IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2024, No. 2, pp. 166–189. DOI:10.46586/tosc.v2024.i2.166-189

Differential-Linear Cryptanalysis of Reduced Round ChaCha

Zhichao Xu, Hong Xu(✉), Lin Tan and Wenfeng Qi

Information Engineering University, Zheng Zhou, China
xuzhichao4484@163.com,xuhong0504@163.com,tanlin100@163.com,wenfeng.qi@263.net

Abstract. ChaCha is a well-known stream cipher that has been used in many network protocols and software. In this paper, we study the security of reduced round ChaCha. First, by considering the differential-linear hull effect, we improve the correlation of a four-round differential-linear distinguisher proposed at FSE 2023 by providing other intermediate linear masks. Then, based on the four-round differential-linear distinguisher and the PNB method, by using the assignment $100\cdots00$ for consecutive PNBs, higher backward correlation is obtained and improved key recovery attacks of 7-round and 7.25-round ChaCha are obtained with time complexity $2^{189.7}$ and $2^{223.9}$, which improve the previously best-known attacks by $2^{17.1}$ and $2^{14.44}$, respectively. Finally, we consider the equivalence of the security between $(R+0.25)$-round and $(R+0.5)^{\oplus}$-round ChaCha, and show that $(R+0.25)$-round and $(R+0.5)^{\oplus}$-round ChaCha provide the same security against chosen(known) plaintext attacks. As a result, improved differential-linear cryptanalysis of $7.5^{\oplus}$-round ChaCha can also be obtained similarly to that of 7.25-round ChaCha, which improves the previously best-known attack by 2^{19}.

Keywords: ChaCha · Differential-linear cryptanalysis · Probabilistic Neutral Bits(PNBs)

1 Introduction

ARX ciphers are cryptographic primitives composed of modulo addition, bitwise rotation and bitwise XOR only. Due to the excellent performance in software, many symmetric primitives are designed based on ARX structure, including ChaCha [Ber08], Salsa [Ber05], Chaskey [MMH+14], SPECK [BSS+15], SPARX [DPU+16], HIGHT [HSH+06] and so on.

Both Salsa [Ber05] and ChaCha [Ber08] are well-known symmetric stream ciphers, where ChaCha has been implemented by many protocols and software [Cha], such as SSH, Noise, WireGard, and so on. ChaCha is in one of the cipher suites of TLS, which has been supported by Google. Salsa was introduced by Bernstein in 2005 as a candidate for the eSTREAM project and was selected as a finalist of the competition in April 2007. Bernstein later in 2008 introduced ChaCha as a Salsa variant, which can provide better diffusion without slowing down encryption. The total number of rounds is 20. These ciphers also have reduced round variants, such as the 12-round version. Both these ciphers have the 256-bit key version and the 128-bit key version, and the 256-bit key version of ChaCha is studied in this paper.

Differential cryptanalysis [BS90] and linear cryptanalysis [Mat93] are two fundamental methods for block ciphers. Differential-linear cryptanalysis was proposed based on differential cryptanalysis and linear cryptanalysis by Langford and Hellman [LH94], and has been widely used to attack many ciphers such as DES, Serpent and ICEPOLE [BDK02, Lu12, HTW15, BODKW19].

Received: 2024-03-01 Accepted: 2024-05-01 Published: 2024-06-18

For differential-linear attacks on ARX ciphers, at EUROCRYPT 2016, Leurent [Leu16] used the partitioning technique [BC14] to improve the differential cryptanalysis and linear cryptanalysis of addition operations, and proposed an improved differential-linear attack on 7-round Chaskey. At CRYPTO 2020, Beierle *et al.* [BLT20] improved the partitioning technique and presented improved differential-linear attacks on 7-round Chaskey. In the extended version [BBC+22], they further improved the methods of [BLT20], and presented a differential-linear attack on 7.5-round Chaskey.

At EUROCRYPT 2021, Liu *et al.* [LSL21, LNS+23] proposed the rotational differential-linear attacks by replacing the differential part of the differential-linear attacks with rotational differentials. They applied the technique to FRIET, Xoodoo, Alzette, and SipHash when the output linear masks are unit vectors, and obtained improved (rotational) differential-linear distinguishers. At CRYPTO 2022, Niu *et al.* [NSLL22] improved the technique to evaluate the correlations of ARX ciphers when the output linear masks are arbitrary vectors, and presented improved differential-linear distinguishers for Alzette, SipHash, ChaCha, and SPECK.

The concept of Probabilistic Neutral Bits(PNBs) was first introduced by Aumasson et al. in 2008 [AFK+08], which was used to present the first attack on 8-round Salsa and 7-round ChaCha. In 2012, Shi et al. [SZFW13] introduced the idea of column chaining distinguisher(CCD) based on PNBs. In 2015, Maitra [Mai16] provided the idea of chosen IV based on key guessing and improved the attack on 7-round ChaCha with time complexity $2^{238.9}$.

In 2016, Choudhuri et al. [CM16] extended single-bit distinguisher to multi-bit distinguisher by using linear relation, and provided the first 6-round distinguisher for Salsa and five-round distinguisher for ChaCha. In 2017, Dey et al. [DS17] improved the attacks with better PNBs and then provided a proof of these distinguishers in [DS20].

At CRYPTO 2020, Beierle et al. [BLT20] provided the first 3.5-round single-bit distinguisher for ChaCha, and improved the attack on 7-round ChaCha with time complexity $2^{230.86}$. This distinguisher was also observed by Coutinho et al. [CN20] independently. Some other 3.5-round distinguishers were presented by Coutinho et al. [CN21] at EUROCRYPT 2021, and a further improvement was provided by using one of the distinguishers. However, Dey et al. [DDSM22] proved the improvement is invalid because the used distinguisher for key recovery is incorrect.

At EUROCRYPT 2022, Dey et al. [DGSS22] partition the key bits into memory key bits and non-memory key bits, and the right pairs can be constructed by guessing the memory key bits. They improved the key recovery attacks of 7-round ChaCha with time complexity $2^{221.95}$ by the approach. In the extended version [DGSS23], they further present an improved key recovery attack of 7-round ChaCha with time complexity $2^{218.92}$ by choosing a particular assignment $100\cdots00$ for consecutive PNBs.

At FSE 2023, Dey et al. [DGM23] applied a divide-and-conquer approach on 6-round ChaCha, and obtained an improved attack with time complexity $2^{99.48}$. For ChaCha with longer round, Miyashita et al. [MIM22] presented the first differential-linear attack on 7.25-round ChaCha with time complexity $2^{255.62}$ and success probability 0.5.

At CRYPTO 2023, Wang *et al.* [WLHL23] introduced the syncopation technique, and presented a differential-linear attack on 7-round ChaCha with time complexity $2^{210.3}$. Towards a closer analysis of 8-round ChaCha, they analyzed $7.5^{\oplus}$-round ChaCha where four additions are added to 7.25-round ChaCha, and presented a differential-linear attack with time complexity $2^{242.9}$. At FSE 2023, Bellini *et al.* [BGG+23] found a differential-linear distinguisher for four-round ChaCha with correlation $2^{-34.15}$, and presented differential-linear attacks for 7-round and 7.25-round ChaCha with time complexity $2^{206.8}$ and $2^{238.34}$, respectively. They also presented a differential-linear attack on $7.5^{\oplus}$-round ChaCha, and the time complexity is similar to that of 7.25-round ChaCha.

Our Contribution. In this paper, we study the security of reduced round ChaCha.

Table 1: Summary of cryptanalysis for reduced round ChaCha

Rounds	Time	Data	Source
7	2^{248}	2^{27}	[AFK+08]
	$2^{246.5}$	2^{27}	[SZFW13]
	$2^{238.9}$	2^{96}	[Mai16]
	$2^{237.7}$	2^{96}	[CM16]
	$2^{235.22}$	-	[DS17]
	$2^{230.86}$	$2^{48.83}$	[BLT20]
	$2^{221.95}$	$2^{90.20}$	[DGSS22]
	$2^{218.92}$	$2^{87.18}$	[DGSS23]
	$2^{216.9}$	$2^{68.9}$	[WLHL23]
	$2^{210.3}$	$2^{103.3}$	[WLHL23]
	$2^{206.8}$	$2^{110.81}$	[BGG+23]
	$2^{189.7}$	$2^{102.63}$	this paper
7.25	$2^{255.62}$	$2^{48.36}$	[MIM22]
	$2^{244.85}$	$2^{93.24}$	[DGSS23]
	$2^{238.34}$	$2^{122.34}$	[BGG+23]
	$2^{223.9}$	$2^{100.8}$	this paper
$7.5^{\oplus}$	$2^{244.9}$	$2^{104.9}$	[WLHL23]
	$2^{242.9}$	$2^{125.8}$	[WLHL23]
	$2^{223.9}$	$2^{100.8}$	this paper

Our results are summarized as follows, and a comparison of cryptanalysis for reduced round ChaCha is shown in Table 1.

First, by considering the differential-linear hull effect, we improve the correlation of a four-round differential-linear distinguisher proposed at FSE 2023. When more intermediate linear masks are used, the correlation is improved from $2^{-34.15}$ to $2^{-32.2}$.

Then, based on the four-round differential-linear distinguisher and the PNB method, by using the assignment $100\cdots00$ for consecutive PNBs, higher backward correlation is obtained. For 7-round ChaCha, backward correlation is improved from $2^{-14.18}$ to $2^{-11.855}$, and the number of PNBs increases from 160 to 169. For 7.25-round ChaCha, backward correlation is improved from $2^{-16.85}$ to $2^{-11.25}$. As a result, improved key recovery attacks of 7-round and 7.25-round ChaCha are obtained with time complexity $2^{189.7}$ and $2^{223.9}$, which improve the previously best-known attacks by $2^{17.1}$ and $2^{14.44}$, respectively.

Finally, we consider the equivalence of the security between $(R+0.25)$-round and $(R+0.5)^{\oplus}$-round ChaCha, and we show that $(R+0.25)$-round and $(R+0.5)^{\oplus}$-round ChaCha provide the same security against chosen(known) plaintext attacks. As a result, improved differential-linear attack of $7.5^{\oplus}$-round ChaCha can also be obtained similarly to that of 7.25-round ChaCha, which improves the previously best-known attack by 2^{19}.

Organization of the Paper. In Section 2, some notations, a brief review of ChaCha and differential-linear cryptanalysis are presented. In Section 3, the correlation of a four-round differential-linear distinguisher is improved. In Section 4, improved differential-linear attacks on 7-round and 7.25-round ChaCha are presented. In Section 5, the equivalence between $(R+0.25)$-round and $(R+0.5)^{\oplus}$-round ChaCha is presented, and the improved differential-linear attack on $7.5^{\oplus}$-round ChaCha is presented. Finally, we conclude in Section 6.

2 Preliminaries

2.1 Notations

In this subsection, some notations used in this paper are introduced, which are shown in Table 2.

