Kerman, Sara J. (Fed)

From: Sumanta Sarkar <sumanta.sarkar@gmail.com>
Sent: Thursday, April 25, 2019 3:59 PM
To: lightweight-crypto; NILANJAN DATTA; ashrujit@cs.washington.edu; debdeep; sikhar.patranabis@iitkgp.ac.in; s.picek@tudelft.nl; RAJAT SADHUKHAN
Cc: lwc-forum@list.nist.gov
Subject: Re: TRIFLE S-box has some structural weakness

Hi TRIFLE Team,

I observe that there are some structural weakness in TRIFLE S-box.
This S-box has 4 fixed points:
0 -> 0
5 -> 5
A -> A
F -> F

What is more worrisome is that these fixed points are forming a subspace (U), that is S(U) = U. Having the design where diffusion depends on the bit permutation and there are only a few places where round constants are being added, this makes a perfect stage for mounting invariant subspace attack.

Please let me know if my understanding is not correct.

Thanks
Sumanta

From: Siang Meng Sim <crypto.s.m.sim@gmail.com>
Sent: Wednesday, June 26, 2019 12:43 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: TRIFLE
Attachments: TRIFLE-BC_weakness.pdf

Dear TRIFLE team and all,

We would like to quickly highlight some weaknesses of TRIFLE-BC, the underlying block cipher of TRIFLE, namely:
1) 2 rounds partial decryption without key
2) existence of arbitrary long single active bit differential/linear trails
3) existence of iterative subspace transitions through TRIFLE-BC S-box
The draft is in the attachment, we hope that the TRIFLE team could verify them.

We believe some of these weaknesses can be exploited to mount key-recovery attack on TRIFLE-BC, we are currently working on it.

Previously, the TRIFLE team has responded to Sumanta's concern about invariant subspace attack on TRIFLE-BC, as I quote
"Thank you for your observation. Indeed, we were aware of this property of the S-Box. We believe that adding constant to the most significant bit of some nibbles at each round breaks the propagation of invariant subspace, and full round TRIFLE should resist against such attacks."
This belief is not entirely true, as we have pointed it out in Section 5 of our draft that there exists one subspace transition that is not broken by adding constant to the most significant bit of some nibbles.

--
Best Regards,
Siang Meng Sim
on behalf of Thomas Peyrin, Sumanta Sarkar, Yu Sasaki

A Study on TRIFLE-BC

Thomas Peyrin, Sumanta Sarkar, Yu Sasaki, Siang Meng Sim

1 Introduction

TRIFLE is one of the round 1 candidates in the ongoing NIST Lightweight Cryptography competition, it is a AEAD scheme which uses an SPN based block cipher TRIFLE-BC as its underlying encryption algorithm.

Although the design of TRIFLE-BC is heavily inspired by GIFT and PRESENT, the combination of its building blocks (operations in its round function) result in several potential weaknesses. In this study, we highlight the undesired cryptographic properties and the potential exploitation of these properties to launch attacks on TRIFLE.

2 Notations

Let SN, BP, AK denotes SubNibbles (using S-box S), BitPermutation (using bit permutation P), AddRoundKey plus AddRoundConst respectively, and $R = AK \circ BP \circ SN$. The round key for round r is denoted as RK^r. Let $X_i^r[j]$ denotes the bit j of nibble i in round r, where $r \in \{0, \ldots, 49\}$, $i \in \{0, \ldots, 31\}$ and $j \in \{0, \ldots, 3\}$.

$$PT = X^0 \xrightarrow[S^0]{SN} Y^0 \xrightarrow[P]{BP} Z^0 \xrightarrow[\oplus RK^0]{AK} X^1 \xrightarrow{R} \ldots \xrightarrow{R} X^{49} \xrightarrow[P,S^{49}]{BP \circ SN} Z^{49} \xrightarrow[\oplus RK^{49}]{AK} X^{50} = CT$$

3 Key-independent Decryption

The grouping of TRIFLE-BC S-boxes is as follows:

