Mixderive: A New Framework of Deriving Linear Approximations and Improved Differential-Linear Distinguishers for ChaCha (*Full Version*)

Zhengting Li, Lin Ding[†], Xinhai Wang, Jiang Wan

Information Engineering University, Zhengzhou 450001, China

Abstract. ChaCha is a well-known ARX-based cipher and has become one of the most widely used ciphers in the real world. In this paper, a systematic three-case framework called *Mixderive* to find linear approximations for ChaCha is proposed. By this new framework, new linear approximations for 3.5- and 4-round ChaCha are found, which are significantly better than the existing linear approximations proposed at EUROCRYPT 2021 and ASIACRYPT 2022. These improvements confirm the effectiveness of *Mixderive*. In addition, new 2- and 2.5-round linear approximations for ChaCha are found by *Mixderive*. Based on these new findings, new differential-linear distinguishers for 7- and 7.5-round ChaCha256 with complexities $2^{162.28}$ and $2^{247.08}$ are proposed, which improve the best known distinguishers by factors of $2^{4.61}$ and $2^{4.46}$, respectively. To the best of our knowledge, both cryptanalytic results are the best.

Keywords: Cryptanalysis · Linear approximation · Differential-linear distinguisher · ChaCha · Stream cipher.

1 Introduction

Cryptography plays a crucial role in the modern digital world. One significant aspect of cryptography is symmetric-key cryptography, where the same key is used for both encryption and decryption of data. Symmetric-key ciphers offer efficiency and simplicity, making them suitable for the applications where speed and low computational overhead are crucial. Among symmetric-key ciphers, the ARX-based design has gained considerable attention. ARX stands for modular Addition, word-wise Rotation and bit-wise XOR. ARX-based design has not only good security properties, but also high efficiency. Up to now, ARX-based design has been used in stream ciphers (e.g., Salsa [6] and ChaCha [7]), block ciphers (e.g., Sparx [21]), cryptographic permutations (e.g., Sparkle [3]), Hash functions (e.g., Blake [2]) and MAC algorithms (e.g., Chaskey [27]).

Salsa [6] is an ARX-based cipher designed by Bernstein in 2005 and its 12-round version was accepted into the final eSTREAM software portfolio. ChaCha

[7], a variant of Salsa designed in 2008, can provide better diffusion and higher resistance to cryptanalysis without slowing down encryption. ChaCha has been used by Google as one of the cipher suites for the new Transport Layer Security (TLS) 1.3 [23] in Chrome and Android. In addition, it is also used as a pseudo-random number generator in any operating system running Linux kernel 4.8 or newer and widely used in many protocols like SSH. It has become one of the most widely used ciphers in the real world. The ChaCha stream cipher consists of two versions, i.e., a 256-bit key version called ChaCha256 and a 128-bit key version called ChaCha128. In this paper, we mainly concentrate on the cryptanalysis of ChaCha256 due to its wide deployment.

1.1 Related Works

Many cryptanalytic attacks on ChaCha256 have been published, since it was proposed in 2008. These attacks generally fall into two categories: distinguishers and key recovery attacks. This paper only focuses on distinguishers and does not discuss key recovery attacks. For the existing key recovery attacks on ChaCha, we refer to [1, 28, 24, 10, 20, 11, 4, 18, 26, 19, 29, 5, 17, 30, 15].

