Differential Cryptanalysis of the BSPN Block Cipher Structure

Liam Keliher

AceCrypt Research Group
Department of Mathematics & Computer Science
Mount Allison University
Sackville, New Brunswick, Canada
lkeliher@mta.ca

Abstract. BSPN (*byte-oriented SPN*) is a general block cipher structure presented at SAC'96 by Youssef et al. It was designed as a more efficient version of the *bit*-oriented SPN structure published earlier in 1996 by Heys and Tavares in the Journal of Cryptology. BSPN is a flexible SPN structure in which only the linear transformation layer is exactly specified, while s-boxes, key-scheduling details, and number of rounds are intentionally left unspecified. Because BSPN can be implemented very efficiently in hardware, several researchers have recommended the 64-bit version as a lightweight cipher for use in wireless sensor networks (WSNs). Youssef et al. perform preliminary analysis on BSPN (using typical block sizes and numbers of rounds) and claim it is resistant to differential and linear cryptanalysis. However, in this paper we show that even if BSPN (similarly parameterized) is instantiated with strong AES-like s-boxes, there exist high probability differentials that allow BSPN to be broken using differential cryptanalysis. In particular, up to 9 rounds of BSPN with a 64-bit block size can be attacked, and up to 18 rounds with a 128-bit block size can be attacked.

Keywords: BSPN, block cipher, SPN, differential cryptanalysis, wireless sensor network (WSN)

1 Introduction

BSPN (*byte-oriented SPN*) is a general block cipher structure presented at SAC'96 by Youssef et al. [19]. It was designed as a more efficient byte-oriented version of the *bit*-oriented SPN structure published by Heys and Tavares in the Journal of Cryptology [5]. BSPN is a flexible SPN structure in which only the linear transformation layer is exactly specified, while s-boxes, key-scheduling details, and number of rounds are intentionally left unspecified.[1]

As an important aspect of the designers' emphasis on efficiency, BSPN is structured to be *involutional* (self-inverting). This involutional structure has

[1] Youssef et al. did not originally use the term BSPN; this was introduced in [20].

influenced designers of other involutional ciphers such as KHAZAD [1] and CURUPIRA [2]. Several researchers have considered hardware implementations of 64-bit BSPN, and have recommended it as a *lightweight cipher* [15] for use in *wireless sensor networks* (WSNs) because of its high speed, low power usage, and low chip area [9, 20, 21].

Youssef et al. perform preliminary analysis on BSPN (using typical block sizes and numbers of rounds) and claim it is resistant to differential cryptanalysis [3] and linear cryptanalysis [12], but in this paper we show that this analysis is incomplete. Even if BSPN is instantiated with strong AES-like s-boxes [4], there exist high probability differentials that allow BSPN to be broken using differential cryptanalysis. In particular, up to 9 rounds with a 64-bit block size can be attacked, and up to 18 rounds with a 128-bit block size can be attacked.

The remainder of the paper is organized as follows. In Section 2 we give the structure of BSPN, and in Section 3 we examine the properties of the BSPN linear transformation. We review concepts from differential cryptanalysis in Section 4, and in Section 5 we apply differential cryptanalysis to BSPN. In Section 6 we conclude.

2 BSPN Structure

BSPN has a standard multi-round SPN structure in which each round consists of three layers: *key mixing*, *substitution*, and *permutation*. Let n denote the block size, where $n = 8m$, and m is even. In the key mixing layer, an n-bit subkey is bitwise XORed with the current block. In the substitution stage, the current block is partitioned into m bytes, each of which is input to an 8×8 bijective s-box. In the permutation stage, the s-box outputs are recombined into an n-bit block that is fed into an invertible linear transformation $\{0,1\}^n \to \{0,1\}^n$ (traditionally a bitwise permutation). A final n-bit *whitening subkey* is XORed with the output of the last round to form the ciphertext. It follows that BSPN with R rounds requires $R+1$ subkeys. For the purposes of this paper, the most general situation is assumed for key scheduling, namely that each subkey is chosen uniformly and independently from $\{0,1\}^n$.

We use BSPN-n to denote BSPN with an n-bit block size. Youssef et al. do not specify the value of n in [19], although they analyze BSPN-64. We focus on $n = 128$ (so $m = 16$), the most common modern block size, and $n = 64$ ($m = 8$), a typical block size for lightweight ciphers.