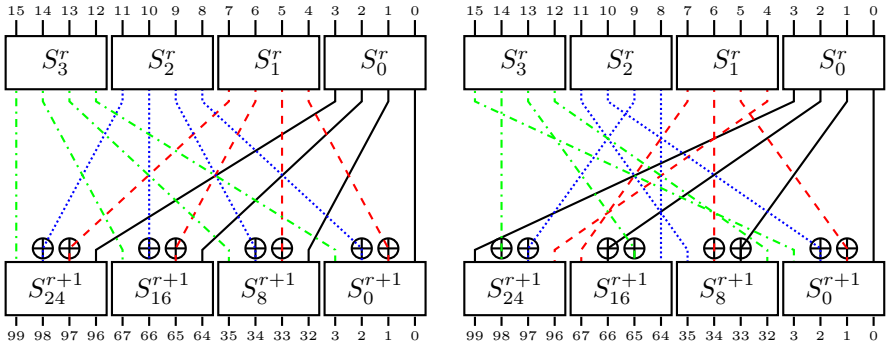
$$\begin{aligned}
\{S_0^r, S_1^r, S_2^r, S_3^r\} &\rightarrow \{S_0^{r+1}, S_8^{r+1}, S_{16}^{r+1}, S_{24}^{r+1}\} \\
\{S_4^r, S_5^r, S_6^r, S_7^r\} &\rightarrow \{S_1^{r+1}, S_9^{r+1}, S_{17}^{r+1}, S_{25}^{r+1}\} \\
\{S_8^r, S_9^r, S_{10}^r, S_{11}^r\} &\rightarrow \{S_2^{r+1}, S_{10}^{r+1}, S_{18}^{r+1}, S_{26}^{r+1}\} \\
\{S_{12}^r, S_{13}^r, S_{14}^r, S_{15}^r\} &\rightarrow \{S_3^{r+1}, S_{11}^{r+1}, S_{19}^{r+1}, S_{27}^{r+1}\} \\
\{S_{16}^r, S_{17}^r, S_{18}^r, S_{19}^r\} &\rightarrow \{S_4^{r+1}, S_{12}^{r+1}, S_{20}^{r+1}, S_{28}^{r+1}\} \\
\{S_{20}^r, S_{21}^r, S_{22}^r, S_{23}^r\} &\rightarrow \{S_5^{r+1}, S_{13}^{r+1}, S_{21}^{r+1}, S_{29}^{r+1}\} \\
\{S_{24}^r, S_{25}^r, S_{26}^r, S_{27}^r\} &\rightarrow \{S_6^{r+1}, S_{14}^{r+1}, S_{22}^{r+1}, S_{30}^{r+1}\} \\
\{S_{28}^r, S_{29}^r, S_{30}^r, S_{31}^r\} &\rightarrow \{S_7^{r+1}, S_{15}^{r+1}, S_{23}^{r+1}, S_{31}^{r+1}\},
\end{aligned}$$

where all groupings use the same 16-bit group mapping.

Following the footsteps of GIFT-128, TRIFLE-BC XORs key material to bit 1 and bit 2 or each nibble. However, the latter adopts the PRESENT group mapping rather than the GIFT group mapping, the main difference is that under the

PRESENT group mapping, bit i can be mapped to any bit j (where $i, j \in \{0, 1, 2, 3\}$) depending on the S-box position.

While in the forward direction (encryption), 2 of the 4 input bits to every S-box is masked with some secret key material, it is not the case from the backward direction (decryption).



TRIFLE-BC group mapping GIFT-128 group mapping

As one can see from the figures above, 2 of the 4 S-boxes (black and green) in the previous round of TRIFLE-BC is not masked by any key material. Such property does not exist in PRESENT because all bits are masked with some key material. Whereas for GIFT, bit i is mapped to bit i, thus 2 of the 4 output bits to every S-box is masked with some key material.

Lemma 1: Given $\{X_i^{r+1}, X_{i+8}^{r+1}, X_{i+16}^{r+1}, X_{i+24}^{r+1}\}$, the value of X_{4i}^r, X_{4i+3}^r can be fully determined and are independent of the secret key.