Table 2: Notations

Symbol	Description
X	the state matrix of the input of the cipher ChaCha consisting of 16 words
X_i	the i-th word of the state matrix X
X^r	the state matrix of the output of the r-round ChaCha
X_i^r	the i-th word of the state matrix X^r
$X_i[j]$	the state matrix where the j-th bit of the i-th word is 1 and the other bits are 0
Δ^r	the matrix of the output difference of the r-round ChaCha
Γ^r	the matrix of the output linear mask of the r-round ChaCha
$\boxplus$	addition modulo 2^{32}
$\boxminus$	subtraction modulo 2^{32}
$x \lll l$	left rotation of x by l bits
$x \ggg l$	right rotation of x by l bits
$\oplus$	XOR operation
x_i	the i-th bit of the n-bit vector x
$x \cdot y$	the inner product of two n-bit vectors x and y, *i.e.* $x \cdot y = \oplus_{i=0}^{n-1} x_i y_i$
$\#S$	number of elements in set S
$\Pr_{x \in F_2^n}(f(x) = g(x))$	$\frac{\#\{x \in F_2^n \mid f(x)=g(x)\}}{2^n}$
$C_E(\Gamma_1, \Gamma_2)$	$2^{-n} \sum_{x \in F_2^n} (-1)^{\Gamma_1 \cdot x \oplus \Gamma_2 \cdot E(x)}$
$\mathrm{Aut}_E(\Delta, \Gamma)$	$2^{-n} \sum_{x \in F_2^n} (-1)^{\Gamma \cdot E(x) \oplus \Gamma \cdot E(x \oplus \Delta)}$

For simplicity, for state matrices X and Y consisting of 16 words, $X \boxplus Y$ and $X \boxminus Y$ mean the word-based addition and subtraction, *i.e.* $(X \boxplus Y)_i = X_i \boxplus Y_i$ and $(X \boxminus Y)_i = X_i \boxminus Y_i$, where $i = \{0, 1, \cdots, 15\}$.

2.2 Structure of ChaCha with 256-Bit Key

The stream cipher ChaCha operates on 32-bit words, which takes as input a 256-bit key $k = (k_0, k_1, \cdots, k_7)$, a 128-bit constant $c = (c_0, c_1, c_2, c_3)$ and a 128-bit initialization vector (IV) $v = (t_0, v_0, v_1, v_2)$. They are organised in a 4×4 matrix of the form X, where

$$X = \begin{pmatrix} X_0 & X_1 & X_2 & X_3 \\ X_4 & X_5 & X_6 & X_7 \\ X_8 & X_9 & X_{10} & X_{11} \\ X_{12} & X_{13} & X_{14} & X_{15} \end{pmatrix} = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ t_0 & v_0 & v_1 & v_2 \end{pmatrix} \tag{1}$$

and $c_0 = 0x61707865$, $c_1 = 0x3320646e$, $c_2 = 0x79622d32$, $c_3 = 0x6b206574$.

Each ChaCha round function *Round* consists of four QR function $(a'', b'', c'', d'') = QR(a, b, c, d)$ as shown in Figure 1. The QR function is given by the following equations:

$$\begin{aligned} a' &= a \boxplus b; & d' &= ((d \oplus a') \lll 16); \\ c' &= c \boxplus d'; & b' &= ((b \oplus c') \lll 12); \\ a'' &= a' \boxplus b'; & d'' &= ((d' \oplus a'') \lll 8); \\ c'' &= c' \boxplus d''; & b'' &= ((b' \oplus c'') \lll 7); \end{aligned} \tag{2}$$

For odd round, the QR function is applied to four column vectors (X_0, X_4, X_8, X_{12}), (X_1, X_5, X_9, X_{13}), $(X_2, X_6, X_{10}, X_{14})$, and $(X_3, X_7, X_{11}, X_{15})$, respectively. On the other hand, for even round, the QR function is applied to the diagonal vectors $(X_0, X_5, X_{10}, X_{15})$, $(X_1, X_6, X_{11}, X_{12})$, (X_2, X_7, X_8, X_{13}), and (X_3, X_4, X_9, X_{14}), respectively.

The initial state X is also denoted by X^0, and X^r denote the output of the r-round ChaCha, *i.e.* $X^r = Round^r(X^0)$. The inverse of round function is denoted as $Round^{-1}$, then $X^0 = Round^{-r}(X^r)$. After R iterations of the ChaCha round functions, the final state X^R is added word-wise (modulo 2^{32}) to the initial state X^0 to form the key stream Z, *i.e.* $Z = X^0 \boxplus X^R$.

For more details on ChaCha, please refer to [Ber08].

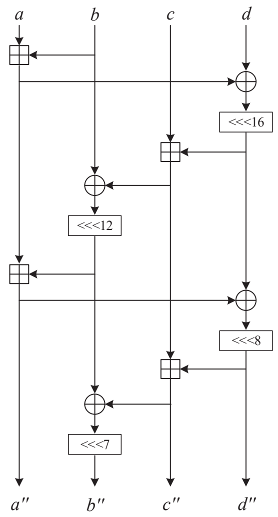


Figure 1: QR function $QR(a,b,c,d)$ of ChaCha

2.3 Differential-Linear Distinguisher

Differential-linear cryptanalysis [LH94] was introduced by Langford and Hellman. For given input difference Δ_{in} and output linear mask Γ_{out} of cipher E, the correlation c of the differential-linear distinguisher $\Delta_{in} \xrightarrow{E} \Gamma_{out}$ is defined by

$$\Pr_{x\in F_2^n}\left(\Gamma_{out}\cdot(E(x)\oplus E(x\oplus\Delta_{in}))=0\right)=\frac{1}{2}(1+c). \tag{3}$$

By preparing ϵc^{-2} input pairs $(x, x\oplus\Delta_{in})$, where ϵ is a small constant, the cipher E can be distinguished from a pseudorandom permutation.

Differential-linear distinguishers can be constructed with Differential-Linear Connectivity Table (DLCT) [BODKW19]. Assume cipher E can be divided into three sub-ciphers E_1, E_m and E_2, such that $E = E_2 \circ E_m \circ E_1$. If there exists a differential characteristic $\Delta_{in} \xrightarrow{E_1} \Delta_m$, a differential-linear distinguisher $\Delta_m \xrightarrow{E_m} \Gamma_m$ and a linear approximation $\Gamma_m \xrightarrow{E_2} \Gamma_{out}$ for E_1, E_m and E_2 with probability p, correlation r and correlation q, respectively, *i.e.*

$$\begin{aligned}
&\Pr_{x\in F_2^n}\left(E_1(x)\oplus E_1(x\oplus\Delta_{in})=\Delta_m\right)=p,\\
&\Pr_{x\in F_2^n}\left(\Gamma_m\cdot(E_m(x)\oplus E_m(x\oplus\Delta_m))=0\right)=\frac{1}{2}(1+r),\\
&\Pr_{x\in F_2^n}\left(\Gamma_m\cdot x\oplus\Gamma_{out}\cdot E_2(x)=0\right)=\frac{1}{2}(1+q),
\end{aligned} \tag{4}$$

then there exists a differential-linear distinguisher $\Delta_{in} \xrightarrow{E} \Gamma_{out}$ for E with correlation prq^2, *i.e.*

$$\Pr_{x\in F_2^n}\left(\Gamma_{out}\cdot(E(x)\oplus E(x\oplus\Delta_{in}))=0\right)=\frac{1}{2}(1+prq^2). \tag{5}$$

By preparing $\epsilon(prq^2)^{-2} = \epsilon p^{-2}r^{-2}q^{-4}$ input pairs $(x, x\oplus\Delta_{in})$, where ϵ is a small constant, the cipher E can be distinguished from a pseudorandom permutation.

In this paper, we use the symbols $\mathrm{Aut}_{E_1}(\Delta_m,\Gamma_m)$ and $C_{E_2}(\Gamma_m,\Gamma_{out})$ to represent the correlations of the differential-linear distinguisher $\Delta_m \xrightarrow{E_m} \Gamma_m$ and the linear approximation $\Gamma_m \xrightarrow{E_2} \Gamma_{out}$. By adopting all intermediate linear masks, Blondeau *et al.* [BLN17] presented the following proposition to compute the correlation of the differential-linear distinguisher based on the differential-linear hull.

Proposition 1. [BLN17] *Assume cipher E can be divided into two sub-ciphers $E_1 : F_2^n \to F_2^n$ and $E_2 : F_2^n \to F_2^n$, such that $E = E_2 \circ E_1$, where E_1 and E_2 are independent. For any $\Delta_m, \Gamma_{out} \in F_2^n$, we have*

$$\mathrm{Aut}_{E_2 \circ E_1}(\Delta_m, \Gamma_{out}) = \sum_{\Gamma_m \in F_2^n} \mathrm{Aut}_{E_1}(\Delta_m, \Gamma_m) C_{E_2}(\Gamma_m, \Gamma_{out})^2, \tag{6}$$

where

$$\begin{aligned} \mathrm{Aut}_{E_1}(\Delta_m, \Gamma_m) &= 2^{-n} \sum_{x \in F_2^n} (-1)^{\Gamma_m \cdot E_1(x) \oplus \Gamma_m \cdot E_1(x \oplus \Delta_m)}, \\ C_{E_2}(\Gamma_m, \Gamma_{out}) &= 2^{-n} \sum_{x \in F_2^n} (-1)^{\Gamma_m \cdot x \oplus \Gamma_{out} \cdot E_2(x)}. \end{aligned} \tag{7}$$

For simplicity, in this paper, $\mathrm{Aut}_{E_1}(\Delta_m, \Gamma_m)$ and $C_{E_2}(\Gamma_m, \Gamma_{out})$ are also denoted by $\mathrm{Aut}(\Delta_m, \Gamma_m)$ and $C(\Gamma_m, \Gamma_{out})$ when E_1 and E_2 are known.

2.4 PNB-Based Key Recovery

At FSE 2008, Aumasson *et al.* [AFK+08] presented the first attack on ChaCha by the probabilistic neutral bits (PNBs). The PNB-based key recovery of R-round ChaCha mainly consists of the following steps.

Pre-processing Stage: Selecting PNBs and Evaluating the Backward Correlation.

Step 1: Find an r-round differential-linear distinguisher $\Delta^0 \to \Gamma^r$ with correlation ϵ_d, *i.e.*

$$\Pr_X \left(\Gamma^r \cdot (X^r \oplus X'^r) = 0 | X \oplus X' = \Delta^0 \right) = \frac{1}{2}(1 + \epsilon_d), \tag{8}$$

where $r < R$, (X, X') is the input pair of ChaCha, and (X^r, X'^r) is the output pair of r-round ChaCha.

Step 2: Select the PNBs by a threshold γ. Construct multiple input pairs (X, X'), where $X' = X \oplus \Delta^0$, and generate corresponding output key streams (Z, Z'), *i.e.* $Z = X \boxplus X^R$ and $Z' = X' \boxplus X'^R$. Construct pairs $(\overline{X}, \overline{X'})$ from (X, X') such that the i-th key bit is complemented while the other bits take the same values. Compute $Y = \mathit{Round}^{-(R-r)}(Z \boxminus \overline{X})$, $Y' = \mathit{Round}^{-(R-r)}(Z' \boxminus \overline{X'})$. Then $\Gamma^r \cdot (Y \oplus Y')$ is a approximation of $\Gamma^r \cdot (X^r \oplus X'^r)$ with correlation γ_i, *i.e.*

$$\Pr_X(\Gamma^r \cdot (X^r \oplus X'^r) = \Gamma^r \cdot (Y \oplus Y')) = \frac{1}{2}(1 + \gamma_i). \tag{9}$$

When $\gamma_i > \gamma$, the i-th key bit is selected as a PNB, otherwise the i-th key bit is a non-PNB.

