# Multiple-Tweak Differential Attack Against SCARF

Christina Boura[1], Shahram Rasoolzadeh[2], Dhiman Saha[3] and Yosuke Todo[4]

[1] IRIF, Université Paris Cité, Paris, France
christina.boura@irif.fr
[2] Ruhr University Bochum, Bochum, Germany
shahram.rasoolzadeh@rub.de
[3] de.ci.phe.red Lab, Department of Computer Science and Engineering, Indian Institute of Technology, Bhilai, 492015, India
dhiman@iitbhilai.ac.in
[4] NTT Social Informatics Laboratories, Tokyo, Japan
yosuke.todo@ntt.com

**Abstract.** In this paper, we present the first third-party cryptanalysis of SCARF, a tweakable low-latency block cipher designed to thwart contention-based cache attacks through cache randomization. We focus on multiple-tweak differential attacks, exploiting biases across multiple tweaks. We establish a theoretical framework explaining biases for any number of rounds and verify this framework experimentally. Then, we use these properties to develop a key recovery attack on 7-round SCARF with a time complexity of $2^{76}$, achieving a 98.9% success rate in recovering the 240-bit secret key. Additionally, we introduce a distinguishing attack on the full 8-round SCARF in a multi-key setting, with a complexity of $c \times 2^{67.55}$, demonstrating that SCARF does not provide 80-bit security under these conditions. We also explore whether our approach could be extended to the single-key model and discuss the implications of different S-box choices on the attack success.

**Keywords:** SCARF · cache randomization · low latency · differential cryptanalysis · multiple-tweak differential attack

## 1 Introduction

Due to the significant disparity in performance between the CPU and main memory, a strategy used in modern CPUs is to store frequently accessed data within fast and compact memory modules, situated physically close to the cores. This form of memory, referred to as cache, has been the target of several devastating attacks in recent years. Among these attacks, those known as contention-based, exploit the internal architecture of caches and are particularly hard to prevent. A common countermeasure against them consists in randomizing the address-to-cache-index mapping by some randomization function. Such a function needs to have extremely low latency while also ensuring security.

With this objective in mind, Canale et al. designed SCARF in 2023 [CGL$^+$23], the first dedicated cache randomization cipher that achieves low latency and is cryptographically secure in the cache attacker model. Given its particular application scenario, SCARF differs significantly from traditional ciphers like the `AES` [aes01], as well as from previous low-latency designs such as `PRINCE` [BCG$^+$12] or `MANTIS` [BJK$^+$16]. Notably, SCARF is an 8-round tweakable block cipher that operates on blocks of only 10 bits, whereas traditional block ciphers utilize much larger blocks. Additionally, it employs a large 240-bit key, which is integrated into the state within a few rounds through a nonlinear key schedule and a unique function, i.e., the $G$ function.

A particularly interesting aspect of SCARF, making its security analysis a very challenging task, is its specific security model. Due to the way SCARF is meant to be employed, an attacker is able to choose the plaintexts (index part of the address) and tweaks (tag part of the address) to be encrypted, but cannot observe the ciphertexts computed. The only information an attacker can obtain is whether two ciphertexts collide. This led the designers to state a first security requirement for SCARF: If an attacker queries an oracle with message-tweak inputs $(P_1, T_1), (P_2, T_2)$ and gets as a response 1 if the ciphertext of $P_1$ encrypted with the tweak $T_1$ equals the ciphertext of $P_2$ encrypted with the tweak $T_2$ and 0 otherwise, he cannot tell if the ciphertexts were produced with SCARF parametrized with some secret key or by a tweakable random permutation with the same input/tweak/output lengths to SCARF with at most $2^{40}$ queries and at most $2^{80}$ running time.

The issue with this first security requirement, is that it does not allow cryptanalysts to use common and well-understood security arguments and techniques to assess the security of the cipher. For this reason, the designers provided a second security requirement by observing that whenever two plaintexts $P_1$ and $P_2$ and two tweaks $T_1$ and $T_2$ lead to the same ciphertext and hence satisfy $E_{T_1}(P_1) = E_{T_2}(P_2)$ then the attacker can learn the evaluation of the function $E_{T_2}^{-1} \circ E_{T_1}(P_1) = P_2$ in case of a collision and can learn that $E_{T_2}^{-1} \circ E_{T_1}(P_1) \neq P_2$ otherwise. Therefore, the second security requirement states that an attacker that asks for the computation of $C = E_{T_2}^{-1} \circ E_{T_1}(P)$ for a plaintext $P$ and a pair of tweaks $T_1, T_2$ and that is limited to $2^{40}$ queries and $2^{80}$ running time, cannot tell if the computation was done with SCARF or with a tweakable random permutation with the same input/tweak/output lengths to SCARF.

The designers of SCARF provided an extended security analysis of $E_T$ and $\tilde{E}_{T_1,T_2} = E_{T_2}^{-1} \circ E_{T_1}$ against different cryptanalysis techniques such as differential [BS90] or linear [Mat93] cryptanalysis. The small block size of SCARF, particularly facilitates the analysis against those classical attacks, especially statistical ones, as one can easily study the distribution of the different statistical properties by simply computing the relevant tables such as the Difference Distribution Table (DDT), the Linear Approximation Table (LAT) or the Boomerang Connectivity Table (BCT) [CHP$^+$18]. This is not possible for traditional ciphers with larger blocks. However, the designers' initial analysis did not identify any distinguishing attack or key-recovery attack on the full cipher. Among the different techniques against reduced-round versions of SCARF, the ones that were identified by the designers to be the most promising ones were the multiple-tweak attacks.

The objective of these attacks is to exploit the fact that the block length of SCARF is smaller than the tweak length and significantly smaller than the security level. This allows for the potential observation of a bias across multiple tweaks, indicating a property that occurs with a probability of $\frac{1}{2^n-1} + \varepsilon$, where $n$ represents the block size, even if $\varepsilon$ is much smaller than $\frac{1}{2^n-1}$. The designers of SCARF analyzed such biases occurring in the case of differential properties. For example, they observed the existence of multiple-tweak differentials for $(5+5)$-round SCARF with biases of approximately $2^{-30}$, and they also predicted the existence of multiple-tweak differentials for $(6+6)$-round SCARF with biases of about $2^{-40}$. However, these biases were only determined experimentally or through analogical reasoning, and no theoretical analysis was provided. Additionally, the designers did not propose any key recovery procedure based on these distinguishing properties.

**Our Contributions.** In this work, we provide the first third-party cryptanalysis of SCARF by focusing on multiple-tweak differential attacks for $E_{T_2}^{-1} \circ E_{T_1}$. We first provide a theoretical framework to explain the biases for any number of rounds. Our framework is based on an efficient method to compute the expected differential probability (EDP). We also show that the experimentally observed biases perfectly match the theoretical analysis for up to 5+5 rounds. Using these properties as a distinguisher, we present a key recovery attack on 7-round SCARF with a time complexity of $2^{76}$. This attack allows the recovery of the 240-bit secret key with a success probability of 98.9%. Next, we provide a distinguishing attack for the full 8-round SCARF in the multi-key setting. Our distinguishing attack has a complexity of $c \times 2^{67.55}$ for some constant $c$ and demonstrates that SCARF does not provide 80-bit security in this setting. Whether our approach leads to a distinguishing attack in the single-key model is an interesting open question. Answering this requires a deep understanding of the definition of bit security [MW18,WY21,WY23], which we discuss extensively later in this work. Finally, we examine the impact of the choice of S-box on this attack and compare the success of the attack when the actual S-box is replaced by other relevant permutations.

The rest of the article is organized as follows. In Section 2, the specifications of SCARF and its security requirements are provided together with a brief introduction to differential cryptanalysis. Section 3 presents in detail the idea of multiple-tweak differential attacks and discusses different related works. Section 4 is dedicated to analyzing the bias theoretically, while Section 5 presents our key recovery on 7-round SCARF. Section 6 discusses multi-key distinguishing attacks on full SCARF, and finally, Section 7 provides an analysis of the impact of the S-box choice on this attack.

## 2 Preliminaries

We start this section by first describing SCARF and then discussing its security requirements as stated by the designers. At the end, we briefly discuss how to compute the differential probability of a differential transition over several rounds by recalling notably the notion of excepted differential probability (EDP).

### 2.1 SCARF

SCARF (Secure CAche Randomization Function) is a tweakable block cipher designed by Canale, Güneysu, Leander, Thoma, Todo and Ueno [CGL+23]. SCARF was designed to be the first dedicated cache randomization cipher to threaten a particular class of cache attacks. It processes blocks of 10 bits and uses a 48-bit tweak and a 240-bit secret key. Its design, composed of a tweakey schedule and a data encryption part, can be visualised in Figure 1.

**Data Encryption Part.** This part takes as input a plaintext block $P \in \mathbb{F}_2^{10}$ and produces a ciphertext block $C \in \mathbb{F}_2^{10}$ by first iterating 7 times a round function $R_1$ and then applying once a different round function $R_2$, as seen in Figure 1. Each round function is parametrized by a 30-bit subkey $k$ generated by the tweakey schedule.

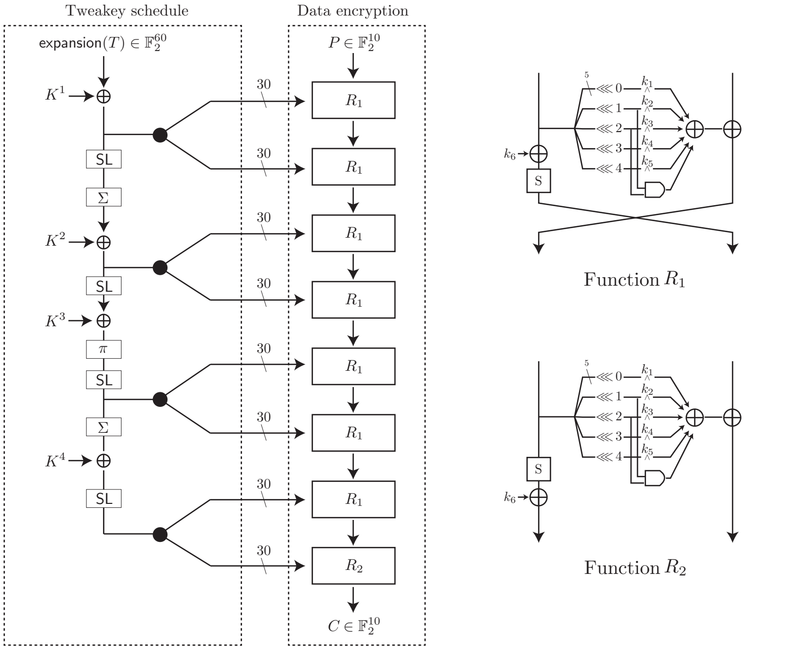

**Fig. 1.** The structure of SCARF together with its two round functions $R_1$ and $R_2$.

*Round Functions $R_1$ and $R_2$.* Both round functions follow a Feistel-like structure and take as input a 10-bit value $x$ and a 30-bit subkey $k$. The subkey $k$ can be seen as a concatenation of six 5-bit values, i.e., $k = k_6||k_5||k_4||k_3||k_2||k_1$. The value $x$ is also divided into two 5-bit halves, i.e. $x = x_L||x_R$. We further denote by $\tau_i$ the left rotation of $x$ by $i$ positions, i.e., $\tau_i(x) = x \lll i$. The function $R_1$ updates $x$ by applying the following steps:

$$\begin{aligned} y &= G(x_L, k_1, k_2, k_3, k_4, k_5) \oplus x_R, \\ x_R &= S(x_L \oplus k_6), \\ x_L &= y, \end{aligned}$$

where $G$ is

$$G(x, k_1, k_2, k_3, k_4, k_5) = \left[\bigoplus_{i=0}^{4}(\tau_i(x) \wedge k_{i+1})\right] \oplus (\tau_1(x) \wedge \tau_2(x))$$

and $S$ is a 5-bit S-box defined as

$$S(x) = \Big((\tau_0(x) \vee \tau_1(x)) \wedge (\overline{\tau_3(x)} \vee \overline{\tau_4(x)})\Big) \oplus \Big((\tau_0(x) \vee \tau_2(x)) \wedge (\overline{\tau_2(x)} \vee \tau_3(x))\Big).$$

The S-box $S$ was chosen with low-latency criteria in mind by following the framework of Rasoolzadeh [Ras22]. It has an algebraic degree 4, a differential uniformity of 4 and a linearity of 12.

The final round function $R_2$ is very similar to $R_1$. Indeed, the only differences in $R_2$ is that the order of applying the S-box and the key addition with $k_6$ is swapped with respect to $R_1$ and the swap of the branches is omitted:

$$\begin{aligned} x_R &= G(x_L, k_1, k_2, k_3, k_4, k_5) \oplus x_R, \\ x_L &= S(x_L) \oplus k_6. \end{aligned}$$

Both round functions are depicted in Figure 1.

**Tweakey Schedule.** The tweakey schedule takes as input a 48-bit tweak $T$ and a 240-bit secret key $K = K^1||K^2||K^3||K^4$, where $K^i \in \mathbb{F}_2^{60}$, $i = 1, 2, 3, 4$ and produces four tweakey values $T^1, T^2, T^3, T^4$ of 60 bits each by applying the following algorithm:

$$\begin{aligned} T^1 &= \text{expansion}(T) \oplus K^1, \\ T^2 &= \mathit{\Sigma}(\text{SL}(T^1)) \oplus K^2, \\ T^3 &= \text{SL}(\pi(\text{SL}(T^2) \oplus K^3)), \\ T^4 &= \text{SL}(\mathit{\Sigma}(T^3) \oplus K^4). \end{aligned}$$

The role of the expansion function is to extend the 48-bit tweak to a 60-bit value as follows:

$$\begin{aligned} \text{expansion}(T) = 0 \,||\, &T[48] \,||\, T[47] \,||\, T[46] \,||\, T[45] \,|| \\ 0 \,||\, &T[44] \,||\, T[43] \,||\, T[42] \,||\, T[41] \,|| \cdots || \\ 0 \,||\, &T[4] \,||\, T[3] \,||\, T[2] \,||\, T[1]. \end{aligned}$$

The function $\Sigma$ is a linear function defined as

$$\Sigma(x) = x \oplus \tau_6(x) \oplus \tau_{12}(x) \oplus \tau_{19}(x) \oplus \tau_{29}(x) \oplus \tau_{43}(x) \oplus \tau_{51}(x).$$

The function SL is just the application six times in parallel of the S-box $S$ defined above. Finally, $\pi$ is a bit-permutation, mapping $x_i$ to $x_{P[i]}$, where $P$ is given by

$$\begin{aligned} P = {} & 1, 6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, \\ & 2, 7, 12, 17, 22, 27, 32, 37, 42, 47, 52, 57, \\ & 3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58, \\ & 4, 9, 14, 19, 24, 29, 34, 39, 44, 49, 54, 59, \\ & 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60. \end{aligned}$$

Once the four tweakeys $T^1, T^2, T^3$ and $T^4$ have been computed, each of them is split into two equal parts and each part forms a 30-bit subkey $rk_i$, for the $i$-th round ($i = 1, \ldots, 8$):

$$rk_2 \,||\, rk_1 = T_1, \qquad rk_4 \,||\, rk_3 = T_2, \qquad rk_6 \,||\, rk_5 = T_3, \qquad rk_8 \,||\, rk_7 = T_4.$$

### 2.2 Security Claims

Because of the specific application scenario SCARF was designed for, the attacker model is very different from the models cryptanalysts have traditionally dealt with for more classical ciphers and applications. In particular, while an attacker can choose the message and the tweak, he can never observe the ciphertext produced. The only thing an attacker can observe is whether a cache hit or a cache miss occurred, which corresponds to detecting ciphertext collisions.

The first security requirement stated by the designers for SCARF, given below, specifies that if an attacker can choose plaintexts and tweaks and can observe whether a collision in the ciphertexts occurs, he should not be able to distinguish between SCARF and a tweakable random permutation of the same dimensions. This is under the condition that the attacker is allowed at most $2^{40}$ queries and his computation time does not exceed $2^{80}$.

**Security Requirement 1 [CGL+23].** Let $O_{real}$ be the oracle in the real world that takes addresses $(x_1, T_1)$ and $(x_2, T_2)$, and returns 1 if $E_{T_1}(x_1) = E_{T_2}(x_2)$ and 0 otherwise, where $E$ is SCARF. Let $O_{ideal}$ be the oracle in the ideal world that takes addresses $(x_1, T_1)$ and $(x_2, T_2)$, and returns 1 if $\Pi_{T_1}(x_1) = \Pi_{T_2}(x_2)$ and 0 otherwise, where $\Pi$ is a tweakable random permutation with the same input/tweak/output lengths to SCARF. An adversary is allowed to make at most $2^{40}$ queries. Then, the adversary running in time at most $2^{80}$ cannot distinguish the real from the ideal world.

The above security requirement is quite uncommon compared to the security requirements for more traditional ciphers. Furthermore, it is not clear how cryptanalysts can use well-known methods and tools to assess the security of SCARF under this requirement. For this reason, the designers transformed the problem of collision detection into a problem that is easier to study from a cryptanalytic point of view. Indeed, if the attacker detects that for two plaintexts $P_1$ and $P_2$ and for two tweaks $T_1$ and $T_2$, the corresponding ciphertexts $C_1 = E_{T_1}(P_1)$ and $C_2 = E_{T_2}(P_2)$ collide, then this equivalently means that $P_2$ is the decryption of $C_1 = C_2$ under $T_2$, that is $P_2 = E_{T_2}^{-1} \circ E_{T_1}(P_1)$.

So we can now suppose that an attacker can query

$$\tilde{E}_{T_1,T_2}(P) := E_{T_2}^{-1} \circ E_{T_1}(P) = C,$$

for a chosen plaintext $P$ and for two chosen tweaks $T_1, T_2$. The second security requirement stated by the designers is that an attacker that can do at most $2^{40}$ queries and whose computation time is bounded by $2^{80}$ cannot distinguish whether he is interacting with SCARF or with a tweakable random permutation with the same length parameters as SCARF.

**Security Requirement 2 [CGL+23].** Let $\tilde{O}_{real}$ be the oracle in the real world that takes a plaintext $P$ and a pair of tweaks $T_1, T_2$ as input and returns $C$ such that $C = E_{T_2}^{-1} \circ E_{T_1}(P)$, where $E$ is SCARF. Let $\tilde{O}_{ideal}$ be the oracle in the ideal world that takes a plaintext $P$ and a pair of tweaks $T_1, T_2$ as input and returns $C$ such that $C = \mathit{\Pi}_{T_2}^{-1} \circ \mathit{\Pi}_{T_1}(P)$, where $\mathit{\Pi}$ is a tweakable random permutation with the same input/tweak/output lengths to SCARF. An adversary is allowed to make at most $2^{40}$ queries. Then, the adversary running in time at most $2^{80}$ cannot distinguish the real from the ideal world.

Our analysis tackles mainly this second security requirement but we will eventually discuss the impact of our distinguishers and attacks on the first security requirement too.

### 2.3 Differential Cryptanalysis and Expected Differential Probability

Differential cryptanalysis exploits the existence of high-probability differentials for a reduced-round version of the target cipher. Let $E_k$ be a $n$-bit block cipher parametrized by a secret key $k$. We will write $\alpha \xrightarrow{E_k} \beta$ to denote that an input difference $\alpha$ propagates to an output difference $\beta$ through $E_k$. The couple $(\alpha, \beta)$ is called a *differential* for $E_k$.

We now define the notions of differential probability and expected differential probability (EDP) for $E_k$.

**Definition 1 (Differential Probability).** *Let $E_k$ be a $n$-bit block cipher and let $\alpha, \beta \in \mathbb{F}_2^n$. The (fixed-key)* differential probability *of the differential $(\alpha, \beta)$ over $E_k$ is defined as*

$$\mathrm{DP}[a \xrightarrow{E_k} b] := \frac{|\{x \in \mathbb{F}_2^n : E_k(x) \oplus E_k(x \oplus \alpha) = \beta\}|}{2^n}.$$

As the key is unknown to the attacker, what he is aiming to compute is what is called the expected differential probability (EDP) which is defined as the average of the probabilities, taken over all keys, of a differential $(\alpha, \beta)$.

**Definition 2 (Expected Differential Probability).** *Let $E$ be a $n$-bit block cipher and let $\alpha, \beta \in \mathbb{F}_2^n$. The* expected differential probability *of the differential $(\alpha, \beta)$ over $E$ is defined as*

$$\mathrm{EDP}[\alpha \xrightarrow{E} \beta] := 2^{-\kappa} \times \sum_{k \in \mathbb{F}_2^\kappa} \mathrm{DP}[a \xrightarrow{E_k} b],$$

*which is the average over all keys $k \in \mathbb{F}_2^\kappa$, where it is assumed that the keys are uniformly distributed.*

If the block size is sufficiently small, it is possible to compute the EDP over a single round of the cipher, for all possible input differences $\alpha$ and all possible output differences $\beta$ and store these values in a $2^n \times 2^n$ matrix. Then, by considering each round key to be independent, one can compute the probability of any transition over several rounds, by simply computing the powers of this EDP matrix [LMM91].

## 3 Multiple-Tweak Differential Attack

The designers of SCARF identified the multiple-tweak differential cryptanalysis as being one of the most powerful attack strategies against this design. The idea is to observe for some well-chosen differences $\alpha$ and $\beta$, a bias $\varepsilon$ such that

$$\Pr_{x,T_1,T_2}\left(\tilde{E}_{T_1,T_2}(x) \oplus \tilde{E}_{T_1,T_2}(x \oplus \alpha) = \beta\right) = p + \varepsilon,$$

where $p = \frac{1}{2^n-1}$, e.g., $p = \frac{1}{1023}$ for SCARF. When we use $M$ pairs, assuming a binomial distribution, the average of the empirical number of pairs satisfying the differential is $M \times (p+\varepsilon)$, and the variance is $M \times (p+\varepsilon)\,(1-(p+\varepsilon))$. The main focus of the multiple-tweak differential attack is the case where $\varepsilon \ll p$. Then, the variance is approximated by $M \times 2^{-n}$. To distinguish from the ideal case, i.e., $\varepsilon = 0$, we need to use at least $\varepsilon^{-2} \times 2^{-n}$ pairs. Moreover, we approximate the binomial distribution to the normal distribution to estimate the distinguishing advantage, similar to what is done in linear cryptanalysis. Namely, we use the following distributions.

$$\begin{cases} \mathcal{N}(M\,(p+\varepsilon)\,,\; M \times 2^{-n}), & \text{real} \\ \mathcal{N}(M \times p,\; M \times 2^{-n}), & \text{ideal.} \end{cases}$$

The designers of SCARF developed an efficient algorithm that constructs $\left(\frac{N_T}{2}\right)^2 \times 2^9$ pairs with a query/time complexity of $N_T \times 2^{10}$ and $2^{20}$ memory only. They used $N_T = 2^{23}$, i.e., $M = 2^{55}$ pairs, and experimentally observed the bias up to 5+5 rounds, where this notation means that the cipher $\tilde{E}_{T_1,T_2}$ is restricted to 5 rounds for $E_{T_1}$ and 5 rounds for $E_{T_2}^{-1}$. In particular, for $\alpha = \beta = (\mathtt{0x001}, \mathtt{0x001})$, the observed bias for each round $(r+r)$, $r = 2, 3, 4, 5$ was:

| Round | Bias $\varepsilon$ |
|---|---|
| 2+2 | $2^{-9.6792}$ |
| 3+3 | $2^{-14.6761}$ |
| 4+4 | $2^{-24.8467}$ |
| 5+5 | $2^{-29.8025}$ |

The designers did not provide a theoretical explanation for the observed bias. They expected the bias to be close to $2^{-40}$ in 6+6 rounds, but their experiments could not permit to observe a differential bias due to the extremely high computational complexity. One of the goals in this paper is to provide a theoretical explanation for the experimentally observed differential bias for any number of rounds and in particular to estimate the bias for more than 6+6 rounds.

### 3.1 LLR Statistic

A multiple-tweak multiple-differential attack is a natural extension of a multiple-tweak differential attack. The idea is to exploit multiple differences instead of a single one. Nowadays, we have substantial knowledge about this type of extension in the context of linear cryptanalysis [BJV04] or differential cryptanalysis [BGN12].

The Log-Likelihood Ratio (LLR) is a classical approach to hypothesis testing. It is used to compare the goodness of fit between two competing hypotheses. Specifically, it compares the likelihood of the data under one hypothesis (usually the null hypothesis) to the likelihood of the data under an alternative hypothesis.

We assume that each differential bias is statistically independent for each pair of $\alpha$ and $\beta$. Let $V$ be a set of pairs of input and output differences. Then, the LLR statistic in the case of a multiple-tweak multiple-differential attack can be computed as:

$$LLR = \sum_{(\alpha,\beta)\in V} N(\alpha,\beta) \times \log \frac{p + \varepsilon_{\alpha,\beta}}{p} \approx \sum_{(\alpha,\beta)\in V} N(\alpha,\beta) \times \frac{\varepsilon_{\alpha,\beta}}{p},$$

where $N(a, b)$ denotes the number of pairs satisfying the differential transition from $\alpha$ to $\beta$.

**Definition 3 (KL Divergence).** *Let $q$ and $q'$ be two probability distribution vectors over $V$. The* Kullback-Leibler divergence *between $q$ and $q'$ is defined as*

$$D(q\|q') := \sum_{v\in V} q_v \times \log\left(\frac{q_v}{q'_v}\right)$$

*We also define the following metrics*

$$D_2(q\|q') := \sum_{v\in V} q_v \times \log^2\left(\frac{q_v}{q'_v}\right) \quad \text{and} \quad \varDelta D(q\|q') := D_2(q\|q') - D(q\|q')^2$$

In our case, $q = p + \varepsilon$ and $q' = p$. The notion of KL divergence can be used to prove that the LLR statistic asymptotically tends towards a normal distribution. The mean and variance exhibit the following properties.

**Proposition 1 (Proposition 3 in [BJV04]).** *The distributions of LLR asymptotically tend toward a normal distribution as the number of samples $M$ increases. If samples are obtained from the real (resp. ideal) distribution, the LLR statistic tends toward $\mathcal{N}(M\mu_0, M\sigma_0^2)$ (resp. $\mathcal{N}(M\mu_1, M\sigma_1^2)$), where*

$$\begin{aligned}
\mu_0 &= D(q\|q') = \sum_{(\alpha,\beta)\in V} (p + \varepsilon_{\alpha,\beta}) \times \log \frac{p + \varepsilon_{\alpha,\beta}}{p}, \\
\mu_1 &= -D(q'\|q) = \sum_{(\alpha,\beta)\in V} p \times \log \frac{p + \varepsilon_{\alpha,\beta}}{p}, \\
\sigma_0^2 &= \mathit{\Delta} D(q\|q') = \left( \sum_{(\alpha,\beta)\in V} (p + \varepsilon_{\alpha,\beta}) \times \log^2 \frac{p + \varepsilon_{\alpha,\beta}}{p} \right) - \mu_0^2, \\
\sigma_1^2 &= \mathit{\Delta} D(q'\|q) = \left( \sum_{(\alpha,\beta)\in V} p \times \log^2 \frac{p + \varepsilon_{\alpha,\beta}}{p} \right) - \mu_1^2.
\end{aligned}$$

In our case, $|\varepsilon_{\alpha,\beta}| \ll p$ and $\left(\sum \varepsilon_{\alpha,\beta}\right)^2 \ll p^{-1} \times \sum \varepsilon_{\alpha,\beta}^2$ hold. Then approximately, we have

$$\mu_0 - \mu_1 \approx \sigma_0^2 \approx \sigma_1^2 \approx \frac{1}{p} \times \sum_{(\alpha,\beta)\in V} \varepsilon_{\alpha,\beta}^2.$$

We sometimes refer to the quantity $\frac{1}{p} \times \sum_{(\alpha,\beta)\in V} \varepsilon_{\alpha,\beta}^2$ as *capacity*. Roughly, the number of required samples, $M$, must be at least the inverse of the capacity to be able to distinguish between two distributions using the LLR statistic.

### 3.2 Related Works

The concept of a multiple-tweak differential attack is not entirely novel. Patarin, in particular, discussed this in the context of Feistel ciphers using several permutations [Pat01,Pat04,Pat08]. A similar attack was also discussed against format-preserving encryption [DKLS20].

*Generic Attacks against the Luby-Rackoff Construction.* Patarin's work provides a precise differential bias of the so-called Luby-Rackoff construction, which is a Feistel cipher instantiated with pseudo-random functions. However, SCARF is not a Feistel cipher and contains an S-box. Moreover, the $G$ function and the S-box are fully specified, and cannot be regarded as pseudo-random functions. Therefore, we cannot directly use Patarin's approach in our work.

*Attack against Feistel-Based Format-Preserving Encryption.* Dunkelman et al. discussed the same attack in [DKLS20]. They provided a more straightforward method to estimate the differential bias. First, similar to traditional differential attacks, they focused on the following two-round iterative trail

$$(\delta, 0) \xrightarrow[prob.=2^{-n}]{\text{1 round}} (0, \delta) \xrightarrow[prob.=1]{\text{1 round}} (\delta, 0).$$

Assuming that pairs that do not satisfy this trail behave randomly, the probability such that $(0, \delta)$ transits to $(0, \delta)$ by $2r$ rounds is estimated as $2^{-2n} + 2^{-nr}$. A truncated differential allows for extension by additional two rounds as

$$(0, \delta) \xrightarrow[prob.=1]{\text{1 round}} (\delta, 0) \xrightarrow[prob.=2^{-n}]{2r \text{ rounds}} (\delta, 0) \xrightarrow[prob.=1]{\text{1 round}} (*, \delta),$$

and they estimated this probability to be $2^{-n} + 2^{-nr}$. In conclusion, while their estimation requires assumptions, the result is almost identical to Patarin's result.