Corollary 1: Given the knowledge of an entire state X^r, the value of 16 nibbles of the state in the previous round, namely X_{4i}^{r-1} and X_{4i+3}^{r-1}, and the value of 8 nibbles of the state two rounds before, namely X_0^{r-2}, X_3^{r-2}, X_{12}^{r-2}, X_{15}^{r-2}, X_{16}^{r-2}, X_{19}^{r-2}, X_{28}^{r-2}, X_{31}^{r-2} are independent of the secret key and can be fully determined with probability 1.

In other words, without any guessing of key bit, one can decrypt 2 rounds of TRIFLE-BC and determine the value of a quarter of the state trivially.

4 Single Active Bit Differential/Linear Trail

Differential cryptanalysis (DC) is one of the 2 classical attacks on block ciphers that designers should always prove that their proposal to be resistant against it. PRESENT achieves that using S-box with differential branching number 3, guaranteeing that any single active bit input (resp. output) to an S-box will propagate to at least 2 active S-boxes in the next (resp. previous) round. On the other hand, GIFT proposed a paradigm called *Bad-Output must go to Good-Input* (BOGI), with a careful selection of S-box with desired BOGI property and

construct the bit permutation incoherent with the S-box properties, it ensures that there will not be consecutive *single active bit transitions* (S-box with single input and output bit active only). Surprisingly, `TRIFLE-BC` did not adopt either of these design philosophies; Thus not surprisingly, there exists infinitely long single active bit transitions.

A quick check on the `TRIFLE-BC` S-box shows that there exists 4 Hamming weight 1 differential transitions, namely

$$\begin{aligned}
\texttt{0x1} &\rightarrow \texttt{0x8} \\
\texttt{0x2} &\rightarrow \texttt{0x1} \\
\texttt{0x4} &\rightarrow \texttt{0x2} \\
\texttt{0x8} &\rightarrow \texttt{0x4}
\end{aligned}$$

This means that regardless of the position of the single active bit input, there always exists a single active bit output. Independently, the authors of [2] presented an attack on `TRIFLE` using one of such differential trails.

Each single active bit S-box transition holds with probability 2^{-3}. Thus, one can start from any single active bit and there is an unique single bit trail through r-round of `TRIFLE-BC` that holds with probability 2^{-3r}.

We can have a slightly better probability differential trail if we choose the input difference to the first round S-box such that it propagates to single active bit with probability 2^{-2}. For instance, $\texttt{0xD} \rightarrow \texttt{0x1}$, and this is always possible for any single active bit output. Similarly for the output difference, any single active bit input, there is some output that holds with proability 2^{-2}. For instance, $\texttt{0x2} \rightarrow \texttt{0x9}$.

Lemma 2: An optimal r-round differential characteristic has a maximum differential probability of 2^{3r-2}.

This formula is a simple generalisation of the bounds found by the designers in Table 4.2.

On a side note, the designers of `TRIFLE` argued that it is resistance against DC by showing there is no meaningful (probability lower than 2^{-127}) 50-round differential characteristics. However, they did not consider the fact that the several rounds could be extended before and after a differential characteristic, leaving very little security margin against DC.

The situation for the linear case seems worse, there exists multiple single bit linear trails as it has 12 Hamming weight 1 linear transitions:

$$\begin{aligned}
&\texttt{0x1} \rightarrow \texttt{0x1}\ ,\ \texttt{0x1} \rightarrow \texttt{0x4}\ ,\ \texttt{0x1} \rightarrow \texttt{0x8} \\
&\texttt{0x2} \rightarrow \texttt{0x1}\ ,\ \texttt{0x2} \rightarrow \texttt{0x2}\ ,\ \texttt{0x2} \rightarrow \texttt{0x8} \\
&\texttt{0x4} \rightarrow \texttt{0x1}\ ,\ \texttt{0x4} \rightarrow \texttt{0x2}\ ,\ \texttt{0x4} \rightarrow \texttt{0x4} \\
&\texttt{0x8} \rightarrow \texttt{0x2}\ ,\ \texttt{0x8} \rightarrow \texttt{0x4}\ ,\ \texttt{0x8} \rightarrow \texttt{0x8}
\end{aligned}$$

5 Subspace Transition

Apart from having 4 fixed points in the S-box (which not exactly a good feature to have), these 4 fixed points also forms an subspace transition, as first pointed out by Sarkar [3].