Step 3: Evaluate the backward correlation. Construct multiple input pairs (X, X'), where $X' = X \oplus \Delta^0$, and generate corresponding output key streams (Z, Z'), *i.e.* $Z = X \boxplus X^R$ and $Z' = X' \boxplus X'^R$. Construct pairs $(\hat{X}, \hat{X}')$ from (X, X') such that all PNBs are assigned fixed value (or random value) while the other bits take the same values as (X, X'). Compute $\hat{Y} = \mathit{Round}^{-(R-r)}(Z \boxminus \hat{X})$, $\hat{Y}' = \mathit{Round}^{-(R-r)}(Z' \boxminus \hat{X}')$. The backward correlation ϵ_a is computed by

$$\Pr_X \left(\Gamma^r \cdot (X^r \oplus X'^r) = \Gamma^r \cdot (\hat{Y} \oplus \hat{Y}') \right) = \frac{1}{2}(1 + \epsilon_a). \tag{10}$$

Then by equations (8) and (10), and the Piling-up lemma, we have

$$\Pr_X \left(\Gamma^r \cdot (\hat{Y} \oplus \hat{Y}') = 0 | X \oplus X' = \Delta^0 \right) = \frac{1}{2}(1 + \epsilon_a \epsilon_d). \tag{11}$$

Online Stage: Recovering the Correct Key.

In the actual attack, all PNBs are assigned the same fixed value as in Step 3 (or random values). We guess partial key bits, *i.e.* the non-PNBs in X, and compute the probability $\Pr_X\left(\Gamma^r \cdot (\hat{Y} \oplus \hat{Y}') = 0 | X \oplus X' = \Delta^0\right)$. When the key bits are correctly guessed, the equation (11) holds. Otherwise, a random event will be observed, *i.e.*

$$\Pr_X\left(\Gamma^r \cdot (\hat{Y} \oplus \hat{Y}') = 0 | X \oplus X' = \Delta^0\right) = \frac{1}{2}. \tag{12}$$

We set a predetermined threshold, and count the number that $\Gamma^r \cdot (\hat{Y} \oplus \hat{Y}') = 0$ occurs when multiple input pairs are used. If the number is larger than the threshold, the guess for the non-PNBs is selected as a candidate key. The unique correct key can be further recovered from the remaining candidate keys by exhaustive search.

New Assignment for PNBs.

In Step 3 of the pre-processing stage or the online stage, the assignments for PNBs are usually all zeros or random values. In [DGSS23], Dey et al. proposed a new assignment for the PNBs. For a set of consecutive PNBs $\{a, a-1, a-2, \cdots\}$, the assignment for the a-th PNB is 1 and the assignments for the remaining PNBs are 0. Dey et al. find this assignment $100\cdots00$ can provide a better backward correlation than the all zero assignment and the random assignment.

2.5 Complexity of PNB-Based Key Recovery

Assume cipher E can be divided into three sub-ciphers E_1, E_m and E_2, such that $E = E_2 \circ E_m \circ E_1$. There exists a differential characteristic and a differential-linear distinguisher for E_1 and E_m with probability p and forward correlation ϵ_d, respectively. For E_2, backward correlation ϵ_a is obtained with n PNBs.

The total correlation for $E_2 \circ E_m$ is $\epsilon_d\epsilon_a$. Using the Neyman-Pearson lemma, for advantage α, required number of input pairs N for $E_2 \circ E_m$ is

$$N = \left(\frac{\sqrt{\alpha \log(4)} + 3\sqrt{1-(\epsilon_d\epsilon_a)^2}}{\epsilon_d\epsilon_a}\right)^2. \tag{13}$$

By [AFK+08], the time complexity for $E_2 \circ E_m$ is

$$2^{256-n}N + 2^{256-\alpha}. \tag{14}$$

By using the technique in [BLT20], the attack needs to be repeated for p^{-1} times. Thus the total data complexity is $p^{-1}N$, and the total time complexity is

$$p^{-1}2^{256-n}N + p^{-1}2^{256-\alpha}. \tag{15}$$

3 More Accurate Correlation of the Differential-Linear Distinguisher for Four-Round ChaCha

At FSE 2023, Bellini *et al.* [BGG+23] found a two-round differential-linear distinguisher $\Delta^1 \to \Gamma_0^3$ with the correlation $2^{-30.15}$ from the second round to the third round and a two-round linear approximation $\Gamma_0^3 \to \Gamma^5$ with the correlation 2^{-2} from the fourth round to the fifth round, and obtained a four-round differential-linear distinguisher $\Delta^1 \to \Gamma^5$ with the correlation $2^{-30.15} \cdot (2^{-2})^2 = 2^{-34.15}$ by splicing the two-round differential-linear distinguisher and the two-round linear approximation, where

$$\begin{aligned}
\Delta^1 &= X_3[25] \oplus X_3[5] \oplus X_7[28] \oplus X_7[12] \oplus X_{11}[25] \oplus X_{11}[21] \oplus X_{15}[21] \oplus X_{15}[13], \\
\Gamma_0^3 &= X_2[4,3,0] \oplus X_7[20,4,0] \oplus X_8[20,19] \oplus X_{13}[4], \\
\Gamma^5 &= X_2[0] \oplus X_6[7] \oplus X_6[19] \oplus X_{10}[12] \oplus X_{14}[0].
\end{aligned} \tag{16}$$

In this paper, we find that the intermediate linear mask Γ_0^3 can be replaced by other linear masks. From Proposition 1 we know that the correlation of $\Delta^1 \to \Gamma^5$ can be improved with the differential-linear hull as follows.

$$\mathrm{Aut}(\Delta^1, \Gamma^5) = \sum_{\Gamma^3} \mathrm{Aut}(\Delta^1, \Gamma^3) C(\Gamma^3, \Gamma^5)^2. \tag{17}$$

We use the automatic tool SAT to search for the linear approximation $\Gamma^3 \to \Gamma^5$ from the fourth round to the fifth round when the output linear mask is fixed as Γ^5 in the equation (16). Using a similar method as in [LWR16, SWW21], the propagation of a linear approximation can be transformed into the SAT instance. Then the SAT solver CryptoMiniSat [SNC09] is used to solve the SAT instance. If the SAT instance is satisfiable, then the SAT solver will return a solution related to the linear approximation $\Gamma^3 \to \Gamma^5$. The detailed search process for the linear approximation is presented in Appendix A. Multiple linear masks Γ_i^3 are obtained when the correlations $C(\Gamma_i^3, \Gamma^5)$ in the SAT instance are restricted as $\pm 2^{-2}$ and $\pm 2^{-3}$. The detailed linear masks Γ_i^3 are shown in Table 3 and Table 4.

Table 3: Linear masks Γ_i^3 when $C(\Gamma_i^3, \Gamma^5) = \pm 2^{-2}$

	Linear mask
Γ_0^3	$X_2[4,3,0] \oplus X_7[20,4,0] \oplus X_8[20,19] \oplus X_{13}[4]$
Γ_1^3	$X_2[4,0] \oplus X_7[20,4,3,0] \oplus X_8[20,19] \oplus X_{13}[4]$
Γ_2^3	$X_2[4,0] \oplus X_7[20,4,0] \oplus X_8[20] \oplus X_{13}[4,3]$
Γ_3^3	$X_2[4,3,0] \oplus X_7[20,4,3,0] \oplus X_8[20] \oplus X_{13}[4,3]$

Table 4: Linear masks Γ_i^3 when $C(\Gamma_i^3, \Gamma^5) = \pm 2^{-3}$

	Linear mask
Γ_4^3	$X_2[4,2,0] \oplus X_7[20,4,0] \oplus X_8[20,19] \oplus X_{13}[4]$
Γ_5^3	$X_2[4,3,2,0] \oplus X_7[20,4,3,0] \oplus X_8[20,19] \oplus X_{13}[4]$
Γ_6^3	$X_2[4,0] \oplus X_7[20,4,2,0] \oplus X_8[20,19] \oplus X_{13}[4]$
Γ_7^3	$X_2[4,3,0] \oplus X_7[20,4,3,2,0] \oplus X_8[20,19] \oplus X_{13}[4]$
Γ_8^3	$X_2[4,3,2,0] \oplus X_7[20,4,0] \oplus X_8[20] \oplus X_{13}[4,3]$
Γ_9^3	$X_2[4,3,0] \oplus X_7[20,4,2,0] \oplus X_8[20] \oplus X_{13}[4,3]$
Γ_{10}^3	$X_2[4,0] \oplus X_7[20,4,3,2,0] \oplus X_8[20] \oplus X_{13}[4,3]$
Γ_{11}^3	$X_2[4,2,0] \oplus X_7[20,4,3,0] \oplus X_8[20] \oplus X_{13}[4,3]$
Γ_{12}^3	$X_2[4,3,0] \oplus X_7[20,4,0] \oplus X_8[20,18] \oplus X_{13}[4]$
Γ_{13}^3	$X_2[4,0] \oplus X_7[20,4,3,0] \oplus X_8[20,18] \oplus X_{13}[4]$
Γ_{14}^3	$X_2[4,0] \oplus X_7[20,4,0] \oplus X_8[20,19,18] \oplus X_{13}[4,3]$
Γ_{15}^3	$X_2[4,3,0] \oplus X_7[20,4,3,0] \oplus X_8[20,19,18] \oplus X_{13}[4,3]$

To use the differential-linear hull as in equation (17), we need to compute the correlation $\mathrm{Aut}(\Delta^1, \Gamma_i^3)$ by experiments. However, it's difficult to directly evaluate the correlation $\mathrm{Aut}(\Delta^1, \Gamma_i^3)$ by experiments because the correlation is too small. To overcome this, Bellini *et al.* [BGG+23] partitioned the masks Γ_0^3 into several partitions, and used the Piling-up Lemma to evaluate the correlation $\mathrm{Aut}(\Delta^1, \Gamma^3)$. The same method is also used to evaluate the correlation $\mathrm{Aut}(\Delta^1, \Gamma_i^3)$ in this paper.

