod-3 weak PRF that preserves a parity of $[\mathbf{Ax}]_2$ if $h_{\mathbf{x}}$ is even for any circulant matrix $\mathbf{A}$. To avoid a weakness, we inject extra secret vector and generate a new secret key $\mathbf{B}$ with two secret vectors. We name $\mathbf{B}$ a semi-circulant key. Previously, a circulant secret key is generated by a single vector. For explanation, let $\mathbf{a}$ and $\mathbf{b}$ be secret vectors. Then, we construct a secret matrix $\mathbf{B}$ as follows. For simple description, assume that n is even.

- Set initial vectors such that the first row of $\mathbf{B}$ is $\mathbf{a}$ and $n/2$-th row of $\mathbf{B}$ is $\mathbf{b}$.
- For each $2 \le i \le n/2$, i-th row of $\mathbf{B}$ is $\rho_i(\mathbf{a})$, where $\rho_i(\mathbf{a})$ shifts one element to the right relative to the $\rho_{i-1}(\mathbf{a})$ with $\rho_1(\mathbf{a}) = \mathbf{a}$ and $\rho_{n+1}(\mathbf{a}) = \mathbf{a}$.
- Similarly, for each $n/2 < j \le n$, j-th row of $\mathbf{B}$ is $\rho_j(\mathbf{b})$.

Then, we observe that each column of a matrix $\mathbf{B}$ does not preserve hamming weights, so vectors of ones $(1, \cdots, 1)$ is not a left-eigenvector of $\mathbf{B}$. Thus, we can easily fix a circulant Mod-2/Mod-3 weak PRF against all known attacks including our statistical attack. Moreover, the size of PRF key is still smaller than that of random key, and it preserve a current parameter n and depth-2 ACC^0 circuits.

To support that the simple modification with a semi-circulant key $\mathbf{B}$ is reasonable, we conducted experiments for several n and types of secret key; random $\mathbf{A}$ and semi-circulant $\mathbf{B}$. To construct a semi-circulant key $\mathbf{B}$, we randomly choose two vectors from $\{0,1\}^n$. For $n = 16, 18$, we experimented with 128 different secret keys to compute (averages of) logarithm biases of the statistical attack. Similarly, for $n = 24, 28$, we provided experimental results for 20 different secret keys. Moreover, for each case, 2^n samples were used to compute accurate $M = \max_{\alpha,\beta}\{M_{\alpha,\beta}\}_{\alpha\in\{0,2\},\beta\in\{\text{odd, even}\}}$.

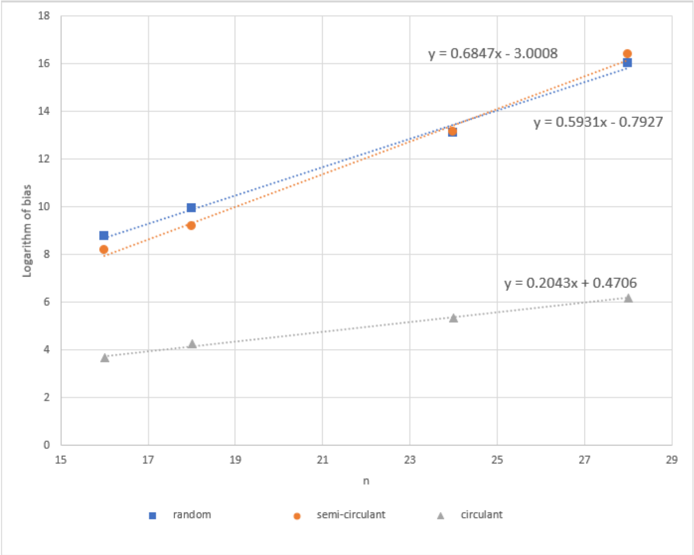


Fig. 3: Averages of (logarithm) biases according to n and types of secret keys and their trend lines.