The BSPN linear transformation is given as follows: Let $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ be the input to the linear transformation, and let $\mathbf{Y} = [\mathbf{y}_1, \ldots, \mathbf{y}_m]$ be the corresponding output, where each $\mathbf{x}_i$, $\mathbf{y}_j$ is a byte. Then

$$\mathbf{y}_j = \bigoplus_{i=1, i \neq j}^{m} \mathbf{x}_i \tag{1}$$

It is easy to see that this leads to efficient implementations, since if $\mathbf{Q} = \bigoplus_{i=1}^{m} \mathbf{x}_i$, then $\mathbf{y}_j = \mathbf{x}_j \oplus \mathbf{Q}$. It is also easy to see that this linear transformation is its own

inverse, i.e., is an involution. It follows that if involutional 8×8 s-boxes are used, BSPN is itself an involution, i.e., decryption equals encryption with the subkeys applied in reverse order.[2]

3 Properties of BSPN Linear Transformation

The BSPN linear transformation $L : \{0,1\}^n \rightarrow \{0,1\}^n$ given by (1) has two related properties that make the cipher structure vulnerable to cryptanalysis:

1. a large number of fixed points
2. low diffusion

3.1 Fixed Points

A *fixed point* for L is an input $\mathbf{X} \in \{0,1\}^n$ for which $L(\mathbf{X}) = \mathbf{X}$.

Theorem 1. *The BSPN linear transformation $L : \{0,1\}^n \rightarrow \{0,1\}^n$ has 2^{n-8} fixed points.*

Proof. Let $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ be an input for L, and let $\mathbf{Q} = \bigoplus_{i=1}^{m} \mathbf{x}_i$. Then $\mathbf{X}$ is a fixed point for L if and only if $\mathbf{Q} = \mathbf{0}$. Since this occurs with probability 2^{-8}, it follows that L has 2^{n-8} fixed points. □

Remark 1. Clearly any $\mathbf{X}$ containing *exactly two identical nonzero bytes* is a fixed point for L. We exploit fixed points of this form.

Note that when $n = 64$, L has 2^{56} fixed points, and when $n = 128$ (as in the AES), L has 2^{120} fixed points.

3.2 Low Diffusion

Let $wt_B(\mathbf{Z})$ denote the number of nonzero bytes in $\mathbf{Z} \in \{0,1\}^n$. The *branch number*, $\mathcal{B}$, of linear transformation L is given by[3]

$$\mathcal{B} = \min_{\mathbf{X} \in \{0,1\}^n \setminus \mathbf{0}} \{wt_B(\mathbf{X}) + wt_B(L(\mathbf{X}))\}$$

It is well known that $2 \leq \mathcal{B} \leq m + 1$ [4]. A low branch number indicates that a linear transformation has weak *diffusive* properties. Good diffusion in a cipher means that a small change in the plaintext will influence the entire block after a small number of rounds, and this often depends on the diffusive properties of the linear transformation. Poor diffusion in a cipher may create vulnerabilities to a number of attacks, including differential cryptanalysis.

[2] This holds as long as the positions of distinct s-boxes do not violate the involution property, i.e., as long as the row of s-boxes in round r is identical to the row of s-boxes in round $(R - r + 1)$, for $1 \leq r \leq R$. This is trivially the case if the same s-box is used everywhere, as in the AES [4].

[3] Technically this is the *differential branch number*. The *linear branch number* has a different, but closely related, definition [4]. For certain linear transformations, however, the two definitions become equivalent; this is the case for BSPN.

Theorem 2. *If $m \geq 4$, then $\mathcal{B} = 4$ for the BSPN linear transformation.*

Proof. If $\mathbf{X} \neq \mathbf{0}$, then $L(\mathbf{X}) \neq \mathbf{0}$, so $wt_B(\mathbf{X}) \geq 1$ and $wt_B(L(\mathbf{X})) \geq 1$. It follows that when $wt_B(\mathbf{X}) \geq 3$, we have $wt_B(\mathbf{X}) + wt_B(L(\mathbf{X})) \geq 4$, so we only need to consider the cases $wt_B(\mathbf{X}) = 1$ and $wt_B(\mathbf{X}) = 2$.

