Weak Subtweakeys in SKINNY

Daniël Kuijsters, Denise Verbakel, and Joan Daemen

Radboud University, The Netherlands
joan.daemen@ru.nl, denise.verbakel@ru.nl, Daniel.Kuijsters@ru.nl

Abstract. Lightweight cryptography is characterized by the need for low implementation cost, while still providing sufficient security. This requires careful analysis of building blocks and their composition.
SKINNY is an ISO/IEC standardized family of tweakable block ciphers and is used in the NIST lightweight cryptography standardization process finalist Romulus. We present non-trivial linear approximations of two-round SKINNY that have correlation one or minus one and that hold for a large fraction of all round tweakeys. Moreover, we show how these could have been avoided.

Keywords: cryptanalysis, lightweight symmetric cryptography, block ciphers

1 Introduction

In 2018, NIST initiated a process for the standardization of *lightweight cryptography* [14], i.e., cryptography that is suitable for use in constrained environments. A typical cryptographic primitive is built by composing a relatively simple round function with itself a number of times. To choose this number of rounds, a trade-off is made between the security margin and the performance.

One of the finalists in this standardization process is the Romulus [8] scheme for authenticated encryption with associated data. This scheme is based on the ISO/IEC 18033-7:2022 [1] standardized lightweight tweakable block cipher SKINNY [2].

Two of the most important techniques for the analysis of symmetric primitives are differential [3] and linear cryptanalysis [12]. To reason about the security against these attacks, the designers of SKINNY have computed lower bounds on the number of *active* S-boxes in linear and differential trails. However, at the end of Section 4.1 of [2] they write:

> The above bounds are for single characteristic, thus it will be interesting to take a look at differentials and linear hulls. Being a rather complex task, we leave this as future work.

Building on the work of [4], [15] investigated clustering of two-round trails in SKINNY and in this paper we report and explain its most striking finding.

By examination of two rounds, we argue why it is sensible to look at the substructure that consists of a double S-box with a subtweakey addition in between.

We study this double S-box structure both from an algebraic point of view and a statistical point of view. We found that for some subtweakeys there are non-trivial *perfect* linear approximations, i.e., that have correlation one or minus one. We present them in this paper together with their constituent linear trails. For both the version of SKINNY that uses the 4-bit S-box and the version that uses the 8-bit S-box, we present one non-trivial perfect linear approximation of the double S-box structure that holds for 1/4 of all subtweakeys and four non-trivial perfect linear approximations that each hold for 1/16 of all subtweakeys. In total, 1/4 of the subtweakeys is *weak*, i.e., it has an associated non-trivial perfect linear approximation. The linear approximations of the double S-box structure can be extended to linear approximations of the full two rounds of SKINNY. From the fact that the double S-box structure appears in four different locations, it follows that $1-(3/4)^4 \approx 68\%$ of the round tweakeys is weak, i.e., two rounds have a non-trivial perfect linear approximation.

Despite requiring more resources to compute, this shows that for many round tweakeys two rounds are weaker than a single round. Moreover, this also shows that the bounds on the squared correlations of linear approximations that are based on counting the number of active S-boxes in linear trails may not be readily assumed.

We conclude by showing how this undesired property could have easily been avoided by composing the S-box with a permutation of its output bits, which has a negligible impact on the implementation cost.

1.1 Outline and Contributions

In Section 2 we remind the reader of the parts of the SKINNY block cipher specification that are relevant to our analysis. We argue why it is reasonable to study the double S-box structure and explore its algebraic properties. Section 3 serves as a reminder for the reader of the relevant statistical analysis tools of linear cryptanalysis. Section 4 presents our findings from the study of the linear trails of the double S-box structure. We show how the problem could have been avoided in Section 5. Finally, we state the main message behind our findings in Section 6.

