To demonstrate the syncopation technique, two practical key-recovery attack have been implemented on 5 rounds and 6 rounds of ChaCha with 64 unknown key bits. Specifically, in order to make the process of key recovery practical, it is assumed that the attack is performed, under the condition that 192 out of 256 key bits have been obtained and known, to recover some of the remaining 64 secret key bits.

The first section summarizes our experimental results on 5-round and 6-round ChaCha with 64 unknown key bits. In the second section, we take the analysis of 5-round ChaCha to give a specific explanation for some concepts used in our attack.

1 Report of Experiments

Environment of experiments. We have implemented the procedure of new (partial) key-recovery attack with the syncopation technique through C++ programming, that is, steps 1 to 5 of Algorithm 3. All the experiments are conducted on Linux version 6.2.9-arch1-1 with Intel Core i9-13900KF and RAM of 128 GB.

Taking 5-round ChaCha as an example, the attack uses a forward differential with 2.5 rounds, and approximates 2.5 rounds in backward direction with some PNBs of 64 unknown key bits. More precisely, the median correlation of forward differential is $|\varepsilon_d| = 0.838$ with input difference at $\Delta x_{13}^{(0)}[6]$ and output difference at $\Delta x_2^{(2.5)}[0]$, and 56 PNBs are found for backward approximation. Accordingly, the 8 non-PNBs are $\{k_0[i],\, i \in \{6, 9, 10, 11, 12, 13, 18\}\}$ and $k_1[6]$. With the syncopation technique, the conditional backward correlation is $|\varepsilon_a| = 0.752$ under the following four constraints $k_0[i] \neq z_4^{(5)}[i]$, $i \in \{6, 9, 18\}$ and $k_1[6] \neq z_5^{(5)}[6]$. However, without the syncopation technique, the median correlation of backward approximation is experimentally estimated as $|\varepsilon_a| = 2^{-7.6}$ by fixing 56 PNBs into zeros. Therefore, the backward correlation is significantly amplified by utilizing the syncopation technique.

To recover 8 non-PNBs of 64 secret key bits with the syncopation technique, we only need to implement steps 1 to 5 of Algorithm 3. According to the complexity analysis, the time complexity of key-recovery attack is $T = 2^8 \times N^* + N$, data complexity is $N = 2^{2\times 4} \times N^*$ and memory complexity is $M = 2^4 \times N^*$. The Neyman-Pearson decision theory gives the results about estimating the number of samples N^* required to get the bounds on probabilities of false alarm p_{fa} and non-detection p_{nd}. It can be shown that $N^* \approx \left(\frac{\sqrt{\alpha \log 4} + 3\sqrt{1-(\varepsilon_a \varepsilon_d)^2}}{\varepsilon_a \varepsilon_d} \right)^2$ samples suffices to achieve $p_{nd} = 1.3 \times 10^{-3}$ and $p_{fa} = 2^{-\alpha}$. With $\alpha = 8$, the time complexity is $T = 2^{15.4}$, data complexity is $N = 2^{14.4}$ and memory complexity is $M = 2^{10.4}$. As pointed out in [1], with using median correlation in the above equation, we have a success probability of at least $\frac{1}{2}(1 - p_{nd}) \approx \frac{1}{2}$ for the attack.

Result of experiments of 5-round ChaCha. It takes about 22 seconds to run the C++ program 10000 times. As a result, for 10000 randomly generated key, 7071

of them are successfully recovered 8 guessed key bits with the syncopation techniques, and thus the success probability is about 70.7%. The attacks on ChaCha5 are summarized in Table 1.

Table 1. Summary of attacks on ChaCha5 with 64 unknown key bits.

Attack method	Analysis	$\lvert\varepsilon_a\rvert$	T	N	#Random keys	Success probability
With syncopation	Theoretical	-	$2^{15.4}$	$2^{14.4}$	-	≥ 0.5
	Experimental	0.752	2.2×2^{-3} seconds	$2^{14.4}$	10000	$\frac{7071}{10000} \approx 70.7\%$
Without syncopation	Theoretical	-	$2^{29.1}$	$2^{21.1}$	-	≥ 0.5
	Experimental	$2^{-7.6}$	22.5 seconds	$2^{21.1}$	100	$\frac{16}{100} \approx 16\%$

As for 6-round ChaCha, the attack is similar to the one of 5-round ChaCha, except that a forward differential with 3.5 rounds is used, and thus backward approximation consists of 2.5 rounds from the 6-th to 3.5-th round. Specifically, the forward differential takes $\Delta x_{13}^{(0)}[6]$ as the input difference and observes the output difference at $\Delta x_{2}^{(3.5)}[0]$. As shown in [2], the correlation of the forward characteristic is evaluated as $2^{-8.3}$ under that condition that the differential at the first found has the minimum Hamming weight which takes about 2^5 iteration to achieve this.