If $wt_B(\mathbf{X}) = 1$, then $\mathbf{X}$ has a single nonzero byte $\mathbf{b}$ in some position i, so $L(\mathbf{X})$ will contain $\mathbf{0}$ in position i and $\mathbf{b}$ in the remaining $(m-1)$ positions. Therefore $wt_B(L(\mathbf{X})) = (m-1) \geq 3$.

If $wt_B(\mathbf{X}) = 2$, then $\mathbf{X}$ contains nonzero bytes $\mathbf{b}$ and $\mathbf{b}'$ in positions i and i' $(i \neq i')$. If $\mathbf{b} \neq \mathbf{b}'$, then $L(\mathbf{X})$ will contain $\mathbf{b}'$ in position i, $\mathbf{b}$ in position i', and $\mathbf{b} \oplus \mathbf{b}' \neq \mathbf{0}$ in the remaining $(m-2)$ positions, so $wt_B(L(\mathbf{X})) = m \geq 4$. If $\mathbf{b} = \mathbf{b}'$, then, as noted in Remark 1, $\mathbf{X}$ is a fixed point, so $wt_B(L(\mathbf{X})) = 2$ and $wt_B(\mathbf{X}) + wt_B(L(\mathbf{X})) = 4$. □

For $n = 128$ $(m = 16)$, the maximum possible branch number is 17, so clearly L has low diffusion. It is interesting that $\mathcal{B} = 5$ for the AES, but the AES was designed using the *wide-trail strategy* [4], which guarantees good diffusion over four or more rounds. This strategy was not employed for BSPN.

4 Differential Cryptanalysis Concepts

Differential cryptanalysis [3] is a chosen plaintext attack that has been used successfully against many block ciphers. We do not describe the attack here, but we review some standard definitions.

4.1 Differential Probability

For any function $f : \{0,1\}^d \to \{0,1\}^d$, let $\Delta\mathbf{x}, \Delta\mathbf{y}, \mathbf{X} \in \{0,1\}^d$, where $\Delta\mathbf{x}, \Delta\mathbf{y}$ are fixed and $\mathbf{X}$ is a uniformly distributed random variable. The *differential probability* $DP(\Delta\mathbf{x}, \Delta\mathbf{y})$ is defined as

$$DP(\Delta\mathbf{x}, \Delta\mathbf{y}) = \text{Prob}_{\mathbf{X}} \{f(\mathbf{X}) \oplus f(\mathbf{X} \oplus \Delta\mathbf{x}) = \Delta\mathbf{y}\} \tag{2}$$

Here $\Delta\mathbf{x}$ / $\Delta\mathbf{y}$ are called input/output *differences*. It is natural to view DP values as entries in a $2^d \times 2^d$ table.

If f is parameterised by a key, $\mathbf{k}$, we write $DP(\Delta\mathbf{x}, \Delta\mathbf{y}; \mathbf{k})$, and the expected differential probability $EDP(\Delta\mathbf{x}, \Delta\mathbf{y})$ is $E_{\mathbf{K}}[DP(\Delta\mathbf{x}, \Delta\mathbf{y}; \mathbf{K})]$, where $E[\ ]$ denotes expectation and $\mathbf{K}$ is a random variable uniformly distributed over the space of keys.

Differential cryptanalysis exploits relatively large EDP values over $T \leq R$ "core" rounds of the cipher (recall that R denotes the total number of rounds). Attackers often use $T = (R-1)$ or $T = (R-2)$. The *data complexity* of the attack (number of chosen plaintexts required) is given by

$$\frac{c}{EDP^*} \tag{3}$$

where EDP^* is the EDP value being used by the attacker, and c is a small constant (we assume $c = 2$). A cipher designer can claim *provable security* against differential cryptanalysis [14] if the *maximum* EDP value (MEDP) is sufficiently small (for any number of core rounds an attacker would consider) that the data complexity is prohibitively large (e.g., close to 2^n).[4]

4.2 Characteristics and Differentials

For T core rounds, a *differential characteristic* is a vector $\Omega = \langle \Delta\mathbf{x}^1, \ldots, \Delta\mathbf{x}^{T+1} \rangle$, where $\Delta\mathbf{x}^t$ and $\Delta\mathbf{x}^{t+1}$ are input/output differences for round t ($1 \leq t \leq T$). It follows that $\Delta\mathbf{x}^t$ and $\Delta\mathbf{y}^t = L^{-1}(\Delta\mathbf{x}^{t+1})$ are input/output differences for the substitution stage of round t, yielding input/output differences for each s-box S_i^t in round t, denoted $\Delta\mathbf{x}_i^t$ / $\Delta\mathbf{y}_i^t$ ($1 \leq i \leq m$). ($L^{-1} = L$ for BSPN, since L is an involution.)

