Advances in Computer Science Research, volume 88
International Conference on Computer, Network, Communication and Information Systems (CNCI 2019)

Provable Security against Differential Attacks for Generalized SPN Structures

Ruya Fan[1, a]
Information Science and Technology Institute, Zhengzhou, China
fanruya@126.com

Abstract. In the practice of block cipher design, designers usually choose linear functions over $GF(2^n)$ with large branch numbers to achieve provable security against differential and linear attack. Recently, the Internet-of-Things gives rise to a number of applications that require Lightweight block ciphers, some new extensions of the diffusion layer were proposed, and these diffusion layers are designed by the matrices over commutative rings. Compared with the matrices which were defined over $GF(2^n)$, these matrices need less cost in hardware implementation and are thus more suitable for lightweight ciphers. In this work, we prove that the SPN structure with an extended diffusion layer provides a provable security against differential attack and linear attack. The probability of each differential of the SPS function is bounded by p^{r-1}, where p is the maximum differential probability of S-boxes used in the substitution layer, and r denotes the branch number of the diffusion layer. Similarly, the results of maximum linear hull bias could also be obtained. With the application of our method, we give the first security evaluation for some SPS structures with the matrix over $GF(2)$ against differential attack.

Keywords: Block ciphers, SPN, generalized diffusion layer, provable security, differential attack.

1. Introduction

The Substitution-Permutation Networks (SPN) is a basic design of block cipher, which is highly parallelizable and could process the whole data block within one single round function. Compared with the Feistel-family and other structures, this structure provides faster diffusion and confusion. Since its design, it was adopted by massive famous block ciphers such as AES [1], ARIA [2], 3D [3] etc.

The core problem in designing the SPN structure is to design its diffusion layer. For decades, the most attractive diffusion layers are those having matrix representations over $GF(2^n)$, where n is usually consistent to the bit length of S-box used in the confusion layer. Many block ciphers [1,2,3,4], especially AES, use this design strategy to construct their diffusion layers. In FSE 2012, Sajadieh et.al [5] extended this design strategy, and the diffusion matrix from this strategy can be treated as an $mn \times mn$ matrix over $GF(2^n)$ or an $m \times m$ matrix composed of linear transformations over F_2^n. This kind of diffusion layer has already been used in the block cipher SMS4 [6] and the hash function SHA-2 [7]. In SAC2012, Wu et. al. [8] provided an impressive work in constructing a special kind of such diffusion layers in a recursive way, and these matrices often require smaller hardware implementations. Since the multiplication operations with elements in $GF(2^n)$ are specific linear transformations of vector space F_2^n, this new design strategy can be treated as a generalization of the old ones, thus may provide more choices in constructing diffusion layers. Especially for the lightweight block ciphers and hash functions [9].

Our motivation is, in SPN cipher, if we replace the diffusion layer by a more generalized one [10,11], how will it affect the security level of our block ciphers?

1.1 Related Work

Among all ways of attacks on block ciphers, the most famous ones are differential attack (DA) [12,13] and linear attack (LA) [14,15]. Thus it is a basic requisite for the designer to evaluate the security of any new proposed cipher against these two attacks, and to prove that it is sufficiently resistant against them. In DA, one uses characteristic to describe the behavior of input and output differences for some number of consecutive rounds. However, it may not be necessary to fix the values of input and output differences for the intermediate rounds in a characteristic, so naturally the notion of differential was introduced [16]. The same statements can be applied to LA [17]. Named by Nyberg and Knudsen, a block cipher is said to have provable security against DA and LA, if the upper bounds of the maximum average of differential and linear hull probabilities are sufficiently small [18]. S. Hong et. al. studied the provable security of SPN structure whose diffusion layer is chosen as the maximal or semi-maximal matrices over $GF(2^n)$ [19], and later, Kang et. al. made an extension, they worked on the diffusion layers matrices over $GF(2^n)$, and removed the branch number limits on matrices [20].