Γ_i^3 is partitioned into two partitions $\Gamma_{i,0}^3$ and $\Gamma_{i,1}^3$, such that $\Gamma_i^3 = \Gamma_{i,0}^3 \oplus \Gamma_{i,1}^3$, where $\Gamma_{i,0}^3$ represents the linear mask for the seventh word X_7^3, and $\Gamma_{i,1}^3$ represents the linear mask for the other word. For example, $\Gamma_{0,0}^3 = X_7[20,4,0]$, and $\Gamma_{0,1}^3 = X_2[4,3,0] \oplus X_8[20,19] \oplus X_{13}[4]$. The correlations $\mathrm{Aut}(\Delta^1, \Gamma_{i,0}^3)$ and $\mathrm{Aut}(\Delta^1, \Gamma_{i,1}^3)$ are evaluated by experiments with 2^{48} samples, and the correlation $\mathrm{Aut}(\Delta^1, \Gamma_i^3)$ is computed as $\mathrm{Aut}(\Delta^1, \Gamma_i^3) = \mathrm{Aut}(\Delta^1, \Gamma_{i,0}^3) \cdot \mathrm{Aut}(\Delta^1, \Gamma_{i,1}^3)$ by the Piling-up Lemma. The detailed correlations are shown in Table 5.

Table 5: Correlation with different intermediate linear masks

i	$\text{Aut}(\Delta^1, \Gamma^3_{i,0})$	$\text{Aut}(\Delta^1, \Gamma^3_{i,1})$	$\text{Aut}(\Delta^1, \Gamma^3_i)$
1	$-2^{-17.7}$	$-2^{-12.8}$	$2^{-30.5}$
2	$-2^{-17.7}$	$-2^{-12.8}$	$2^{-30.5}$
3	$-2^{-17.7}$	$-2^{-12.8}$	$2^{-30.5}$
4	$-2^{-17.7}$	$-2^{-14.0}$	$2^{-31.7}$
5	$-2^{-17.7}$	$-2^{-14.0}$	$2^{-31.7}$
6	$-2^{-21.3}$	$-2^{-12.8}$	$2^{-34.1}$
7	$-2^{-21.1}$	$-2^{-12.8}$	$2^{-33.9}$
8	$-2^{-17.7}$	$-2^{-14.0}$	$2^{-31.7}$
9	$-2^{-21.3}$	$-2^{-12.8}$	$2^{-34.1}$
10	$-2^{-21.1}$	$-2^{-12.8}$	$2^{-33.9}$
11	$-2^{-17.7}$	$-2^{-14.0}$	$2^{-31.7}$
12	$-2^{-17.7}$	$-2^{-14.8}$	$2^{-32.5}$
13	$-2^{-17.7}$	$-2^{-14.8}$	$2^{-32.5}$
14	$-2^{-17.7}$	$-2^{-14.8}$	$2^{-32.5}$
15	$-2^{-17.7}$	$-2^{-14.8}$	$2^{-32.5}$

Therefore, the correlation $\text{Aut}(\Delta^1, \Gamma^5)$ can be evaluated as

$$\text{Aut}(\Delta^1, \Gamma^5) \approx \sum_{i \in \{0,1,2,\ldots,15\}} \text{Aut}(\Delta^1, \Gamma^3_i) C(\Gamma^3_i, \Gamma^5)^2 \approx 2^{-32.2} \tag{18}$$

by the differential-linear hull.

To verify the effect of the differential-linear hull, we estimate the correlations $\text{Aut}(\Delta^1, \Gamma^5)$ with 2^{32} samples when the differences Δ^1 are $X_3[25] \oplus X_3[5]$, $X_7[28] \oplus X_7[12]$, $X_{11}[25] \oplus X_{11}[21]$ and $X_{15}[21] \oplus X_{15}[13]$, respectively. The detailed correlations are shown in Table 6, where DL means that the correlation $\text{Aut}(\Delta^1, \Gamma^5)$ is evaluated by the single differential-linear distinguisher as

$$\text{Aut}(\Delta^1, \Gamma^5) = \text{Aut}(\Delta^1, \Gamma^3_0) C(\Gamma^3_0, \Gamma^5)^2,$$

and DLH_1 and DLH_2 mean that the correlation $\text{Aut}(\Delta^1, \Gamma^5)$ is evaluated by the differential-linear hull as follows,

$$\begin{aligned} \text{DLH}_1: \quad \text{Aut}(\Delta^1, \Gamma^5) &= \sum_{0 \le i \le 3} \text{Aut}(\Delta^1, \Gamma^3_i) C(\Gamma^3_i, \Gamma^5)^2, \\ \text{DLH}_2: \quad \text{Aut}(\Delta^1, \Gamma^5) &= \sum_{0 \le i \le 15} \text{Aut}(\Delta^1, \Gamma^3_i) C(\Gamma^3_i, \Gamma^5)^2. \end{aligned} \tag{19}$$

From Table 6 we know that the differential-linear hull provides closer correlations to the experimental correlations than a single differential-linear distinguisher. Particularly, the more intermediate linear masks Γ^3_i are used, the closer the evaluated correlations are to the experimental correlations. Also, there exists a gap between the experimental method and the differential-linear hull method. We conjecture this happens because some intermediate linear masks are not used in our differential-linear hull.

4 Differential-Linear Attacks on Reduced Round ChaCha

In this section, we present the differential-linear attacks on reduced round ChaCha. The source codes for the evaluation of backward correlations are publicly available at https://github.com/newstudent2018/Differential-Linear-Cryptanalysis-of-Reduced-Round-ChaCha.

Table 6: Comparison of the correlation $\mathrm{Aut}(\Delta^1, \Gamma^5)$

Δ^1	Experimental correlation	DL	DLH_1	DLH_2
$X_3[25] \oplus X_3[5]$	$2^{-11.0}$	$2^{-14.0}$	$2^{-12.0}$	$2^{-11.6}$
$X_7[28] \oplus X_7[12]$	$2^{-13.2}$	$2^{-17.0}$	$2^{-15.1}$	$2^{-14.4}$
$X_{11}[25] \oplus X_{11}[21]$	$2^{-7.9}$	$2^{-11.5}$	$2^{-9.5}$	$2^{-9.2}$
$X_{15}[21] \oplus X_{15}[13]$	$2^{-6.3}$	$2^{-10.3}$	$2^{-8.3}$	$2^{-7.6}$

The reduced round ChaCha E is divided into three parts $E = E_2 \circ E_m \circ E_1$, where E_1 covers one round, E_m covers four rounds, and E_2 covers the remaining rounds. At FSE 2023, Bellini *et al.* [BGG+23] found a one-round differential distinguisher $\Delta^0 \xrightarrow{E_1} \Delta^1$ with probability 2^{-7} for E_1 and a four-round differential-linear distinguisher $\Delta^1 \xrightarrow{E_m} \Gamma^5$ with correlation $2^{-34.15}$ for E_m, where

$$\begin{aligned} &\Delta^0 = X_{15}[29] \oplus X_{15}[9], \\ &\Delta^1 = X_3[25] \oplus X_3[5] \oplus X_7[28] \oplus X_7[12] \oplus X_{11}[25] \oplus X_{11}[21] \oplus X_{15}[21] \oplus X_{15}[13], \\ &\Gamma^5 = X_2[0] \oplus X_6[7] \oplus X_6[19] \oplus X_{10}[12] \oplus X_{14}[0]. \end{aligned} \tag{20}$$

By splicing the one-round differential distinguisher and the four-round differential-linear distinguisher, they obtained a five-round differential-linear distinguisher $\Delta^0 \xrightarrow{E_m \circ E_1} \Gamma^5$ for $E_m \circ E_1$.

Based on the distinguisher, Bellini *et al.* evaluated the backward correlation of E_2 when all PNBs are assigned with 0, and presented differential-linear attacks for reduced round ChaCha with the PNB approach.

In this section, we use the five-round differential-linear distinguisher $\Delta^0 \xrightarrow{E_m \circ E_1} \Gamma^5$ to attack reduced round ChaCha with the PNB approach. By using the differential-linear hull as in Section 3, the correlation of the four-round differential-linear distinguisher $\Delta^1 \xrightarrow{E_m} \Gamma^5$ is improved from $2^{-34.15}$ to $2^{-32.2}$. The PNB approach is also used when $100 \cdots 00$ is assigned to consecutive PNBs as in [DGSS23], and 0 is assigned to PNBs that are not consecutive, the backward correlation of E_2 is improved. The time complexity is significantly reduced because of the differential-linear hull and the new assignment for PNBs.

To search for a better PNB set, the search process is divided into two steps, and two thresholds γ_0 and γ_1 are used, where $\gamma_0 > \gamma_1 > 0$. γ_0 is used to directly select PNBs, and γ_1 is used to select candidate PNBs that need further evaluation. In the first step, the key bit is selected in the PNB set PNB when it provides higher backward correlation than γ_0, and the key bit is selected in the candidate PNB set PNB_{pre} when the backward correlation is lower than γ_0 and higher than γ_1. In the second step, a greedy algorithm is used by selecting the PNBs one by one. In the i-th iteration of the second step, a temporary PNB set PNB_{temp} is constructed by adding a key bit from PNB_{pre} into the PNB set PNB, and the backward correlation is tested with the temporary PNB set PNB_{temp}. The key bit with the maximal backward correlation will be selected as the i-th PNB of the second step. The iteration is repeated until all PNBs are selected. The detailed search process is shown in Algorithm 1.

4.1 Discussion of Algorithm 1

In this subsection, we will analyze the efficiency of Algorithm 1 by presenting an instance. From equation (10) of Subsection 2.4 we know that the backward correlation ϵ_a is evaluated by

$$\Pr_X \left(\Gamma^r \cdot (X^r \oplus X'^r) = \Gamma^r \cdot (\hat{Y} \oplus \hat{Y}') \right) = \frac{1}{2}(1 + \epsilon_a). \tag{21}$$

Algorithm 1 The algorithm for searching a PNB set

Input: Two threshold correlations γ_0 and γ_1, a size n of a PNB set;
Output: The PNB set and its backward correlation;

Initialize the PNB set $PNB = \emptyset$;
Initialize the candidate set $PNB_{pre} = \emptyset$;
for $i \in \{0, 1, \cdots, 255\}$ **do**
  Test the backward correlation ϵ_i when the i-th key bit is selected as a PNB;
  if $\gamma_0 \leq \epsilon_i$ **then**
    $PNB = PNB \cup \{i\}$;
  else if $\gamma_1 \leq \epsilon_i < \gamma_0$ **then**
    $PNB_{pre} = PNB_{pre} \cup \{i\}$;
  end if
end for
while $\#PNB < n$ **do**
  for $i \in PNB_{pre}$ **do**
    $PNB_{temp} = PNB \cup \{i\}$;
    Test the backward correlation ϵ_i with the PNB set PNB_{temp};
  end for
  Choose the index i with the maximal backward correlation ϵ_i, $PNB = PNB \cup \{i\}$;
end while
return the PNB set PNB and the corresponding backward correlation;

Similar as in [WLHL23], under the assumption of independence, the backward correlation ϵ_a can be computed by

$$\epsilon_a = (\epsilon'_a)^2, \tag{22}$$

where ϵ'_a is evaluated by

$$\Pr_X \left(\Gamma^r \cdot X^r = \Gamma^r \cdot \hat{Y} \right) = \frac{1}{2}(1 + \epsilon'_a). \tag{23}$$