At FSE 2017, Choudhuri and Maitra [10] presented the first differential-linear distinguishers for 4-, 4.5-, 5- and 6-round ChaCha256 by considering the multi-bit differentials together with linear approximations. At EUROCRYPT 2021, Coutinho and Souza [14] proposed a new technique to find linear approximations for ARX ciphers, and presented an improved differential-linear distinguisher for 6-round ChaCha256 with complexity 2^{51} and two differential-linear distinguishers for 7-round ChaCha256 with complexities 2^{224} and 2^{218}, respectively. However, Dey et al. revisited their work in [16] and found the distinguisher with complexity 2^{218} is invalid, while the distinguisher with complexity 2^{224} is valid. At ASIACRYPT 2022, Coutinho et al. [13] proposed a new way to approach the derivation of linear approximations by viewing the cipher in terms of simpler subrounds and presented an improved differential-linear distinguisher for 7-round ChaCha256 with complexity 2^{214}. Soon after, at FSE 2023, Bellini et al. [5] introduced the idea of using a carefully crafted MILP tool to find linear approximations, and presented an improved differential-linear distinguisher for 7-round ChaCha256 with complexity $2^{166.89}$. They also proposed the first-ever differential-linear distinguisher for 7.5-round ChaCha256 with complexity $2^{251.54}$.

1.2 Our Contributions

In this paper, we propose a new framework of deriving linear approximations for ChaCha and present improved differential-linear distinguishers for 7- and 7.5-round ChaCha256. We provide a summary of our cryptanalytic results in Table 1, with a comparison of the existing works.

- *Technical Contributions.* In this paper, a new rule to derive linear approximations for ChaCha is proposed, and then a systematic three-case framework

called *Mixderive* to find linear approximations for ChaCha is provided. In this new framework, the different rules that expand the same bits or sums are utilized to derive linear approximations in a mixed mode, rather than utilized individually. This is the most significant difference between *Mixderive* and the known approach proposed at ASIACRYPT 2022. By *Mixderive*, new linear approximations for 3.5- and 4-round ChaCha are found, which are significantly better than the existing linear approximations proposed at EUROCRYPT 2021 and ASIACRYPT 2022. These improvements confirm the effectiveness of *Mixderive*. In addition, we present new linear approximations for 2- and 2.5-round ChaCha, which are used in our improved differential-linear distinguishers for 7- and 7.5-round ChaCha256, respectively.
– *Improved Differential-Linear Distinguishers.* Based on the new linear approximations found by *Mixderive*, new differential-linear distinguishers for 7- and 7.5-round ChaCha256 with complexities $2^{158.6}$ and $2^{243.4}$ are proposed, which improve the best known distinguishers by factors of $2^{4.61}$ and $2^{4.46}$, respectively. To the best of our knowledge, both cryptanalytic results are the best.

Table 1. Summary of differential-linear distinguishers for ChaCha256.

Rounds	Time Complexity	Data Complexity	Ref.
4	2^{6}	2^{6}	[10]
4.5	2^{12}	2^{12}	
5	2^{16}	2^{16}	
6	2^{116}	2^{116}	
7	2^{224}	2^{224}	[14]
	2^{214}	2^{214}	[13]
	$2^{166.89}$	$2^{166.89}$	[5]
	$\mathbf{2^{162.28}}$	$\mathbf{2^{162.28}}$	**This paper**
7.5	$2^{251.54}$	$2^{251.54}$	[5]
	$\mathbf{2^{247.08}}$	$\mathbf{2^{247.08}}$	**This paper**

Organization of the Paper. In Sect. 2, a brief description of ChaCha256 is given, the cryptanalytic methods and techniques used in this paper are introduced, and a review of the approach to derive linear approximations for ChaCha proposed at ASIACRYPT 2022 is given. Our new framework of deriving linear approximations for ChaCha is introduced in Sect. 3. In Sect. 4 and 5, improved linear approximations and new linear approximations for ChaCha obtained by *Mixderive* are presented. In Sect. 6, improved differential-linear distinguishers for 7- and 7.5-round ChaCha256 are given. Sect. 7 concludes this paper.

2 Preliminaries

In this section, a brief description of ChaCha256, and the basic idea of differential-linear cryptanalysis are introduced. To improve readability, we provide a list of the main notations used throughout the paper in Table 2.

Table 2. List of the main notations used throughout the paper.

