Des. Codes Cryptogr. (2014) 73:667–682
DOI 10.1007/s10623-014-9970-4

Towards the optimality of Feistel ciphers with substitution-permutation functions

Kyoji Shibutani · Andrey Bogdanov

Received: 1 September 2013 / Revised: 1 April 2014 / Accepted: 2 April 2014 /
Published online: 23 April 2014

Abstract We explore the optimality of balanced Feistel ciphers with SP-type F-functions with respect to their resistance against differential and linear cryptanalysis. Instantiations of Feistel ciphers with the wide class of $(\mathrm{SP})^u$ and $(\mathrm{SP})^u\mathrm{S}$ F-functions are considered: one F-function can contain an arbitrary number of S-box layers interleaved with linear diffusion. For the matrices with maximum diffusion, it is proven that SPS and SPSP F-functions are optimal in terms of the proportion of active S-boxes in all S-boxes—a common efficiency metric for substitution-permutation ciphers. Interestingly, one SP-layer in the F-function is not enough to attain optimality whereas taking more than two S-box layers does not increase the efficiency either.

Keywords Block cipher · Balanced Feistel networks · Differential cryptanalysis · Linear cryptanalysis · Active S-boxes · MDS codes

Mathematics Subject Classification 94A60

1 Introduction

Balanced Feistel networks (BFNs) are one of the most widely used structures for a block cipher. In fact, BFNs are adopted in a large number of symmetric key primitives, e.g., the former U.S. encryption standard DES [13], the current Russian encryption standard GOST

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

K. Shibutani (✉)
Sony Corporation, 1-7-1 Konan, Minato-ku, Tokyo 108-0075, Japan
e-mail: Kyoji.Shibutani@jp.sony.com

A. Bogdanov
ESAT/SCD/COSIC, KU Leuven, Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
e-mail: andrey.bogdanov@esat.kuleuben.be

blockcipher [20], and KASUMI which is the core of A5/3 cryptosystem in mobile networks [30]. Besides, a considerable number of analytic papers for the structure of the BFNs and the specific instantiation of the BFNs have been published since it was developed in the 1970s. However, the optimal design strategy with respect to both the security and the efficiency for its F-function is still an open problem.

This article addresses this problem in a wide class of typical underlying functions for a BFN (substitution-permutation functions with any finite number of layers). To do that, for each of them, we first prove tight bounds on the security parameter (number of active S-boxes). Then the security parameter is related to the computational workload of a cipher implementation (modelled as the number of S-boxes computed in the cipher) to obtain an efficiency parameter. Finally, the optimal constructions are those with the maximum resulting efficiency parameter.

The class of ciphers We focus on *balanced Feistel networks with SP-type bijective F-functions*, that is, with underlying functions whose internal structure is a substitution-permutation network (SPN). An SPN consists of several sequential applications of an S-box layer (S)—several small nonlinear maps applied in parallel—and a diffusion layer (P)—multiplication by a matrix over a binary finite field. We treat F-functions with $(\mathrm{SP})^{2t}$, $(\mathrm{SP})^{2t+1}$, $(\mathrm{SP})^{2t-1}\mathrm{S}$ and $(\mathrm{SP})^{2t}\mathrm{S}$-type F-functions for integer $t \geq 1$. For instance, an $(\mathrm{SP})^2\mathrm{S}$-type F-function consists of two consecutive SP-functions followed by an S-box layer, namely an SPSPS F-function. The instantiation of a Feistel network with an SP-type F-function is deployed in many cryptographic algorithms including E2 [16], TWOFISH [22], CAMELLIA [2], CLEFIA [28], SHAvite-3 [4], and PICCOLO [23].

Security parameter Counting the *minimum number of active S-boxes* is a widely accepted argument [12] to demonstrate the immunity of a cryptographic algorithm against differential [5] and linear [18] cryptanalysis which are two fundamental attacks on block ciphers. Lower bounds on the number of active S-boxes are closely related to the probability of differential trails and linear trails [12].

For each of the BFN instantiations above, we prove lower bounds on the number of differentially and linearly active S-boxes. In contrast to the previous works [6,15], our results with respect to this security parameter:

- generalize the type of the F-function, while [6,15] only contain lower bounds for BFNs with SP- and SPS- functions,
- hold for any number of rounds (those of [6,15] hold only for a few rounds), and
- contain proofs of tightness for the bounds when the matrices used in the diffusion layers of BFNs are maximum distance separable (MDS).

Efficiency metric To measure the efficiency of a construction, we are using the *ratio between active S-boxes and all S-boxes* in a cipher—a reasonable efficiency metric introduced in [25] and extensively used in [6–9]. It is based on the assumption that most workload one has to perform in the implementation of an SP-type construction is the computation of the S-boxes. Since we are mainly interested in MDS matrices that are equal in all rounds and intend to compare block ciphers of the same block length only, we will ignore the cost of the linear operations for the purposes of comparison. Note that this efficiency metric cannot capture all implementation possibilities and constraints in the field.

Optimality In the wide class of our target ciphers, we prove optimality of several instances with respect to the efficiency parameter. More specifically, among BFN block ciphers with bijective SP-type F-functions and MDS diffusion, we prove *BFNs with SPS and SPSP functions to maximize the efficiency* in terms of the proportion of active S-boxes in all S-boxes.

Interestingly, one SP-layer in the function is not enough to attain optimality, whereas taking more than two S-box layers does not increase the efficiency either.

Organization of the article The remainder of this article is organized as follows. Section 2 describes the target structure and definitions. The duality of differential and linear trails is explained in Sect. 3. Section 4 gives proofs for lower bounds on the numbers of differentially and linearly active S-boxes for the BFNs and its results are summarized in Table 1. Section 5 shows the tightness of those bounds. Section 6 discusses the optimality of the BFNs. Finally, we conclude in Sect. 7.

2 Preliminaries

2.1 Target structures

In this paper, we focus on balanced Feistel networks (BFNs) with bijective F-functions. A $2mn$-bit plaintext $\mathcal{P}$ is divided into two subblocks as $\mathcal{P} = (X_L^{(1)}, X_U^{(1)})$, where $X_L^{(i)}, X_U^{(i)} \in \{0,1\}^{mn}$. Then the i-th round output is calculated as follows:

$$\left(X_L^{(i+1)}, X_U^{(i+1)}\right) \leftarrow \left(F(X_L^{(i)}) \oplus X_U^{(i)}, X_L^{(i)}\right),$$

where $F : \{0,1\}^{mn} \rightarrow \{0,1\}^{mn}$ is an F-function in the i-th round. A $2mn$-bit ciphertext $\mathcal{C}$ for the r-round encryption function is derived as $\mathcal{C} = (X_U^{(r+1)}, X_L^{(r+1)})$, i.e., the last exchange is omitted. Each F-function consists of some S-box layers and linear diffusion layers (P-layers), and all S-box layers and P-layers are bijective. While mn-bit subkeys are XORed before each S-box layer, we omit these subkey additions in this paper for simplicity. An S-box layer consists of m n-bit bijective S-boxes, and a linear diffusion layer consists of mn-bit linear Boolean function. BFN-(SP)^u denotes BFN with F-functions consisting of u consecutive SP-functions. BFN-(SP)^{u}S denotes BFN with F-functions consisting of u consecutive SP-functions followed by one additional S-box layer. See Figs. 1 and 2.

2.2 Differential and linear cryptanalyses

Differential cryptanalysis was published in 1990 by Biham and Shamir [5] with applications to DES. However, it has been known to the designers of DES at IBM in early 1970s [11]. As the name suggests, the main idea of differential cryptanalysis is to exploit correlations between differences in the inputs and outputs of a block cipher to recover the key. It is a chosen-plaintext attack, in which an attacker is allowed to choose arbitrary plaintexts and obtain the corresponding ciphertexts.