To show the efficiency of Algorithm 1, we construct a toy cipher as shown in Figure 2 by splicing the 1.5-round QR function, 0.5-round QR function and the last key addition operations. For the toy cipher, there exists a 1.5-round differential-linear distinguisher $\Delta^0 \to \Gamma^{1.5}$, where $\Delta^0 = X_2[31]$ and $\Gamma^{1.5} = X_0[13] \oplus X_0[18] \oplus X_2[23]$. We use the equation (24) to evaluate the backward correlation ϵ'_a of the last 0.5-round toy cipher when the PNBs are selected from the keys k_1 and k_2.

$$\Pr_X \left(\Gamma^{1.5} \cdot X^{1.5} = \Gamma^{1.5} \cdot \hat{Y} \right) = \frac{1}{2}(1 + \epsilon'_a). \tag{24}$$

Now we consider three candidate PNBs $k_{1,17}$, $k_{2,20}$ and $k_{2,21}$, *i.e.* the 17th bit of k_1, and the 20th and 21st bits of k_2. We select one bit or two bits from the set $\{k_{1,17}, k_{2,20}, k_{2,21}\}$ as PNBs, and evaluate the backward correlation ϵ'_a experimentally. The corresponding backward correlations are shown in Table 7. If we use a fixed threshold 0.5 to select two PNBs, the two bits $k_{1,17}$ and $k_{2,20}$ with higher backward correlations will be selected, and the backward correlation for the PNB set $\{k_{1,17}, k_{2,20}\}$ is experimentally evaluated as 0.66 when the PNBs are assigned random value. If we use Algorithm 1 to select two PNBs with thresholds $\gamma_0 = 0.6$ and $\gamma_1 = 0.2$, the key bit $k_{2,20}$ with the highest backward correlation will be selected first. Then we evaluate the backward correlations for the temporary PNB sets $\{k_{1,17}, k_{2,20}\}$ and $\{k_{2,20}, k_{2,21}\}$ experimentally when the PNBs are assigned random value, and obtain backward correlations 0.66 and 0.688 respectively. Thus from Algorithm 1 we obtain a better PNB set $\{k_{2,20}, k_{2,21}\}$ with a higher backward correlation 0.688.

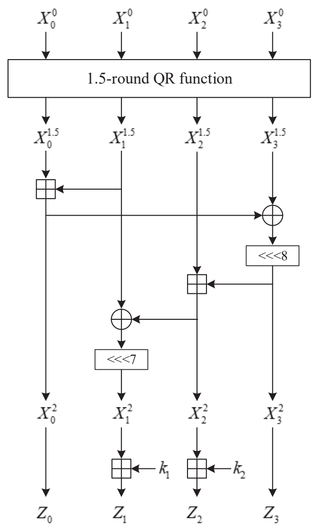


Figure 2: A toy cipher

This improvement is related to the mutual influence of PNBs. When we compute $\hat{Y}$ as in Subsection 2.4, random differences are introduced to PNBs, and propagate to the middle data pair $(X^{1.5}, \hat{Y})$. For the middle linear mask $\Gamma^{1.5}$, the backward difference propagations of PNBs $k_{1,17}$ and $k_{2,20}$ have little mutual influence on each other. However, the backward difference propagations of $k_{2,20}$ and $k_{2,21}$ have much mutual influence on each other. Thus, when $k_{2,20}$ has been selected as a PNB, selecting $k_{2,21}$ as a PNB will be better than selecting $k_{1,17}$ although $k_{2,21}$ performs worse as a single PNB than $k_{1,17}$.

Similarly, when more PNBs are used for ChaCha, many PNBs may have mutual influences. Some candidate bits may have better performance when certain PNBs have been selected. When this happens, Algorithm 1 may help to find a better PNB set.

Table 7: Comparison of the backward correlations for the toy cipher

	single PNB			fixed threshold	Algorithm 1
PNB location	$k_{1,17}$	$k_{2,20}$	$k_{2,21}$	$k_{1,17}$, $k_{2,20}$	$k_{2,20}$, $k_{2,21}$
backward correlation	0.51	0.75	0.50	0.66	0.688

4.2 Differential-Linear Attack on 7-Round ChaCha

For 7-round ChaCha, E_2 covers two rounds. We use Algorithm 1 to search PNBs with two thresholds $\gamma_0 = 0.5$ and $\gamma_1 = 0.2$. In the first step, 147 PNBs are selected. In the second step, the other 22 PNBs are selected. The 169 PNBs are listed below. To improve the backward correlation, we assign $100\cdots00$ to consecutive PNBs and assign 0 to PNBs that are not consecutive. When 2^{36} samples are used, we can get a backward correlation $0.00027 = 2^{-11.855}$.

0, 1, 2, 3, 4, 5, 6, 7, 8, 19, 20, 31, 32, 33, 34, 35, 36, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 71, 72, 73, 74, 77, 78, 79, 80, 83, 84, 85, 86, 89, 90, 95, 99, 100, 103, 104, 105, 106, 107, 108, 109, 123, 124, 125, 126, 127, 128, 129, 140, 141, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 198, 199, 200, 204, 205, 206, 207, 210, 211, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 244, 245, 246, 247, 255, 248, 9, 130, 142, 21, 91, 212, 110, 231, 22, 143, 232, 111, 228, 10, 201, 249, 115, 147, 14, 81, 26.

To compare the effect of different methods, we also evaluate the backward correlation with other PNB set and assignment method. The detailed backward correlations are listed in Table 8. In Table 8, Experiment 1 is the method used in [BGG+23] with 160 PNBs. When the assignment for consecutive PNBs is $10\cdots00$ as shown in Experiment 2, the backward correlation is improved from $2^{-14.18}$ to $2^{-9.29}$. In this paper, we use the method in Experiment 3. Algorithm 1 is used to search PNBs with the two thresholds $\gamma_0 = 0.5$ and $\gamma_1 = 0.2$ in Experiment 3, and 169 PNBs are obtained with the backward correlation $2^{-11.855}$. Because the number of PNBs is improved in Experiment 3, the time complexity is further reduced.

Table 8: Comparison of the PNBs and the backward correlation for 7-round ChaCha

	assignment	threshold	PNBs	backward correlation
Experiment 1	$00\cdots00$	$\gamma = 0.34$	160	$2^{-14.18}$
Experiment 2	$10\cdots00$	$\gamma = 0.34$	160	$2^{-9.29}$
Experiment 3	$10\cdots00$	$\gamma_0 = 0.5$, $\gamma_1 = 0.2$	169	$2^{-11.855}$

Complexity analysis. The correlation of four-round differential-linear distinguisher for E_m is $\epsilon_d = 2^{-32.2}$ and the backward correlation is $\epsilon_a = 2^{-11.855}$ for 169 PNBs. When $\alpha = 80$, from formula (13) in Subsection 2.5 we know that required number of input pairs is

$$N = \left(\frac{\sqrt{\alpha \log(4)} + 3\sqrt{1 - \epsilon_a^2 \epsilon_d^2}}{\epsilon_a \epsilon_d} \right)^2 = 2^{95.63}. \tag{25}$$

Since the differential probability for E_1 is 2^{-7}, the attacks need to be repeated for 2^7 times. Then the total data complexity is $2^{95.63} \times 2^7 = 2^{102.63}$. From formula (15) in Subsection 2.5 we know that the total time complexity is $2^7 \cdot 2^{256-169} \cdot N + 2^7 \cdot 2^{256-\alpha} = 2^{189.7}$.

4.3 Differential-Linear Attack on 7.25-Round ChaCha

The 7.25-round ChaCha is an extension of 7-round ChaCha by adding the 7.25-th functions as shown in Figure 3. For 7.25-round ChaCha, E_2 covers 2.25 rounds. We use Algorithm 1 to search PNBs with two thresholds $\gamma_0 = 0.5$ and $\gamma_1 = 0.2$. In the first step, 111 PNBs are selected. In the second step, the other 22 PNBs are selected. The 133 PNBs are listed below. When $100\cdots00$ is assigned to consecutive PNBs, and 0 is assigned to PNBs that are not consecutive, we can get backward correlations $2^{-11.25}$ when 2^{36} samples are used.

20, 31, 44, 45, 46, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 71, 72, 73, 74, 77, 80, 83, 84, 85, 86, 89, 90, 95, 99, 108, 109, 123, 124, 125, 126, 127, 128, 129, 140, 141, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 198, 199, 200, 204, 205, 206, 207, 210, 211, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 244, 245, 246, 247, 255, 142, 47, 21, 248, 110, 7, 8, 130, 91, 212, 100, 231, 111, 232, 143, 22, 48, 249, 51, 35, 81, 0.

To compare the effect of different methods, we also evaluate the backward correlation with other PNB set and assignment method for 7.25-round ChaCha. The detailed backward correlations are listed in Table 9. In Table 9, Experiment 4 is the method used in [BGG+23] with 133 PNBs. When the assignment for consecutive PNBs is $10 \cdots 00$ as shown in Experiment 5, the backward correlation is improved from $2^{-16.85}$ to $2^{-11.8}$. In this paper, we use the method in Experiment 6. Algorithm 1 is used to search PNBs with the two thresholds $\gamma_0 = 0.5$ and $\gamma_1 = 0.2$ in Experiment 6, and 133 PNBs are obtained with backward correlation $2^{-11.25}$.

Table 9: Comparison of the PNBs and the backward correlation for 7.25-round ChaCha

	assignment	threshold	PNBs	backward correlation
Experiment 4	$00 \cdots 00$	$\gamma = 0.28$	133	$2^{-16.85}$
Experiment 5	$10 \cdots 00$	$\gamma = 0.28$	133	$2^{-11.8}$
Experiment 6	$10 \cdots 00$	$\gamma_0 = 0.5,\ \gamma_1 = 0.2$	133	$2^{-11.25}$

Complexity analysis. The correlation of four-round differential-linear distinguisher for E_m is $\epsilon_d = 2^{-32.2}$ and the backward correlation is $\epsilon_a = 2^{-11.25}$ for 133 PNBs. When $\alpha = 45$, from formula (13) in Subsection 2.5 we know that required number of input pairs is

$$N = \left(\frac{\sqrt{\alpha \log(4)} + 3\sqrt{1 - \epsilon_a^2 \epsilon_d^2}}{\epsilon_a \epsilon_d} \right)^2 = 2^{93.8}. \tag{26}$$

Since the differential probability for E_1 is 2^{-7}, the attacks need to be repeated for 2^7 times. Then the total data complexity is $2^{93.8} \times 2^7 = 2^{100.8}$. From formula (15) in Subsection 2.5 we know that the total time complexity is $2^7 \cdot 2^{256-133} \cdot N + 2^7 \cdot 2^{256-\alpha} = 2^{223.9}$.

5 Equivalence of Reduced Round ChaCha

In this paper, we will present the equivalence between $(R + 0.25)$-round and $(R + 0.5)^{\oplus}$-round ChaCha, where $R \in \{1, 2, 3, \cdots\}$. For simplicity, we directly consider the case of $R = 7$, and prove the equivalence between 7.25-round and $7.5^{\oplus}$-round ChaCha. For the other case with different R, the equivalence between $(R+0.25)$-round and $(R+0.5)^{\oplus}$-round ChaCha can be proved similarly.