1.2 Our Contribution

Inspirited by Hongs and Kang's work [19,20], in this paper we consider the provable security measure of generalized SPN, namely, the diffusion layer is chosen as an $m \times m$ matrix composed of linear transformations over F_2^n, while most of the previous results are based on the matrices over $GF(2^n)$. Our main results can be concluded by:

We prove that for the generalized diffusion layer $P_{m\times m}$, if we have $y = Px$, then from any of its $2m-r+1$ components we can determine the rest $r-1$ components.

If the maximum differential probability of S-boxes is p and the differential branch number of the diffusion layer is denoted by r, then the differential probability of SPS is bounded by p^{r-1}. Similarly, if the maximum liner hull probability of S-boxes is denoted by q and the linear branch number of the diffusion layer is denoted by r, then the linear hull bias of SPS is bounded by q^{r-1}.

Applying our results on traditional SPS structures (means the entries in the diffusion layer are selected from $GF(2^n)$), we may get the same results as in [11], what's more, our results are compatible with Crypton [22] and other generalized SPS structures whose diffusion matrix are defined over $GF(2)$).

1.3 Organization

This paper is organized as follows: Section 2 introduces some notations and definitions. Section 3 works on the properties of the generalized diffusion layers, Section 4 provides a provable security for the generalized SPN structure against DA and LA. Section 5 applies our results on some well-known SPS structures. Final Section 6 draws the conclusion.

2. Preliminaries

In this paper, we use the following symbols:

$\oplus$	XOR operation;
Δx	the XOR difference of x and x';
$w_n(X)$	the number of nonzero bundle in vector $X=(x_0,x_1,\cdots,x_{m-1})$, where each $x_i \in F_2^n$;
E	the identity matrix;
A^T	the transpose of matrix A;
$\mid$	matrices concatenation;
$\mathrm{B}_{n\times n}$	set of all $n\times n$ matrices with entries in $GF(2)$;
F_2^n	n-dimension vector space over $\{0,1\}$.

The substitution layer S is a non-linear transformation on $\{0,1\}^{mn}$ defined by m parallel non-linear bijections $S_0,\cdots,S_{m-1}$ map on n-bit word, i.e.

$S(x_0,\cdots,x_{m-1})=(s_0(x_0),\cdots,s_{m-1}(x_{m-1}))$,

the permutation layer $P:\{0,1\}^{mn}\to\{0,1\}^{mn}$ is a linear bijection, and one round SPN structure is defined as

$SP(x,k)=P(S(x\oplus k))$

where $k=(k_0,\cdots,k_{m-1})$ is the subkey.

SPN is a basic structure of modern ciphers, and many ciphers employ this structure in their round functions. In two rounds SPN, since the last P layer does not affect the security, we omit this layer in this paper, i.e. in this paper, we only focus on the SPS structure.

In SPN cipher, the most popular design of the diffusion layer is based on the $m\times m$ matrix over the field $GF(2^n)$, such sound examples are AES [1], ARIA [2], LED [21] and Gimli [23], employ this kind of diffusion layers, in which the inputs are transformed through several constant multipliers and then to the outputs word-wise. The constant multipliers of $GF(2^n)$ could be treated as special form linear transformations over $\{0,1\}^n$. Thus these matrices can be treated as $mn\times mn$ matrices over F_2, instead of those with entries selected from $GF(2^n)$. In [5], Sajadieh et.al extended this design strategy, they proposed an $m\times m$ matrix composed of linear transformations over F_2^n, using basic linear algebraic theory, this kind of matrices could also be treated as $mn\times mn$ matrices over $GF(2)$.

According to the different design strategies, the diffusion layer P can be classified into two kinds: the matrices can be seen as the matrix over a finite field $GF(2^n)$ and those cannot. No matter which kind of diffusion layer P we choose, P always forms a linear mapping transformations over $GF(2^n)$, thus can be written as a multiplication by a matrix $P_{mn\times mn}$, i.e. $y=Px$.

