Towards Minimizing Non-linearity in Type-II Generalized Feistel Networks

Yuqing Zhao[1,2], Chun Guo[1,2,3(✉)], and Weijia Wang[1,2,4]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China
[2] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China,
[3] Shandong Research Institute of Industrial Technology, Jinan, Shandong, 250102, China
[4] Quan Cheng Laboratory,250103, Jinan, Shandong, China
yqzhao@mail.sdu.edu.cn,chun.guo@sdu.edu.cn,wjwang@sdu.edu.cn

Abstract. Recent works have revisited blockcipher structures to achieve MPC- and ZKP-friendly designs. In particular, Albrecht et al. (EUROCRYPT 2015) first pioneered using a novel structure *SP networks with partial non-linear layers (P-SPNs)* and then (ESORICS 2019) repopularized using *multi-line generalized Feistel networks (GFNs)*. In this paper, we persist in exploring symmetric cryptographic constructions that are conducive to the applications such as MPC. In order to study the minimization of non-linearity in Type-II Generalized Feistel Networks, we generalize the (extended) GFN by replacing the bit-wise shuffle in a GFN with the stronger linear layer in P-SPN and introducing the key in each round. We call this scheme Generalized Extended Generalized Feistel Network (GEGFN). When the block-functions (or S-boxes) are public random permutations or (domain-preserving) functions, we prove CCA security for the 5-round GEGFN. Our results also hold when the block-functions are over the prime fields $\mathbb{F}_p$, yielding blockcipher constructions over $(\mathbb{F}_p)^*$.

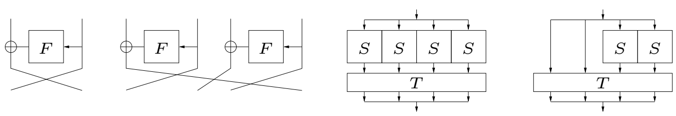
Keywords: blockciphers · Generalized Feistel networks · substitution-permutation networks · provable security · prime fields

1 Introduction

The Feistel network has become one of the main flavors of blockciphers. A classical Feistel network, as shown in Fig. 1 (a), proceeds with iterating a Feistel permutation $\Psi^F(A,B) := (B, A \oplus F(B))$, where F is a domain-preserving block-function. The generalized Feistel network (GFN) is a generalized form of the classical Feistel network. A popular version of GFN, called Type-II, show in Fig. 1 (b), in which a single round uses a block-function F to map an input $(m_1, m_1, ..., m_w)$ to $(c_1, c_2, ..., c_w) = \big(m_2, m_3 \oplus F(m_4), m_4, m_5 \oplus$

$F(m_6), ..., m_w, m_1 \oplus F(m_2)\big)$. As we can see, this operation is equivalent to applying Feistel permutation for every two blocks and then performing a (left) cyclic shift of sub-blocks.

Type-II GFNs have many desirable features for implementation. In particular, they are *inverse-free*, i.e., they allow constructing invertible blockciphers from non-invertible block-functions with small domains. This reduces the implementation cost of deciphering and has attracted attention. A drawback, however, is the slow diffusion (when w is large), and security can only be ensured with many rounds [35,23,33]. To remedy this, a series of works [32,5,7,10] investigated replacing the block-wise cyclic shift with more sophisticated (though linear) permutations. These studies build secure GFN ciphers having fewer rounds than Type-II, while simultaneously ensuring simplicity of structure and without increasing the implementation cost as much as possible. Thus, a common feature of linear permutations is block-wise operations.



(a) (b) (c) (d)

Fig. 1. Different blockcipher structures. (a) Feistel network; (b) multi-line generalized Feistel, with 4 chunks; (c) the classical SPN; (d) partial SPN.

Motivated by new applications such as secure Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Zero-Knowledge proofs (ZKP), the need for symmetric encryption schemes that minimize non-linear operations in their natural algorithmic description is apparent. This can be primarily attributed to the comparatively lower cost of linear operations compared to nonlinear operations.

In recent years, many works have been devoted to the research of construction strategies for symmetric cryptographic structures that are advantageous for applications such as secure MPC. Initiated by Zorro [14] and popularized by LowMC [2], a number of blockcipher designs followed an SPN variant depicted in Fig. 1 (d). This structure was named *SP network with partial non-linear layers* [4] or *partial SPN* (P-SPN). Guo et al. [19] establish strong pseudorandom security for different instances of partial SPNs using MDS linear layers. The recent HADES design [16,18] combines the classical SPN (shown in Fig. 1 (c)) with the P-SPN, where a middle layer that consists of P-SPN rounds is surrounded by outer layers of SPN rounds. Albrecht et al. [1] study approaches to generalized Feistel constructions with low-degree round functions and introduce a new variant of the generalized Feistel networks, which is called "Multi-Rotating Feistel network" that provides extremely fast diffusion.

Our Results. In this work, we continue the exploration of construction strategies for constructions for symmetric cryptography, which benefits applications such as MPC. Particular emphasis is placed on the investigation of the Type-II

GFNs. By the nature of the problem, we are interested in two different metrics. One metric refers to what is commonly called multiplicative complexity (MC), and the other metric refers to the multiplicative depth (AND Depth). Our aim is to minimize both of these metrics as much as possible.

Due to the use of stronger diffusion layers, SPNs and P-SPNs enjoy much better diffusion than Type-II GFNs. This is also indicated by provable CCA security results: the best Type-II GFN variant [5] needs 10 rounds and $5w$ block-function applications, while the SPN, resp. P-SPN, requires only 3 rounds, resp. 5 rounds, and $3w$, resp. $5w/2$, block-function applications. It is thus natural to ask if the non-linear operations can reduce by leveraging the relatively cheaper linear operations, such as strong diffusion layers in SPNs and P-SPNs.

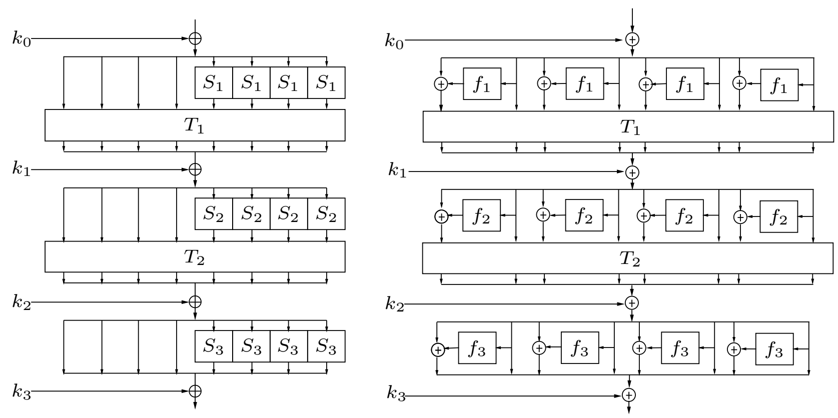


Fig. 2. Partial SPNs (with rate 1/2) and GEGFNs, with $w = 8$.

Regarding the above question, a natural idea is to "inject" the (strong) diffusion layers of SPNs/P-SPNs into Type-II GFNs, as shown in Fig. 2 (right). This model further generalizes the (extended) GFN by replacing the linear layer and permutation layer in [5] with strong diffusion layers in SPNs and P-SPNs, and introducing the key in each round. We call this scheme Generalized Extended Generalized Feistel Networks (GEGFNs).

From an alternative perspective, GEGFN is very similar to the so-called *rate*-1/2 *partial Substitution-Permutation Networks (P-SPNs)*, as shown in Fig. 2 (left). We can also get our construction by replacing the non-linear layer of P-SPN with the non-linear layer of Type-II GFN. GEGFN allows enjoying "the best of the two worlds"– the stronger diffusion provided by the P-SPN construction, along with the inverse-free of the Type-II GFN construction.

To provide a theoretical justification, we investigate the CCA security of GEGFNs. Noting that a number of recent MPC- and ZKP-friendly blockciphers operate on the prime field $\mathbb{F}_p$ [17,3], we consider general block-functions f_i : $\mathbb{F}_N \to \mathbb{F}_N$ with N equals 2^n or some prime p and addition $\bigoplus$ over $\mathbb{F}_N$ instead of the typical XOR action $\oplus$ (as indicated in Fig. 2 right).

Table 1. Comparison to existing wide SPRP structures. The *Rounds* column presents the number of rounds sufficient for birthday-bound security, where $\lambda(w) = \lceil \log_2 1.44w \rceil$. For Type-II GFN (i.e., GFNs with $w/2$ block-functions per round, see Fig. 1 (b)), note that $2\lambda(w) = 2\lceil \log_2 1.44w \rceil \geq 6$ when $w \geq 4$. *Depth* stands for *AND Depth* and *Inv-free* means *Inverse-free*. Parameters in the *MC* and *AND Depth* columns are relative w.r.t. the S-box. The mode XLS [31] is excluded due to attacks [28,29]. Tweakable blockcipher-based modes [6,26,27] are also excluded due to incomparability.

Structure	Rounds	MC	Depth	Inv-free?	Reference
Optimal Type-II GFN	$2\lambda(w)$	$w\lambda(w)$	$2\lambda(w)$	✓	[32,10]
Extended GFN	10	$5w$	10	✓	[5]
Linear SPN	3	$3w$	3	✗	[11]
HADES	4	$3w$	4	✗	[13]
CMC	-	$2w$	$2w$	✗	[21]
EME & EME*	-	$2w+1$	3	✗	[22,20]
Rate 1/2 P-SPN	5	$2.5w$	5	✗	[19]
GEGFN	**5**	$\mathbf{2.5w}$	**5**	✓	Theorems 1 and 2

We first note that the 3-round GEGFN is insecure: the attack idea against 3-round P-SPN [19] can be (easily) adapted to GEGFN and extended to the more general field $\mathbb{F}_N$. Towards positive results, we follow Dodis et al. [12,11] and model the block-functions as public, random primitives available to all parties, while the diffusion layer T as linear permutations. With these, we prove CCA security up to $N^{1/2}$ queries (i.e., the birthday bound over $\mathbb{F}_N$) for 5-round GEGFNs, in two concrete settings:

(i) The block-functions are *random permutations* over $\mathbb{F}_N$;
(ii) The block-functions are *random functions* from $\mathbb{F}_N$ to $\mathbb{F}_N$.

In both cases, the linear layer T shall satisfy a certain property similar to [19] (generalized to the setting of $\mathbb{F}_N$), which is slightly stronger than an MDS transformation. To show the existence of such linear permutations, we exhibit examples in Appendix D.

Discussion. Being compatible with non-bijective block-functions is valuable for MPC-friendly ciphers. For example, as commented by Grassi et al. [15], if constructions incompatible with non-bijective block-functions (e.g., SPNs) are used then designers have to adopt functions of degree at least 3 over $\mathbb{F}_p$. They eventually resorted to a variant of Type-III GFNs. This work provide another choice.

On the other hand, while (GE) GFNs allow using non-bijective block-functions, our treatments include random permutation-based GEGFNs to justify using bijective block-functions. In fact, practical GFN blockciphers such as LBlock [34], Twine insist on using bijections, probably due to the difficulty in designing good non-bijective block-functions. Though, for certain bijections such as the power function $x \mapsto x^3$, $x \in \mathbb{F}_p$, designers are reluctant to use their inefficient inverse in deciphering. These motivated using inverse-free constructions, including blockcipher structures and protocols, and permutation-based GEGFNs may offer solutions.

As shown in Table 1, GEGFNs do enjoy fast diffusion, which is comparable with P-SPNs. In addition, in the CCA setting, its non-linearity cost is comparable with P-SPNs. This means it can be a promising candidate structure for blockciphers with low multiplicative complexities. In this respect, its inverse-freeness increases flexibility by allowing for more choices of S-boxes. On the other hand, the linear layer of GEGFNs is much more costly than the "ordinary" GFNs [32,7,10] (including the "extended" GFN [5]). Therefore, GEGFNs are better used in settings where non-linear operations are much more costly than linear ones (e.g., the MPC setting).

Lastly, as in similar works [35,24,32,5,12,9,19], provable security is limited by the domain of the block-functions and becomes meaningless when the block-functions are small S-boxes. E.g., the block-function in Twine is a 4-bit S-box, and our bounds indicate security up to 2^2 queries. Though, blockcipher structures are typically accomplished by such small-box provable security justification, and we refer to [35,24,32,5] as examples. Meanwhile, recent blockciphers such as the Rescue [3] also used large block-functions $f : \mathbb{F}_N \to \mathbb{F}_N$, $N \approx 2^{252}$, on which the provable result may shed more light.

Organization. Sect. 2 presents notations, definitions and tools. Then, we describe the attack against 3-round GEGFNs in Sect. 3. In Sect. 4 and Sect. 5, we prove SPRP security for 5-round GEGFNs with random permutations and functions, respectively. We finally conclude in Sect. 6.

2 Preliminaries

$(\mathbb{F}_N, +, \cdot) \equiv (\mathrm{GF}(N), +, \cdot)$, where N is either a power of 2 or a prime number and where $+$ and $\cdot$ are resp. the addition and the multiplication in $\mathrm{GF}(N)$. We view N as a cryptographic security parameter. For any positive integer w, we consider a string consisting of w field elements in $\mathbb{F}_N$, which is also viewed as a *column vector* in $\mathbb{F}_N^w$, where w is also called *width*. Indeed, strings and column vectors are just two sides of the same coin. Let x be a *column vector* in $\mathbb{F}_N^w$, then x^{T} is a row vector obtained by transposing x. Throughout the remaining, depending on the context, the same notation, e.g., x, may refer to both a string and a column vector, without additional highlight. In the same vein, the concatenation $x\|y$ is also "semantically equivalent" to the column vector $\binom{x}{y}$.

In this respect, for $x \in \mathbb{F}_N^w$, we denote the j-th entry of x (for $j \in \{1, ..., w\}$) by $x[j]$ and define $x[a..b] := (x[a], ..., x[b])$ for any integers $1 \le a < b \le w$. Let's assume that w is an even number. We define $x[\mathsf{even}] := (x[2], x[4], \ldots, x[w])$ and $x[\mathsf{odd}] := (x[1], x[3], \ldots, x[w-1])$. For $x, y \in \mathbb{F}_N^w$, we denote the difference of x and y by

$$(x[1] - y[1])\|(x[2] - y[2])\|...\|(x[w] - y[w]),$$

where $-$ represents $\oplus$ when N is a power of 2 and represents $\big((x[i] - y[i]) \bmod N\big)$ when N is a prime number.

The zero entry of $\mathbb{F}_N$ is denoted by $\mathsf{0}$ and we write $\mathsf{0}^w$ for the all-zero vector in $\mathbb{F}_N^w$. We write $\mathcal{P}(w)$ for the set of permutations of $\mathbb{F}_N^w$ and $\mathcal{F}(w)$ for the set of functions of $\mathbb{F}_N^w$.

Let T be a matrix. We denote by T_{OE} the submatrix composed of odd rows and even columns of matrix T, by T_{OO} the submatrix composed of odd rows and odd columns of matrix T, by T_{EE} the submatrix composed of even rows and even columns of matrix T, and by T_{EO} the submatrix composed of even rows and odd columns of matrix T.

Given a function $f : \mathbb{F}_N \to \mathbb{F}_N$, for any positive integer m and any vector $x \in \mathbb{F}_N^m$, we define $\overline{f}(x) := \big(f(x[1]), ..., f(x[m])\big)$. For integers $1 \le b \le a$, we write $(a)_b := a(a-1)...(a-b+1)$ and $(a)_0 := 1$ by convention.

MDS Matrix. For any (column) vector $x \in \mathbb{F}_N^w$, the *Hamming weight* of x is defined as the number of non-zero entries of x, i.e.,

$$\mathsf{wt}(x) := \big|\{i | x[i] \neq \mathsf{0}, i = 1, \ldots, w\}\big|.$$

Let T be a $w \times w$ matrix over $\mathbb{F}_N$. The *branch number* of T is the minimum number of non-zero components in the input vector x and output vector $u = T \cdot x$ as we search all non-zero $x \in \mathbb{F}_N^w$, i.e., the *branch number* of $w \times w$ matrix T is $\min_{x \in \mathbb{F}_N^w, x \neq \mathsf{0}} \{\mathsf{wt}(x) + \mathsf{wt}(T \cdot x)\}$. A matrix $T \in \mathbb{F}_N^{w \times w}$ reaching $w + 1$, the upper bound on such branch numbers, is called *Maximum Distance Separable* (MDS). MDS matrices have been widely used in modern blockciphers, including the AES, since the ensured lower bounds on weights typically transform into bounds on the number of active S-boxes.

GEGFNs. When we replace the linear layer of Type-II GFN with the linear layer of P-SPN and introduce the key in each round, we get our construction $\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}$ (shown in Fig. 2 (right)) that is defined by linear permutations $\{T_i \in \mathbb{F}_N^{w \times w}\}_{i=1}^{\lambda-1}$ and a distribution $\mathcal{K}$ over $K_0 \times \ldots \times K_\lambda$ and that take *oracle* access to λ public, random functions $\mathbf{f} = \{f_i : \mathbb{F}_N \to \mathbb{F}_N\}_{i=1}^{\lambda}$, where $\mathbf{k} = (k_0, \ldots, k_\lambda)$ and λ is the number of rounds. Given input $x \in \mathbb{F}_N^w$, the output of the GEGFN is computed as follows:

- Let $u_1 := k_0 + x$.
- for $i = 1, \ldots, \lambda - 1$ do:
  1. $v_i := \mathsf{PGF}^{f_i}(u_i)$, where
  $\mathsf{PGF}^{f_i}(u_i) = \big(u_i[1] + f_i(u_i[2])\big) \| u_i[2] \| \ldots \| \big(u_i[w-1] + f_i(u_i[w])\big) \| u_i[w]$.
  2. $u_{i+1} = k_i + T_i \cdot v_i$.
- $v_\lambda := \mathsf{PGF}^{f_\lambda}(u_\lambda)$.
- $u_{\lambda+1} = k_\lambda + v_\lambda$.
- Outputs $u_{\lambda+1}$.