The 7.25-round ChaCha presented in [MIM22, BGG+23, DGSS23] and the $7.5^{\oplus}$-round ChaCha presented in [BGG+23, WLHL23] are both reduced round versions of 8-round ChaCha, which can also be seen as the extensions of 7-round ChaCha by adding the 7.25-th and $7.5^{\oplus}$-th round functions as shown in Figure 3 and Figure 4. Denote by $X^{7.25}$ the output of 7.25-round ChaCha, and $Z^{7.25}$ the key stream produced by 7.25-round ChaCha, that is, $Z^{7.25} = X^{7.25} \boxplus X$. Similarly, denote by $X^{7.5^{\oplus}}$ the output of $7.5^{\oplus}$-round ChaCha, and $Z^{7.5^{\oplus}}$ the key stream produced by $7.5^{\oplus}$-round ChaCha, that is, $Z^{7.5^{\oplus}} = X^{7.5^{\oplus}} \boxplus X$.

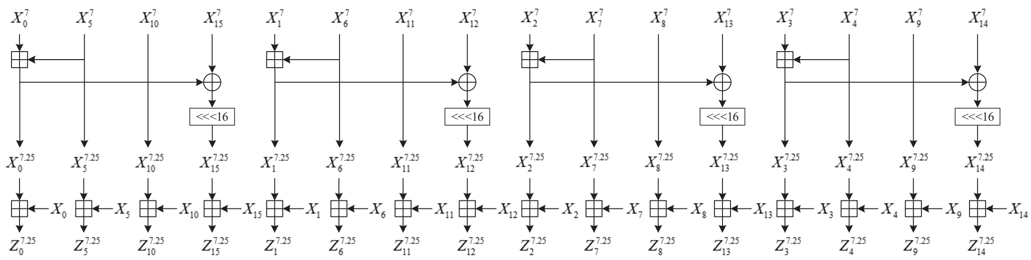


Figure 3: The 7.25-th round function of ChaCha

Compared to 7.25-round ChaCha, $7.5^{\oplus}$-round ChaCha adopts four more additions. It seems that $7.5^{\oplus}$-round ChaCha provides more security than 7.25-round ChaCha. However, in this section, we will show that $7.5^{\oplus}$-round ChaCha and 7.25-round ChaCha provide

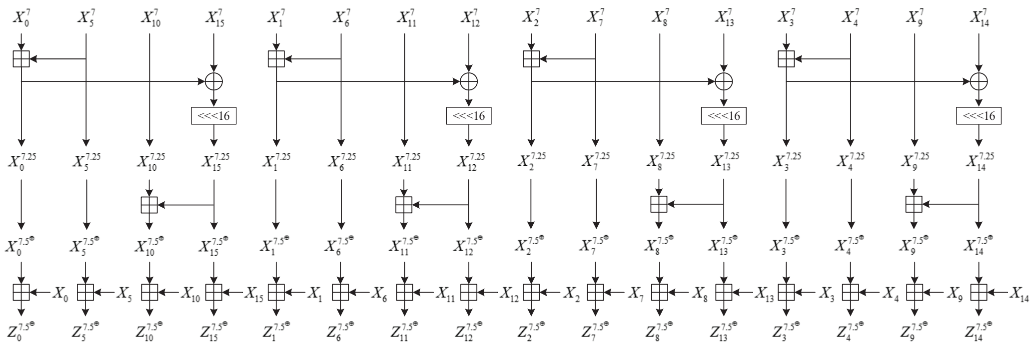


Figure 4: The $7.5^{\oplus}$-th round function of ChaCha

the same security against chosen(known) plaintext attacks. In other words, if we can find a chosen(known) plaintext attack on 7.25-round ChaCha, then we can also attack $7.5^{\oplus}$-round ChaCha, and vice versa.

Because of the commutativity of modular additions, *i.e.* $a \boxplus b \boxplus c = a \boxplus c \boxplus b$, we exchange the order of the last two layers of modular addition in Figure 4, and present the equivalent $7.5^{\oplus}$-th round functions of ChaCha with the structure as shown in Figure 5.

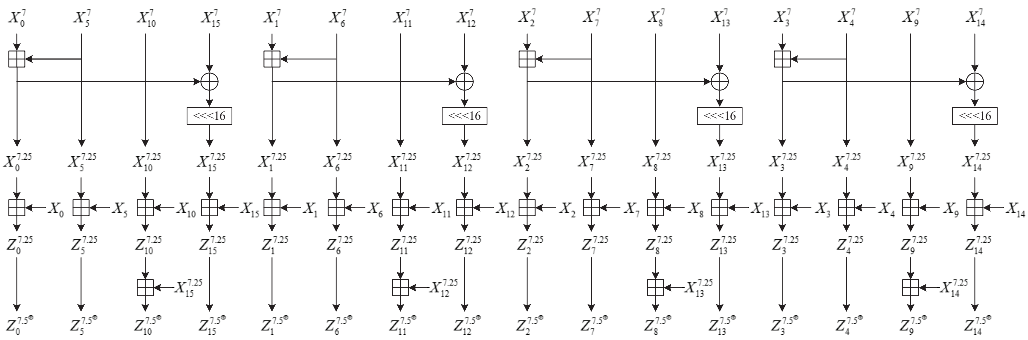


Figure 5: Equivalent $7.5^{\oplus}$-th round function of ChaCha with commutative modular additions

Denote by X_{IV} the IV value $(X_{12}, X_{13}, X_{14}, X_{15})$. From Figure 5 we know that the key streams $Z^{7.25}$ and $Z^{7.5^{\oplus}}$ can be converted to each other when the four words ($X_{12}^{7.25}$, $X_{13}^{7.25}$, $X_{14}^{7.25}$, $X_{15}^{7.25}$) are obtained from (X_{IV}, $Z^{7.25}$) or (X_{IV},$Z^{7.5^{\oplus}}$). Thus when the IV value X_{IV} is known, the key streams $Z^{7.25}$ and $Z^{7.5^{\oplus}}$ can be converted to each other. For simplicity, we use a function G to represent the conversion from $(X_{\mathrm{IV}}, Z^{7.5^{\oplus}})$ to $(X_{\mathrm{IV}}, Z^{7.25})$, *i.e.* $(X_{\mathrm{IV}}, Z^{7.25}) = G(X_{\mathrm{IV}}, Z^{7.5^{\oplus}})$.

Denote by $\mathbb{X}_{\mathrm{IV}}$, $\mathbb{Z}^{7.25}$ and $\mathbb{Z}^{7.5^{\oplus}}$ the IV set and the key stream sets of 7.25-round and $7.5^{\oplus}$-round ChaCha, respectively. Assume 7.25-round ChaCha can be attacked by certain chosen(known) plaintext method F, and the key k can be recovered from ($\mathbb{X}_{\mathrm{IV}}$, $\mathbb{Z}^{7.25}$) as follows.

$$(\mathbb{X}_{\mathrm{IV}}, \mathbb{Z}^{7.25}) \xrightarrow{F} k. \tag{27}$$

Then $7.5^{\oplus}$-round ChaCha can also be attacked based on F, and the key k can be recovered from ($\mathbb{X}_{\mathrm{IV}}$, $\mathbb{Z}^{7.5^{\oplus}}$) as follows.

$$(\mathbb{X}_{\mathrm{IV}}, \mathbb{Z}^{7.5^{\oplus}}) \xrightarrow{G} (\mathbb{X}_{\mathrm{IV}}, \mathbb{Z}^{7.25}) \xrightarrow{F} k, \tag{28}$$

Thus, when 7.25-round ChaCha can be attacked by certain chosen(known) plaintext method, $7.5^{\oplus}$-round ChaCha can also be attacked. On the other hand, when $7.5^{\oplus}$-round ChaCha can be attacked by certain chosen(known) plaintext method, 7.25-round ChaCha can also be attacked. Thus, 7.25-round ChaCha and $7.5^{\oplus}$-round ChaCha provide the same security against chosen(known) plaintext attacks.

This property can be extended to general $(R + 0.25)$-round and $(R + 0.5)^{\oplus}$-round ChaCha, where $R \in \{1, 2, 3, \cdots\}$, *i.e.* $(R + 0.25)$-round ChaCha and $(R + 0.5)^{\oplus}$-round ChaCha provide the same security against chosen(known) plaintext attacks.

The PNB-based differential-linear attack is one of the chosen plaintext attacks. Thus, $(R+0.25)$-round ChaCha and $(R+0.5)^{\oplus}$-round ChaCha provide the same security against the PNB-based differential-linear attack. On the other hand, we can also directly prove the equivalent security against the PNB-based differential-linear attack between 7.25-round ChaCha and $7.5^{\oplus}$-round ChaCha, and the detailed proof is presented in Appendix B. By the equivalent security, improved differential-linear attack of $7.5^{\oplus}$-round ChaCha can also be obtained based on the differential-linear attack of 7.25-round ChaCha as in Subsection 4.3. The time complexity is $2^{223.9}$, which improves the previously best-known attack by 2^{19}.

6 Conclusion

In this paper, we study the security of reduced round ChaCha. First, based on the differential-linear hull, we improve the correlation of a four-round differential-linear distinguisher proposed at FSE 2023 by finding the other intermediate linear masks. Then, we present the differential-linear cryptanalysis of 7-round and 7.25-round ChaCha based on the PNB approach. By using the assignment $100 \cdots 00$ for consecutive PNBs, the backward correlation is significantly increased. Because of the improved correlation of the four-round differential-linear distinguisher and the improved backward correlation, improved key recovery attacks of 7-round and 7.25-round ChaCha are obtained. Finally, we show that $(R+0.25)$-round and $(R+0.5)^{\oplus}$-round ChaCha provide the same security against chosen(known) plaintext attacks. As a result, improved key recovery attack of $7.5^{\oplus}$-round ChaCha is obtained based on the key recovery attack of 7.25-round ChaCha. How to present better differential-linear distinguishers and how to present longer differential-linear cryptanalysis for reduced round ChaCha will be our future work.

Acknowledgments

We thank the anonymous reviewers for their careful reading of our paper and helpful comments. This work is supported by the National Natural Science Foundation of China(Grant Numbers 62202494 and 62372464).

References

[AFK+08] Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, and Christian Rechberger. New features of latin dances: Analysis of Salsa, ChaCha, and Rumba. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 470–488. Springer, 2008.

[BBC+22] Christof Beierle, Marek Broll, Federico Canale, Nicolas David, Antonio Flórez-Gutiérrez, Gregor Leander, María Naya-Plasencia, and Yosuke Todo.

Improved differential-linear attacks with applications to ARX ciphers. *J. Cryptol.*, 35(4):29, 2022.

[BC14] Eli Biham and Yaniv Carmeli. An improvement of linear cryptanalysis with addition operations with applications to FEAL-8X. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, volume 8781 of *Lecture Notes in Computer Science*, pages 59–76. Springer, 2014.

[BDK02] Eli Biham, Orr Dunkelman, and Nathan Keller. Enhancing differential-linear cryptanalysis. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 254–266. Springer, 2002.