Since the estimation focusing on the trail provides a good estimation for Feistel ciphers, we tried to estimate the bias of SCARF by using this method. Unfortunately, such an estimation leads to completely inaccurate results. We discuss this case in Appendix B.

## 4 Efficient Estimation of the Differential Bias of SCARF

Because of the heavy tweakey-schedule, it is natural to assume that each round function of SCARF is independent. Then, the expected differential probability (EDP) can be computed as the power of the so-called EDP matrix [LMM91,BDD$^+$23] (see Section 2.3). For $n$-bit block ciphers, one constructs an $2^n \times 2^n$ matrix, and the EDP is evaluated as a power of this matrix. This computation can be done with complexity $2^{3n}$.

Usually, this method is not computationally feasible for common block ciphers with typical block sizes of 64, 128, or 256 bits. However, the block size of SCARF is 10 bits, so the above computation requires only $2^{30}$ operations and can thus be performed in practice. Nevertheless, we propose a more efficient algorithm for this computation, as $2^{30}$ operations, while feasible, remain inefficient.

We focus on differential transitions from $\alpha = (\alpha^L, \alpha^R)$ to $\beta = (\beta^L, \beta^R)$ on $\tilde{E}$. We write

$$\alpha \xrightarrow{R+R'} \beta$$

where $\tilde{E}$ is the enc-then-dec structure whose encryption and decryption are composed of $R$ and $R'$ rounds, respectively. Moreover,

$$\mathrm{EDP}[\alpha \xrightarrow{R+R'} \beta]$$

denotes the expected differential probability of the differential transition.

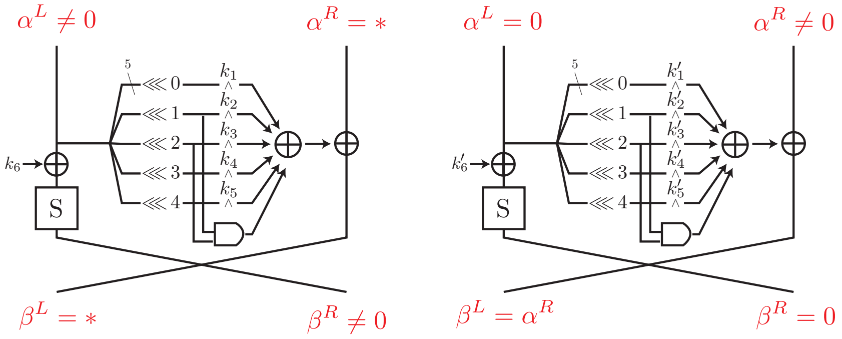

**Fig. 2.** Differential transitions for $R_1$

When the round numbers $R$ and $R'$ are explicit from the context, we will simply write $p_{\alpha,\beta}$ to denote the expected differential probability of the transition from $\alpha$ to $\beta$. Let $\varepsilon_{\alpha,\beta}$ be the differential bias, i.e., $p_{\alpha,\beta} = \frac{1}{1023} + \varepsilon_{\alpha,\beta}$.

To evaluate the EDP efficiently, we fully exploit the structure of SCARF, particularly the property of the $G$ function. As a result, we show that we can evaluate the EDP from all $\alpha$ to all $\beta$ with a complexity of $2^{15}$. This complexity improvement is important as, in Section 7, we discuss how the use of an alternative S-box could improve the security against the proposed attacks. To find the S-box that would provide the higher resistance, we need to estimate the EDP for many S-box candidates. This is the reason why the efficiency of this computation is important, as we need to repeat it several times.

### 4.1 Some Unique Properties of SCARF

Before analyzing SCARF in detail, we first describe the differential properties of the $G$ function. By averaging on the keys, the differential probability of the $G$ function is

$$\mathrm{EDP}[\alpha \xrightarrow{G} \beta] = \begin{cases} 2^{-5}, & \text{if } \alpha \neq 0, \beta = *, \\ 1, & \text{if } \alpha = 0, \beta = 0, \\ 0, & \text{if } \alpha = 0, \beta \neq 0, \end{cases}$$

where $*$ denotes an arbitrary difference (including the zero difference). Therefore, the differential probability for $R_1$ from $\alpha = (\alpha^L, \alpha^R)$ to $\beta = (\beta^L, \beta^R)$ is

$$\mathrm{EDP}[\alpha \xrightarrow{R_1} \beta] = \begin{cases} P_S[\alpha^L, \beta^R] \times 2^{-5}, & \text{if } \alpha^L \neq 0, \\ 1, & \text{if } \alpha^L = 0 \text{ and } (\beta_L, \beta_R) = (\alpha_R, 0), \\ 0, & \text{if } \alpha^L = 0 \text{ and } (\beta_L, \beta_R) \neq (\alpha_R, 0), \end{cases}$$

where $P_S[\alpha^L, \beta^R]$ denotes the differential probability for the S-box.

Table 7 in Appendix A shows the difference distribution table (DDT) of the S-box of SCARF. Figure 2 shows each differential transition. Interestingly, when $\alpha^L \neq 0$, the differential probability is independent of $\alpha^R$ and $\beta^L$.

More importantly, when considering the composition of $R_1$ with some arbitrary permutation $F$, the EDP of $F \circ R_1$ does not depend on $\alpha^R$ in the case $\alpha^L \neq 0$. This is demonstrated in the following lemma.

**Lemma 1.** *Let $F$ denote an arbitrary permutation from $\mathbb{F}_2^{10}$ to $\mathbb{F}_2^{10}$. Then, the EDP of the differential transition from $\alpha = (\alpha^L, \alpha^R)$ to $\beta = (\beta^L, \beta^R)$ for $F \circ R_1$ does not depend on $\alpha^R$ in the case $\alpha^L \neq 0$.*

*Proof.* Suppose $\alpha^L \neq 0$. Then,

$$\begin{aligned}\mathrm{EDP}[\alpha \xrightarrow{F \circ R_1} \beta] &= \sum_{\gamma} \mathrm{EDP}[\alpha \xrightarrow{R_1} \gamma] \times \mathrm{EDP}[\gamma \xrightarrow{F} \beta] \\ &= \sum_{\gamma} 2^{-5} \times P_S[\alpha^L, \gamma^R] \times \mathrm{EDP}[\gamma \xrightarrow{F} \beta].\end{aligned}$$

We see indeed from the above formula that $\alpha^R$ is not involved in the evaluation of the EDP of $\alpha \xrightarrow{F \circ R_1} \beta$. □

In Lemma 1, $R_1$ is applied before $F$. However, a similar property holds if $R_1^{-1}$ is applied after $F$. Then, the EDP of the differential transition from $\alpha = (\alpha^L, \alpha^R)$ to $\beta = (\beta^L, \beta^R)$ for $R_1^{-1} \circ F$ does not depend on $\beta^R$ in the case $\beta^L \neq 0$.

### 4.2 Analysis for 1+1 Rounds

Although it is straightforward, we begin our discussion with this case. For any non-zero $\alpha$ and $\beta$, it holds that

$$\mathrm{EDP}[\alpha \xrightarrow{1+1} \beta] = \begin{cases} 1, & \alpha = (0, \alpha^R), \beta = (0, \beta^R), \alpha^R = \beta^R, \\ 0, & \alpha = (0, *), \beta = (\beta^L, *), \beta^L \neq 0, \\ 0, & \alpha = (\alpha^L, *), \beta = (0, *), \alpha^L \neq 0, \\ P_{\tilde{S}}[\alpha^L, \beta^L] \times 2^{-5}, & \alpha = (\alpha^L, *), \beta = (\beta^L, *), \alpha^L \neq 0, \beta^L \neq 0, \end{cases}$$

where $*$ denotes an arbitrary difference (including the zero difference). The first three cases are trivial.

For the last equation, since $k_{8,6} \oplus k'_{8,6}$ is a variable depending on the tweak value in the multiple-tweak differential attack, the EDP from $\alpha^L$ to $\beta^L$ is

$$P_{\tilde{S}}(\alpha^L, \beta^L) = \frac{\#\{(x, k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5 \mid S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha^L) \oplus k) = \beta^L\}}{2^5 \times 2^5}.$$

Table 8 in Appendix A shows the number of solutions of the equation

$$\#\{(x, k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5 \mid S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha^L) \oplus k) = \beta^L\}$$

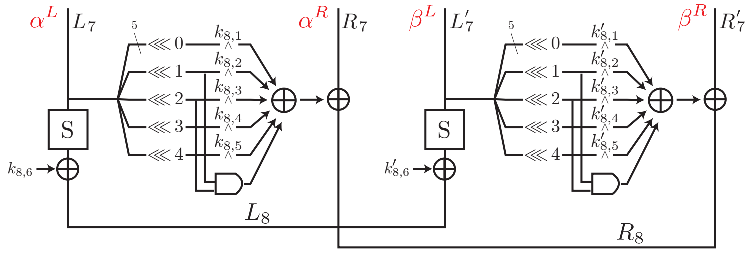

**Fig. 3.** Differential transitions from $\alpha$ to $\beta$ through 1+1 rounds.

for all possible differences $\alpha^L$ and $\beta^L$. This table can be seen as a special form of DDT for $\tilde{S} = S^{-1} \circ S(\cdot \oplus k)$ that takes the values of the key into account.

The probability that $R'_7$ (see Fig. 3) has zero difference, i.e., $\Delta R'_7 = 0$, is

$$\sum_{\gamma \in \mathbb{F}_2^5} \mathrm{EDP}[\alpha^L \xrightarrow{G} \gamma] \times \mathrm{EDP}[\beta^L \xrightarrow{G} \gamma].$$

Due to the property of the $G$ function, by averaging on the keys, the expected differential probability of any non-zero input difference to any output difference (including the zero difference) is $2^{-5}$. Therefore, the probability is $2^{5-5-5} = 2^{-5}$.

### 4.3 Analysis for $R + R'$ Rounds

Recall Lemma 1. The EDP from $\alpha$ to $\beta$ through $F \circ R_1$ is determined independently of $\alpha^R$ when $\alpha^L \neq 0$. Similarly, the EDP from $\alpha$ to $\beta$ for $R_1^{-1} \circ F$ is determined independently of $\beta^R$ when $\beta^L \neq 0$. Taking these properties into account, we obtain the following proposition, since SCARF is represented as $R_1^{-1} \circ F \circ R_1$.

**Proposition 2.** *When $\alpha^L \neq 0$, the* $\mathrm{EDP}[(\alpha^L, \alpha^R) \xrightarrow{R+R'} (\beta^L, \beta^R)]$ *does not depend on $\alpha^R$. Similarly, when $\beta^L \neq 0$, the* $\mathrm{EDP}[(\alpha^L, \alpha^R) \xrightarrow{R+R'} (\beta^L, \beta^R)]$ *does not depend on $\beta^R$.*

The proof of Proposition 2 is trivial due to Lemma 1. Proposition 2 implies that instead of computing all EDPs from $\alpha \to \beta$, considering the following four cases is enough:

$$\mathrm{EDP}[(0, \alpha^R) \xrightarrow{R+R'} (0, \beta^R)], \qquad \mathrm{EDP}[(0, \alpha^R) \xrightarrow{R+R'} (\beta^L, *)],$$
$$\mathrm{EDP}[(\alpha^L, *) \xrightarrow{R+R'} (0, \beta^R)], \qquad \mathrm{EDP}[(\alpha^L, *) \xrightarrow{R+R'} (\beta^L, *)].$$

Here, $*$ denotes any arbitrary difference, and Proposition 2 shows that these EDPs are determined independently of the value of $*$. While the size of the full EDP matrix is $1023 \times 1023$, considering only four $31 \times 31$ matrices is enough to compute each EDP.

Note that $\mathrm{EDP}[\alpha \xrightarrow{1+1} \beta]$ also satisfies the same property. Namely,

$$\begin{aligned}
\mathrm{EDP}[(0,\alpha^R) &\xrightarrow{1+1} (0,\beta^R)] = 1, \quad \text{if} \quad \alpha^R = \beta^R \\
\mathrm{EDP}[(0,\alpha^R) &\xrightarrow{1+1} (\beta^L,*)] = 0 \\
\mathrm{EDP}[(\alpha^L,*) &\xrightarrow{1+1} (0,\beta^R)] = 0 \\
\mathrm{EDP}[(\alpha^L,*) &\xrightarrow{1+1} (\beta^L,*)] = P_{\tilde{S}}[\alpha^L,\beta^L] \times 2^{-5}.
\end{aligned}$$

Given four EDP matrices for $R+R'$ rounds, it is easy to compute four EDP matrices for $R+(R'+1)$ rounds or $(R+1)+R'$ rounds. Specifically, to compute four EDP matrices for $(R+1)+R'$ rounds, we have

$$\begin{aligned}
\mathrm{EDP}[(0,\alpha^R) \xrightarrow{R+(R'+1)} (0,\beta^R)] &= \mathrm{EDP}[(0,\alpha^R) \xrightarrow{R+R'} (\beta^R,0)], \\
\mathrm{EDP}[(0,\alpha^R) \xrightarrow{R+(R'+1)} (\beta^L,*)] &= \sum_{\gamma^R \neq 0} 2^{-5} \times P_S[\beta^L,\gamma^R] \times \mathrm{EDP}[(0,\alpha^R) \xrightarrow{R+R'} (0,\gamma^R)] \\
&\quad + \sum_{\gamma^L \neq 0} 2^{-5} \times \mathrm{EDP}[(0,\alpha^R) \xrightarrow{R+R'} (\gamma^L,*)], \\
\mathrm{EDP}[(\alpha^L,*) \xrightarrow{R+(R'+1)} (0,\beta^R)] &= \mathrm{EDP}[(\alpha^L,*) \xrightarrow{R+R'} (\beta^R,0)], \\
\mathrm{EDP}[(\alpha^L,*) \xrightarrow{R+(R'+1)} (\beta^L,*)] &= \sum_{\gamma^R \neq 0} 2^{-5} \times P_S[\beta^L,\gamma^R] \times \mathrm{EDP}[(\alpha^L,*) \xrightarrow{R+R'} (0,\gamma^R)] \\
&\quad + \sum_{\gamma^L \neq 0} 2^{-5} \times \mathrm{EDP}[(\alpha^L,*) \xrightarrow{R+R'} (\gamma^L,*)].
\end{aligned}$$

In a similar way, we can compute the $\mathrm{EDP}[\alpha \xrightarrow{(R+1)+R'} \beta]$. Given $\alpha$, $\beta$, and four EDP matrices for $R+R'$ rounds, the complexity to update four EDP matrices as above is approximately $4 \times 2^{15}$.

**Summary of the Results.** For an arbitrary number of rounds $R$, we can obtain the EDP for $R+R$ rounds very efficiently. On the other hand, we notice that $\mathrm{EDP}[(0,\alpha^R) \xrightarrow{R+R} (0,\beta^R)]$ is significantly more biased than the others. This is not surprising, as their EDPs are equal to $\mathrm{EDP}[(\alpha^R,0) \xrightarrow{(R-1)+(R-1)} (\beta^R,0)]$.

Tables 1 and 2 summarize differential biases computed by EDPs for 2+2 and 3+3 rounds, respectively. Each row corresponds to a value of $\alpha^R$ and each column to a value of $\beta^R$. The values of $\alpha^L$ and $\beta^L$ are fixed to 0. Differential biases for other number of rounds are summarized in Appendix C.

Table 3 summarizes the capacity of the differential biases for different numbers of rounds. Note that, the capacities $C$ and $C_{all}$ are estimated as

$$C = 1023 \times \sum_{\alpha^R \neq 0} \sum_{\beta^R \neq 0} \varepsilon^2_{(0,\alpha^R),(0,\beta^R)}, \tag{1}$$

**Table 1.** Summary of differential bias for 2+2 rounds. Each element of this table corresponds to $-\log_2(|\varepsilon|)$ for a differential bias $\varepsilon$. The elements colored in light-blue have a negative bias, i.e., $\varepsilon < 0$.

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 9.68 | 12.99 | 11.41 | 13.01 | 13.01 | 20.00 | 20.00 | 13.01 | 11.41 | 12.01 | 13.01 | 20.00 | 11.99 | 12.01 | 12.99 | 12.99 | 20.00 | 12.01 | 12.99 | 13.01 | 12.99 | 11.99 | 20.00 | 20.00 | 12.01 | 20.00 | 12.99 | 13.01 | 12.01 | 11.99 | 20.00 |
| 02 | 12.99 | 9.68 | 20.00 | 12.99 | 12.01 | 11.41 | 12.99 | 13.01 | 13.01 | 13.01 | 12.99 | 20.00 | 11.99 | 20.00 | 20.00 | 13.01 | 20.00 | 11.41 | 12.01 | 12.01 | 20.00 | 13.01 | 12.99 | 20.00 | 13.01 | 11.99 | 12.01 | 12.01 | 11.99 | 12.99 | 20.00 |
| 03 | 11.41 | 20.00 | 9.68 | 20.00 | 12.99 | 12.01 | 11.99 | 20.00 | 12.99 | 11.99 | 20.00 | 11.42 | 20.00 | 12.01 | 20.00 | 20.00 | 12.01 | 20.00 | 13.01 | 11.99 | 20.00 | 20.00 | 11.42 | 11.42 | 20.00 | 20.00 | 20.00 | 12.99 | 11.99 | 12.99 | 11.41 |
| 04 | 13.01 | 12.99 | 20.00 | 9.68 | 11.41 | 20.00 | 12.01 | 12.99 | 12.01 | 12.01 | 20.00 | 11.41 | 13.01 | 12.99 | 12.99 | 13.01 | 20.00 | 13.01 | 13.01 | 13.01 | 11.99 | 12.99 | 12.01 | 20.00 | 12.01 | 11.99 | 11.99 | 20.00 | 12.99 | 20.00 | 20.00 |
| 05 | 13.01 | 12.01 | 12.99 | 11.41 | 9.68 | 20.00 | 11.99 | 13.01 | 20.00 | 12.99 | 12.99 | 12.99 | 12.01 | 13.01 | 11.99 | 12.01 | 11.99 | 12.99 | 20.00 | 20.00 | 11.00 | 12.99 | 13.01 | 11.99 | 11.99 | 20.00 | 20.00 | 13.01 | 12.99 | 12.01 | 13.01 |
| 06 | 20.00 | 11.41 | 12.01 | 20.00 | 20.00 | 9.68 | 13.01 | 20.00 | 11.99 | 12.99 | 20.00 | 12.01 | 20.00 | 11.99 | 11.42 | 20.00 | 11.42 | 12.99 | 20.00 | 11.99 | 20.00 | 20.00 | 20.00 | 11.42 | 12.99 | 20.00 | 11.99 | 12.01 | 12.99 | 20.00 | 11.41 |
| 07 | 20.00 | 12.99 | 11.99 | 12.01 | 11.99 | 13.01 | 9.42 | 13.01 | 13.01 | 20.00 | 12.99 | 20.00 | 12.99 | 12.01 | 11.99 | 12.01 | 12.01 | 13.01 | 12.01 | 11.99 | 11.41 | 20.00 | 20.00 | 12.99 | 11.99 | 11.41 | 13.01 | 11.99 | 13.01 | 11.99 | 11.00 |
| 08 | 13.01 | 13.01 | 20.00 | 12.99 | 13.01 | 20.00 | 13.01 | 9.68 | 13.01 | 11.41 | 11.99 | 20.00 | 12.99 | 12.01 | 12.01 | 12.99 | 20.00 | 12.01 | 12.01 | 12.01 | 11.99 | 20.00 | 11.99 | 11.41 | 20.00 | 13.01 | 12.99 | 12.99 | 20.00 | 12.99 | 20.00 |
| 09 | 11.41 | 13.01 | 12.99 | 12.01 | 20.00 | 11.99 | 13.01 | 13.01 | 9.68 | 20.00 | 12.01 | 11.99 | 11.00 | 11.99 | 12.99 | 12.01 | 20.00 | 12.99 | 13.01 | 12.99 | 12.99 | 20.00 | 12.01 | 12.99 | 11.99 | 12.99 | 11.99 | 20.00 | 13.01 | 20.00 | 13.01 |
| 0A | 12.01 | 13.01 | 11.99 | 12.01 | 12.99 | 12.99 | 20.00 | 11.41 | 20.00 | 9.68 | 11.00 | 20.00 | 12.99 | 11.99 | 13.01 | 13.01 | 11.99 | 20.00 | 11.99 | 12.99 | 20.00 | 12.99 | 20.00 | 12.99 | 13.01 | 12.01 | 12.99 | 13.01 | 12.01 | 11.99 | 13.01 |
| 0B | 13.01 | 12.99 | 20.00 | 20.00 | 12.99 | 20.00 | 12.99 | 11.99 | 12.01 | 11.00 | 9.42 | 20.00 | 11.99 | 11.41 | 13.01 | 11.99 | 20.00 | 12.99 | 20.00 | 20.00 | 12.01 | 12.01 | 13.01 | 20.00 | 12.99 | 11.99 | 12.01 | 11.41 | 11.00 | 11.99 | 11.99 |
| 0C | 20.00 | 20.00 | 11.42 | 11.41 | 12.99 | 12.01 | 20.00 | 20.00 | 11.99 | 20.00 | 20.00 | 9.68 | 20.00 | 13.01 | 20.00 | 20.00 | 11.42 | 11.99 | 12.99 | 12.99 | 20.00 | 20.00 | 11.99 | 12.01 | 12.01 | 20.00 | 12.99 | 11.99 | 20.00 | 11.42 | 11.41 |
| 0D | 11.99 | 11.99 | 20.00 | 13.01 | 12.01 | 20.00 | 12.99 | 12.99 | 11.00 | 12.99 | 11.99 | 20.00 | 9.42 | 20.00 | 12.01 | 20.00 | 20.00 | 20.00 | 11.41 | 12.99 | 11.99 | 12.01 | 11.00 | 20.00 | 11.41 | 12.01 | 11.99 | 12.99 | 13.01 | 13.01 | 11.99 |
| 0E | 12.01 | 20.00 | 12.01 | 12.99 | 13.01 | 11.99 | 12.01 | 12.01 | 11.99 | 11.99 | 11.41 | 13.01 | 20.00 | 9.42 | 20.00 | 13.01 | 12.99 | 13.01 | 11.99 | 20.00 | 11.41 | 12.99 | 13.01 | 20.00 | 11.99 | 12.99 | 13.01 | 12.01 | 11.99 | 11.99 | 11.00 |
| 0F | 12.99 | 20.00 | 20.00 | 12.99 | 11.99 | 11.42 | 11.99 | 12.01 | 12.99 | 13.01 | 13.01 | 20.00 | 12.01 | 20.00 | 9.68 | 11.99 | 12.99 | 12.01 | 11.99 | 20.00 | 11.99 | 13.01 | 12.99 | 11.99 | 13.01 | 11.00 | 20.00 | 13.01 | 20.00 | 12.99 | 11.99 |
| 10 | 12.99 | 13.01 | 20.00 | 13.01 | 12.01 | 20.00 | 12.01 | 12.99 | 12.01 | 13.01 | 11.99 | 20.00 | 20.00 | 13.01 | 11.99 | 9.68 | 11.41 | 13.01 | 20.00 | 11.41 | 13.01 | 11.99 | 12.99 | 20.00 | 12.99 | 12.99 | 20.00 | 12.01 | 12.99 | 12.01 | 20.00 |
| 11 | 20.00 | 20.00 | 12.01 | 20.00 | 11.99 | 11.42 | 12.01 | 20.00 | 20.00 | 11.99 | 20.00 | 11.42 | 20.00 | 12.99 | 12.99 | 11.41 | 9.68 | 12.99 | 11.99 | 12.99 | 20.00 | 20.00 | 20.00 | 12.01 | 13.01 | 20.00 | 11.42 | 20.00 | 20.00 | 11.99 | 11.41 |
| 12 | 12.01 | 11.41 | 20.00 | 13.01 | 12.99 | 12.99 | 13.01 | 12.01 | 12.99 | 20.00 | 12.99 | 11.99 | 20.00 | 13.01 | 12.01 | 13.01 | 12.99 | 9.68 | 11.99 | 20.00 | 12.99 | 12.01 | 11.99 | 11.99 | 20.00 | 11.00 | 13.01 | 11.99 | 20.00 | 12.99 | 13.01 |
| 13 | 12.99 | 12.01 | 13.01 | 13.01 | 20.00 | 20.00 | 12.01 | 12.01 | 13.01 | 11.99 | 20.00 | 12.99 | 11.41 | 11.99 | 11.99 | 20.00 | 11.99 | 11.99 | 9.42 | 13.01 | 12.99 | 12.99 | 11.99 | 12.01 | 12.01 | 11.41 | 20.00 | 11.99 | 13.01 | 13.01 | 11.00 |
| 14 | 13.01 | 12.01 | 11.99 | 13.01 | 20.00 | 11.99 | 11.99 | 12.01 | 12.99 | 12.99 | 20.00 | 12.99 | 12.99 | 20.00 | 20.00 | 11.41 | 12.99 | 20.00 | 13.01 | 9.68 | 12.01 | 11.00 | 12.99 | 20.00 | 13.01 | 12.99 | 12.01 | 11.99 | 11.99 | 13.01 | 13.01 |
| 15 | 12.99 | 20.00 | 20.00 | 11.99 | 11.00 | 20.00 | 11.41 | 11.99 | 12.99 | 20.00 | 12.01 | 20.00 | 11.99 | 11.41 | 11.99 | 13.01 | 20.00 | 12.99 | 12.99 | 12.01 | 9.42 | 11.99 | 13.01 | 20.00 | 20.00 | 12.01 | 13.01 | 12.99 | 12.01 | 11.00 | 11.99 |
| 16 | 11.99 | 13.01 | 20.00 | 12.99 | 12.99 | 20.00 | 20.00 | 20.00 | 20.00 | 12.99 | 12.01 | 20.00 | 12.01 | 12.99 | 13.01 | 11.99 | 20.00 | 12.01 | 12.99 | 11.00 | 11.99 | 9.42 | 12.01 | 20.00 | 11.41 | 11.99 | 11.00 | 11.41 | 11.99 | 13.01 | 11.99 |
| 17 | 20.00 | 12.99 | 11.42 | 12.01 | 13.01 | 20.00 | 20.00 | 11.99 | 12.01 | 20.00 | 13.01 | 11.99 | 11.00 | 13.01 | 12.99 | 12.99 | 20.00 | 11.99 | 11.99 | 12.99 | 13.01 | 12.01 | 9.68 | 12.99 | 11.99 | 11.99 | 12.99 | 13.01 | 20.00 | 20.00 | 11.99 |
| 18 | 20.00 | 20.00 | 11.42 | 20.00 | 11.99 | 11.42 | 12.99 | 11.41 | 12.99 | 12.99 | 20.00 | 12.01 | 20.00 | 20.00 | 11.99 | 20.00 | 12.01 | 11.99 | 12.01 | 20.00 | 20.00 | 20.00 | 12.99 | 9.68 | 11.99 | 20.00 | 20.00 | 13.01 | 11.42 | 20.00 | 11.41 |
| 19 | 12.01 | 13.01 | 20.00 | 12.01 | 11.99 | 12.99 | 11.99 | 20.00 | 11.99 | 13.01 | 12.99 | 12.01 | 11.41 | 11.99 | 13.01 | 12.99 | 13.01 | 20.00 | 12.01 | 13.01 | 20.00 | 11.41 | 11.99 | 11.99 | 9.42 | 12.99 | 11.99 | 12.01 | 20.00 | 13.01 | 11.00 |
| 1A | 20.00 | 11.99 | 20.00 | 11.99 | 20.00 | 20.00 | 11.41 | 13.01 | 12.99 | 12.01 | 11.99 | 20.00 | 12.01 | 12.99 | 11.00 | 12.99 | 20.00 | 11.00 | 11.41 | 12.99 | 12.01 | 11.99 | 11.99 | 20.00 | 12.99 | 9.42 | 13.01 | 20.00 | 13.01 | 12.01 | 11.99 |
| 1B | 12.99 | 12.01 | 20.00 | 11.99 | 20.00 | 11.99 | 13.01 | 12.99 | 11.99 | 12.99 | 12.01 | 12.99 | 11.99 | 13.01 | 20.00 | 20.00 | 11.42 | 13.01 | 20.00 | 12.01 | 13.01 | 11.00 | 12.99 | 20.00 | 11.99 | 13.01 | 9.68 | 11.99 | 12.99 | 20.00 | 11.99 |
| 1C | 13.01 | 12.01 | 12.99 | 20.00 | 13.01 | 12.01 | 11.99 | 12.99 | 20.00 | 13.01 | 11.41 | 11.99 | 12.99 | 12.01 | 13.01 | 12.01 | 20.00 | 11.99 | 11.99 | 11.99 | 12.99 | 11.41 | 13.01 | 13.01 | 12.01 | 20.00 | 11.99 | 9.42 | 11.99 | 20.00 | 11.00 |
| 1D | 12.01 | 11.99 | 11.99 | 12.99 | 12.99 | 12.99 | 13.01 | 20.00 | 13.01 | 12.01 | 11.00 | 20.00 | 13.01 | 11.99 | 20.00 | 12.99 | 20.00 | 20.00 | 13.01 | 11.99 | 12.01 | 11.99 | 20.00 | 11.42 | 20.00 | 13.01 | 12.99 | 11.99 | 9.68 | 12.99 | 11.99 |
| 1E | 11.99 | 12.99 | 12.99 | 20.00 | 12.01 | 20.00 | 11.99 | 12.99 | 20.00 | 11.99 | 11.99 | 11.42 | 13.01 | 11.99 | 12.99 | 12.01 | 11.99 | 12.99 | 13.01 | 13.01 | 11.00 | 13.01 | 20.00 | 20.00 | 13.01 | 12.01 | 20.00 | 20.00 | 12.99 | 9.68 | 11.99 |
| 1F | 20.00 | 20.00 | 11.41 | 20.00 | 13.01 | 11.41 | 11.00 | 20.00 | 13.01 | 13.01 | 11.99 | 11.41 | 11.99 | 11.00 | 11.99 | 20.00 | 11.41 | 13.01 | 11.00 | 13.01 | 11.99 | 11.99 | 11.99 | 11.41 | 11.00 | 11.99 | 11.99 | 11.00 | 11.99 | 11.99 | 8.83 |

$$C_{all} = 1023 \times \sum_{\alpha \neq 0} \sum_{\beta \neq 0} \varepsilon^2_{\alpha,\beta}. \tag{2}$$

Of course, $C_{all}$ has a higher capacity, but it is computed on almost twice as many biases. Because of the cost increase for computing the LLR statistics exploiting $1023 \times 1023$ input and output differences, we only focus on the cases for which $\alpha^L = \beta^L = 0$.