SPRP Security of GEGFNs. Following [11], we consider GEGFN construction and analyze the security of the construction against unbounded-time attackers making a bounded number of queries to the construction and to $\mathbf{f}$. Formally, we consider the ability of an adversary D to distinguish two worlds: the "real world", in which it is given oracle access to $\mathbf{f}$ and $\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}$ (for unknown keys $\mathbf{k}$

sampled according to $\mathcal{K}$), and an "ideal world" in which it has access to $\mathbf{f}$ and a random permutation $P : \mathbb{F}_N^w \to \mathbb{F}_N^w$. We allow D to make forward and inverse queries to $\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}$ or P, and we always allow D to make forward queries to random functions $\mathbf{f} = \{f_1, ..., f_\lambda\}$. However, whether D makes inverse queries to $\mathbf{f}$ depends on whether $\mathbf{f}$ are random permutations. With these, for a distinguisher D, we define its *strong-PRP advantage* against the construction $\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}$ as

$$\mathsf{Adv}_{\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}}^{\mathsf{sprp}}(D) := \Big| \Pr\big[\mathbf{k} \xleftarrow{\$} \mathcal{K} : D^{\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}, \mathbf{f}} = 1\big] - \Pr\big[P \xleftarrow{\$} \mathcal{P}(w) : D^{P, \mathbf{f}} = 1\big]\Big|,$$

where $\mathbf{f} = (f_1, \ldots, f_\lambda)$ are λ independent, uniform functions on $\mathbb{F}_N$. The *strong-PRP (SPRP) security* of $\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}$ is

$$\mathsf{Adv}_{\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}}^{\mathsf{sprp}}(q_C, q_f) := \max_D \big\{\mathsf{Adv}_{\mathcal{C}\lambda_{\mathbf{k}}^{\mathbf{f}}}^{\mathsf{sprp}}(D)\big\},$$

where the maximum is taken over all distinguishers that make most q_C queries to their left oracle and q_f queries to their right oracles.

A Useful Operator on the Linear Layer. We will frequently write $M \in \mathbb{F}_N^{w \times w}$ in the block form of 4 submatrices in $\mathbb{F}_N^{w/2 \times w/2}$. For this, we follow the convention using U, B, L, R for *upper*, *bottom*, *left*, and *right* resp., i.e.,

$$M = \begin{pmatrix} M_{\text{UL}} & M_{\text{UR}} \\ M_{\text{BL}} & M_{\text{BR}} \end{pmatrix}.$$

We use brackets, i.e., $(M^{-1})_{\text{XX}}$, $\text{XX} \in \{\text{UL}, \text{UR}, \text{BL}, \text{BR}\}$, to distinguish submatrices of M^{-1} (the inverse of M) from M_{XX}^{-1}, the inverse of M_{XX}.

As per our convention, we view $u, v \in \mathbb{F}_N^w$ as column vectors. During the proof, we will need to derive the "second halves" $u_2 := u[w/2 + 1..w]$ and $v_2 := v[w/2 + 1..w]$ from the "first halves" $u_1 := u[1..w/2], v_1 := v[1..w/2]$, and the equality $v = T \cdot u$. To this end, we follow [19] and define an operator on T:

$$\widehat{T} := \begin{pmatrix} -T_{\text{UR}}^{-1} \cdot T_{\text{UL}} & T_{\text{UR}}^{-1} \\ T_{\text{BL}} - T_{\text{BR}} \cdot T_{\text{UR}}^{-1} \cdot T_{\text{UL}} & T_{\text{BR}} \cdot T_{\text{UR}}^{-1} \end{pmatrix}, \tag{1}$$

which satisfies

$$v = T \cdot u \;\Leftrightarrow\; \begin{pmatrix} u_2 \\ v_2 \end{pmatrix} = \widehat{T} \cdot \begin{pmatrix} u_1 \\ v_1 \end{pmatrix}.$$

3 A Chosen-Plaintext Attack on 3 Rounds

Guo et al. [19] showed a chosen-plaintext attack on 3-round P-SPN. We adapt that idea to our context.[5] Concretely, let $\mathcal{C}3_{\mathbf{k}}^{\mathbf{f}}$ be the 3-round GEGFN using any invertible linear transformations T_1, T_2. I.e.,

$$\mathcal{C}3_{\mathbf{k}}^{\mathbf{f}}(x) := k_3 + \mathsf{PGF}^{f_3}\Big(k_2 + T_2 \cdot \Big(\mathsf{PGF}^{f_2}\big(k_1 + T_1 \cdot \big(\mathsf{PGF}^{f_1}(k_0 + x)\big)\big)\Big)\Big).$$

[5] We followed the attack idea in [19]. However, due to the difference between our construction and the P-SPN in the round function, the collision-inducing positions considered in our attack are distinct.

We show a chosen-plaintext attacker D, given access to an oracle $\mathcal{O} : \mathbb{F}_N^w \to \mathbb{F}_N^w$, that distinguishes whether $\mathcal{O}$ is an instance of $\mathcal{C}3_{\mathbf{k}}^{\mathbf{f}}$ using uniform keys or a random permutation. The attacker D proceeds as follows:

1. Fix $\delta \in \mathbb{F}_N \backslash \{\mathsf{0}\}$ in arbitrary, let $\Delta_3 = \delta \| \mathsf{0}^{w/2-1}$, and compute two differences $\Delta_1 := (T_1)_{\text{EO}}^{-1} \cdot \Delta_3$ and $\Delta_2 := (T_1)_{\text{OO}} \cdot \Delta_1$. Note that this means
$$\Big(T_1 \cdot \big(\Delta_1[1] \| \mathsf{0} \| \Delta_1[2] \| \mathsf{0} \| \dots \| \Delta_1[w/2] \| \mathsf{0}\big)\Big)[\mathsf{odd}] = \Delta_2,$$
$$\Big(T_1 \cdot \big(\Delta_1[1] \| \mathsf{0} \| \Delta_1[2] \| \mathsf{0} \| \dots \| \Delta_1[w/2] \| \mathsf{0}\big)\Big)[\mathsf{even}] = \Delta_3.$$
2. For all $\delta^* \in \mathbb{F}_N$ (we note that if f_2 is permutation, we have $\delta^* \in \mathbb{F}_N \backslash \{\mathsf{0}\}$), compute
$$\begin{aligned}\Delta^* :&= T_2 \cdot \big(\Delta_2[1] \oplus \delta^* \| \Delta_3[1] \| \Delta_2[2] \| \Delta_3[2] \| \dots \| \Delta_2[w/2] \| \Delta_3[w/2]\big)\\ &= T_2 \cdot \big(\Delta_2[1] \oplus \delta^* \| \delta \| \Delta_2[2] \| \mathsf{0} \| \dots \| \Delta_2[w/2] \| \mathsf{0}\big),\end{aligned}$$
and add $\Delta^*[\mathsf{even}]$ into a set Set.[6]
3. Choose inputs x, x' such that $(x - x')[\mathsf{odd}] = \Delta_1$ and $(x - x')[\mathsf{even}] = \mathsf{0}^{w/2}$, query $\mathcal{O}(x)$ and $\mathcal{O}(x')$ to obtain y and y' respectively, and compute the output difference $\Delta_4 := y - y'$.
4. If $\Delta_4[\mathsf{even}] \in \mathsf{Set}$ then output 1; otherwise, output 0.

It is not hard to see that if $\mathcal{O}$ is a w width random permutation then D outputs 1 with probability $O(N/N^{w/2})$. On the other hand, we claim that when $\mathcal{O}$ is an instance of the 3-round GEGFN then D always outputs 1.

For this, consider the propagation of the input difference Δ_1^* , where $\Delta_1^*[\mathsf{odd}] = \Delta_1$ and $\Delta_1^*[\mathsf{even}] = \mathsf{0}^{w/2}$. By step 1, the 2nd round input difference must be Δ_2^*, where $\Delta_2^*[\mathsf{odd}] = \Delta_2$ and $\Delta_2^*[\mathsf{even}] = \Delta_3$. Since $\Delta_3 = \delta \| \mathsf{0}^{w/2-1}$, the output difference of the 2nd function $\overline{f}(\Delta_3)$ action must be in the set $\{\delta^* \| \mathsf{0}^{w/2-1}\}_{\delta^* \in \mathbb{F}_N}$ of size at most N. This means the 3rd round input difference, denoted Δ_3^*, must be in a set of size N. Since the 3rd round PGF^{f_3} action does not affect $\Delta_3^*[\mathsf{even}]$, it can be seen $\Delta_4[\mathsf{even}]$, is also in a set of size N. Furthermore, this set *is* the set Set derived in step 2. This completes the analysis.

4 SPRP Security at 5 Rounds with Public permutations

We will prove security for 5-round GEGFNs built upon 5 "S-boxes"/random permutations $\mathcal{S} = \{S_1, S_2, S_3, S_4, S_5\}$ and a *single linear layer* T. Formally,

$$\begin{aligned}\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}(x) := k_5 + \mathsf{PGF}^{S_5}\big(k_4 + T \cdot \big(\mathsf{PGF}^{S_4}\big(k_3 + T \cdot \big(\mathsf{PGF}^{S_3}\big(k_2 + T \cdot \big(\mathsf{PGF}^{S_2}\big(\\ k_1 + T \cdot \big(\mathsf{PGF}^{S_1}(k_0 + x)\big)\big)\big)\big)\big)\big)\big)\big)\big). \qquad (2)\end{aligned}$$

[6] Here we consider the information-theoretic setting, with no limit on the time complexity. In practice, N is usually small, especially in the binary fields, and this enumeration remains feasible.

Using a single linear layer simplifies the construction. Recall from our convention that $T_{\text{OE}}, \ldots, (T^{-1})_{\text{EE}}$ constitute the eight submatrices of T and T^{-1}. In fact, $(T^{-1})_{\text{OE}}, \ldots, (T^{-1})_{\text{EE}}$ can be derived from $T_{\text{OE}}, \ldots, T_{\text{EE}}$, but the expressions are too complicated to use.

We next characterize the properties on T that are sufficient for security.

Definition 1 (Good Linear Layer for 5 Rounds with Permutations). *A matrix $T \in \mathbb{F}_N^{w\times w}$ is good if T is MDS, and the 6 induced matrices T_{EO}, $-T_{\text{EO}}^{-1} \cdot T_{\text{EE}} \cdot T_{\text{EO}} - T_{\text{OO}}$, $\big(T_{\text{OE}} - T_{\text{OO}} \cdot T_{\text{EO}}^{-1} \cdot T_{\text{EE}}\big) \cdot T_{\text{EO}}$, $(T^{-1})_{\text{EO}}$, $(T^{-1})_{\text{OO}} - T_{\text{OO}} \cdot T_{\text{EO}}^{-1} \cdot (T^{-1})_{\text{EO}}$, and $T_{\text{EO}}^{-1} \cdot (T^{-1})_{\text{EO}}$ are such that:*

1. *They contain no zero entries, and*
2. *Any column vector of the 6 induced matrices consists of $w/2$ distinct entries.*

We remark that, as T is MDS, all the four matrices $T_{\text{OE}}, T_{\text{OO}}, T_{\text{EO}}$ and T_{EE} are all MDS (and invertible). A natural question is whether such a strong T exists at all. For this, we give several MDS matrices in Appendix D that follow our definition.

With such a good T, we have the following theorem on 5-round GEGFNs with public random permutations.

Theorem 1. *Assume $w \geq 2$, and $q_S + wq_C/2 \leq N/2$. Let $\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}$ be a 5-round, linear GEGFN structure defined in Eq. (2), with distribution $\mathcal{K}$ over keys $\mathbf{k} = (k_0, \ldots, k_5)$. If k_0 and k_5 are uniformly distributed and the matrix T fulfills Definition 1, then*

$$\mathsf{Adv}^{\mathsf{sprp}}_{\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}}(q_C, q_S) \leq \frac{12wq_Cq_S + 7w^2q_C^2}{2N} + \frac{2q_C^2}{N^{w/2}}. \tag{3}$$

All the remaining of this section devotes to proving Theorem 1. We employ Patarin's H-coefficient method [30], which we recall in Appendix A. Following the paradigm of H-coefficient, we first establish notations in the Sect. 4.1. We then complete the two steps of *defining and analyzing bad transcripts* and *bounding the ratio $\mu(\tau)/\nu(\tau)$ for good transcripts* in Sect. 4.2 and 4.3 resp.

4.1 Proof Setup

Fix a deterministic distinguisher D. Wlog assume D makes exactly q_C (non-redundant) forward/inverse queries to its left oracle that is either $\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}$ or P, and exactly q_S (non-redundant) forward/inverse queries to each of the oracle S_i on its right side. We call a query from D to its left oracle a *construction query* and a query from D to one of its right oracles an *S-box query*.

The interaction between D and its oracles is recorded in the form of 6 lists of pairs $Q_{\mathcal{C}} \subseteq \mathbb{F}_N^w \times \mathbb{F}_N^w$ and $Q_{S_1}, \ldots, Q_{S_5} \subseteq \mathbb{F}_N \times \mathbb{F}_N$. Among them, $Q_{\mathcal{C}} = ((x^{(1)}, y^{(1)}), \ldots, (x^{(q_C)}, y^{(q_C)}))$ lists the construction queries-responses of D *in chronological order*, where the i-th pair $(x^{(i)}, y^{(i)})$ indicates the i-th such query is either a forward query $x^{(i)}$ that was answered by $y^{(i)}$ or an inverse query $y^{(i)}$ that was answered by $x^{(i)}$. $Q_{S_1}, \ldots, Q_{S_5}$ are defined similarly with respect to queries to $S_1, \ldots, S_5$. Define $Q_{\mathcal{S}} := (Q_{S_1}, \ldots, Q_{S_5})$. Note that D's interaction with its oracles can be unambiguously reconstructed from these sets since D is deterministic. For convenience, for $i \in \{1,2,3,4,5\}$ we define

$$\mathrm{Dom}_i := \big\{a : (a,b) \in Q_{S_i} \text{ for some } b \in \mathbb{F}_N\big\}, \quad \mathrm{Rng}_i := \big\{b : (a,b) \in Q_{S_i} \text{ for } a \in \mathbb{F}_N\big\}.$$

Following [8], we augment the transcript $(Q_{\mathcal{C}}, Q_{\mathcal{S}})$ with a key value $\mathbf{k} = (k_0, \ldots, k_5)$. In the real world, $\mathbf{k}$ is the actual key used by the construction. In the ideal world, $\mathbf{k}$ is a dummy key sampled independently from all other values according to the prescribed key distribution $\mathcal{K}$. Thus, a transcript τ has the final form $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})$.

4.2 Bad Transcripts

Let $\mathcal{T}$ be the set of all possible transcripts that can be generated by D in the ideal world (note that this includes all transcripts that can be generated with non-zero probability in the real world). Let μ, ν be the distributions over transcripts in the real and ideal worlds, respectively (as in Appendix A).

We define a set $\mathcal{T}_2 \subseteq \mathcal{T}$ of *bad transcripts* as follows: a transcript $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})$ is bad if and only if one of the following events occurs:

1. There exist a pair $(x,y) \in Q_{\mathcal{C}}$ and an index $i \in \{2,4,\ldots,w\}$ such that $(x+k_0)[i] \in \mathrm{Dom}_1$ or $(y-k_5)[i] \in \mathrm{Dom}_5$.
2. There exist a pair $(x,y) \in Q_{\mathcal{C}}$ and distinct $i, i' \in \{2,4\ldots,w\}$ such that $(x+k_0)[i] = (x+k_0)[i']$ or $(y-k_5)[i] = (y-k_5)[i']$.
3. There exist distinct $(x,y),(x',y') \in Q_{\mathcal{C}}$ and distinct $i, i' \in \{2,4,\ldots,w\}$ such that $(x+k_0)[i] = (x'+k_0)[i']$ or $(y-k_5)[i] = (y'-k_5)[i']$.
4. There exist two indices $i, \ell \in \{1,\ldots,q_C\}$ such that $\ell > i$, and:
   - $(x^{(\ell)}, y^{(\ell)})$ was due to a forward query, and $y^{(\ell)}[\mathsf{even}] = y^{(i)}[\mathsf{even}]$; or,
   - $(x^{(\ell)}, y^{(\ell)})$ was due to a inverse query, and $x^{(\ell)}[\mathsf{even}] = x^{(i)}[\mathsf{even}]$.

Let $\mathcal{T}_1 := \mathcal{T} \backslash \mathcal{T}_2$ be the set of *good* transcripts.

To understand the conditions, consider a good transcript $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})$ and let's see some properties (informally). First, since the 1st condition is not fulfilled, each construction query induces $w/2$ inputs to the 1st round S-box and $w/2$ inputs to the 5th round S-box, the outputs of which are *not* fixed by $Q_{\mathcal{S}}$. Second, since neither the 2nd nor the 3rd condition is fulfilled, the inputs to the 1st round (5th round, resp.) S-boxes induced by the construction queries are distinct unless unavoidable. These ensure that the induced 2nd and 4th intermediate values are somewhat random and free from multiple forms of collisions. Finally, the last condition will be crucial for some structural properties of the queries that will be crucial in the subsequent analysis (see Appendix B.2, the proof of Lemma 2).

Let's then analyze the probabilities of the conditions in turn. Since, in the ideal world, the values k_0, k_5 are independent of $Q_{\mathcal{C}}, Q_{\mathcal{S}}$ and (individually) uniform in $\mathbb{F}_N^w$, it is easy to see that the probabilities of the first three events do not exceed wq_Cq_S/N, $\binom{w/2}{2} \cdot \frac{2q_C}{N} \leq w^2q_C/4N$, and $\binom{w/2}{2} \cdot \binom{q_C}{2} \cdot \frac{2}{N} \leq w^2q_C(q_C-1)/8N \leq w^2q_C(q_C-1)/4N$, respectively.