[Ber05] Daniel J Bernstein. Salsa20. Technical Report 2005/025. eSTREAM, ECRYPT Stream Cipher Project, 2005. http://www.ecrypt.eu.org/stream/papers.html.

[Ber08] Daniel J Bernstein. ChaCha, a variant of Salsa20. 2008. http://cr.yp.to/chacha.html.

[BGG+23] Emanuele Bellini, David Gérault, Juan Grados, Rusydi H. Makarim, and Thomas Peyrin. Boosting differential-linear cryptanalysis of ChaCha7 with MILP. *IACR Trans. Symmetric Cryptol.*, 2023(2):189–223, 2023.

[BLN17] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-linear cryptanalysis revisited. *J. Cryptol.*, 30(3):859–888, 2017.

[BLT20] Christof Beierle, Gregor Leander, and Yosuke Todo. Improved differential-linear attacks with applications to ARX ciphers. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 329–358, Cham, 2020. Springer International Publishing.

[BODKW19] Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman. DLCT: A new tool for differential-linear cryptanalysis. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 313–342, Cham, 2019. Springer International Publishing.

[BS90] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

[BSS+15] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015*, pages 175:1–175:6. ACM, 2015.

[Cha] Chacha Usage & Deployment. https://ianix.com/pub/chacha-deployment.html.

[CM16] Arka Rai Choudhuri and Subhamoy Maitra. Significantly improved multi-bit differentials for reduced round Salsa and ChaCha. *IACR Trans. Symmetric Cryptol.*, 2016(2):261–287, 2016.

[CN20] Murilo Coutinho and T. C. Souza Neto. New multi-bit differentials to improve attacks against ChaCha. *IACR Cryptol. ePrint Arch.*, page 350, 2020.

[CN21] Murilo Coutinho and Tertuliano C. Souza Neto. Improved linear approximations to ARX ciphers and attacks against ChaCha. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 711–740. Springer, 2021.

[DDSM22] Sabyasachi Dey, Chandan Dey, Santanu Sarkar, and Willi Meier. Revisiting cryptanalysis on ChaCha from crypto 2020 and eurocrypt 2021. *IEEE Trans. Inf. Theory*, 68(9):6114–6133, 2022.

[DGM23] Sabyasachi Dey, Hirendra Kumar Garai, and Subhamoy Maitra. Cryptanalysis of reduced round ChaCha - new attack & deeper analysis. *IACR Trans. Symmetric Cryptol.*, 2023(1):89–110, 2023.

[DGSS22] Sabyasachi Dey, Hirendra Kumar Garai, Santanu Sarkar, and Nitin Kumar Sharma. Revamped differential-linear cryptanalysis on reduced round ChaCha. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 86–114. Springer, 2022.

[DGSS23] Sabyasachi Dey, Hirendra Kumar Garai, Santanu Sarkar, and Nitin Kumar Sharma. Enhanced differential-linear attacks on reduced round ChaCha. *IEEE Trans. Inf. Theory*, 69(8):5318–5336, 2023.

[DPU+16] Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for ARX with provable bounds: SPARX and LAX. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016*, pages 484–513, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[DS17] Sabyasachi Dey and Santanu Sarkar. Improved analysis for reduced round Salsa and ChaCha. *Discret. Appl. Math.*, 227:58–69, 2017.

[DS20] Sabyasachi Dey and Santanu Sarkar. Proving the biases of Salsa and ChaCha in differential attack. *Des. Codes Cryptogr.*, 88(9):1827–1856, 2020.

[HSH+06] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee. HIGHT: A new block cipher suitable for low-resource device. In Louis Goubin and Mitsuru Matsui, editors, *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, volume 4249 of *Lecture Notes in Computer Science*, pages 46–59. Springer, 2006.

[HTW15] Tao Huang, Ivan Tjuawinata, and Hongjun Wu. Differential-linear cryptanalysis of ICEPOLE. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 243–263. Springer, 2015.

[Leu16] Gaëtan Leurent. Improved differential-linear cryptanalysis of 7-round Chaskey with partitioning. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 344–371. Springer, 2016.

[LH94] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 17–25. Springer, 1994.

[LNS+23] Yunwen Liu, Zhongfeng Niu, Siwei Sun, Chao Li, and Lei Hu. Rotational differential-linear cryptanalysis revisited. *J. Cryptol.*, 36(1):3, 2023.

[LSL21] Yunwen Liu, Siwei Sun, and Chao Li. Rotational cryptanalysis from a differential-linear perspective - practical distinguishers for round-reduced FRIET, Xoodoo, and Alzette. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 741–770. Springer, 2021.

[Lu12] Jiqiang Lu. A methodology for differential-linear cryptanalysis and its applications - (extended abstract). In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 69–89. Springer, 2012.

[LWR16] Yunwen Liu, Qingju Wang, and Vincent Rijmen. Automatic search of linear trails in ARX with applications to SPECK and Chaskey. In Mark Manulis, Ahmad-Reza Sadeghi, and Steve A. Schneider, editors, *Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*, volume 9696 of *Lecture Notes in Computer Science*, pages 485–499. Springer, 2016.

[Mai16] Subhamoy Maitra. Chosen IV cryptanalysis on reduced round ChaCha and Salsa. *Discret. Appl. Math.*, 208:88–97, 2016.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[MIM22] Shotaro Miyashita, Ryoma Ito, and Atsuko Miyaji. PNB-focused differential cryptanalysis of ChaCha stream cipher. In Khoa Nguyen, Guomin Yang, Fuchun Guo, and Willy Susilo, editors, *Information Security and*

Privacy - 27th Australasian Conference, ACISP 2022, Wollongong, NSW, Australia, November 28-30, 2022, Proceedings, volume 13494 of *Lecture Notes in Computer Science*, pages 46–66. Springer, 2022.

[MMH+14] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, volume 8781 of *Lecture Notes in Computer Science*, pages 306–323. Springer, 2014.

[NSLL22] Zhongfeng Niu, Siwei Sun, Yunwen Liu, and Chao Li. Rotational differential-linear distinguishers of ARX ciphers with arbitrary output linear masks. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2022.

[Sch13] Ernst Schulte-Geers. On CCZ-equivalence of addition mod 2^n. *Des. Codes Cryptogr.*, 66(1-3):111–127, 2013.

[Sin05] Carsten Sinz. Towards an optimal CNF encoding of boolean cardinality constraints. In Peter van Beek, editor, *Principles and Practice of Constraint Programming - CP 2005, 11th International Conference, CP 2005, Sitges, Spain, October 1-5, 2005, Proceedings*, volume 3709 of *Lecture Notes in Computer Science*, pages 827–831, Berlin, Heidelberg, 2005. Springer.

[SNC09] Mate Soos, Karsten Nohl, and Claude Castelluccia. Extending SAT solvers to cryptographic problems. In Oliver Kullmann, editor, *Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings*, volume 5584 of *Lecture Notes in Computer Science*, pages 244–257. Springer, 2009.

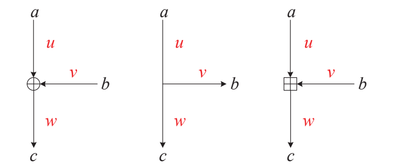
[SWW21] Ling Sun, Wei Wang, and Meiqin Wang. Accelerating the search of differential and linear characteristics with the SAT method. *IACR Trans. Symmetric Cryptol.*, 2021(1):269–315, 2021.

[SZFW13] Zhenqing Shi, Bin Zhang, Dengguo Feng, and Wenling Wu. Improved key recovery attacks on reduced-round Salsa20 and ChaCha. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *Information Security and Cryptology – ICISC 2012*, pages 337–351, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[WLHL23] Shichang Wang, Meicheng Liu, Shiqi Hou, and Dongdai Lin. Moving a step of ChaCha in syncopated rhythm. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 273–304, Cham, 2023. Springer.

A SAT Model of Linear Approximations for ChaCha

There are four basic operations in ChaCha, including XOR, branching, rotation, and modular addition. For rotation operation $x \lll r$, the output linear mask β can be directly obtained from input linear mask α by $\beta = \alpha \lll r$. Suppose $a = (a_{n-1}, a_{n-2}, ..., a_0)$, $b = (b_{n-1}, b_{n-2}, ..., b_0)$ and $c = (c_{n-1}, c_{n-2}, ..., c_0)$ are n-bit variables, and $u = (u_{n-1}, u_{n-2}, ..., u_0)$, $v = (v_{n-1}, v_{n-2}, ..., v_0)$, $w = (w_{n-1}, w_{n-2}, ..., w_0)$ are the corresponding n-bit linear masks of a, b and c. For the remaining three operations as shown in Figure 6, the propagation of linear masks can be transformed into a system of logical equations in CNF as follows.



(a) XOR (b) Branching (c) Modular addition

Figure 6: Basic operations of ChaCha

A.1 SAT Model for XOR Operation

For the n-bit XOR operation $a \oplus b = c$ as shown in Figure 6 (a), the correlation for the linear approximation $(u, v) \to w$ of the XOR operation is nonzero if and only if $u = v = w$, so a valid linear approximation $(u, v) \to w$ of the XOR operation can be described by the following clauses.

$$\left.\begin{aligned} u_i \vee \overline{v_i} &= 1 \\ \overline{u_i} \vee v_i &= 1 \\ u_i \vee \overline{w_i} &= 1 \\ \overline{u_i} \vee w_i &= 1 \end{aligned}\right\} 0 \le i \le n-1 \tag{29}$$

A.2 SAT Model for Branching Operation

For the n-bit branching operation $a = b = c$ as shown in Figure 6 (b), the correlation for the linear approximation $u \to (v, w)$ of the branching operation is nonzero if and only if $u = v \oplus w$ for $i \in \{0, 1, ..., n-1\}$, so a valid linear approximation $u \to (v, w)$ of the branching operation can be described by the following clauses.

$$\left.\begin{aligned} u_i \vee v_i \vee \overline{w_i} &= 1 \\ u_i \vee \overline{v_i} \vee w_i &= 1 \\ \overline{u_i} \vee v_i \vee w_i &= 1 \\ \overline{u_i} \vee \overline{v_i} \vee \overline{w_i} &= 1 \end{aligned}\right\} 0 \le i \le n-1 \tag{30}$$

A.3 SAT Model for Modular Addition

For the n-bit modular addition operation $a \boxplus b = c$ as shown in Figure 6 (c), Schulte-Geers [Sch13] proposed a method to calculate the correlations of linear approximations, and Liu *et al.* [LWR16] presented the SAT model for the linear approximation of modular addition.