Linear cryptanalysis as applied to DES was proposed by Matsui in 1993 [18]. However, similar ideas were published by Shamir [21] in 1985 as well as Tardy-Corfdir and Gilbert [29] in 1991. Linear cryptanalysis uses linear approximations of block ciphers to perform

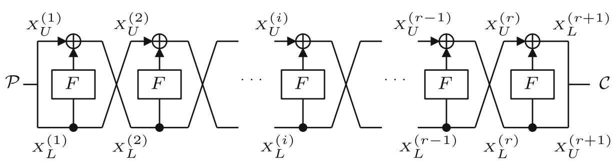

Fig. 1 r-round BFN with bijective F-functions

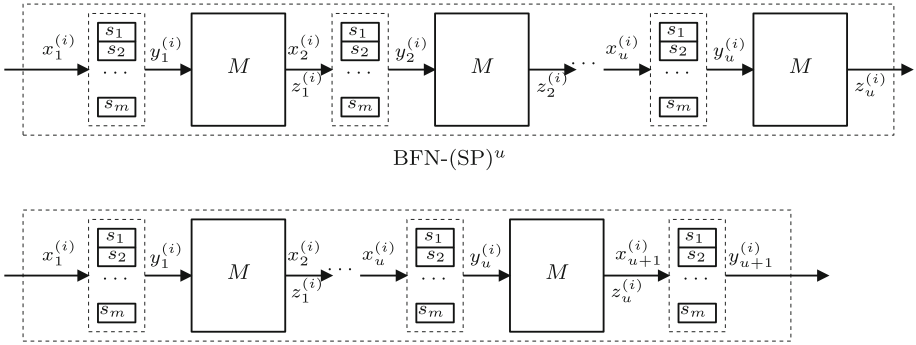

Fig. 2 The i-th round F-function of BFN-(SP)^u and BFN-(SP)^{u}S

key recovery. It is a known-plaintext attack, in which an attacker knows some plaintexts and the corresponding ciphertexts.

For an n-bit function $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$, a differential probability used in differential cryptanalysis and a linear probability used in linear cryptanalysis are defined as follows, respectively.

Definition 1 (*Differential probability*) Given an input difference Δx and an output difference Δy, a differential probability of f is defined as follows:

$$DP_f(\Delta x, \Delta y) = \Pr_{x \in \{0,1\}^n}(f(x) \oplus f(x \oplus \Delta x) = \Delta y),$$

where $x, \Delta x, \Delta y \in \{0, 1\}^n$.

Definition 2 (*Linear probability*) Given an input linear mask value Γx and an output linear mask value Γy, a linear probability of f is defined as follows:

$$LP_f(\Gamma x, \Gamma y) = \left(2 \cdot \Pr_{x \in \{0,1\}^n}\left(x \bullet \Gamma x = f(x) \bullet \Gamma y\right) - 1\right)^2,$$

where $\bullet$ denotes dot products and $x, \Gamma x, \Gamma y \in \{0, 1\}^n$.

2.3 Notations

We give the standard definitions of bundle weight and branch number followed by more specific notations [12].

Definition 3 (*Bundle Weight*) Let $x \in \{0, 1\}^{mn}$ be represented as $x = (x_1, x_2, \ldots, x_m)$, where $x_i \in \{0, 1\}^n$, then the n-bit bundle weight $w_n(x)$ is defined as

$$w_n(x) = \sharp\{i | 1 \leq i \leq m, x_i \neq 0\}. \tag{1}$$

Definition 4 (*Branch Number*) Let $M : \{0, 1\}^{mn} \rightarrow \{0, 1\}^{mn}$. The branch number of M is defined as

$$\mathcal{B}(M) = \min_{a \neq 0}\{w_n(a) + w_n(M(a))\}. \tag{2}$$

Besides the bundle weight w_n and branch number $\mathcal{B}$, throughout this paper, we use the following notations:

- $x_j^{(i)}$, $y_j^{(i)}$: input and output of the j-th S-box layer in the i-th round.
- $z_j^{(i)}$: output of the j-th linear diffusion layer in the i-th round.
- $\Delta x_j^{(i)}$: a difference of $x_j^{(i)}$.
- $d_j^{(i)}$: a truncated difference weight of $x_j^{(i)}$, i.e., $d_j^{(i)} = w_n(\Delta x_j^{(i)})$.
- $d^{(i)}$: the number of differentially active S-boxes in the i-th round.
- $\mathcal{D}(r)$: the minimum number of active S-boxes in r consecutive rounds.
- $\Gamma y_j^{(i)}$: a linear mask value of $y_j^{(i)}$.

2.4 Efficiency metric

The proportion of active S-boxes in all S-boxes is a reasonable efficiency metric with respect to differential and linear cryptanalysis for ciphers based on substitution-permutation. It was introduced in [25] by Shirai and Preneel for BFNs and used in [6–9] for estimating and comparing the efficiency of diverse Feistel constructions, including BFNs.

Both the number of active S-boxes and the number of all S-boxes over several rounds of a BFN depend on the number r of rounds considered and the number m of S-boxes in one F-function.

Definition 5 (E_m *and* E) The efficiency metric E_m is defined as $E_m = \lim_{r\to\infty} A_{m,r}/S_{m,r}$, where $A_{m,r}$ is the minimum number of active S-boxes over r rounds and $S_{m,r}$ is the total number of S-box computations over r rounds. The efficiency metric E is defined as $E = \lim_{m\to\infty} E_m$, where the number of active S-boxes $A_{m,r}$ is measured when the underlying diffusion matrix is MDS, i.e., $\mathcal{B}(M) = m + 1$.

Note that this efficiency metric E_m cannot capture all implementation possibilities and constraints in the field, though it is believed to provide an indication of the efficiency of a block cipher towards the two fundamental types of cryptanalysis, see [6–9,25] for some extensions and discussions with respect to efficiency metrics.

3 Duality of trails

In this section, we demonstrate an equivalence between differential and linear trails for the BFNs. This equivalence follows from Biham's considerations in [3] and is provided here for completeness. It allows us to work with the minimum numbers of differentially and linearly active S-boxes simultaneously. We first show an equivalent transform for BFN-(SP)^u.

Property 1 Suppose that both S-box layer and linear diffusion layer are bijective. Any BFN consisting of u consecutive SP-functions, BFN-(SP)^u, can be equivalently transformed into a BFN consisting of u consecutive PS-functions with an initial and a final linear function.

This property is seen as a generalization of [15]. Let $v_j^{(i)} = P^{-1}(x_j^{(i)})$. From the definition, $P(y_u^{(i)}) = x_1^{(i-1)} \oplus x_1^{(i+1)}$, then $y_u^{(i)} = P^{-1}(x_1^{(i-1)} \oplus x_1^{(i+1)})$. Since P is linear, $y_u^{(i)} = v_1^{(i-1)} \oplus v_1^{(i+1)}$. Meanwhile, $y_u^{(i)} = S(P(S(\cdots P(S(x_1^{(i)}))\cdots)))$, then $y_u^{(i)} = S(P(S(\cdots P(S(P(v_1^{(i)})))\cdots)))$. Combining the above equations, $v_1^{(i+1)} = S(P(S(\cdots P(S(P(v_1^{(i)})))\cdots))) \oplus v_1^{(i-1)}$. Now we have BFN-(PS)^u from BFN-(SP)^u by using equivalent transforms.