Definition 1 [8]. A bijection $P:F_2^{mn}\to F_2^{mn}$ is defined as a generalized diffusion layer, if it could be represented by an $mn\times mn$ binary matrix.

Definition 2 [16,17]. Let f be a mapping defined over $\{0,1\}^n$, then for any given $\Delta x,\Delta y,\Gamma x,\Gamma y\in\{0,1\}^n$, the differential probability and the linear bias are defined as follows

$$p_f(\Delta x\to\Delta y)=\frac{\#\left\{x\in\{0,1\}^n : f(x)\oplus f(x\oplus\Delta x)=\Delta y\right\}}{2^n}$$

$$\rho_f(\Delta x\to\Delta y)=\left(\frac{\#\left\{x\in\{0,1\}^n : \langle\Gamma x,x\rangle\oplus\langle\Gamma y,f(x)\rangle=0\right\}}{2^{n-1}}-1\right)^2$$

where $\langle a,b\rangle$ denotes the parity of bit-wise product of a and b.

Throughout this paper, we use the following two symbols:

$p=\max\limits_{\substack{\Delta x\neq 0,\Delta y\\ 0\le i\le m-1}}\{p_{s_i}(\Delta x\to\Delta y)\}$ and $\rho=\max\limits_{\substack{\Gamma x,\Gamma y\neq 0\\ 0\le i\le m-1}}\{\rho_{s_i}(\Gamma x\to\Gamma y)\}$, people often use p, ρ and the branch number to describe the resistances of an SPS function against the traditional differential attack and the linear attack by bounding the probability of the characteristics.

Definition 3 [1]. Let $P=(p_{i,j})_{mn\times mn}$ be a matrix over $\{0,1\}$, then the n bundle differential branch number of P is defined as

$$Bd_n(P)=\min\left\{wt_n(x)+wt_n(Px):x\in\{0,1\}^{mn}\setminus\{0\}\right\}$$

and the n bundle linear branch number of P is defined as

$$Bl_n(P)=\min\left\{wt_n(x)+wt_n(P^Tx):x\in\{0,1\}^{mn}\setminus\{0\}\right\}$$

3. Properties of the Generalized Diffusion Layer

In this section, we focus on the cryptographic properties of the generalized diffusion layers.

Lemma 1[8]. Let $P=(P_{i,j})_{m\times m}$ be an $m\times m$ matrix over $\mathrm{B}_{n\times n}$, $Bd_n(P)=m+1$, then for any two permutations π_1,π_2 over the set $\{0,1,\cdots,m-1\}$ and integer $1\le k\le m$, the matrix $Q(\pi_1,\pi_2)=(Q_{i,j})_{k\times k}$ with $Q_{i,j}=P_{\pi_1(i),\pi_2(j)}$ is nonsingular.

Remark. In this paper, the linearly-dependency property is considered over $GF(2)$. Using Lemma 1, we conclude the result below.

Lemma 2[8]. Let $P=(P_{i,j})_{m\times m}$ be an $m\times m$ matrix over $\mathrm{B}_{n\times n}$, then $Bd_n(P)=m+1$ iff $Bl_n(P)=m+1$.

Definition 4. ($\mathrm{B}_{n\times n}$ -column) Let $P=(p_{i,j})_{mn\times mn}$ be an $mn\times mn$ matrix over $GF(2)$, then the sub-matrix $P_{\{k\}}=(q_{i,j})_{mn\times n}$ is called the k -th $\mathrm{B}_{n\times n}$ -column of P, where $q_{i,j}=p_{i,(j+k\times(n-1))}$.

Take consider of the differential property of the generalized diffusion layer, the input difference is $A=(A_0,A_1,\cdots,A_{m-1})$ and the output difference is $B=(B_0,B_1,\cdots,B_{m-1})$, each A_i (resp. B_i) is said to be a 'bundle' of the differential.