According to the above graph, we observe that a semi-circulant weak PRF with $\mathbf{B}$, behaves Mod-2/Mod-3 weak PRF with random secret key $\mathbf{A}$. Moreover, the fixed candidate is secure against all known attacks under the current parameters $n = m = 256$ since its advantage is already larger than $2^{-0.5n}$.

Remark 5.1 We observe that the weakness of a circulant Mod-2/Mod-3 weak PRF might come from a structured property of $\mathbf{A}$. Indeed, we observe that if we break up the property using two secret vectors, then a Mod-2/Mod-3 weak PRF with secret key $\mathbf{B}$ is secure against our attack although a circulant with key $\mathbf{A}$ is vulnerable to our attack. Thus, we can make a hypothesis that a structured chaos of the secret key implies the security of weak PRF candidates.

5.2 Analysis of a Mod-2/Mod-3 weak PRF based on k-xor Problem

In this section, we introduce a new analysis to support our hypothesis in the Remark 5.1. A new statistical analysis shows that a Mod-2/Mod-3 weak PRF with a random key $\mathbf{A}$ is hard even if we can solve k-xor problem. Hence, a basic Mod-2/Mod-3 might satisfy the exponential hardness based on our observation.

For an analysis, we borrow a polynomial representation of $\mathcal{F}_{\mathbf{A}}(\mathbf{x})$ in [BIP+18].

$$\mathcal{F}_{\mathbf{A}}(\mathbf{x}) = \sum_{i=1}^{m} \left(\prod_{j=1}^{n} (1+x_j)^{a_{i,j}} - 1 \right),$$

where a matrix $\mathbf{A} = (a_{i,j}) \in \{0.1\}^{m \times n}$ and a vector $\mathbf{x} = (x_i) \in \{0,1\}^n$. Note that since $a_{i,j}$ is 0 or 1, the following lemma is trivial.

Lemma 5.2 *Mod-2/Mod-3 weak PRF is interpreted as a product of matrices. More precisely, for a key $\mathbf{A} = (a_{i,j}) \in \{0,1\}^{m \times n}$ and a vector $\mathbf{x} = (x_i) \in \{0,1\}^n$,*

$$\mathcal{F}_{\mathbf{A}}(\mathbf{x}) + n = \sum_{i=1}^{n} f_i(\mathbf{x}) = \mathbf{1}^T \cdot \prod_{i=1}^{n} (\mathbf{I} + \mathsf{diag}(x_i \mathbf{A}_i)) \cdot \mathbf{1}$$

where $\mathbf{A}_i$ is the i-th column of $\mathbf{A}$, and $f_i(\mathbf{x}) = \prod_{j=1}^{n}(1 + a_{i,j}x_j)$, and $\mathsf{diag}(x_i\mathbf{A}_i)$ is a diagonal matrix whose j-th diagonal entry is the same as j-th component of a vector $x_i\mathbf{A}_i$.

Above lemmas provide the closed matrix form of Mod-2/Mod-3 weak PRFs. The closed-form induces an interesting property that $\prod_{i=1}^{n}(\mathbf{I} + \mathsf{diag}(x_i\mathbf{A}_i))$ has an input-homomorphic structure, which is the crucial observation that enables us a new analysis using its structure. We leave a proof in the Appendix B.

Lemma 5.3 *Let $\mathbf{H}(\mathbf{x})$ be a function defined as $\mathbf{H}(\mathbf{x}) := \prod_{i=1}^{n}(\mathbf{I} + \mathsf{diag}(x_i\mathbf{A}_i))$ where $\mathbf{A}_i$ and x_i's are the same as the above Lemma 5.2. Then, for arbitrary binary vectors $\mathbf{x}$ and $\mathbf{y}$, it holds that*

$$\mathbf{H}([\mathbf{x}+\mathbf{y}]_2) = \mathbf{H}(\mathbf{x}) \cdot \mathbf{H}(\mathbf{y}) \bmod 3$$

Therefore, $\mathcal{F}_{\mathbf{A}}([\mathbf{x}+\mathbf{y}]_2) + n = \sum_{i=1}^{n} f_i(\mathbf{x}) \cdot f_i(\mathbf{y})$ where $\mathcal{F}_{\mathbf{A}}(\mathbf{x}) + n = \sum_{i=1}^{n} f_i(\mathbf{x})$ and $\mathcal{F}_{\mathbf{A}}(\mathbf{y}) + n = \sum_{i=1}^{n} f_i(\mathbf{y})$. Here $f_i(\mathbf{x})$ is 1 or 2.

