Cryptanalysis of 10-round SKINNY-128-128 for the SKINNY 2018-2019 Competition

Aleksei Udovenko*

aleksei.udovenko@uni.lu
SnT, University of Luxembourg

Abstract. SKINNY [1] is a recently designed lightweight tweakable block cipher. The designers organize yearly competitions on cryptanalysis of SKINNY. In the 2018-2019 competition, they suggest to recover the secret key from a given encryption of a known book with 2^{20} blocks. The suggested SKINNY instances are 4- to 20-round reduced variants of SKINNY-64-128 and SKINNY-128-128. In this short note, we explain how to solve the challenge for the 10-round SKINNY-128-128 in time 2^{48}. The cryptanalysis method is the second-order truncated differential attack, i.e. an integral attack. The required plaintext structures were found in the pool of given encryptions; only 24 actual plaintext-ciphertext pairs are needed.

Keywords: SKINNY, competition, cryptanalysis, truncated differentials, higher-order differentials, integral cryptanalysis

1 Mining Truncated Differentials

In the known-plaintext scenario, differential attacks usually do not come to mind. Indeed, differential analysis gives concrete trails and observing a concrete difference in a pool of random plaintexts is very improbable. For example, for a concrete n-bit difference to be observed with high probability, it is required that the pool has size close to $2^{n/2}$. Even more data is needed for a higher-order differential, or if the differential is probabilistic. However, a truncated differential has much higher chance to be observed. The chances are even higher if the random plaintext blocks have low entropy, for example, if the plaintext is a text of a book.

In the known-plaintext data from the SKINNY 2018-2019 competition (for the 10-round SKINNY-128-128), we managed to find quadruples of plaintexts that differ in at most two bytes and that sum to zero. That is, these quadruples form a second-order difference with two active bytes. We encrypted these quadruples with random keys and observed that after full 6 rounds, the cell with coordinates $(2, 1)$ sums to zero over the four encryptions. This observation

* The work of Aleksei Udovenko is supported by the Fonds National de la Recherche, Luxembourg (project reference 9037104).

corresponds to the second-order truncated differential (see [2,3]):

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \beta \end{bmatrix} \xrightarrow{6 \text{ rounds}} \begin{bmatrix} ? & ? & ? & ? \\ ? & 0 & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix},$$

where $\otimes$ means that the second-order differential is formed by the two operands as the basis. That is, the last two bytes must have differences $(0,0), (\alpha,0), (0,\beta), (\alpha,\beta)$ from one of the plaintexts in the quadruple, for any $\alpha, \beta \in \mathbb{F}_2^8$. For example, the following message blocks satisfy the second-order difference:

```
< for a moment an>
< for a moment at>
< for a moment in>
< for a moment it>
```

We found 9 quadruples that form the required second order difference. There are also 3 quadruples satisfying another second-order truncated trail of probability 1:

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \beta \end{bmatrix} \xrightarrow{6 \text{ rounds}} \begin{bmatrix} ? & ? & ? & ? \\ 0 & ? & 0 & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}.$$

2 Key-Recovery using Truncated Differentials

In the first truncated differential, the cell with coordinates $(2,1)$ sums to zero after full 6 encryption rounds. Denote it by $s_{6,(2,1)}$ It can be computed from the ciphertext and 6 bytes of the key (I denotes the inverse of the SKINNY-128 S-Box, $c \in (\mathbb{F}_2^8)^{16}$ is the ciphertext and $k \in (\mathbb{F}_2^8)^{16}$ is the master key):

$$\begin{aligned}
&s_{6,(2,1)} = I(I(k_{12} \oplus a \oplus b \oplus c) \oplus I(d \oplus e)), \text{ where} \\
&a = I(3 \oplus k_7 \oplus I(k_9 \oplus c_6 \oplus c_{10} \oplus c_{14}) \oplus I(c_7 \oplus c_{15}) \oplus I(c_0 \oplus c_{12})), \\
&b = I(2 \oplus I(k_{15} \oplus c_7 \oplus c_{11} \oplus c_{15}) \oplus I(c_1 \oplus c_{13})), \\
&c = I(I(k_8 \oplus c_7) \oplus I(c_2 \oplus c_{14})), \\
&d = I(k_3 \oplus I(k_{15} \oplus c_7 \oplus c_{11} \oplus c_{15})), \\
&e = I(I(k_{12} \oplus c_5) \oplus I(c_0 \oplus c_{12})).
\end{aligned}$$

Note that $s_{6,(2,1)}$ depends only on 6 key bytes:

$$k_3, k_7, k_8, k_9, k_{12}, k_{15}.$$

9 quadruples following the trail provide strong filter of the probability 2^{-72}. These 6 bytes of the key can be found by exhaustive search. The check consists in computation of $s_{6,(2,1)}$ from ciphertexts using the equation above and verifying that the sum is equal to zero. The rest of the key can be recovered in a similar way, but with exhaustive searches of less than 6-bytes.

References

1. 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. Volume 9815 of Lecture Notes in Computer Science., Springer (2016) 123–153
2. Lai, X.: Higher order derivatives and differential cryptanalysis. In Blahut, R.E., Costello, D.J., Maurer, U., Mittelholzer, T., eds.: Communications and Cryptography: Two Sides of One Tapestry, Boston, MA, Springer US (1994) 227–233
3. Knudsen, L.R.: Truncated and higher order differentials. In Preneel, B., ed.: Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings. Volume 1008 of Lecture Notes in Computer Science., Springer (1994) 196–211