NOTE ON THE CRYPTANALYSIS OF SPEEDY

TIM BEYNE AND ADDIE NEYT

ABSTRACT. At Eurocrypt 2023, a differential attack on the block cipher SPEEDY-7-192 was presented. This note shows that the main differential characteristic that this attack is based on has probability zero.

In a paper at Eurocrypt 2023 [2], a key-recovery attack on SPEEDY-7-192 was proposed based on multiple 5 round differential characteristics. The authors estimated that the main characteristic used in the attack has probability $2^{-170.56}$; the other characteristics were reported to have 'quite bad probabilities compared to the main one', but they are not provided so it is not possible to verify them.

The main characteristic is based on a four-round 'core trail', the first round of which is shown in Figure 1. The SB operation applies an S-box S to every 6-bit row, the SC function rotates the $i^{\rm th}$ state column upwards by i bits. The orange cells correspond to difference bits equal to one. The blue cells indicate mask bits equal to one in a quasidifferential trail with the same differences as the characteristic.

The characteristic shown in Figure 1 was estimated to have probability 2^{-42} in [2]. This corresponds to the correlation of the quasidifferential trail with all masks equal to zero. However, as shown in the figure, there exists a second quasidifferential trail with correlation -2^{-42} . Hence, by [1, Theorem 4.2 (2)], the probability of the entire characteristic is equal to zero. The correlation can be computed from the quasidifferential transition matrix of S, which satisfies (indices in hexadecimal)

$$D_{(\mathtt{20},\mathtt{10}),(\mathtt{00},\mathtt{01})}^{\mathsf{S}} = -\frac{1}{8} \quad \text{and} \quad D_{(\mathtt{00},\mathtt{04}),(\mathtt{20},\mathtt{10})}^{\mathsf{S}} = \frac{1}{8} \, .$$

The quasidifferential trail in Figure 1 corresponds to a local contradiction, which can easily be verified by hand. The characteristic used in the attack on SPEEDY-6-192 in [2, Figure 8] has essentially the same issue, but the contradiction instead occurs in the last three rows. In future work, we will investigate to what extent the attack can be fixed or improved by using other characteristics.

REFERENCES

- [1] Tim Beyne and Vincent Rijmen. Differential cryptanalysis in the fixed-key model. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology CRYPTO 2022*, pages 687–716, Cham, 2022. Springer Nature Switzerland.
- [2] Christina Boura, Nicolas David, Rachelle Heim Boissier, and María Naya-Plasencia. Better steady than speedy: Full break of speedy-7-192. In Carmit Hazay and Martijn Stam, editors, Advances in Cryptology – EUROCRYPT 2023, pages 36–66, Cham, 2023. Springer Nature Switzerland.

COSIC, KU LEUVEN

Email address: first.lastname@esat.kuleuven.be

Date: February 15, 2024.

Tim Beyne is supported by the Research Foundation – Flanders (FWO) reference № 1274724N.

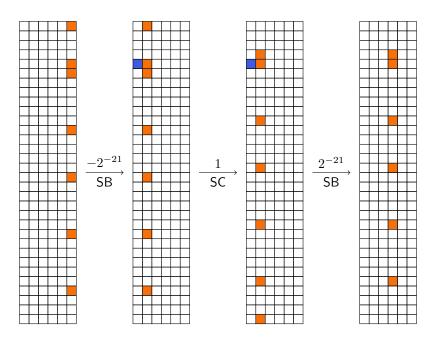


FIGURE 1. Quasidifferential trail with correlation -2^{-42} for the first round of the core characteristic for SPEEDY-7-192 from [2, Figure 4].