Theorem 1. Let $P=(P_{i,j})_{m\times m}$ be an $m\times m$ matrix over $\mathrm{B}_{n\times n}$ and E be an $m\times m$ identity matrix over $\mathrm{B}_{n\times n}$, matrix $M=[P\mid E]=(B_{i,j})_{m\times m}$, then $Bd_n(P)\ge r+1$ iff for any integer $k\le r$, k $\mathrm{B}_{n\times n}$-columns of M are linearly independent.

Proof. (Necessity)By Definition 4,

$$\begin{aligned}Bd_n(P)&=\min_{x\neq 0}\{w_n(x)+w_n(Px)\}\\&=\min_{x\neq 0}\{w_n(x,y):Px=Ey\}\\&=\min_{x\neq 0}\left\{w_n(x,y):M\begin{pmatrix}x\\y\end{pmatrix}=0\right\}\ge r+1,\end{aligned}$$

which indicates that for any nonzero (x,y) pair such that $w_n(x,y)\le r$,the equation $M\begin{pmatrix}x\\y\end{pmatrix}=0$ does not hold, thus any $w_n(x,y)(\le r)$ $\mathrm{B}_{n\times n}$-columns of M are linearly independent.

(Sufficiency) Since for any integer $k\le r$, k $\mathrm{B}_{n\times n}$-columns of M are linearly independent, which means we cannot find such $w_n(x,y)\le r$ such that $M\begin{pmatrix}x\\y\end{pmatrix}=0$. Thus we conclude

$$Bd_n(P) = \min_{x \neq 0}\left\{ w_n(x,y) : M\begin{pmatrix} x \\ y \end{pmatrix} = 0 \right\} \geq r+1.$$

Theorem 2. Let $P = (P_{i,j})_{m\times m}$ be an $m \times m$ matrix over $\mathrm{B}_{n\times n}$, $Bd_n(P) = r < m+1$, then for any $B = PA$, the pair (A,B) is determined by any of its $2m-r+1$ bundles.

Proof. Since $B = PA$ could be rewritten as $[P \mid E]\begin{pmatrix} A \\ B \end{pmatrix} = 0$, we note $[P \mid E] = M_{m\times 2m}$, $\begin{pmatrix} A \\ B \end{pmatrix} = z$, then for any $0 \leq i \leq n-1$, we have $\sum_{j=0}^{2m-1} M_{i,j} \cdot z_j = 0$. Let π be a bijection over $\{0,1,\cdots,2m-1\}$, then we may have $\sum_{j=0}^{r-2} M_{i,\pi(j)} \cdot z_{\pi(j)} = \sum_{j=r-2}^{2m-1} M_{i,\pi(j)} \cdot z_{\pi(j)}$ hold for any $0 \leq i \leq n-1$, which could be represented by matrix multiplications, i.e.

$$\begin{pmatrix} M_{0,\pi(0)} & M_{0,\pi(1)} & \cdots & M_{0,\pi(r-2)} \\ M_{1,\pi(0)} & M_{1,\pi(1)} & \cdots & M_{1,\pi(r-2)} \\ \vdots & & \ddots & \vdots \\ M_{m-1,\pi(0)} & M_{m-1,\pi(1)} & \cdots & M_{m-1,\pi(r-2)} \end{pmatrix}\begin{pmatrix} z_{\pi(0)} \\ z_{\pi(1)} \\ \vdots \\ z_{\pi(r-2)} \end{pmatrix}$$
$$= \begin{pmatrix} M_{0,\pi(r-1)} & M_{0,\pi(r)} & \cdots & M_{0,\pi(2m-1)} \\ M_{1,\pi(r-1)} & M_{1,\pi(r)} & \cdots & M_{1,\pi(2m-1)} \\ \vdots & & \ddots & \vdots \\ M_{m-1,\pi(r-1)} & M_{m-1,\pi(r)} & \cdots & M_{m-1,\pi(2m-1)} \end{pmatrix}\begin{pmatrix} z_{\pi(r-1)} \\ z_{\pi(r)} \\ \vdots \\ z_{\pi(2m-1)} \end{pmatrix}$$