For the 4-th condition, consider the ℓ-th construction query $(x^{(\ell)}, y^{(\ell)})$. When it is forward, in the ideal world, it means D issued $P(x^{(\ell)})$ to the w width random permutation P and received $y^{(\ell)}$, which is uniform in $N^w - \ell + 1$ possibilities. Thus, when $\ell \le q_C \le N^w/2$,

$$\Pr\Big[\exists i \le \ell - 1 : y^{(\ell)}[\mathsf{even}] = y^{(i)}[\mathsf{even}]\Big]$$
$$= \sum_{i \le \ell-1, z \in \mathbb{F}_N^{w/2}} \Pr\Big[y^{(\ell)} = \big(z \| y^{(i)}[\mathsf{even}]\big)\Big] \le \frac{(\ell-1)\cdot N^{w/2}}{N^w - \ell + 1} \le \frac{2(\ell-1)}{N^{w/2}}.$$

A similar result follows when $(x^{(\ell)}, y^{(\ell)})$ is inverse. A union bound thus yields

$$\Pr\big[\nu \in \mathcal{T}_2\big] \le \frac{wq_Cq_S}{N} + \frac{w^2q_C^2}{4N} + \sum_{\ell=1}^{q_C} \frac{2(\ell-1)}{N^{w/2}} \le \frac{wq_Cq_S}{N} + \frac{w^2q_C^2}{4N} + \frac{q_C^2}{N^{w/2}}. \quad (4)$$

4.3 Bounding the Ratio $\mu(\tau)/\nu(\tau)$

Let $\Omega_X = \big(\mathcal{P}(1)\big)^5 \times \mathcal{K}$ be the probability space underlying the real world, whose measure is the product of the uniform measure on $(\mathcal{P}(1))^5$ and the measure induced by the distribution $\mathcal{K}$ on keys. (Thus, each element of Ω_X is a tuple $(\mathcal{S}, \mathbf{k})$ with $\mathcal{S} = (S_1, \ldots, S_5)$, $S_1, \ldots, S_5 \in \mathcal{P}(1)$ and $\mathbf{k} = (k_0, \ldots, k_5) \in \mathcal{K}$.) Also, let $\Omega_Y = \mathcal{P}(w) \times \big(\mathcal{P}(1)\big)^5 \times \mathcal{K}$ be the probability space underlying the ideal world, whose measure is the product of the uniform measure on $\mathcal{P}(w)$ with the measure on Ω_X.

Let $\tau' = (Q_{\mathcal{C}}^{\tau'}, Q_{\mathcal{S}}^{\tau'}, \mathbf{k}^{\tau'})$ be a transcript. We introduce four types of *compatibility* as follows.

- First, an element $\omega = (\mathcal{S}^*, \mathbf{k}^*) \in \Omega_X$ is *compatible with* τ' if: (a) $\mathbf{k}^* = \mathbf{k}^{\tau'}$, and (b) $S_i^*(a) = b$ for all $(a, b) \in Q_{S_i}^{\tau'}$, and (c) $\mathcal{C}5_{\mathbf{k}^*}^{\mathcal{S}^*}(x) = y$ for all $(x, y) \in Q_{\mathcal{C}}^{\tau'}$.
- Second, an element $\omega = (P^*, \mathcal{S}^*, \mathbf{k}^*) \in \Omega_Y$ is *compatible with* τ' if: (a) $\mathbf{k}^* = \mathbf{k}^{\tau'}$, and (b) $S_i^*(a) = b$ for all $(a, b) \in Q_{S_i}^{\tau'}$, and (c) $P^*(x) = y$ for all $(x, y) \in Q_{\mathcal{C}}^{\tau'}$. We write
$$\omega \downarrow \tau'$$
to indicate that an element $\omega \in \Omega_X \cup \Omega_Y$ is compatible with τ'.
- Third, a tuple of S-boxes $\mathcal{S}^* \in (\mathcal{P}(1))^5$ is *compatible* with $\tau' = (Q_{\mathcal{C}}^{\tau'}, Q_{\mathcal{S}}^{\tau'}, \mathbf{k}^{\tau'})$, and write $\mathcal{S}^* \downarrow \tau'$, if $(\mathcal{S}^*, \mathbf{k}) \in \Omega_X$ is compatible with τ', where $\mathbf{k}$ is the key value of the fixed transcript τ.
- Last, we say that $(P^*, \mathcal{S}^*) \in \mathcal{P}(w) \times (\mathcal{P}(1))^5$ is *compatible* with $\tau' = (Q_{\mathcal{C}}^{\tau'}, Q_{\mathcal{S}}^{\tau'}, \mathbf{k}^{\tau'})$ and write $(P^*, \mathcal{S}^*) \downarrow \tau'$, if $(P^*, \mathcal{S}^*, \mathbf{k}^{\tau'}) \downarrow \tau'$.

For the rest of the proof, we fix a transcript $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \in \mathcal{T}_1$. Since $\tau \in \mathcal{T}$, it is easy to see (cf. [8]) that

$$\mu(\tau) = \Pr[\omega \leftarrow \Omega_X : \omega \downarrow \tau], \qquad \nu(\tau) = \Pr[\omega \leftarrow \Omega_Y : \omega \downarrow \tau],$$

where the notation indicates that ω is sampled from the relevant probability space according to that space's probability measure. We bound $\mu(\tau)/\nu(\tau)$ by reasoning about the latter probabilities. In detail, with the third and fourth types of compatibility notions, the product structure of Ω_X, Ω_Y implies

$$\Pr[\omega \leftarrow \Omega_X : \omega \downarrow \tau] = \Pr[\mathbf{k}^* = \mathbf{k}] \cdot \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau],$$
$$\Pr[\omega \leftarrow \Omega_Y : \omega \downarrow \tau] = \Pr[\mathbf{k}^* = \mathbf{k}] \cdot \Pr_{P^*,\mathcal{S}^*}[(P^*, \mathcal{S}^*) \downarrow \tau],$$

where $\mathcal{S}^*$ and $(P^*, \mathcal{S}^*)$ are sampled uniformly from $(\mathcal{P}(1))^5$ and $\mathcal{P}(w) \times (\mathcal{P}(1))^5$, respectively. Thus,

$$\frac{\mu(\tau)}{\nu(\tau)} = \frac{\Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau]}{\Pr_{P^*,\mathcal{S}^*}[(P^*, \mathcal{S}^*) \downarrow \tau]}.$$

By these, and by $|Q_{\mathcal{C}}| = q_C, |Q_{S_1}| = \ldots = |Q_{S_5}| = q_S$, it is immediate that

$$\Pr_{P^*,\mathcal{S}^*}\big[(P^*, \mathcal{S}^*) \downarrow \tau\big] = \frac{1}{(N^w)_{q_C} \cdot \big((N)_{q_S}\big)^5}.$$

To compute $\Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau]$, we start by writing

$$\begin{aligned}
\Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau] &= \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})] \\
&= \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})] \cdot \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})] \\
&= \frac{1}{((N)_{q_S})^5} \cdot \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})].
\end{aligned}$$

To analyze $\Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})]$, we proceed in two steps. First, based on $Q_{\mathcal{C}}$ and two outer S-boxes S_1^*, S_5^*, we derive the 2nd and 4th rounds intermediate values: these constitute a special transcript Q_{mid} on the middle 3 rounds. We characterize conditions on S_1^*, S_5^* that will ensure certain good properties in the derived Q_{mid}, which will ease the analysis. Therefore, in the second step, we analyze such "good" Q_{mid} to yield the final bounds. Each of the two steps will take a paragraph as follows.

The outer 2 rounds. Given a tuple of S-boxes $\mathcal{S}^*$, we let $\mathsf{Bad}(\mathcal{S}^*)$ be a predicate of $\mathcal{S}^*$ that holds if any of the following conditions is met:

- (B-1) There exist $(x, y) \in Q_{\mathcal{C}}$ and $i \in \{2, 4, \ldots, w\}$ such that $\big(T \cdot (\mathsf{PGF}^{S_1^*}(x + k_0)) + k_1\big)[i] \in \mathrm{Dom}_2$ or $\big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[i] \in \mathrm{Dom}_4$.
- (B-2) There exist $(x, y) \in Q_{\mathcal{C}}$ and distinct indices $i, i' \in \{2, 4, \ldots, w\}$ such that $\big(T \cdot (\mathsf{PGF}^{S_1^*}(x + k_0)) + k_1\big)[i] = \big(T \cdot (\mathsf{PGF}^{S_1^*}(x + k_0)) + k_1\big)[i']$, or $\big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[i] = \big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[i']$.
- (B-3) There exist distinct pairs $(x, y), (x', y') \in Q_{\mathcal{C}}$ and two indices $i, i' \in \{2, 4, \ldots, w\}$ such that:
  1. $x[\mathsf{even}] \neq x'[\mathsf{even}]$, yet $\big(T \cdot (\mathsf{PGF}^{S_1^*}(x + k_0)) + k_1\big)[i] = \big(T \cdot (\mathsf{PGF}^{S_1^*}(x' + k_0)) + k_1\big)[i']$; or

2. $x[\mathsf{even}] = x'[\mathsf{even}]$, $i \neq i'$, yet $\big(T \cdot (\mathsf{PGF}^{S_1^*}(x + k_0)) + k_1\big)[i] = \big(T \cdot (\mathsf{PGF}^{S_1^*}(x' + k_0)) + k_1\big)[i']$; or
3. $y[\mathsf{even}] \neq y'[\mathsf{even}]$, yet it holds $\big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[i] = \big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[i']$; or
4. $y[\mathsf{even}] = y'[\mathsf{even}]$, $i \neq i'$, yet $\big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[i] = \big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[i']$.

(B-1) captures the case that a 2nd round S-box input or a 4th round S-box input has been in $Q_{\mathcal{S}}$, (B-2) captures collisions among the 2nd round S-box inputs & 4th round S-box inputs for a single construction query, while (B-3) captures various collisions between the 2nd round S-box inputs, resp. 4th round S-box inputs from two distinct queries. Note that essentially, $\mathsf{Bad}(\mathcal{S}^*)$ only concerns the randomness of the outer 2 S-boxes S_1^* and S_5^*. For simplicity, define $\mathsf{Good}(\mathcal{S}^*) := (\mathcal{S}^* \downarrow Q_{\mathcal{S}}) \wedge \neg\mathsf{Bad}(\mathcal{S}^*)$. Then it holds

$$\begin{aligned}
&\Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \\
\geq\ &\Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \\
=\ &\Pr_{\mathcal{S}^*}\big[\mathsf{Good}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \cdot \Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big]. \quad (5)
\end{aligned}$$

Hence, all that remains is to lower bound the two terms in the product of (5). We serve the result below and defer the proof to the Appendix B.1.

Lemma 1. *When $q_S + w \leq N/2$, we have*

$$\Pr_{\mathcal{S}^*}\big[\mathsf{Bad}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \leq \frac{4wq_Cq_S + w^2q_C + w^2q_C^2}{2N}. \quad (6)$$

Analyzing the 3 middle rounds. Our next step is to lower bound the term $\Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big]$ from Eq. (5). Given $\mathcal{S}^*$ for which $\mathsf{Good}(\mathcal{S}^*)$ holds, for every $(x^{(i)}, y^{(i)}) \in Q_{\mathcal{C}}$, we define $u_1^{(i)} := x^{(i)} + k_0$, $v_1^{(i)} := \mathsf{PGF}^{S_1^*}(u_1^{(i)})$ (this means $v_1^{(i)}[\mathsf{even}] = u_1^{(i)}[\mathsf{even}]$), $u_2^{(i)} := T \cdot v_1^{(i)} + k_1$; $v_5^{(i)} := y^{(i)} - k_5$, $u_5^{(i)} := \big(\mathsf{PGF}^{S_5^*}\big)^{-1}(v_5^{(i)})$ (where $v_5^{(i)}[\mathsf{even}] = u_5^{(i)}[\mathsf{even}]$), $v_4^{(i)} := T^{-1} \cdot (u_5^{(i)} - k_4)$. With these, we obtain

$$Q_{mid} = \Big(\big(u_1^{(1)}, u_2^{(1)}, v_4^{(1)}, v_5^{(1)}\big), \ldots, \big(u_1^{(q_C)}, u_2^{(q_C)}, v_4^{(q_C)}, v_5^{(q_C)}\big)\Big),$$

in which the tuples follow exactly the same chronological order as in $Q_{\mathcal{C}}$. Define

$$\mathcal{C}3^{\mathcal{S}^*}_{(k_2,k_3)}(u) = \mathsf{PGF}^{S_4^*}\big(T \cdot \big(\mathsf{PGF}^{S_3^*}\big(T \cdot \big(\mathsf{PGF}^{S_2^*}(u)\big) + k_2\big)\big) + k_3\big),$$

and write $\mathcal{S}^* \downarrow (Q_{mid}, Q_{\mathcal{S}}, \mathbf{k})$ for the event that "$\mathcal{C}3^{\mathcal{S}^*}_{(k_2,k_3)}(u_2) = v_4$ for every (u_1, u_2, v_4, v_5) in the set Q_{mid}". Then it can be seen

$$\Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big] = \Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{mid}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big]. \quad (7)$$

To bound Eq. (7), we will divide Q_{mid} into multiple sets according to collisions on the "even halves" $u_1[\mathsf{even}]$ and $v_5[\mathsf{even}]$, and consider the probability that $\mathcal{S}^*$ is compatible with each set in turn. In detail, the sets are arranged according to the following rules:

- $Q_{m_1} := \big\{(u_1, u_2, v_4, v_5) \in Q_{mid} : u_1[\mathsf{even}] = u_1^{(1)}[\mathsf{even}]\big\}$;
- For $\ell = 2, 3, \ldots$, if $\cup_{i=1}^{\ell-1} Q_{m_i} = Q_{m_1} \cup Q_{m_2} \cup \ldots \cup Q_{m_{\ell-1}} \subset Q_{mid}$, then we define Q_{m_ℓ}. Let j be the minimum index such that $(u_1^{(j)}, u_2^{(j)}, v_4^{(j)}, v_5^{(j)})$ remains in $Q_{mid} \backslash \cup_{i=1}^{\ell-1} Q_{m_i}$. Then:
  - If $v_5^{(j)}$ has collisions, i.e., there exists $(u_1^*, u_2^*, v_4^*, v_5^*) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ such that $v_5^*[\mathsf{even}] = v_5^{(j)}[\mathsf{even}]$, then we define $Q_{m_\ell} := \big\{(u_1, u_2, v_4, v_5) \in Q_{mid} \backslash \cup_{i=1}^{\ell-1} Q_{m_i} : v_5[\mathsf{even}] = v_5^{(j)}[\mathsf{even}]\big\}$. We call such sets **Type-II**.
  - Else, $Q_{m_\ell} := \big\{(u_1, u_2, v_4, v_5) \in Q_{mid} \backslash \cup_{i=1}^{\ell-1} Q_{m_i} : u_1[\mathsf{even}] = u_1^{(j)}[\mathsf{even}]\big\}$. We call such sets as well as Q_{m_1} **Type-I**.

Assume that Q_{mid} is divided into α disjoint sets by the above rules, with $|Q_{m_\ell}| = \beta_\ell$. Then $\sum_{\ell=1}^{\alpha} \beta_\ell = q_C$, and

$$\begin{aligned} &\Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{mid}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big] \\ = &\prod_{\ell=1}^{\alpha} \Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big]. \end{aligned} \tag{8}$$

Now we could focus on analyzing the ℓ-th set Q_{m_ℓ}. Assume that

$$Q_{m_\ell} = \Big(\big(u_1^{(\ell,1)}, u_2^{(\ell,1)}, v_4^{(\ell,1)}, v_5^{(\ell,1)}\big), \ldots, \big(u_1^{(\ell,\beta_\ell)}, u_2^{(\ell,\beta_\ell)}, v_4^{(\ell,\beta_\ell)}, v_5^{(\ell,\beta_\ell)}\big)\Big).$$

The superscript (ℓ, i) indicates that it is the i-th tuple in this ℓ-th set Q_{m_ℓ}. For this index ℓ, we define six sets $\mathrm{ExtDom}_i^{(\ell)}$ and $\mathrm{ExtRng}_i^{(\ell)}$, $i = 2, 3, 4$, as follows:

$$\begin{aligned} &\mathrm{ExtDom}_2^{(\ell)} := \big\{u_2[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \{2, 4, \ldots, w\}\big\} \\ &\mathrm{ExtRng}_2^{(\ell)} := \big\{S_2^*(a) : a \in \mathrm{ExtDom}_2^{(\ell)}\big\} \\ &\mathrm{ExtDom}_3^{(\ell)} := \Big\{\big(T \cdot \big(\mathsf{PGF}^{S_2^*}(u_2)\big) + k_2\big)[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \{2, 4, \ldots, w\}\Big\} \\ &\mathrm{ExtRng}_3^{(\ell)} := \big\{S_3^*(a) : a \in \mathrm{ExtDom}_3^{(\ell)}\big\} \\ &\mathrm{ExtDom}_4^{(\ell)} := \Big\{v_4[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \big\{2, 4, \ldots, w\big\}\Big\} \\ &\mathrm{ExtRng}_4^{(\ell)} := \big\{S_4^*(a) : a \in \mathrm{ExtDom}_4^{(\ell)}\big\} \end{aligned}$$

Note that, conditioned on $\mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)$, the values in $\mathrm{ExtDom}_i^{(\ell)}$ and $\mathrm{ExtRng}_i^{(\ell)}$, $i = 2, 3, 4$, are compatible with the set $\cup_{i=1}^{\ell-1} Q_{m_i}$. For Q_{m_ℓ}, two useful properties regarding the arrangement of tuples and the derived intermediate values resp. could be exhibited.

Lemma 2. *Consider the ℓ-th set $Q_{m_\ell} = \big((u_1^{(\ell,1)}, u_2^{(\ell,1)}, v_4^{(\ell,1)}, v_5^{(\ell,1)}), \ldots\big)$. If it is of* **Type-I***, then the number of tuples $(u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ with $u_1[\mathsf{even}] = u_1^{(\ell,1)}[\mathsf{even}]$ is at most 1; if it is of* **Type-II***, then the number of $(u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ with $v_5[\mathsf{even}] = v_5^{(\ell,1)}[\mathsf{even}]$ is also at most 1.*

The proof is deferred to the Appendix B.2.