Our analysis consists of two steps. First, we employ an algorithm for solving k-xor problem to find vectors $\mathbf{x}_1, \cdots, \mathbf{x}_k$ such that $\mathbf{x}_1 + \cdots + \mathbf{x}_k = 0 \bmod 2$ using $O(k \cdot 2^{n/(1+\lfloor \log_2 k \rfloor)})$ time and space. (See the Section 2.2 for results of the k-xor problem.) Then, without loss of generality, let $\mathbf{x}_k := \mathbf{x}_1 + \cdots + \mathbf{x}_{k-1} \bmod 2$. Then, $\mathcal{F}_{\mathbf{A}}(\mathbf{x}_k)$ is written as $\sum_{i=1}^{n} f_i(\mathbf{x}_1) \cdots f_i(\mathbf{x}_{k-1})$ for f_i defined as Lemma 5.3. As a next step, we compute conditional probabilities according to k for analysis.

Case $\boldsymbol{k} = 2$. First, find vectors $\mathbf{x}_1, \mathbf{x}_2$ such that $\mathbf{x}_1 + \mathbf{x}_2 = \mathbf{0} \bmod 2$ using $O(2^{n/2})$ time and space. Note that $\mathbf{x}_1$ is equal to $\mathbf{x}_2$ since the equation holds over modular 2. Therefore, $\mathcal{F}_{\mathbf{A}}(\mathbf{x}_1)$ must be equal to $\mathcal{F}_{\mathbf{A}}(\mathbf{x}_2)$, and then the below theorem trivially holds.

Theorem 5.4 *Let λ be the security parameter, and n and m parameters of Mod-2/Mod-3 weak PRF candidate. Then, if $\ell > c_1 \cdot 2^{n/2}$ for some constant c_1, there exist solutions of the 2-xor problem. Then we show that for a key $\mathbf{A} \overset{\$}{\leftarrow} \{0,1\}^{m\times n}$ and inputs $\mathbf{x}_i \overset{\$}{\leftarrow} \{0,1\}^n$ for all $i \in [\ell]$, it holds that for any $y_i \overset{\$}{\leftarrow} \mathbb{Z}_3$ $i \in [\ell]$,*

$$\left| \Pr\left[\mathcal{F}_{\mathbf{A}}(\mathbf{x}_1) - \mathcal{F}_{\mathbf{A}}(\mathbf{x}_2) = 0 \bmod 3 \mid \sum_{i=1}^{2} \mathbf{x}_i \ = \mathbf{0} \right] - \frac{1}{3} \right| = \frac{2}{3}$$

Therefore, there exists an adversary $\mathcal{A}$ in running time $c_2 \cdot 2^{n/2}$ for some constant c_2 such that

$$\left| \Pr[\mathcal{A}(1^\lambda, \{(\mathbf{x}_i, \mathcal{F}_\lambda(\mathbf{x}_i, \mathbf{A})\}_{i=1}^{\ell}] - \Pr[\mathcal{A}(1^\lambda, \{(\mathbf{x}_i, y_i\}_{i=1}^{\ell})] \right| = \frac{2}{3}$$

Based on the k-xor problem, we analyze $k = 3, 4$ and $k \geq 5$ cases, respectively.