By Theorem 1, any $r-1$ $\mathrm{B}_{n\times n}$-columns of $M_{m\times 2m}$ are linearly independent. Then there exists $(r-1)n$ rows in the $mn \times (r-1)n$ binary matrix

$$\begin{pmatrix} M_{0,\pi(0)} & M_{0,\pi(1)} & \cdots & M_{0,\pi(r-2)} \\ M_{1,\pi(0)} & M_{1,\pi(1)} & \cdots & M_{1,\pi(r-2)} \\ \vdots & & \ddots & \vdots \\ M_{m-1,\pi(0)} & M_{m-1,\pi(1)} & \cdots & M_{m-1,\pi(r-2)} \end{pmatrix}$$

Without loss of generality, we assume the row coordinates are $l_0, l_1, \cdots, l_{n(r-2)}$, then we pick up these $(r-1)n$ rows from the equations above, and get

$$\begin{pmatrix} m_{l_0,0} & m_{l_0,1} & \cdots & m_{l_0,n(r-2)} \\ m_{l_1,0} & m_{l_1,1} & \cdots & m_{l_1,n(r-2)} \\ \vdots & & \ddots & \vdots \\ m_{l_{n(r-2)},0} & m_{l_{n(r-2)},1} & \cdots & m_{l_{n(r-2)},n(r-2)} \end{pmatrix}\begin{pmatrix} z_{\pi(0)} \\ z_{\pi(1)} \\ \vdots \\ z_{\pi(r-2)} \end{pmatrix}$$
$$= \begin{pmatrix} q_{l_0,0} & q_{l_0,1} & \cdots & q_{l_0,n(2m-r-1)} \\ q_{l_1,0} & q_{l_1,1} & \cdots & q_{l_1,n(2m-r-1)} \\ \vdots & & \ddots & \vdots \\ q_{l_{n(r-2)},0} & q_{l_{n(r-2)},1} & \cdots & q_{l_{n(r-2)},n(2m-r-1)} \end{pmatrix}\begin{pmatrix} z_{\pi(r-1)} \\ z_{\pi(r)} \\ \vdots \\ z_{\pi(2m-1)} \end{pmatrix}$$

Since the left matrix in the equation above is invertible, thus we end the proof.

Theorem 2 tells that even though the entries of the matrix are chosen from $\mathrm{B}_{n\times n}$ instead of $GF(2^n)$, we can still fix any $2m-r+1$ bundles of the generalized diffusion layer P and determine the rests uniquely. This property forms the basis of our analysis next.

4. Provable Security for Generalized SPN Structure Against DA and LA

With the preparation above, we are arriving at our main theorems.

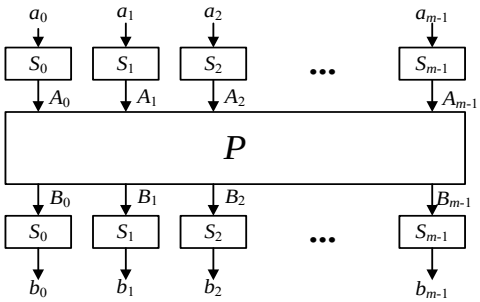

Fig. 1 Differential propagating of SPS structure

Theorem 3. Assume that the round keys, which are XOR-ed to the input data at each round, are independent and uniformly random. If $Bd_n(P) = r \le m+1$, the probability of each differential of SPS function is bounded by p^{r-1}, where p denotes the maximum differential probability of all the S-boxes, and the P layer is defined by an $m \times m$ matrix over $\mathrm{B}_{n\times n}$.