Lemma 3. *Consider the ℓ-th set Q_{m_ℓ} and any two distinct elements $\big(u_1^{(\ell,i_1)}, u_2^{(\ell,i_1)}, v_4^{(\ell,i_1)}, v_5^{(\ell,i_1)}\big)$ and $\big(u_1^{(\ell,i_2)}, u_2^{(\ell,i_2)}, v_4^{(\ell,i_2)}, v_5^{(\ell,i_2)}\big)$ in Q_{m_ℓ}. Then, there exist two indices $j_1, j_2 \in \{2, 4, \ldots, w\}$ such that,*

- *when Q_{m_ℓ} is of* **Type-I***: $u_2^{(\ell,i_1)}[j_1] \notin Dom_2 \cup ExtDom_2^{(\ell)}$, $u_2^{(\ell,i_2)}[j_2] \notin Dom_2 \cup ExtDom_2^{(\ell)}$, and $(u_2^{(\ell,i_1)}[j_1], u_2^{(\ell,i_1)}[j_2]) \neq (u_2^{(\ell,i_2)}[j_1], u_2^{(\ell,i_2)}[j_2])$;*
- *when Q_{m_ℓ} is of* **Type-II***: $v_4^{(\ell,i_1)}[j_1] \notin Dom_4 \cup ExtDom_4^{(\ell)}$, $v_4^{(\ell,i_2)}[j_2] \notin Dom_4 \cup ExtDom_4^{(\ell)}$, and $(v_4^{(\ell,i_1)}[j_1], v_4^{(\ell,i_1)}[j_2]) \neq (v_4^{(\ell,i_2)}[j_1], v_4^{(\ell,i_2)}[j_2])$.*

The proof is deferred to the Appendix B.3. With the help of these two lemmas, we are able to bound the probability that the randomness is compatible with the ℓ-th set Q_{m_ℓ}.

Lemma 4. *For the ℓ-th set Q_{m_ℓ}, it holds*

$$\begin{aligned}&\Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big]\\ \geq\ &\Big(1 - \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{4N}\Big) \cdot \frac{1}{N^{w\beta_\ell}}.\end{aligned} \tag{9}$$

The proof is deferred to the Appendix B.4.

From Eq. (9), Eq. (8), and using $\sum_{\ell=1}^{\alpha} \beta_\ell = q_C$, we obtain

$$\begin{aligned}&\Pr_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{mid}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big]\\ \geq\ &\prod_{\ell=1}^{\alpha}\Big(\Big(1 - \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{4N}\Big) \cdot \frac{1}{N^{w\beta_\ell}}\Big)\\ \geq\ &\Big(1 - \sum_{\ell=1}^{\alpha} \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{4N}\Big) \cdot \frac{1}{N^{w\sum_{\ell=1}^{\alpha}\beta_\ell}}\\ \geq\ &\Big(1 - \frac{12wq_C(q_S + wq_C/2) + 3w^2 q_C^2}{4N}\Big) \cdot \frac{1}{N^{wq_C}}.\end{aligned}$$

Gathering this and Eqs. (7), (6), and (5), we finally reach

$$\begin{aligned}\frac{\mu(\tau)}{\nu(\tau)} &\geq \Big(1 - \frac{4wq_Cq_S + w^2q_C + w^2q_C^2}{2N}\Big)\Big(1 - \frac{12wq_C(q_S + wq_C/2) + 3w^2q_C^2}{4N}\Big) \cdot \frac{(N^w)_{q_C}}{N^{wq_C}}\\ &\geq \Big(1 - \frac{4wq_Cq_S + w^2q_C + w^2q_C^2}{2N}\Big)\Big(1 - \frac{12wq_C(q_S + wq_C/2) + 3w^2q_C^2}{4N}\Big) \cdot \Big(1 - \frac{q_C^2}{N^w}\Big)\\ &\geq 1 - \frac{20wq_Cq_S + 13w^2q_C^2}{4N} - \frac{q_C^2}{N^w} \ \geq\ 1 - \frac{20wq_Cq_S + 13w^2q_C^2}{4N} - \frac{q_C^2}{N^{w/2}}.\end{aligned}$$

Further, using Eq. (4) yields the bound in Eq. (3) and completes the proof.

5 SPRP Security at 5 Rounds with Public Functions

In this section, we will prove security for 5-round GEGFNs built upon 5 random functions $\mathbf{F} = \{F_1, F_2, F_3, F_4, F_5\}$ and a *single linear layer* T. Firstly, we modify the definition 1 to apply to the situation of using random functions.

Definition 2 (Good Linear Layer for 5 Rounds with Functions). *A matrix $T \in \mathbb{F}_N^{w\times w}$ is good if T is MDS, and the 2 induced matrices T_{EO} and $(T^{-1})_{\text{EO}}$ are such that:*

1. *They contain no zero entries, and*
2. *Any column vector of the 2 induced matrices consists of $w/2$ distinct entries.*

With a good linear layer in Definition 2, we have the following theorem on 5-round GEGFNs with public random functions.

Theorem 2. *Assume $w \geq 2$. Let $\mathcal{C}5_{\mathbf{k}}^{\boldsymbol{F}}$ be a 5-round, linear GEGFN structure defined in Eq. (10), with distribution $\mathcal{K}$ over keys $\mathbf{k} = (k_0, \ldots, k_5)$ and public functions $\boldsymbol{F} = (F_1, F_2, F_3, F_4, F_5)$.*

$$\mathcal{C}5_{\mathbf{k}}^{\boldsymbol{F}}(x) := k_5 + \mathsf{PGF}^{F_5}\big(k_4 + T\cdot\big(\mathsf{PGF}^{F_4}\big(k_3 + T\cdot\big(\mathsf{PGF}^{F_3}\big(k_2 + T\cdot\big(\mathsf{PGF}^{F_2}\big(k_1 + T\cdot\big(\mathsf{PGF}^{F_1}(k_0 + x)\big)\big)\big)\big)\big)\big)\big)\big). \quad (10)$$

If k_0 and k_5 are uniformly distributed and the matrix T fulfills Definition 2, then

$$\mathsf{Adv}^{\mathsf{sprp}}_{\mathcal{C}5_{\mathbf{k}}^{F}}(q_C, q_F) \leq \frac{20wq_Cq_F + 9w^2q_C^2}{8N} + \frac{2q_C^2}{N^{w/2}}. \quad (11)$$

Since $\mathcal{C}5_{\mathbf{k}}^{\mathbf{F}}$ is defined on random functions instead of random permutations, which slightly deviates from the permutation case, for the proof, we only need to make some moderate modifications to the previous proof for $\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}$. We follow the proof idea of $\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}$ and reduce proof as follows.

Proof Setup. Fix a deterministic distinguisher D. Similar to Sect. 4.1, we assume D makes exactly q_C (non-redundant) forward/inverse queries to its left oracle that is either $\mathcal{C}5_{\mathbf{k}}^{\mathbf{F}}$ or P, and exactly q_F (non-redundant) forward queries to each of the oracle F_i on its right side. We call a query from D to its left oracle a *construction query* and a query from D to one of its right oracles a *function query.*

The interaction between D and its oracles is recorded in the form of 6 lists of pairs $Q_{\mathcal{C}} \subseteq \mathbb{F}_N^w \times \mathbb{F}_N^w$ and $Q_{F_1}, \ldots, Q_{F_5} \subseteq \mathbb{F}_N \times \mathbb{F}_N$. The definition of $Q_{\mathcal{C}}$ remains unchange, $Q_{F_1}, \ldots, Q_{F_5}$ are defined similarly with respect to queries to $F_1, \ldots, F_5$. Define $Q_{\mathbf{F}} := (Q_{F_1}, \ldots, Q_{F_5})$. For convenience, for $i \in \{1, 2, 3, 4, 5\}$ we define

$$\mathrm{Dom}_i := \big\{a : (a, b) \in Q_{F_i} \text{ for some } b \in \mathbb{F}_N\big\}, \mathrm{Rng}_i := \big\{b : (a, b) \in Q_{F_i} \text{ for } a \in \mathbb{F}_N\big\}.$$

Similar to Sect. 4.1, we augment the transcript $(Q_{\mathcal{C}}, Q_{\mathbf{F}})$ with a key value $\mathbf{k} = (k_0, \ldots, k_5)$. Thus, a transcript τ has the final form $\tau = (Q_{\mathcal{C}}, Q_{\mathbf{F}}, \mathbf{k})$.

Completing the Proof. Note that since F_i is a random function, for a new input x, the function value $F_i(x)$ is uniform in $\mathbb{F}_N$, for $i = 1, 2, 3, 4, 5$, i.e., for any y, the probability of $F_i(x) = y$ is $1/N$. This is the main difference from the proof of $\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}$.

In detail, we recall the definition of bad transcripts in Sect. 4.2 and we also have the same definition of bad transcripts in $\mathcal{C}5_{\mathbf{k}}^{\mathbf{F}}$. Therefore,

Lemma 5. *The upper bounding of getting bad transcripts in the ideal world is*

$$\Pr\big[\nu \in \mathcal{T}_2\big] \le \frac{wq_C q_S}{N} + \frac{w^2 q_C^2}{4N} + \sum_{\ell=1}^{q_C} \frac{2(\ell-1)}{N^{w/2}} \le \frac{wq_C q_F}{N} + \frac{w^2 q_C^2}{4N} + \frac{q_C^2}{N^{w/2}}. \quad (12)$$

Then, following the idea as before, we bound the ratio $\mu(\tau)/\nu(\tau)$. Let $\Omega_X = \big(\mathcal{F}(1)\big)^5 \times \mathcal{K}$ be the probability space underlying the real world and $\Omega_Y = \mathcal{P}(w) \times \big(\mathcal{F}(1)\big)^5 \times \mathcal{K}$ be the probability space underlying the ideal world. We fix a transcript $\tau = (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \in \mathcal{T}_1$. Since $\tau \in \mathcal{T}$, it is easy to see (cf. [8]) that

$$\begin{aligned}\mu(\tau) &= \Pr[\omega \leftarrow \Omega_X : \omega \downarrow \tau] = \Pr[\mathbf{k}^* = \mathbf{k}] \cdot \Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow \tau],\\ \nu(\tau) &= \Pr[\omega \leftarrow \Omega_Y : \omega \downarrow \tau] = \Pr[\mathbf{k}^* = \mathbf{k}] \cdot \Pr_{P^*,\mathbf{F}^*}[(P^*, \mathbf{F}^*) \downarrow \tau],\end{aligned}$$

where the notation indicates that ω is sampled from the relevant probability space according to that space's probability measure and $\mathbf{F}^*$ and $(P^*, \mathbf{F}^*)$ are sampled uniformly from $(\mathcal{F}(1))^5$ and $\mathcal{P}(w) \times (\mathcal{F}(1))^5$, respectively. Thus,

$$\frac{\mu(\tau)}{\nu(\tau)} = \frac{\Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow \tau]}{\Pr_{P^*,\mathbf{F}^*}[(P^*, \mathbf{F}^*) \downarrow \tau]}.$$

By these, and by $|Q_\mathcal{C}| = q_C, |Q_{F_1}| = \ldots = |Q_{F_5}| = q_F$, it is immediate that

$$\Pr_{P^*,\mathbf{F}^*}\big[(P^*, \mathbf{F}^*) \downarrow \tau\big] = \frac{1}{(N^w)_{q_C} \cdot \big(N^{q_F}\big)^5}.$$

To compute $\Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow \tau]$ we start by writing

$$\begin{aligned}\Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow \tau] &= \Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k})]\\ &= \Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})] \cdot \Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})]\\ &= \frac{1}{(N^{q_F})^5} \cdot \Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})].\end{aligned}$$

Now let's focus on $\Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})]$. To analyze $\Pr_{\mathbf{F}^*}[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})]$, we proceed in two steps. First, based on $Q_\mathcal{C}$ and two outer random functions F_1^*, F_5^*, we derive the 2nd and 4th rounds intermediate values: these constitute a special transcript Q_{mid} on the middle 3 rounds. We characterize conditions on F_1^*, F_5^* that will ensure certain good properties in the derived Q_{mid}, which will ease the analysis. Therefore, in the second step, we analyze such "good" Q_{mid} to yield the final bounds. Thus,

$$\begin{aligned}&\Pr_{\mathbf{F}^*}\big[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})\big]\\ \ge\; &\Pr_{\mathbf{F}^*}\big[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*) \mid \mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})\big]\\ =\; &\Pr_{\mathbf{F}^*}\big[\mathsf{Good}(\mathbf{F}^*) \mid \mathbf{F}^* \downarrow (\emptyset, Q_\mathbf{F}, \mathbf{k})\big] \cdot \Pr_{\mathbf{F}^*}\big[\mathbf{F}^* \downarrow (Q_\mathcal{C}, Q_\mathbf{F}, \mathbf{k}) \mid \mathsf{Good}(\mathbf{F}^*)\big]. \quad (13)\end{aligned}$$

In the first step, we define $\mathsf{Bad}(\mathbf{F}^*)$ the same as $\mathsf{Bad}(\mathcal{S}^*)$. So we have the following lemma,

Lemma 6.

$$\Pr_{\boldsymbol{F}^*}\left[\mathsf{Bad}(\boldsymbol{F}^*) \mid \boldsymbol{F}^* \downarrow (\emptyset, Q_{\boldsymbol{F}}, \mathbf{k})\right] \leq \frac{4wq_Cq_F + w^2q_C + w^2q_C^2}{4N}. \tag{14}$$

The proof is deferred to the Appendix C.1.

Then, in the second step, we analyze $\Pr_{\mathbf{F}^*}\left[\mathbf{F}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathbf{F}}, \mathbf{k}) \mid \mathsf{Good}(\mathbf{F}^*)\right]$. We define Q_{mid} as before and we have $\Pr_{\mathbf{F}^*}\left[\mathbf{F}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathbf{F}}, \mathbf{k}) \mid \mathsf{Good}(\mathbf{F}^*)\right] = \Pr_{\mathbf{F}^*}\left[\mathbf{F}^* \downarrow (Q_{mid}, Q_{\mathbf{F}}, \mathbf{k}) \mid \mathsf{Good}(\mathbf{F}^*)\right]$.

Lemma 7. *For the set Q_{mid}, it holds*

$$\Pr_{\boldsymbol{F}^*}\left[\boldsymbol{F}^* \downarrow (Q_{mid}, Q_{\boldsymbol{F}}, \mathbf{k}) \mid \mathsf{Good}(\boldsymbol{F}^*)\right] \geq \left(1 - \frac{4wq_C(q_F + wq_C/2) + w^2q_C^2}{8N}\right) \cdot \frac{1}{N^{wq_C}}. \tag{15}$$

The proof is deferred to the Appendix C.2.

Gathering Eq. (13) and Eqs. (14) and (15), we finally reach

$$\begin{aligned}
\frac{\mu(\tau)}{\nu(\tau)} \geq & \left(1 - \frac{4wq_Cq_F + w^2q_C + w^2q_C^2}{4N}\right)\left(1 - \frac{4wq_C(q_F + wq_C/2) + w^2q_C^2}{8N}\right) \cdot \frac{(N^w)_{q_C}}{N^{wq_C}} \\
\geq & \left(1 - \frac{4wq_Cq_F + w^2q_C + w^2q_C^2}{4N}\right)\left(1 - \frac{4wq_C(q_F + wq_C/2) + w^2q_C^2}{8N}\right) \cdot \left(1 - \frac{q_C^2}{N^w}\right) \\
\geq & 1 - \frac{12wq_Cq_F + 7w^2q_C^2}{8N} - \frac{q_C^2}{N^w} \geq 1 - \frac{12wq_Cq_F + 7w^2q_C^2}{8N} - \frac{q_C^2}{N^{w/2}}.
\end{aligned}$$

Further, using Eq. (12) yield the bound in Eq. (11) and complete the proof.

6 Conclusion

In this paper, we explore the problem of minimizing non-linearity in Type-II Generalized Feistel Networks. Inspired by the fast diffusion of SPNs, we consider incorporating their (strong) diffusion layers into Type-II Generalized Feistel Networks and introduce the key in each round. Thus, we introduce a new variant of the generalized Feistel Networks, which we call GEGFN. To provide a theoretical justification, we study SPRP security of GEGFN using random permutation or function in binary fields $\mathbb{F}_{2^n}$ and prime fields $\mathbb{F}_p$, with p being prime. Our research proves birthday-bound security at 5 rounds.

Acknowledgments

We thank the anonymous reviewers for their invaluable comments and suggestions, which helped us improve the manuscript. Yuqing Zhao and Chun Guo were partly supported by the Program of Qilu Young Scholars (Grant No. 61580089963177) of Shandong University. Weijia Wang was partly supported by the Program of Qilu Young Scholars (Grant No. 61580082063088) of Shandong University.