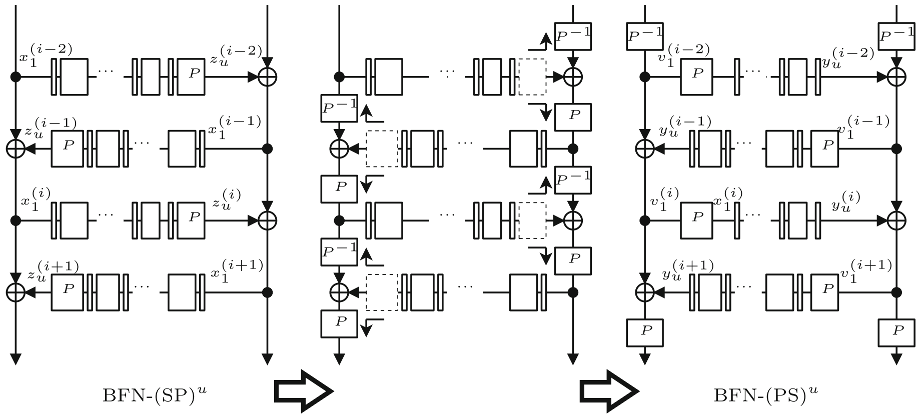

Fig. 3 Equivalent transform (BFN-(SP)^u to BFN-(PS)^u), where *thin boxes* and *thick boxes* denote S-box layers and P-layers, respectively

Note that BFN-(PS)^u takes $\mathcal{P}' = (P^{-1}(X_L^{(1)}), P^{-1}(X_U^{(1)}))$ as a plaintext and outputs a ciphertext $\mathcal{C}' = (P(X_U^{(r+1)}), P(X_L^{(r+1)}))$. Since these initial and final linear functions do not affect the minimum numbers of active S-boxes, we can ignore these functions when studying the minimum numbers of active S-boxes. An illustration of these equivalent transforms is given in Fig. 3.

From the concatenation rules [3,19], $\Gamma v_1^{(i)} = \Gamma y_u^{(i-1)} \oplus \Gamma y_u^{(i+1)} =^t P(\Gamma x_1^{(i)})$, where ${}^tP$ is the bit-based transpose matrix of P. Thus, for BFN-(SP)^u, the linear trails can be transformed to the corresponding differential trails by replacing $(\Delta x_1^{(i)}, \Delta x_2^{(i)}, \ldots, \Delta x_u^{(i)})$, $(\Delta z_1^{(i)}, \Delta z_2^{(i)}, \ldots, \Delta z_u^{(i)})$ and P with $(\Gamma y_u^{(i)}, \Gamma y_{u-1}^{(i)}, \ldots, \Gamma y_1^{(i)})$, $(\Gamma v_u^{(i)}, \Gamma v_{u-1}^{(i)}, \ldots, \Gamma v_1^{(i)})$ and ${}^tP$, respectively. Similarly, for BFN-(SP)^{u}S, the linear trails can be treated as the differential trails by replacing $(\Delta x_1^{(i)}, \Delta x_2^{(i)}, \ldots, \Delta x_{u+1}^{(i)})$, $(\Delta y_1^{(i)}, \Delta y_2^{(i)}, \ldots, \Delta y_{u+1}^{(i)})$ and P by $(\Gamma y_{u+1}^{(i)}, \Gamma y_u^{(i)}, \ldots, \Gamma y_1^{(i)})$, $(\Gamma x_{u+1}^{(i)}, \Gamma x_u^{(i)}, \ldots, \Gamma x_1^{(i)})$ and ${}^tP$, respectively. Therefore, since the constraints for differential and linear trails for the BFNs are the same, the minimum numbers of differentially and linearly active S-boxes can be derived simultaneously. The above discussions yield the following theorem.

Theorem 1 *For BFN-(SP)^u and BFN-(SP)^{u}S, assuming that both S-box layer and linear diffusion layer are bijective, the lower bounds on the number of differentially active S-boxes derived from the property of the linear diffusion layer hold also for the number of linearly active S-boxes by changing the linear diffusion layer to the transposed one.*

In the sequel, we only discuss the minimum numbers of differentially active S-boxes for simplicity, keeping in mind, however, that the minimum numbers of linearly active S-boxes can be derived in the same way.

4 Bounds for active functions

In this section, we give proofs for lower bounds on the minimum number of differentially active S-boxes for BFN-(SP)$^{2t+1}$, -(SP)^{2t}, -(SP)$^{2t-1}$S and -(SP)^{2t}S. These results are summarized in Table 1.

Table 1 Summary of our results, where $\mathcal{B}$ is the branch number of the diffusion matrix or its transpose, $E_m = \lim_{r\to\infty} A_{m,r}/S_{m,r}$, and $E = \lim_{m\to\infty} E_m$

Structure of F	$(\mathrm{SP})^{2t}$	$(\mathrm{SP})^{2t-1}\mathrm{S}$	$(\mathrm{SP})^{2t+1}$, $t=0$
Proven tight bounds (min. # of active S-boxes/# of rounds)	$2t\mathcal{B}R/3R$ $2t\mathcal{B}R/(3R+1)$ $(2t\mathcal{B}R + t\mathcal{B})/(3R+2)$ $(Th.4)$, $(Th.5)$		$((\mathcal{B}+1)R-1)/4R$ $(\mathcal{B}+1)R/(4R+1)$ $((\mathcal{B}+1)R+1)/(4R+2)$ $((\mathcal{B}+1)R+2)/(4R+3)$ $(Th.2)$
# of S-boxes in 1-round	$2mt$	$2mt$	m
E_m	$2t\mathcal{B}/6mt$		$(\mathcal{B}+1)/4m$
E ($\mathcal{B}=m+1$)	1/3		1/4

Structure of F	$(\mathrm{SP})^{2t+1}$, $t>0$	$(\mathrm{SP})^{2t}\mathrm{S}$
Proven tight bounds (min. # of active S-boxes/# of rounds)	$((2t+1)\mathcal{B}R - \mathcal{B} + 2)/3R$ $(2t+1)\mathcal{B}R/(3R+1)$ $((2t+1)\mathcal{B}R + t\mathcal{B} + 1)/(3R+2)$ $(Th.3)$	$2(t\mathcal{B}+1)R/3R$ $2(t\mathcal{B}+1)R/(3R+1)$ $(2(t\mathcal{B}+1)R + t\mathcal{B} + 1)/(3R+2)$ $(Th.6)$
# of S-boxes in 1-round	$(2t+1)m$	$(2t+1)m$
E_m	$(2t+1)\mathcal{B}/3(2t+1)m$	$2(t\mathcal{B}+1)/3(2t+1)m$
E ($\mathcal{B}=m+1$)	$2t/3(2t+1)$	$2t/3(2t+1)$

To prove those bounds, we utilize the following property and lemmata for BFNs consisting of bijective F-functions.

Property 2 For each nonzero input difference, any two and three consecutive rounds of BFN consisting of bijective F-functions have at least one and two active functions, respectively.

Proof If two consecutive F-functions of the i-th and $(i+1)$-th rounds are both non-active, i.e., $\Delta X_L^{(i)}$ and $\Delta X_L^{(i+1)}$ are zero, the input difference $\Delta X_L^{(i)}$ and $\Delta X_U^{(i)} (= \Delta X_L^{(i+1)}$, since the output difference of the i-th round F-function is zero) are zero. Since this contradicts the assumption, at least one of two F-functions is active. From this, each of two consecutive rounds starting from the $(i-1)$-th round and the i-th round has at least one active F-function, which is an F-function whose input difference is nonzero. Obviously, if the i-th round F-function is non-active, three consecutive rounds starting from the $(i-1)$-th round have at least two active F-functions. If the i-th round F-function is active, $\Delta X_L^{(i-1)} (= \Delta X_U^{(i)})$ and $\Delta X_L^{(i+1)}$ cannot be zero simultaneously since the output difference of the i-th round F-function is nonzero. Therefore, there exist at least two active F-functions in three consecutive rounds. □

Meanwhile, the numbers of differentially active S-boxes for each differentially active F-function, which is an F-function whose input difference is nonzero, are lower-bounded by the following lemmata. Recall that $\mathcal{B}$ denotes the branch number of the linear layer.