Case $\boldsymbol{k} = 3$. Similar to $k = 2$, we first find vectors $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ such that $\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = \mathbf{0} \bmod 2$ using $O(2^{n/2})$ time and space. Since $\mathbf{x}_3 = \mathbf{x}_1 + \mathbf{x}_2 \bmod 2$, $f_i(\mathbf{x}_3)$ is equal to $f_i(\mathbf{x}_1) \cdot f_i(\mathbf{x}_2)$ for all $i \in [n]$ from the Lemma 5.3. Then, for such three vectors, we observe that

$$\sum_{i=1}^{3} (\mathcal{F}_{\mathbf{A}}(\mathbf{x}_i) + n) = \sum_{i=1}^{m} (f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_3)) \tag{2}$$

$$= \sum_{i=1}^{m} (f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_1) \cdot f_i(\mathbf{x}_2)) \tag{3}$$

Now, we compute a conditional probability that $\sum_{i=1}^{3} (\mathcal{F}_{\mathbf{A}}(\mathbf{x}_i) + n)$ is "zero" given that $\mathbf{x}_i$'s are uniformly sampled from $\{0,1\}^n$ such that $\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = \mathbf{0} \bmod 2$. As a result, we obtain the following theorem 5.5. We also leave the proof in the Appendix B.

Theorem 5.5 *Let λ be the security parameter, and n and m parameters of Mod-2/Mod-3 weak PRF candidate. Then, if $\ell > c_1 \cdot 2^{n/2}$ for some constant c_1, there exist roots of the 3-xor problem. Then, for a key $\mathbf{A} \overset{\$}{\leftarrow} \{0,1\}^{m\times n}$ and inputs $\mathbf{x}_i \overset{\$}{\leftarrow} \{0,1\}^n$ for all $i \in [n]$, it holds that*

$$\left| \Pr\left[\sum_{i=1}^{3} (\mathcal{F}_{\mathbf{A}}(\mathbf{x}_i) + n) = 0 \bmod 3 \mid \sum_{i=1}^{3} \mathbf{x}_i = \mathbf{0} \bmod 2 \right] - \frac{1}{3} \right| = \frac{d_m}{2^{0.60m}}$$

for some constant d_m. Therefore, there exists an adversary $\mathcal{A}$ in running time $c_2 \cdot 2^{n/2}$ for some constant c_2 such that for any $y_i \xleftarrow{\$} \mathbb{Z}_3$ $i \in [\ell]$,

$$\left|\Pr[\mathcal{A}(1^\lambda, \{(\mathbf{x}_i, \mathcal{F}_\lambda(\mathbf{x}_i, \mathbf{A})\}_{i=1}^{\ell}] - \Pr[\mathcal{A}(1^\lambda, \{(\mathbf{x}_i, y_i\}_{i=1}^{\ell})]\right| \geq \frac{d_m}{2^{0.60m}}$$

Case $\boldsymbol{k = 4}$. Except for complex computations, almost parts of the attack are the same as the analysis of $k = 3$. In this case, We can find vectors $\mathbf{x}_1, \cdots, \mathbf{x}_4$ such that $\mathbf{x}_1 + \cdots + \mathbf{x}_4 = \mathbf{0} \bmod 2$ using $O(2^{n/3})$ time and space. Let $\mathbf{x}_4 = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 \bmod 2$. Then, $f_i(\mathbf{x}_4)$ is equal to $f_i(\mathbf{x}_1) \cdot f_i(\mathbf{x}_2) \cdot f_i(\mathbf{x}_3)$ for $i \in [n]$. In a similar way to $k = 3$, we obtain the following theorem 5.5.

Theorem 5.6 *Let λ be the security parameter, and n and m parameters of Mod-2/Mod-3 weak PRF candidate. Then, if $\ell > c_1 \cdot 2^{n/3}$, there exists solutions of 4-xor problems. For a key $\mathbf{A} \xleftarrow{\$} \{0,1\}^{m \times n}$ and inputs $\mathbf{x}_i \xleftarrow{\$} \{0,1\}^n$ for all $i \in [\ell]$, it holds that*

$$\left|\Pr\left[\sum_{i=1}^{4}(\mathcal{F}_{\mathbf{A}}(\mathbf{x}_i) + n) = 0 \bmod 3 \mid \sum_{i=1}^{4}\mathbf{x}_i = \mathbf{0}\right] - \frac{1}{3}\right| = \frac{d_m}{2^{0.68m}}$$