**Experimental Verification.**

*2+2 Rounds.* To verify the Markov assumption in practice, we experimentally computed each differential bias for 2+2 rounds by using $2^{15}$ tweaks $T_i$ and $2^{15}$ tweaks $T_j$. In total, our experiments use $2^{15} \times 2^{15} \times 2^9 = 2^{39}$ pairs. Table 1 summarizes the differential biases computed by each EDP. Some differential biases are as low as $-2^{-20.00}$, but $2^{39}$ pairs are still enough to confirm such a low bias experimentally. The detail of our experimental results is summarized in Appendix D.1. Here, we just focus on some concrete cases of interest.

- When $(\alpha^R, \beta^R) = (\texttt{0x01}, \texttt{0x01})$, the theoretical bias is estimated as $+2^{-9.68}$. Experimentally, we also obtain the same bias.
- When $(\alpha^R, \beta^R) = (\texttt{0x02}, \texttt{0x1F})$, the theoretical bias is estimated as $-2^{-20.00}$. The same bias is also obtained experimentally for those differences.

*3+3 Rounds.* We next verify experimentally the differential bias for 3+3 rounds, and Table 2 summarizes these results. To experimentally verify each differential bias, we used $2^{17}$ tweaks $T_i$ and $2^{17}$ tweaks $T_j$. In total, our experiments use $2^{17} \times 2^{17} \times 2^9 = 2^{43}$ pairs. Our experimental results are summarized in Appendix D.2. Here, we depict some concrete cases of interest.

**Table 2.** Summary of differential bias for 3+3 rounds. Each element of this table corresponds to $-\log_2(|\varepsilon|)$ for a differential bias $\varepsilon$. The elements colored in light-blue have a negative bias, i.e., $\varepsilon < 0$.

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 14.71 | 17.68 | 16.30 | 18.42 | 18.42 | 20.00 | 20.00 | 18.42 | 16.30 | 17.19 | 18.42 | 20.00 | 16.83 | 17.19 | 17.68 | 17.68 | 20.00 | 17.19 | 17.68 | 18.42 | 17.68 | 16.83 | 20.00 | 20.00 | 17.19 | 20.00 | 17.68 | 18.42 | 17.19 | 16.83 | 20.00 |
| 02 | 17.68 | 14.71 | 20.00 | 17.68 | 17.19 | 16.30 | 17.68 | 18.42 | 18.42 | 18.42 | 17.68 | 20.00 | 16.83 | 20.00 | 20.00 | 18.42 | 20.00 | 16.30 | 17.19 | 17.19 | 20.00 | 18.42 | 17.68 | 20.00 | 18.42 | 16.83 | 17.19 | 17.19 | 16.83 | 17.68 | 20.00 |
| 03 | 16.30 | 20.00 | 14.71 | 20.00 | 17.68 | 17.19 | 16.83 | 20.00 | 17.68 | 16.83 | 20.00 | 16.54 | 20.00 | 17.19 | 20.00 | 20.00 | 17.19 | 20.00 | 18.42 | 16.83 | 20.00 | 20.00 | 16.54 | 16.54 | 20.00 | 20.00 | 20.00 | 17.68 | 16.83 | 17.68 | 16.30 |
| 04 | 18.42 | 17.68 | 20.00 | 14.71 | 16.30 | 20.00 | 17.19 | 17.68 | 17.19 | 17.19 | 20.00 | 16.30 | 18.42 | 17.68 | 17.68 | 18.42 | 20.00 | 18.42 | 18.42 | 18.42 | 16.83 | 17.68 | 17.19 | 20.00 | 17.19 | 16.83 | 16.83 | 20.00 | 17.68 | 20.00 | 20.00 |
| 05 | 18.42 | 17.19 | 17.68 | 16.30 | 14.71 | 20.00 | 16.83 | 18.42 | 20.00 | 17.68 | 17.68 | 17.68 | 17.19 | 18.42 | 16.83 | 17.19 | 16.83 | 17.68 | 20.00 | 20.00 | 16.09 | 17.68 | 18.42 | 16.83 | 16.83 | 20.00 | 20.00 | 18.42 | 17.68 | 17.19 | 18.42 |
| 06 | 20.00 | 16.30 | 17.19 | 20.00 | 20.00 | 14.71 | 18.42 | 20.00 | 16.83 | 17.68 | 20.00 | 17.19 | 20.00 | 16.83 | 16.54 | 20.00 | 16.54 | 17.68 | 20.00 | 16.83 | 20.00 | 20.00 | 20.00 | 16.54 | 17.68 | 20.00 | 16.83 | 17.19 | 17.68 | 20.00 | 16.30 |
| 07 | 20.00 | 17.68 | 16.83 | 17.19 | 16.83 | 18.42 | 14.45 | 18.42 | 18.42 | 20.00 | 17.68 | 20.00 | 17.68 | 17.19 | 16.83 | 17.19 | 17.19 | 18.42 | 17.19 | 16.83 | 16.30 | 20.00 | 20.00 | 17.68 | 16.83 | 16.30 | 18.42 | 16.83 | 18.42 | 16.83 | 16.09 |
| 08 | 18.42 | 18.42 | 20.00 | 17.68 | 18.42 | 20.00 | 18.42 | 14.71 | 18.42 | 16.30 | 16.83 | 20.00 | 17.68 | 17.19 | 17.19 | 17.68 | 20.00 | 17.19 | 17.19 | 17.19 | 16.83 | 20.00 | 16.83 | 16.30 | 20.00 | 18.42 | 17.68 | 17.68 | 20.00 | 17.68 | 20.00 |
| 09 | 16.30 | 18.42 | 17.68 | 17.19 | 20.00 | 16.83 | 18.42 | 18.42 | 14.71 | 20.00 | 17.19 | 16.83 | 16.09 | 16.83 | 17.68 | 17.19 | 20.00 | 17.68 | 18.42 | 17.68 | 17.68 | 20.00 | 17.19 | 17.68 | 16.83 | 17.68 | 16.83 | 20.00 | 18.42 | 20.00 | 18.42 |
| 0A | 17.19 | 18.42 | 16.83 | 17.19 | 17.68 | 17.68 | 20.00 | 16.30 | 20.00 | 14.71 | 16.09 | 20.00 | 17.68 | 16.83 | 18.42 | 18.42 | 16.83 | 20.00 | 16.83 | 17.68 | 20.00 | 17.68 | 20.00 | 17.68 | 18.42 | 17.19 | 17.68 | 18.42 | 17.19 | 16.83 | 18.42 |
| 0B | 18.42 | 17.68 | 20.00 | 20.00 | 17.68 | 20.00 | 17.68 | 16.83 | 17.19 | 16.09 | 14.45 | 20.00 | 16.83 | 16.30 | 18.42 | 16.83 | 20.00 | 17.68 | 20.00 | 20.00 | 17.19 | 17.19 | 18.42 | 20.00 | 17.68 | 16.83 | 17.19 | 16.30 | 16.09 | 16.83 | 16.83 |
| 0C | 20.00 | 20.00 | 16.54 | 16.30 | 17.68 | 17.19 | 20.00 | 20.00 | 16.83 | 20.00 | 20.00 | 14.71 | 20.00 | 18.42 | 20.00 | 20.00 | 16.54 | 16.83 | 17.68 | 17.68 | 20.00 | 20.00 | 16.83 | 17.19 | 17.19 | 20.00 | 17.68 | 16.83 | 20.00 | 16.54 | 16.30 |
| 0D | 16.83 | 16.83 | 20.00 | 18.42 | 17.19 | 20.00 | 17.68 | 17.68 | 16.09 | 17.68 | 16.83 | 20.00 | 14.45 | 20.00 | 17.19 | 20.00 | 20.00 | 20.00 | 16.30 | 17.68 | 16.83 | 17.19 | 16.09 | 20.00 | 16.30 | 17.19 | 16.83 | 17.68 | 18.42 | 18.42 | 16.83 |
| 0E | 17.19 | 20.00 | 17.19 | 17.68 | 18.42 | 16.83 | 17.19 | 17.19 | 16.83 | 16.83 | 16.30 | 18.42 | 20.00 | 14.45 | 20.00 | 18.42 | 17.68 | 18.42 | 16.83 | 20.00 | 16.30 | 17.68 | 18.42 | 20.00 | 16.83 | 17.68 | 18.42 | 17.19 | 16.83 | 16.83 | 16.09 |
| 0F | 17.68 | 20.00 | 20.00 | 17.68 | 16.83 | 16.54 | 16.83 | 17.19 | 17.68 | 18.42 | 18.42 | 20.00 | 17.19 | 20.00 | 14.71 | 16.83 | 17.68 | 17.19 | 16.83 | 20.00 | 16.83 | 18.42 | 17.68 | 16.83 | 18.42 | 16.09 | 20.00 | 18.42 | 20.00 | 17.68 | 16.83 |
| 10 | 17.68 | 18.42 | 20.00 | 18.42 | 17.19 | 20.00 | 17.19 | 17.68 | 17.19 | 18.42 | 16.83 | 20.00 | 20.00 | 18.42 | 16.83 | 14.71 | 16.30 | 18.42 | 20.00 | 16.30 | 18.42 | 16.83 | 17.68 | 20.00 | 17.68 | 17.68 | 20.00 | 17.19 | 17.68 | 17.19 | 20.00 |
| 11 | 20.00 | 20.00 | 17.19 | 20.00 | 16.83 | 16.54 | 17.19 | 20.00 | 20.00 | 16.83 | 20.00 | 16.54 | 20.00 | 17.68 | 17.68 | 16.30 | 14.71 | 17.68 | 16.83 | 17.68 | 20.00 | 20.00 | 20.00 | 17.19 | 18.42 | 20.00 | 16.54 | 20.00 | 20.00 | 16.83 | 16.30 |
| 12 | 17.19 | 16.30 | 20.00 | 18.42 | 17.68 | 17.68 | 18.42 | 17.19 | 17.68 | 20.00 | 17.68 | 16.83 | 20.00 | 18.42 | 17.19 | 18.42 | 17.68 | 14.71 | 16.83 | 20.00 | 17.68 | 17.19 | 16.83 | 16.83 | 20.00 | 16.09 | 18.42 | 16.83 | 20.00 | 17.68 | 18.42 |
| 13 | 17.68 | 17.19 | 18.42 | 18.42 | 20.00 | 20.00 | 17.19 | 17.19 | 18.42 | 16.83 | 20.00 | 17.68 | 16.30 | 16.83 | 16.83 | 20.00 | 16.83 | 16.83 | 14.45 | 18.42 | 17.68 | 17.68 | 16.83 | 17.19 | 17.19 | 16.30 | 20.00 | 16.83 | 18.42 | 18.42 | 16.09 |
| 14 | 18.42 | 17.19 | 16.83 | 18.42 | 20.00 | 16.83 | 16.83 | 17.19 | 17.68 | 17.68 | 20.00 | 17.68 | 17.68 | 20.00 | 20.00 | 16.30 | 17.68 | 20.00 | 18.42 | 14.71 | 17.19 | 16.09 | 17.68 | 20.00 | 18.42 | 17.68 | 17.19 | 16.83 | 16.83 | 18.42 | 18.42 |
| 15 | 17.68 | 20.00 | 20.00 | 16.83 | 16.09 | 20.00 | 16.30 | 16.83 | 17.68 | 20.00 | 17.19 | 20.00 | 16.83 | 16.30 | 16.83 | 18.42 | 20.00 | 17.68 | 17.68 | 17.19 | 14.45 | 16.83 | 18.42 | 20.00 | 20.00 | 17.19 | 18.42 | 17.68 | 17.19 | 16.09 | 16.83 |
| 16 | 16.83 | 18.42 | 20.00 | 17.68 | 17.68 | 20.00 | 20.00 | 20.00 | 20.00 | 17.68 | 17.19 | 20.00 | 17.19 | 17.68 | 18.42 | 16.83 | 20.00 | 17.19 | 17.68 | 16.09 | 16.83 | 14.45 | 17.19 | 20.00 | 16.30 | 16.83 | 16.09 | 16.30 | 16.83 | 18.42 | 16.83 |
| 17 | 20.00 | 17.68 | 16.54 | 17.19 | 18.42 | 20.00 | 20.00 | 16.83 | 17.19 | 20.00 | 18.42 | 16.83 | 16.09 | 18.42 | 17.68 | 17.68 | 20.00 | 16.83 | 16.83 | 17.68 | 18.42 | 17.19 | 14.71 | 17.68 | 16.83 | 16.83 | 17.68 | 18.42 | 20.00 | 20.00 | 16.83 |
| 18 | 20.00 | 20.00 | 16.54 | 20.00 | 16.83 | 16.54 | 17.68 | 16.30 | 17.68 | 17.68 | 20.00 | 17.19 | 20.00 | 20.00 | 16.83 | 20.00 | 17.19 | 16.83 | 17.19 | 20.00 | 20.00 | 20.00 | 17.68 | 14.71 | 16.83 | 20.00 | 20.00 | 18.42 | 16.54 | 20.00 | 16.30 |
| 19 | 17.19 | 18.42 | 20.00 | 17.19 | 16.83 | 17.68 | 16.83 | 20.00 | 16.83 | 18.42 | 17.68 | 17.19 | 16.30 | 16.83 | 18.42 | 17.68 | 18.42 | 20.00 | 17.19 | 18.42 | 20.00 | 16.30 | 16.83 | 16.83 | 14.45 | 17.68 | 16.83 | 17.19 | 20.00 | 18.42 | 16.09 |
| 1A | 20.00 | 16.83 | 20.00 | 16.83 | 20.00 | 20.00 | 16.30 | 18.42 | 17.68 | 17.19 | 16.83 | 20.00 | 17.19 | 17.68 | 16.09 | 17.68 | 20.00 | 16.09 | 16.30 | 17.68 | 17.19 | 16.83 | 16.83 | 20.00 | 17.68 | 14.45 | 18.42 | 20.00 | 18.42 | 17.19 | 16.83 |
| 1B | 17.68 | 17.19 | 20.00 | 16.83 | 20.00 | 16.83 | 18.42 | 17.68 | 16.83 | 17.68 | 17.19 | 17.68 | 16.83 | 18.42 | 20.00 | 20.00 | 16.54 | 18.42 | 20.00 | 17.19 | 18.42 | 16.09 | 17.68 | 20.00 | 16.83 | 18.42 | 14.71 | 16.83 | 17.68 | 20.00 | 16.83 |
| 1C | 18.42 | 17.19 | 17.68 | 20.00 | 18.42 | 17.19 | 16.83 | 17.68 | 20.00 | 18.42 | 16.30 | 16.83 | 17.68 | 17.19 | 18.42 | 17.19 | 20.00 | 16.83 | 16.83 | 16.83 | 17.68 | 16.30 | 18.42 | 18.42 | 17.19 | 20.00 | 16.83 | 14.45 | 16.83 | 20.00 | 16.09 |
| 1D | 17.19 | 16.83 | 16.83 | 17.68 | 17.68 | 17.68 | 18.42 | 20.00 | 18.42 | 17.19 | 16.09 | 20.00 | 18.42 | 16.83 | 20.00 | 17.68 | 20.00 | 20.00 | 18.42 | 16.83 | 17.19 | 16.83 | 20.00 | 16.54 | 20.00 | 18.42 | 17.68 | 16.83 | 14.71 | 17.68 | 16.83 |
| 1E | 16.83 | 17.68 | 17.68 | 20.00 | 17.19 | 20.00 | 16.83 | 17.68 | 20.00 | 16.83 | 16.83 | 16.54 | 18.42 | 16.83 | 17.68 | 17.19 | 16.83 | 17.68 | 18.42 | 18.42 | 16.09 | 18.42 | 20.00 | 20.00 | 18.42 | 17.19 | 20.00 | 20.00 | 17.68 | 14.71 | 16.83 |
| 1F | 20.00 | 20.00 | 16.30 | 20.00 | 18.42 | 16.30 | 16.09 | 20.00 | 18.42 | 18.42 | 16.83 | 16.30 | 16.83 | 16.09 | 16.83 | 20.00 | 16.30 | 18.42 | 16.09 | 18.42 | 16.83 | 16.83 | 16.83 | 16.30 | 16.09 | 16.83 | 16.83 | 16.09 | 16.83 | 16.83 | 13.85 |

**Table 3.** Theoretical capacity of differential biases for each number of rounds.

| capacity | 2+2 | 3+3 | 4+4 | 5+5 | 6+6 | 7+7 | 8+8 |
|---|---|---|---|---|---|---|---|
| $-\log_2(C)$ | 3.37 | 13.39 | 32.20 | 42.20 | 60.89 | 70.89 | 88.95 |
| $-\log_2(C_{all})$ | 2.38 | 13.38 | 31.20 | 42.19 | 59.89 | 70.88 | 87.95 |

- When $(\delta_i, \delta_j) = (\texttt{0x01}, \texttt{0x01})$, the theoretical bias is estimated as $+2^{-14.71}$. Experimentally, we obtain that this bias equals $2^{-17.68}$.
- When $(\delta_i, \delta_j) = (\texttt{0x02}, \texttt{0x1E})$, the theoretical bias is estimated as $-2^{-17.68}$. Experimentally, we obtain that this bias equals $-2^{-17.66}$.

*4+4 Rounds and LLR Statistics.* Besides the Markov assumption, we need an independent assumption for the LLR statistics. To verify the statistically independent assumption, we experimentally compared the LLR statistics for 4+4 rounds and the ideal case. The experiments used $2^{13} \times 2^{13} \times 2^{9} = 2^{35}$ pairs and were repeated 5000 times. According to Proposition 1, each distribution tends toward the following distributions

$$Real \sim \mathcal{N}(965.43, 6.98) \qquad\qquad Ideal \sim \mathcal{N}(958.45, 6.98). \qquad (3)$$

Figure 4 compares the theoretical estimation and experimental frequencies, which justifies the correctness of our theoretical estimation.

*5+5 Rounds and LLR Statistics.* Similar to the experiment for 4+4 rounds, we experimentally compared the LLR statistics for 5+5 rounds and the ideal case. The experiments used $2^{18} \times 2^{18} \times 2^{9} = 2^{45}$ pairs and were repeated 5000

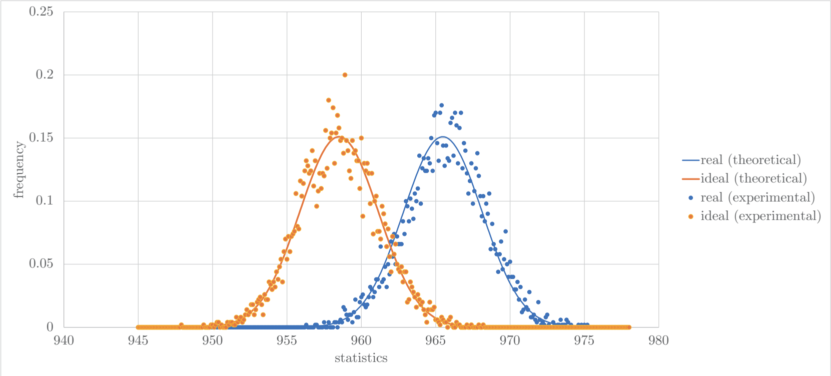

**Fig. 4.** Comparison between the theoretical estimations and the experimental results of LLR statistics for 4+4 rounds and the ideal distribution.

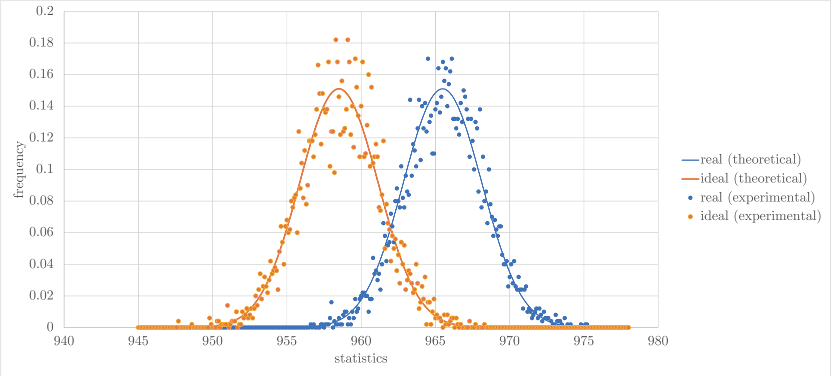

**Fig. 5.** Comparison between the theoretical estimations and the experimental results of LLR statistics for 5+5 rounds and the ideal distribution.

times. When we use $2^{45}$ pairs, each distribution tends towards the same distribution as Eq.(3). Figure 5 compares the theoretical estimation and experimental frequencies.

## 5 Key-Recovery Attack on 7-Round SCARF

In this section, we propose a key-recovery attack on 7-round SCARF.

First of all, we define a proper "reduced-round SCARF" version. To reduce SCARF to 7 rounds, we decided to remove the first round function, $R_1$. Of course, another choice would have been to remove the last round, $R_2$, but $R_2$ was designed to prevent that the last S-box is always canceled. Such a reduced-round version would change the security property of SCARF significantly. Therefore, we believe that removing the first round is more meaningful for discussing the security margin of the full cipher. The tweakey schedule is also nonlinear, and it has a block-cipher-like structure. In our 7-round SCARF, we decided to take the most conservative choice and to use the same tweakey schedule as the original one. Therefore, the secret key size is still $60 \times 4 = 240$ bits even after removing the first round.

### 5.1 Attack Procedure on Security Requirement 2

**Step 1: Partial Key Recovery using the (6+6)-Round Multiple Differential Distinguisher.** We first collect data by using the enc-then-dec oracle, $\tilde{E}$. We use $2^{30}$ tweaks $T_i$, where the bottom 30 bits of $T_i$ are active, i.e., $T_i := 0^{18} \| i$. In the security requirement 2, the oracle accepts a plaintext and a pair of tweaks. Therefore, we choose another fixed tweak, $T'$, different from any of the $T_i$, e.g., $T' = 1^{48}$. We query the full code book for the $2^{30}$ $T_i$ and a fixed tweak $T'$ and store $\tilde{E}_{T_i,T'}(x)$ for all $x \in \mathbb{F}_2^{10}$. From these plaintext-ciphertext pairs, we have $\tilde{E}_{T_i,T_j} = \tilde{E}^{-1}_{T_j,T'} \circ \tilde{E}_{T_i,T'}$ and can construct $M = 2^{29+29+9} = 2^{67}$ pairs[5].

The initial goal is to recover the top 30 bits of $K^1$ by using the (6+6)-round distinguisher. The highest differential bias is $2^{-38.19}$, which is not always sufficient to filter key candidates with a reasonable success probability. Therefore, we use multiple differentials and the LLR statistic. According to Proposition 1, we compute $\mu_0$, $\mu_1$, $\sigma_0^2$, and $\sigma_1^2$. Then, $(\mu_0 - \mu_1) \approx \sigma_0^2 \approx \sigma_1^2 \approx 2^{-60.8887}$. When we use $2^{67}$ pairs, each distribution tends towards the following distribution

$$\text{Real} \sim \mathcal{N}(34.56, 69.13) \qquad\qquad \text{Ideal} \sim \mathcal{N}(-34.56, 69.13),$$

where, from each average, we subtract $(\mu_0 + \mu_1)/2$ in the sake of readability, i.e., Real $\sim \mathcal{N}(M \times \left(\mu_0 - \frac{\mu_0+\mu_1}{2}\right), M\sigma_0^2)$ and Ideal $\sim \mathcal{N}(M \times \left(\mu_1 - \frac{\mu_0+\mu_1}{2}\right), M\sigma_1^2)$ here. We can construct a 30-bit filter with a success probability of 98.9 %. In other words, we can uniquely recover the key candidates for the last 30 bits of $K^1$ with a high probability.

Algorithm 1 shows the detailed attack procedure. The algorithm requires $2 \times 31 \times 2^{20}$ memory and $2 \times 2^{30} \times 2^{29} \times 31 \times 2^{10} = 2^{74.95}$ time.

**Step 2: Partial Key Recovery using (5S+5S)-Round Differential Distinguisher.** We next recover the bottom 30 bits of $K^1$ and the 5 bits of $K^2$. Note that we already know the top 30 bits of $K^1$ from Step 1.

Instead of the (6+6)-round distinguisher, we introduce a (5S+5S)-round distinguisher, where the S-box layer is added to the (5+5)-round distinguisher. By applying the S-box transition probability from the EDPs of 5+5 rounds, we can estimate these biases. As a result, for any $\delta$ with Hamming weight 1, we have

$$\text{Prob}[(\delta, 0) \xrightarrow{5S+5S} (\delta, 0)] = \frac{1}{1023} + 2^{-34.17}. \qquad (4)$$

[5] It is also possible to construct $\binom{2^{30}}{2} 2^9 \approx 2^{68}$ pairs by considering all combinations of tweaks. However, if we do this, we have a critical problem with the independence of every pair. Indeed, when we observe the differential property by $E^{-1}_{T_2} \circ E_{T_1}$ and $E^{-1}_{T_3} \circ E_{T_1}$, we cannot include $E^{-1}_{T_3} \circ E_{T_2}$ as a statistically independent sample.

**Algorithm 1** Algorithm to recover the top 30 bits of $K^1$

```
Input: $2^{30}$ tweaks $T_i$, a tweak $T'$, differential probability $p_{\delta_{in},\delta_{out}}$, a threshold $\theta$.
Output: The top 30 bits of $K^1$.
  Prepare two two-dimensional arrays $A[][]$ and $B[][]$, of size $31 \times 2^{20}$.
  for $K^1 \in \mathbb{F}_2^{30} \| 0^{30}$ do
      for $i = 0$ to $2^{29} - 1$ do
          Derive $rk_2$ from $K^1$ and $T_i$.
          for all $\delta \in \mathbb{F}_2^5 \setminus \{0\}$ do
              for all $x_1 \in \mathbb{F}_2^{10}$ do
                  $x_0 = R_1^{-1}(x_1, rk_2)$.
                  $x_0' = R_1^{-1}(x_1 \oplus 0^5 \| \delta, rk_2)$.
                  if $\tilde{E}_{T_i,T'}(x_0) < \tilde{E}_{T_i,T'}(x_0')$ then
                      $y = \tilde{E}_{T_i,T'}(x_0) \| \tilde{E}_{T_i,T'}(x_0')$
                      $A[\delta][y] = A[\delta][y] + 1$
      Repeat the same procedure as above for $i = 2^{29}$ to $2^{30} - 1$ and get $B[\delta][y]$.
      $s = 0$.
      for all $\delta_{in} \in \mathbb{F}_2^5 \setminus \{0\}$ do
          for all $\delta_{out} \in \mathbb{F}_2^5 \setminus \{0\}$ do
              $n = 0$.
              for all $y \in \mathbb{F}_2^{20}$ do
                  $n = n + A[\delta_{in}][y] \times B[\delta_{out}][y]$
              $s = s + n \times \log(\frac{p_{\delta_{in},\delta_{out}}}{1/1023})$
      if $s > \theta$ then
          Return $K^1$
```

When the Hamming weight of $\delta$ is 1, the $G$ function in the 3rd round involves only 5 bits of the subkey, and they are computed by guessing the 30-bit $K^1$ and the 5-bit $K^2$ when the tweak is active. Using $2^{67}$ pairs is enough to construct a 35-bit filter with a success probability of almost one. The time complexity is $2^{35} \times 2^{40} = 2^{75}$.

We experimentally verified the differential bias of Eq.(4) by using $2^{26} \times 2^{26} \times 2^9 = 2^{61}$ pairs and were repeated 10 times. As a result, we observed $2^{-34.29}$ of differential bias experimentally.