Lemma 1 (active S-boxes for 1-round BFN-$(\mathrm{SP})^u$) *For BFN-*$(\mathrm{SP})^u$*, if* $d^{(i)}$ *is not zero,* $d^{(i)} \geq \lfloor u/2 \rfloor \mathcal{B} + (u \mod 2)$.

Proof If an input difference of two consecutive SP-functions is not zero, there exist at least $\mathcal{B}$ active S-boxes, e.g., $d_1^{(i)} + d_2^{(i)} \geq \mathcal{B}$. Since BFN-$(\mathrm{SP})^u$ has $\lfloor u/2 \rfloor$ independent two consecutive SP-functions and $(u \mod 2)$ SP-functions, it has at least $\lfloor u/2 \rfloor \mathcal{B} + (u \mod 2)$ active S-boxes when the input difference is not zero. □

Similarly to Lemma 1, one derives the following lemma.

Lemma 2 (active S-boxes for 1-round BFN-(SP)^{u}S) *For BFN-(SP)^{u}S, if $d^{(i)}$ is not zero, $d^{(i)} \geq \lceil u/2 \rceil \mathcal{B} + ((u+1) \mod 2)$.*

These lemmata show that the number of active S-boxes can be derived from the number of S-box layers when we treat only one active F-function. However, when we consider some consecutive rounds, the number of active S-boxes does not depend only on the number of S-box layers.

Starting from here, we treat four cases of the F-function construction separately: (SP)$^{2t+1}$, (SP)^{2t}, (SP)$^{2t-1}$S, and (SP)^{2t}S, as those exhibit essential differences.

4.1 Differentially active S-boxes in BFN-(SP)$^{2t+1}$

For BFN-(SP)$^{2t+1}$, which consists of odd number of SP-layers, the proofs for the lower bounds are the most complicated among other BFNs, since the number of differentially active S-boxes cannot be directly obtained from the number of differentially active F-functions. We find tight lower bounds on the minimum number of differentially active S-boxes by carefully observing two cases separately: $t = 0$ and other cases.

For BFN-(SP)$^{2t+1}$, Lemma 1 directly translates to the following corollary.

Corollary 1 *For BFN-(SP)$^{2t+1}$, if $d^{(i)}$ is not zero, $d^{(i)} \geq t\mathcal{B} + 1$.*

Property 2 and Corollary 1 directly show that any three consecutive rounds of BFN-(SP)$^{2t+1}$ have at least $2(t\mathcal{B}+1)$ active S-boxes. However, when the center of the F-function in the three consecutive rounds is active, there exist more active S-boxes as follows.

Lemma 3 *For BFN-(SP)$^{2t+1}$, if $d^{(i)}$ is not zero, $d^{(i-1)} + d^{(i)} + d^{(i+1)} \geq (2t+1)\mathcal{B}$.*

Proof From the definition, $\Delta x_1^{(i-1)} \oplus \Delta x_1^{(i+1)} = M(\Delta y_{2t+1}^{(i)})$. If $d^{(i)}$ is not zero, then $\Delta y_{2t+1}^{(i)}$ is not zero due to the invertibility. Since $\Delta y_{2t+1}^{(i)}$ is not zero, $w_n(\Delta x_1^{(i-1)}) + w_n(\Delta x_1^{(i+1)}) + w_n(\Delta y_{2t+1}^{(i)}) \geq \mathcal{B}$, i.e., $d_1^{(i-1)} + d_{2t+1}^{(i)} + d_1^{(i+1)} \geq \mathcal{B}$. Also, if $\Delta y_{2t+1}^{(i)}$ is not zero, $\Delta x_1^{(i-1)}$ and $\Delta x_1^{(i+1)}$ cannot be zero simultaneously. Thus $d_1^{(i-1)} + \cdots + d_{2t}^{(i-1)} \geq t\mathcal{B}$ or $d_1^{(i+1)} + \cdots + d_{2t}^{(i+1)} \geq t\mathcal{B}$. Therefore $\Sigma_{j=1}^{2t+1}(d_j^{(i-1)} + d_j^{(i)} + d_j^{(i+1)}) \geq (2t+1)\mathcal{B}$. □

The lower bounds on the minimum number of active S-boxes in any consecutive rounds of BFN-(SP)$^{2t+1}$ are directly derived by the lemmata above. First, we prove the bounds on $\mathcal{D}(r)$, $r \leq 4$ by Lemma 4, then show the bounds on $\mathcal{D}(r)$, $r > 4$ by Lemma 5.

Lemma 4 *For BFN-(SP)$^{2t+1}$, $\mathcal{D}(1) = 0$, $\mathcal{D}(2) = t\mathcal{B} + 1$, $\mathcal{D}(3) = 2(t\mathcal{B} + 1)$, and $\mathcal{D}(4) = (2t+1)\mathcal{B}$.*

Proof Since any two consecutive rounds have at least one active F-function, $\mathcal{D}(2) = t\mathcal{B} + 1$ from Corollary 1. We consider $d^{(i-1)}$, $d^{(i)}$ and $d^{(i+1)}$. If $d^{(i)}$ is not zero, then $d^{(i-1)} + d^{(i)} + d^{(i+1)} \geq (2t+1)\mathcal{B}$. If $d^{(i)}$ is zero, then both $d^{(i-1)}$ and $d^{(i+1)}$ are not zero from Property 2. In that case, $d^{(i-1)} + d^{(i)} + d^{(i+1)} \geq 2(t\mathcal{B}+1)$ from Corollary 1. Since $\mathcal{B} \geq 2$ from the invertibility and $(2t+1)\mathcal{B} \geq 2(t\mathcal{B}+1)$, we obtain $\mathcal{D}(3) = 2(t\mathcal{B}+1)$. We consider $d^{(i-1)}$, $d^{(i)}$, $d^{(i+1)}$ and $d^{(i+2)}$. If $d^{(i)}$ is not zero, $d^{(i-1)} + d^{(i)} + d^{(i+1)} \geq (2t+1)\mathcal{B}$ from Lemma 3. If $d^{(i)}$ is zero, then $d^{(i+1)}$ is not zero due to the invertibility. Then $d^{(i)} + d^{(i+1)} + d^{(i+2)} \geq (2t+1)\mathcal{B}$. Thus, $\mathcal{D}(4) = (2t+1)\mathcal{B}$. □

The bounds on $\mathcal{D}(r)$, $r > 4$, are given as inductive forms.

Lemma 5 *Let* $r > 4$, $\mathcal{D}(r) = \min(\mathcal{D}(r-3) + (2t+1)\mathcal{B}, \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1)$ *for BFN-(SP)*$^{2t+1}$.