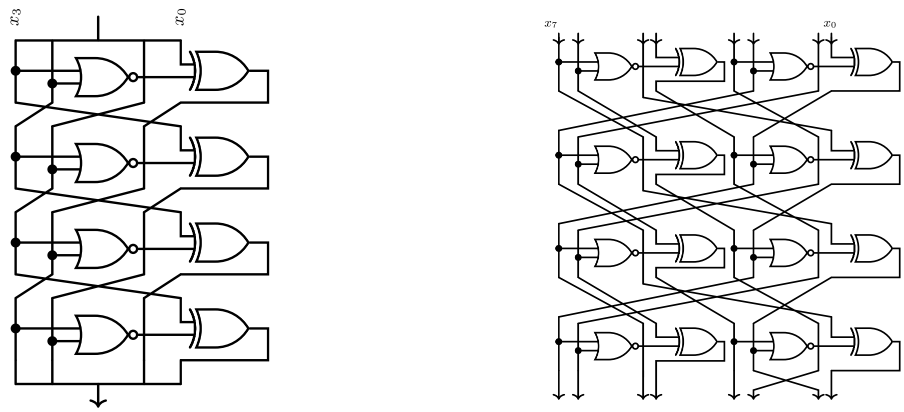
2 The SKINNY Family of Block Ciphers

SKINNY [2] is a family of tweakable block ciphers. A member of the SKINNY family is denoted by SKINNY-b-t, where b denotes the block size and t denotes the size of the tweakey [10]. The block size b is equal to 64 bits or 128 bits. The tweakey t is b, $2b$, or $3b$ bits.

The AES-like [7] data path of the SKINNY block cipher is the repeated application of a round function on a representation of the state as a four by four array of m-bit vectors, where m is either four or eight.

Pairs (i, j) comprising a row index i and column index j with $0 \leq i, j \leq 3$ are used to index into the state array. For example, $(0, 0)$ refers to the entry in the top left and $(3,3)$ to the entry in the bottom right. The m-bit entries $x^{(i,j)}$ are of the form $(x_{m-1}^{(i,j)}, \ldots, x_0^{(i,j)})$.

The round function consists of the following steps in sequence: `SubCells`, `AddConstants`, `AddRoundTweakey`, `ShiftRows`, and `MixColumns`.



(a) 4-bit S-box S_4. **(b)** 8-bit S-box S_8.

Fig. 1: Circuit-level representation of S_4 and S_8. (Figure adapted from [9].)

Figure 1 shows the circuit-level view of the S-boxes that are used in the `SubCells` step of SKINNY.

The block matrix that is used in the `MixColumns` step is equal to

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} ,$$

where 0 denotes the zero matrix of size $m \times m$ and 1 denotes the identity matrix of size m. Each of the four columns of the state is multiplied by M in parallel.

The composition of two rounds is depicted in Figure 2.

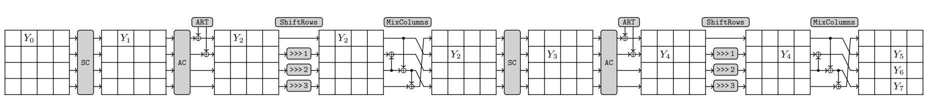


Fig. 2: Two-round SKINNY. (Figure adapted from [9].)

Consider the entry of the state at position $(0,1)$ in Figure 2. It is of the form $Y_0 = x^{(0,1)}$. This expression propagates through the step functions of two rounds and leads to the following intermediate expressions:

$$
\begin{aligned}
Y_1 &= \mathrm{S}_m(x^{(0,1)}) \\
Y_2 &= \mathrm{S}_m(x^{(0,1)}) + k^{(0)} \\
Y_3 &= \mathrm{S}_m(\mathrm{S}_m(x^{(0,1)}) + k^{(0)}) \\
Y_4 &= \mathrm{S}_m(\mathrm{S}_m(x^{(0,1)}) + k^{(0)}) + k^{(1)} \\
Y_5 + Y_6 + Y_7 &= \mathrm{S}_m(\mathrm{S}_m(x^{(0,1)}) + k^{(0)}) + k^{(1)} \,,
\end{aligned}
$$

Here, $k^{(0)}$ and $k^{(1)}$ are subtweakeys, which are linear expressions in the cipher key and tweak bits (assuming that the tweakey does not consist entirely of cipher key bits). These linear expressions depend on the round number, but they are known to the attacker. The tweak can be chosen by the attacker and the cipher key is unknown to the attacker. By choosing the tweak, the attacker can attain all values of $k^{(0)}$ and $k^{(1)}$ for a given cipher key.