For a given characteristic, Ω, an s-box with nonzero input/output differences is called *active*. The EDP associated with Ω is a formal product (not the probability of an actual event) defined as

$$EDP(\Omega) = \prod_{t=1}^{T} \prod_{i=1}^{m} DP^{S_i^t}(\Delta\mathbf{x}_i^t, \Delta\mathbf{y}_i^t) \tag{4}$$

where $DP^{S_i^t}(\cdot, \cdot)$ is a DP value for s-box S_i^t. In general, characteristics with larger EDP values have fewer active s-boxes, since a *non*-active s-box always has a DP value equal to 1.

The *differential* $DIFF(\Delta\mathbf{x}, \Delta\mathbf{y})$ is the set of all characteristics whose first difference is $\Delta\mathbf{x}$ and whose last difference is $\Delta\mathbf{y}$. Lai et al. [10] showed that

$$EDP(\Delta\mathbf{x}, \Delta\mathbf{y}) = \sum_{\Omega \in DIFF(\Delta\mathbf{x}, \Delta\mathbf{y})} EDP(\Omega) \tag{5}$$

Remark 2. For most ciphers it is easier to calculate EDP values associated with characteristics than with differentials, so cipher designers will often prove that no high probability characteristics exist, and then claim resistance to differential cryptanalysis on this basis. Knudsen refers to this as *practical security* [8]. This is the approach taken by Youssef et al. in [19].

5 Applying Differential Cryptanalysis to BSPN

In order to look for high probability characteristics and differentials for BSPN, we need at least partial information about the s-boxes. We assume the best case situation for the designer (worst case for the attacker) by using optimal AES-like

[4] The word "provable" is not an absolute guarantee, since there are advanced variations of differential cryptanalysis a designer should consider, e.g., [18]. Also note that "provable security" has other well-established meanings within cryptography [17].

s-boxes. In other words, we assume they belong to the family of s-boxes based on inversion in the finite field $GF(2^8)$:

$$S(\mathbf{x}) = \begin{cases} \mathbf{x}^{-1} & \text{if } \mathbf{x} \neq \mathbf{0} \\ \mathbf{0} & \text{if } \mathbf{x} = \mathbf{0} \end{cases} \tag{6}$$

All such s-boxes are clearly involutional. The AES s-box has the same underlying mapping, but is further modified via an affine transformation (which, among other things, makes it non-involutional). S-boxes in this family were shown by Nyberg [13] to have maximum DP value equal to 2^{-6}, which is the smallest possible maximum for an 8×8 s-box. Further, it is known that every nontrivial row and column of the $2^8 \times 2^8$ s-box DP table has the distribution in Table 1 [16] (where # denotes number of occurrences). For simplicity we will assume that all BSPN s-boxes are identical.

DP	2^{-6}	2^{-7}	0
#	1	126	129

Table 1. Distribution of DP values for any row/column of an AES-like s-box

5.1 Best Characteristics for BSPN

From Remark 1 and the proof of Theorem 2 it is clear that multi-round differential characteristics with the smallest possible number of active s-boxes will involve exactly *two* active s-boxes per round, and the same two s-boxes will be active in each round. In other words, the *best* (highest probability) characteristics for BSPN will have the form in Table 2, where each $\mathbf{z}_t \in \{0,1\}^8 \setminus \mathbf{0}$. (For the sake of computing probabilities, we assume, without loss of generality, that the first two s-boxes in each round are active. In an actual attack the location of the active s-boxes would be varied to allow different bytes of the outermost subkeys to be targeted.) We refer to characteristics of this form as *2A-restricted characteristics*.