**Step 3: Full Key Recovery.** A single $\delta$ in Step 2 is enough to recover the entire $K^1$. Therefore, we can compute the first $\Sigma \circ \mathsf{SL}$ layer in the tweakey schedule for arbitrary tweaks. This implies that the first two rounds, including the tweakey schedule, are peeled off. While we do not explicitly show the procedure to recover $K^2$, $K^3$, and $K^4$, we can recover these keys by auxiliary procedures because it should be easier than recovering $K^1$.

In summary, with a complexity of about $2^{76}$, we can recover the 240-bit key with a success probability of 98.9 %.

### 5.2 The Case of the Security Requirement 1

When we consider the security requirement 1 instead of the security requirement 2, the number of available pairs is further limited. As discussed in [CGL$^+$23], we need approximately $2^{18}$ queries to collect the full-code book data. Therefore, $2^{40}$ queries allow us to collect the full code book for $2^{22}$ different tweaks. As a result, we only have $2^{21+21+9} = 2^{51}$ pairs. The distinguishing advantage of the attacker is not enough in this case to filter the wrong keys.

## 6 Multi-Key Distinguishing Attacks on Full SCARF

The highest differential bias for full-round SCARF is $2^{-52.34}$. To detect this bias, $2^{52.34 \times 2}/1024 = 2^{94.68}$ pairs are needed. As the security requirements for SCARF restrict the number of queries, it is unlikely to collect such a large number of pairs. If we instead use the LLR statistic, the capacity is $2^{-88.95}$. This means that the number of needed pairs is approximately $2^{88.95}$, and it is still unlikely to collect them due to the restriction on the number of queries.

Nevertheless, in this section, we discuss the advantage of the distinguishing algorithm against the full-round SCARF. This discussion is motivated by the state-of-the-art theory regarding the definition of *bit security* [MW18,WY21,WY23], which defines *bit security* based on the adversary's time and advantage.

### 6.1 Time and Advantage of the Distinguishing Algorithm

When we compute the LLR statistic on the full-round SCARF, we do not need to guess the key. Therefore, a simplification of Algorithm 1 allows us to compute the LLR statistic with a time complexity of $31 \times 2^{40} \approx 2^{44.95}$. The capacity of the differential bias for the full-round SCARF is $2^{-88.95}$. When we compute the LLR statistic using $2^{67}$ pairs, after adjusting the average by subtracting from it $(\mu_0 + \mu_1)/2$, each distribution has

$$\text{Real} \sim \mathcal{N}(2^{-22.95}, 2^{-21.95}) \qquad \text{Ideal} \sim \mathcal{N}(-2^{-22.95}, 2^{-21.95}).$$

It is unlikely to distinguish these two worlds in practice because $\sigma_0 \sim \sigma_1 \gg \mu_0 - \mu_1$. However, we do have a non-negligible distinguishing advantage. When we estimate the probability that the statistic is higher than $-2^{-22.95}$, it is 0.5 in the ideal case but 0.5001982 in the real case. This implies that the (traditional) distinguishing advantage is

$$0.5001982 - 0.5 = 0.0001982 \approx 2^{-12.30}.$$

Micciancio and Walter defined the notion of *bit security* from the adversary's time, $T(A)$, and advantage, $adv^A$ [MW18].

**Definition 4 (Bit Security of a Primitive [MW18]).** *Let $T(A)$ be the time complexity of the algorithm $A$, that is linear under repetition. For any primitive, its bit security is defined as* $\min_A \log \frac{T(A)}{adv^A}$.

Here, $adv^A$ is defined by the Shannon entropy and mutual information. In our attack scenario, $adv^A = (2 \times (0.5 + 2^{-12.30}) - 1)^2 = 2^{-22.60}$. Therefore, the bit security of SCARF is defined as

$$44.95 + 22.60 = 67.55.$$

It is significantly less than 80. Therefore, we can conclude that SCARF does not provide an 80-bit security in the context of [MW18].

Watanabe and Yasunaga also defined a notion of *bit security* as the computational cost of winning the game [WY21]. Later, they showed that the two definitions are equivalent [WY23].

### 6.2 Multi-Key Distinguisher

On the other hand, it is not easy to conclude that the above observation implies a security claim break. The definition of [MW18] does not provide an explicit attack algorithm that wins a distinguishing game with high probability by the computational cost of the bit security. The definition in [WY21] provides an explicit attack algorithm, but their distinguishing game accesses multiple encryption oracles while re-keying the oracle. Finally, the adversary wins the distinguishing game by combining all knowledge gained from the oracles with multiple keys. Such an attack setting can be classified as a *multi-key model* rather than a *single-key model*. Indeed, we have the following concrete attack procedure to distinguish the full SCARF in the multi-key setting.

1. The attacker accesses an oracle and evaluates the LLR statistic. If it is higher than $\mu_1$, the score is increased. Otherwise, the score remains unchanged.
2. The attacker re-keys the oracle and repeats Step 1, $c \times 2^{22.60}$ times, for some constant $c$.
3. Check the score. If it is significantly higher than $c \times 2^{21.60}$, the attacker returns 1. Otherwise, he returns 0.

The procedure above distinguishes SCARF from the ideal with a complexity of $c \times 2^{44.95+22.60} = c \times 2^{67.55}$. It is clear that SCARF does not provide a 80-bit security in the multi-key setting[6].

On the contrary, to the best of our knowledge, we do not have an explicit algorithm to win the distinguishing game with this bit security notion in a single-key model. This is different from a key-recovery attack with a low success probability. In a key-recovery attack with a success probability $p$, we might repeat the attack procedure $p^{-1}$ times while re-keying. However, unlike the multi-key attack, we do not need to combine all knowledge from the re-keyed oracles.

[6] We also have another procedure, where instead of computing the LLR statistics every time, we collect pairs while re-keying. We have $2^{67}$ pairs for each key. Therefore, roughly, $2^{88.95-67} = 2^{21.95}$ re-keys are enough to collect $2^{88.95}$ pairs. As a result, both procedures successfully distinguish the full SCARF with almost the same complexity on the multi-key setting.

**The Case of the Security Requirement 1.** When we consider the Security Requirement 1, the number of available pairs is reduced to $2^{51}$. Then, the traditional distinguishing advantage is

$$0.500000774 - 0.5 = 0.000000774 \approx 2^{-20.30}.$$

The adversary needs at least $2^{40}$ times as the query complexity. The time to compute the LLR statistics is negligible because it is $2 \times 2^{21} \times 31 \times 2^{10} \approx 2^{36.95}$. Therefore, the bit security is $40+19.30\times 2 = 78.6$. Even for Security Requirement 1, SCARF does not provide an 80-bit security in the multi-key setting.

### 6.3 Discussion and Open Questions

The existing definition of bit security and our multi-key distinguishing attack prompt several discussions and open questions in both practice and theory.

First, should we distinguish between the single-key and multi-key models? Currently, the existing definition of bit security [MW18,WY21,WY23] does not make this distinction. However, these two attack models are regarded as different in practice [ML15]. We presented one such example. Bridging this gap between theory and practice is an interesting open question.

From a practical perspective, the question is whether we have an explicit distinguishing attack in the single-key model with even a slight advantage. If such an attack is found, it would imply that the security requirements of SCARF would be broken. It may be beneficial to redefine bit security by distinguishing between the single-key and multi-key models. This redefinition would be useful for primitives whose claimed security level exceeds the block length and where the number of queries is limited.

Finally, does our conclusion that SCARF does not provide 80-bit security in the multi-key setting pose a practical problem for its use case? SCARF is used to counter (contention-based) cache attacks. With each exhaustion of the limited queries, the key is re-keyed, creating an environment where a multi-key distinguishing attack could be executed in practice. However, the attacker's true goal is to efficiently construct a victim set to mount the cache attack. Whether the existence of a multi-key distinguisher aids in constructing these victim sets remains an open question.

## 7 Impact of the S-box Choice on the Differential Bias

The differential properties of the S-box play an important role in the multiple-tweak differential attack and influence the magnitude of the differential bias. The goal of this section is to provide a deeper understanding of the role that the S-box plays in the attack and to discuss the impact of choosing a different S-box would have on the bias.

### 7.1 Impact of the S-box on the bias for 2+2 and 3+3 rounds

As shown in Section 4, the differential bias for 1+1 rounds depends on the properties of the function $S^{-1} \circ S(\cdot \oplus k)$. More precisely, for a couple of differences $(\alpha, \beta)$, the bias depends on the number of solutions of the equation :

$$S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha) \oplus k) = \beta, \tag{5}$$

for all couples $(x, k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5$. This number of solutions for all possible differences $\alpha$ and $\beta$ is given in Table 8 of Appendix A.

We provide now an analysis of the number of solutions of Eq. (5) in the case $\alpha = \beta$. Then, we analyze the more general case $\alpha \neq \beta$.

**Case $\boldsymbol{\alpha = \beta}$.** We show that in the case where $\alpha = \beta$ the elements of Table 8, are directly related to a classical table, called the Boomerang Connectivity Table (BCT) [CHP+18], used to estimate the power of boomerang attacks at the S-box level.

For an $n$-bit invertible S-box $S$, the BCT of $S$ is a $2^n \times 2^n$ table, denoted by $B_S$ and defined as follows:

$$B_S(\alpha, \beta) = \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus \beta) \oplus S^{-1}(S(x \oplus \alpha) \oplus \beta) = \alpha\}.$$

Let's see how the number of solutions of Eq. (5) is related to the BCT of $S$ in the case where $\alpha = \beta$:

$$\begin{aligned} &\#\{(x, k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5 : S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha) \oplus k) = \alpha\} \\ = &\sum_{k=0}^{2^5-1} \#\{x \in \mathbb{F}_2^5 : S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha) \oplus k) = \alpha\} = \sum_{k=0}^{2^5-1} B_S(\alpha, k). \end{aligned}$$

The above computation shows that for a given $\alpha$ the number of solutions of Eq. (5) is just the sum of all the elements of the BCT of $S$ on the row $\alpha$.

**Case $\boldsymbol{\alpha \neq \beta}$.** We define for any $k \in \mathbb{F}_2^5$, the permutation $S_k$ that maps $x$ to $S^{-1}(S(x) + k)$. Then,

$$\begin{aligned} &\#\{(x, k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5 : S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha) \oplus k) = \beta\} \\ =&\#\{(x, k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5 : S_k(x) \oplus S_k(x \oplus \alpha) = \beta\} \\ =&\sum_{k=0}^{2^5-1} \mathrm{DDT}_{S_k}(\alpha, \beta). \end{aligned}$$

We see from the above equation, that in the case $\alpha \neq \beta$ we obtain a quite different interpretation for the elements in Table 8. Indeed, the elements of this table that are not on the diagonal can be interpreted as the sum, for all the $2^5$ different functions $k$ of the $S_k$'s Difference Distribution Table (DDT) coefficient at row $\alpha$ and column $\beta$.

We can observe from Table 8 that the coefficients on the diagonal (corresponding to the case $\alpha = \beta$) have much higher values than the other coefficients. This could be potentially explained by the fact that in general, BCTs have higher coefficients than DDTs. However, obtaining a more precise explanation is hard, as the correlation between the DDTs of the different functions $S_k$ and their relation to the BCT of $S$ is unclear.

We investigate now the role that plays the S-box in the biases for 2+2 and 3+3 rounds. For this, we explicitly provide the EDPs for this number of rounds by using the formulas given in Section 4.3.

For any non-zero $\alpha$ and $\beta$ from $\mathbb{F}_2^5$, we have for 2+2 rounds:

$$\mathrm{EDP}[(0,\alpha) \xrightarrow{2+2} (0,\beta)] = 2^{-5} \times P_{\tilde{S}}(\alpha,\beta)$$

The formulas for 3+3 rounds are as follows:

$$\mathrm{EDP}[(0,\alpha) \xrightarrow{3+3} (0,\beta)] = 2^{-10} \times (1 - 2^{-5}) + 2^{-10} \times P_{\tilde{S}}(\alpha,\beta),$$

It can be seen from the above formulas that the differential properties of the function $S^{-1} \circ S(\cdot \oplus k)$ influence the bias for 2+2 and 3+3 rounds. More precisely, as in the analysis of 1+1 rounds, the BCT of $S$ plays a role in the case where $\alpha = \beta$. The higher the boomerang uniformity (the maximal non-trivial value in a BCT), the higher the bias is expected to be in the differential transitions $(0,\alpha) \xrightarrow{R+R} (0,\beta)$, for $R = 1, 2, 3$.

**Other S-boxes.** It is interesting to see at this point, what the bias would have been if a different S-box than the original one of SCARF had been used instead. It is important to notice that contrary to the more classical 4-bit or 8-bit S-boxes, very few 5-bit S-boxes are used in the literature. However, in odd dimension, and contrary to the 4-bit and 8-bit cases, there exist S-boxes that ensure optimal resistance to differential cryptanalysis. Such S-boxes are called Almost Perfect Nonlinear (APN). These are S-boxes that have only 0 and 2 in their Difference Distribution Table (DDT). What is also known about these S-boxes is that their BCT is also optimal which means it also has only the elements 0 and 2 inside (see for example [CHP$^+$18] or [BC18]). Further, we know that the sum of all elements in the BCT of an $n$-bit APN S-box equals $2^{n+1}$. This explains why in the case of a 5-bit APN S-box, in the case $\alpha = \beta$, the number of solutions of Eq. (5) is always equal to $2^{5+1} = 64$.

As can be seen from Table 8, the values on the diagonal for the SCARF S-box are higher than 64, which means that if an APN S-box had been used instead of the original SCARF S-box, this would have led to much lower biases for 2+2 and 3+3 rounds in the case of $\alpha = \beta$. On the other hand, there are other popular choices for a 5-bit S-box that would have produced for some values a much higher bias than the one observed for SCARF. This is notably the case of the 5-bit S-box used in `Ascon` [DEMS21], which is affine equivalent to the $\chi$-mapping used in `Keccak` [BDPA11]. The `Ascon` S-box has a differential uniformity of 8 (maximal non-trivial coefficient in the DDT) and a boomerang uniformity of 16 (maximal non-trivial coefficient in the BCT). In comparison, the same numbers for the SCARF S-box are 4 and 6 respectively. Table 4 provides the theoretical bias obtained by the corresponding EDPs for all differences $\alpha = \beta = (0, \delta)$ for the original S-box of SCARF, the S-box of `Ascon` and a 5-bit APN S-box.

**Table 4.** Bias (in $\log_2$ representation) for $3+3$ rounds of `SCARF` with an APN S-box, with the `ASCON` S-box and the original S-box. All biases appear with the (+) sign.

| $\delta$ | APN | ASCON | SCARF | $\delta$ | APN | ASCON | SCARF |
|---|---|---|---|---|---|---|---|
| 0x1 | -15.046 | -13.430 | -14.715 | 0x11 | -15.046 | -12.199 | -14.715 |
| 0x2 | -15.046 | -13.430 | -14.715 | 0x12 | -15.046 | -15.046 | -14.715 |
| 0x3 | -15.046 | -13.430 | -14.715 | 0x13 | -15.046 | -12.199 | -14.445 |
| 0x4 | -15.046 | -12.199 | -14.715 | 0x14 | -15.046 | -13.430 | -14.715 |
| 0x5 | -15.046 | -13.430 | -14.715 | 0x15 | -15.046 | -13.430 | -14.445 |
| 0x6 | -15.046 | -15.046 | -14.715 | 0x16 | -15.046 | -15.046 | -14.445 |
| 0x7 | -15.046 | -13.430 | -14.445 | 0x17 | -15.046 | -13.430 | -14.715 |
| 0x8 | -15.046 | -13.430 | -14.715 | 0x18 | -15.046 | -15.046 | -14.715 |
| 0x9 | -15.046 | -15.046 | -14.715 | 0x19 | -15.046 | -13.430 | -14.445 |
| 0xa | -15.046 | -15.046 | -14.715 | 0x1a | -15.046 | -15.046 | -14.445 |
| 0xb | -15.046 | -15.046 | -14.445 | 0x1b | -15.046 | -15.046 | -14.715 |
| 0xc | -15.046 | -12.199 | -14.715 | 0x1c | -15.046 | -13.430 | -14.445 |
| 0xd | -15.046 | -15.046 | -14.445 | 0x1d | -15.046 | -13.430 | -14.715 |
| 0xe | -15.046 | -13.430 | -14.445 | 0x1e | -15.046 | -15.046 | -14.715 |
| 0xf | -15.046 | -13.430 | -14.715 | 0x1f | -15.046 | -13.430 | -13.850 |
| 0x10 | -15.046 | -12.199 | -14.715 | | | | |

### 7.2 Analysis for a Higher Number of Rounds

For a higher number of rounds, we expect that the difference distribution table (DDT) of the S-box and specifically its interaction with the properties of $S^{-1} \circ S(\cdot \oplus k)$ plays an important role in the estimation of the bias. This can be seen from the formulas given in Section 4.3 where the probabilities of differential transitions over $S$ clearly appear and are multiplied with the EDP for the transition over a smaller number of rounds, where we showed the function $S^{-1} \circ S(\cdot \oplus k)$ to play a role.

Understanding better the interaction of the differential properties of those two functions and their influence on the bias is an interesting open question.

We computed the theoretical bias for up to 8+8 rounds for the original SCARF S-box, the `Ascon` S-box and the 5-bit APN used inside the cipher `Fides` [BBK$^+$13]. We observed that for these computations for many difference values, the bias was higher for `Ascon` than for SCARF and the APN S-box. This can be explained by the fact that the differential spectrum of the S-box of `Ascon` (the set of all the elements in the DDT) has much higher values than the differential spectrum of the SCARF S-box and of course of any APN S-box.

**Table 5.** Theoretical capacity for each number of rounds when we replace the S-box by $S_{alt}$, where $C$ and $C_{all}$ are computed as in Eq.(1) and Eq.((2), respectively.

| capacity | 2+2 | 3+3 | 4+4 | 5+5 | 6+6 | 7+7 | 8+8 |
|---|---|---|---|---|---|---|---|
| $\log_2(C)$ | $-3.29$ | $-13.30$ | $-32.43$ | $-42.43$ | $-63.29$ | $-73.29$ | $-93.49$ |
| $\log_2(C_{all})$ | $-2.30$ | $-13.30$ | $-31.43$ | $-42.43$ | $-62.29$ | $-73.29$ | $-92.49$ |

### 7.3 Searching for Alternative S-boxes for SCARF

An interesting question is whether we can replace the original SCARF S-box with a different 5-bit S-box such that the bias after 8+8 rounds is lower than for the original SCARF. Of course, the new S-box has to follow the same design criteria as the original one. More precisely, it must ensure the low latency of the global design, i.e., the maximum gate depth using 2-bit `NAND`, 2-bit `NOR` and `INV` gates should be 4. It must also have the same cryptographic properties as the original S-box, which means having a differential uniformity of at most 4, a linearity of at most 12 and a maximal algebraic degree, i.e., 4.

Using the tool of [Ras22], given the above criteria and a restriction on the coordinate functions to be extended bit-permutation equivalent of each other, we found 1016 S-box representatives up to equivalence. Note that in the SCARF original S-box, all the coordinates are the same function and the inputs for each coordinate is just a rotation of the inputs for the first coordinate. However, in this search, by fixing all the coordinates to use the same function, we allow the inputs to be any permutation of the inputs for the first coordinate along with a constant addition.

Applying bit-permutations, one at the input and one at the output of an S-box, does not change the aforementioned criteria, but it can affect the capacity. However, using two bit-permutations, $P_0$ and $P_1$, on either side of the S-box will result in the same capacity as using the combined bit-permutation $P_0 \circ P_1$ on just one side of the S-box. Therefore, we explored 1016 × 5! S-boxes and estimated the capacity using our tool as described in Section 4. Among them, the one with table representation

$$\begin{aligned} S_{alt} =[&\texttt{00}, \texttt{01}, \texttt{03}, \texttt{0D}, \texttt{06}, \texttt{13}, \texttt{16}, \texttt{0F}, \texttt{19}, \texttt{10}, \texttt{0B}, \texttt{17}, \texttt{09}, \texttt{1D}, \texttt{1A}, \texttt{1C}, \\ &\texttt{1E}, \texttt{0C}, \texttt{15}, \texttt{04}, \texttt{08}, \texttt{1B}, \texttt{11}, \texttt{0A}, \texttt{1F}, \texttt{14}, \texttt{12}, \texttt{02}, \texttt{05}, \texttt{07}, \texttt{18}, \texttt{0E}] \end{aligned}$$

achieves the best security against the multiple-tweak differential attack in 8+8 rounds. Table 5 summarizes $C$ and $C_{all}$ when we replace the S-box with $S_{alt}$. Interestingly, $S_{alt}$ is worse than the original S-box up to 3+3 rounds but improves the security from 4+4 rounds. Finally, the theoretical capacity reaches $2^{-93.49}$ for 8+8 rounds, which is better than $2^{-88.9514}$ for the original S-box.

We finally revisit the bit security when we replace the S-box. On the security requirement 2, we can collect $2^{29} \times 2^{29} \times 2^{9} = 2^{67}$ pairs. Then, the distinguishing advantage is about $2^{-14.57}$. Therefore, the bit security is $44.95 + 13.57 \times 2 = 72.09$. Although it is improved, the bit security is still lower than 80. In other

**Table 6.** Experimental comparison for 4+4 rounds with four S-boxes. We obtained these results using $2^{35}$ pairs with 5000 repetitions. Note that to compute $\mu_1$, we did experiments using a random 10-bit tweakable block cipher.

| | capacity | theoretical estimations | | experimental results | |
|---|---|---|---|---|---|
| | | $\mu_1 - \mu_0$ | $\sigma_1^2$ | $\mu_1 - \mu_0$ | $\sigma_1^2$ |
| $S_{orig.}$ | $2^{-32.20}$ | 6.98 | 6.98 | 7.18 | 7.09 |
| $S_{\mathtt{Fides}}$ | $2^{-35.09}$ | 0.94 | 0.94 | 1.00 | 0.96 |
| $S_{\mathtt{Ascon}}$ | $2^{-25.89}$ | 533.75 | 533.82 | 553.12 | 682.20 |
| $S_{alt.}$ | $2^{-32.43}$ | 5.95 | 5.95 | 5.85 | 5.92 |

words, the multi-key distinguishing attack still works even if we replace the S-box with $S_{alt}$. The security requirement 1 limits the number of pairs that can be collected by $2^{51}$. Then, the distinguishing advantage is 22.57. Thus, we have $40 + 21.57 \times 2 = 83.14$, which is larger than 80.

### 7.4 Experiments

We provide an experimental verification for our discussion. We compared differential capacities for 4+4 rounds among four S-boxes, $S_{orig.}$, $S_{alt.}$, $S_{\mathtt{Ascon}}$, and $S_{\mathtt{Fides}}$, where $S_{\mathtt{Ascon}}$ and $S_{\mathtt{Fides}}$ are

$$\begin{aligned} S_{\mathtt{Ascon}} =& [\mathtt{04}, \mathtt{0b}, \mathtt{1f}, \mathtt{14}, \mathtt{1a}, \mathtt{15}, \mathtt{09}, \mathtt{02}, \mathtt{1b}, \mathtt{05}, \mathtt{08}, \mathtt{12}, \mathtt{1d}, \mathtt{03}, \mathtt{06}, \mathtt{1c}, \\ & \mathtt{1e}, \mathtt{13}, \mathtt{07}, \mathtt{0e}, \mathtt{00}, \mathtt{0d}, \mathtt{11}, \mathtt{18}, \mathtt{10}, \mathtt{0c}, \mathtt{01}, \mathtt{19}, \mathtt{16}, \mathtt{0a}, \mathtt{0f}, \mathtt{17}], \\ S_{\mathtt{Fides}} =& [\mathtt{01}, \mathtt{00}, \mathtt{19}, \mathtt{1a}, \mathtt{11}, \mathtt{1d}, \mathtt{15}, \mathtt{1b}, \mathtt{14}, \mathtt{05}, \mathtt{04}, \mathtt{17}, \mathtt{0e}, \mathtt{12}, \mathtt{02}, \mathtt{1c}, \\ & \mathtt{0f}, \mathtt{08}, \mathtt{06}, \mathtt{03}, \mathtt{0d}, \mathtt{07}, \mathtt{18}, \mathtt{10}, \mathtt{1e}, \mathtt{09}, \mathtt{1f}, \mathtt{0a}, \mathtt{16}, \mathtt{0c}, \mathtt{0b}, \mathtt{13}]. \end{aligned}$$

For all S-boxes, our experimental results almost match the theoretical estimations based on the EDP. As expected, $S_{\mathtt{Fides}}$ is the most secure, $S_{\mathtt{Ascon}}$ is weak, and $S_{alt}$ is superior to the original S-box, $S_{orig.}$.

## 8 Conclusion

In this work, we provided the first third-party cryptanalysis of the tweakable block cipher SCARF, by means of multiple-tweak differential cryptanalysis. We first provided a theoretical framework to compute the bias of the differential transitions for any number of rounds and confirmed the theory by experimental verification for up to 5 rounds. We then mounted a key recovery attack on 7 out of 8 rounds of the cipher. In parallel, we showed distinguishing attacks on full 8-round SCARF in the multi-key setting that demonstrate that in this particular scenario the cipher does not offer the claimed 80-bit security. An interesting open question is what could be said in the single-key model, and to answer this question the actual notion of bit security should probably be re-defined. Finally, the practical impact of SCARF's vulnerabilities in real-world applications, such as its effectiveness against cache attacks under realistic conditions, needs further exploration to understand whether there is a true risk posed by multi-key distinguishers in constructing victim sets for cache attacks. Last, we analyzed the role that the differential properties of the S-box play in this attack. We showed in particular that it is possible to replace the original S-box of SCARF with a different one that follows the same design criteria as the S-box of SCARF but that offers a higher resistance against multiple-tweak differential attacks. However, we also showed that the replacement of the S-box with the best possible variant would still not prevent the distinguisher on 8+8 rounds in the multi-key setting.

**Acknowledgements.** Christina Boura was partially supported by the French Agence Nationale de la Recherche through the SWAP project under Contract ANR-21-CE39-0012 and through the France 2030 program under grant agreement No. ANR-22-PECY-0010. Besides, Shahram Rasoolzadeh is funded by the ERC project 101097056 (SYMTRUST) and Dhiman Saha was supported by the Science and Engineering Research Board (SERB), Department of Science and Technology, Government of India, under MATRICS scheme File No. MTR/2023/001161. Finally, the authors would like to thank the Dagstuhl Seminar 24041 on Symmetric Cryptography that gave the opportunity to the authors to initiate this collaboration.

## References

aes01. Advanced encryption standard (AES). National Institute of Standards and Technology. NIST FIPS PUB 197, U.S. Department of Commerce, 2001.

BBK$^+$13. Begül Bilgin, Andrey Bogdanov, Miroslav Knezevic, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES 2013*, volume 8086 of *Lecture Notes in Computer Science*, pages 142–158. Springer, 2013.

BC18. Christina Boura and Anne Canteaut. On the boomerang uniformity of cryptographic Sboxes. *IACR Trans. Symmetric Cryptol.*, 2018(3):290–310, 2018.

BCG$^+$12. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.

BDD$^+$23. Yanis Belkheyar, Joan Daemen, Christoph Dobraunig, Santosh Ghosh, and Shahram Rasoolzadeh. BipBip: A low-latency tweakable block cipher with small dimensions. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2023(1):326–368, 2023.

BDPA11. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The Keccak reference. Submission to NIST (Round 3), 2011.

BGN12. Céline Blondeau, Benoît Gérard, and Kaisa Nyberg. Multiple differential cryptanalysis using LLR and $\chi$ 2 statistics. In Ivan Visconti and Roberto De Prisco, editors, *SCN 2012*, volume 7485 of *Lecture Notes in Computer Science*, pages 343–360. Springer, 2012.

BJK$^+$16. Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

BJV04. Thomas Baignères, Pascal Junod, and Serge Vaudenay. How far can we go beyond linear cryptanalysis? In Pil Joong Lee, editor, *ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 432–450. Springer, 2004.

BS90. Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

CGL$^+$23. Federico Canale, Tim Güneysu, Gregor Leander, Jan Philipp Thoma, Yosuke Todo, and Rei Ueno. SCARF - A low-latency block cipher for secure cache-randomization. In Joseph A. Calandrino and Carmela Troncoso, editors, *USENIX 2023*, pages 1937–1954. USENIX Association, 2023.

CHP$^+$18. Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714. Springer, 2018.

DEMS21. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.*, 34(3):33, 2021.

DKLS20. Orr Dunkelman, Abhishek Kumar, Eran Lambooij, and Somitra Kumar Sanadhya. Cryptanalysis of Feistel-based format-preserving encryption. *IACR Cryptol. ePrint Arch.*, page 1311, 2020.

LMM91. Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald W. Davies, editor, *EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer, 1991.

Mat93. Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Tor Helleseth, editor, *EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

ML15. Nicky Mouha and Atul Luykx. Multi-key security: The Even-Mansour construction revisited. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 209–223. Springer, 2015.

MW18. Daniele Micciancio and Michael Walter. On the bit security of cryptographic primitives. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 3–28. Springer, 2018.

Pat01. Jacques Patarin. Generic attacks on Feistel schemes. In Colin Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 2001.

Pat04. Jacques Patarin. Security of random Feistel schemes with 5 or more rounds. In Matthew K. Franklin, editor, *CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2004.