Having (affine) subspace transitions through the non-linear component of a cipher could lead to invariant subspace attacks (ISA) even though it is proven to be strong against several cryptanalysis [1]. Since the designers of `TRIFLE` did not mention about ISA, we study the (affine) subspace transitions though `TRIFLE-BC` S-box.

Notably, there are a total of 5 subspace transitions that maps to itself through the `TRIFLE-BC` S-box, as listed below:

$$\{\texttt{0x0}, \texttt{0x1}, \texttt{0xC}, \texttt{0xD}\} \rightarrow \{\texttt{0x0}, \texttt{0x1}, \texttt{0xC}, \texttt{0xD}\}$$
$$\{\texttt{0x0}, \texttt{0x2}, \texttt{0x9}, \texttt{0xB}\} \rightarrow \{\texttt{0x0}, \texttt{0x2}, \texttt{0x9}, \texttt{0xB}\}$$
$$\{\texttt{0x0}, \texttt{0x3}, \texttt{0x4}, \texttt{0x7}\} \rightarrow \{\texttt{0x0}, \texttt{0x3}, \texttt{0x4}, \texttt{0x7}\}$$
$$\{\texttt{0x0}, \texttt{0x5}, \texttt{0xA}, \texttt{0xF}\} \rightarrow \{\texttt{0x0}, \texttt{0x5}, \texttt{0xA}, \texttt{0xF}\}$$
$$\{\texttt{0x0}, \texttt{0x6}, \texttt{0x8}, \texttt{0xE}\} \rightarrow \{\texttt{0x0}, \texttt{0x6}, \texttt{0x8}, \texttt{0xE}\}$$

Among them, the most worrisome is the last subspace transition. Putting the BitPermutation (BP) aside for the time being, we consider a very simple ISA using the subspace $\mathbb{S} = \{\texttt{0x0}, \texttt{0x6}, \texttt{0x8}, \texttt{0xE}\}$ propagate through the $SubNibbles$ (SN), $AddRoundKey$ (AK) and $AddRoundConst$ (AC).

As shown above, if $X_i^r \in \mathbb{S}$, then after SN we have $Y_i^r \in \mathbb{S}$. Since AC updates the bit 3 of some nibbles with 0 or 1, it is equivalent to XORing $c \in \{\texttt{0x0}, \texttt{0x8}\}$ to each nibble. On the other hand, AK adds round key RK^r to bit 1 and 2 of each nibble. For some weak keys that have the round keys XORing $k \in \{\texttt{0x0}, \texttt{0x6}\}$ to each nibble, then the combination of AK and AC is equivalent to XORing some value $v \in \{\texttt{0x0}, \texttt{0x6}, \texttt{0x8}, \texttt{0xE}\} = \mathbb{S}$ to each nibble and the subspace $\mathbb{S}$ is preserved for arbitrary number of rounds.

Although the BP does destroy this subspace $\mathbb{S}$ above, it is still unclear if there could be other invariant subspace transition.

6 Conclusion

In this study, we highlighted 3 undesirable cryptographic properties of `TRIFLE-BC` which, to the best of our knowledge, do not exist in other block ciphers of similar structure, like `GIFT`, `PRESENT` and `RECTANGLE`.

References

1. Guo, J., Jean, J., Nikolic, I., Qiao, K., Sasaki, Y., Sim, S.M.: Invariant subspace attack against midori64 and the resistance criteria for s-box designs. IACR Transactions on Symmetric Cryptology **2016**(1) (Dec. 2016) 33–56
2. Liu, F., Isobe, T.: Iterative differential characteristic of trifle-bc. Cryptology ePrint Archive, Report 2019/727 (2019) https://eprint.iacr.org/2019/727.

3. Sarkar, S.: Nist lightweight cryptography competition. Offical comments on the Round 1 Candidate — TRIFLE (2019) https://csrc.nist.gov/Projects/Lightweight-Cryptography/Round-1-Candidates.