The final expression shows that the sum of certain triples of state entries at the output of the second round is equal to the application of two S-boxes and subtweakey additions to a single entry of the input to the first round. The second subtweakey addition does not have an important influence on the statistical properties of this expression, so we remove it and turn our attention to the properties of the function

$$\mathrm{D}_{m,k} = \mathrm{S}_m \circ \mathrm{T}_{m,k} \circ \mathrm{S}_m \,,$$

where $\mathrm{T}_{m,k}$ is defined by $x \mapsto x + k$ for $x \in \mathbb{F}_2^m$. We will refer to $\mathrm{D}_{m,k}$ as the *double S-box structure*.

For reasons of simplicity, we study SKINNY-64-t, i.e., the version with 4-bit S-boxes. However, our results can be extended to the case of 8-bit S-boxes as well.

By concatenating two copies of the 4-bit S-box circuit with a subtweakey addition layer in between we obtain the circuit-level view of $\mathrm{D}_{4,k}$ that is depicted in Figure 3. Consider the input x_1. It passes through an XOR gate, the subtweakey addition layer, and finally through a second XOR gate before being routed to the third component of the output of $\mathrm{D}_{4,k}$. If $k_3 = k_2 = 0$, then the XOR gates cancel each other out and the third component of $\mathrm{D}_{4,k}$ is equal to $x_1 + k_0$. This observation does not depend on the value of k_1.

Let us now derive this same result in an algebraic way. Of course, we could compute the algebraic expression for $\mathrm{D}_{4,k}$ directly, but it is more insightful to study the S-box and its inverse.

The 4-bit S-box is of the form

$$\mathrm{S}_4 = \mathrm{N}_4 \circ \mathrm{L}_4 \circ \mathrm{N}_4 \circ \mathrm{L}_4 \circ \mathrm{N}_4 \circ \mathrm{L}_4 \circ \mathrm{N}_4$$

where

$$
\begin{aligned}
\mathrm{N}_4(x_3, x_2, x_1, x_0) &= (x_3, x_2, x_1, x_2 x_3 + x_0 + x_2 + x_3 + 1) \quad \text{and} \\
\mathrm{L}_4(x_3, x_2, x_1, x_0) &= (x_2, x_1, x_0, x_3) \,.
\end{aligned}
$$

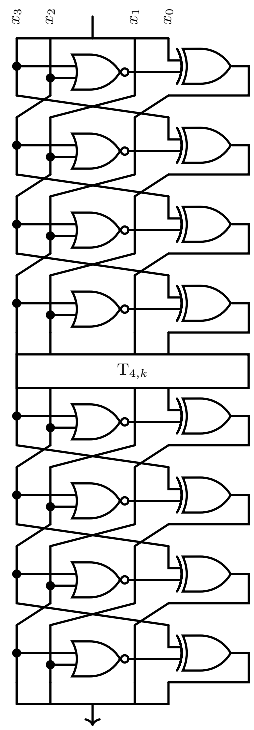


Fig. 3: Circuit-level representation of $D_{4,k}$. (Figure adapted from [9].)

It follows that $S_4 = (S_4^{(3)}, S_4^{(2)}, S_4^{(1)}, S_4^{(0)})$ where

$$\begin{aligned}
S_4^{(3)} &= x_2x_3 + x_0 + x_2 + x_3 + 1 \\
S_4^{(2)} &= x_1x_2 + x_1 + x_2 + x_3 + 1 \\
S_4^{(1)} &= x_1x_2x_3 + x_0x_1 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_3 \\
S_4^{(0)} &= x_0x_1x_2 + x_1x_2x_3 + x_0x_1 + x_0x_2 + x_0x_3 + x_1x_3 + x_1 + x_2 + x_3
\end{aligned}$$