References

1. Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel structures for mpc, and more. In: Sako, K., Schneider, S.A., Ryan, P.Y.A. (eds.) Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security, Luxembourg, September 23-27, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11736, pp. 151–171. Springer (2019). https://doi.org/10.1007/978-3-030-29962-0_8, https://doi.org/10.1007/978-3-030-29962-0_8
2. Albrecht, M.R., Rechberger, C., Schneider, T., Tiessen, T., Zohner, M.: Ciphers for MPC and FHE. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 430–454. Springer, Heidelberg (Apr 2015). https://doi.org/10.1007/978-3-662-46800-5_17
3. Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of symmetric-key primitives for advanced cryptographic protocols. IACR Trans. Symm. Cryptol. **2020**(3), 1–45 (2020). https://doi.org/10.13154/tosc.v2020.i3.1-45
4. Bar-On, A., Dinur, I., Dunkelman, O., Lallemand, V., Keller, N., Tsaban, B.: Cryptanalysis of SP networks with partial non-linear layers. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 315–342. Springer, Heidelberg (Apr 2015). https://doi.org/10.1007/978-3-662-46800-5_13
5. Berger, T.P., Francq, J., Minier, M., Thomas, G.: Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. IEEE Trans. Computers **65**(7), 2074–2089 (2016). https://doi.org/10.1109/TC.2015.2468218, https://doi.org/10.1109/TC.2015.2468218
6. Bhaumik, R., List, E., Nandi, M.: ZCZ - achieving n-bit SPRP security with a minimal number of tweakable-block-cipher calls. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part I. LNCS, vol. 11272, pp. 336–366. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03326-2_12
7. Cauchois, V., Gomez, C., Thomas, G.: General diffusion analysis: How to find optimal permutations for generalized type-II Feistel schemes. IACR Trans. Symm. Cryptol. **2019**(1), 264–301 (2019). https://doi.org/10.13154/tosc.v2019.i1.264-301
8. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (May 2014). https://doi.org/10.1007/978-3-642-55220-5_19
9. Cogliati, B., Dodis, Y., Katz, J., Lee, J., Steinberger, J.P., Thiruvengadam, A., Zhang, Z.: Provable security of (tweakable) block ciphers based on substitution-permutation networks. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part I. LNCS, vol. 10991, pp. 722–753. Springer, Heidelberg (Aug 2018). https://doi.org/10.1007/978-3-319-96884-1_24
10. Derbez, P., Fouque, P., Lambin, B., Mollimard, V.: Efficient search for optimal diffusion layers of generalized feistel networks. IACR Trans. Symmetric Cryptol. **2019**(2), 218–240 (2019). https://doi.org/10.13154/tosc.v2019.i2.218-240, https://doi.org/10.13154/tosc.v2019.i2.218-240
11. Dodis, Y., Katz, J., Steinberger, J., Thiruvengadam, A., Zhang, Z.: Provable security of substitution-permutation networks. Cryptology ePrint Archive, Report 2017/016 (2017), https://eprint.iacr.org/2017/016

12. Dodis, Y., Stam, M., Steinberger, J.P., Liu, T.: Indifferentiability of confusion-diffusion networks. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 679–704. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_24
13. Gao, Y., Guo, C.: Provable Security Of HADES Structure. In: Cryptology and Network Security: 21st International Conference, CANS 2022, Abu Dhabi, United Arab Emirates, November 13–16, 2022, Proceedings. p. 258–276. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-20974-1_13, https://doi.org/10.1007/978-3-031-20974-1_13
14. Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.X.: Block ciphers that are easier to mask: How far can we go? In: Bertoni, G., Coron, J.S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 383–399. Springer, Heidelberg (Aug 2013). https://doi.org/10.1007/978-3-642-40349-1_22
15. Grassi, L., Hao, Y., Rechberger, C., Schofnegger, M., Walch, R., Wang, Q.: Horst meets fluid-spn: Griffin for zero-knowledge applications. Cryptology ePrint Archive, Paper 2022/403 (2022), https://eprint.iacr.org/2022/403, https://eprint.iacr.org/2022/403. To appear at CRYPTO 2023.
16. Grassi, L., Kales, D., Khovratovich, D., Roy, A., Rechberger, C., Schofnegger, M.: Starkad and Poseidon: New hash functions for zero knowledge proof systems. Cryptology ePrint Archive, Report 2019/458 (2019), https://eprint.iacr.org/2019/458
17. Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., Schofnegger, M.: Poseidon: A new hash function for zero-knowledge proof systems. In: USENIX Security Symposium (2021)
18. Grassi, L., Lüftenegger, R., Rechberger, C., Rotaru, D., Schofnegger, M.: On a generalization of substitution-permutation networks: The HADES design strategy. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 674–704. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45724-2_23
19. Guo, C., Standaert, F.X., Wang, W., Wang, X., Yu, Y.: Provable Security of SP Networks with Partial Non-Linear Layers. In: FSE 2021. pp. 353–388 (2021). https://doi.org/10.46586/tosc.v2021.i2.353-388
20. Halevi, S.: EME*: Extending EME to handle arbitrary-length messages with associated data. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 315–327. Springer, Heidelberg (Dec 2004)
21. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 482–499. Springer, Heidelberg (Aug 2003). https://doi.org/10.1007/978-3-540-45146-4_28
22. Halevi, S., Rogaway, P.: A parallelizable enciphering mode. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 292–304. Springer, Heidelberg (Feb 2004). https://doi.org/10.1007/978-3-540-24660-2_23
23. Hoang, V.T., Rogaway, P.: On generalized Feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (Aug 2010). https://doi.org/10.1007/978-3-642-14623-7_33
24. Iwata, T., Kurosawa, K.: On the pseudorandomness of the AES finalists - RC6 and Serpent. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 231–243. Springer, Heidelberg (Apr 2001). https://doi.org/10.1007/3-540-44706-7_16
25. Lacan, J., Fimes, J.: Systematic mds erasure codes based on vandermonde matrices. IEEE Communications Letters **8**, 570–572 (2004)

26. Nakamichi, R., Iwata, T.: Iterative block ciphers from tweakable block ciphers with long tweaks. IACR Trans. Symm. Cryptol. **2019**(4), 54–80 (2019). https://doi.org/10.13154/tosc.v2019.i4.54-80
27. Nakaya, K., Iwata, T.: Generalized feistel structures based on tweakable block ciphers. IACR Trans. Symmetric Cryptol. **2022**(4), 24–91 (2022). https://doi.org/10.46586/tosc.v2022.i4.24-91, https://doi.org/10.46586/tosc.v2022.i4.24-91
28. Nandi, M.: XLS is not a strong pseudorandom permutation. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part I. LNCS, vol. 8873, pp. 478–490. Springer, Heidelberg (Dec 2014). https://doi.org/10.1007/978-3-662-45611-8_25
29. Nandi, M.: On the optimality of non-linear computations of length-preserving encryption schemes. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II. LNCS, vol. 9453, pp. 113–133. Springer, Heidelberg (Nov / Dec 2015). https://doi.org/10.1007/978-3-662-48800-3_5
30. Patarin, J.: The "coefficients H" technique (invited talk). In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (Aug 2009). https://doi.org/10.1007/978-3-642-04159-4_21
31. Ristenpart, T., Rogaway, P.: How to enrich the message space of a cipher. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 101–118. Springer, Heidelberg (Mar 2007). https://doi.org/10.1007/978-3-540-74619-5_7
32. Suzaki, T., Minematsu, K.: Improving the generalized Feistel. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 19–39. Springer, Heidelberg (Feb 2010). https://doi.org/10.1007/978-3-642-13858-4_2
33. Wu, S., Wang, M.: Automatic search of truncated impossible differentials for word-oriented block ciphers. In: Galbraith, S.D., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 283–302. Springer, Heidelberg (Dec 2012). https://doi.org/10.1007/978-3-642-34931-7_17
34. Wu, W., Zhang, L.: LBlock: A lightweight block cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 11. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (Jun 2011). https://doi.org/10.1007/978-3-642-21554-4_19
35. Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO'89. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (Aug 1990). https://doi.org/10.1007/0-387-34805-0_42

A The H-coefficient Technique

We use Patarin's H-coefficient technique [30] to prove the SPRP security of GEGFNs. We provide a quick overview of its main ingredients here. Our presentation borrows heavily from that of [8]. Fix a distinguisher D that makes at most q queries to its oracles. As in the security definition presented above, D's aim is to distinguish between two worlds: a "real world" and an "ideal world". Assume wlog that D is deterministic. The execution of D defines a *transcript* that includes the sequence of queries and answers received from its oracles; D's output is a deterministic function of its transcript. Thus, if μ, ν denote the probability distributions on transcripts induced by the real and ideal worlds, respectively, then D's distinguishing advantage is upper bounded by the statistical distance

$$\mathsf{Dist}(\mu,\nu) := \frac{1}{2}\sum_{\tau}\big|\mu(\tau)-\nu(\tau)\big|, \tag{16}$$

where the sum is taken over all possible transcripts τ.

Let $\mathcal{T}$ denote the set of all transcripts such that $\nu(\tau) > 0$ for all $\tau \in \mathcal{T}$. We look for a partition of $\mathcal{T}$ into two sets $\mathcal{T}_1$ and $\mathcal{T}_2$ of "good" and "bad" transcripts, respectively, along with a constant $\epsilon_1 \in [0,1)$ such that

$$\tau \in \mathcal{T}_1 \Longrightarrow \mu(\tau)/\nu(\tau) \geq 1-\epsilon_1. \tag{17}$$

It is then possible to show (see [8] for details) that

$$\mathsf{Dist}(\mu,\nu) \leq \epsilon_1 + \Pr[\nu \in \mathcal{T}_2] \tag{18}$$

is an upper bound on the distinguisher's advantage.

B Deferred Proofs for Theorem 1

B.1 Proof of Lemma 1

This requires to bound $\Pr_{\mathcal{S}^*}\big[(\text{B-}\ell) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big]$ for $\ell = 1,2,3$. Consider condition (B-1) first. Fix some $(x,y) \in Q_{\mathcal{C}}$ and an index $i \in \{2,4,\dots,w\}$. Since τ is good, $(x+k_0)[w] \notin \mathrm{Dom}_1$, and $(x+k_0)[w] \neq (x+k_0)[i']$ for $i' \neq w$. So after conditioning on $\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})$ and the values of $S_1^*((x+k_0)[i'])$ for $i' \neq w$, the value $S_1^*((x+k_0)[w])$ is uniform in a set of size $N - q_S - w/2 + 1$. The MDS property implies that every entry in the $(w-1)$-th column of T is non-zero, and thus

$$\Pr_{\mathcal{S}^*}\Big[\big(T\cdot(\mathsf{PGF}^{S_1^*}(x+k_0))+k_1\big)[i] \in \mathrm{Dom}_2 \mid \mathcal{S}^*\downarrow(\emptyset,Q_{\mathcal{S}},\mathbf{k})\Big] \leq \frac{q_S}{N-q_S-w/2}.$$

Similarly by symmetry, we have

$$\Pr_{\mathcal{S}^*}\Big[\big(T^{-1}\cdot(((\mathsf{PGF}^{S_5^*})^{-1}(y-k_5))-k_4)\big)[i] \in \mathrm{Dom}_4 \mid \mathcal{S}^*\downarrow(\emptyset,Q_{\mathcal{S}},\mathbf{k})\Big] \leq \frac{q_S}{N-q_S-w/2}.$$

Summing over $(x, y) \in Q_{\mathcal{C}}$, $i \in \{2, 4, \ldots, w\}$, we reach

$$\Pr_{\mathcal{S}^*}\left[(\text{B-1}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \frac{wq_C q_S}{N - q_S - w/2}. \tag{19}$$

Next, consider (B-2). Fix $(x, y) \in Q_{\mathcal{C}}$ and $i, i' \in \{1, 2, \ldots, w/2\}$, and let $u_1 = x + k_0$, $u_2 = T \cdot (\mathsf{PGF}^{S_1^*}(u_1)) + k_1$. Then the "even half" $u_2[\mathsf{even}] = T_{\text{EO}} \cdot \overline{S_1^*}(u_1[\mathsf{even}]) + T_{\text{EO}} \cdot u_1[\mathsf{odd}] + T_{\text{EE}} \cdot u_1[\mathsf{even}] + k_1[\mathsf{even}]$. Since T is MDS, T_{EO} is nonsingular. This means T_{EO} is invertible, and further that the i-th and i'-th rows of T_{EO} are linearly independent and, in particular, there exists an index $j_0 \in \{1, \ldots, w/2\}$ such that the (i, j_0)-th and (i', j_0)-th entries of T_{EO} are not equal. After conditioning on $\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})$ and the values of $S_1^*(u_1[2 \cdot j_1])$ for $j_1 \neq j_0$, the value of $S_1^*(u_1[2 \cdot j_0])$ is uniform in $N - q_S - w/2 + 1$ values. Therefore,

$$\Pr_{\mathcal{S}^*}\Big[u_2[2 \cdot i] = u_2[2 \cdot i'] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\Big] \leq \frac{1}{N - q_S - w/2}.$$

Similarly by symmetry, the probability of have $\big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[2 \cdot i] = \big(T^{-1} \cdot (((\mathsf{PGF}^{S_5^*})^{-1}(y - k_5)) - k_4)\big)[2 \cdot i']$ is also at most $1/(N - q_S - w/2)$. By a union bound over all pairs $(x, y) \in Q_{\mathcal{C}}$ and all $i, i' \in \{1, \ldots, w/2\}$, we reach

$$\Pr_{\mathcal{S}^*}\left[(\text{B-2}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \binom{w/2}{2} \cdot \frac{2q_C}{N - q_S - w/2} \leq \frac{w^2 q_C}{4(N - q_S - w/2)}. \tag{20}$$

We now consider (B-3). We first fix $(x, y), (x', y') \in Q_{\mathcal{C}}$ and $i, i' \in \{2, 4, \ldots, w\}$ with $x[\mathsf{even}] \neq x'[\mathsf{even}]$ for the 1st condition. This means $x[j_0] \neq x'[j_0]$ for some $j_0 \in \{2, 4, \ldots, w\}$. Since τ is good, for $j_1 \in \{2, 4, \ldots, w\}$, $(x + k_0)[j_0] \neq (x + k_0)[j_1]$ for all $j_1 \neq j_0$ and $(x + k_0)[j_0] \neq (x' + k_0)[j_1]$ for all j_1. So after conditioning on $\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})$ and the values of $S_1^*((x + k_0)[j_1])$ for $j_1 \neq j_0$ and $S_1^*((x' + k_0)[j_1])$ for $j_1 \in \{2, 4, \ldots, w\}$, the value of $S_1^*((x + k_0)[j_0])$ is uniform in $\geq N - q_S - w + 1$ possibilities. Because every entry in the $(j_0 - 1)$-th column of T is non-zero, we have

$$\Pr_{\mathcal{S}^*}\Big[\big(T(\mathsf{PGF}^{S_1^*}(x + k_0)) + k_1\big)[i] = \big(T(\mathsf{PGF}^{S_1^*}(x' + k_0)) + k_1\big)[i'] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\Big]$$
$$\leq \frac{1}{N - q_S - w}.$$

We next fix $(x, y), (x', y') \in Q_{\mathcal{C}}$ and $i \neq i' \in \{2, 4, ..., w\}$ with $x[\mathsf{even}] = x'[\mathsf{even}]$ for the 2nd condition. While this case concerns distinct construction queries, the argument is an extension of that of (B-2). In detail, let $u_1 = x + k_0$, $u_2 = T \cdot (\mathsf{PGF}^{S_1^*}(u_1)) + k_1$, $u_1' = x' + k_0$, and $u_2' = T \cdot (\mathsf{PGF}^{S_1^*}(u_1')) + k_1$. By the analysis for (B-2), we have $\Pr_{\mathcal{S}^*}\left[u_2[i] = u_2[i'] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \frac{1}{N - q_S - w/2}$. Since $x[\mathsf{even}] = x'[\mathsf{even}]$, it can be seen as $u_2' - u_2 = T \cdot (x' - x)$, meaning that

$$u_2'[i'] = u_2[i'] + \underbrace{\big(T_{\text{EO}} \cdot (x'[\mathsf{odd}] - x[\mathsf{odd}])\big)[i'/2]}_{\delta}.$$

The offset δ is fixed by τ and is independent of S_1^*. Therefore,

$$\Pr_{\mathcal{S}^*}\left[u_2[i] = u_2'[i'] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \Pr_{\mathcal{S}^*}\left[u_2[i] = u_2[i'] + \delta \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right]$$

$$\leq \frac{1}{N - q_S - w/2}.$$

For each choice of $(x, y), (x', y')$, the 1st and 2nd conditions are mutually exclusive (i.e., only one may be fulfilled). Hence, summing over all pairs $(x, y, i), (x', y', i') \in Q_{\mathcal{C}} \times \{2, 4, \ldots, w\}$, the probability that either of the two is fulfilled is at most

$$\binom{wq_C/2}{2} \cdot \frac{1}{N - q_S - w} \leq \frac{w^2 q_C^2}{8(N - q_S - w)}.$$

Similarly by symmetry, the probability that either the 3rd or the 4th condition is fulfilled is at most $\frac{w^2 q_C^2}{8(N - q_S - w)}$. Thus

$$\Pr_{\mathcal{S}^*}\left[\text{(B-3)} \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \frac{w^2 q_C^2}{4(N - q_S - w)}. \tag{21}$$

Summing over Eqs. (19), (20), and (21), we reach Eq. (6):

$$\Pr_{\mathcal{S}^*}\left[\mathsf{Bad}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \frac{wq_C q_S}{N - q_S - w/2} + \frac{w^2 q_C + w^2 q_C^2}{4(N - q_S - w)}.$$

B.2 Proof of Lemma 2

Wlog, consider the case of **Type-I** Q_{m_ℓ}, as the other case is just symmetric. Assume otherwise, and assume that $\mathsf{tuple}_1 = \left(u_1^{(j_1)}, u_2^{(j_1)}, v_4^{(j_1)}, v_5^{(j_1)}\right)$ and $\mathsf{tuple}_2 = \left(u_1^{(j_2)}, u_2^{(j_2)}, v_4^{(j_2)}, v_5^{(j_2)}\right)$ in $\cup_{i=1}^{\ell-1} Q_{m_i}$ are such two tuples with the smallest indices j_1, j_2. Wlog assume $j_2 > j_1$, i.e., tuple_2 was later. Then tuple_2 was necessarily a forward query, as otherwise $u_1^{(j_1)}[\mathsf{even}] = u_1^{(j_2)}[\mathsf{even}]$ would contradict the goodness of τ (the 4th condition). By this and further by the 4th condition, $v_5^{(j_2)}[\mathsf{even}]$ is "new", and tuple_2 cannot be in any **Type-II** set Q_{m_i}, $i \leq \ell - 1$. This means there exists a **Type-I** set Q_{m_i}, $i \leq \ell - 1$, such that $\mathsf{tuple}_2 \in Q_{m_i}$. By our rules, the tuples in the purported Q_{m_ℓ} should have been Q_{m_i}, and thus Q_{m_ℓ} should not exist, reaching a contradiction.

B.3 Proof of Lemma 3

Wlog consider a **Type-I** Q_{m_ℓ}. First, note that by $\neg$(B-1) (the 1st condition), $u_2^{(\ell,i_1)}[j] \notin \text{Dom}_2$ and $u_2^{(\ell,i_2)}[j] \notin \text{Dom}_2$ for any $j \in \{2, 4, \ldots, w\}$. We then distinguish two cases depending on $\cup_{i=1}^{\ell-1} Q_{m_i}$ (which contribute to $\text{ExtDom}_2^{(\ell)}$):

Case 1: $\boldsymbol{u_1^{(\ell,i_1)}}$[even] $\boldsymbol{\neq u_1}$[even] for all $\boldsymbol{(u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}}$. Then by $\neg$(B-3), $u_2^{(\ell,i_1)}[j], u_2^{(\ell,i_2)}[j] \notin \text{ExtDom}_2^{(\ell)}$ *for all* $j \in \{2, 4, \ldots, w\}$. Among these $w/2$ indices, there exists j_1 such that $u_2^{(\ell,i_1)}[j_1] \neq u_2^{(\ell,i_2)}[j_1]$, as otherwise, it would contradict the "q_C non-redundant forward/inverse queries". Therefore, we complete the argument for this case.