Notation	Description
X	The state matrix of ChaCha256 consisting of 16 words
$X^{(0)}$	The initial state matrix of ChaCha256
$X^{(r)}$	The state matrix after application of r round functions
$X^{[s]}$	The state matrix after application of s subround functions
$x_i^{(r)}$	The i-th word of the state matrix $X^{(r)}$
$x_{i,j}^{(r)}$	The j-th bit of i-th word of the state matrix $X^{(r)}$
$x_i^{(r)}[j_0, j_1, \ldots, j_t]$	The sum $x_{i,j_0}^{(r)} \oplus x_{i,j_1}^{(r)} \oplus \cdots \oplus x_{i,j_t}^{(r)}$
$x \boxplus y$	Addition of x and y modulo 2^{32}
$x \oplus y$	Bitwise XOR of x and y
$x \lll l$	Rotation of x by l bits to the left

2.1 A Brief Description of ChaCha256

In 2008, Bernstein proposed ChaCha as an improvement of Salsa. It consists of two versions, i.e., a 256-bit key version called ChaCha256 and a 128-bit key version called ChaCha128. The description of ChaCha128 is omitted here, since this paper only concentrates on ChaCha256. For complete description of ChaCha, we refer to the specification [7]. The ChaCha256 stream cipher operates on 16 32-bit words, organized as a 4×4 matrix X. The initial state matrix of ChaCha256 is given as follows.

$$X^{(0)} = \begin{pmatrix} x_0^{(0)} & x_1^{(0)} & x_2^{(0)} & x_3^{(0)} \\ x_4^{(0)} & x_5^{(0)} & x_6^{(0)} & x_7^{(0)} \\ x_8^{(0)} & x_9^{(0)} & x_{10}^{(0)} & x_{11}^{(0)} \\ x_{12}^{(0)} & x_{13}^{(0)} & x_{14}^{(0)} & x_{15}^{(0)} \end{pmatrix} = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ t_0 & v_0 & v_1 & v_2 \end{pmatrix}$$

where $c_0 = 0x61707865$, $c_1 = 0x3320646e$, $c_2 = 0x79622d32$ and $c_3 = 0x6b206574$ are four constant words, $k_0, k_1, \cdots, k_7$ are eight key words, t_0 is a counter word and v_0, v_1, v_2 are three nonces. In the subsequent content, we will refer to the nonce and counter words together as IV words.

The initial state matrix is updated by the *Round function*, which consists of four parallel applications of the function *Quarter Round* (QR). Taking four

words $x_a^{(r-1)}, x_b^{(r-1)}, x_c^{(r-1)}, x_d^{(r-1)}$ as input, we can obtain four output words by the function QR via four intermediate words :

$$\begin{aligned}
&x_{a'}^{(r-1)} = x_a^{(r-1)} \boxplus x_b^{(r-1)}; x_{d'}^{(r-1)} = \left(x_d^{(r-1)} \oplus x_{a'}^{(r-1)}\right) \lll 16;\\
&x_{c'}^{(r-1)} = x_c^{(r-1)} \boxplus x_{d'}^{(r-1)}; x_{b'}^{(r-1)} = \left(x_b^{(r-1)} \oplus x_{c'}^{(r-1)}\right) \lll 12;\\
&x_a^{(r)} = x_{a'}^{(r-1)} \boxplus x_{b'}^{(r-1)}; x_d^{(r)} = \left(x_{d'}^{(r-1)} \oplus x_a^{(r)}\right) \lll 8;\\
&x_c^{(r)} = x_{c'}^{(r-1)} \boxplus x_d^{(r)}; x_b^{(r)} = \left(x_{b'}^{(r-1)} \oplus x_c^{(r)}\right) \lll 7.
\end{aligned}$$