The S-box has a generalized Feistel structure [13]. Therefore, it is not difficult to deduce that the inverse of $T_{4,k} \circ S_4$ is of the form

$$I_{4,k} = (T_{4,k} \circ S_4)^{-1} = N_4 \circ R_4 \circ N_4 \circ R_4 \circ N_4 \circ R_4 \circ N_4 \circ T_{4,k}\,,$$

where $\mathrm{R}_4(x_3, x_2, x_1, x_0) = (x_0, x_3, x_2, x_1)$. It follows that $I_{4,k}$ is of the form $(I_{4,k}^{(3)}, I_{4,k}^{(2)}, I_{4,k}^{(1)}, I_{4,k}^{(0)})$ where

$$
\begin{aligned}
I_{4,k}^{(3)} &= x_1x_2x_3 + x_0x_1 + x_0x_3 + x_1x_2(k_3+1) + x_1x_3(k_2+1) + x_2x_3k_1 \\
&\quad + x_1(k_2k_3 + k_0 + k_2 + k_3) + x_2(k_1k_3 + k_1 + 1) + x_3(k_1k_2 + k_0 + k_1 + 1) \\
&\quad + x_0(k_1 + k_3) + k_1k_2k_3 + k_0k_1 + k_0k_3 + k_1k_2 + k_1k_3 + k_2 + k_3\,, \\
I_{4,k}^{(2)} &= x_0x_3 + x_2x_3 + x_0(k_3+1) + x_2(k_3+1) + x_3(k_0+k_2) + x_1 + k_0k_3 + k_2k_3 \\
&\quad + k_0 + k_1 + k_2\,, \\
I_{4,k}^{(1)} &= x_2x_3 + x_2(k_3+1) + x_3(k_2+1) + x_0 + k_2k_3 + k_0 + k_2 + k_3 + 1\,, \\
I_{4,k}^{(0)} &= x_0x_2x_3 + x_1x_2x_3 + x_0x_2(k_3+1) + x_0x_3k_2 + x_1x_2k_3 + x_1x_3(k_2+1) \\
&\quad + x_2x_3(k_0+k_1) + x_0x_1 + x_0(k_2k_3 + k_1 + k_2 + 1) + x_1(k_2k_3 + k_0 + k_3 + 1) \\
&\quad + x_2(k_0k_3 + k_1k_3 + k_0 + 1) + x_3(k_0k_2 + k_1k_2 + k_1) + k_0k_2k_3 + k_1k_2k_3 \\
&\quad + k_0k_1 + k_0k_2 + k_1k_3 + k_0 + k_1 + k_2 + 1\,.
\end{aligned}
$$

We observe that if $k_3 = k_2 = 0$, then the component $I_{4,k}^{(1)}$ differs from $\mathrm{S}_4^{(3)}$ by the constant k_0 for any value of k_1. This implies that $\mathrm{D}_{4,(0,0,k_1,k_0)}^{(3)} = x_1 + k_0$.

3 Linear Cryptanalysis

To analyze $\mathrm{D}_{m,k}$ in more detail, we use the statistical framework of linear cryptanalysis [6, 12].

The important concept here is a *linear approximation*, i.e., an ordered pair of linear masks $(u, v) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$ that determine linear combinations of output and input bits, respectively. A mask u defines a *linear functional*

$$x \mapsto u^\top x = u_0x_0 + \cdots + u_{m-1}x_{m-1}\,.$$

We measure the quality of a linear approximation with the correlation between the linear functionals defined by the masks.

Definition 1. *The (signed)* correlation *between the linear functional defined by the mask $u \in \mathbb{F}_2^m$ at the output of a function $G\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ and the linear functional defined by the mask $v \in \mathbb{F}_2^m$ at its input is defined as*

$$\mathrm{C_G}(u, v) = \frac{1}{2^m} \sum_{x \in \mathbb{F}_2^m} (-1)^{u^\top \mathrm{G}(x) + v^\top x}\,.$$

The $2^m \times 2^m$ matrix $\mathrm{C_G}$ with entries $\mathrm{C_G}(u, v)$ is called the *correlation matrix* of the function G. We call a linear approximation with a correlation of one or minus one *perfect*.

In addition to specifying masks at the input and output of $\mathrm{D}_{m,k}$, we may also specify intermediate masks.

Definition 2. *A sequence* $(u, v, w) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2^m$ *is called a* linear trail *of* $\mathrm{D}_{m,k}$ *if it satisfies the following conditions:*

1. $\mathrm{C}_{\mathrm{S}_m}(u, v) \neq 0$;
2. $\mathrm{C}_{\mathrm{S}_m}(v, w) \neq 0$.

Each of the trails contributes to the correlation of the linear approximation.