Proof. We take consideration of the differentials depicted in Fig. 1. Let η, ς be two permutations over $\{0,1,\cdots,m-1\}$, without loss of generality, we may assume $a_{\eta(0)}, a_{\eta(1)}, \cdots, a_{\eta(s-1)}$ and $b_{\varsigma(0)}, b_{\varsigma(1)}, \cdots, b_{\varsigma(h-1)}$ are nonzero and $a_{\eta(s)} = \cdots = a_{\eta(m-1)} = b_{\varsigma(h)} = \cdots = b_{\varsigma(m-1)} = 0$. Then we have

$$
\begin{aligned}
& p(a \to b) \\
&= \sum_{A,B} p(a \to A \to B \to b) \\
&= \sum_{A,B} p_S(a \to A) p_P(A \to B) p_S(B \to b) \\
&= \sum_{A} p_S(a \to A) p_S(PA^T \to b) \\
&= \sum_{A \in \Omega} p_S(a \to A) p_S(PA^T \to b),
\end{aligned}
$$

where $\Omega = \{A : p_S(a \to A) p_S(PA \to b) > 0\}$

If $h < r-1$, i.e. $h+s-r+1 < s$, which implies

$\{A_{\eta(0)}, A_{\eta(1)}, \cdots, A_{\eta(h+s-r)}\} \bigcap \{A_{\eta(s)}, \cdots, A_{\eta(m-1)}\} = \phi$,

since $B_n(P) = r$, by Theorem 2, if any $2m-r+1$ bundles are fixed, then the rest $r-1$ bundles are determined. By our assumption, in the pair (A, PA^T), there are $(m-h)+(m-s)$ bundles of 0. Notice $\{A_{\eta(0)}, A_{\eta(1)}, \cdots, A_{\eta(h+s-r)}\} \bigcap \{A_{\eta(s)}, \cdots, A_{\eta(m-1)}\} = \phi$, which means by fixing $A_{\eta(0)}, A_{\eta(1)}, \cdots, A_{\eta(h+s-r)}$, we can fix the value of A, thus we have

$$
\begin{aligned}
& p(a \to b) \\
&= \sum_{A \in \Omega} p_S(a \to A)\, p_S(PA^T \to b) \\
&= \sum_{A \in \Omega} [\prod_{i=0}^{m-1} p_{s_i}(a_i \to A_i)][\prod_{i=0}^{m-1} p_{s_i}(B_i \to b_i)] \\
&= \sum_{A \in \Omega} [\prod_{i=0}^{s-1} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})][\prod_{i=0}^{h-1} p_{s_{\varsigma(i)}}(B_{\varsigma(i)} \to b_{\varsigma(i)})] \\
&= \sum_{A_{\eta(0)}} \sum_{A_{\eta(1)}} \cdots \sum_{A_{\eta(s-1)}} [\prod_{i=0}^{s+h-r} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})] \\
&\times [\prod_{i=s+h-r+1}^{s-1} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})][\prod_{i=0}^{h-1} p_{s_{\varsigma(i)}}(B_{\varsigma(i)} \to b_{\varsigma(i)})] \\
&= \sum_{A_{\eta(0)}} \sum_{A_{\eta(1)}} \cdots \sum_{A_{\eta(s+h-r)}} [\prod_{i=0}^{s+h-r} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})] \\
&\times [\prod_{i=s+h-r+1}^{s-1} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})][\prod_{i=0}^{h-1} p_{s_{\varsigma(i)}}(B_{\varsigma(i)} \to b_{\varsigma(i)})] \\
&\le p^{r-h-1} p^h \sum_{A_{\eta(0)}} \sum_{A_{\eta(1)}} \cdots \sum_{A_{\eta(s+h-r)}} [\prod_{i=0}^{s+h-r} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})] \\
&= p^{r-1}
\end{aligned}
$$