Therefore, there exists an adversary $\mathcal{A}$ in running time $c_2 \cdot 2^{n/3}$ such that for any $y_i \xleftarrow{\$} \mathbb{Z}_3$ with $i \in [\ell]$,

$$\left|\Pr[\mathcal{A}(1^\lambda, \{(\mathbf{x}_i, \mathcal{F}_\lambda(\mathbf{x}_i, \mathbf{A})\}_{i=1}^{\ell}] - \Pr[\mathcal{A}(1^\lambda, \{(\mathbf{x}_i, y_i\}_{i=1}^{\ell})]\right| \geq \frac{d_m}{2^{0.68m}}$$

Case $\boldsymbol{k \geq 5}$. Our statistical analysis heavily depends on the bias of a conditional probability of some polynomial $G(\mathbf{x}_1, \cdots, \mathbf{x}_k)$ defined on mod 3 given by solutions of the k-xor problem. As k increases, conditional probabilities of $G(\mathbf{x}_1, \cdots, \mathbf{x}_k)$ mod 3 being $0, 1, 2$ for any G given by roots of the k-xor problem are close to $1/3$, so the advantage of statistical analysis decreases. Indeed, if $k = 5$, the advantage is already smaller than $\frac{1}{2^m}$ in our approach.

References

ABG+14. Adi Akavia, Andrej Bogdanov, Siyao Guo, Akshay Kamath, and Alon Rosen. Candidate weak pseudorandom functions in ac0◯ mod2. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 251–260, 2014.

ABSV15. Prabhanjan Ananth, Zvika Brakerski, Gil Segev, and Vinod Vaikuntanathan. From selective to adaptive security in functional encryption. In *Annual Cryptology Conference*, pages 657–677. Springer, 2015.

App14. Benny Applebaum. Bootstrapping obfuscators via fast pseudorandom functions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 162–172. Springer, 2014.

ASA17. Jacob Alperin-Sheriff and Daniel Apon. Weak is better: Tightly secure short signatures from weak prfs. *IACR Cryptol. ePrint Arch.*, 2017.

BCK96. Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *Annual international cryptology conference*, pages 1–15. Springer, 1996.

Bel15. Mihir Bellare. New proofs for nmac and hmac: security without collision resistance. *Journal of Cryptology*, 28(4):844–878, 2015.

Ber07. Daniel J Bernstein. Better price-performance ratios for generalized birthday attacks. 2007.

BHI$^+$20. Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu, and Tal Malkin. On the complexity of decomposable randomized encodings, or: How friendly can a garbling-friendly prf be? In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.

BIP$^+$18. Dan Boneh, Yuval Ishai, Alain Passelègue, Amit Sahai, and David J Wu. Exploring crypto dark matter. In *Theory of Cryptography Conference*, pages 699–729. Springer, 2018.

BLN$^+$09. Daniel J. Bernstein, Tanja Lange, Ruben Niederhagen, Christiane Peters, and Peter Schwabe. Implementing wagner's generalized birthday attack against the SHA-3 round-1 candidate FSB. *IACR Cryptol. ePrint Arch.*, 2009:292, 2009.

BR17. Andrej Bogdanov and Alon Rosen. Pseudorandom functions: Three decades later. In *Tutorials on the Foundations of Cryptography*, pages 79–158. Springer, 2017.

CHVW19. Yilei Chen, Minki Hhan, Vinod Vaikuntanathan, and Hoeteck Wee. Matrix prfs: Constructions, attacks, and applications to obfuscation. In *Theory of Cryptography Conference*, pages 55–80. Springer, 2019.

CVW18. Yilei Chen, Vinod Vaikuntanathan, and Hoeteck Wee. GGH15 beyond permutation branching programs: Proofs, attacks, and candidates. In *CRYPTO 2018, Part II*, pages 577–607, 2018.

DDKS19. Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Efficient dissection of bicomposite problems with cryptanalytic applications. *Journal of Cryptology*, 32(4):1448–1490, 2019.