The 8 non-PNBs are and $k_0[6]$ and $\{k_1[i], i \in \{6, 9, 10, 11, 12, 13, 18\}\}$. The conditional backward correlation is $|\varepsilon_a| = 0.759$ under the following four constraints $k_0[6] \neq z_4^{(6)}[6]$ and $k_1[i] \neq z_5^{(6)}[i]$, $i \in \{6, 9, 18\}$. According to the complexity analysis, the time complexity of key-recovery attack is $T = 2^5 \times (2^8 \times N^* + N)$, data complexity is $N = 2^{5+2\times4} \times N^*$ and memory complexity is $M = 2^4 \times N^*$, and with $\alpha = 13$, $T = 2^{37.1}$, $N = 2^{36.1}$ and $M = 2^{27.1}$.

Result of experiments of 6-round ChaCha. It takes about 1.6 hours to run once the C++ program with RAM about 24 GB for key-recovery attack of ChaCha6. As a result, for 16 randomly generated key, 10 of them are successfully recovered 8 guessed key bits with the syncopation techniques, and thus the success probability among all keys is about 62.5%. In another experiment with 32 randomly generated key, there are 21 weak keys 15 keys of which are successfully recovered 8 guessed key bits with the syncopation techniques, and thus the success probability of key-recovery attack in Algorithm 3 is about $\frac{15}{21} \approx 71.4\%$.

2 Explanation for Some Concepts

Here we take 5-round ChaCha as an example to make a specific explanation of some concepts used in our attacks.

A simple example. Let us focus on the operation $x_4^{(5)} = z_4^{(5)} \boxminus k_0$ (see Fig. 1 for details) in inverse function. For this simple example, the syncopated segment in secret key $k_0^o = k_0[13 : 10]$ and restricted syncopation in secret key

$k^{\mathcal{R}} = \{k_0[i], i \in \{6, 9, 18\}\}$. For example, according to Lemma 2, the syncopated segment in internal state $x_4^{(5)}[13:10]$ is independent with PNBs under the condition that $k_0[9] \neq z_4^{(5)}[9]$.

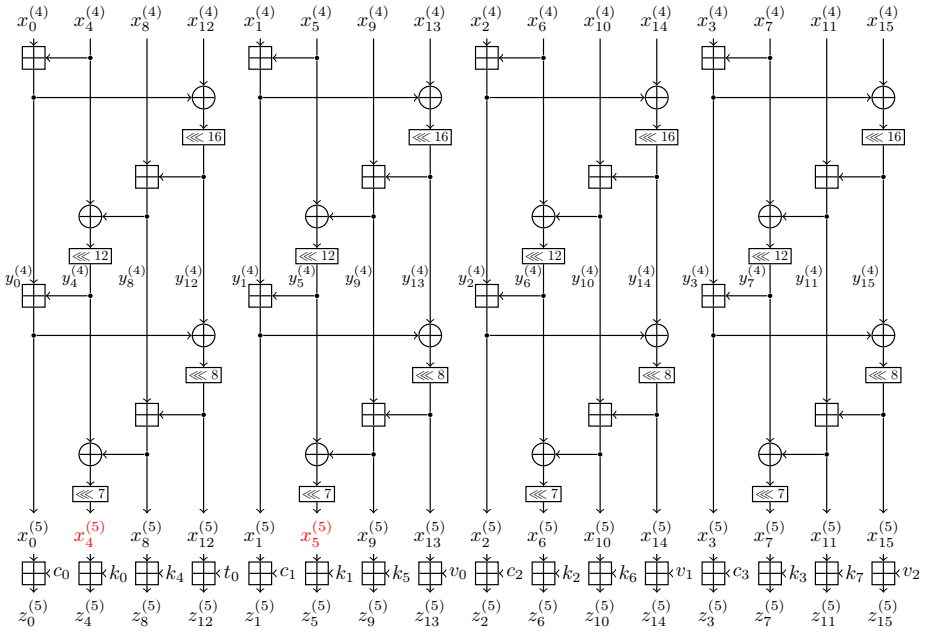

Fig. 1. Last round of ChaCha5.