Case 2: there exists $(u_1^*, u_2^*, v_4^*, v_5^*) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ with $u_1^*[\mathsf{even}] = u_1^{(\ell,i_1)}[\mathsf{even}]$. Then by construction, we have $u_2^{(\ell,i_1)}[\mathsf{even}] = u_2^*[\mathsf{even}] + \Delta_{i_1}$ and $u_2^{(\ell,i_2)}[\mathsf{even}] = u_2^*[\mathsf{even}] + \Delta_{i_2}$, where $\Delta_{i_1} = T_{\text{EO}} \cdot \big(u_1^{(\ell,i_1)}[\mathsf{odd}] - u_1^*[\mathsf{odd}]\big)$ and $\Delta_{i_2} = T_{\text{EO}} \cdot \big(u_1^{(\ell,i_2)}[\mathsf{odd}] - u_1^*[\mathsf{odd}]\big)$. Let $\mathcal{J}_{i_1}$ be the subset of $\{2,4,\ldots,w\}$ such that $\Delta_{i_1}[j] \neq 0$ iff. $j \in \mathcal{J}_{i_1}$, and $\mathcal{J}_{i_2} \subseteq \{2,4,\ldots,w\}$ be such that $\Delta_{i_2}[j] \neq 0$ iff. $j \in \mathcal{J}_{i_2}$. We distinguish three subcases depending on $\mathcal{J}_{i_1}$ and $\mathcal{J}_{i_2}$:

- Subcase 2.1: $\mathcal{J}_{i_1} \backslash \mathcal{J}_{i_2} \neq \emptyset$. Then, let $j_1 \in \mathcal{J}_{i_1} \backslash \mathcal{J}_{i_2}$, and $j_2 \in \mathcal{J}_{i_2}$ in arbitrary. This means $j_1 \neq j_2$, $\Delta_{i_1}[j_1] \neq 0$ but $\Delta_{i_2}[j_1] = 0$, and then $u_2^{(\ell,i_1)}[j_1] \neq u_2^{(\ell,i_2)}[j_1]$. Moreover,
  - $u_2^{(\ell,i_1)}[j_1] \neq u_2^*[j_3]$ for any $j_3 \notin \{2,4,\ldots,w\} \backslash \{j_1\}$, by $\neg$(B-3) (the 2nd condition); $u_2^{(\ell,i_1)}[j_1] \neq u_2^*[j_1]$ since $j_1 \in \mathcal{J}_{i_1}$. Thus $u_2^{(\ell,i_1)}[j_1] \notin \text{ExtDom}_2^{(\ell)}$. Similarly for $u_2^{(\ell,i_2)}$.
  - $u_1^{(\ell,i_1)}[\mathsf{even}] \neq u_1^{**}[\mathsf{even}]$ for any $(u_1^{**}, u_2^{**}, v_4^{**}, v_5^{**}) \neq (u_1^*, u_2^*, v_4^*, v_5^*)$ in $\cup_{i=1}^{\ell-1} Q_{m_i}$ (by Lemma 2), and thus $u_2^{(\ell,i_1)}[j_1] \neq u_2^{**}[j']$ for any $j' \in \{2,4,\ldots,w\}$ by $\neg$(B-3) (the 1st condition). Similarly for $u_2^{(\ell,i_2)}$.
- Subcase 2.2: $\mathcal{J}_{i_2} \backslash \mathcal{J}_{i_1} \neq \emptyset$. Then, let $j_2 \in \mathcal{J}_{i_2} \backslash \mathcal{J}_{i_1}$, and $j_1 \in \mathcal{J}_{i_1}$, and the argument is similar to subcase 2.1 by symmetry.
- Subcase 2.3: $\mathcal{J}_{i_1} = \mathcal{J}_{i_2}$. Then there exists $j \in \mathcal{J}_{i_1}$ such that $\Delta_{i_1}[j] \neq \Delta_{i_2}[j]$, as otherwise $\Delta_{i_1} = \Delta_{i_2}$, meaning a contradiction. Let $j_1 = j_2 = j$, then it's easy to see all the claims hold.

By the above, for **Type-I** sets, the claims hold in all cases. Thus the claim.

B.4 Proof of Lemma 4

We distinguish two cases depending on the type of Q_{m_ℓ}.

Case 1: Q_{m_ℓ} is Type-I. By our dividing rules, the tuples in this Q_{m_ℓ} may have the same inputs to the 2nd round S-boxes. We define a bad predicate BadII_ℓ that concerns with the 2nd round outputs $v_2^{(\ell,1)} := \mathsf{PGF}^{S_2^*}(u_2^{(\ell,1)}), \ldots, v_2^{(\ell,\beta_\ell)} := \mathsf{PGF}^{S_2^*}(u_2^{(\ell,\beta_\ell)})$. With these notations, $\mathsf{BadII}_\ell(\mathcal{S}^*)$ is fulfilled, if either (C-1) or (C-2) is fulfilled:

- (C-1) S_2^* leads to unfresh intermediate values: there exists $i \in \{1,\ldots,\beta_\ell\}$ and $j \in \{1,3,\ldots,w-1\}$ such that $u_3^{(\ell,i)}[j+1] \in \text{Dom}_3 \cup \text{ExtDom}_3^{(\ell)}$, or $(v_3^{(\ell,i)}[j] - u_3^{(\ell,i)}[j]) \in \text{Rng}_3 \cup \text{ExtRng}_3^{(\ell)}$, or $(v_4^{(\ell,i)}[j] - u_4^{(\ell,i)}[j]) \in \text{Rng}_4 \cup \text{ExtRng}_4^{(\ell)}$.
- (C-2) S_2^* leads to colliding intermediate values: there exists distinct (i_1,j_1), $(i_2,j_2) \in \{1,\ldots,\beta_\ell\} \times \{1,3,\ldots,w-1\}$ such that $u_3^{(\ell,i_1)}[j_1+1] = u_3^{(\ell,i_2)}[j_2+1]$, or $v_3^{(\ell,i_1)}[j_1] - u_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_2)}[j_2] - u_3^{(\ell,i_2)}[j_2]$, or $v_4^{(\ell,i_1)}[j_1] - u_4^{(\ell,i_1)}[j_1] = v_4^{(\ell,i_2)}[j_2] - u_4^{(\ell,i_2)}[j_2]$.

Consider (C-1) first. Fix $(i,j) \in \{1,\ldots,\beta_\ell\} \times \{1,3,\ldots,w-1\}$, and consider the condition $u_3^{(\ell,i)}[j+1] \in \text{Dom}_3 \cup \text{ExtDom}_3^{(\ell)}$ first. By Lemma 3, conditioned on $\mathsf{Good}(\mathcal{S}^*)$ and the values in $\text{Rng}_2 \cup \text{ExtRng}_2^{(\ell)}$, there exists $j' \in \{2,4,\ldots,w\}$ such that $v_2^{(\ell,i)}[j'-1]-u_2^{(\ell,i)}[j'-1] = S_2^*\big(u_2^{(\ell,i)}[j']\big)$ is uniform in at least $N-q_S-wq_C/2$ possibilities. Since

$$\begin{aligned} u_3^{(\ell,i)}[\mathsf{even}] &= T_{\text{EO}}\cdot v_2^{(\ell,i)}[\mathsf{odd}] + T_{\text{EE}}\cdot u_2^{(\ell,i)}[\mathsf{even}]+k_2[\mathsf{even}] \\ &= T_{\text{EO}}\cdot\overline{S_2^*}\big(u_2^{(\ell,i)}[\mathsf{even}]\big)+T_{\text{EO}}\cdot u_2^{(\ell,i)}[\mathsf{odd}]+T_{\text{EE}}\cdot u_2^{(\ell,i)}[\mathsf{even}]+k_2[\mathsf{even}], \end{aligned} \tag{22}$$

and since every entry in the $(j'/2)$-th column of T_{EO} is non-zero, for any $j \in \{1, 3, \dots, w-1\}$, we have

$$\begin{aligned} &\Pr_{\mathcal{S}^*}\Big[u_3^{(\ell,i)}[j+1]\in(\mathrm{Dom}_3\cup\mathrm{ExtDom}_3^{(\ell)})\mid \mathcal{S}^*\downarrow(\cup_{i=1}^{\ell-1}Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k})\wedge\mathsf{Good}(\mathcal{S}^*)\Big] \\ &\le\frac{q_S+wq_C/2}{N-q_S-wq_C/2}. \end{aligned}$$

We proceed to consider $v_3^{(\ell,i)}[j]-u_3^{(\ell,i)}[j]$ and $v_4^{(\ell,i)}[j]-u_4^{(\ell,i)}[j]$. Note that

$$\begin{pmatrix}(u_4^{(\ell,i)}-k_3)[1]\\(u_4^{(\ell,i)}-k_3)[2]\\ \dots\\(u_4^{(\ell,i)}-k_3)[w]\end{pmatrix}=T\cdot\begin{pmatrix}v_3^{(\ell,i)}[1]\\v_3^{(\ell,i)}[2]\\ \dots\\v_3^{(\ell,i)}[w]\end{pmatrix}\Leftrightarrow\begin{pmatrix}(u_4^{(\ell,i)}-k_3)[\mathsf{even}]\\(u_4^{(\ell,i)}-k_3)[\mathsf{odd}]\end{pmatrix}=\underbrace{\begin{pmatrix}T_{\text{EE}} & T_{\text{EO}}\\T_{\text{OE}} & T_{\text{OO}}\end{pmatrix}}_{T_1}\cdot\begin{pmatrix}v_3^{(\ell,i)}[\mathsf{even}]\\v_3^{(\ell,i)}[\mathsf{odd}]\end{pmatrix},$$

and

$$\begin{pmatrix}v_3^{(\ell,i)}[\mathsf{odd}]\\u_4^{(\ell,i)}[\mathsf{odd}]\end{pmatrix}=\widehat{T_1}\cdot\begin{pmatrix}v_3^{(\ell,i)}[\mathsf{even}]\\(u_4-k_3)^{(\ell,i)}[\mathsf{even}]\end{pmatrix}+\begin{pmatrix}0^{\frac{w}{2}}\\k_3[\mathsf{odd}]\end{pmatrix}.$$

By Eq. (1), it can be seen $v_3^{(\ell,i)}[\mathsf{odd}]-u_3^{(\ell,i)}[\mathsf{odd}]$ is written as

$$\begin{aligned} &v_3^{(\ell,i)}[\mathsf{odd}]-u_3^{(\ell,i)}[\mathsf{odd}] \\ &=\big(-T_{\text{EO}}^{-1}\cdot T_{\text{EE}}\cdot T_{\text{EO}}-T_{\text{OO}}\big)\cdot v_2^{(\ell,i)}[\mathsf{odd}]+g_1\Big(u_2^{(\ell,i)}[\mathsf{even}], v_4^{(\ell,i)}[\mathsf{even}], k_2, k_3\Big) \\ &=\big(-T_{\text{EO}}^{-1}\cdot T_{\text{EE}}\cdot T_{\text{EO}}-T_{\text{OO}}\big)\cdot\overline{S_2^*}\big(u_2^{(\ell,i)}[\mathsf{even}]\big) \\ &\qquad\qquad+g_2\Big(u_2^{(\ell,i)}[\mathsf{even}], u_2^{(\ell,i)}[\mathsf{odd}], v_4^{(\ell,i)}[\mathsf{even}], k_2, k_3\Big), \end{aligned} \tag{23}$$

where g_1 and g_2 are (complicated) functions of $u_2^{(\ell,i)}[\mathsf{even}]$, $u_2^{(\ell,i)}[\mathsf{odd}]$, $v_4^{(\ell,i)}[\mathsf{even}]$, k_2, and k_3. Similarly,

$$\begin{aligned} &v_4^{(\ell,i)}[\mathsf{odd}]-u_4^{(\ell,i)}[\mathsf{odd}] \\ &=-\big(T_{\text{OE}}-T_{\text{OO}}\cdot T_{\text{EO}}^{-1}\cdot T_{\text{EE}}\big)\cdot T_{\text{EO}}\cdot v_2^{(\ell,i)}[\mathsf{odd}]+g_3\Big(u_2^{(\ell,i)}[\mathsf{even}], v_4^{(\ell,i)}, k_2, k_3\Big) \\ &=-\big(T_{\text{OE}}-T_{\text{OO}}\cdot T_{\text{EO}}^{-1}\cdot T_{\text{EE}}\big)\cdot T_{\text{EO}}\cdot\overline{S_2^*}\big(u_2^{(\ell,i)}[\mathsf{even}]\big)+g_4\Big(u_2^{(\ell,i)}, v_4^{(\ell,i)}, k_2, k_3\Big), \end{aligned} \tag{24}$$

where g_3 and g_4 are (complicated) functions of $u_2^{(\ell,i)}$, $v_4^{(\ell,i)}$, k_2, and k_3. As we assumed that neither $-T_{\text{EO}}^{-1}\cdot T_{\text{EE}}\cdot T_{\text{EO}}-T_{\text{OO}}$ nor $-\big(T_{\text{OE}}-T_{\text{OO}}\cdot T_{\text{EO}}^{-1}\cdot T_{\text{EE}}\big)\cdot T_{\text{EO}}$ contains zero entries (see Definition 1), and,—by Lemma 3,—conditioned on $\mathsf{Good}(\mathcal{S}^*)$

and the values in $\mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, there exists $j' \in \{2, 4, \ldots, w\}$ such that $S_2^*\big(u_2^{(\ell,i)}[j']\big)$ is uniform in $\geq N - q_S - wq_C/2$ possibilities, the probability of having $(v_3^{(\ell,i)}[j] - u_3^{(\ell,i)}[j]) \in \mathrm{Rng}_3 \cup \mathrm{ExtRng}_3^{(\ell)}$, or $(v_4^{(\ell,i)}[j] - u_4^{(\ell,i)}[j]) \in \mathrm{Rng}_4 \cup \mathrm{ExtRng}_4^{(\ell)}$ is at most $\frac{q_S + wq_C/2}{N - q_S - wq_C/2}$.

Summing over the $\beta_\ell w/2$ choices of $(i,j) \in \{1, \ldots, \beta_\ell\} \times \{1, 3, \ldots, w-1\}$, we reach

$$\Pr_{\mathcal{S}^*}\big[(\text{C-1}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \leq \frac{3\beta_\ell w(q_S + wq_C/2)}{2(N - q_S - wq_C/2)}.$$

Next, consider (C-2). Depending on whether $i_1 = i_2$, we will divide the discussion into two cases.

For the case of $i_1 = i_2 \in \{1, \ldots, \beta_\ell\}$, fix distinct $j_1, j_2 \in \{1, 3, \ldots, w-1\}$. Consider the condition $u_3^{(\ell,i_1)}[j_1 + 1] = u_3^{(\ell,i_1)}[j_2 + 1]$ first. By Lemma 3, conditioned on $\mathsf{Good}(\mathcal{S}^*)$ and the values in $\mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, there exists $j_3 \in \{2, 4, \ldots, w\}$ such that $S_2^*\big(u_2^{(\ell,i_1)}[j_3]\big)$ is uniform in at least $N - q_S - wq_C/2$ possibilities. We refer to Eq. (22) for the expression of $u_3^{(\ell,i)}[\mathsf{even}]$. By the 2nd condition in Definition 1, the $\big((j_1{+}1)/2, j_3/2\big)$-th and $\big((j_2{+}1)/2, j_3/2\big)$-th entries of T_{EO} are not equal. So, the probability of having $u_3^{(\ell,i_1)}[j_1 + 1] = u_3^{(\ell,i_1)}[j_2 + 1]$ is equal to the probability that $S_2^*\big(u_2^{(\ell,i_1)}[j_3]\big)$ equals some fixed value, which is at most $1/(N - q_S - wq_C/2)$.

For condition $v_3^{(\ell,i_1)}[j_1] - u_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_2)}[j_2] - u_3^{(\ell,i_2)}[j_2]$ and $v_4^{(\ell,i_1)}[j_1] - u_4^{(\ell,i_1)}[j_1] = v_4^{(\ell,i_2)}[j_2] - u_4^{(\ell,i_2)}[j_2]$, the arguments follow similar flows. Concretely, we refer to Eq. (23) and (24) for the expressions of $v_3^{(\ell,i)}[\mathsf{odd}] - u_3^{(\ell,i)}[\mathsf{odd}]$ and $v_4^{(\ell,i)}[\mathsf{odd}] - u_4^{(\ell,i)}[\mathsf{odd}]$ resp. By the 2nd condition in Definition 1, the $\big((j_1 + 1)/2, j_3/2\big)$-th and $\big((j_2 + 1)/2, j_3/2\big)$-th entries of $-T_{\text{EO}}^{-1} \cdot T_{\text{EE}} \cdot T_{\text{EO}} - T_{\text{OO}}$ differ; the $\big((j_1 + 1)/2, j_3/2\big)$-th and $\big((j_2 + 1)/2, j_3/2\big)$-th entries of $-\big(T_{\text{OE}} - T_{\text{OO}} \cdot T_{\text{EO}}^{-1} \cdot T_{\text{EE}}\big) \cdot T_{\text{EO}}$ differ. By these, the probability of having $v_3^{(\ell,i_1)}[j_1] - u_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_2)}[j_2] - u_3^{(\ell,i_2)}[j_2]$ or $v_4^{(\ell,i_1)}[j_1] - u_4^{(\ell,i_1)}[j_1] = v_4^{(\ell,i_2)}[j_2] - u_4^{(\ell,i_2)}[j_2]$ is at most $1/(N - q_S - wq_C/2)$.

For the case of $i_1 \neq i_2$, fix $j_1, j_2 \in \{1, 3, \ldots, w-1\}$. By Lemma 3, there exists $j_3, j_4 \in \{2, 4, \ldots, w\}$ such that:

- $u_2^{(\ell,i_1)}[j_3] \notin \mathrm{Dom}_2 \cup \mathrm{ExtDom}_2^{(\ell)}$, $u_2^{(\ell,i_2)}[j_4] \notin \mathrm{Dom}_2 \cup \mathrm{ExtDom}_2^{(\ell)}$, and
- either $u_2^{(\ell,i_1)}[j_3] \neq u_2^{(\ell,i_2)}[j_3]$ or $u_2^{(\ell,i_1)}[j_4] \neq u_2^{(\ell,i_2)}[j_4]$.