Pat08. Jacques Patarin. Generic attacks on Feistel schemes. *IACR Cryptol. ePrint Arch.*, page 36, 2008.

Ras22. Shahram Rasoolzadeh. Low-latency Boolean functions and bijective S-boxes. *IACR Trans. Symmetric Cryptol.*, 2022(3):403–447, 2022.

WY21. Shun Watanabe and Kenji Yasunaga. Bit security as computational cost for winning games with high probability. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part III*, volume 13092 of *Lecture Notes in Computer Science*, pages 161–188. Springer, 2021.

WY23. Shun Watanabe and Kenji Yasunaga. Unified view for notions of bit security. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part VI*, volume 14443 of *Lecture Notes in Computer Science*, pages 361–389. Springer, 2023.

# A DDT for $S$ and special DDT for $S^{-1} \circ S$

## A.1 DDT for $S$

**Table 7.** Difference distribution table (DDT) of the S-box $S$. The element at row $\alpha$ and column $\beta$ corresponds to the number of solutions of the equation $\#\{x \in \mathbb{F}_2^5 \mid S(x) \oplus S(x \oplus \alpha) = \beta\}$

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 32 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 01 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 2 | 4 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 |
| 02 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 0 |
| 03 | 0 | 2 | 2 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 2 |
| 04 | 0 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 0 |
| 05 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 2 |
| 06 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 2 |
| 07 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 0 | 2 | 2 | 0 | 4 | 0 | 2 | 0 | 0 | 0 |
| 08 | 0 | 0 | 4 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 0 |
| 09 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 4 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 2 |
| 0A | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 4 | 0 | 0 | 2 |
| 0B | 0 | 0 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 4 | 2 | 2 | 2 |
| 0C | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 2 | 0 | 2 |
| 0D | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 4 | 4 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 2 |
| 0E | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 2 | 4 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0F | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 4 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 2 | 0 | 2 | 2 | 0 |
| 10 | 0 | 2 | 0 | 2 | 4 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 0 |
| 11 | 0 | 2 | 2 | 4 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 2 |
| 12 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 4 | 2 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 2 | 2 |
| 13 | 0 | 2 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 4 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 2 |
| 15 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 2 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 4 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 4 | 2 | 2 | 0 | 2 | 2 | 2 |
| 17 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 4 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 |
| 18 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 2 | 4 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 |
| 19 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 0 |
| 1A | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 4 | 0 | 4 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 2 |
| 1B | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 |
| 1C | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 |
| 1D | 0 | 0 | 2 | 2 | 0 | 4 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 |
| 1E | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 4 | 2 | 0 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 |
| 1F | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 4 | 4 | 0 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 2 |

## A.2 Special DDT for $S^{-1} \circ S$

Table 8 provides the number of solutions of the equation $\#\{(x, k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5 \mid S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha) \oplus k) = \beta\}$. It can be seen as a special form of DDT for the function $S^{-1} \circ S$, where the key is taken into account.

**Table 8.** $\#\{(x,k) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5 \mid S^{-1}(S(x) \oplus k) \oplus S^{-1}(S(x \oplus \alpha) \oplus k) = \beta\}$

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | $2^{10}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 01 | 0 | 72 | 28 | 20 | 36 | 36 | 32 | 32 | 36 | 20 | 40 | 36 | 32 | 24 | 40 | 28 | 28 | 32 | 40 | 28 | 36 | 28 | 24 | 32 | 32 | 40 | 32 | 28 | 36 | 40 | 24 | 32 |
| 02 | 0 | 28 | 72 | 32 | 28 | 40 | 20 | 28 | 36 | 36 | 36 | 28 | 32 | 24 | 32 | 32 | 36 | 32 | 20 | 40 | 40 | 32 | 36 | 28 | 32 | 36 | 24 | 40 | 40 | 24 | 28 | 32 |
| 03 | 0 | 20 | 32 | 72 | 32 | 28 | 40 | 24 | 32 | 28 | 24 | 32 | 44 | 32 | 40 | 32 | 32 | 40 | 32 | 36 | 24 | 32 | 32 | 44 | 44 | 32 | 32 | 32 | 28 | 24 | 28 | 20 |
| 04 | 0 | 36 | 28 | 32 | 72 | 20 | 32 | 40 | 28 | 40 | 40 | 32 | 20 | 36 | 28 | 28 | 36 | 32 | 36 | 36 | 36 | 24 | 28 | 40 | 32 | 40 | 24 | 24 | 32 | 28 | 32 | 32 |
| 05 | 0 | 36 | 40 | 28 | 20 | 72 | 32 | 24 | 36 | 32 | 28 | 28 | 28 | 40 | 36 | 24 | 40 | 24 | 28 | 32 | 32 | 48 | 28 | 36 | 24 | 24 | 32 | 32 | 36 | 28 | 40 | 36 |
| 06 | 0 | 32 | 20 | 40 | 32 | 32 | 72 | 36 | 32 | 24 | 28 | 32 | 40 | 32 | 24 | 44 | 32 | 44 | 28 | 32 | 24 | 32 | 32 | 32 | 44 | 28 | 32 | 24 | 40 | 28 | 32 | 20 |
| 07 | 0 | 32 | 28 | 24 | 40 | 24 | 36 | 80 | 36 | 36 | 32 | 28 | 32 | 28 | 40 | 24 | 40 | 40 | 36 | 40 | 24 | 20 | 32 | 32 | 28 | 24 | 20 | 36 | 24 | 36 | 24 | 48 |
| 08 | 0 | 36 | 36 | 32 | 28 | 36 | 32 | 36 | 72 | 36 | 20 | 24 | 32 | 28 | 40 | 40 | 28 | 32 | 40 | 40 | 40 | 24 | 32 | 24 | 20 | 32 | 36 | 28 | 28 | 32 | 28 | 32 |
| 09 | 0 | 20 | 36 | 28 | 40 | 32 | 24 | 36 | 36 | 72 | 32 | 40 | 24 | 48 | 24 | 28 | 40 | 32 | 28 | 36 | 28 | 28 | 32 | 40 | 28 | 24 | 28 | 24 | 32 | 36 | 32 | 36 |
| 0A | 0 | 40 | 36 | 24 | 40 | 28 | 28 | 32 | 20 | 32 | 72 | 48 | 32 | 28 | 24 | 36 | 36 | 24 | 32 | 24 | 28 | 32 | 28 | 32 | 28 | 36 | 40 | 28 | 36 | 40 | 24 | 36 |
| 0B | 0 | 36 | 28 | 32 | 32 | 28 | 32 | 28 | 24 | 40 | 48 | 80 | 32 | 24 | 20 | 36 | 24 | 32 | 28 | 32 | 32 | 40 | 40 | 36 | 32 | 28 | 24 | 40 | 20 | 48 | 24 | 24 |
| 0C | 0 | 32 | 32 | 44 | 20 | 28 | 40 | 32 | 32 | 24 | 32 | 32 | 72 | 32 | 36 | 32 | 32 | 44 | 24 | 28 | 28 | 32 | 32 | 24 | 40 | 40 | 32 | 28 | 24 | 32 | 44 | 20 |
| 0D | 0 | 24 | 24 | 32 | 36 | 40 | 32 | 28 | 28 | 48 | 28 | 24 | 32 | 80 | 32 | 40 | 32 | 32 | 32 | 20 | 28 | 24 | 40 | 48 | 32 | 20 | 40 | 24 | 28 | 36 | 36 | 24 |
| 0E | 0 | 40 | 32 | 40 | 28 | 36 | 24 | 40 | 40 | 24 | 24 | 20 | 36 | 32 | 80 | 32 | 36 | 28 | 36 | 24 | 32 | 20 | 28 | 36 | 32 | 24 | 28 | 36 | 40 | 24 | 24 | 48 |
| 0F | 0 | 28 | 32 | 32 | 28 | 24 | 44 | 24 | 40 | 28 | 36 | 36 | 32 | 40 | 32 | 72 | 24 | 28 | 40 | 24 | 32 | 24 | 36 | 28 | 24 | 36 | 48 | 32 | 36 | 32 | 28 | 24 |
| 10 | 0 | 28 | 36 | 32 | 36 | 40 | 32 | 40 | 28 | 40 | 36 | 24 | 32 | 32 | 36 | 24 | 72 | 20 | 36 | 32 | 20 | 36 | 24 | 28 | 32 | 28 | 28 | 32 | 40 | 28 | 40 | 32 |
| 11 | 0 | 32 | 32 | 40 | 32 | 24 | 44 | 40 | 32 | 32 | 24 | 32 | 44 | 32 | 28 | 28 | 20 | 72 | 28 | 24 | 28 | 32 | 32 | 32 | 40 | 36 | 32 | 44 | 32 | 32 | 24 | 20 |
| 12 | 0 | 40 | 20 | 32 | 36 | 28 | 28 | 36 | 40 | 28 | 32 | 28 | 24 | 32 | 36 | 40 | 36 | 28 | 72 | 24 | 32 | 28 | 40 | 24 | 24 | 32 | 48 | 36 | 24 | 32 | 28 | 36 |
| 13 | 0 | 28 | 40 | 36 | 36 | 32 | 32 | 40 | 40 | 36 | 24 | 32 | 28 | 20 | 24 | 24 | 32 | 24 | 24 | 80 | 36 | 28 | 28 | 24 | 40 | 40 | 20 | 32 | 24 | 36 | 36 | 48 |
| 14 | 0 | 36 | 40 | 24 | 36 | 32 | 24 | 24 | 40 | 28 | 28 | 32 | 28 | 28 | 32 | 32 | 20 | 28 | 32 | 36 | 72 | 40 | 48 | 28 | 32 | 36 | 28 | 40 | 24 | 24 | 36 | 36 |
| 15 | 0 | 28 | 32 | 32 | 24 | 48 | 32 | 20 | 24 | 28 | 32 | 40 | 32 | 24 | 20 | 24 | 36 | 32 | 28 | 28 | 40 | 80 | 24 | 36 | 32 | 32 | 40 | 36 | 28 | 40 | 48 | 24 |
| 16 | 0 | 24 | 36 | 32 | 28 | 28 | 32 | 32 | 32 | 32 | 28 | 40 | 32 | 40 | 28 | 36 | 24 | 32 | 40 | 28 | 48 | 24 | 80 | 40 | 32 | 20 | 24 | 48 | 20 | 24 | 36 | 24 |
| 17 | 0 | 32 | 28 | 44 | 40 | 36 | 32 | 32 | 24 | 40 | 32 | 36 | 24 | 48 | 36 | 28 | 28 | 32 | 24 | 24 | 28 | 36 | 40 | 72 | 28 | 24 | 24 | 28 | 36 | 32 | 32 | 24 |
| 18 | 0 | 32 | 32 | 44 | 32 | 24 | 44 | 28 | 20 | 28 | 28 | 32 | 40 | 32 | 32 | 24 | 32 | 40 | 24 | 40 | 32 | 32 | 32 | 28 | 72 | 24 | 32 | 32 | 36 | 44 | 32 | 20 |
| 19 | 0 | 40 | 36 | 32 | 40 | 24 | 28 | 24 | 32 | 24 | 36 | 28 | 40 | 20 | 24 | 36 | 28 | 36 | 32 | 40 | 36 | 32 | 20 | 24 | 24 | 80 | 28 | 24 | 40 | 32 | 36 | 48 |
| 1A | 0 | 32 | 24 | 32 | 24 | 32 | 32 | 20 | 36 | 28 | 40 | 24 | 32 | 40 | 28 | 48 | 28 | 32 | 48 | 20 | 28 | 40 | 24 | 24 | 32 | 28 | 80 | 36 | 32 | 36 | 40 | 24 |
| 1B | 0 | 28 | 40 | 32 | 24 | 32 | 24 | 36 | 28 | 24 | 28 | 40 | 28 | 24 | 36 | 32 | 32 | 44 | 36 | 32 | 40 | 36 | 48 | 28 | 32 | 24 | 36 | 72 | 24 | 28 | 32 | 24 |
| 1C | 0 | 36 | 40 | 28 | 32 | 36 | 40 | 24 | 28 | 32 | 36 | 20 | 24 | 28 | 40 | 36 | 40 | 32 | 24 | 24 | 24 | 28 | 20 | 36 | 36 | 40 | 32 | 24 | 80 | 24 | 32 | 48 |
| 1D | 0 | 40 | 24 | 24 | 28 | 28 | 28 | 36 | 32 | 36 | 40 | 48 | 32 | 36 | 24 | 32 | 28 | 32 | 32 | 36 | 24 | 40 | 24 | 32 | 44 | 32 | 36 | 28 | 24 | 72 | 28 | 24 |
| 1E | 0 | 24 | 28 | 28 | 32 | 40 | 32 | 24 | 28 | 32 | 24 | 24 | 44 | 36 | 24 | 28 | 40 | 24 | 28 | 36 | 36 | 48 | 36 | 32 | 32 | 36 | 40 | 32 | 32 | 28 | 72 | 24 |
| 1F | 0 | 32 | 32 | 20 | 32 | 36 | 20 | 48 | 32 | 36 | 36 | 24 | 20 | 24 | 48 | 24 | 32 | 20 | 36 | 48 | 36 | 24 | 24 | 24 | 20 | 48 | 24 | 24 | 48 | 24 | 24 | 104 |

# B On the Trail-Based Estimation

In [DKLS20], the authors estimated the differential bias on Feistel ciphers by using the trail-based method. This estimation is indeed easy to understand, and is not contradicted in practice in the case of Feistel ciphers.

When we adopt such a view, we will focus on the following trials for $2r + 2r$ rounds:

$$\begin{aligned} &(0, \delta_0) \xrightarrow{R^2} (0, \delta_1) \rightarrow \cdots \rightarrow (0, \delta_r) \\ \rightarrow &(0, \delta_r) \xrightarrow{R^{-2}} (0, \delta_{r+1}) \rightarrow \cdots \rightarrow (0, \delta_{2r}) \end{aligned}$$

For arbitrary differences $\delta_0$ and $\delta_{2r}$, we estimate the differential bias as follows:

$$\varepsilon_{(0,\delta_0),(0,\delta_{2r})} = \sum_{(\delta_1,\delta_2,\ldots,\delta_{2r-2})} \prod_{i=0}^{r} P_S[\delta_i, \delta_{i+1}] \times P_S[\delta_{r+i+1}, \delta_{r+i}] \times 2^{-5r},$$

where $P_S$ denotes the differential probability for the S-box. This estimation is clearly inaccurate. We cannot explain that there is some differential bias leaning towards the negative in practice. This simple analysis does not work mainly because the assumption that the differential probability will behave randomly if the characteristics do not follow these trails is unrealistic.

Our theoretical estimation is based on the EDP. It assumes the Markov assumption only, and it can be justified in the multiple-tweak differential attack experimentally.

## C Details of Theoretical Estimation

We summarize the bias $\varepsilon$ for $4+4$, $5+5$, $6+6$, $7+7$, and $8+8$ (full) rounds in Tables 9, 10, 11, 12, and 13, respectively. Each row indicates the right-hand input difference, and each column indicates the right-hand output difference. Note that the left-hand input and output differences are always 0. Each entry corresponds to the $\log_2(|\varepsilon|)$ of the corresponding bias, and it is highlighted in light blue whenever $\varepsilon < 0$.

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 24.71 | 29.41 | 27.83 | 26.36 | 30.00 | 31.00 | 26.75 | 26.36 | 26.91 | 26.36 | 30.00 | 28.42 | 26.41 | 30.00 | 26.68 | 29.41 | 27.68 | 27.00 | 27.83 | 27.19 | 30.00 | 26.19 | 31.00 | 27.42 | 28.41 | 26.68 | 25.87 | 29.41 | 27.83 | 28.19 | 25.64 |
| 02 | 29.41 | 24.71 | 27.68 | 29.41 | 27.00 | 27.83 | 27.83 | 26.36 | 27.19 | 30.00 | 30.00 | 31.00 | 26.19 | 26.75 | 31.00 | 26.36 | 27.42 | 26.91 | 28.41 | 26.36 | 26.68 | 30.00 | 25.87 | 28.42 | 29.41 | 26.41 | 27.83 | 30.00 | 28.19 | 26.68 | 25.64 |
| 03 | 27.83 | 27.68 | 24.87 | 27.42 | 26.19 | 26.75 | 28.00 | 28.42 | 26.68 | 25.79 | 28.19 | 26.36 | 27.83 | 25.71 | 31.00 | 31.00 | 26.75 | 26.75 | 28.42 | 25.36 | 25.64 | 31.00 | 26.14 | 26.36 | 28.19 | 26.19 | 28.00 | 27.00 | 28.41 | 27.00 | 28.00 |
| 04 | 26.36 | 29.41 | 27.42 | 24.71 | 26.91 | 27.68 | 28.41 | 29.41 | 26.36 | 27.00 | 26.68 | 27.83 | 30.00 | 27.83 | 25.87 | 26.36 | 28.42 | 27.19 | 29.41 | 30.00 | 26.41 | 30.00 | 27.83 | 31.00 | 30.00 | 26.19 | 28.19 | 26.75 | 26.68 | 31.00 | 25.64 |
| 05 | 30.00 | 27.00 | 26.19 | 26.91 | 24.12 | 26.75 | 26.09 | 27.19 | 28.68 | 25.71 | 25.87 | 26.68 | 26.05 | 28.00 | 26.41 | 26.36 | 25.79 | 25.71 | 25.51 | 28.68 | 25.30 | 29.42 | 28.00 | 25.36 | 25.91 | 25.51 | 26.83 | 27.30 | 26.61 | 26.91 | 30.00 |
| 06 | 31.00 | 27.83 | 26.75 | 27.68 | 26.75 | 24.87 | 28.42 | 27.42 | 25.36 | 26.19 | 25.64 | 26.75 | 31.00 | 28.00 | 26.14 | 28.42 | 26.36 | 26.68 | 28.19 | 25.79 | 26.19 | 28.19 | 28.00 | 26.36 | 27.00 | 27.83 | 28.41 | 25.71 | 27.00 | 31.00 | 28.00 |
| 07 | 26.75 | 27.83 | 28.00 | 28.41 | 26.09 | 28.42 | 24.33 | 29.41 | 27.30 | 25.51 | 28.41 | 28.19 | 27.54 | 26.05 | 26.68 | 30.00 | 25.71 | 28.00 | 26.05 | 25.91 | 26.25 | 27.30 | 28.00 | 27.00 | 26.25 | 25.57 | 25.57 | 26.25 | 26.25 | 28.00 | 28.68 |
| 08 | 26.36 | 26.36 | 28.42 | 29.41 | 27.19 | 27.42 | 29.41 | 24.71 | 30.00 | 26.91 | 26.41 | 27.68 | 30.00 | 28.41 | 27.83 | 29.41 | 31.00 | 26.36 | 30.00 | 27.00 | 26.19 | 26.68 | 28.19 | 27.83 | 26.75 | 30.00 | 26.68 | 27.83 | 31.00 | 25.87 | 25.64 |
| 09 | 26.91 | 27.19 | 26.68 | 26.36 | 28.68 | 25.36 | 27.30 | 30.00 | 24.12 | 28.68 | 26.05 | 25.79 | 25.30 | 25.91 | 26.61 | 27.00 | 26.75 | 25.71 | 28.00 | 25.71 | 29.42 | 25.51 | 26.91 | 26.19 | 26.09 | 25.87 | 26.41 | 25.51 | 28.00 | 26.83 | 30.00 |
| 0A | 26.36 | 30.00 | 25.79 | 27.00 | 25.71 | 26.19 | 25.51 | 26.91 | 28.68 | 24.12 | 25.30 | 26.75 | 29.42 | 26.09 | 28.00 | 27.19 | 25.36 | 28.68 | 25.91 | 25.71 | 25.51 | 25.87 | 26.83 | 26.68 | 27.30 | 26.05 | 26.61 | 28.00 | 26.91 | 26.41 | 30.00 |
| 0B | 30.00 | 30.00 | 28.19 | 26.68 | 25.87 | 25.64 | 28.41 | 26.41 | 26.05 | 25.30 | 23.75 | 26.19 | 25.22 | 26.25 | 27.41 | 26.19 | 31.00 | 29.42 | 27.30 | 25.51 | 26.83 | 26.83 | 26.48 | 27.83 | 27.54 | 25.22 | 25.91 | 25.57 | 25.61 | 25.12 | 27.00 |
| 0C | 28.42 | 31.00 | 26.36 | 27.83 | 26.68 | 26.75 | 28.19 | 27.68 | 25.79 | 26.75 | 26.19 | 24.87 | 28.19 | 28.42 | 28.00 | 27.42 | 26.36 | 25.36 | 27.00 | 26.19 | 27.83 | 25.64 | 28.41 | 26.75 | 25.71 | 31.00 | 27.00 | 28.00 | 31.00 | 26.14 | 28.00 |
| 0D | 26.41 | 26.19 | 27.83 | 30.00 | 26.05 | 31.00 | 27.54 | 30.00 | 25.30 | 29.42 | 25.22 | 28.19 | 23.75 | 27.30 | 25.91 | 26.68 | 26.19 | 25.51 | 25.57 | 25.87 | 25.22 | 26.83 | 25.61 | 25.64 | 26.25 | 26.83 | 25.12 | 28.41 | 27.41 | 26.48 | 27.00 |
| 0E | 30.00 | 26.75 | 25.71 | 27.83 | 28.00 | 28.00 | 26.05 | 28.41 | 25.91 | 26.09 | 26.25 | 28.42 | 27.30 | 24.33 | 28.00 | 29.41 | 27.00 | 27.30 | 26.25 | 25.51 | 25.57 | 28.41 | 25.57 | 28.19 | 26.25 | 27.54 | 26.25 | 26.05 | 28.00 | 26.68 | 28.68 |
| 0F | 26.68 | 31.00 | 31.00 | 25.87 | 26.41 | 26.14 | 26.68 | 27.83 | 26.61 | 28.00 | 27.41 | 28.00 | 25.91 | 28.00 | 24.09 | 28.19 | 27.00 | 26.91 | 28.00 | 26.83 | 25.12 | 26.48 | 26.00 | 28.41 | 26.25 | 25.61 | 28.19 | 25.57 | 28.19 | 26.00 | 28.00 |
| 10 | 29.41 | 26.36 | 31.00 | 26.36 | 26.36 | 28.42 | 30.00 | 29.41 | 27.00 | 27.19 | 26.19 | 27.42 | 26.68 | 29.41 | 28.19 | 24.71 | 27.83 | 30.00 | 26.75 | 26.91 | 30.00 | 26.41 | 26.68 | 27.68 | 27.83 | 30.00 | 31.00 | 28.41 | 25.87 | 27.83 | 25.64 |
| 11 | 27.68 | 27.42 | 26.75 | 28.42 | 25.79 | 26.36 | 25.71 | 31.00 | 26.75 | 25.36 | 31.00 | 26.36 | 26.19 | 27.00 | 27.00 | 27.83 | 24.87 | 26.19 | 28.00 | 26.68 | 28.19 | 27.83 | 31.00 | 26.75 | 28.42 | 25.64 | 26.14 | 28.19 | 28.00 | 28.41 | 28.00 |
| 12 | 27.00 | 26.91 | 26.75 | 27.19 | 25.71 | 26.68 | 28.00 | 26.36 | 25.71 | 28.68 | 29.42 | 25.36 | 25.51 | 27.30 | 26.91 | 30.00 | 26.19 | 24.12 | 26.09 | 28.68 | 25.87 | 26.05 | 26.41 | 25.79 | 25.51 | 25.30 | 28.00 | 25.91 | 26.83 | 26.61 | 30.00 |
| 13 | 27.83 | 28.41 | 28.42 | 29.41 | 25.51 | 28.19 | 26.05 | 30.00 | 28.00 | 25.91 | 27.30 | 27.00 | 25.57 | 26.25 | 28.00 | 26.75 | 28.00 | 26.09 | 24.33 | 27.30 | 28.41 | 27.54 | 26.68 | 25.71 | 26.05 | 26.25 | 28.00 | 26.25 | 25.57 | 26.25 | 28.68 |
| 14 | 27.19 | 26.36 | 25.36 | 30.00 | 28.68 | 25.79 | 25.91 | 27.00 | 25.71 | 25.71 | 25.51 | 26.19 | 25.87 | 25.51 | 26.83 | 26.91 | 26.68 | 28.68 | 27.30 | 24.12 | 26.05 | 25.30 | 26.61 | 26.75 | 28.00 | 29.42 | 26.91 | 26.09 | 26.41 | 28.00 | 30.00 |
| 15 | 30.00 | 26.68 | 25.64 | 26.41 | 25.30 | 26.19 | 26.25 | 26.19 | 29.42 | 25.51 | 26.83 | 27.83 | 25.22 | 25.57 | 25.12 | 30.00 | 28.19 | 25.87 | 28.41 | 26.05 | 23.75 | 25.22 | 27.41 | 31.00 | 27.30 | 26.83 | 26.48 | 27.54 | 25.91 | 25.61 | 27.00 |
| 16 | 26.19 | 30.00 | 31.00 | 30.00 | 29.42 | 28.19 | 27.30 | 26.68 | 25.51 | 25.87 | 26.83 | 25.64 | 26.83 | 28.41 | 26.48 | 26.41 | 27.83 | 26.05 | 27.54 | 25.30 | 25.22 | 23.75 | 25.91 | 26.19 | 25.57 | 25.22 | 25.61 | 26.25 | 25.12 | 27.41 | 27.00 |
| 17 | 31.00 | 25.87 | 26.14 | 27.83 | 28.00 | 28.00 | 28.00 | 28.19 | 26.91 | 26.83 | 26.48 | 28.41 | 25.61 | 25.57 | 26.00 | 26.68 | 31.00 | 26.41 | 26.68 | 26.61 | 27.41 | 25.91 | 24.09 | 27.00 | 28.00 | 25.12 | 26.00 | 26.25 | 28.19 | 28.19 | 28.00 |
| 18 | 27.42 | 28.42 | 26.36 | 31.00 | 25.36 | 26.36 | 27.00 | 27.83 | 26.19 | 26.68 | 27.83 | 26.75 | 25.64 | 28.19 | 28.41 | 27.68 | 26.75 | 25.79 | 25.71 | 26.75 | 31.00 | 26.19 | 27.00 | 24.87 | 28.00 | 28.19 | 31.00 | 28.42 | 26.14 | 28.00 | 28.00 |
| 19 | 28.41 | 29.41 | 28.19 | 30.00 | 25.91 | 27.00 | 26.25 | 26.75 | 26.09 | 27.30 | 27.54 | 25.71 | 26.25 | 26.25 | 26.25 | 27.83 | 28.42 | 25.51 | 26.05 | 28.00 | 27.30 | 25.57 | 28.00 | 28.00 | 24.33 | 28.41 | 26.68 | 26.05 | 28.00 | 25.57 | 28.68 |
| 1A | 26.68 | 26.41 | 26.19 | 26.19 | 25.51 | 27.83 | 25.57 | 30.00 | 25.87 | 26.05 | 25.22 | 31.00 | 26.83 | 27.54 | 25.61 | 30.00 | 25.64 | 25.30 | 26.25 | 29.42 | 26.83 | 25.22 | 25.12 | 28.19 | 28.41 | 23.75 | 27.41 | 27.30 | 26.48 | 25.91 | 27.00 |
| 1B | 25.87 | 27.83 | 28.00 | 28.19 | 26.83 | 28.41 | 25.57 | 26.68 | 26.41 | 26.61 | 25.91 | 27.00 | 25.12 | 26.25 | 28.19 | 31.00 | 26.14 | 28.00 | 28.00 | 26.91 | 26.48 | 25.61 | 26.00 | 31.00 | 26.68 | 27.41 | 24.09 | 28.00 | 26.00 | 28.19 | 28.00 |
| 1C | 29.41 | 30.00 | 27.00 | 26.75 | 27.30 | 25.71 | 26.25 | 27.83 | 25.51 | 28.00 | 25.57 | 28.00 | 28.41 | 26.05 | 25.57 | 28.41 | 28.19 | 25.91 | 26.25 | 26.09 | 27.54 | 26.25 | 26.25 | 28.42 | 26.05 | 27.30 | 28.00 | 24.33 | 26.68 | 28.00 | 28.68 |
| 1D | 27.83 | 28.19 | 28.41 | 26.68 | 26.61 | 27.00 | 26.25 | 31.00 | 28.00 | 26.91 | 25.61 | 31.00 | 27.41 | 28.00 | 28.19 | 25.87 | 28.00 | 26.83 | 25.57 | 26.41 | 25.91 | 25.12 | 28.19 | 26.14 | 28.00 | 26.48 | 26.00 | 26.68 | 24.09 | 26.00 | 28.00 |
| 1E | 28.19 | 26.68 | 27.00 | 31.00 | 26.91 | 31.00 | 28.00 | 25.87 | 26.83 | 26.41 | 25.12 | 26.14 | 26.48 | 26.68 | 26.00 | 27.83 | 28.41 | 26.61 | 26.25 | 28.00 | 25.61 | 27.41 | 28.19 | 28.00 | 25.57 | 25.91 | 28.19 | 28.00 | 26.00 | 24.09 | 28.00 |
| 1F | 25.64 | 25.64 | 28.00 | 25.64 | 30.00 | 28.00 | 28.68 | 25.64 | 30.00 | 30.00 | 27.00 | 28.00 | 27.00 | 28.68 | 28.00 | 25.64 | 28.00 | 30.00 | 28.68 | 30.00 | 27.00 | 27.00 | 28.00 | 28.00 | 28.68 | 27.00 | 28.00 | 28.68 | 28.00 | 28.00 | 24.48 |