To form best characteristics over T core rounds, the (nonzero) value of $\mathbf{z}_1$ can be chosen arbitrarily, and subsequent values of $\mathbf{z}_t$ must be selected so that each active s-box DP value is 2^{-6}. The EDP of the resulting characteristic is $\left(\left(2^{-6}\right)^2\right)^T = 2^{-12T}$. When $T = 5$, this gives an EDP of 2^{-60}, which means that if $T = R - 2$, then BSPN-64 with $R = 7$ rounds can be attacked, since the data complexity is 2^{61} (see (3)). On the other hand, when $R \geq 8$ the data complexity is $\geq 2^{73}$, so the characteristic-based approach fails, i.e., BSPN-64 with $R \geq 8$ is practically secure against differential cryptanalysis.

In contrast, BSPN-128 with $R = 12$ can be attacked, since if $T = R - 2 = 10$, we can construct characteristics with EDP $= 2^{-120}$, corresponding to a data

t	$\Delta\mathbf{x}^t$
1	$\mathbf{z}_1\ \mathbf{z}_1\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \ldots$
2	$\mathbf{z}_2\ \mathbf{z}_2\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \ldots$
3	$\mathbf{z}_3\ \mathbf{z}_3\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \mathbf{0}\ \ldots$
$\vdots$	$\vdots$

Table 2. Structure of 2A-restricted characteristics

complexity of 2^{121}. This compares poorly with the AES, which has a 128-bit block size, for which high probability characteristics can only be found over $T \leq 3$ rounds [4].

5.2 High Probability Differentials for BSPN

We focus on differentials $DIFF(\Delta\mathbf{x}, \Delta\mathbf{y})$ over T core rounds consisting exclusively of 2A-restricted characteristics. (Technically, these are *sub*-differentials.) Therefore $\Delta\mathbf{x} = \langle \mathbf{a}, \mathbf{a}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \ldots \rangle$ and $\Delta\mathbf{y} = \langle \mathbf{b}, \mathbf{b}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \ldots \rangle$, for some (nonzero) $\mathbf{a}, \mathbf{b} \in \{0,1\}^8$. Our goal is to sum the probabilities of these constituent characteristics, thereby obtaining a lower bound on $EDP(\Delta\mathbf{x}, \Delta\mathbf{y})$. It is not hard to see that for $T \geq 2$, the number of 2A-restricted characteristics in a differential over T rounds is $2^{8(T-2)}$, which is exponential in T. However, we can compute the desired lower bounds very efficiently. First we introduce some notation:

- Let $DP_S(\alpha, \beta)$ be the differential probability for the BSPN s-box with input difference α and output difference β (simplification of notation in Section 4.2)
- Let $\mathcal{F}[0 \ldots T_{\mathrm{MAX}}][0 \ldots 255][0 \ldots 255]$ be a 3D array, where T_{MAX} is the maximum number of core rounds of interest to us; our goal is that $\mathcal{F}[T][\mathbf{a}][\mathbf{b}]$ be assigned the sum of the EDP values of all 2A-restricted characteristics over T core rounds with initial difference $\Delta\mathbf{x} = \langle \mathbf{a}, \mathbf{a}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \ldots \rangle$ and final difference $\Delta\mathbf{y} = \langle \mathbf{b}, \mathbf{b}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \ldots \rangle$

Now consider the algorithm in Fig. 1.

Theorem 3. *If $\mathcal{F}[\cdot][\cdot][\cdot]$ is filled using the algorithm given in Fig. 1, then for $1 \leq T \leq T_{\mathrm{MAX}}$ and $\mathbf{a}, \mathbf{b} \in \{0,1\}^8$, $\mathcal{F}[T][\mathbf{a}][\mathbf{b}]$ contains the sum of the probabilities of all 2A-restricted characteristics over T core rounds with initial difference $\Delta\mathbf{x} = \langle \mathbf{a}, \mathbf{a}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \ldots \rangle$ and final difference $\Delta\mathbf{y} = \langle \mathbf{b}, \mathbf{b}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \ldots \rangle$.*

Proof. The correctness of the algorithm is an immediate consequence of the following relationship, for $T \geq 2$ and $\Delta\mathbf{x}, \Delta\mathbf{y} \in \{0,1\}^n$:

$$EDP^{[1\ldots T]}(\Delta\mathbf{x}, \Delta\mathbf{y}) = \sum_{\Delta\mathbf{z} \in \{0,1\}^n} EDP^{[1\ldots(T-1)]}(\Delta\mathbf{x}, \Delta\mathbf{z}) \cdot EDP^{T}(\Delta\mathbf{z}, \Delta\mathbf{y}) \quad (7)$$