Wlog assume $u_2^{(\ell,i_1)}[j_3] \neq u_2^{(\ell,i_2)}[j_3]$. Note that, by $\neg$(B-3) (the 2nd condition), $u_2^{(\ell,i_1)}[j_3] \neq u_2^{(\ell,i_2)}[j_5]$ for any $j_5 \in \{2, 4, \ldots, w\} \backslash \{j_3\}$. Therefore, conditioned on the values in $\mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, on the $w/2-1$ values $\big\{S_2^*\big(u_2^{(\ell,i_1)}[j]\big)\big\}_{j \in \{2,4,\ldots,w\} \backslash \{j_3\}}$, and on the $w/2$ values $\big\{S_2^*\big(u_2^{(\ell,i_2)}[j]\big)\big\}_{j \in \{2,4,\ldots,w\}}$, $S_2^*\big(u_2^{(\ell,i_1)}[j_3]\big)$ remains uniform in at least $N - q_S - wq_C/2$ possibilities. By this,

- since (the $\big(j_3/2\big)$-th column of) T_{EO} has no zero entry, the probability of having $u_3^{(\ell,i_1)}[j_1{+}1] = u_3^{(\ell,i_2)}[j_2{+}1]$ is equal to the probability that $S_2^*(u_2^{(\ell,i_1)}[j_3])$ equals some fixed value, which is at most $1/(N - q_S - wq_C/2)$;

- since $-T_{\text{EO}}^{-1} \cdot T_{\text{EE}} \cdot T_{\text{EO}} - T_{\text{OO}}$ has no zero entry, the probability of having $v_3^{(\ell,i_1)}[j_1] - u_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_2)}[j_2] - u_3^{(\ell,i_2)}[j_2]$ is at most $1/(N - q_S - wq_C/2)$.
- since $-\big(T_{\text{OE}} - T_{\text{OO}} \cdot T_{\text{EO}}^{-1} \cdot T_{\text{EE}}\big) \cdot T_{\text{EO}}$ has no zero entry, the probability of having $v_4^{(\ell,i_1)}[j_1] - u_4^{(\ell,i_1)}[j_1] = v_4^{(\ell,i_2)}[j_2] - u_4^{(\ell,i_2)}[j_2]$ is at most $1/(N - q_S - wq_C/2)$.

By a union bound over the conditions and over all i_1, i_2, j_1, j_2, we reach

$$\Pr_{\mathcal{S}^*}\left[(\text{C-2}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right] \leq \binom{w\beta_\ell/2}{2} \cdot \frac{3}{N - q_S - wq_C/2}.$$

Using $q_S + wq_C/2 \leq N/2$, we finally have

$$\Pr_{\mathcal{S}^*}\left[\mathsf{BadII}_\ell(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right] \leq \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{4N}.$$

Now, conditioned on $\neg\mathsf{BadII}_\ell(\mathcal{S}^*)$, $\mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k})$, and $\mathsf{Good}(\mathcal{S}^*)$, the event that $\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k})$ is equivalent to S_3^* and S_4^* satisfying $w\beta_\ell$ new and distinct equations, i.e., $S_3^*\big(u_3^{(\ell,i)}[j]\big) = v_3^{(\ell,i)}[j-1] - u_3^{(\ell,i)}[j-1]$, $S_4^*\big(u_4^{(\ell,i)}[j]\big) = v_4^{(\ell,i)}[j-1] - u_4^{(\ell,i)}[j-1]$, $i = 1, \ldots, \beta_\ell$, $j \in \{2, 4, \ldots, w\}$: they are new due to $\neg$(C-1) and $\neg$(B-3), and they are distinct due to $\neg$(C-2) and $\neg$(B-3). The probability that S_3^* and S_4^* satisfy these equations is *at least* $1/N^{w\beta_\ell}$. Therefore,

$$\begin{aligned}
& \Pr_{\mathcal{S}^*}\left[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right] \\
\geq\ & \Pr_{\mathcal{S}^*}\left[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \neg\mathsf{BadII}_\ell(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right] \\
=\ & \Pr_{\mathcal{S}^*}\left[\neg\mathsf{BadII}_\ell(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right] \\
& \cdot \Pr_{\mathcal{S}^*}\left[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \neg\mathsf{BadII}_\ell(\mathcal{S}^*) \wedge \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right] \\
=\ & \big(1 - \Pr_{\mathcal{S}^*}\left[\mathsf{BadII}_\ell(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right]\big) \\
& \cdot \Pr_{\mathcal{S}^*}\left[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \neg\mathsf{BadII}_\ell(\mathcal{S}^*) \wedge \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\right] \\
\geq\ & \Big(1 - \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{4N}\Big) \cdot \frac{1}{N^{w\beta_\ell}}.
\end{aligned}$$

Case 2: Q_{m_ℓ} is Type-II. The argument is symmetric to the above for **Type-I** group. More concretely, we define a bad predicate BadII_ℓ that concerns the 4nd round S-box inputs as well as the other values involved in the inverse computation. For every $(u_1^{(\ell,i)}, u_2^{(\ell,i)}, v_4^{(\ell,i)}, v_5^{(\ell,i)}) \in Q_{m_\ell}$, $i = 1, \ldots, \beta_\ell$, define $u_4^{(\ell,i)} := \big(\mathsf{PGF}^{S_4^*}\big)^{-1}(v_4^{(\ell,i)})$, $v_3^{(\ell,i)} := T^{-1} \cdot \big(u_4^{(\ell,i)} - k_3\big)$,

$$\begin{pmatrix} (u_3^{(\ell,i)} - k_2)[1] \\ (u_3^{(\ell,i)} - k_2)[2] \\ \ldots \\ (u_3^{(\ell,i)} - k_2)[w] \end{pmatrix} = T \cdot \begin{pmatrix} v_2^{(\ell,i)}[1] \\ v_2^{(\ell,i)}[2] \\ \ldots \\ v_2^{(\ell,i)}[w] \end{pmatrix} \Leftrightarrow \begin{pmatrix} (u_3^{(\ell,i)} - k_2)[\mathsf{even}] \\ (u_3^{(\ell,i)} - k_2)[\mathsf{odd}] \end{pmatrix} = \underbrace{\begin{pmatrix} T_{\text{EE}} & T_{\text{EO}} \\ T_{\text{OE}} & T_{\text{OO}} \end{pmatrix}}_{T_2} \cdot \begin{pmatrix} v_2^{(\ell,i)}[\mathsf{even}] \\ v_2^{(\ell,i)}[\mathsf{odd}] \end{pmatrix},$$

and

$$\begin{pmatrix} v_2^{(\ell,i)}[\mathsf{odd}] \\ u_3^{(\ell,i)}[\mathsf{odd}] \end{pmatrix} = \widehat{T_2} \cdot \begin{pmatrix} v_2^{(\ell,i)}[\mathsf{even}] \\ (u_3 - k_2)^{(\ell,i)}[\mathsf{even}] \end{pmatrix} + \begin{pmatrix} 0^{\frac{w}{2}} \\ k_2[\mathsf{odd}] \end{pmatrix}.$$

These indicate

$$v_3^{(\ell,i)}[\mathsf{even}] = -(T^{-1})_{\mathrm{EO}} \cdot \overline{S_4^*}\big(v_4^{(\ell,i)}[\mathsf{even}]\big) + g_5\Big(v_4^{(\ell,i)}[\mathsf{even}], v_4^{(\ell,i)}[\mathsf{odd}], k_3\Big),$$

$$v_3^{(\ell,i)}[\mathsf{odd}] - u_3^{(\ell,i)}[\mathsf{odd}] = -\Big((T^{-1})_{\mathrm{OO}} - T_{\mathrm{OO}} \cdot T_{\mathrm{EO}}^{-1} \cdot (T^{-1})_{\mathrm{EO}}\Big) \cdot \overline{S_4^*}(v_4^{(\ell,i)}[\mathsf{even}]) + g_6\Big(v_4^{(\ell,i)}, u_2^{(\ell,i)}[\mathsf{even}], k_2, k_3\Big),$$

$$v_2^{(\ell,i)}[\mathsf{odd}] - u_2^{(\ell,i)}[\mathsf{odd}] = -T_{\mathrm{EO}}^{-1} \cdot (T^{-1})_{\mathrm{EO}} \cdot \overline{S_4^*}(v_4^{(\ell,i)}[\mathsf{even}]) + g_7\Big(v_4^{(\ell,i)}, u_2^{(\ell,i)}, k_2, k_3\Big),$$

where g_5, g_6, g_7 are (complicated) functions of parameters. Then, $\mathsf{BadII}_\ell(\mathcal{S}^*)$ is fulfilled, if either (C-1) or (C-2) is fulfilled:

- (C-1) There exists $i \in \{1, \ldots, \beta_\ell\}$ and $j \in \{1, 3, \ldots, w-1\}$ such that $v_3^{(\ell,i)}[j+1] \in \mathrm{Dom}_3 \cup \mathrm{ExtDom}_3^{(\ell)}$, or $v_3^{(\ell,i)}[j] - u_3^{(\ell,i)}[j] \in \mathrm{Rng}_3 \cup \mathrm{ExtRng}_3^{(\ell)}$, or $v_2^{(\ell,i)}[j] - u_2^{(\ell,i)}[j] \in \mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$.
- (C-2) There exists distinct pairs $(i_1, j_1), (i_2, j_2) \in \{1, \ldots, \beta_\ell\} \times \{1, 3, \ldots, w-1\}$ such that $v_3^{(\ell,i_1)}[j_1+1] = v_3^{(\ell,i_2)}[j_2+1]$, or $v_3^{(\ell,i_1)}[j_1] - u_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_2)}[j_2] - u_3^{(\ell,i_2)}[j_2]$, or $v_2^{(\ell,i_1)}[j_1] - u_2^{(\ell,i_1)}[j_1] = v_2^{(\ell,i_2)}[j_2] - u_2^{(\ell,i_2)}[j_2]$.

The argument then follows similarly, using the goodness (see Definition 1) of the three matrices $(T^{-1})_{\mathrm{EO}}$, $(T^{-1})_{\mathrm{OO}} - T_{\mathrm{OO}} \cdot T_{\mathrm{EO}}^{-1} \cdot (T^{-1})_{\mathrm{EO}}$ and $T_{\mathrm{EO}}^{-1} \cdot (T^{-1})_{\mathrm{EO}}$, and yielding $w\beta_\ell$ new and distinct equations on S_2^* and S_3^*. Thus Eq. (9) remains true.

C Proof of Theorem 2

C.1 Proof of Lemma 6

Note that since F_i is a random function, for a new input x, the function value $F_i(x)$ is uniform in $\mathbb{F}_N$, for $i = 1, 2, 3, 4, 5$, i.e., for any y, the probability of $F_i(x) = y$ is $1/N$. This is the main difference from the proof of $\mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}$. We define $\mathsf{Bad}(\mathbf{F}^*)$ the same as $\mathsf{Bad}(\mathcal{S}^*)$. Since we use the random function, the probabilities are as follows:

(i) $\Pr_{\mathbf{F}^*}\big[(\text{B-1}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_{\mathbf{F}}, \mathbf{k})\big] \le \frac{w q_C q_F}{N}$,
(ii) $\Pr_{\mathbf{F}^*}\big[(\text{B-2}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_{\mathbf{F}}, \mathbf{k})\big] \le \binom{w/2}{2} \cdot \frac{2q_C}{N} \le \frac{w^2 q_C}{4N}$,
(iii) $\Pr_{\mathbf{F}^*}\big[(\text{B-3}) \mid \mathbf{F}^* \downarrow (\emptyset, Q_{\mathbf{F}}, \mathbf{k})\big] \le \frac{w^2 q_C^2}{4N}$.

Summing the probabilities above, we have the Lemma 6.

C.2 Proof of Lemma 7

We still assume that Q_{mid} is divided into α disjoint sets by the above rules, with $|Q_{m_\ell}| = \beta_\ell$. Then $\sum_{\ell=1}^{\alpha} \beta_\ell = q_C$, and

$$\Pr_{\mathbf{F}^*}\big[\mathbf{F}^* \downarrow (Q_{mid}, Q_{\mathbf{F}}, \mathbf{k}) \mid \mathsf{Good}(\mathbf{F}^*)\big]$$

$$= \prod_{\ell=1}^{\alpha} \Pr_{\mathbf{F}^*}\left[\mathbf{F}^* \downarrow (Q_{m_\ell}, Q_{\mathbf{F}}, \mathbf{k}) \mid \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right]. \quad (25)$$

Now we could focus on analyzing the ℓ-th set Q_{m_ℓ}. Assume that

$$Q_{m_\ell} = \Big(\big(u_1^{(\ell,1)}, u_2^{(\ell,1)}, v_4^{(\ell,1)}, v_5^{(\ell,1)}\big), \ldots, \big(u_1^{(\ell,\beta_\ell)}, u_2^{(\ell,\beta_\ell)}, v_4^{(\ell,\beta_\ell)}, v_5^{(\ell,\beta_\ell)}\big)\Big).$$

The superscript (ℓ, i) indicates that it is the i-th tuple in this ℓ-th set Q_{m_ℓ}. For this index ℓ, we define six sets $\mathrm{ExtDom}_i^{(\ell)}$ and $\mathrm{ExtRng}_i^{(\ell)}$, $i = 2, 3, 4$, as follows:

$$\mathrm{ExtDom}_2^{(\ell)} := \left\{u_2[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \{2, 4, \ldots, w\}\right\}$$
$$\mathrm{ExtRng}_2^{(\ell)} := \left\{F_2^*(a) : a \in \mathrm{ExtDom}_2^{(\ell)}\right\}$$
$$\mathrm{ExtDom}_3^{(\ell)} := \Big\{\big(T \cdot \big(\mathsf{PGF}^{F_2^*}(u_2)\big) + k_2\big)[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \{2, 4, \ldots, w\}\Big\}$$
$$\mathrm{ExtRng}_3^{(\ell)} := \left\{F_3^*(a) : a \in \mathrm{ExtDom}_3^{(\ell)}\right\}$$
$$\mathrm{ExtDom}_4^{(\ell)} := \Big\{v_4[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \{2, 4, \ldots, w\}\Big\}$$
$$\mathrm{ExtRng}_4^{(\ell)} := \left\{F_4^*(a) : a \in \mathrm{ExtDom}_4^{(\ell)}\right\}$$

Note that, conditioned on $\mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)$, the values in $\mathrm{ExtDom}_i^{(\ell)}$ and $\mathrm{ExtRng}_i^{(\ell)}$, $i = 2, 3, 4$, are compatible with the set $\cup_{i=1}^{\ell-1} Q_{m_i}$. For Q_{m_ℓ}, Lemma 2 and 3 will also be hold. With the help of these two lemmas, we are able to bound the probability that the randomness is compatible with the ℓ-th set Q_{m_ℓ}.

Following the idea as before, we define $\mathsf{BadII}_\ell(\mathbf{F}^*)$:

- (C-1) F_2^* (or F_4^*) leads to unfresh intermediate values: there exists $i \in \{1, \ldots, \beta_\ell\}$ and $j \in \{2, 4, \ldots, w\}$ such that $u_3^{(\ell,i)}[j] \in \mathrm{Dom}_3 \cup \mathrm{ExtDom}_3^{(\ell)}$.
- (C-2) F_2^* (or F_4^*) leads to colliding intermediate values: there exists distinct $(i_1, j_1), (i_2, j_2) \in \{1, \ldots, \beta_\ell\} \times \{2, 4, \ldots, w\}$ such that $u_3^{(\ell,i_1)}[j_1] = u_3^{(\ell,i_2)}[j_2]$.

The probabilities make the following modifications:

(i) $\Pr_{\mathbf{F}^*}\left[\text{(C-1)} \mid \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right] \le \frac{\beta_\ell w(q_F + wq_C/2)}{2N}$,

(ii) $\Pr_{\mathbf{F}^*}\left[\text{(C-2)} \mid \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right] \le \binom{w\beta_\ell/2}{2} \cdot \frac{1}{N} \le \frac{w^2\beta_\ell^2}{8N}$.

We finally have

$$\begin{aligned} &\Pr_{\mathbf{F}^*}\left[\mathsf{BadII}_\ell(\mathbf{F}^*) \mid \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right] \\ \le\ & \frac{4\beta_\ell w(q_F + wq_C/2) + \beta_\ell^2 w^2}{8N}. \end{aligned}$$

Now, conditioned on $\neg\mathsf{BadII}_\ell(\mathbf{F}^*)$, $\mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k})$, and $\mathsf{Good}(\mathbf{F}^*)$, the event that $\mathbf{F}^* \downarrow (Q_{m_\ell}, Q_{\mathbf{F}}, \mathbf{k})$ is equivalent to F_3^* and F_4^* satisfying $w\beta_\ell$ new and distinct equations, or F_3^* and F_2^* satisfying $w\beta_\ell$ new and distinct equations. They are new due to $\neg$(C-1) and $\neg$(B-3), and they are distinct due to $\neg$(C-2) and

$\neg$(B-3). The probability that F_3^* and F_4^* (or F_3^* and F_2^*) satisfy these equations is $1/N^{w\beta_\ell}$. Therefore,

$$\begin{aligned}
& \Pr_{\mathbf{F}^*}\left[\mathbf{F}^* \downarrow (Q_{m_\ell}, Q_{\mathbf{F}}, \mathbf{k}) \mid \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right] \\
\geq\ & \Pr_{\mathbf{F}^*}\left[\mathbf{F}^* \downarrow (Q_{m_\ell}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \neg\mathsf{BadII}_\ell(\mathbf{F}^*) \mid \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right] \\
=\ & \left(1 - \Pr_{\mathbf{F}^*}\left[\mathsf{BadII}_\ell(\mathbf{F}^*) \mid \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right]\right) \\
& \cdot \Pr_{\mathbf{F}^*}\left[\mathbf{F}^* \downarrow (Q_{m_\ell}, Q_{\mathbf{F}}, \mathbf{k}) \mid \neg\mathsf{BadII}_\ell(\mathbf{F}^*) \wedge \mathbf{F}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathbf{F}}, \mathbf{k}) \wedge \mathsf{Good}(\mathbf{F}^*)\right] \\
\geq\ & \left(1 - \frac{4\beta_\ell w(q_F + wq_C/2) + \beta_\ell^2 w^2}{8N}\right) \cdot \frac{1}{N^{w\beta_\ell}}. \qquad (26)
\end{aligned}$$

From Eq. (26) and using $\sum_{\ell=1}^{\alpha} \beta_\ell = q_C$, we obtain the Lemma 7.