**Table 9.** Differential biases for 4+4 rounds.

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 29.72 | 34.39 | 32.82 | 31.36 | 34.96 | 36.09 | 31.75 | 31.36 | 31.91 | 31.36 | 35.05 | 33.43 | 31.41 | 35.05 | 31.67 | 34.39 | 32.67 | 32.01 | 32.82 | 32.20 | 35.05 | 31.19 | 36.09 | 32.42 | 33.40 | 31.68 | 30.87 | 34.39 | 32.84 | 33.18 | 30.64 |
| 02 | 34.39 | 29.72 | 32.67 | 34.39 | 32.01 | 32.82 | 32.82 | 31.36 | 32.20 | 34.96 | 35.05 | 36.09 | 31.19 | 31.75 | 36.09 | 31.36 | 32.42 | 31.91 | 33.40 | 31.36 | 31.68 | 35.05 | 30.87 | 33.43 | 34.39 | 31.41 | 32.84 | 35.05 | 33.18 | 31.67 | 30.64 |
| 03 | 32.82 | 32.67 | 29.87 | 32.42 | 31.19 | 31.76 | 33.01 | 33.43 | 31.67 | 30.79 | 33.18 | 31.36 | 32.84 | 30.72 | 35.91 | 36.09 | 31.76 | 31.75 | 33.43 | 30.35 | 30.64 | 35.91 | 31.15 | 31.36 | 33.21 | 31.19 | 32.99 | 32.01 | 33.40 | 31.99 | 32.99 |
| 04 | 31.36 | 34.39 | 32.42 | 29.72 | 31.91 | 32.67 | 33.40 | 34.39 | 31.36 | 32.01 | 31.68 | 32.82 | 35.05 | 32.82 | 30.87 | 31.36 | 33.43 | 32.20 | 34.39 | 34.96 | 31.41 | 35.05 | 32.84 | 36.09 | 35.05 | 31.19 | 33.18 | 31.75 | 31.67 | 36.09 | 30.64 |
| 05 | 34.96 | 32.01 | 31.19 | 31.91 | 29.12 | 31.75 | 31.09 | 32.20 | 33.70 | 30.72 | 30.87 | 31.67 | 31.05 | 32.99 | 31.41 | 31.36 | 30.79 | 30.72 | 30.51 | 33.70 | 30.30 | 34.45 | 32.99 | 30.35 | 30.91 | 30.51 | 31.83 | 32.29 | 31.60 | 31.92 | 35.05 |
| 06 | 36.09 | 32.82 | 31.76 | 32.67 | 31.75 | 29.87 | 33.43 | 32.42 | 30.35 | 31.19 | 30.64 | 31.76 | 35.91 | 33.01 | 31.15 | 33.43 | 31.36 | 31.67 | 33.21 | 30.79 | 31.19 | 33.18 | 32.99 | 31.36 | 32.01 | 32.84 | 33.40 | 30.72 | 31.99 | 35.91 | 32.99 |
| 07 | 31.75 | 32.82 | 33.01 | 33.40 | 31.09 | 33.43 | 29.33 | 34.39 | 32.29 | 30.51 | 33.40 | 33.21 | 32.53 | 31.05 | 31.67 | 35.05 | 30.72 | 32.99 | 31.05 | 30.91 | 31.24 | 32.31 | 33.01 | 32.01 | 31.24 | 30.57 | 30.58 | 31.24 | 31.25 | 32.99 | 33.70 |
| 08 | 31.36 | 31.36 | 33.43 | 34.39 | 32.20 | 32.42 | 34.39 | 29.72 | 34.96 | 31.91 | 31.41 | 32.67 | 35.05 | 33.40 | 32.84 | 34.39 | 36.09 | 31.36 | 35.05 | 32.01 | 31.19 | 31.68 | 33.18 | 32.82 | 31.75 | 35.05 | 31.67 | 32.82 | 36.09 | 30.87 | 30.64 |
| 09 | 31.91 | 32.20 | 31.67 | 31.36 | 33.70 | 30.35 | 32.29 | 34.96 | 29.12 | 33.70 | 31.05 | 30.79 | 30.30 | 30.91 | 31.60 | 32.01 | 31.75 | 30.72 | 32.99 | 30.72 | 34.45 | 30.51 | 31.92 | 31.19 | 31.09 | 30.87 | 31.41 | 30.51 | 32.99 | 31.83 | 35.05 |
| 0A | 31.36 | 34.96 | 30.79 | 32.01 | 30.72 | 31.19 | 30.51 | 31.91 | 33.70 | 29.12 | 30.30 | 31.75 | 34.45 | 31.09 | 32.99 | 32.20 | 30.35 | 33.70 | 30.91 | 30.72 | 30.51 | 30.87 | 31.83 | 31.67 | 32.29 | 31.05 | 31.60 | 32.99 | 31.92 | 31.41 | 35.05 |
| 0B | 35.05 | 35.05 | 33.18 | 31.68 | 30.87 | 30.64 | 33.40 | 31.41 | 31.05 | 30.30 | 28.75 | 31.19 | 30.22 | 31.24 | 32.41 | 31.19 | 35.91 | 34.45 | 32.31 | 30.51 | 31.84 | 31.84 | 31.47 | 32.84 | 32.53 | 30.22 | 30.92 | 30.57 | 30.61 | 30.12 | 32.01 |
| 0C | 33.43 | 36.09 | 31.36 | 32.82 | 31.67 | 31.76 | 33.21 | 32.67 | 30.79 | 31.75 | 31.19 | 29.87 | 33.18 | 33.43 | 32.99 | 32.42 | 31.36 | 30.35 | 32.01 | 31.19 | 32.84 | 30.64 | 33.40 | 31.76 | 30.72 | 35.91 | 31.99 | 33.01 | 35.91 | 31.15 | 32.99 |
| 0D | 31.41 | 31.19 | 32.84 | 35.05 | 31.05 | 35.91 | 32.53 | 35.05 | 30.30 | 34.45 | 30.22 | 33.18 | 28.75 | 32.31 | 30.92 | 31.68 | 31.19 | 30.51 | 30.57 | 30.87 | 30.22 | 31.84 | 30.61 | 30.64 | 31.24 | 31.84 | 30.12 | 33.40 | 32.41 | 31.47 | 32.01 |
| 0E | 35.05 | 31.75 | 30.72 | 32.82 | 32.99 | 33.01 | 31.05 | 33.40 | 30.91 | 31.09 | 31.24 | 33.43 | 32.31 | 29.33 | 33.01 | 34.39 | 32.01 | 32.29 | 31.24 | 30.51 | 30.57 | 33.40 | 30.58 | 33.21 | 31.24 | 32.53 | 31.25 | 31.05 | 32.99 | 31.67 | 33.70 |
| 0F | 31.67 | 36.09 | 35.91 | 30.87 | 31.41 | 31.15 | 31.67 | 32.84 | 31.60 | 32.99 | 32.41 | 32.99 | 30.92 | 33.01 | 29.09 | 33.18 | 31.99 | 31.92 | 32.99 | 31.83 | 30.12 | 31.47 | 31.00 | 33.40 | 31.25 | 30.61 | 33.21 | 30.58 | 33.21 | 31.00 | 33.01 |
| 10 | 34.39 | 31.36 | 36.09 | 31.36 | 31.36 | 33.43 | 35.05 | 34.39 | 32.01 | 32.20 | 31.19 | 32.42 | 31.68 | 34.39 | 33.18 | 29.72 | 32.82 | 34.96 | 31.75 | 31.91 | 35.05 | 31.41 | 31.67 | 32.67 | 32.82 | 35.05 | 36.09 | 33.40 | 30.87 | 32.84 | 30.64 |
| 11 | 32.67 | 32.42 | 31.76 | 33.43 | 30.79 | 31.36 | 30.72 | 36.09 | 31.75 | 30.35 | 35.91 | 31.36 | 31.19 | 32.01 | 31.99 | 32.82 | 29.87 | 31.19 | 33.01 | 31.67 | 33.18 | 32.84 | 35.91 | 31.76 | 33.43 | 30.64 | 31.15 | 33.21 | 32.99 | 33.40 | 32.99 |
| 12 | 32.01 | 31.91 | 31.75 | 32.20 | 30.72 | 31.67 | 32.99 | 31.36 | 30.72 | 33.70 | 34.45 | 30.35 | 30.51 | 32.29 | 31.92 | 34.96 | 31.19 | 29.12 | 31.09 | 33.70 | 30.87 | 31.05 | 31.41 | 30.79 | 30.51 | 30.30 | 32.99 | 30.91 | 31.83 | 31.60 | 35.05 |
| 13 | 32.82 | 33.40 | 33.43 | 34.39 | 30.51 | 33.21 | 31.05 | 35.05 | 32.99 | 30.91 | 32.31 | 32.01 | 30.57 | 31.24 | 32.99 | 31.75 | 33.01 | 31.09 | 29.33 | 32.29 | 33.40 | 32.53 | 31.67 | 30.72 | 31.05 | 31.24 | 33.01 | 31.24 | 30.58 | 31.25 | 33.70 |
| 14 | 32.20 | 31.36 | 30.35 | 34.96 | 33.70 | 30.79 | 30.91 | 32.01 | 30.72 | 30.72 | 30.51 | 31.19 | 30.87 | 30.51 | 31.83 | 31.91 | 31.67 | 33.70 | 32.29 | 29.12 | 31.05 | 30.30 | 31.60 | 31.75 | 32.99 | 34.45 | 31.92 | 31.09 | 31.41 | 32.99 | 35.05 |
| 15 | 35.05 | 31.68 | 30.64 | 31.41 | 30.30 | 31.19 | 31.24 | 31.19 | 34.45 | 30.51 | 31.84 | 32.84 | 30.22 | 30.57 | 30.12 | 35.05 | 33.18 | 30.87 | 33.40 | 31.05 | 28.75 | 30.22 | 32.41 | 35.91 | 32.31 | 31.84 | 31.47 | 32.53 | 30.92 | 30.61 | 32.01 |
| 16 | 31.19 | 35.05 | 35.91 | 35.05 | 34.45 | 33.18 | 32.31 | 31.68 | 30.51 | 30.87 | 31.84 | 30.64 | 31.84 | 33.40 | 31.47 | 31.41 | 32.84 | 31.05 | 32.53 | 30.30 | 30.22 | 28.75 | 30.92 | 31.19 | 30.57 | 30.22 | 30.61 | 31.24 | 30.12 | 32.41 | 32.01 |
| 17 | 36.09 | 30.87 | 31.15 | 32.84 | 32.99 | 32.99 | 33.01 | 33.18 | 31.92 | 31.83 | 31.47 | 33.40 | 30.61 | 30.58 | 31.00 | 31.67 | 35.91 | 31.41 | 31.67 | 31.60 | 32.41 | 30.92 | 29.09 | 31.99 | 32.99 | 30.12 | 31.00 | 31.25 | 33.21 | 33.21 | 33.01 |
| 18 | 32.42 | 33.43 | 31.36 | 36.09 | 30.35 | 31.36 | 32.01 | 32.82 | 31.19 | 31.67 | 32.84 | 31.76 | 30.64 | 33.21 | 33.40 | 32.67 | 31.76 | 30.79 | 30.72 | 31.75 | 35.91 | 31.19 | 31.99 | 29.87 | 33.01 | 33.18 | 35.91 | 33.43 | 31.15 | 32.99 | 32.99 |
| 19 | 33.40 | 34.39 | 33.21 | 35.05 | 30.91 | 32.01 | 31.24 | 31.75 | 31.09 | 32.29 | 32.53 | 30.72 | 31.24 | 31.24 | 31.25 | 32.82 | 33.43 | 30.51 | 31.05 | 32.99 | 32.31 | 30.57 | 32.99 | 33.01 | 29.33 | 33.40 | 31.67 | 31.05 | 33.01 | 30.58 | 33.70 |
| 1A | 31.68 | 31.41 | 31.19 | 31.19 | 30.51 | 32.84 | 30.57 | 35.05 | 30.87 | 31.05 | 30.22 | 35.91 | 31.84 | 32.53 | 30.61 | 35.05 | 30.64 | 30.30 | 31.24 | 34.45 | 31.84 | 30.22 | 30.12 | 33.18 | 33.40 | 28.75 | 32.41 | 32.31 | 31.47 | 30.92 | 32.01 |
| 1B | 30.87 | 32.84 | 32.99 | 33.18 | 31.83 | 33.40 | 30.58 | 31.67 | 31.41 | 31.60 | 30.92 | 31.99 | 30.12 | 31.25 | 33.21 | 36.09 | 31.15 | 32.99 | 33.01 | 31.92 | 31.47 | 30.61 | 31.00 | 35.91 | 31.67 | 32.41 | 29.09 | 32.99 | 31.00 | 33.21 | 33.01 |
| 1C | 34.39 | 35.05 | 32.01 | 31.75 | 32.29 | 30.72 | 31.24 | 32.82 | 30.51 | 32.99 | 30.57 | 33.01 | 33.40 | 31.05 | 30.58 | 33.40 | 33.21 | 30.91 | 31.24 | 31.09 | 32.53 | 31.24 | 31.25 | 33.43 | 31.05 | 32.31 | 32.99 | 29.33 | 31.67 | 33.01 | 33.70 |
| 1D | 32.84 | 33.18 | 33.40 | 31.67 | 31.60 | 31.99 | 31.25 | 36.09 | 32.99 | 31.92 | 30.61 | 35.91 | 32.41 | 32.99 | 33.21 | 30.87 | 32.99 | 31.83 | 30.58 | 31.41 | 30.92 | 30.12 | 33.21 | 31.15 | 33.01 | 31.47 | 31.00 | 31.67 | 29.09 | 31.00 | 33.01 |
| 1E | 33.18 | 31.67 | 31.99 | 36.09 | 31.92 | 35.91 | 32.99 | 30.87 | 31.83 | 31.41 | 30.12 | 31.15 | 31.47 | 31.67 | 31.00 | 32.84 | 33.40 | 31.60 | 31.25 | 32.99 | 30.61 | 32.41 | 33.21 | 32.99 | 30.58 | 30.92 | 33.21 | 33.01 | 31.00 | 29.09 | 33.01 |
| 1F | 30.64 | 30.64 | 32.99 | 30.64 | 35.05 | 32.99 | 33.70 | 30.64 | 35.05 | 35.05 | 32.01 | 32.99 | 32.01 | 33.70 | 33.01 | 30.64 | 32.99 | 35.05 | 33.70 | 35.05 | 32.01 | 32.01 | 33.01 | 32.99 | 33.70 | 32.01 | 33.01 | 33.70 | 33.01 | 33.01 | 29.48 |

**Table 10.** Differential biases for 5+5 rounds.

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 39.17 | 43.40 | 50.00 | 40.75 | 44.39 | 41.73 | 41.88 | 40.75 | 39.98 | 41.87 | 42.16 | 40.77 | 39.94 | 43.62 | 40.85 | 43.40 | 43.85 | 42.63 | 42.71 | 42.71 | 42.88 | 39.93 | 43.08 | 41.36 | 40.91 | 42.19 | 40.60 | 44.71 | 42.21 | 43.34 | 39.94 |
| 02 | 43.40 | 39.17 | 43.85 | 43.40 | 42.63 | 50.00 | 42.71 | 40.75 | 42.71 | 44.39 | 42.88 | 41.73 | 39.93 | 41.88 | 43.08 | 40.75 | 41.36 | 39.98 | 40.91 | 41.87 | 42.19 | 42.16 | 40.60 | 40.77 | 44.71 | 39.94 | 42.21 | 43.62 | 43.34 | 40.85 | 39.94 |
| 03 | 50.00 | 43.85 | 39.62 | 41.36 | 44.79 | 41.42 | 45.48 | 40.77 | 44.17 | 40.88 | 40.77 | 41.50 | 40.32 | 40.61 | 41.50 | 41.73 | 41.42 | 43.26 | 41.15 | 40.49 | 40.32 | 41.93 | 40.92 | 41.50 | 40.85 | 41.16 | 40.61 | 45.75 | 41.26 | 40.51 | 42.01 |
| 04 | 40.75 | 43.40 | 41.36 | 39.17 | 39.98 | 43.85 | 40.91 | 43.40 | 41.87 | 42.63 | 42.19 | 50.00 | 42.16 | 42.71 | 40.60 | 40.75 | 40.77 | 42.71 | 44.71 | 44.39 | 39.94 | 42.88 | 42.21 | 41.73 | 43.62 | 39.93 | 43.34 | 41.88 | 40.85 | 43.08 | 39.94 |
| 05 | 44.39 | 42.63 | 44.79 | 39.98 | 38.92 | 43.26 | 41.70 | 42.71 | 39.96 | 41.56 | 39.54 | 44.17 | 40.68 | 39.92 | 43.59 | 41.87 | 40.88 | 41.56 | 39.98 | 39.96 | 40.75 | 40.89 | 42.31 | 40.49 | 40.38 | 39.40 | 50.00 | 40.65 | 42.20 | 41.24 | 42.41 |
| 06 | 41.73 | 50.00 | 41.42 | 43.85 | 43.26 | 39.62 | 41.15 | 41.36 | 40.49 | 44.79 | 40.32 | 41.42 | 41.93 | 45.48 | 40.92 | 40.77 | 41.50 | 44.17 | 40.85 | 40.88 | 41.16 | 40.77 | 40.61 | 41.50 | 45.75 | 40.32 | 41.26 | 40.61 | 40.51 | 41.50 | 42.01 |
| 07 | 41.88 | 42.71 | 45.48 | 40.91 | 41.70 | 41.15 | 38.69 | 44.71 | 40.65 | 39.98 | 41.71 | 40.85 | 43.56 | 40.44 | 40.33 | 43.62 | 40.61 | 39.92 | 40.44 | 40.38 | 39.70 | 40.01 | 42.78 | 45.75 | 39.74 | 39.54 | 40.04 | 39.74 | 41.34 | 41.18 | 43.59 |
| 08 | 40.75 | 40.75 | 40.77 | 43.40 | 42.71 | 41.36 | 44.71 | 39.17 | 44.39 | 39.98 | 39.94 | 43.85 | 42.88 | 40.91 | 42.21 | 43.40 | 41.73 | 41.87 | 43.62 | 42.63 | 39.93 | 42.19 | 43.34 | 50.00 | 41.88 | 42.16 | 40.85 | 42.71 | 43.08 | 40.60 | 39.94 |
| 09 | 39.98 | 42.71 | 44.17 | 41.87 | 39.96 | 40.49 | 40.65 | 44.39 | 38.92 | 39.96 | 40.68 | 40.88 | 40.75 | 40.38 | 42.20 | 42.63 | 43.26 | 41.56 | 39.92 | 41.56 | 40.89 | 39.40 | 41.24 | 44.79 | 41.70 | 39.54 | 43.59 | 39.98 | 42.31 | 50.00 | 42.41 |
| 0A | 41.87 | 44.39 | 40.88 | 42.63 | 41.56 | 44.79 | 39.98 | 39.98 | 39.96 | 38.92 | 40.75 | 43.26 | 40.89 | 41.70 | 42.31 | 42.71 | 40.49 | 39.96 | 40.38 | 41.56 | 39.40 | 39.54 | 50.00 | 44.17 | 40.65 | 40.68 | 42.20 | 39.92 | 41.24 | 43.59 | 42.41 |
| 0B | 42.16 | 42.88 | 40.77 | 42.19 | 39.54 | 40.32 | 41.71 | 39.94 | 40.68 | 40.75 | 38.19 | 41.16 | 39.28 | 39.70 | 40.75 | 39.93 | 41.93 | 40.89 | 40.01 | 39.40 | 40.13 | 40.13 | 40.82 | 40.32 | 43.56 | 39.28 | 39.99 | 39.54 | 39.66 | 40.61 | 40.61 |
| 0C | 40.77 | 41.73 | 41.50 | 50.00 | 44.17 | 41.42 | 40.85 | 43.85 | 40.88 | 43.26 | 41.16 | 39.62 | 40.77 | 41.15 | 40.61 | 41.36 | 41.50 | 40.49 | 45.75 | 44.79 | 40.32 | 40.32 | 41.26 | 41.42 | 40.61 | 41.93 | 40.51 | 45.48 | 41.50 | 40.92 | 42.01 |
| 0D | 39.94 | 39.93 | 40.32 | 42.16 | 40.68 | 41.93 | 43.56 | 42.88 | 40.75 | 40.89 | 39.28 | 40.77 | 38.19 | 40.01 | 39.99 | 42.19 | 41.16 | 39.40 | 39.54 | 39.54 | 39.28 | 40.13 | 39.66 | 40.32 | 39.70 | 40.13 | 40.61 | 41.71 | 40.75 | 40.82 | 40.61 |
| 0E | 43.62 | 41.88 | 40.61 | 42.71 | 39.92 | 45.48 | 40.44 | 40.91 | 40.38 | 41.70 | 39.70 | 41.15 | 40.01 | 38.69 | 42.78 | 44.71 | 45.75 | 40.65 | 39.74 | 39.98 | 39.54 | 41.71 | 40.04 | 40.85 | 39.74 | 43.56 | 41.34 | 40.44 | 41.18 | 40.33 | 43.59 |
| 0F | 40.85 | 43.08 | 41.50 | 40.60 | 43.59 | 40.92 | 40.33 | 42.21 | 42.20 | 42.31 | 40.75 | 40.61 | 39.99 | 42.78 | 38.81 | 43.34 | 40.51 | 41.24 | 41.18 | 50.00 | 40.61 | 40.82 | 40.99 | 41.26 | 41.34 | 39.66 | 47.19 | 40.04 | 47.19 | 40.99 | 43.15 |
| 10 | 43.40 | 40.75 | 41.73 | 40.75 | 41.87 | 40.77 | 43.62 | 43.40 | 42.63 | 42.71 | 39.93 | 41.36 | 42.19 | 44.71 | 43.34 | 39.17 | 50.00 | 44.39 | 41.88 | 39.98 | 42.16 | 39.94 | 40.85 | 43.85 | 42.71 | 42.88 | 43.08 | 40.91 | 40.60 | 42.21 | 39.94 |
| 11 | 43.85 | 41.36 | 41.42 | 40.77 | 40.88 | 41.50 | 40.61 | 41.73 | 43.26 | 40.49 | 41.93 | 41.50 | 41.16 | 45.75 | 40.51 | 50.00 | 39.62 | 44.79 | 45.48 | 44.17 | 40.77 | 40.32 | 41.50 | 41.42 | 41.15 | 40.32 | 40.92 | 40.85 | 40.61 | 41.26 | 42.01 |
| 12 | 42.63 | 39.98 | 43.26 | 42.71 | 41.56 | 44.17 | 39.92 | 41.87 | 41.56 | 39.96 | 40.89 | 40.49 | 39.40 | 40.65 | 41.24 | 44.39 | 44.79 | 38.92 | 41.70 | 39.96 | 39.54 | 40.68 | 43.59 | 40.88 | 39.98 | 40.75 | 42.31 | 40.38 | 50.00 | 42.20 | 42.41 |
| 13 | 42.71 | 40.91 | 41.15 | 44.71 | 39.98 | 40.85 | 40.44 | 43.62 | 39.92 | 40.38 | 40.01 | 45.75 | 39.54 | 39.74 | 41.18 | 41.88 | 45.48 | 41.70 | 38.69 | 40.65 | 41.71 | 43.56 | 40.33 | 40.61 | 40.44 | 39.70 | 42.78 | 39.74 | 40.04 | 41.34 | 43.59 |
| 14 | 42.71 | 41.87 | 40.49 | 44.39 | 39.96 | 40.88 | 40.38 | 42.63 | 41.56 | 41.56 | 39.40 | 44.79 | 39.54 | 39.98 | 50.00 | 39.98 | 44.17 | 39.96 | 40.65 | 38.92 | 40.68 | 40.75 | 42.20 | 43.26 | 39.92 | 40.89 | 41.24 | 41.70 | 43.59 | 42.31 | 42.41 |
| 15 | 42.88 | 42.19 | 40.32 | 39.94 | 40.75 | 41.16 | 39.70 | 39.93 | 40.89 | 39.40 | 40.13 | 40.32 | 39.28 | 39.54 | 40.61 | 42.16 | 40.77 | 39.54 | 41.71 | 40.68 | 38.19 | 39.28 | 40.75 | 41.93 | 40.01 | 40.13 | 40.82 | 43.56 | 39.99 | 39.66 | 40.61 |
| 16 | 39.93 | 42.16 | 41.93 | 42.88 | 40.89 | 40.77 | 40.01 | 42.19 | 39.40 | 39.54 | 40.13 | 40.32 | 40.13 | 41.71 | 40.82 | 39.94 | 40.32 | 40.68 | 43.56 | 40.75 | 39.28 | 38.19 | 39.99 | 41.16 | 39.54 | 39.28 | 39.66 | 39.70 | 40.61 | 40.75 | 40.61 |
| 17 | 43.08 | 40.60 | 40.92 | 42.21 | 42.31 | 40.61 | 42.78 | 43.34 | 41.24 | 50.00 | 40.82 | 41.26 | 39.66 | 40.04 | 40.99 | 40.85 | 41.50 | 43.59 | 40.33 | 42.20 | 40.75 | 39.99 | 38.81 | 40.51 | 41.18 | 40.61 | 40.99 | 41.34 | 47.19 | 47.19 | 43.15 |
| 18 | 41.36 | 40.77 | 41.50 | 41.73 | 40.49 | 41.50 | 45.75 | 50.00 | 44.79 | 44.17 | 40.32 | 41.42 | 40.32 | 40.85 | 41.26 | 43.85 | 41.42 | 40.88 | 40.61 | 43.26 | 41.93 | 41.16 | 40.51 | 39.62 | 45.48 | 40.77 | 41.50 | 41.15 | 40.92 | 40.61 | 42.01 |
| 19 | 40.91 | 44.71 | 40.85 | 43.62 | 40.38 | 45.75 | 39.74 | 41.88 | 41.70 | 40.65 | 43.56 | 40.61 | 39.70 | 39.74 | 41.34 | 42.71 | 41.15 | 39.98 | 40.44 | 39.92 | 40.01 | 39.54 | 41.18 | 45.48 | 38.69 | 41.71 | 40.33 | 40.44 | 42.78 | 40.04 | 43.59 |
| 1A | 42.19 | 39.94 | 41.16 | 39.93 | 39.40 | 40.32 | 39.54 | 42.16 | 39.54 | 40.68 | 39.28 | 41.93 | 40.13 | 43.56 | 39.66 | 42.88 | 40.32 | 40.75 | 39.70 | 40.89 | 40.13 | 39.28 | 40.61 | 40.77 | 41.71 | 38.19 | 40.75 | 40.01 | 40.82 | 39.99 | 40.61 |
| 1B | 40.60 | 42.21 | 40.61 | 43.34 | 50.00 | 41.26 | 40.04 | 40.85 | 43.59 | 42.20 | 39.99 | 40.51 | 40.61 | 41.34 | 47.19 | 43.08 | 40.92 | 42.31 | 42.78 | 41.24 | 40.82 | 39.66 | 40.99 | 41.50 | 40.33 | 40.75 | 38.81 | 41.18 | 40.99 | 47.19 | 43.15 |
| 1C | 44.71 | 43.62 | 45.75 | 41.88 | 40.65 | 40.61 | 39.74 | 42.71 | 39.98 | 39.92 | 39.54 | 45.48 | 41.71 | 40.44 | 40.04 | 40.91 | 40.85 | 40.38 | 39.74 | 41.70 | 43.56 | 39.70 | 41.34 | 41.15 | 40.44 | 40.01 | 41.18 | 38.69 | 40.33 | 42.78 | 43.59 |
| 1D | 42.21 | 43.34 | 41.26 | 40.85 | 42.20 | 40.51 | 41.34 | 43.08 | 42.31 | 41.24 | 39.66 | 41.50 | 40.75 | 41.18 | 47.19 | 40.60 | 40.61 | 50.00 | 40.04 | 43.59 | 39.99 | 40.61 | 47.19 | 40.92 | 42.78 | 40.82 | 40.99 | 40.33 | 38.81 | 40.99 | 43.15 |
| 1E | 43.34 | 40.85 | 40.51 | 43.08 | 41.24 | 41.50 | 41.18 | 40.60 | 50.00 | 43.59 | 40.61 | 40.92 | 40.82 | 40.33 | 40.99 | 42.21 | 41.26 | 42.20 | 41.34 | 42.31 | 39.66 | 40.75 | 47.19 | 40.61 | 40.04 | 39.99 | 47.19 | 42.78 | 40.99 | 38.81 | 43.15 |
| 1F | 39.94 | 39.94 | 42.01 | 39.94 | 42.41 | 42.01 | 43.59 | 39.94 | 42.41 | 42.41 | 40.61 | 42.01 | 40.61 | 43.59 | 43.15 | 39.94 | 42.01 | 42.41 | 43.59 | 42.41 | 40.61 | 40.61 | 43.15 | 42.01 | 43.59 | 40.61 | 43.15 | 43.59 | 43.15 | 43.15 | 38.93 |