Proposition 2. [Sch13] *Let $z = (z_{n-1}, z_{n-2}, ..., z_0)$ be an n-bit vector satisfying $z \oplus (z \gg 1) \oplus ((u \oplus v \oplus w) \gg 1) = 0$, $z_{n-1} = 0$, where u and v are the input linear masks, w is the output linear mask in a linear approximation for addition modulo 2^n. Then the correlation for the linear approximation $(u, v) \to w$ of the modular addition can be given by*

$$C((u, v), w) = 1_{w \oplus v \preceq z} 1_{w \oplus u \preceq z} (-1)^{(w \oplus v)\cdot(w \oplus u)} 2^{-\mathrm{wt}(z)} \tag{31}$$

where $x \preceq y$ *means* $x_i \leq y_i$ *for* $i \in \{0, 1, ..., n-1\}$ *and*

$$1_{x \preceq y} = \begin{cases} 1, \text{ if } x \preceq y, \\ 0, \text{ otherwise.} \end{cases}$$

Based on Proposition 2, the following constraints can be used to describe the relation between the linear masks (u, v) and w with the auxiliary variable z.

$$\begin{cases} z_{n-1} = 0 \\ z_{n-2} = u_{n-1} \oplus v_{n-1} \oplus w_{n-1} \\ z_j = z_{j+1} \oplus u_{j+1} \oplus v_{j+1} \oplus w_{j+1} \\ z_i \geq w_i \oplus u_i \\ z_i \geq w_i \oplus v_i \end{cases} \tag{32}$$

where $0 \leq i \leq n-1, 0 \leq j \leq n-3$.

The XOR operation in equation (32) can be described by the method of Subsection A.1, and the inequality $z_i \geq w_i \oplus u_i$ in equation (32) can be translated into the following two clauses in an SAT instance.

$$\begin{cases} \overline{w_i} \vee u_i \vee z_i = 1 \\ w_i \vee \overline{u_i} \vee z_i = 1 \end{cases} \tag{33}$$

A.4 SAT Model for Objective Function

We need to calculate the product of the correlations for all modular additions as the total correlation of a linear approximation. Let $z^j = (z^j_{n-1}, z^j_{n-2}, ..., z^j_0)$ be the n-bit vector related to the linear approximation for the j-th modular addition as shown in Proposition 2. In order to find linear approximations with high correlations, the total Hamming weight of z^j, *i.e.* $\sum_j \mathrm{wt}(z^j) = \sum_{i,j} z^j_i$, need to be limited. Particularly, we can set an objective function $\sum_{i,j} z^j_i \leq k$ for some positive integer k, and search for linear approximations with the correlation $2^{-\sum_j wt(z^j)} \geq 2^{-k}$.

Following the approaches in [LWR16, SWW21], we can use the sequential encoding method [Sin05] to describe the objective function like $\sum_{j=0}^{n-1} x_j \leq k$ by the following clauses in an SAT instance,

$$\begin{array}{l} \overline{x_0} \vee s_{0,0} = 1 \\ \overline{s_{0,j}} = 1, 1 \leq j \leq k-1 \\ \left.\begin{array}{l} \overline{x_i} \vee s_{i,0} = 1 \\ \overline{s_{i-1,0}} \vee s_{i,0} = 1 \\ \left.\begin{array}{l} \overline{x_i} \vee \overline{s_{i-1,j-1}} \vee s_{i,j} = 1 \\ \overline{x_{i-1,j}} \vee s_{i,j} = 1 \end{array}\right\} 1 \leq j \leq k-1 \\ \overline{x_i} \vee \overline{s_{i-1,k-1}} = 1 \end{array}\right\} 1 \leq i \leq n-2 \\ \overline{x_{n-1}} \vee \overline{s_{n-2,k-1}} = 1 \end{array} \tag{34}$$

where $s_{i,j}$ $(1 \leq i \leq n-2,\ 1 \leq j \leq k-1)$ are binary auxiliary variables.

A.5 Algorithm to Search for Linear Approximations

Algorithm 2 illustrates the process to search for the linear approximation $\Gamma^3 \rightarrow \Gamma^5$ with prescribed bound 2^{-k} on the correlation when the output linear mask is fixed as Γ^5 in the equation (16).

Once a linear approximation is obtained, we can add a clause into the SAT model as in Line 11 of Algorithm 2 to remove the linear approximation, and search for other linear approximations. For example, if an assignment $[1, 0, 0, 1, 1]$ is obtained for variables x_0, x_1, x_2, x_3 and x_4, we can remove the assignment by add a clause $\overline{x_0} \vee x_1 \vee x_2 \vee \overline{x_3} \vee \overline{x_4} = 1$. Finally, all the linear approximations with correlations higher than 2^{-k} will be obtained.

Algorithm 2 Automatic search of the linear approximation $\Gamma^3 \rightarrow \Gamma^5$ for two-round ChaCha with prescribed bound 2^{-k} on the correlation

Input: output linear mask Γ^5, bound 2^{-k} on the correlation;
Output: input linear mask Γ^3;
1: **for** $4 \leq i \leq 5$ **do**
2: Construct the SAT model for the linear approximations of the operations in the i-th round function of ChaCha as in Subsections A.1, A.2 and A.3;
3: **end for**
4: Construct the SAT model for the constraint $\sum_{i,j} z_i^j \leq k$ as in Subsection A.4;
5: Set the output linear mask as Γ^5;
6: Flag=1;
7: **while** Flag==1 **do**
8: Use the SAT solver to solve the SAT model;
9: **if** the SAT solver returns a solution **then**
10: **output** the corresponding linear approximation;
11: Add a clause into the SAT model to remove the linear approximation;
12: **else**
13: **break**
14: **end if**
15: **end while**
16: **if** no linear approximation is outputted **then**
17: There exists no linear approximation such that the correlation $C(\Gamma^3, \Gamma^5) \geq 2^{-k}$;
18: **end if**

B Equivalent Security against PNB-Based Differential-Linear Attack between $(R+0.25)$-Round and $(R+0.5)^{\oplus}$-Round ChaCha

The equivalent security against chosen(known) plaintext attack in Section 5 is obtained based on the conversion between $(R + 0.25)$-round and $(R + 0.5)^{\oplus}$-round ChaCha. In this section, we directly present the equivalent security against PNB-based differential-linear attack between $(R + 0.25)$-round and $(R + 0.5)^{\oplus}$-round ChaCha, *i.e.* the backward correlations are the same for $(R + 0.25)$-round and$(R + 0.5)^{\oplus}$-round ChaCha when the same PNBs are used.

For simplicity, we first consider the case of $R = 7$, and present the equivalent security against PNB-based differential-linear attack between 7.25-round and $7.5^{\oplus}$-round ChaCha. Without loss of generality, assume the differential-linear distinguisher $\Delta^0 \rightarrow \Gamma^5$ covers five rounds. Let $Round^{-2.25}$ be the decryption function of ChaCha from $X^{7.25}$ to X^5, *i.e.* $X^5 = Round^{-2.25}(X^{7.25})$, let $Round^{-2.5^{\oplus}}$ be the decryption function of ChaCha from $X^{7.5^{\oplus}}$ to X^5, *i.e.* $X^5 = Round^{-2.5^{\oplus}}(X^{7.5^{\oplus}})$, and let g be the encryption function from $X^{7.25}$ to $X^{7.5^{\oplus}}$ as shown in Figure 7. Then we have

$$Round^{-2.25} = Round^{-2.5^{\oplus}} \circ g. \qquad (35)$$

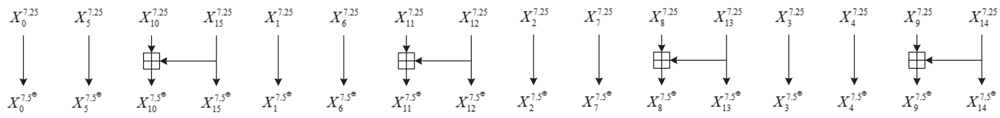


Figure 7: The encryption function $X^{7.5^{\oplus}} = g(X^{7.25})$

Theorem 1. *Let (X, X') be the input difference pair of ChaCha, where $X' = X \oplus \Delta^0$. $(\overline{X}, \overline{X'})$ are constructed from (X, X') such that all PNBs are assigned fixed value (or random value) while the other bits take the same values as (X, X'). Then $X_i = \overline{X_i}$ and $X'_i = \overline{X'_i}$ for $i \in \{0, 1, 2, 3, 12, 13, 14, 15\}$. Let the backward correlation ϵ_a for 7.25-round ChaCha be computed by*

$$\Pr_X \left(\Gamma^5 \cdot \left(Round^{-2.25}(X^{7.25} \boxplus X \boxminus \overline{X}) \oplus Round^{-2.25}(X'^{7.25} \boxplus X' \boxminus \overline{X'}) \oplus X^5 \oplus X'^5\right) = 0\right) = \frac{1}{2}(1 + \epsilon_a), \tag{36}$$

and let the backward correlation ϵ'_a for $7.5^{\oplus}$-round ChaCha be computed by

$$\Pr_X \left(\Gamma^5 \cdot \left(Round^{-2.5^{\oplus}}(X^{7.5^{\oplus}} \boxplus X \boxminus \overline{X}) \oplus Round^{-2.5^{\oplus}}(X'^{7.5^{\oplus}} \boxplus X' \boxminus \overline{X'}) \oplus X^5 \oplus X'^5\right) = 0\right) = \frac{1}{2}(1 + \epsilon'_a), \tag{37}$$

then we have $\epsilon_a = \epsilon'_a$.

Proof. We only need to show that $Round^{-2.25}(X^{7.25} \boxplus X \boxminus \overline{X})$ and $Round^{-2.5^{\oplus}}(X^{7.5^{\oplus}} \boxplus X \boxminus \overline{X})$ are the same functions, *i.e.*

$$Round^{-2.25}(X^{7.25} \boxplus X \boxminus \overline{X}) = Round^{-2.5^{\oplus}}(X^{7.5^{\oplus}} \boxplus X \boxminus \overline{X}). \tag{38}$$

From equation (35), we only need to prove that the equivalent equation (39) holds.

$$g(X^{7.25} \boxplus X \boxminus \overline{X}) = X^{7.5^{\oplus}} \boxplus X \boxminus \overline{X}, \tag{39}$$

where g is the encryption function from $X^{7.25}$ to $X^{7.5^{\oplus}}$ as shown in Figure 7.

From Figure 7 we have

$$g(X^{7.25} \boxplus X \boxminus \overline{X}) = g(X^{7.25}) \boxplus g(X \boxminus \overline{X}) = X^{7.5^{\oplus}} \boxplus g(X \boxminus \overline{X}). \tag{40}$$

Because $(X \boxminus \overline{X})_i = 0$ for $i \in \{12, 13, 14, 15\}$, from Figure 7 we have

$$g(X \boxminus \overline{X}) = X \boxminus \overline{X}. \tag{41}$$

By equations (40) and (41), we know that equation (38) and equation (39) hold.

Then by equations (36),(37) and (38), we have $\epsilon_a = \epsilon'_a$. □

From Theorem 1 we know that the backward correlations are the same for 7.25-round and $7.5^{\oplus}$-round ChaCha when the same PNBs are used. Then by equations (13) and (15) in Subsection 2.5 we know that the PNB-based differential-linear attacks for 7.25-round and $7.5^{\oplus}$-round ChaCha have the same time complexity.

This property can be extended to general $(R + 0.25)$-round and $(R + 0.5)^{\oplus}$-round ChaCha, where $R \in \{1, 2, 3, \cdots\}$. The PNB-based differential-linear attack has the same effect on $(R + 0.25)$-round and $(R + 0.5)^{\oplus}$-round ChaCha.