Din19. Itai Dinur. An algorithmic framework for the generalized birthday problem. *Designs, Codes and Cryptography*, 87(8):1897–1926, 2019.

DKPW12. Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 355–374. Springer, 2012.

DN02. Ivan Damgåard and Jesper Buus Nielsen. Expanding pseudorandom functions; or: From known-plaintext security to chosen-plaintext security. In *Annual International Cryptology Conference*, pages 449–464. Springer, 2002.

GGM86. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

Gol86. Oded Goldreich. Two remarks concerning the goldwasser-micali-rivest signature scheme. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 104–110. Springer, 1986.

LM13. Vadim Lyubashevsky and Daniel Masny. Man-in-the-middle secure authentication schemes from lpn and weak prfs. In *Annual Cryptology Conference*, pages 308–325. Springer, 2013.

MS07. Ueli Maurer and Johan Sjödin. A fast and key-efficient reduction of chosen-ciphertext to known-plaintext security. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 498–516. Springer, 2007.

MW18. Daniele Micciancio and Michael Walter. On the bit security of cryptographic primitives. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 3–28. Springer, 2018.

NPS20. María Naya-Plasencia and André Schrottenloher. Optimal merging in quantum k-xor and k-xor-sum algorithms. In *Advances in Cryptology – EUROCRYPT 2020*, pages 311–340, Cham, 2020. Springer International Publishing.

NS15. Ivica Nikolić and Yu Sasaki. Refinements of the k-tree algorithm for the generalized birthday problem. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 683–703. Springer, 2015.

Pie09. Krzysztof Pietrzak. A leakage-resilient mode of operation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 462–482. Springer, 2009.

Wag02. David Wagner. A generalized birthday problem. In *Annual International Cryptology Conference*, pages 288–304. Springer, 2002.

A Simple Non-Adaptive Attack

In this section, we provide a simple non adaptive attack of a basic Mod-2/Mod-3 weak PRF, which runs in polynomial time n. The attack is motivated by rank attack [CVW18, CHVW19].

Assume that adversary has exponentially many samples $(\mathbf{z}_i, v_i)$. The goal is to determine whether v_i is uniformly sampled from $\mathbb{Z}_3$ or sampled from a Mod-2/Mod-3weak PRF.

Let s be an integer $> \max\{m, n\}$. Then, our attack is:

1. Find s^2 pairs of vectors $\{(\mathbf{x}_i, \mathbf{y}_j)\}_{i,j\in[s]}$ such that $\mathbf{z}_{i,j} = \mathbf{x}_i + \mathbf{y}_j$ for some $\mathbf{z}_{i,j}$ in a list of samples.
2. Construct a matrix $\mathbf{M} = (v_{i,j})$, where $v_{i,j}$ is a sample corresponding to a vector $\mathbf{z}_{i,j}$.
3. Compute a rank of $\mathbf{M}$.

When $v_{i,j}$'s are truly random, a rank of $\mathbf{M}$ is s with high probability. However, if it is of the form $\mathsf{map}(\mathbf{A} \cdot ([\mathbf{x}_i + \mathbf{y}_j)]_2)$, then a matrix $\mathbf{M}$ is divided into a product of two matrices using the Lemma 5.2.

$$\mathbf{M} = \begin{pmatrix} \mathbf{1}^T \cdot \mathbf{H}(\mathbf{x}_1) \\ \mathbf{1}^T \cdot \mathbf{H}(\mathbf{x}_2) \\ \mathbf{1}^T \cdot \mathbf{H}(\mathbf{x}_3) \\ \vdots \\ \mathbf{1}^T \cdot \mathbf{H}(\mathbf{x}_\rho) \end{pmatrix} \cdot \Big(\mathbf{H}(\mathbf{y}_1) \cdot \mathbf{1}, \mathbf{H}(\mathbf{y}_2) \cdot \mathbf{1}, \mathbf{H}(\mathbf{y}_3) \cdot \mathbf{1}, \cdots, \mathbf{H}(\mathbf{y}_\rho) \cdot \mathbf{1} \Big)$$

Hence, a rank of $\mathbf{M}$ is bounded by $\min(m, n)$ with high probability. The attack runs in $O(n)$ time and space.