**Table 11.** Differential biases for 6+6 rounds.

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 44.17 | 48.40 | 54.96 | 45.75 | 49.39 | 46.73 | 46.88 | 45.75 | 44.98 | 46.87 | 47.16 | 45.77 | 44.94 | 48.63 | 45.85 | 48.40 | 48.85 | 47.63 | 47.71 | 47.71 | 47.88 | 44.93 | 48.08 | 46.36 | 45.91 | 47.19 | 45.60 | 49.72 | 47.21 | 48.34 | 44.94 |
| 02 | 48.40 | 44.17 | 48.85 | 48.40 | 47.63 | 54.96 | 47.71 | 45.75 | 47.71 | 49.39 | 47.88 | 46.73 | 44.93 | 46.88 | 48.08 | 45.75 | 46.36 | 44.98 | 45.91 | 46.87 | 47.19 | 47.16 | 45.60 | 45.77 | 49.72 | 44.94 | 47.21 | 48.63 | 48.34 | 45.85 | 44.94 |
| 03 | 54.96 | 48.85 | 44.62 | 46.36 | 49.79 | 46.42 | 50.48 | 45.77 | 49.17 | 45.88 | 45.77 | 46.50 | 45.32 | 45.61 | 46.50 | 46.73 | 46.42 | 48.26 | 46.15 | 45.49 | 45.32 | 46.93 | 45.92 | 46.50 | 45.85 | 46.16 | 45.61 | 50.75 | 46.26 | 45.51 | 47.01 |
| 04 | 45.75 | 48.40 | 46.36 | 44.17 | 44.98 | 48.85 | 45.91 | 48.40 | 46.87 | 47.63 | 47.19 | 54.96 | 47.16 | 47.71 | 45.60 | 45.75 | 45.77 | 47.71 | 49.72 | 49.39 | 44.94 | 47.88 | 47.21 | 46.73 | 48.63 | 44.93 | 48.34 | 46.88 | 45.85 | 48.08 | 44.94 |
| 05 | 49.39 | 47.63 | 49.79 | 44.98 | 43.92 | 48.26 | 46.70 | 47.71 | 44.96 | 46.56 | 44.54 | 49.17 | 45.68 | 44.92 | 48.59 | 46.87 | 45.88 | 46.56 | 44.98 | 44.96 | 45.75 | 45.89 | 47.31 | 45.49 | 45.38 | 44.40 | 55.05 | 45.65 | 47.20 | 46.24 | 47.41 |
| 06 | 46.73 | 54.96 | 46.42 | 48.85 | 48.26 | 44.62 | 46.15 | 46.36 | 45.49 | 49.79 | 45.32 | 46.42 | 46.93 | 50.48 | 45.92 | 45.77 | 46.50 | 49.17 | 45.85 | 45.88 | 46.16 | 45.77 | 45.61 | 46.50 | 50.75 | 45.32 | 46.26 | 45.61 | 45.51 | 46.50 | 47.01 |
| 07 | 46.88 | 47.71 | 50.48 | 45.91 | 46.70 | 46.15 | 43.69 | 49.72 | 45.65 | 44.98 | 46.71 | 45.85 | 48.56 | 45.44 | 45.33 | 48.63 | 45.61 | 44.92 | 45.44 | 45.38 | 44.70 | 45.01 | 47.78 | 50.75 | 44.74 | 44.54 | 45.04 | 44.74 | 46.34 | 46.18 | 48.59 |
| 08 | 45.75 | 45.75 | 45.77 | 48.40 | 47.71 | 46.36 | 49.72 | 44.17 | 49.39 | 44.98 | 44.94 | 48.85 | 47.88 | 45.91 | 47.21 | 48.40 | 46.73 | 46.87 | 48.63 | 47.63 | 44.93 | 47.19 | 48.34 | 54.96 | 46.88 | 47.16 | 45.85 | 47.71 | 48.08 | 45.60 | 44.94 |
| 09 | 44.98 | 47.71 | 49.17 | 46.87 | 44.96 | 45.49 | 45.65 | 49.39 | 43.92 | 44.96 | 45.68 | 45.88 | 45.75 | 45.38 | 47.20 | 47.63 | 48.26 | 46.56 | 44.92 | 46.56 | 45.89 | 44.40 | 46.24 | 49.79 | 46.70 | 44.54 | 48.59 | 44.98 | 47.31 | 55.05 | 47.41 |
| 0A | 46.87 | 49.39 | 45.88 | 47.63 | 46.56 | 49.79 | 44.98 | 44.98 | 44.96 | 43.92 | 45.75 | 48.26 | 45.89 | 46.70 | 47.31 | 47.71 | 45.49 | 44.96 | 45.38 | 46.56 | 44.40 | 44.54 | 55.05 | 49.17 | 45.65 | 45.68 | 47.20 | 44.92 | 46.24 | 48.59 | 47.41 |
| 0B | 47.16 | 47.88 | 45.77 | 47.19 | 44.54 | 45.32 | 46.71 | 44.94 | 45.68 | 45.75 | 43.19 | 46.16 | 44.28 | 44.70 | 45.75 | 44.93 | 46.93 | 45.89 | 45.01 | 44.40 | 45.13 | 45.13 | 45.82 | 45.32 | 48.56 | 44.28 | 44.99 | 44.54 | 44.66 | 45.61 | 45.61 |
| 0C | 45.77 | 46.73 | 46.50 | 54.96 | 49.17 | 46.42 | 45.85 | 48.85 | 45.88 | 48.26 | 46.16 | 44.62 | 45.77 | 46.15 | 45.61 | 46.36 | 46.50 | 45.49 | 50.75 | 49.79 | 45.32 | 45.32 | 46.26 | 46.42 | 45.61 | 46.93 | 45.51 | 50.48 | 46.50 | 45.92 | 47.01 |
| 0D | 44.94 | 44.93 | 45.32 | 47.16 | 45.68 | 46.93 | 48.56 | 47.88 | 45.75 | 45.89 | 44.28 | 45.77 | 43.19 | 45.01 | 44.99 | 47.19 | 46.16 | 44.40 | 44.54 | 44.54 | 44.28 | 45.13 | 44.66 | 45.32 | 44.70 | 45.13 | 45.61 | 46.71 | 45.75 | 45.82 | 45.61 |
| 0E | 48.63 | 46.88 | 45.61 | 47.71 | 44.92 | 50.48 | 45.44 | 45.91 | 45.38 | 46.70 | 44.70 | 46.15 | 45.01 | 43.69 | 47.78 | 49.72 | 50.75 | 45.65 | 44.74 | 44.98 | 44.54 | 46.71 | 45.04 | 45.85 | 44.74 | 48.56 | 46.34 | 45.44 | 46.18 | 45.33 | 48.59 |
| 0F | 45.85 | 48.08 | 46.50 | 45.60 | 48.59 | 45.92 | 45.33 | 47.21 | 47.20 | 47.31 | 45.75 | 45.61 | 44.99 | 47.78 | 43.81 | 48.34 | 45.51 | 46.24 | 46.18 | 55.05 | 45.61 | 45.82 | 45.99 | 46.26 | 46.34 | 44.66 | 52.20 | 45.04 | 52.20 | 45.99 | 48.15 |
| 10 | 48.40 | 45.75 | 46.73 | 45.75 | 46.87 | 45.77 | 48.63 | 48.40 | 47.63 | 47.71 | 44.93 | 46.36 | 47.19 | 49.72 | 48.34 | 44.17 | 54.96 | 49.39 | 46.88 | 44.98 | 47.16 | 44.94 | 45.85 | 48.85 | 47.71 | 47.88 | 48.08 | 45.91 | 45.60 | 47.21 | 44.94 |
| 11 | 48.85 | 46.36 | 46.42 | 45.77 | 45.88 | 46.50 | 45.61 | 46.73 | 48.26 | 45.49 | 46.93 | 46.50 | 46.16 | 50.75 | 45.51 | 54.96 | 44.62 | 49.79 | 50.48 | 49.17 | 45.77 | 45.32 | 46.50 | 46.42 | 46.15 | 45.32 | 45.92 | 45.85 | 45.61 | 46.26 | 47.01 |
| 12 | 47.63 | 44.98 | 48.26 | 47.71 | 46.56 | 49.17 | 44.92 | 46.87 | 46.56 | 44.96 | 45.89 | 45.49 | 44.40 | 45.65 | 46.24 | 49.39 | 49.79 | 43.92 | 46.70 | 44.96 | 44.54 | 45.68 | 48.59 | 45.88 | 44.98 | 45.75 | 47.31 | 45.38 | 55.05 | 47.20 | 47.41 |
| 13 | 47.71 | 45.91 | 46.15 | 49.72 | 44.98 | 45.85 | 45.44 | 48.63 | 44.92 | 45.38 | 45.01 | 50.75 | 44.54 | 44.74 | 46.18 | 46.88 | 50.48 | 46.70 | 43.69 | 45.65 | 46.71 | 48.56 | 45.33 | 45.61 | 45.44 | 44.70 | 47.78 | 44.74 | 45.04 | 46.34 | 48.59 |
| 14 | 47.71 | 46.87 | 45.49 | 49.39 | 44.96 | 45.88 | 45.38 | 47.63 | 46.56 | 46.56 | 44.40 | 49.79 | 44.54 | 44.98 | 55.05 | 44.98 | 49.17 | 44.96 | 45.65 | 43.92 | 45.68 | 45.75 | 47.20 | 48.26 | 44.92 | 45.89 | 46.24 | 46.70 | 48.59 | 47.31 | 47.41 |
| 15 | 47.88 | 47.19 | 45.32 | 44.94 | 45.75 | 46.16 | 44.70 | 44.93 | 45.89 | 44.40 | 45.13 | 45.32 | 44.28 | 44.54 | 45.61 | 47.16 | 45.77 | 44.54 | 46.71 | 45.68 | 43.19 | 44.28 | 45.75 | 46.93 | 45.01 | 45.13 | 45.82 | 48.56 | 44.99 | 44.66 | 45.61 |
| 16 | 44.93 | 47.16 | 46.93 | 47.88 | 45.89 | 45.77 | 45.01 | 47.19 | 44.40 | 44.54 | 45.13 | 45.32 | 45.13 | 46.71 | 45.82 | 44.94 | 45.32 | 45.68 | 48.56 | 45.75 | 44.28 | 43.19 | 44.99 | 46.16 | 44.54 | 44.28 | 44.66 | 44.70 | 45.61 | 45.75 | 45.61 |
| 17 | 48.08 | 45.60 | 45.92 | 47.21 | 47.31 | 45.61 | 47.78 | 48.34 | 46.24 | 55.05 | 45.82 | 46.26 | 44.66 | 45.04 | 45.99 | 45.85 | 46.50 | 48.59 | 45.33 | 47.20 | 45.75 | 44.99 | 43.81 | 45.51 | 46.18 | 45.61 | 45.99 | 46.34 | 52.20 | 52.20 | 48.15 |
| 18 | 46.36 | 45.77 | 46.50 | 46.73 | 45.49 | 46.50 | 50.75 | 54.96 | 49.79 | 49.17 | 45.32 | 46.42 | 45.32 | 45.85 | 46.26 | 48.85 | 46.42 | 45.88 | 45.61 | 48.26 | 46.93 | 46.16 | 45.51 | 44.62 | 50.48 | 45.77 | 46.50 | 46.15 | 45.92 | 45.61 | 47.01 |
| 19 | 45.91 | 49.72 | 45.85 | 48.63 | 45.38 | 50.75 | 44.74 | 46.88 | 46.70 | 45.65 | 48.56 | 45.61 | 44.70 | 44.74 | 46.34 | 47.71 | 46.15 | 44.98 | 45.44 | 44.92 | 45.01 | 44.54 | 46.18 | 50.48 | 43.69 | 46.71 | 45.33 | 45.44 | 47.78 | 45.04 | 48.59 |
| 1A | 47.19 | 44.94 | 46.16 | 44.93 | 44.40 | 45.32 | 44.54 | 47.16 | 44.54 | 45.68 | 44.28 | 46.93 | 45.13 | 48.56 | 44.66 | 47.88 | 45.32 | 45.75 | 44.70 | 45.89 | 45.13 | 44.28 | 45.61 | 45.77 | 46.71 | 43.19 | 45.75 | 45.01 | 45.82 | 44.99 | 45.61 |
| 1B | 45.60 | 47.21 | 45.61 | 48.34 | 55.05 | 46.26 | 45.04 | 45.85 | 48.59 | 47.20 | 44.99 | 45.51 | 45.61 | 46.34 | 52.20 | 48.08 | 45.92 | 47.31 | 47.78 | 46.24 | 45.82 | 44.66 | 45.99 | 46.50 | 45.33 | 45.75 | 43.81 | 46.18 | 45.99 | 52.20 | 48.15 |
| 1C | 49.72 | 48.63 | 50.75 | 46.88 | 45.65 | 45.61 | 44.74 | 47.71 | 44.98 | 44.92 | 44.54 | 50.48 | 46.71 | 45.44 | 45.04 | 45.91 | 45.85 | 45.38 | 44.74 | 46.70 | 48.56 | 44.70 | 46.34 | 46.15 | 45.44 | 45.01 | 46.18 | 43.69 | 45.33 | 47.78 | 48.59 |
| 1D | 47.21 | 48.34 | 46.26 | 45.85 | 47.20 | 45.51 | 46.34 | 48.08 | 47.31 | 46.24 | 44.66 | 46.50 | 45.75 | 46.18 | 52.20 | 45.60 | 45.61 | 55.05 | 45.04 | 48.59 | 44.99 | 45.61 | 52.20 | 45.92 | 47.78 | 45.82 | 45.99 | 45.33 | 43.81 | 45.99 | 48.15 |
| 1E | 48.34 | 45.85 | 45.51 | 48.08 | 46.24 | 46.50 | 46.18 | 45.60 | 55.05 | 48.59 | 45.61 | 45.92 | 45.82 | 45.33 | 45.99 | 47.21 | 46.26 | 47.20 | 46.34 | 47.31 | 44.66 | 45.75 | 52.20 | 45.61 | 45.04 | 44.99 | 52.20 | 47.78 | 45.99 | 43.81 | 48.15 |
| 1F | 44.94 | 44.94 | 47.01 | 44.94 | 47.41 | 47.01 | 48.59 | 44.94 | 47.41 | 47.41 | 45.61 | 47.01 | 45.61 | 48.59 | 48.15 | 44.94 | 47.01 | 47.41 | 48.59 | 47.41 | 45.61 | 45.61 | 48.15 | 47.01 | 48.59 | 45.61 | 48.15 | 48.59 | 48.15 | 48.15 | 43.93 |

**Table 12.** Differential biases for 7+7 rounds.

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 53.66 | 55.41 | 56.39 | 55.12 | 57.09 | 57.22 | 55.86 | 55.12 | 54.59 | 55.66 | 55.97 | 54.89 | 53.95 | 56.07 | 55.08 | 55.41 | 60.61 | 55.88 | 57.16 | 55.98 | 55.13 | 54.02 | 55.85 | 56.59 | 54.82 | 57.11 | 55.30 | 59.96 | 57.42 | 55.35 | 53.82 |
| 02 | 55.41 | 53.66 | 60.61 | 55.41 | 55.88 | 56.39 | 57.16 | 55.12 | 55.98 | 57.09 | 55.13 | 57.22 | 54.02 | 55.86 | 55.85 | 55.12 | 56.59 | 54.59 | 54.82 | 55.66 | 57.11 | 55.97 | 55.30 | 54.89 | 59.96 | 53.95 | 57.42 | 56.07 | 55.35 | 55.08 | 53.82 |
| 03 | 56.39 | 60.61 | 54.13 | 56.59 | 57.76 | 55.75 | 55.72 | 54.89 | 58.67 | 54.69 | 54.26 | 59.47 | 54.45 | 54.04 | 58.94 | 57.22 | 55.75 | 56.35 | 55.67 | 54.65 | 53.81 | 55.26 | 54.78 | 59.47 | 55.18 | 55.32 | 56.11 | 55.25 | 54.96 | 54.82 | 56.38 |
| 04 | 55.12 | 55.41 | 56.59 | 53.66 | 54.59 | 60.61 | 54.82 | 55.41 | 55.66 | 55.88 | 57.11 | 56.39 | 55.97 | 57.16 | 55.30 | 55.12 | 54.89 | 55.98 | 59.96 | 57.09 | 53.95 | 55.13 | 57.42 | 57.22 | 56.07 | 54.02 | 55.35 | 55.86 | 55.08 | 55.85 | 53.82 |
| 05 | 57.09 | 55.88 | 57.76 | 54.59 | 53.29 | 56.35 | 54.75 | 55.98 | 54.26 | 55.47 | 53.90 | 58.67 | 54.46 | 54.64 | 55.72 | 55.66 | 54.69 | 55.47 | 54.13 | 54.26 | 55.39 | 54.79 | 56.55 | 54.65 | 55.44 | 53.59 | 55.79 | 54.89 | 56.75 | 55.92 | 57.15 |
| 06 | 57.22 | 56.39 | 55.75 | 60.61 | 56.35 | 54.13 | 55.67 | 56.59 | 54.65 | 57.76 | 53.81 | 55.75 | 55.26 | 55.72 | 54.78 | 54.89 | 59.47 | 58.67 | 55.18 | 54.69 | 55.32 | 54.26 | 56.11 | 59.47 | 55.25 | 54.45 | 54.96 | 54.04 | 54.82 | 58.94 | 56.38 |
| 07 | 55.86 | 57.16 | 55.72 | 54.82 | 54.75 | 55.67 | 53.00 | 59.96 | 54.89 | 54.13 | 54.00 | 55.18 | 55.68 | 54.68 | 54.11 | 56.07 | 54.04 | 54.64 | 54.68 | 55.44 | 53.87 | 53.63 | 59.52 | 55.25 | 53.74 | 53.18 | 53.90 | 53.74 | 55.40 | 54.16 | 57.99 |
| 08 | 55.12 | 55.12 | 54.89 | 55.41 | 55.98 | 56.59 | 59.96 | 53.66 | 57.09 | 54.59 | 53.95 | 60.61 | 55.13 | 54.82 | 57.42 | 55.41 | 57.22 | 55.66 | 56.07 | 55.88 | 54.02 | 57.11 | 55.35 | 56.39 | 55.86 | 55.97 | 55.08 | 57.16 | 55.85 | 55.30 | 53.82 |
| 09 | 54.59 | 55.98 | 58.67 | 55.66 | 54.26 | 54.65 | 54.89 | 57.09 | 53.29 | 54.26 | 54.46 | 54.69 | 55.39 | 55.44 | 56.75 | 55.88 | 56.35 | 55.47 | 54.64 | 55.47 | 54.79 | 53.59 | 55.92 | 57.76 | 54.75 | 53.90 | 55.72 | 54.13 | 56.55 | 55.79 | 57.15 |
| 0A | 55.66 | 57.09 | 54.69 | 55.88 | 55.47 | 57.76 | 54.13 | 54.59 | 54.26 | 53.29 | 55.39 | 56.35 | 54.79 | 54.75 | 56.55 | 55.98 | 54.65 | 54.26 | 55.44 | 55.47 | 53.59 | 53.90 | 55.79 | 58.67 | 54.89 | 54.46 | 56.75 | 54.64 | 55.92 | 55.72 | 57.15 |
| 0B | 55.97 | 55.13 | 54.26 | 57.11 | 53.90 | 53.81 | 54.00 | 53.95 | 54.46 | 55.39 | 52.34 | 55.32 | 53.15 | 53.87 | 53.86 | 54.02 | 55.26 | 54.79 | 53.63 | 53.59 | 53.89 | 53.89 | 54.87 | 54.45 | 55.68 | 53.15 | 53.63 | 53.18 | 53.57 | 55.49 | 54.59 |
| 0C | 54.89 | 57.22 | 59.47 | 56.39 | 58.67 | 55.75 | 55.18 | 60.61 | 54.69 | 56.35 | 55.32 | 54.13 | 54.26 | 55.67 | 56.11 | 56.59 | 59.47 | 54.65 | 55.25 | 57.76 | 54.45 | 53.81 | 54.96 | 55.75 | 54.04 | 55.26 | 54.82 | 55.72 | 58.94 | 54.78 | 56.38 |
| 0D | 53.95 | 54.02 | 54.45 | 55.97 | 54.46 | 55.26 | 55.68 | 55.13 | 55.39 | 54.79 | 53.15 | 54.26 | 52.34 | 53.63 | 53.63 | 57.11 | 55.32 | 53.59 | 53.18 | 53.90 | 53.15 | 53.89 | 53.57 | 53.81 | 53.87 | 53.89 | 55.49 | 54.00 | 53.86 | 54.87 | 54.59 |
| 0E | 56.07 | 55.86 | 54.04 | 57.16 | 54.64 | 55.72 | 54.68 | 54.82 | 55.44 | 54.75 | 53.87 | 55.67 | 53.63 | 53.00 | 59.52 | 59.96 | 55.25 | 54.89 | 53.74 | 54.13 | 53.18 | 54.00 | 53.90 | 55.18 | 53.74 | 55.68 | 55.40 | 54.68 | 54.16 | 54.11 | 57.99 |
| 0F | 55.08 | 55.85 | 58.94 | 55.30 | 55.72 | 54.78 | 54.11 | 57.42 | 56.75 | 56.55 | 53.86 | 56.11 | 53.63 | 59.52 | 53.31 | 55.35 | 54.82 | 55.92 | 54.16 | 55.79 | 55.49 | 54.87 | 60.15 | 54.96 | 55.40 | 53.57 | 55.18 | 53.90 | 55.18 | 60.15 | 56.91 |
| 10 | 55.41 | 55.12 | 57.22 | 55.12 | 55.66 | 54.89 | 56.07 | 55.41 | 55.88 | 55.98 | 54.02 | 56.59 | 57.11 | 59.96 | 55.35 | 53.66 | 56.39 | 57.09 | 55.86 | 54.59 | 55.97 | 53.95 | 55.08 | 60.61 | 57.16 | 55.13 | 55.85 | 54.82 | 55.30 | 57.42 | 53.82 |
| 11 | 60.61 | 56.59 | 55.75 | 54.89 | 54.69 | 59.47 | 54.04 | 57.22 | 56.35 | 54.65 | 55.26 | 59.47 | 55.32 | 55.25 | 54.82 | 56.39 | 54.13 | 57.76 | 55.72 | 58.67 | 54.26 | 54.45 | 58.94 | 55.75 | 55.67 | 53.81 | 54.78 | 55.18 | 56.11 | 54.96 | 56.38 |
| 12 | 55.88 | 54.59 | 56.35 | 55.98 | 55.47 | 58.67 | 54.64 | 55.66 | 55.47 | 54.26 | 54.79 | 54.65 | 53.59 | 54.89 | 55.92 | 57.09 | 57.76 | 53.29 | 54.75 | 54.26 | 53.90 | 54.46 | 55.72 | 54.69 | 54.13 | 55.39 | 56.55 | 55.44 | 55.79 | 56.75 | 57.15 |
| 13 | 57.16 | 54.82 | 55.67 | 59.96 | 54.13 | 55.18 | 54.68 | 56.07 | 54.64 | 55.44 | 53.63 | 55.25 | 53.18 | 53.74 | 54.16 | 55.86 | 55.72 | 54.75 | 53.00 | 54.89 | 54.00 | 55.68 | 54.11 | 54.04 | 54.68 | 53.87 | 59.52 | 53.74 | 53.90 | 55.40 | 57.99 |
| 14 | 55.98 | 55.66 | 54.65 | 57.09 | 54.26 | 54.69 | 55.44 | 55.88 | 55.47 | 55.47 | 53.59 | 57.76 | 53.90 | 54.13 | 55.79 | 54.59 | 58.67 | 54.26 | 54.89 | 53.29 | 54.46 | 55.39 | 56.75 | 56.35 | 54.64 | 54.79 | 55.92 | 54.75 | 55.72 | 56.55 | 57.15 |
| 15 | 55.13 | 57.11 | 53.81 | 53.95 | 55.39 | 55.32 | 53.87 | 54.02 | 54.79 | 53.59 | 53.89 | 54.45 | 53.15 | 53.18 | 55.49 | 55.97 | 54.26 | 53.90 | 54.00 | 54.46 | 52.34 | 53.15 | 53.86 | 55.26 | 53.63 | 53.89 | 54.87 | 55.68 | 53.63 | 53.57 | 54.59 |
| 16 | 54.02 | 55.97 | 55.26 | 55.13 | 54.79 | 54.26 | 53.63 | 57.11 | 53.59 | 53.90 | 53.89 | 53.81 | 53.89 | 54.00 | 54.87 | 53.95 | 54.45 | 54.46 | 55.68 | 55.39 | 53.15 | 52.34 | 53.63 | 55.32 | 53.18 | 53.15 | 53.57 | 53.87 | 55.49 | 53.86 | 54.59 |
| 17 | 55.85 | 55.30 | 54.78 | 57.42 | 56.55 | 56.11 | 59.52 | 55.35 | 55.92 | 55.79 | 54.87 | 54.96 | 53.57 | 53.90 | 60.15 | 55.08 | 58.94 | 55.72 | 54.11 | 56.75 | 53.86 | 53.63 | 53.31 | 54.82 | 54.16 | 55.49 | 60.15 | 55.40 | 55.18 | 55.18 | 56.91 |
| 18 | 56.59 | 54.89 | 59.47 | 57.22 | 54.65 | 59.47 | 55.25 | 56.39 | 57.76 | 58.67 | 54.45 | 55.75 | 53.81 | 55.18 | 54.96 | 60.61 | 55.75 | 54.69 | 54.04 | 56.35 | 55.26 | 55.32 | 54.82 | 54.13 | 55.72 | 54.26 | 58.94 | 55.67 | 54.78 | 56.11 | 56.38 |
| 19 | 54.82 | 59.96 | 55.18 | 56.07 | 55.44 | 55.25 | 53.74 | 55.86 | 54.75 | 54.89 | 55.68 | 54.04 | 53.87 | 53.74 | 55.40 | 57.16 | 55.67 | 54.13 | 54.68 | 54.64 | 53.63 | 53.18 | 54.16 | 55.72 | 53.00 | 54.00 | 54.11 | 54.68 | 59.52 | 53.90 | 57.99 |
| 1A | 57.11 | 53.95 | 55.32 | 54.02 | 53.59 | 54.45 | 53.18 | 55.97 | 53.90 | 54.46 | 53.15 | 55.26 | 53.89 | 55.68 | 53.57 | 55.13 | 53.81 | 55.39 | 53.87 | 54.79 | 53.89 | 53.15 | 55.49 | 54.26 | 54.00 | 52.34 | 53.86 | 53.63 | 54.87 | 53.63 | 54.59 |
| 1B | 55.30 | 57.42 | 56.11 | 55.35 | 55.79 | 54.96 | 53.90 | 55.08 | 55.72 | 56.75 | 53.63 | 54.82 | 55.49 | 55.40 | 55.18 | 55.85 | 54.78 | 56.55 | 59.52 | 55.92 | 54.87 | 53.57 | 60.15 | 58.94 | 54.11 | 53.86 | 53.31 | 54.16 | 60.15 | 55.18 | 56.91 |
| 1C | 59.96 | 56.07 | 55.25 | 55.86 | 54.89 | 54.04 | 53.74 | 57.16 | 54.13 | 54.64 | 53.18 | 55.72 | 54.00 | 54.68 | 53.90 | 54.82 | 55.18 | 55.44 | 53.74 | 54.75 | 55.68 | 53.87 | 55.40 | 55.67 | 54.68 | 53.63 | 54.16 | 53.00 | 54.11 | 59.52 | 57.99 |
| 1D | 57.42 | 55.35 | 54.96 | 55.08 | 56.75 | 54.82 | 55.40 | 55.85 | 56.55 | 55.92 | 53.57 | 58.94 | 53.86 | 54.16 | 55.18 | 55.30 | 56.11 | 55.79 | 53.90 | 55.72 | 53.63 | 55.49 | 55.18 | 54.78 | 59.52 | 54.87 | 60.15 | 54.11 | 53.31 | 60.15 | 56.91 |
| 1E | 55.35 | 55.08 | 54.82 | 55.85 | 55.92 | 58.94 | 54.16 | 55.30 | 55.79 | 55.72 | 55.49 | 54.78 | 54.87 | 54.11 | 60.15 | 57.42 | 54.96 | 56.75 | 55.40 | 56.55 | 53.57 | 53.86 | 55.18 | 56.11 | 53.90 | 53.63 | 55.18 | 59.52 | 60.15 | 53.31 | 56.91 |
| 1F | 53.82 | 53.82 | 56.38 | 53.82 | 57.15 | 56.38 | 57.99 | 53.82 | 57.15 | 57.15 | 54.59 | 56.38 | 54.59 | 57.99 | 56.91 | 53.82 | 56.38 | 57.15 | 57.99 | 57.15 | 54.59 | 54.59 | 56.91 | 56.38 | 57.99 | 54.59 | 56.91 | 57.99 | 56.91 | 56.91 | 52.74 |