The state matrix $X^{(r)}$ is obtained from $X^{(r-1)}$ by applying the function QR. However, there is a difference between odd and even rounds. For odd rounds, the function QR is applied to the four columns (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 $(x_3, x_7, x_{11}, x_{15})$. For even rounds, the function QR is applied to the four diagonals $(x_0, x_5, x_{10}, x_{15}), (x_1, x_6, x_{11}, x_{12}), (x_2, x_7, x_8, x_{13})$ and (x_3, x_4, x_9, x_{14}). The keystream block Z after R-rounds is obtained as the word-wise modular addition of the states $X^{(0)}$ and $X^{(R)}$, i.e., $Z = X^{(0)} \boxplus X^{(R)}$, where $X^{(R)}$ is the state matrix after application of R round functions. It should be noted that the round function of ChaCha is inverse, i.e., $X^{(0)} = \mathit{Round}^{-R}\left(X^{(R)}\right)$, where Round^{-1} denotes the inverse round function of ChaCha.

2.2 Differential-Linear Cryptanalysis

Differential-linear attack [22] is a general cryptanalytic method that combines the ideas of differential attack [8] and linear attack [25]. Let E be a cipher. Assume that E can be divided into two parts E_1 and E_2 such that $E = E_2 \circ E_1$ (see the left side of Fig. 1) and a differential attack and a linear attack can be applied to the first and second parts, respectively. In particular, assume that the differential part $\Delta_{in} \xrightarrow{E_1} \Delta_m$ holds with probability $p = \Pr_{x \in F_2^n}\left(E_1(x) \oplus E_1(x \oplus \Delta_{in}) = \Delta_m\right) = \frac{1}{2}(1 + \varepsilon_d)$, where ε_d is the differential correlation. Let us further assume that the linear part $\Gamma_m \xrightarrow{E_2} \Gamma_{out}$ holds with correlation ε_L, i.e. $\varepsilon_L = \mathbf{Cor}_{x \in F_2^n}\left[\langle \Gamma_m, x\rangle \oplus \langle \Gamma_{out}, E_2(x)\rangle\right]$, By assuming that $E_1(x)$ and $E_2(x)$ are independent random variables, a differential-linear distinguisher $\Delta_{in} \xrightarrow{E} \Gamma_{out}$ with correlation $\varepsilon_d \varepsilon_L^2$ can be obtained. Thus, one can distinguish the cipher E from a random permutation with complexity $O\left(\varepsilon_d^{-2}\varepsilon_L^{-4}\right)$.

In practice, the assumption that $E_1(x)$ and $E_2(x)$ are independent random variables may result in overestimates or underestimates for the correlation. To address this issue, a common solution is adding a middle part E_m and dividing the cipher E into three parts E_1, E_m and E_2 such that $E = E_2 \circ E_m \circ E_1$, see the right side of Fig. 1. Assume that the middle part $\Delta_m \xrightarrow{E_m} \Gamma_m$ holds with correlation $r = \mathbf{Cor}_{x \in \mathcal{S}}\left[\langle \Gamma_m, E_m(x)\rangle \oplus \langle \Gamma_m, E_m(x \oplus \Delta_m)\rangle\right]$, where $\mathcal{S}$ is the set of samples over which the correlation r is computed. This part is generally evaluated experimentally. Now, the differential-linear distinguisher holds

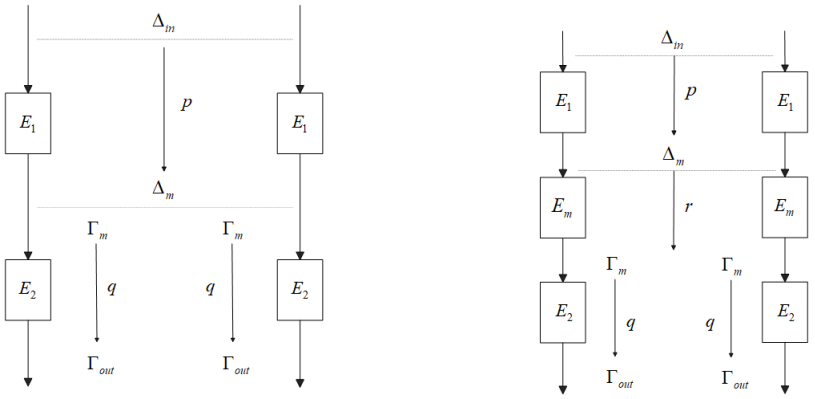

Fig. 1. A classical differential-linear distinguisher (on the left) and a differential-linear distinguisher with experimental evaluation of the correlation r (on the right).