The rank attack only successes when adversary is possible to use an oracle access to input queries. However, in the setting of weak PRF, inputs are selected randomly from $\{0,1\}^n$, our attack does not work anymore.

B Proofs of Theorems

In this section, we provide proofs of Lemma 5.3, Theorem 5.5 and 5.6.

Proof (of Lemma 5.3).

$$\begin{aligned}
\mathbf{H}(\mathbf{x}) \cdot \mathbf{H}(\mathbf{y}) &= \prod_{i=1}^{n} (\mathbf{I} + \mathsf{diag}(x_i \mathbf{A}_i)) \cdot \prod_{i=1}^{n} (\mathbf{I} + \mathsf{diag}(y_i \mathbf{A}_i)) \\
&= \prod_{i=1}^{n} (\mathbf{I} + \mathsf{diag}(x_i \mathbf{A}_i))(\mathbf{I} + \mathsf{diag}(y_i \mathbf{A}_i)), \\
\mathbf{H}([\mathbf{x}+\mathbf{y}]_2) &= \prod_{i=1}^{n} (\mathbf{I} + \mathsf{diag}([x_i + y_i]_2 \mathbf{A}_i))
\end{aligned}$$

It is enough to check that

$$(\mathbf{I} + \mathsf{diag}([x_i + y_i]_2 \mathbf{A}_i)) \equiv (\mathbf{I} + \mathsf{diag}(x_i \mathbf{A}_i))(\mathbf{I} + \mathsf{diag}(y_i \mathbf{A}_i)) \bmod 3. \tag{4}$$

If (x_i, y_i) is one of $(0,0), (1,0)$, and $(0,1)$, the above identity is trivial.

For the last case $(x_i, y_i) = (1,1)$, the right-hand side of an equation (4) is the identity matrix. Moreover, the left-hand side of the equation is the same as $(\mathbf{I} + \mathsf{diag}(\mathbf{A}_i))^2$. Note that $1^2 \equiv 2^2 \equiv 1 \bmod 3$, and every element of $\mathbf{A}$ is binary, it must hold that $(\mathbf{I} + \mathsf{diag}(\mathbf{A}_i))^2 \equiv \mathbf{I} \bmod 3$. Hence, the proof is completed. □

Proof (of Theorem 5.5). Let $\{\mathbf{x}_i\}_{i=1}^3$ be vectors such that $\sum_{i=1}^3 \mathbf{x}_i = \mathbf{0} \bmod 2$. Since a key $\mathbf{A}$ is randomly chosen matrix, $f_i(\mathbf{x}_k)$ and $f_j(\mathbf{x}_k)$ are independent with distinct i, j for all k.

Also, without loss of generality, assume that $\mathbf{x}_1, \mathbf{x}_2$ are mutually independent since $\mathbf{x}_3$ can be regarded as $\mathbf{x}_3 = [\mathbf{x}_1 + \mathbf{x}_2]_2$. Moreover, for sufficient large n, it could be assumed that $f_i(\mathbf{x}_k)$ is uniformly drawn from $\{1,2\}$ since for any j, k, $\Pr[f_j(\mathbf{x}_k) = 1] \approx 1/2 + 1/2^{n+1}$, and $f_j(\mathbf{x}_k)$'s are independent as stated above.