**Table 13.** Differential biases for 8+8 rounds.

# D Details of Our Experimental Verification

## D.1 2+2 Rounds

| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 9.68 | 12.99 | 11.41 | 13.01 | 13.01 | 20.46 | 19.68 | 13.01 | 11.41 | 12.01 | 13.01 | 19.88 | 11.99 | 12.00 | 12.99 | 12.99 | 20.09 | 12.01 | 12.99 | 13.01 | 12.99 | 11.99 | 20.55 | 19.66 | 12.00 | 19.99 | 12.99 | 13.01 | 12.01 | 12.00 | 20.81 |
| 02 | 12.99 | 9.68 | 20.33 | 12.99 | 12.00 | 11.41 | 12.99 | 13.01 | 13.01 | 13.01 | 12.99 | 19.98 | 11.99 | 20.51 | 19.77 | 13.02 | 20.16 | 11.41 | 12.00 | 12.00 | 20.11 | 13.01 | 12.98 | 19.81 | 13.01 | 11.99 | 12.00 | 12.01 | 11.99 | 12.99 | 20.39 |
| 03 | 11.41 | 20.20 | 9.68 | 19.61 | 12.99 | 12.00 | 12.00 | 19.90 | 12.99 | 11.99 | 20.16 | 11.42 | 20.59 | 12.01 | 20.11 | 19.29 | 12.01 | 20.01 | 13.01 | 11.99 | 20.71 | 19.90 | 11.42 | 11.42 | 20.10 | 19.99 | 19.90 | 12.99 | 11.99 | 12.99 | 11.41 |
| 04 | 13.01 | 12.99 | 20.06 | 9.68 | 11.41 | 19.92 | 12.01 | 12.99 | 12.00 | 12.00 | 20.04 | 11.41 | 13.01 | 12.99 | 12.99 | 13.01 | 20.01 | 13.01 | 13.01 | 13.01 | 11.99 | 12.99 | 12.00 | 21.27 | 12.01 | 11.99 | 11.99 | 20.05 | 12.99 | 20.19 | 20.30 |
| 05 | 13.01 | 12.00 | 12.99 | 11.41 | 9.68 | 20.03 | 11.99 | 13.01 | 20.02 | 12.99 | 12.99 | 12.99 | 12.00 | 13.01 | 11.99 | 12.01 | 11.99 | 12.99 | 20.20 | 20.10 | 11.00 | 12.99 | 13.01 | 11.99 | 12.00 | 19.82 | 20.12 | 13.01 | 12.99 | 12.00 | 13.01 |
| 06 | 20.14 | 11.41 | 12.01 | 20.60 | 20.42 | 9.68 | 13.01 | 20.65 | 11.99 | 12.99 | 19.96 | 12.01 | 19.62 | 12.00 | 11.42 | 19.88 | 11.42 | 12.99 | 20.95 | 12.00 | 19.97 | 20.64 | 20.23 | 11.42 | 12.99 | 20.02 | 11.99 | 12.01 | 12.99 | 19.67 | 11.41 |
| 07 | 19.96 | 12.99 | 12.00 | 12.00 | 11.99 | 13.02 | 9.42 | 13.01 | 13.01 | 20.23 | 12.99 | 19.81 | 12.99 | 12.01 | 12.00 | 12.00 | 12.00 | 13.02 | 12.01 | 12.00 | 11.41 | 20.22 | 19.80 | 12.99 | 12.00 | 11.41 | 13.01 | 11.99 | 13.00 | 11.99 | 11.00 |
| 08 | 13.01 | 13.01 | 20.03 | 12.99 | 13.01 | 20.36 | 13.00 | 9.68 | 13.01 | 11.41 | 11.99 | 21.04 | 12.98 | 12.01 | 12.01 | 12.99 | 19.80 | 12.01 | 12.01 | 12.01 | 11.99 | 19.84 | 11.99 | 11.41 | 20.02 | 13.01 | 12.99 | 12.99 | 20.02 | 12.99 | 21.10 |
| 09 | 11.41 | 13.01 | 12.98 | 12.01 | 20.16 | 12.00 | 13.01 | 13.01 | 9.68 | 20.39 | 12.00 | 11.99 | 11.00 | 11.99 | 12.99 | 12.00 | 20.32 | 12.99 | 13.01 | 12.99 | 12.99 | 19.93 | 12.00 | 12.99 | 11.99 | 12.99 | 12.00 | 19.70 | 13.01 | 20.16 | 13.01 |
| 10 | 12.01 | 13.02 | 11.99 | 12.00 | 12.99 | 12.99 | 19.75 | 11.41 | 19.60 | 9.68 | 11.00 | 20.11 | 12.99 | 11.99 | 13.01 | 13.01 | 12.00 | 19.73 | 12.00 | 12.99 | 20.00 | 12.99 | 20.58 | 12.99 | 13.01 | 12.01 | 12.99 | 13.01 | 12.01 | 11.99 | 13.01 |
| 11 | 13.01 | 12.99 | 19.97 | 19.59 | 12.99 | 20.32 | 12.98 | 11.99 | 12.00 | 11.00 | 9.41 | 20.27 | 11.99 | 11.41 | 13.01 | 11.99 | 20.23 | 12.99 | 20.19 | 19.40 | 12.01 | 12.00 | 13.01 | 20.49 | 12.99 | 11.99 | 12.00 | 11.41 | 11.00 | 11.99 | 11.99 |
| 12 | 20.54 | 19.96 | 11.42 | 11.41 | 12.99 | 12.00 | 22.24 | 19.94 | 11.99 | 19.48 | 20.39 | 9.68 | 20.06 | 13.01 | 20.45 | 20.17 | 11.42 | 12.00 | 12.98 | 12.99 | 19.51 | 20.07 | 12.00 | 12.01 | 12.00 | 20.58 | 12.99 | 11.99 | 20.36 | 11.42 | 11.41 |
| 13 | 11.99 | 11.99 | 20.51 | 13.01 | 12.01 | 21.59 | 12.99 | 12.99 | 11.00 | 12.99 | 12.00 | 19.93 | 9.42 | 20.43 | 12.01 | 20.22 | 20.24 | 20.04 | 11.41 | 12.98 | 12.00 | 12.01 | 11.00 | 19.76 | 11.41 | 12.01 | 12.00 | 12.99 | 13.01 | 13.01 | 11.99 |
| 14 | 12.01 | 19.48 | 12.01 | 12.99 | 13.01 | 11.99 | 12.01 | 12.00 | 11.99 | 11.99 | 11.41 | 13.01 | 19.55 | 9.42 | 19.94 | 13.02 | 12.98 | 13.01 | 12.00 | 19.66 | 11.41 | 12.99 | 13.02 | 19.99 | 12.00 | 12.99 | 13.01 | 12.01 | 11.99 | 11.99 | 11.00 |
| 15 | 12.99 | 19.71 | 20.30 | 12.99 | 12.00 | 11.42 | 11.99 | 12.01 | 12.99 | 13.01 | 13.01 | 20.18 | 12.01 | 20.62 | 9.68 | 11.99 | 12.98 | 12.01 | 11.99 | 20.75 | 11.99 | 13.01 | 12.99 | 11.99 | 13.00 | 11.00 | 20.08 | 13.01 | 19.84 | 12.99 | 11.99 |
| 16 | 12.99 | 13.01 | 20.00 | 13.01 | 12.00 | 19.27 | 12.01 | 12.99 | 12.01 | 13.01 | 11.99 | 20.10 | 19.73 | 13.01 | 11.99 | 9.68 | 11.41 | 13.01 | 19.78 | 11.41 | 13.01 | 12.00 | 12.99 | 20.00 | 12.99 | 12.99 | 20.28 | 12.01 | 12.99 | 12.00 | 19.96 |
| 17 | 20.49 | 20.02 | 12.00 | 19.71 | 12.00 | 11.42 | 12.01 | 20.33 | 21.29 | 11.99 | 19.38 | 11.42 | 19.76 | 12.99 | 12.99 | 11.41 | 9.68 | 12.99 | 11.99 | 12.99 | 19.72 | 20.32 | 20.07 | 12.00 | 13.01 | 20.07 | 11.42 | 20.07 | 19.85 | 12.00 | 11.41 |
| 18 | 12.01 | 11.41 | 19.49 | 13.01 | 12.99 | 12.99 | 13.01 | 12.00 | 12.98 | 19.70 | 12.99 | 12.00 | 19.96 | 13.02 | 12.00 | 13.01 | 12.99 | 9.68 | 12.00 | 19.92 | 12.99 | 12.00 | 11.99 | 11.99 | 19.96 | 11.00 | 13.01 | 12.00 | 19.64 | 12.99 | 13.01 |
| 19 | 12.99 | 12.01 | 13.01 | 13.01 | 20.13 | 19.90 | 12.01 | 12.01 | 13.01 | 11.99 | 20.18 | 12.99 | 11.41 | 11.99 | 12.00 | 20.40 | 11.99 | 11.99 | 9.41 | 13.01 | 12.99 | 12.99 | 12.00 | 12.00 | 12.01 | 11.41 | 19.84 | 11.99 | 13.01 | 13.01 | 11.00 |
| 20 | 13.01 | 12.01 | 12.00 | 13.01 | 20.34 | 11.99 | 11.99 | 12.00 | 12.98 | 12.99 | 19.63 | 12.99 | 12.99 | 20.43 | 19.82 | 11.41 | 12.99 | 19.78 | 13.01 | 9.68 | 12.01 | 11.00 | 12.99 | 19.58 | 13.01 | 12.99 | 12.01 | 11.99 | 11.99 | 13.01 | 13.01 |
| 21 | 12.99 | 19.87 | 19.82 | 11.99 | 11.00 | 20.18 | 11.41 | 11.99 | 12.98 | 20.08 | 12.01 | 19.51 | 12.00 | 11.41 | 11.99 | 13.01 | 20.43 | 12.99 | 12.99 | 12.01 | 9.41 | 11.99 | 13.01 | 20.89 | 20.17 | 12.01 | 13.01 | 12.99 | 12.01 | 11.00 | 11.99 |
| 22 | 11.99 | 13.01 | 20.00 | 12.99 | 12.99 | 19.65 | 20.37 | 19.64 | 20.11 | 12.99 | 12.01 | 19.82 | 12.01 | 12.99 | 13.01 | 11.99 | 20.29 | 12.01 | 12.99 | 11.00 | 12.00 | 9.42 | 12.00 | 20.31 | 11.41 | 11.99 | 11.00 | 11.41 | 11.99 | 13.01 | 11.99 |
| 23 | 20.49 | 12.98 | 11.42 | 12.01 | 13.01 | 20.50 | 20.21 | 12.00 | 12.01 | 19.86 | 13.01 | 11.99 | 11.00 | 13.01 | 12.99 | 12.99 | 19.50 | 12.00 | 11.99 | 12.99 | 13.02 | 12.01 | 9.68 | 12.99 | 12.00 | 11.99 | 12.99 | 13.01 | 20.34 | 19.85 | 11.99 |
| 24 | 19.59 | 20.21 | 11.42 | 20.59 | 11.99 | 11.42 | 12.99 | 11.41 | 12.99 | 12.99 | 21.47 | 12.01 | 20.01 | 19.75 | 11.99 | 19.41 | 12.00 | 11.99 | 12.01 | 19.98 | 19.73 | 20.17 | 12.99 | 9.68 | 11.99 | 20.13 | 19.72 | 13.01 | 11.42 | 19.55 | 11.41 |
| 25 | 12.01 | 13.02 | 19.57 | 12.01 | 11.99 | 12.99 | 12.00 | 19.59 | 11.99 | 13.01 | 12.98 | 12.00 | 11.41 | 12.00 | 13.01 | 12.99 | 13.01 | 20.20 | 12.01 | 13.01 | 20.23 | 11.41 | 12.00 | 11.99 | 9.42 | 12.99 | 12.00 | 12.01 | 20.41 | 13.01 | 11.00 |
| 26 | 20.50 | 12.00 | 19.51 | 11.99 | 20.29 | 19.65 | 11.41 | 13.01 | 12.99 | 12.01 | 11.99 | 20.56 | 12.00 | 12.99 | 11.00 | 12.99 | 20.87 | 11.00 | 11.41 | 12.99 | 12.01 | 11.99 | 12.00 | 19.92 | 12.99 | 9.42 | 13.01 | 20.42 | 13.01 | 12.00 | 11.99 |
| 27 | 12.99 | 12.01 | 20.11 | 11.99 | 19.95 | 12.00 | 13.01 | 12.99 | 12.00 | 12.99 | 12.01 | 12.99 | 12.00 | 13.01 | 19.79 | 19.95 | 11.42 | 13.01 | 21.26 | 12.01 | 13.01 | 11.00 | 12.99 | 19.95 | 11.99 | 13.01 | 9.68 | 12.00 | 12.99 | 19.69 | 11.99 |
| 28 | 13.02 | 12.00 | 12.98 | 19.86 | 13.01 | 12.01 | 11.99 | 12.99 | 20.78 | 13.01 | 11.41 | 11.99 | 12.99 | 12.01 | 13.01 | 12.00 | 20.08 | 12.00 | 11.99 | 11.99 | 12.99 | 11.41 | 13.01 | 13.01 | 12.00 | 19.71 | 11.99 | 9.42 | 11.99 | 20.20 | 11.00 |
| 29 | 12.01 | 11.99 | 11.99 | 12.99 | 12.99 | 12.99 | 13.01 | 20.28 | 13.01 | 12.01 | 11.00 | 20.10 | 13.01 | 11.99 | 19.86 | 12.99 | 20.30 | 21.06 | 13.01 | 11.99 | 12.01 | 12.00 | 19.78 | 11.42 | 19.80 | 13.02 | 12.99 | 11.99 | 9.68 | 12.99 | 11.99 |
| 30 | 12.00 | 12.99 | 12.99 | 20.38 | 12.01 | 21.05 | 11.99 | 12.99 | 19.79 | 12.00 | 12.00 | 11.42 | 13.01 | 12.00 | 12.99 | 12.01 | 11.99 | 12.99 | 13.01 | 13.02 | 11.00 | 13.01 | 19.77 | 20.12 | 13.01 | 12.01 | 20.36 | 19.59 | 12.98 | 9.68 | 11.99 |
| 31 | 19.88 | 20.86 | 11.41 | 20.00 | 13.01 | 11.41 | 11.00 | 20.06 | 13.01 | 13.01 | 11.99 | 11.41 | 11.99 | 11.00 | 12.00 | 20.24 | 11.41 | 13.01 | 11.00 | 13.01 | 11.99 | 11.99 | 12.00 | 11.41 | 11.00 | 11.99 | 11.99 | 11.00 | 11.99 | 11.99 | 8.83 |

**Table 14.** Experimental results of differential bias for 2+2 using $2^{39}$ pairs. Let $\varepsilon$ be an empirical differential bias, and each cell shows $-\log_2(|\varepsilon|)$. The cells colored light-blue have a negative bias, i.e., $\varepsilon < 0$.

To verify the correctness of our theoretical estimation, we experimentally computed each differential bias by using $2^{15} \times 2^{15} \times 2^{9}$ pairs. These experimental results are summarized in Table 14.

## D.2 3+3 Rounds

To verify the correctness of our theoretical estimation, we experimentally computed each differential bias by using $2^{17} \times 2^{17} \times 2^{9}$ pairs. These experimental results are summarized in Table 15.

|  | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 14.68 | 17.72 | 16.26 | 18.43 | 18.36 | 19.78 | 20.24 | 18.53 | 16.28 | 17.15 | 18.23 | 20.12 | 16.78 | 17.17 | 17.65 | 17.66 | 19.86 | 17.19 | 17.65 | 18.40 | 17.59 | 16.86 | 20.05 | 20.00 | 17.17 | 19.91 | 17.70 | 18.42 | 17.29 | 16.86 | 20.27 |
| 02 | 17.72 | 14.67 | 20.20 | 17.66 | 17.23 | 16.30 | 17.68 | 18.45 | 18.68 | 18.42 | 17.77 | 19.97 | 16.86 | 20.06 | 19.70 | 18.48 | 20.24 | 16.31 | 17.17 | 17.25 | 20.10 | 18.30 | 17.73 | 20.52 | 18.41 | 16.87 | 17.20 | 17.21 | 16.79 | 17.66 | 20.44 |
| 03 | 16.35 | 19.79 | 14.67 | 19.86 | 17.70 | 17.18 | 16.82 | 19.56 | 17.71 | 16.82 | 19.99 | 16.52 | 19.93 | 17.20 | 20.08 | 19.58 | 17.20 | 19.68 | 18.54 | 16.80 | 19.70 | 19.83 | 16.46 | 16.50 | 19.86 | 19.82 | 20.88 | 17.70 | 16.87 | 17.66 | 16.27 |
| 04 | 18.43 | 17.67 | 20.24 | 14.68 | 16.30 | 20.04 | 17.22 | 17.72 | 17.14 | 17.16 | 20.02 | 16.28 | 18.49 | 17.70 | 17.66 | 18.46 | 19.97 | 18.32 | 18.45 | 18.42 | 16.84 | 17.56 | 17.21 | 19.61 | 17.22 | 16.80 | 16.82 | 19.79 | 17.69 | 19.92 | 20.20 |
| 05 | 18.44 | 17.25 | 17.58 | 16.27 | 14.68 | 19.99 | 16.82 | 18.36 | 19.80 | 17.64 | 17.73 | 17.69 | 17.31 | 18.58 | 16.83 | 17.23 | 16.85 | 17.69 | 20.45 | 19.83 | 16.10 | 17.58 | 18.69 | 16.79 | 16.78 | 19.93 | 20.76 | 18.52 | 17.78 | 17.23 | 18.44 |
| 06 | 19.97 | 16.27 | 17.16 | 20.35 | 20.70 | 14.70 | 18.71 | 19.60 | 16.90 | 17.71 | 21.16 | 17.20 | 19.92 | 16.81 | 16.54 | 20.10 | 16.51 | 17.67 | 20.08 | 16.82 | 19.99 | 20.16 | 19.54 | 16.51 | 17.58 | 19.37 | 16.82 | 17.21 | 17.67 | 19.99 | 16.30 |
| 07 | 20.12 | 17.74 | 16.80 | 17.30 | 16.84 | 18.37 | 14.41 | 18.43 | 18.54 | 20.15 | 17.67 | 19.70 | 17.74 | 17.22 | 16.84 | 17.15 | 17.20 | 18.39 | 17.20 | 16.83 | 16.29 | 19.61 | 19.57 | 17.65 | 16.83 | 16.36 | 18.27 | 16.81 | 18.31 | 16.82 | 16.05 |
| 08 | 18.33 | 18.34 | 20.48 | 17.75 | 18.36 | 19.95 | 18.38 | 14.69 | 18.56 | 16.30 | 16.81 | 19.99 | 17.58 | 17.23 | 17.17 | 17.68 | 19.82 | 17.27 | 17.23 | 17.27 | 16.84 | 19.97 | 16.78 | 16.31 | 19.99 | 18.36 | 17.71 | 17.72 | 20.04 | 17.64 | 20.21 |
| 09 | 16.30 | 18.41 | 17.63 | 17.31 | 20.80 | 16.82 | 18.35 | 18.45 | 14.67 | 20.05 | 17.07 | 16.84 | 16.08 | 16.79 | 17.69 | 17.17 | 20.08 | 17.63 | 18.40 | 17.69 | 17.65 | 19.87 | 17.31 | 17.63 | 16.87 | 17.61 | 16.85 | 20.40 | 18.58 | 19.54 | 18.29 |
| 0A | 17.23 | 18.30 | 16.80 | 17.21 | 17.70 | 17.67 | 20.10 | 16.29 | 20.04 | 14.71 | 16.10 | 20.12 | 17.67 | 16.79 | 18.40 | 18.54 | 16.80 | 19.55 | 16.80 | 17.70 | 20.22 | 17.63 | 19.74 | 17.60 | 18.54 | 17.11 | 17.68 | 18.71 | 17.20 | 16.85 | 18.61 |
| 0B | 18.69 | 17.67 | 19.63 | 19.70 | 17.66 | 20.21 | 17.68 | 16.81 | 17.17 | 16.07 | 14.40 | 19.84 | 16.86 | 16.31 | 18.39 | 16.80 | 20.02 | 17.63 | 20.13 | 20.16 | 17.22 | 17.16 | 18.32 | 19.72 | 17.56 | 16.81 | 17.24 | 16.27 | 16.08 | 16.83 | 16.81 |
| 0C | 19.97 | 20.32 | 16.54 | 16.32 | 17.64 | 17.20 | 20.22 | 20.10 | 16.79 | 19.98 | 20.02 | 14.68 | 20.09 | 18.59 | 20.13 | 20.13 | 16.48 | 16.87 | 17.66 | 17.66 | 20.48 | 19.89 | 16.82 | 17.21 | 17.21 | 19.69 | 17.68 | 16.84 | 20.15 | 16.54 | 16.26 |
| 0D | 16.89 | 16.87 | 20.09 | 18.63 | 17.17 | 20.03 | 17.78 | 17.63 | 16.13 | 17.59 | 16.77 | 20.01 | 14.40 | 20.01 | 17.14 | 19.49 | 19.99 | 20.11 | 16.28 | 17.66 | 16.89 | 17.25 | 16.11 | 19.89 | 16.28 | 17.21 | 16.86 | 17.59 | 18.38 | 18.41 | 16.79 |
| 0E | 17.23 | 20.30 | 17.19 | 17.63 | 18.49 | 16.84 | 17.24 | 17.24 | 16.81 | 16.83 | 16.32 | 18.42 | 20.01 | 14.41 | 19.90 | 18.43 | 17.76 | 18.40 | 16.87 | 19.62 | 16.28 | 17.73 | 18.33 | 20.53 | 16.82 | 17.56 | 18.33 | 17.21 | 16.80 | 16.85 | 16.10 |
| 0F | 17.73 | 19.96 | 19.66 | 17.67 | 16.83 | 16.49 | 16.80 | 17.19 | 17.60 | 18.38 | 18.60 | 20.58 | 17.23 | 20.12 | 14.67 | 16.85 | 17.73 | 17.13 | 16.82 | 20.21 | 16.81 | 18.47 | 17.73 | 16.79 | 18.40 | 16.10 | 19.74 | 18.33 | 20.33 | 17.57 | 16.83 |
| 10 | 17.65 | 18.44 | 20.13 | 18.49 | 17.14 | 20.36 | 17.22 | 17.64 | 17.15 | 18.40 | 16.85 | 20.27 | 20.31 | 18.66 | 16.82 | 14.70 | 16.29 | 18.38 | 19.93 | 16.27 | 18.33 | 16.82 | 17.73 | 19.61 | 17.60 | 17.71 | 19.95 | 17.23 | 17.68 | 17.17 | 19.92 |
| 11 | 20.03 | 19.58 | 17.23 | 20.00 | 16.86 | 16.57 | 17.23 | 20.07 | 20.16 | 16.78 | 19.88 | 16.50 | 20.38 | 17.69 | 17.68 | 16.26 | 14.67 | 17.82 | 16.85 | 17.78 | 20.05 | 19.66 | 19.73 | 17.22 | 18.40 | 19.70 | 16.55 | 20.49 | 19.76 | 16.79 | 16.32 |
| 12 | 17.19 | 16.28 | 20.17 | 18.42 | 17.68 | 17.72 | 18.52 | 17.24 | 17.69 | 19.38 | 17.65 | 16.75 | 20.21 | 18.21 | 17.23 | 18.38 | 17.60 | 14.69 | 16.82 | 20.17 | 17.78 | 17.13 | 16.83 | 16.89 | 19.57 | 16.10 | 18.63 | 16.91 | 19.89 | 17.74 | 18.25 |
| 13 | 17.61 | 17.16 | 18.57 | 18.40 | 20.15 | 19.90 | 17.19 | 17.22 | 18.35 | 16.75 | 19.55 | 17.64 | 16.31 | 16.79 | 16.86 | 19.81 | 16.84 | 16.87 | 14.42 | 18.58 | 17.69 | 17.60 | 16.79 | 17.18 | 17.20 | 16.28 | 20.08 | 16.84 | 18.30 | 18.40 | 16.13 |
| 14 | 18.40 | 17.20 | 16.80 | 18.46 | 20.36 | 16.81 | 16.77 | 17.16 | 17.62 | 17.66 | 20.06 | 17.61 | 17.75 | 20.03 | 20.30 | 16.30 | 17.62 | 19.87 | 18.41 | 14.68 | 17.15 | 16.08 | 17.54 | 19.84 | 18.58 | 17.76 | 17.17 | 16.80 | 16.85 | 18.28 | 18.51 |
| 15 | 17.65 | 19.45 | 19.71 | 16.72 | 16.05 | 20.24 | 16.31 | 16.82 | 17.66 | 19.69 | 17.27 | 19.72 | 16.84 | 16.31 | 16.85 | 18.36 | 20.14 | 17.62 | 17.65 | 17.23 | 14.41 | 16.78 | 18.46 | 20.49 | 20.15 | 17.21 | 18.48 | 17.79 | 17.25 | 16.09 | 16.77 |
| 16 | 16.85 | 18.38 | 20.18 | 17.67 | 17.60 | 20.20 | 19.53 | 19.72 | 19.84 | 17.63 | 17.24 | 19.70 | 17.24 | 17.70 | 18.29 | 16.88 | 20.22 | 17.27 | 17.58 | 16.10 | 16.79 | 14.41 | 17.23 | 20.00 | 16.31 | 16.76 | 16.09 | 16.30 | 16.82 | 18.63 | 16.77 |
| 17 | 19.99 | 17.74 | 16.48 | 17.19 | 18.31 | 20.20 | 20.22 | 16.88 | 17.19 | 19.81 | 18.30 | 16.82 | 16.09 | 18.42 | 17.70 | 17.63 | 19.88 | 16.79 | 16.85 | 17.68 | 18.48 | 17.24 | 14.68 | 17.63 | 16.82 | 16.86 | 17.60 | 18.55 | 19.62 | 19.87 | 16.86 |
| 18 | 20.01 | 20.00 | 16.57 | 19.95 | 16.78 | 16.57 | 17.62 | 16.33 | 17.62 | 17.68 | 19.87 | 17.16 | 20.09 | 19.86 | 16.85 | 20.23 | 17.27 | 16.80 | 17.23 | 20.02 | 20.14 | 20.10 | 17.69 | 14.69 | 16.85 | 19.78 | 19.79 | 18.72 | 16.56 | 19.92 | 16.28 |
| 19 | 17.22 | 18.52 | 19.90 | 17.14 | 16.84 | 17.69 | 16.85 | 20.02 | 16.81 | 18.26 | 17.72 | 17.20 | 16.29 | 16.83 | 18.37 | 17.65 | 18.30 | 20.07 | 17.25 | 18.52 | 20.39 | 16.26 | 16.86 | 16.76 | 14.42 | 17.59 | 16.87 | 17.23 | 19.89 | 18.33 | 16.13 |
| 1A | 19.78 | 16.78 | 19.74 | 16.85 | 19.80 | 19.95 | 16.29 | 18.43 | 17.66 | 17.16 | 16.85 | 19.87 | 17.23 | 17.72 | 16.10 | 17.81 | 20.09 | 16.11 | 16.30 | 17.68 | 17.20 | 16.79 | 16.81 | 20.10 | 17.66 | 14.40 | 18.42 | 19.61 | 18.34 | 17.19 | 16.84 |
| 1B | 17.73 | 17.23 | 20.21 | 16.78 | 19.73 | 16.86 | 18.59 | 17.56 | 16.84 | 17.57 | 17.27 | 17.63 | 16.84 | 18.45 | 19.93 | 20.41 | 16.50 | 18.45 | 20.21 | 17.24 | 18.31 | 16.11 | 17.62 | 19.87 | 16.83 | 18.30 | 14.68 | 16.77 | 17.69 | 19.92 | 16.79 |
| 1C | 18.56 | 17.20 | 17.67 | 19.97 | 18.53 | 17.23 | 16.78 | 17.70 | 19.72 | 18.38 | 16.28 | 16.78 | 17.62 | 17.22 | 18.52 | 17.25 | 19.80 | 16.80 | 16.84 | 16.81 | 17.55 | 16.31 | 18.48 | 18.39 | 17.12 | 19.99 | 16.79 | 14.42 | 16.80 | 19.53 | 16.11 |
| 1D | 17.20 | 16.81 | 16.83 | 17.73 | 17.74 | 17.62 | 18.31 | 19.95 | 18.34 | 17.19 | 16.11 | 20.38 | 18.46 | 16.79 | 20.72 | 17.63 | 19.82 | 19.95 | 18.39 | 16.86 | 17.17 | 16.81 | 19.89 | 16.57 | 20.22 | 18.39 | 17.71 | 16.82 | 14.69 | 17.70 | 16.89 |
| 1E | 16.79 | 17.70 | 17.69 | 20.32 | 17.24 | 19.51 | 16.81 | 17.69 | 19.91 | 16.82 | 16.80 | 16.52 | 18.55 | 16.80 | 17.64 | 17.23 | 16.81 | 17.75 | 18.42 | 18.55 | 16.08 | 18.33 | 20.00 | 19.77 | 18.43 | 17.20 | 19.88 | 19.91 | 17.67 | 14.68 | 16.77 |
| 1F | 19.40 | 20.09 | 16.31 | 19.58 | 18.18 | 16.29 | 16.13 | 19.44 | 18.60 | 18.22 | 16.83 | 16.34 | 16.84 | 16.05 | 16.83 | 20.16 | 16.34 | 18.46 | 16.14 | 18.34 | 16.79 | 16.81 | 16.84 | 16.30 | 16.12 | 16.88 | 16.84 | 16.08 | 16.86 | 16.80 | 13.85 |

**Table 15.** Experimental results of differential bias for 3+3 using $2^{43}$ pairs. Let $\varepsilon$ be an empirical differential bias, and each cell shows $-\log_2(|\varepsilon|)$. The cells colored light-blue have a negative bias, i.e., $\varepsilon < 0$.