Definition 3. *The* correlation contribution *of a linear trail* (u, v, w) *over* $\mathrm{D}_{m,k}$ *equals*

$$\mathrm{C}_{\mathrm{D}_{m,k}}(u, v, w) = (-1)^{v^\top k}\, \mathrm{C}_{\mathrm{S}_m}(u, v)\, \mathrm{C}_{\mathrm{S}_m}(v, w)\,.$$

From the theory of correlation matrices [6], it follows that

$$\begin{aligned}\mathrm{C}_{\mathrm{D}_{m,k}}(u, v) &= \sum_{v \in \mathbb{F}_2^m} \mathrm{C}_{\mathrm{D}_{m,k}}(u, v, w)\\ &= \sum_{v \in \mathbb{F}_2^m} (-1)^{v^\top k}\, \mathrm{C}_{\mathrm{S}_m}(u, v)\, \mathrm{C}_{\mathrm{S}_m}(v, w)\,.\end{aligned}$$

4 Linear Trails of $\mathbf{S}_m \circ \mathbf{T}_{m,k} \circ \mathbf{S}_m$

We can now translate the observations from Section 2 into the language of linear cryptanalysis. The observations state that the linear approximation $(\mathtt{1000}, \mathtt{0010})$ of $\mathrm{D}_{4,(0,0,k_1,k_0)}$ is perfect for all $k_0, k_1 \in \mathbb{F}_2$.

One way of seeing this is directly from the fact that

$$\begin{aligned}(\mathtt{1000})^\top\, \mathrm{D}_{4,(0,0,k_1,k_0)} &= \mathrm{D}^{(3)}_{4,(0,0,k_1,k_0)}\\ &= x_1 + k_0\\ &= (\mathtt{0010})^\top x + k_0\,.\end{aligned}$$

Hence, the correlation is one if k_0 is zero and minus one otherwise.

An alternative view is the following. Due to the equivalence of vectorial Boolean functions and their correlation matrices [6], equality of $\mathrm{S}_4^{(3)}$ and $I_{4,k}^{(1)}$ implies equality of row $\mathtt{1000}$ of $\mathrm{C}_{\mathrm{S}_4}$ and row $\mathtt{0010}$ of $\mathrm{C}_{I_{4,k}}$. The latter corresponds to column $\mathtt{0010}$ of $C_{\mathrm{T}_{4,k} \circ \mathrm{S}_4}$. These are exactly the two vectors that we need to multiply in order to compute $\mathrm{C}_{\mathrm{D}_{4,k}}(\mathtt{1000}, \mathtt{0010})$. Using the orthogonality relations [11], it is not difficult to show that this correlation is either one or minus one, depending on the constant difference between $\mathrm{S}_4^{(3)}$ and $I_{4,k}^{(1)}$, which only influences the sign.

In general, we have computed all the non-trivial perfect linear approximations for each of the 2^m subtweakeys. This was accomplished by considering all the possible linear trails over $\mathrm{D}_{4,k}$. The results are found in Table 1 for the case $m = 4$, i.e., for the 4-bit S-box, and in Table 2 for the case $m = 8$, i.e., for the 8-bit S-box. The first column lists the output masks and the third column lists the input masks. An asterisk denotes that the linear approximation holds for any subtweakey bit in that position. It turns out that in both cases such linear approximations exist for a quarter of the subtweakeys. We call subtweakeys for which this property holds *weak*.

Consider a fixed subtweakey. If (u_1, w_1) and (u_2, w_2) are two perfect linear approximations, then their sum $(u_1 + u_2, w_1 + w_2)$ is again a perfect linear approximation, as evidenced by the tables. Moreover, the pair $(0, 0)$ is always a perfect linear approximation. It follows that the perfect linear approximations for a fixed subtweakey form a linear subspace of $\mathbb{F}_2^m \times \mathbb{F}_2^m$.

5 Patching the Problem

To patch the problem, we search within a specific subset of S-boxes that are *permutation equivalent* [5] to the original.