In case $h \ge r-1$, we have

$$
\begin{aligned}
& p(a \to b) \\
&= \sum_{A \in \Omega} [\prod_{i=0}^{m-1} p_{s_i}(a_i \to A_i)][\prod_{i=0}^{m-1} p_{s_i}(B_i \to b_i)] \\
&= \sum_{A_{\eta(0)}} \sum_{A_{\eta(1)}} \cdots \sum_{A_{\eta(s-1)}} [\prod_{i=0}^{s-1} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})] \\
&\quad \times [\prod_{i=0}^{h-1} p_{s_{\varsigma(i)}}(B_{\varsigma(i)} \to b_{\varsigma(i)})] \\
&\le p^h \sum_{A_{\eta(0)}} \sum_{A_{\eta(1)}} \cdots \sum_{A_{\eta(s-1)}} [\prod_{i=0}^{s-1} p_{s_{\eta(i)}}(a_{\eta(i)} \to A_{\eta(i)})] \\
&\le p^{r-1}
\end{aligned}
$$

Since $Bd_n(P) = Bl_n(P^T)$, then by using the Parseval law, we may arrive to the following Theorem through a very similar proof.

Theorem 4. Assume that the round keys, which are XOR-ed to the input data at each round, are independent and uniformly random. If $Bl_n(P) = r < m+1$, the bias of each linear hull of SPS function is bounded by ρ^{r-1}, where ρ denotes the maximum linear bias of all the S-boxes, and the P layer is defined by an $m \times m$ matrix over $\mathrm{B}_{n \times n}$.

5. Application and Comparison

In this section, we apply our results in estimating the differential probabilities of several famous SPS structures (see Table 1).

In general, if the SPS structure employs the matrix over a finite field, the results proposed by [20] may suit quite well. However, if we choose generalized diffusion layer, for example, Crypton [22], SPS_1 [8] and SPS_2 [6], then the condition of [20] will never be satisfied, thus by their estimation we cannot get any result. With the application of our method, we give the first security evaluation for them against differential attack in Table 1.

Table 1 Differential probability bounds(DPB) of several SPS structures

Source	p value	P -layer	Matrix size	Entry Space	DPB by [20]	DPB by ours
AES	2^{-6}	MixColumn	4×4	$GF(2^8)$	2^{-24}	2^{-24}
FOX64	2^{-4}	MDS matrix	4×4	$GF(2^8)$	2^{-16}	2^{-16}
FOX128	2^{-4}	MDS matrix	8×8	$GF(2^8)$	2^{-32}	2^{-32}
E2	2^{-6}	Binary matrix	8×8	$GF(2^8)$	2^{-32}	2^{-32}
Crypton	2^{-5}	π Transfor-mation[22]	32×32	$GF(2)$	unable	2^{-15}
SPS_1	2^{-2}	Perfect diffusion [8]	16×16	$GF(2)$	unable	2^{-8}
SPS_2	2^{-6}	L layer of SMS4 [6]	32×32	$GF(2)$	unable	2^{-24}

6. Conclusions

Using the matrices over $GF(2^n)$ are sometimes unfitted in resource constrained environments, such as RFID systems and sensor networks, thus people have to employ the matrix over commutative rings to guarantee better implementation performance. As mentioned in [8], these generalized matrices can be used to gain smaller hardware implementations. In this paper, we studied the upper bounds of the maximum average of differential and linear hull probabilities of generalized SPN ciphers, we proved that the probability of each differential (resp. linear hull) of the SPS function with a r-branch number diffusion layer is bounded by p^{r-1} (resp. ρ^{r-1}). These results give a provable security for the generalized SPN structure against DA and LA. Compared with the results of [19] and [20], these generalized matrices provide same security level against DA and LA, thus is suitable to be used in the SPN structure.

References

[1]. J. Daemen, V. Rijmen, “The Design of Rijndael: AES – The Advanced Encryption Standard,” Springer, 2002.

[2]. D. Kwon, J. Kim, S. Park, S. H. Sung et al. “New Block Cipher: ARIA,” ICISC 2003, LNCS 2971, Springer-Verlag, 2004, 432-445.