Proof We consider active S-boxes in r consecutive rounds starting from round $i+1$, i.e., $d^{(i+1)}, \ldots, d^{(i+r)}$. If $d^{(i+r-1)}$ is not zero, then $d^{(i+r-2)} + d^{(i+r-1)} + d^{(i+r)} \geq (2t+1)\mathcal{B}$. Also, $d^{(i+1)} + \cdots + d^{(i+r-3)} \geq \mathcal{D}(r-3)$ from the definition. Therefore, $d^{(i+1)} + \cdots + d^{(i+r)} \geq \mathcal{D}(r-3) + (2t+1)\mathcal{B}$ when $d^{(i+r-1)}$ is not zero. If $d^{(i+r-1)}$ is zero, then both $d^{(i+r-2)}$ and $d^{(i+r)}$ are nonzero. $d^{(i+r-3)} + d^{(i+r-2)} + d^{(i+r-1)} \geq (2t+1)\mathcal{B}$ and $d^{(i+r)} \geq t\mathcal{B} + 1$ from Corollary 1. Also, $d^{(i+1)} + \cdots + d^{(i+r-4)} \geq \mathcal{D}(r-4)$. Therefore, $d^{(i+1)} + \cdots + d^{(i+r)} \geq \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1$ when $d^{(i+r-1)}$ is zero. Combining both results, we obtain $\mathcal{D}(r) = \min(\mathcal{D}(r-3) + (2t+1)\mathcal{B}, \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1)$ when $r > 4$. □

Now we have the lower bounds in any consecutive rounds of BFN-(SP)$^{2t+1}$. However, it is hard to compare its efficiency with other constructions, since the bounds are proven as inductive forms. In order to obtain more accurate bounds, we consider two cases. We start with the special case of $t = 0$.

Theorem 2 (active S-boxes for BFN-(SP)$^{2t+1}$, $t = 0$) *For any nonzero input difference (nonzero input mask), every* $4R$, $4R+1$, $4R+2$, $4R+3$ *rounds of BFN (*$R \geq 1$*) with an SP F-function provide at least* $(\mathcal{B}+1)R-1$, $(\mathcal{B}+1)R$, $(\mathcal{B}+1)R+1$, $(\mathcal{B}+1)R+2$ *differentially (linearly) active S-boxes, respectively, assuming* $\mathcal{B} > 2$, *where* $\mathcal{B}$ *is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

Proof If $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$, $\mathcal{D}(r) = \mathcal{D}(r-4) + \mathcal{B} + 1$ from Lemma 5. Otherwise $\mathcal{D}(r) = \mathcal{D}(r-3) + \mathcal{B}$. Clearly, $\mathcal{D}(r-3) - \mathcal{D}(r-4) = 1$ when $r = 5$ and 6, and $\mathcal{D}(r-3) - \mathcal{D}(r-4) = \mathcal{B} - 2$ when $r = 7$. Since $\mathcal{B} > 2$ from the assumption, $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$ when $r = 7$. Similarly, $\mathcal{D}(r-3) - \mathcal{D}(r-4) = \mathcal{D}(4) - \mathcal{D}(5) = (\mathcal{B}) - (\mathcal{B}+1) = 1$ when $r = 8$. Since $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$ for $r = 5, 6, 7$ and 8, $\mathcal{D}(r-3) - \mathcal{D}(r-4) \geq 1$ when $r \geq 5$. Thus $\mathcal{D}(r) = \mathcal{D}(r-4) + \mathcal{B} + 1$ when $r \geq 5$. Then $\mathcal{D}(r) = \mathcal{D}(r-4) + \mathcal{B} + 1 = \mathcal{D}(r-8) + 2(\mathcal{B}+1) = \cdots = \mathcal{D}(r-4u) + (\mathcal{B}+1)u$. Therefore $\mathcal{D}(4R+1) = \mathcal{D}(4R-3) + \mathcal{B} + 1 = \mathcal{D}(4R-7) + 2(\mathcal{B}+1) = \cdots = \mathcal{D}(1) + (\mathcal{B}+1)R = (\mathcal{B}+1)R$. Similarly, $\mathcal{D}(4R+2) = \mathcal{D}(2) + (\mathcal{B}+1)R = (\mathcal{B}+1)R+1, \mathcal{D}(4R+3) = \mathcal{D}(3) + (\mathcal{B}+1)R = (\mathcal{B}+1)R+2$, $\mathcal{D}(4R) = \mathcal{D}(4) + (R-1)(\mathcal{B}+1) = (\mathcal{B}+1)R - 1$. □

Note that Theorem 2 was conjectured in [24]. For all other integers $t > 0$, the bounds are stated as follows.

Theorem 3 (active S-boxes for BFN-(SP)$^{2t+1}$, $t > 0$) *For any nonzero input difference (nonzero input mask), every* $3R$, $3R+1$, $3R+2$ *rounds of BFN (*$R \geq 1$*) with* $(2t+1)$ *consecutive SP-layers in the F-function (*$t > 0$*) provide at least* $(2t+1)\mathcal{B}R - \mathcal{B} + 2$, $(2t+1)\mathcal{B}R$, $(2t+1)\mathcal{B}R + t\mathcal{B} + 1$ *differentially (linearly) active S-boxes, respectively, where* $\mathcal{B}$ *is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

Proof If $\mathcal{D}(r-3) - \mathcal{D}(r-4) \leq t\mathcal{B} + 1$, $\mathcal{D}(r) = \mathcal{D}(r-3) + (2t+1)\mathcal{B}$ from Lemma 5. Otherwise $\mathcal{D}(r) = \mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1$. From Lemma 4, $\mathcal{D}(r-3) - \mathcal{D}(r-4) = t\mathcal{B} + 1$ when $r = 5$ and 6, and $\mathcal{D}(r-3) - \mathcal{D}(r-4) = \mathcal{B} - 2$ when $r = 7$. Since $t > 0$, $\mathcal{B} - 2 < t\mathcal{B} + 1$. Thus $\mathcal{D}(r) = \mathcal{D}(r-3) + (2t+1)\mathcal{B}$ when $r \geq 5$. Then $\mathcal{D}(r) = \mathcal{D}(r-3) + (2t+1)\mathcal{B} = \mathcal{D}(r-6) + 2(2t+1)\mathcal{B} = \cdots = \mathcal{D}(r-3u) + (2t+1)\mathcal{B}u$. Therefore $\mathcal{D}(3R+1) = \mathcal{D}(3R-2) + (2t+1)\mathcal{B} = \cdots = \mathcal{D}(1) + (2t+1)\mathcal{B}R = (2t+1)\mathcal{B}R$. Similarly, $\mathcal{D}(3R+2) = \mathcal{D}(2) + (2t+1)\mathcal{B}R = (2t+1)\mathcal{B}R + t\mathcal{B} + 1, \mathcal{D}(3R) = \mathcal{D}(3) + (2t+1)(R-1)\mathcal{B} = (2t+1)\mathcal{B}R - \mathcal{B} + 2$. □

Now we have comparable bounds for every four rounds of BFN-(SP)$^{2t+1}$. For the case of $t > 0$, $(\mathcal{D}(r-3) + (2t+1)\mathcal{B})$ is always less than or equal to $(\mathcal{D}(r-4) + (3t+1)\mathcal{B} + 1)$. On the other hands, for the case of $t = 0$, $(\mathcal{D}(r-4) + \mathcal{B} + 1)$ is less than or equal to $(\mathcal{D}(r-3) + \mathcal{B})$ when $\mathcal{B} > 2$ and $r = 4s + 3 (s > 0)$ (e.g., $r = 7, 11, 15, \ldots$). Thus, the bounds for the case $t = 0$ and $t > 0$ are slightly different and those are separately proven. The tightness of these bounds is proven in Sect. 5.

4.2 Differentially active S-boxes in BFN-(SP)^{2t}

For BFN-(SP)^{2t}, which comprises even number of SP-layers, the minimum number of differentially active S-boxes is straightforwardly proven by observing the number of differentially active F-functions.

Lemma 1 yields the following corollary.

Corollary 2 *For BFN-(SP)^{2t}, if $d^{(i)}$ is not zero, $d^{(i)} \geq t\mathcal{B}$.*

This corollary allows us to prove the following theorem.