Definition 4. *Two functions* $\mathrm{F}\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ *and* $\mathrm{G}\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ *are called* permutation equivalent *if there exist bit permutations* σ *and* τ *such that*

$$\mathrm{F} = \tau \circ \mathrm{G} \circ \sigma\,.$$

A bit permutation τ *is a permutation of* $\{0, \ldots, m-1\}$ *that has been extended to* $\mathbb{F}_2^m$ *by*

$$(x_{m-1}, \ldots, x_0) \mapsto (x_{\tau(m-1)}, \ldots, x_{\tau(0)})\,.$$

Many of the cryptographic properties of an S-box are preserved by permutation equivalence, e.g., the algebraic degree, the differential uniformity, the linearity, and the branch number. Moreover, the impact of a bit permutation on the implementation cost is negligible. For example, in hardware it amounts to rewiring of the signals. We have restricted our search to those permutation equivalent S-boxes for which σ is the identity.

Any bit permutation applied to the output bits of S_4 permutes the columns of its correlation matrix. Indeed, we have

$$\mathrm{C}_{\mathrm{G}}(u, v) = \mathrm{C}_{\mathrm{S}_4}(u, \tau^{-1}(v))\,.$$

Table 3 lists the bit permutations τ and the ratio of subtweakeys for which there exist non-trivial perfect linear approximations. For example, the row "(x_2, x_1, x_0, x_3) 0" corresponds to the bit permutation $\tau = \mathrm{L}_4$ for which no subtweakeys are weak. It turns out that there exist many permutation equivalent S-boxes for which the double S-box structure does not have non-trivial perfect linear approximations for any subtweakey.

Similarly, for the 8-bit S-box we found that there exist many permutation equivalent S-boxes for which there exist no non-trivial perfect linear approximations. An example of such an S-box is obtained by applying the bit permutation $\tau(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) = (x_7, x_5, x_6, x_4, x_3, x_2, x_1, x_0)$. Because the number of possible bit permutations is large, we did not include them all here.

Table 1: Perfect linear approximations of $\mathrm{S}_4 \circ \mathrm{T}_{4,k} \circ \mathrm{S}_4$ and their constituent linear trails.

output mask u	intermediate mask v	input mask w	subtweakey k	$\mathrm{C}_{\mathrm{D}_{4,k}}(u,w)$	$\mathrm{C}_{\mathrm{T}_{4,k}}(v,v)$	$\mathrm{C}_{\mathrm{S}}(u,v)$	$\mathrm{C}_{\mathrm{S}}(v,w)$
1000	0001	0010	$00{*}k_0$	$(-1)^{k_0}$	$(-1)^{k_0}$	$1/2$	$1/2$
	0101				$(-1)^{k_0}$	$-1/2$	$-1/2$
	1001				$(-1)^{k_0}$	$-1/2$	$-1/2$
	1101				$(-1)^{k_0}$	$-1/2$	$-1/2$
1010	0001	1110	0001	1	-1	$-1/4$	$1/4$
	0011				-1	$1/4$	$-1/4$
	0100				1	$-1/2$	$-1/2$
	0101				-1	$1/4$	$-1/4$
	0110				1	$-1/2$	$-1/2$
	0111				-1	$-1/4$	$1/4$
	1001				-1	$-1/4$	$1/4$
	1011				-1	$1/4$	$-1/4$
	1101				-1	$-1/4$	$1/4$
	1111				-1	$1/4$	$-1/4$
0010	0001	1100	0001	-1	-1	$1/4$	$1/4$
	0011				-1	$1/4$	$1/4$
	0100				1	$1/2$	$-1/2$
	0101				-1	$-1/4$	$-1/4$
	0110				1	$-1/2$	$1/2$
	0111				-1	$-1/4$	$-1/4$
	1001				-1	$1/4$	$1/4$
	1011				-1	$1/4$	$1/4$
	1101				-1	$1/4$	$1/4$
	1111				-1	$1/4$	$1/4$
0010	0001	1110	0011	-1	-1	$1/4$	$1/4$
	0011				1	$1/4$	$-1/4$
	0100				1	$1/2$	$-1/2$
	0101				-1	$-1/4$	$-1/4$
	0110				-1	$-1/2$	$-1/2$
	0111				1	$-1/4$	$1/4$
	1001				-1	$1/4$	$1/4$
	1011				1	$1/4$	$-1/4$
	1101				-1	$1/4$	$1/4$
	1111				1	$1/4$	$-1/4$
1010	0001	1100	0011	1	-1	$-1/4$	$1/4$
	0011				1	$1/4$	$1/4$
	0100				1	$-1/2$	$-1/2$
	0101				-1	$1/4$	$-1/4$
	0110				-1	$-1/2$	$1/2$
	0111				1	$-1/4$	$-1/4$
	1001				-1	$-1/4$	$1/4$
	1011				1	$1/4$	$1/4$
	1101				-1	$-1/4$	$1/4$
	1111				1	$1/4$	$1/4$