- initialize all entries of $\mathcal{F}[\cdot][\cdot][\cdot]$ to 0

- set $\mathcal{F}[0][\mathbf{x}][\mathbf{x}] = 1 \quad \text{for } \mathbf{x} = 0, \ldots, 255$

for $T = 1, \ldots, T_{\text{MAX}}$
  for $\Delta\mathbf{x} = 1, \ldots, 255$
    for $\Delta\mathbf{y} = 1, \ldots, 255$
      for $\mathbf{z} = 1, \ldots, 255$
        $\mathcal{F}[T][\Delta\mathbf{x}][\Delta\mathbf{y}] \ += \ \mathcal{F}[T-1][\Delta\mathbf{x}][\mathbf{z}] \times (DP_S(\mathbf{z}, \Delta\mathbf{y}))^2$

Fig. 1. Algorithm for computing lower bound on EDP values of differentials

where $EDP^{[i \ldots j]}$ is an EDP value over rounds $i \ldots j$ (inclusive), and EDP^T is a 1-round EDP value for round T. In turn, (7) follows directly from (4) and (5). The squared term $(DP_S(\mathbf{z}, \Delta\mathbf{y}))^2$ is a consequence of activating two neighboring s-boxes in each round, assigning them identical input and output differences. □

Remark 3. The innermost assignment statement in Fig. 1 is executed $T_{\text{MAX}} \cdot 2^{24}$ times, which is negligible on a standard computer for any reasonable value of T_{MAX}.

5.3 Computational Results

We ran the algorithm in Fig. 1 for $1 \leq T \leq 18$ using:

- an involutional s-box defined by inversion in $GF(2^8)$, as in (6) — there are 30 irreducible degree-8 polynomials over $\mathbf{GF}(2)$ (see [11]), and all 30 resulting s-boxes yielded identical lower bounds
- the AES s-box — this non-involutional s-box was used for comparison purposes, since it is considered something of a "gold standard"

The computational results are given in Table 3. For each value of T, we list the largest entry in $\mathcal{F}[T][\cdot][\cdot]$ for each of the two s-box choices. Note that the only differences resulting from the s-box selection occur when $T = 2$ and $T = 3$.

If we assume that $R = T+2$, then BSPN-64 can be attacked using differential cryptanalysis for $R \leq 9$, since $EDP \geq 2^{-56.84}$ for $T = 7$, corresponding to a data complexity of approximately 2^{58}. This contradicts the claim in [19] that 9-round BSPN-64 is secure against differential cryptanalysis.[5] Furthermore, BSPN-128 can be attacked for $R \leq 18$, since $EDP \geq 2^{-119.64}$ for $T = 16$, corresponding to a data complexity of approximately 2^{121}. This is significantly weaker than the AES, for which all EDP values over $T \geq 4$ rounds are upper bounded by 1.14×2^{-111} [7].

[5] Technically the authors assert resistance to differential cryptanalysis for $R = 8$ and $T = R - 1$, but this extends to $R = 9$ when $T = R - 2$.

T	$GF(2^8)$ inversion s-box	AES s-box
1	2^{-12}	2^{-12}
2	$2^{-20.85}$	$2^{-21.51}$
3	$2^{-28.85}$	$2^{-28.90}$
4	$2^{-35.90}$	$2^{-35.90}$
5	$2^{-42.88}$	$2^{-42.88}$
6	$2^{-49.86}$	$2^{-49.86}$
7	$2^{-56.84}$	$2^{-56.84}$
8	$2^{-63.82}$	$2^{-63.82}$
9	$2^{-70.79}$	$2^{-70.79}$
10	$2^{-77.77}$	$2^{-77.77}$
11	$2^{-84.75}$	$2^{-84.75}$
12	$2^{-91.73}$	$2^{-91.73}$
13	$2^{-98.70}$	$2^{-98.70}$
14	$2^{-105.68}$	$2^{-105.68}$
15	$2^{-112.66}$	$2^{-112.66}$
16	$2^{-119.64}$	$2^{-119.64}$
17	$2^{-126.61}$	$2^{-126.61}$
18	$2^{-133.59}$	$2^{-133.59}$

Table 3. Lower bounds on maximum EDP values over T core BSPN rounds

6 Conclusion

By considering properties of the BSPN linear transformation, we find high probability differentials over relatively large numbers of rounds, demonstrating that this lightweight cipher structure has significant vulnerabilities to differential cryptanalysis.