with correlation $\varepsilon_d r \varepsilon_L^2$. Thus, one can distinguish the cipher E from a random permutation with complexity $O\left(\varepsilon_d^{-2} r^{-2} \varepsilon_L^{-4}\right)$.

At FSE 2014, Blondeau et al. [9] presented the following theorem to utilize the idea of differential-linear hull to improve the correlation of differential-linear distinguishers, when some intermediate linear masks are found.

Theorem 1 (Theorem 2 in [9]). *Assume the cipher E can be divided into two parts E_1 and E_2 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*

$$\mathbf{Cor}_E\left(\Delta_m, \Gamma_{out}\right) = \sum_{\Gamma_m} \mathbf{Cor}_{E_1}\left(\Delta_m, \Gamma_m\right) \mathbf{Cor}_{E_2}(\Gamma_m, \Gamma_{out})^2$$

where Γ_m is an intermediate linear mask, $\mathbf{Cor}_{E_1}\left(\Delta_m, \Gamma_m\right)$ and $\mathbf{Cor}_{E_2}\left(\Gamma_m, \Gamma_{out}\right)$ denote the correlations of the differential-linear distinguisher $\Delta_m \xrightarrow{E_1} \Gamma_m$ and the linear approximation $\Gamma_m \xrightarrow{E_2} \Gamma_{out}$.

2.3 The Technique of Right Pair

At CRYPTO 2020, Beierle et al. [4] introduce the concept of *right pair* to amplify the correlation of the differential-linear distinguisher. Formally, the initial states $x, x \oplus \Delta_{in} \in F_2^n$ which satisfy this desired differential Δ_m after E_1 are called *right pairs*. The set of right pairs can be defined as The set of right pairs can be defined as $\mathcal{X} = \{x \in F_2^n \mid E_1(X) \oplus E_1(X \oplus \Delta_{in}) = \Delta_m\}$. In particular, let us assume that the probability to achieve a right pair when the initial states are randomly chosen is p, i.e., $p = \Pr_{x \in F_2^n}\left(E_1\left(X\right) \oplus E_1\left(X \oplus \Delta_{in}\right) = \Delta_m\right)$. The attacker needs to repeat the entire process p^{-1} times on average to achieve the desired correlation. Therefore, the data and time complexities would be multiplied by p^{-1} to obtain the final complexities. This technique is applicable for both distinguisher and key recovery attack.

2.4 A Review of the Approach to Derive Linear Approximations for ChaCha Proposed at ASIACRYPT 2022

Let $\Theta(x,y) = x \oplus y \oplus (x \boxplus y)$ be the carry function of the sum $x \boxplus y$, and $\Theta_i(x,y)$ be the i-th bit of $\Theta(x,y)$, where $\Theta_0(x,y) = 0$ holds. At ASIACRYPT 2022, Coutinho et al. [13] presented an approach to derive linear approximations for ChaCha using the following two simple linear approximations :

$$Pr\left(\Theta_i(x,y) = y_{i-1}\right) = \frac{1}{2}\left(1 + \frac{1}{2}\right), i > 0 \tag{1}$$

$$Pr\left(\Theta_i(x,y) \oplus \Theta_{i-1}(x,y) = 0\right) = \frac{1}{2}\left(1 + \frac{1}{2}\right), i > 0 \tag{2}$$