Theorem 4 (active S-boxes for BFN-(SP)^{2t}) *For any nonzero input difference (nonzero input mask), every $3R$, $3R+1$, $3R+2$ rounds of BFN ($R \geq 1$) with $2t$ consecutive SP layers in the F-function provide at least $2t\mathcal{B}R$, $2t\mathcal{B}R$, $2t\mathcal{B}R + t\mathcal{B}$ differentially (linearly) active S-boxes, respectively, where $\mathcal{B}$ is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

Proof We consider $d^{(i-1)}$, $d^{(i)}$ and $d^{(i+1)}$. If $d^{(i)}$ is zero, then both $d^{(i-1)}$ and $d^{(i+1)}$ are not zero due to the invertibility. Thus there exist at least $2t\mathcal{B}$ active S-boxes from Corollary 2. If $d^{(i)}$ is not zero, then $d^{(i-1)}$ and $d^{(i+1)}$ cannot be zero simultaneously. Therefore there exist at least $2t\mathcal{B}$ active S-boxes from Corollary 2. Since two consecutive rounds have at least $t\mathcal{B}$ active S-boxes, $3R + 2$ consecutive rounds have at least $2t\mathcal{B}R + t\mathcal{B}$ active S-boxes. □

Unlike the case of BFN-(SP)$^{2t+1}$, the lower bounds for BFN-(SP)^{2t} are easily proven. In the other words, the minimum number of differentially active S-boxes for BFN-(SP)^{2t} corresponds to the minimum number of differential active F-functions times $t\mathcal{B}$.

4.3 Differentially active S-boxes in BFN-(SP)$^{2t-1}$S

Since the number of S-box layers is the same in BFN-(SP)$^{2t-1}$S, similarly to the bounds for BFN-(SP)^{2t}, one derives the following theorem.

Theorem 5 (active S-boxes for BFN-(SP)$^{2t-1}$S) *For any nonzero input difference (nonzero input mask), every $3R$, $3R+1$, $3R+2$ rounds of BFN ($R \geq 1$) with $(2t-1)$ consecutive SP-layers followed by an S-box layer in the F-function provide at least $2t\mathcal{B}R$, $2t\mathcal{B}R$, $2t\mathcal{B}R + t\mathcal{B}$ differentially (linearly) active S-boxes, where $\mathcal{B}$ is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

The obtained bounds for BFN-(SP)^{2t}S seem almost same as the bounds for BFN-(SP)^{2t}. However, BFN-(SP)^{2t} has one more P-layer than BFN-(SP)$^{2t-1}$S has when the parameter t is the same. This implies that the last P-layer of BFN-(SP)^{2t} does not improve the security in terms of the number of differentially active S-boxes.

4.4 Differentially active S-boxes in BFN-(SP)^{2t}S

Similarly to BFN-(SP)$^{2t+1}$, BFN-(SP)^{2t}S has odd number of S-layers. However, lack of the last P-layer allows us to prove the bounds for BFN-(SP)^{2t}S easily.

Property 2 and Lemma 2 yield the following theorem.

Theorem 6 (active S-boxes for BFN-(SP)^{2t}S) *For any nonzero input difference (nonzero input mask), every* $3R$, $3R+1$, $3R+2$ *rounds of BFN* ($R \geq 1$) *with* $2t$ *consecutive SP-layers followed by an S-box layer in the F-function provide at least* $2(t\mathcal{B}+1)R$, $2(t\mathcal{B}+1)R$, $(2(t\mathcal{B}+1)R+(t\mathcal{B}+1))$ *differentially (linearly) active S-boxes, where* $\mathcal{B}$ *is the branch number of the diffusion matrix (of the transposed diffusion matrix).*

The proof for BFN-(SP)^{2t}S is similar to the proofs for BFN-(SP)^{2t} and BFN-(SP)$^{2t-1}$S. In other words, for BFN-(SP)^{2t}S, the minimum number of active S-boxes can be proven by studying the number of active F-functions. However, the proven bounds are not same as the bounds for BFN-(SP)^{2t} and BFN-(SP)$^{2t-1}$S, since the number of S-layers is different. In the following sections, we discuss tightness of the bounds proven in this section and their optimality.

5 Tightness of bounds

To demonstrate the tightness of the lower bounds, we provide trails that actually attain those proven bounds when the matrices used in the BFNs are MDS. These trails are given in Figs. 4, 5, 6 and 7 for all the BFN constructions in question. Note that a similar observation for BFN-SP with $m = 8$ was given in Appendix A of [26].

In the figures, Δ and ∇ denote S-box truncated difference 100 . . . 00 (only the first S-box active out of m) and 111 . . . 11 (all m S-boxes active), respectively. Thin boxes and thick

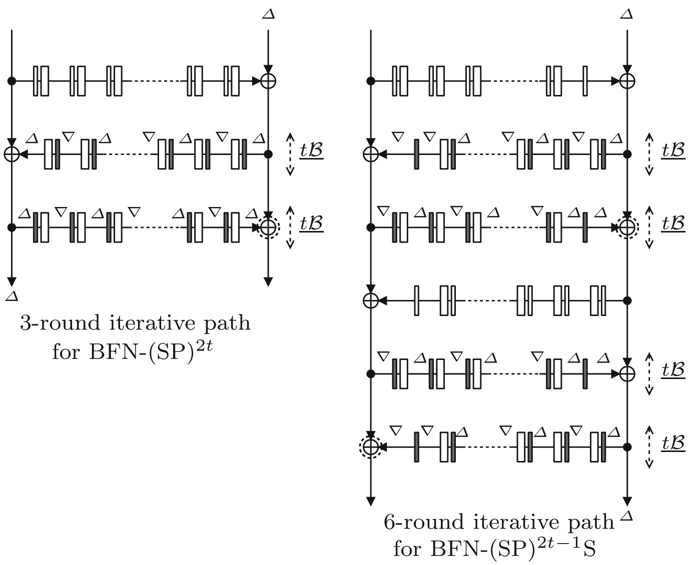

Fig. 4 Truncated differential trails of BFN-(SP)^{2t} (*left* 3-round iterative trail) and BFN-(SP)$^{2t-1}$S (*right* 6-round iterative trail) attaining the lower bounds of Theorems 4 and 5

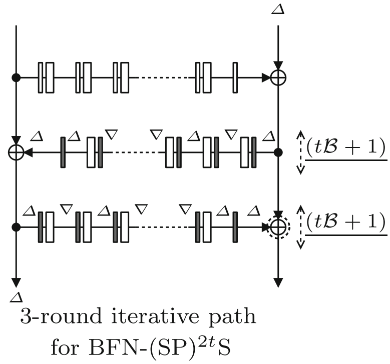

Fig. 5 Truncated differential trails of BFN-(SP)^{2t}S (3-round iterative trail) attaining the lower bounds of Theorem 6

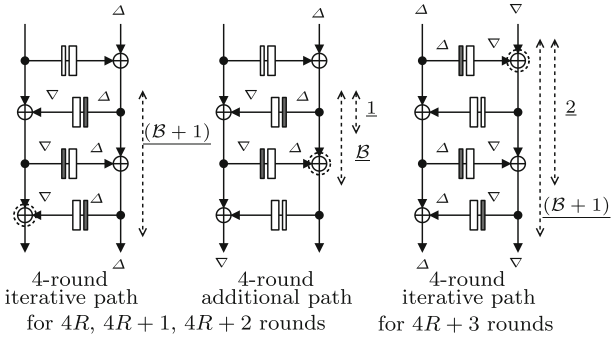

Fig. 6 Truncated differential trails of BFN-SP attaining the lower bounds of Theorem 2

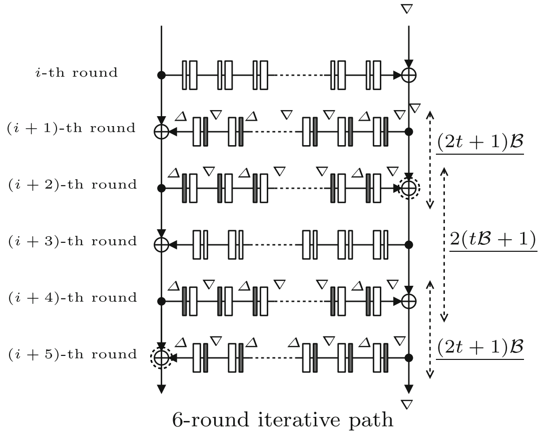

Fig. 7 Truncated differential trails of BFN-(SP)$^{2t+1}$, $t > 0$ (6-round iterative trail) attaining the lower bounds of Theorem 3

boxes denote S-box layers (S-layers) and linear layers (P-layers), respectively. XORs with difference cancellation are marked with dashed circles. Differentially active S-box layers are denoted by grey. The underlined numbers denote the minimum numbers of active S-boxes in the area indicated by a dashed line.

