Revised Paragraphs of Crypto2023-Paper280

Reviewer#B-Q2:

The revised introduction of references [4] (for replacing lines 114-121 in our paper) is as follows:

Recently, Beierle et al. proposed a technique to reduce the complexity [4]. The high-level idea of the technique is as follows. Denote the set of all right pairs for the differential $\mathit{\Delta}_{in} \xrightarrow{E_1} \mathit{\Delta}_m$ by $\mathcal{X}$. To amplify the correlation of the distinguisher $\mathit{\Delta}_{in} \xrightarrow{E_1} \gamma_{out}$, we choose $\epsilon r^{-2} q^{-4}$ right pairs in the set $\mathcal{X}$ to observe its correlation. To efficiently get right pairs, we exploit the structure of the set $\mathcal{X}$. Concretely, the set $\mathcal{X}$ might have a special structure, such that for any $x \in \mathcal{X}$, one can obtain a set $X = \{(x \oplus u, x \oplus u \oplus \mathit{\Delta}_{in}) | u \in \mathcal{U}\}$, where $\mathcal{U}$ is a subspace, such that all elements in X are right pairs for the differential $\mathit{\Delta}_{in} \to \mathit{\Delta}_m$. For a differential whose set of right pairs has such a special structure, once one right pair is obtained, one can generate a set of $2^{\dim \mathcal{U}}$ right pairs for free. To find such subspace $\mathcal{U}$ for a differential, one can use the concept of the differential's neutral bits [BC04]. In particular, we require $2^{\dim \mathcal{U}} \geqslant \epsilon r^{-2} q^{-4}$. For some differentials for which obtaining a large enough $\mathcal{U}$ is difficult, one might use a probabilistic approach related to the concept of probabilistic neutral bits [JS+08]. Assume that the probability that a randomly generated input x belongs to $\mathcal{X}$ is $\overline{p}$. Then the complexity of the distinguisher is $\epsilon \overline{p}^{-1} r^{-2} q^{-4}$.

References

[BC04] Biham, E., Chen, R. (2004). Near-Collisions of SHA-0. In: Franklin, M. (eds) Advances in Cryptology – CRYPTO 2004. CRYPTO 2004. Lecture Notes in Computer Science, vol 3152. Springer, Berlin, Heidelberg.

[JS+08] Aumasson, JP., Fischer, S., Khazaei, S., Meier, W., Rechberger, C. (2008). New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba. In: Nyberg, K. (eds) Fast Software Encryption. FSE 2008. Lecture Notes in Computer Science, vol 5086. Springer, Berlin, Heidelberg.

Reviewer#B-Q3:

The revised tablenotes of Table 4 is as follows:

(r_m, r_2)	$\Delta_m \to \gamma_m \to \gamma_{out}$	**Cor** of $\Delta_m \to \gamma_{out}$
$(8,3)$	$[26] \to * \to [0, 9, 61, 91, 105]$	$2^{-4.679}$
$(8,4)$	$[31] \to * \to [0, 9, 61, 91, 105]$	$-2^{-10.970}$
$(8,5)$	$[31] \to [8, 41, 42, 73, 74] \to$ $[0, 29, 37, 38, 61, 68, 88, 91, 101, 102, 105, 114]$	$-2^{-6.04} \times 2^{-10\times 2}$

[1] $*$: There are many choices searched by Algorithm 2. The maximum hamming weight of returned γ_m is 7. Since many differential-linear approximations share the same output mask γ_{out}, we directly present the experimental correlation of $\Delta_m \to \gamma_{out}$, i.e., $2^{-4.679}$ and $-2^{-10.970}$.

[2] Denote by r_m, r_2 the number of rounds covered by E_m, E_2.

[3] The three correlations $2^{-4.679}$, $-2^{-10.970}$, $-2^{-6.04}$ are estimated again using N plaintext pairs and 100 keys. The three values are the median of 100 experimental correlations. For $2^{-4.679}$ and $-2^{-6.04}$, $N = 2^{24}$. For $-2^{-10.970}$, $N = 2^{32}$. The number 2^{-10} in the third row is the correlation of the linear approximation $\gamma_m \to \gamma_{out}$.

Reviewer#C-Q1:

A more detailed argument for Lemma 3 (for replacing lines 432-437 in our paper) is as follows:

Table 6 summarizes the result of the search. Given any plaintext pair $(P, P \oplus \Delta_{in})$ conforming to the 4-round differential characteristic as shown in Table 5, using the 34 basis elements, one can create from the plaintext pair a plaintext structure consisting of 2^{34} plaintext pairs that are expected to pass the differential characteristic together, with a theoretical probability $2^{-3.7}$ under the assumption that the effects of the 34 basis elements are independent. For verifying the theorectical probability $2^{-3.7}$, we generate 2^{10} plaintext pairs conforming to the 4-round differential characteristic, and find that the empirical probability is $2^{-3.18}$ (resp. $2^{-3.17}$, $2^{-3.33}$) for LEA-128 (resp. LEA-192, LEA-256). Thus, we obtain Lemma 3. The 17-round key recovery attack introduced later uses this linear subspace.

Lemma 3. There is a set $\mathcal{X} \subseteq \mathbb{F}_2^{128}$ of size $2^{128-33-3.7}$ and a 34-dimension linear subspace $\mathcal{U}$, such that for any element $x \in \mathcal{X}$ and any $u \in \mathcal{U}$ it holds that $E_1(x \oplus u) \oplus E_1(x \oplus u \oplus \Delta_{in}) = \Delta_m$ where E_1 denotes 4 rounds of LEA.