Table 2: Perfect linear approximations of $\mathrm{S}_8 \circ \mathrm{T}_{8,k} \circ \mathrm{S}_8$ and their constituent linear trails.

output mask u	intermediate mask v	input mask w	subtweakey k	$\mathrm{C}_{\mathrm{D}_{8,k}}(u,w)$	$\mathrm{C}_{\mathrm{T}_{8,k}}(v,v)$	$\mathrm{C}_{\mathrm{S}}(u,v)$	$\mathrm{C}_{\mathrm{S}}(v,w)$
01000000	00010000	00001000	$00{*}k_4{*}{*}{*}{*}$	$(-1)^{k_4}$	$(-1)^{k_4}$	$1/2$	$1/2$
	01010000				$(-1)^{k_4}$	$-1/2$	$-1/2$
	10010000				$(-1)^{k_4}$	$-1/2$	$-1/2$
	11010000				$(-1)^{k_4}$	$-1/2$	$-1/2$
10010000	00001000	00000010	0001****	-1	1	$-1/2$	$1/2$
	00011000				-1	$-1/4$	$-1/4$
	00101000				1	$1/2$	$-1/2$
	00111000				-1	$-1/4$	$-1/4$
	01011000				-1	$1/4$	$1/4$
	01111000				-1	$1/4$	$1/4$
	10011000				-1	$1/4$	$1/4$
	10111000				-1	$1/4$	$1/4$
	11011000				-1	$1/4$	$1/4$
	11111000				-1	$1/4$	$1/4$
11010000	00001000	00001010	0001****	1	1	$-1/2$	$-1/2$
	00011000				-1	$-1/4$	$1/4$
	00101000				1	$-1/2$	$-1/2$
	00111000				-1	$1/4$	$-1/4$
	01011000				-1	$1/4$	$-1/4$
	01111000				-1	$-1/4$	$1/4$
	10011000				-1	$1/4$	$-1/4$
	10111000				-1	$-1/4$	$1/4$
	11011000				-1	$1/4$	$-1/4$
	11111000				-1	$-1/4$	$1/4$
10010000	00001000	00001010	0011****	1	1	$-1/2$	$-1/2$
	00011000				-1	$-1/4$	$1/4$
	00101000				-1	$1/2$	$-1/2$
	00111000				1	$-1/4$	$-1/4$
	01011000				-1	$1/4$	$-1/4$
	01111000				1	$1/4$	$1/4$
	10011000				-1	$1/4$	$-1/4$
	10111000				1	$1/4$	$1/4$
	11011000				-1	$1/4$	$-1/4$
	11111000				1	$1/4$	$1/4$
11010000	00001000	00000010	0011****	-1	1	$-1/2$	$1/2$
	00011000				-1	$-1/4$	$-1/4$
	00101000				-1	$-1/2$	$-1/2$
	00111000				1	$1/4$	$-1/4$
	01011000				-1	$1/4$	$1/4$
	01111000				1	$-1/4$	$1/4$
	10011000				-1	$1/4$	$1/4$
	10111000				1	$-1/4$	$1/4$
	11011000				-1	$1/4$	$1/4$
	11111000				1	$-1/4$	$1/4$

Table 3: Permutation equivalent S-boxes and their ratio of weak subtweakeys.