From the discussions in Sect. 3, the following observations are directly applicable to the case of the linear cryptanalysis.

5.1 BFN-$(SP)^{2t}$

The left side of Fig. 4 shows a 3-round iterative path that maps $(0, \Delta)$ to $(0, \Delta)$ for BFN-$(SP)^{2t}$. In other words, the i-th round input difference $(\Delta X_L^{(i)}, \Delta X_U^{(i)}) = (0, \Delta)$ and the $(i+3)$-th round input difference $(\Delta X_L^{(i+3)}, \Delta X_U^{(i+3)}) = (0, \Delta)$. Note that, since we use an untwisted form in Fig. 4, an output difference looks reverse in the case of odd number of rounds. The numbers of active S-boxes provided by this figure correspond to the bounds proven in Theorem 4. For instance, the numbers of active S-boxes for 3, 4, 5 and 6 rounds given by the figure are $2t\mathcal{B}$, $2t\mathcal{B}$, $3t\mathcal{B}$ and $4t\mathcal{B}$, respectively, which correspond to the proven bounds. Since the path is 3-round iterative, it shows that the proven bounds are tight.

5.2 BFN-$(SP)^{2t-1}$S and BFN-$(SP)^{2t}$S

The right side of Fig. 4 shows a 6-round iterative path for BFN-$(SP)^{2t-1}$S that maps $(0, \Delta)$ to $(0, \Delta)$. There does not exist a simple 3-round iterative path, since the output difference of the F-function will be $\nabla(\Delta)$ when the input difference of F-function is $\Delta(\nabla)$. However, those become iterative when considered over 6 rounds. The paths shown in the figure provide $2t\mathcal{B}$ active S-boxes for 3 rounds and prove the tightness of the bounds proven in Theorem 5. Figure 5 shows a 3-round iterative path for BFN-$(SP)^{2t}$S that attains the lower bounds proven in Theorem 6.

5.3 BFN-SP

The paths of Fig. 6 for BFN-SP consist of iterative paths and an additional path. In the case of $(4R+3)$ rounds, the tightness is easily proven by the right side of Fig. 6. In the other cases ($4R$, $4R+1$ and $4R+2$ rounds), paths consist of some consecutive 4-round iterative paths on the left and one 4-round additional path in the center of Fig. 6. Each path for $4R$ rounds consists of $(R-1)$ consecutive 4-round iterative paths and one 4-round additional path. Also paths for $4R+1$ and $4R+2$ rounds consist of R consecutive 4-round iterative paths and one 4-round additional path. For example, a path for 12 rounds of BFN-SP consists of two consecutive 4-round iterative paths followed by one 4-round additional path. Similarly, a path for 13 rounds consists of three 4-round iterative paths (12 rounds) followed by the first one round of the 4-round additional path (1 round).

5.4 BFN-$(SP)^{2t+1}$, $t > 0$

Figure 7 shows a 6-round iterative path that attains the bounds proven in Theorem 3. The path starting from the i-th round shows the tightness for $3R+1$ and $3R+2$ rounds. The path starting from the $(i+2)$-th round shows the tightness for $3R$ rounds.

6 Optimality

In this section, it is proven that BFN-SPS and BFN-SPSP are the most efficient with respect to the efficiency metric E_m of Definition 5. Recall that E_m shows the ratio between active S-boxes and all S-boxes when the number of rounds is sufficiently large. Table 2 contains the computation of E_m for the different BFNs in question. The optimality result is formulated as follows.

Table 2 E_m for BFNs with SP-type functions and MDS matrices

Construction	$A_{r,m}$	$S_{r,m}$	$E_m = \lim_{r\to\infty} \frac{A_{r,m}}{S_{r,m}}$
BFN-(SP)^{2t} BFN-(SP)^{2t-1}S	$A_{3R,m} = 2t(m+1)R$ $A_{3R+1,m} = 2t(m+1)R$ $A_{3R+2,m} = (2tR+t)(m+1)$	$2tmr$	$\frac{m+1}{3m}$
BFN-(SP)$^{2t+1}$	$A_{3R,m} = ((2t+1)R-1)(m+1)+2$ $A_{3R+1,m} = (2t+1)(m+1)R$ $A_{3R+2,m} = ((2t+1)R+t)(m+1)+1$	$(2t+1)mr$	$\frac{m+1}{3m}$
BFN-SP	$A_{4R,m} = (m+2)R-1$ $A_{4R+1,m} = (m+2)R$ $A_{4R+2,m} = (m+2)R+1$ $A_{4R+3,m} = (m+2)R+2$	mr	$\frac{m+2}{4m}$
BFN-(SP)^{2t}S	$A_{3R,m} = 2(t(m+1)+1)R$ $A_{3R+1,m} = 2(t(m+1)+1)R$ $A_{3R+2,m} = (2R+1)(t(m+1)+1)$	$(2t+1)mr$	$\frac{2t(m+1)+2}{3(2t+1)m}$

Theorem 7 *When instantiated with MDS matrices for $m \geq 2$, BFN-(SP)^{2t} and BFN-(SP)$^{2t-1}$S provide a higher or equal proportion of active S-boxes than BFN-SP, BFN-(SP)$^{2t+1}$ and BFN-(SP)^{2t}S for any number t of layers. Thus, BFN-SPSP and BFN-SPS are optimal with respect to E_m.*

Proof We compute the values of E_m for all BFN constructions with MDS matrices in Table 2 and compare $E_m = \frac{m+1}{3m}$ for BFN-(SP)^{2t} and BFN-(SP)$^{2t-1}$S to E_m for

- BFN-(SP)$^{2t+1}$. From Table 2, one immediately observes that $\frac{m+1}{3m}$ is no lower than E_m for BFN-(SP)$^{2t+1}$.
- BFN-SP. For $m \geq 2$, the difference $\frac{m+1}{3m} - \frac{m+2}{4m} = \frac{m-2}{12m} \geq 0$ and E_m for BFN-SP is no higher than $\frac{m+1}{3m}$.
- BFN-(SP)^{2t}S. In this case, one has to analyze $\frac{2t(m+1)+2}{3(2t+1)m}$ as a function of t. After taking the value of 0 for $t = -\frac{1}{m+1}$, it grows monotonously for all $t > 0$ and attains its maximum at the infinity. Since

$$\lim_{t\to\infty} \frac{2t(m+1)+2}{3(2t+1)m} = \frac{m+1}{3m},$$

  E_m for BFN-(SP)^{2t}S is no higher than $\frac{m+1}{3m}$.