[3]. J. Nakahara, “3D: A Three-Dimensional Block Cipher,” CANS 2008, LNCS 5339, Springer-Verlag, 2008, 252-267.

[4]. P. Barreto, V. Rijmen, “The Anubis Block Cipher,” NESSIE, Sept. 2000, http://www.cryptonessie.org/.

[5]. M. Sajadieh, M. Dakhilalian, H. Mala, P. Sepehrdad, “Recursive Diffusion Layers for Block Ciphers and Hash Functions,” In: Canteaut, A. (ed.) FSE 2012, LNCS, vol. 7549, Springer, Heidelberg, 2012, 385-401.

[6]. Office of State Commercial Cryptography Administration.: P.R. China, The SMS4 Block Cipher (in Chinese), Archive available at: http://www.oscca.gov.cn/UpFile 200621016423197990.pdf.

[7]. National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) Publication 180-2, Secure Hash Standard (SHS), Feb. 2004.

[8]. S. Wu, M. Wang, and W. Wu, "Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions," In Lars R. Knudsen and Huapeng Wu, editors, Selected Areas in Cryptography, LNCS, vol. 7707, Springer, Heidelberg, 2013, 355-371.

[9]. J. Guo, T. Peyrin, A. Poschmann, "The PHOTON Family of Lightweight Hash Functions," In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, Springer, Heidelberg, 2011, 222-239.

[10]. M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki and K. Ohta, "A Strategy for Constructing Fast Functions with Practical Security against Differential and Linear Cryptanalysis," Proceedings of SAC'98, 1998.

[11]. J. Daemen, R. Govaerts and J. Vandewalle, "Correlation Matrices," Proceedings of the first international workshop of the Fast Software Encryption, LNCS 1008, Springer-Verlag, 1994, 275-285.

[12]. M. Kanda, "Practical Security Evaluation against Differential and Linear Cryptanalyses for Feistel Ciphers with SPN Round Function," Selected Areas in Cryptography, LNCS 2012, Springer-Verlag, 2000, 324-338.

[13]. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystem," Journal of Cryptology, vol. 4, 1991, 3-72.

[14]. E. Biham, "On Matsui's Linear Cryptanalysis," Advanced in cryptology-EUROCRYPT'94, Springer-Verlag, 1994, 341-355.

[15]. M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Advanced in cryptology-EUROCRYPT' 93, Springer-Verlag, 1993, 386-397.

[16]. X. Lai, J. L. Massey and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," Advances in Cryptology-EUROCRYPT'91, Springer-Verlag, 1992, 17-38.

[17]. K. Nyberg, "Linear Approximation of Block Ciphers," Advanced in cryptology-EUROCRYPT'94, Springer-Verlag, 1994, 439-444.

[18]. K. Nyberg and L.R. Knudsen, "Provable Security against Differential Cryptanalysis," Journal of Cryptology, 1995, vol.8, no. 1, 27-37.

[19]. S. Hong, S. Lee, J. Lim, J. Sung, and D. Choen, "Provable Security against Differential and Linear Cryptanaysis for the SPN structure," Proc. of FSE 2000, LNCS Springer-Verlag, 1978, 273-283.

[20]. J. Kang, S. Hong, S. Lee, O. Yi, C. Park and J. Lim, "Practical and Provable Security Against Differential and Linear Cryptanalysis for Substitution-Permutation Networks," ETRI Journal, 2001, vol. 23, no. 4, 158-167.

[21]. J. Guo, T. Peyrin, A. Poschmann, M. Robshaw, "The LED Block Cipher," In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, Springer, Heidelberg, 2011, 326-341.

[22]. C. Lim, "CRYPTON: A new 128-bit block cipher," NIST AES Proposal, 1998.

[23]. D. Bernstein et al, "Gimli: A Cross-Platform Permutation," International Conference on Cryptographic Hardware and Embedded Systems, Springer, Cham, 2017, 299-320.