$\tau(x_3, x_2, x_1, x_0)$	Ratio of weak subtweakeys
(x_3, x_2, x_1, x_0)	4/16
(x_2, x_3, x_1, x_0)	6/16
(x_3, x_1, x_2, x_0)	0
(x_2, x_1, x_3, x_0)	0
(x_1, x_3, x_2, x_0)	0
(x_1, x_2, x_3, x_0)	2/16
(x_3, x_2, x_0, x_1)	0
(x_2, x_3, x_0, x_1)	0
(x_3, x_1, x_0, x_2)	0
(x_2, x_1, x_0, x_3)	0
(x_1, x_3, x_0, x_2)	5/16
(x_1, x_2, x_0, x_3)	0
(x_3, x_0, x_2, x_1)	7/16
(x_2, x_0, x_3, x_1)	0
(x_3, x_0, x_1, x_2)	0
(x_2, x_0, x_1, x_3)	0
(x_1, x_0, x_3, x_2)	6/16
(x_1, x_0, x_2, x_3)	0
(x_0, x_3, x_2, x_1)	10/16
(x_0, x_2, x_3, x_1)	8/16
(x_0, x_3, x_1, x_2)	0
(x_0, x_2, x_1, x_3)	0
(x_0, x_1, x_3, x_2)	0
(x_0, x_1, x_2, x_3)	0

6 Conclusion

The main message that we want to communicate is that the composition of individually strong cryptographic functions may produce a weaker function for a large subset of the round tweakey space. In SKINNY, this weakness holds for *any* cipher key, because the subtweakeys are computed from the both the cipher key and the tweak, the latter of which is chosen by the user. In small structures, such undesired properties can be practically revealed through a combination of algebraic and statistical analysis. This shows that counting the number of active S-boxes in trails may have little meaning. Such properties could have been avoided by moving to a slightly different function at a negligible implementation cost.

We did not expect this kind of problem to exist for the 8-bit version of the SKINNY S-box. However, like the 4-bit S-box, in the composition of the two 8-bit S-boxes, the first stage of the second S-box and the final stage of the first S-box are the same, leading to cancellation. If the matrix that is used in the `MixColumns` step did not have a row with a single one, then this double S-box structure would not exist. As a result, this particular problem would not be there.

Acknowledgements. Joan Daemen and Daniël Kuijsters are supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.

References

1. 27, I.J.S.: Information security — Encryption algorithms — Part 7: Tweakable block ciphers. International Organization for Standardization, Vernier, Geneva, Switzerland, 1 edn. (2022), https://www.iso.org/standard/80505.html
2. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 123–153. Springer (2016), https://doi.org/10.1007/978-3-662-53008-5_5
3. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: CRYPTO '90. https://doi.org/10.1007/3-540-38424-3_1
4. Bordes, N., Daemen, J., Kuijsters, D., Assche, G.V.: Thinking outside the superbox. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III. Lecture Notes in Computer Science, vol. 12827, pp. 337–367. Springer (2021), https://doi.org/10.1007/978-3-030-84252-9_12
5. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press (2021)
6. Daemen, J.: Cipher and hash function design, strategies based on linear and differential cryptanalysis, PhD Thesis. K.U.Leuven (1995)
7. Daemen, J., Rijmen, V.: The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition. Information Security and Cryptography, Springer (2020)
8. Iwata, T., Khairallah, M., Minematsu, K., Peyrin, T.: Duel of the titans: The romulus and remus families of lightweight AEAD algorithms. IACR Trans. Symmetric Cryptol. 2020(1), 43–120 (2020), https://doi.org/10.13154/tosc.v2020.i1.43-120
9. Jean, J.: TikZ for Cryptographers. https://www.iacr.org/authors/tikz/ (2016)
10. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and keys for block ciphers: The TWEAKEY framework. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II. Lecture Notes in Computer Science, vol. 8874, pp. 274–288. Springer (2014), https://doi.org/10.1007/978-3-662-45608-8_15
11. Lidl, R., Niederreiter, H.: Finite fields, Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge, second edn. (1997)
12. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) Advances in Cryptology - EUROCRYPT '93, Proceedings
13. Nyberg, K.: Generalized feistel networks. In: Kim, K., Matsumoto, T. (eds.) Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea,

November 3-7, 1996, Proceedings. Lecture Notes in Computer Science, vol. 1163, pp. 91–104. Springer (1996), https://doi.org/10.1007/BFb0034838
14. Turan, M.S., McKay, K., Chang, D., Calik, C., Bassham, L., Kang, J., Kelsey, J.: Status report on the second round of the nist lightweight cryptography standardization process (2021-07-20 04:07:00 2021), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932630
15. Verbakel, D.: Influence of Design on Differential and Linear Propagation Properties of Block Cipher Family Skinny. Bachelor's thesis, Radboud University, Nijmegen, the Netherlands (2021)