Acknowledgment

This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

1. Barreto, P.S.L.M., Rijmen, V.: The Khazad Legacy-Level Block Cipher. In: Proceedings of First Open NESSIE Workshop (2000)
2. Barreto, P.S.L.M., Simplício, M.A., Jr.: CURUPIRA, A Block Cipher for Constrained Platforms. In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC2007) (2007)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology 4(1), 3–72 (1991)
4. Daemen, J., Rijmen, V.: The Design of Rijndael: AES—The Advanced Encryption Standard. Springer, Heidelberg (2002)
5. Heys, H.M., Tavares, S.E.: Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis. J. Cryptology 9(1), 1–19 (1996)
6. Hong, S, Lee, S., Lim, J., Sung, J., Cheon, D.: Provable Security Against Differential and Linear Cryptanalysis for the SPN Structure. In: Goos, G., Hartmanis, J., van Leeuwen, J., Schneier, B. (eds.) Fast Software Encryption (FSE 2000). LNCS, vol. 1978, pp. 273–283. Springer, Heidelberg (2001)
7. Keliher, L., Sui, J.: Exact Maximum Expected Differential and Linear Probability for 2-round Advanced Encryption Standard IET Information Security 1(2), 53–57 (2007)
8. Knudsen, L.: Practically Secure Feistel Ciphers. In: Anderson, R. (ed.) Fast Software Encryption (FSE'93). LNCS, vol. 809, pp. 211–221. Springer, Heidelberg (1994)
9. Kusagur, R., Leelavathi, G.: Hardware Implementation of Involutional SPN Block Ciphers. Int. J. Eng. Adv. Tech. (IJEAT) 3(1), 2249–8958 (2013)
10. Lai, X., Massey, J., Murphy, S.: Markov Ciphers and Differential Cryptanalysis. In: Davies, D.W. (ed.) Advances in Cryptology—EUROCRYPT'91. LNCS, vol. 547, pp. 17–38. Springer, Heidelberg (1991)
11. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and their Applications, Revised Edition. Cambridge University Press, Cambridge (1994)
12. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, E. (ed.) Advances in Cryptology—EUROCRYPT'93. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
13. Nyberg, K.: Differentially Uniform Mappings for Cryptography. In: Helleseth, T. (ed.) Advances in Cryptology—EUROCRYPT'93. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994)
14. Nyberg, K., Knudsen, L.: Provable Security Against a Differential Attack. J. Cryptology 8(1), 27–37 (1995)
15. Paar, C., Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Springer, Heidelberg (2010)
16. Park, S., Sung, S.H., Lee, S., Lim, J.: Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES. In: Johansson, T. (ed.) Fast Software Encryption (FSE 2003). LNCS, vol. 2887, pp. 247–260. Springer, Heidelberg (2003)
17. Stinson, D.R.: Cryptography: Theory and Practice, Third Edition. Chapman & Hall/CRC, Boca Raton (2006)
18. Wang, M., Sun, Y., Tischhauser, E., Preneel, B.: A Model for Structure Attacks, with Applications to PRESENT and Serpent. In: Canteaut, A. (ed.) Fast Software Encryption (FSE 2012). LNCS, vol. 7549, pp. 49-68. Springer, Heidelberg (2012)
19. Youssef, A.M., Tavares, S.E., Heys, H.M.: A New Class of Substitution-Permutation Networks. In: Proceedings of Third Annual Workshop on Selected Areas in Cryptography (SAC'96), pp. 132–147 (1996)

20. Zhang, X., Heys, H.M., Li, C.: Energy Efficiency of Encryption Schemes Applied to Wireless Sensor Networks. Security and Communication Networks 5(7), 789-808 (2012)
21. Zhang, X., Heys, H.M., Li, C.: FPGA Implementation and Energy Cost Analysis of Two Light-Weight Involutional Block Ciphers Targeted to Wireless Sensor Networks. Mobile Netw. Appl. 18, 222–234 (2013)