D MDS Candidates in $\mathbb{F}_N$

An important question is whether such a strong T in Definition 1 exists at all. Note that if a strong T in Definition 1 exists, then T in Definition 2 naturally exists. Therefore, we give candidates in $\mathbb{F}_N$, where N is either a power of 2 or a prime number.

D.1 MDS in Binary Field

Using the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$, two candidates for $N = 2^8$ and $w = 8, 16$, respectively, are as follows. We employ Vandermonde matrices [25] to generate these MDS matrices.

$$\begin{pmatrix}
0\mathrm{x}87 & 0\mathrm{x}B3 & 0\mathrm{x}1D & 0\mathrm{x}C7 & 0\mathrm{x}27 & 0\mathrm{x}12 & 0\mathrm{x}5A & 0\mathrm{x}83 \\
0\mathrm{x}86 & 0\mathrm{x}3C & 0\mathrm{x}E6 & 0\mathrm{x}3E & 0\mathrm{x}0D & 0\mathrm{x}BA & 0\mathrm{x}E9 & 0\mathrm{x}3D \\
0\mathrm{x}5D & 0\mathrm{x}F4 & 0\mathrm{x}4A & 0\mathrm{x}1C & 0\mathrm{x}0C & 0\mathrm{x}3B & 0\mathrm{x}79 & 0\mathrm{x}B0 \\
0\mathrm{x}51 & 0\mathrm{x}B1 & 0\mathrm{x}A6 & 0\mathrm{x}A5 & 0\mathrm{x}34 & 0\mathrm{x}6A & 0\mathrm{x}A7 & 0\mathrm{x}1B \\
0\mathrm{x}63 & 0\mathrm{x}66 & 0\mathrm{x}BC & 0\mathrm{x}83 & 0\mathrm{x}02 & 0\mathrm{x}C9 & 0\mathrm{x}63 & 0\mathrm{x}93 \\
0\mathrm{x}61 & 0\mathrm{x}B5 & 0\mathrm{x}B6 & 0\mathrm{x}97 & 0\mathrm{x}EE & 0\mathrm{x}67 & 0\mathrm{x}09 & 0\mathrm{x}74 \\
0\mathrm{x}62 & 0\mathrm{x}9E & 0\mathrm{x}42 & 0\mathrm{x}C4 & 0\mathrm{x}50 & 0\mathrm{x}35 & 0\mathrm{x}DA & 0\mathrm{x}C4 \\
0\mathrm{x}A5 & 0\mathrm{x}65 & 0\mathrm{x}FB & 0\mathrm{x}90 & 0\mathrm{x}FC & 0\mathrm{x}8E & 0\mathrm{x}C9 & 0\mathrm{x}11
\end{pmatrix},$$

$$\begin{pmatrix}
0\mathrm{x}52 & 0\mathrm{x}E7 & 0\mathrm{x}AE & 0\mathrm{x}82 & 0\mathrm{x}5E & 0\mathrm{x}47 & 0\mathrm{x}66 & 0\mathrm{x}1C & 0\mathrm{x}7C & 0\mathrm{x}35 & 0\mathrm{x}68 & 0\mathrm{x}BE & 0\mathrm{x}96 & 0\mathrm{x}13 & 0\mathrm{x}D1 & 0\mathrm{x}30 \\
0\mathrm{x}FB & 0\mathrm{x}A2 & 0\mathrm{x}7B & 0\mathrm{x}AB & 0\mathrm{x}2E & 0\mathrm{x}8E & 0\mathrm{x}5A & 0\mathrm{x}F9 & 0\mathrm{x}8C & 0\mathrm{x}07 & 0\mathrm{x}E2 & 0\mathrm{x}C3 & 0\mathrm{x}82 & 0\mathrm{x}c8 & 0\mathrm{x}89 & 0\mathrm{x}E2 \\
0\mathrm{x}D4 & 0\mathrm{x}FA & 0\mathrm{x}EC & 0\mathrm{x}33 & 0\mathrm{x}7E & 0\mathrm{x}E6 & 0\mathrm{x}04 & 0\mathrm{x}BC & 0\mathrm{x}2D & 0\mathrm{x}43 & 0\mathrm{x}2B & 0\mathrm{x}7E & 0\mathrm{x}AB & 0\mathrm{x}DF & 0\mathrm{x}58 & 0\mathrm{x}C7 \\
0\mathrm{x}C4 & 0\mathrm{x}BF & 0\mathrm{x}AF & 0\mathrm{x}1A & 0\mathrm{x}7A & 0\mathrm{x}DF & 0\mathrm{x}BD & 0\mathrm{x}FE & 0\mathrm{x}67 & 0\mathrm{x}5F & 0\mathrm{x}DB & 0\mathrm{x}3E & 0\mathrm{x}52 & 0\mathrm{x}A7 & 0\mathrm{x}DA & 0\mathrm{x}E6 \\
0\mathrm{x}C1 & 0\mathrm{x}18 & 0\mathrm{x}DE & 0\mathrm{x}5C & 0\mathrm{x}1B & 0\mathrm{x}26 & 0\mathrm{x}3D & 0\mathrm{x}C8 & 0\mathrm{x}10 & 0\mathrm{x}4D & 0\mathrm{x}C4 & 0\mathrm{x}D0 & 0\mathrm{x}0D & 0\mathrm{x}62 & 0\mathrm{x}91 & 0\mathrm{x}25 \\
0\mathrm{x}81 & 0\mathrm{x}D8 & 0\mathrm{x}77 & 0\mathrm{x}92 & 0\mathrm{x}12 & 0\mathrm{x}6A & 0\mathrm{x}92 & 0\mathrm{x}3A & 0\mathrm{x}8B & 0\mathrm{x}CF & 0\mathrm{x}AD & 0\mathrm{x}43 & 0\mathrm{x}C4 & 0\mathrm{x}FD & 0\mathrm{x}44 & 0\mathrm{x}BA \\
0\mathrm{x}DF & 0\mathrm{x}67 & 0\mathrm{x}52 & 0\mathrm{x}E2 & 0\mathrm{x}CB & 0\mathrm{x}CC & 0\mathrm{x}8E & 0\mathrm{x}EC & 0\mathrm{x}1E & 0\mathrm{x}EF & 0\mathrm{x}71 & 0\mathrm{x}DC & 0\mathrm{x}D7 & 0\mathrm{x}D1 & 0\mathrm{x}95 & 0\mathrm{x}A3 \\
0\mathrm{x}E4 & 0\mathrm{x}3C & 0\mathrm{x}88 & 0\mathrm{x}E7 & 0\mathrm{x}D2 & 0\mathrm{x}41 & 0\mathrm{x}01 & 0\mathrm{x}20 & 0\mathrm{x}3E & 0\mathrm{x}56 & 0\mathrm{x}11 & 0\mathrm{x}9B & 0\mathrm{x}09 & 0\mathrm{x}FD & 0\mathrm{x}D2 & 0\mathrm{x}C0 \\
0\mathrm{x}F7 & 0\mathrm{x}33 & 0\mathrm{x}8F & 0\mathrm{x}55 & 0\mathrm{x}79 & 0\mathrm{x}65 & 0\mathrm{x}27 & 0\mathrm{x}29 & 0\mathrm{x}48 & 0\mathrm{x}39 & 0\mathrm{x}96 & 0\mathrm{x}B9 & 0\mathrm{x}F6 & 0\mathrm{x}BF & 0\mathrm{x}A5 & 0\mathrm{x}BF \\
0\mathrm{x}AB & 0\mathrm{x}EF & 0\mathrm{x}A0 & 0\mathrm{x}9C & 0\mathrm{x}A7 & 0\mathrm{x}6A & 0\mathrm{x}F0 & 0\mathrm{x}44 & 0\mathrm{x}57 & 0\mathrm{x}63 & 0\mathrm{x}AF & 0\mathrm{x}0F & 0\mathrm{x}79 & 0\mathrm{x}6A & 0\mathrm{x}BA & 0\mathrm{x}3D \\
0\mathrm{x}66 & 0\mathrm{x}52 & 0\mathrm{x}58 & 0\mathrm{x}B5 & 0\mathrm{x}17 & 0\mathrm{x}1B & 0\mathrm{x}58 & 0\mathrm{x}BE & 0\mathrm{x}9C & 0\mathrm{x}BA & 0\mathrm{x}77 & 0\mathrm{x}D6 & 0\mathrm{x}30 & 0\mathrm{x}EA & 0\mathrm{x}A1 & 0\mathrm{x}CE \\
0\mathrm{x}C6 & 0\mathrm{x}9D & 0\mathrm{x}9C & 0\mathrm{x}D2 & 0\mathrm{x}89 & 0\mathrm{x}02 & 0\mathrm{x}5F & 0\mathrm{x}25 & 0\mathrm{x}90 & 0\mathrm{x}25 & 0\mathrm{x}34 & 0\mathrm{x}21 & 0\mathrm{x}D1 & 0\mathrm{x}E9 & 0\mathrm{x}2F & 0\mathrm{x}52 \\
0\mathrm{x}E9 & 0\mathrm{x}37 & 0\mathrm{x}B1 & 0\mathrm{x}F3 & 0\mathrm{x}88 & 0\mathrm{x}0F & 0\mathrm{x}5F & 0\mathrm{x}E7 & 0\mathrm{x}CA & 0\mathrm{x}0D & 0\mathrm{x}F9 & 0\mathrm{x}52 & 0\mathrm{x}9F & 0\mathrm{x}80 & 0\mathrm{x}F5 & 0\mathrm{x}24 \\
0\mathrm{x}13 & 0\mathrm{x}B4 & 0\mathrm{x}F3 & 0\mathrm{x}71 & 0\mathrm{x}0A & 0\mathrm{x}7C & 0\mathrm{x}13 & 0\mathrm{x}CC & 0\mathrm{x}C2 & 0\mathrm{x}04 & 0\mathrm{x}43 & 0\mathrm{x}D3 & 0\mathrm{x}C0 & 0\mathrm{x}AC & 0\mathrm{x}9B & 0\mathrm{x}2C \\
0\mathrm{x}BE & 0\mathrm{x}01 & 0\mathrm{x}7B & 0\mathrm{x}40 & 0\mathrm{x}54 & 0\mathrm{x}49 & 0\mathrm{x}73 & 0\mathrm{x}D9 & 0\mathrm{x}2E & 0\mathrm{x}47 & 0\mathrm{x}A5 & 0\mathrm{x}55 & 0\mathrm{x}3B & 0\mathrm{x}55 & 0\mathrm{x}F7 & 0\mathrm{x}32 \\
0\mathrm{x}5F & 0\mathrm{x}A6 & 0\mathrm{x}19 & 0\mathrm{x}03 & 0\mathrm{x}4D & 0\mathrm{x}3F & 0\mathrm{x}9E & 0\mathrm{x}E8 & 0\mathrm{x}9D & 0\mathrm{x}54 & 0\mathrm{x}C0 & 0\mathrm{x}B6 & 0\mathrm{x}62 & 0\mathrm{x}5C & 0\mathrm{x}E8 & 0\mathrm{x}8F
\end{pmatrix}.$$

Using the primitive polynomial $x^{11} + x^2 + 1$ a candidate for $N = 2^{11}$ and $w = 8$ is as follows:

$$\begin{pmatrix}
0\mathrm{x}078 & 0\mathrm{x}166 & 0\mathrm{x}14D & 0\mathrm{x}019 & 0\mathrm{x}1C8 & 0\mathrm{x}098 & 0\mathrm{x}187 & 0\mathrm{x}09C \\
0\mathrm{x}257 & 0\mathrm{x}436 & 0\mathrm{x}7F9 & 0\mathrm{x}644 & 0\mathrm{x}0F9 & 0\mathrm{x}370 & 0\mathrm{x}634 & 0\mathrm{x}260 \\
0\mathrm{x}777 & 0\mathrm{x}721 & 0\mathrm{x}309 & 0\mathrm{x}609 & 0\mathrm{x}158 & 0\mathrm{x}59B & 0\mathrm{x}353 & 0\mathrm{x}2C7 \\
0\mathrm{x}5FC & 0\mathrm{x}6D8 & 0\mathrm{x}63A & 0\mathrm{x}21A & 0\mathrm{x}78B & 0\mathrm{x}483 & 0\mathrm{x}252 & 0\mathrm{x}65F \\
0\mathrm{x}74C & 0\mathrm{x}4B3 & 0\mathrm{x}068 & 0\mathrm{x}1B5 & 0\mathrm{x}103 & 0\mathrm{x}273 & 0\mathrm{x}263 & 0\mathrm{x}330 \\
0\mathrm{x}568 & 0\mathrm{x}45F & 0\mathrm{x}401 & 0\mathrm{x}5EE & 0\mathrm{x}25B & 0\mathrm{x}541 & 0\mathrm{x}2D4 & 0\mathrm{x}517 \\
0\mathrm{x}60C & 0\mathrm{x}53B & 0\mathrm{x}7EB & 0\mathrm{x}30F & 0\mathrm{x}0B8 & 0\mathrm{x}52D & 0\mathrm{x}35C & 0\mathrm{x}11B \\
0\mathrm{x}67C & 0\mathrm{x}77C & 0\mathrm{x}388 & 0\mathrm{x}749 & 0\mathrm{x}216 & 0\mathrm{x}742 & 0\mathrm{x}52B & 0\mathrm{x}5BF
\end{pmatrix}.$$

We have also found plenty of candidates for other parameters, which are however omitted for the sake of space.

D.2 MDS in Prime Field

Rescue [3] is a symmetric cryptographic algorithm in the prime field. [3] offers to use $m \times 2m$ Vandermonde matrices using powers of an $\mathbb{F}_N$ primitive element. This matrix is then echelon reduced after which the $m \times m$ identity matrix is removed and the MDS matrix is obtained.

The field is $\mathbb{F}_N$ where $N = 2^{61} + 20 \cdot 2^{32} + 1$ and the state consists of $w = 12$ elements. We get an MDS matrix $T^{12\times 12}$ that satisfies Definition 1. Because the matrix is large, we give four submatrices of $T^{12\times 12}$ for convenience.

Remark 1. Our results also apply to some finite commutative rings if these rings exist MDS matrix. We assume that $\mathcal{R}$ is a finite commutative ring with identity and $\mathcal{U}(\mathcal{R})$ be the set of unit elements in $\mathcal{R}$. We note that a square matrix M over $\mathcal{R}$ is an MDS matrix if and only if the determinant of every submatrix of M is an element of $\mathcal{U}(\mathcal{R})$.

$$T_{\mathrm{EO}} = \begin{pmatrix} 2132424736362510249 & 272219690434835935 & 628384112905106413 & 1565489682189437819 & 102647751018558166 & 2301513477475405913 \\ 760420574997441750 & 2035848417468001220 & 367912208253241944 & 547812474641127246 & 1612644506155170807 & 1039051613644087538 \\ 132726795077680251 & 276049002402132600 & 2062106681853038294 & 1798462318189496829 & 876966686293506264 & 287934944924422359 \\ 1264644276986552669 & 959231254313894919 & 1609867535685450063 & 600131831529382266 & 1620659942407802180 & 1917517751863507751 \\ 445000516669406821 & 999425300126380635 & 1424386583549059837 & 1840785481461661844 & 770207555826068291 & 1321685401225718358 \\ 639836024986482499 & 891641509416426249 & 85684006979349218 & 2009314248255768979 & 1461785329408795871 & 614526427234661302 \end{pmatrix},$$

$$T_{\mathrm{EE}} = \begin{pmatrix} 15711484922630962 & 2227517040482465911 & 187890826715913914 & 855185158248966901 & 1240231461853961953 & 52955405230 \\ 1609903324587312789 & 2102895942828698062 & 549219385545962688 & 1695153738293598915 & 2060362812156761441 & 1759676667219874712 \\ 923095709968000189 & 959338751046899491 & 244453736105668101 & 1406898979258649653 & 275447637214934490 & 2285734233230770845 \\ 1265639319216678149 & 697991249395296203 & 1704131864879019365 & 1685146518137773283 & 1060851437983461874 & 1755088683392460390 \\ 2093205648133558759 & 329637479548419001 & 301428008445525907 & 1513566306301422264 & 670626981701496916 & 2125103307689520606 \\ 875144587036228576 & 365539559403463513 & 595494090920351320 & 396294882845853692 & 733908538741415240 & 554203175223363034 \end{pmatrix},$$

$$T_{\mathrm{OE}} = \begin{pmatrix} 1785767748384713920 & 1176202705900433241 & 2002100411542386973 & 391614261697275974 & 360795585898440 & 265720 \\ 1911206489025036282 & 2288800061181620774 & 2022538467220806570 & 1528973107985342496 & 1329417068351153619 & 9741692640081640 \\ 1017975231587935907 & 458455469860708540 & 1509611069489431703 & 1431382453218999763 & 1603062934957270225 & 1154395161414073365 \\ 967955863044139674 & 606678741800936612 & 2152312119329458712 & 1922914078805331422 & 224816859858735634 & 1905450060424727813 \\ 1604595880107521285 & 1868014205588480988 & 2136423194693683476 & 1163035584930921200 & 1169104133940285381 & 398952898784904682 \\ 2174389749072740614 & 1890638126825797984 & 1260330357606851540 & 1134389307747653122 & 1180187000329492200 & 1245356238080565962 \end{pmatrix},$$

$$T_{\mathrm{OO}} = \begin{pmatrix} 648467820989193486 & 229302989012133557 & 1573754073982867168 & 1506606314453584238 & 2215038371668159819 & 2305843077461326703 \\ 1694082666618257031 & 1779960530227737406 & 2076188670648949015 & 68601033256903557 & 1078330817078159304 & 353061061557231418 \\ 2305116735606702210 & 1364902896243084334 & 693700034972091385 & 2150732365748590380 & 2047024234454902938 & 404543078237488362 \\ 1393210217904044083 & 475897447857635565 & 1964414678958219561 & 1764783251126283713 & 170610800668462953 & 286014450900263497 \\ 1004420887426787826 & 2132518609943871819 & 1328965370622617212 & 2032385826938959001 & 111192163100705374 & 1191292909712540868 \\ 1956705709965072738 & 260751610632947425 & 2287279591594228857 & 1266747282502070711 & 835240421619663589 & 648886269814194370 \end{pmatrix}.$$