Thus, E_m for BFN-(SP)^{2t} and BFN-(SP)$^{2t-1}$S is no lower than that for BFN-(SP)$^{2t+1}$, BFN-SP, and BFN-(SP)^{2t}S, which yields the first claim of the theorem. The second claim follows from choosing $t = 1$. □

7 Conclusion

In this work, we considered a wide class of balanced Feistel networks with any number of interleaved S-box layers and linear diffusion layers in their F-function. In this class, we demonstrated that SPS and SPSP F-functions are arguably optimal with respect to the relative number of active S-boxes provided. Our results indicate that one SP-layer in the F-function is not enough to attain optimality, whereas taking more than two S-box layers does not increase the efficiency either. The optimality is shown with respect to the security of a cipher towards differential and linear cryptanalysis.

As nearly any SPN-based block cipher, BFNs with SP-type F-functions exhibit the differential effect—many differential trails contributing to the same differential. Having SPS or SPSP constructions as F-functions—as in the optimal constructions of this paper—simplifies the consideration of upper bounds on the differential probability over several rounds. The work [1] proves that the maximum average differential probability over 3 rounds for a BFN with bijective F-functions is upper-bounded by π^2, where π is the maximum differential probability of the F-function. At the same time, the maximum differential probability of an SPS or SPSP construction with MDS diffusion is known to be upper-bounded by p^m, where p is the maximum differential probability of the underlying S-box [17]. This provides an upper bound of p^{2m} on the average differential probability over 3 rounds of BFN-SPS and BFN-SPSP. Similar considerations apply to the linear probability. However, capturing the differential or linear hull effect for an arbitrary number of rounds and incorporating it into the efficiency metric appears to be a challenging task.

Besides BFNs, generalized Feistel networks (GFNs) are often used in the design of block ciphers. Both CLEFIA [28] and PICCOLO [23] follow this design approach with SP-type F-functions. We conjecture that our optimality result also applies to any GFN under the definition of [10]. In other words, our conjecture is that the instantiation of the F-function with SPS and SPSP will be optimal with respect to the relative number of active S-boxes. We leave this as an important open problem.

References

1. Aoki K., Ohta K.: Strict evaluation of the maximum average of differential probability and the maximum average of linear probability. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E80–A**(1), 2–8 (1997).
2. Aoki K., Ichikawa T., Kanda M., Matsui M., Moriai S., Nakajima J., Tokita T.: Camellia: a 128-bit block cipher suitable for multiple platforms: design and analysis. In: Stinson D.R., Tavares S. (eds.) Proceedings of Selected Areas in Cryptography: SAC 2000. Lecture Notes in Computer Science, vol. 2012, pp. 39–56. Springer, Berlin (2001).
3. Biham E.: On Matsui's linear cryptanalysis. In: Santis A.D. (ed.) Advances in Cryptology: EUROCRYPT '94. Lecture Notes in Computer Science, vol. 950. Springer, Berlin (1994).
4. Biham E., Dunkelman O.: The SHAvite-3 hash function. Tweaked version (2009).
5. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**, 3–72 (1991).
6. Bogdanov A.: On the differential and linear efficiency of balanced Feistel networks. Inf. Process. Lett. **110**(20), 861–866 (2010).
7. Bogdanov A.: On unbalanced Feistel networks with contracting MDS diffusion. Des. Codes Cryptogr. **59**(1—-3), 35–58 (2011).
8. Bogdanov A., Shibutani K.: Analysis of 3-line generalized Feistel networks with double SD-functions. Inf. Process. Lett. **111**(13), 656–660 (2011).
9. Bogdanov A., Shibutani K.: Double SP-functions: enhanced generalized Feistel networks. In: Parampalli U., Hawkes P. (eds.) ACISP'11. Lecture Notes in Computer Science, vol. 6812, pp. 106–119. Springer, Berlin (2011).
10. Bogdanov A., Shibutani K.: Generalized Feistel networks revisited. In: Canteaut A., Augot D. (eds.) Proceedings of International Workshop on Coding and Cryptography (WCC'11). Bergen, Norway (2011).
11. Coppersmith D.: The data encryption standard (DES) and its strength against attacks. IBM J. Res. Dev. **38**(3), 243–250 (1994).
12. Daemen J., Rijmen V.: The Design of Rijndael. The Advanced Encryption Standard (AES, Information Security and Cryptography). Springer, Berlin (2002).

13. FIPS: Data Encryption Standard. National Bureau of Standards. US Department of Commerce, Washington (1997).
14. Feistel H.: Cryptography and computer privacy. Sci. Am. **228**, 1523 (1973).
15. Kanda M.: Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function. In: Stinson D.R., Tavares S. (eds.) SAC 2000. Lecture Notes in Computer Science, vol. 2012. Springer, Berlin (2001).
16. Kanda M., Moriai S., Aoki K., Ueda H., Takashima Y., Ohta K., Matsumoto T.: E2: a new 128-bit block cipher. IEICE Trans. Fundam. **E83–A**(1), 48–59 (2000).
17. Kang J.S., Hong S., Lee S., Yi O., Park C., Lim J.: Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks. ETRI J. **23**(4), 158–167 (2001).
18. Matsui M.: Linear cryptanalysis of the Data Encryption Standard. In: Helleseth T. (ed.) Advances in Cryptology EUROCRYPT'93. Lecture Notes in Computer Science, pp. 386–397. Springer, Berlin (1994).
19. Matsui M.: On correlation between the order of s-boxes and the strength of DES. In: Santis A.D. (ed.) Advances in Cryptology EUROCRYPT'94. Lecture Notes in Computer Science, vol. 950, pp. 366–375. Springer, Berlin (1994).
20. National Soviet Bureau of Standards, Information Processing System: Cryptographic Protection—Cryptographic Algorithm GOST 28147–89 (1989).
21. Shamir A.: On the Security of DES. CRYPTO'85. Lecture Notes in Computer Science. Springer, Berlin (1985).
22. Schneier B., Kelsey J., Whiting D., Wagner D., Hall C., Ferguson N.: The Twofish Encryption Algorithm: A 128-Bit Block Cipher. Wiley, New York (1999).
23. Shibutani K., Isobe T., Hiwatari H., Mitsuda A., Akishita T., Shirai T.: Piccolo: an ultra-lightweight blockcipher. In: Preneel B., Takagi T. (eds.) CHES'11. Lecture Notes in Computer Science, vol. 6917, pp. 342–357. Springer, Berlin (2011).
24. Shimizu H.: On the security of Feistel cipher with SP-type F function. In Proceedings of SCIS (in Japanese) (2001).
25. Shirai T., Preneel B.: On Feistel ciphers using optimal diffusion mappings across multiple rounds. In: Lee P.J. (ed.) ASIACRYPT'04. Lecture Notes in Computer Science, vol. 3329, pp. 1–15. Springer, Berlin (2004).
26. Shirai T., Shibutani K.: Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices. In: Roy B.K., Meier W. (eds.) FSE'04. Lecture Notes in Computer Science, vol. 3017, pp. 260–278. Springer, Berlin (2004).
27. Shirai T., Shibutani K.: On Feistel structures using a diffusion switching mechanism. In: Robshaw M.J.B. (ed.) FSE'06. Lecture Notes in Computer Science, vol. 4047, pp. 41–56. Springer, Berlin (2006).
28. Shirai T., Shibutani K., Akishita T., Moriai S., Iwata T.: The 128-bit blockcipher CLEFIA. In: Biryukov A. (ed.) FSE'07. Lecture Notes in Computer Science, vol. 4953, pp. 181–195. Springer, Berlin (2007).
29. Tardy-Corfdir A., Gilbert H.: A known plaintext attack of FEAL-4 and FEAL-6. In: Feigenbaum J. (ed.) CRYPTO'91. Lecture Notes in Computer Science, vol. 576, pp. 172–181. Springer, Berlin (1991).
30. Third Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification, V3.1.1 (2001).