Then we easily confirm that

$$\begin{aligned}
&\Pr[f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_1) f_i(\mathbf{x}_2) \equiv 0 \bmod 3] = 1/4 \\
&\Pr[f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_1) f_i(\mathbf{x}_2) \equiv 1 \bmod 3] = 0 \\
&\Pr[f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_1) f_i(\mathbf{x}_2) \equiv 2 \bmod 3] = 3/4
\end{aligned}$$

According to an equation (2), we have that

$$\Pr\left[\sum_{i=1}^{3} (\mathcal{F}_{\mathbf{A}}(\mathbf{x}_i) + n) = 0 \bmod 3 \;\middle|\; \sum_{i=1}^{3} \mathbf{x}_i = \mathbf{0}\right]$$

$$= \frac{\sum_{i \equiv 0 \bmod 3} \binom{m}{i} \cdot 3^i}{4^m} = \frac{4^m + (3+\zeta)^m + (3+\zeta^2)^m}{3 \cdot 4^m}$$
$$= \frac{1}{3} + \left(\frac{\delta^m + \bar{\delta}^m}{3}\right) \cdot \left(\frac{\sqrt{7}}{4}\right)^m \approx \frac{1}{3} + c_m \cdot \frac{1}{2^{0.60m}}$$

where ζ is 3-th root of unity, $\frac{-1+\sqrt{3}}{2}$ and δ is $\frac{5+i\sqrt{3}}{2\sqrt{7}}$. □

Similarly, for $k = 4$, we can provide a proof by computing almost the same procedures.

Proof (of Theorem 5.6). Let $\{\mathbf{x}_i\}_{i=1}^4$ be vectors such that $\sum_{i=1}^4 \mathbf{x}_i = \mathbf{0} \bmod 2$. Since a key $\mathbf{A}$ is randomly chosen matrix, $f_i(\mathbf{x}_k)$ and $f_j(\mathbf{x}_k)$ are independent with distinct i, j for all k. Without loss of generality, assume that $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are mutually independent since $\mathbf{x}_4$ can be regarded as $\mathbf{x}_4 = [\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3]_2$. Moreover, for sufficient large n, it could be assumed that $f_i(\mathbf{x}_k)$ is uniformly drawn from $\{1, 2\}$ since for any j, k, $\Pr[f_j(\mathbf{x}_k) = 1] \approx 1/2 + 1/2^{n+1}$, and $f_j(\mathbf{x}_k)$'s are independent as stated above. Then, we observe that

$$\Pr[f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_3) + f_i(\mathbf{x}_1)f_i(\mathbf{x}_2)f_i(\mathbf{x}_3) \equiv 0 \bmod 3] = 3/4$$
$$\Pr[f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_3) + f_i(\mathbf{x}_1)f_i(\mathbf{x}_2)f_i(\mathbf{x}_3) \equiv 1 \bmod 3] = 1/8$$
$$\Pr[f_i(\mathbf{x}_1) + f_i(\mathbf{x}_2) + f_i(\mathbf{x}_3) + f_i(\mathbf{x}_1)f_i(\mathbf{x}_2)f_i(\mathbf{x}_3) \equiv 2 \bmod 3] = 1/8$$

According to similar analysis, it holds that

$$\Pr\left[\sum_{i=1}^4 (\mathcal{F}_{\mathbf{A}}(\mathbf{x}_i) + n) = 0 \bmod 3 \mid \sum_{i=1}^4 \mathbf{x}_i = \mathbf{0}\right]$$
$$= \frac{\sum_{i=0}^m \left(\binom{m}{i} 6^i \cdot \sum_{m-i+j \equiv 0 \bmod 3} \binom{m-i}{j}\right)}{8^m}$$
$$= \frac{\sum_{i=0}^m \left(\binom{m}{i} 6^i \cdot \frac{1}{3}(2^{m-i} + \zeta^{m-i}(\zeta+1)^{m-i} + \zeta^{2m-2i}(\zeta^2+1)^{m-i})\right)}{8^m}$$
$$= \frac{1}{3} + \frac{\sum_{i=0}^m \left(\binom{m}{i} 6^i \cdot ((-1)^{m-i} + (-1)^{m-i})\right)}{3 \cdot 8^m}$$
$$= \frac{1}{3} + \frac{2}{3} \cdot \left(\frac{-5}{8}\right)^m \approx \frac{1}{3} + c_m \cdot \frac{1}{2^{0.68m}},$$

where ζ is 3-th root of unity, $\frac{-1+\sqrt{3}}{2}$. □