In their approach, they introduced a concept called *Subround Function* (shortcut *SRF*), denoted by

$$\left(x_a^{[s]}, x_b^{[s]}, x_c^{[s]}, x_d^{[s]}\right) = SRF\left(x_a^{[s-1]}, x_b^{[s-1]}, x_c^{[s-1]}, x_d^{[s-1]}, r_1, r_2\right)$$

where

$$\begin{aligned} x_a^{[s]} =& x_a^{[s-1]} \boxplus x_b^{[s-1]}, \quad x_d^{[s]} = \left(x_d^{[s-1]} \oplus x_a^{[s]}\right) \lll r_1; \\ x_c^{[s]} =& x_c^{[s-1]} \boxplus x_d^{s}, \quad x_b^{[s]} = \left(x_b^{[s-1]} \oplus x_c^{[s]}\right) \lll r_2. \end{aligned}$$

After that, the *QR* function can be rewritten in terms of the *SRF* as follows.

$$\begin{gathered} QR\left(x_a^{(r-1)}, x_b^{(r-1)}, x_c^{(r-1)}, x_d^{(r-1)}\right) = \\ SRF\left(SRF\left(x_a^{(r-1)}, x_b^{(r-1)}, x_c^{(r-1)}, x_d^{(r-1)}, 16, 12\right), 8, 7\right) \end{gathered}$$

By the concept of *SRF*, $X^{(s)} = X^{[2s]}$ holds. Based on this new concept and the two linear approximations above, Coutinho et al. [13] proposed an approach to derive linear approximations for ChaCha at ASIACRYPT 2022. The proposed approach consists of the following five lemmas, which are also used in our new framework.

Lemma 1 (Eqs. 22 and 24 of [13] respectively). *For one active input bit in subround $s-1$ and multiple output bits in subround s, the following linear approximations hold with probability 1 for the SRF with rotation distances r_1 and r_2 when $i > 0$*

$$\begin{aligned} x_{b,i}^{[s-1]} &= x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \\ x_{d,i}^{[s-1]} &= x_{a,i}^{[s]} \oplus x_{d,i+r_1}^{[s]} \end{aligned}$$

Lemma 2 (Lemma 4 of [13]). *Consider the SRF with rotation distances r_1 and r_2. Then we have that*

$$x_{a,0}^{[s-1]} = x_{a,0}^{[s]} \oplus x_{b,r_2}^{[s]} \oplus x_{c,0}^{[s]}$$
$$x_{c,0}^{[s-1]} = x_{c,0}^{[s]} \oplus x_{d,0}^{[s]}$$

Lemma 3 (Lemma 5 of [13]). *For one active input bit in subround $s-1$ and multiple output bits in subround s, the following linear approximations hold with probability $\frac{1}{2}\left(1+\frac{1}{2}\right)$ for the SRF with rotation distances r_1 and r_2 when $i > 0$*

$$x_{a,i}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{b,i+r_2-1}^{[s]} \oplus x_{c,i-1}^{[s]}$$
$$x_{c,i}^{[s-1]} = x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus x_{d,i-1}^{[s]}$$

Lemma 4 (Lemma 6 of [13]). *For two active input bits in subround $s-1$ and multiple output bits in subround s, the following linear approximations hold with probability $\frac{1}{2}\left(1+\frac{1}{2}\right)$ for the SRF with rotation distances r_1 and r_2*

$$x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{a,i-1}^{[s]} \oplus x_{b,i+r_2-1}^{[s]} \oplus x_{c,i-1}^{[s]}$$
$$x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]} = x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus x_{c,i-1}^{[s]} \oplus x_{d,i-1}^{[s]}$$

Lemma 5 (Lemma 7 of [13]). *For two active input bits in subround $s-1$ and multiple output bits in subround s, the following linear approximations hold with probability $\frac{1}{2}\left(1+\frac{1}{2}\right)$ for the SRF with rotation distances r_1 and r_2*

$$x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]}$$
$$x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]} = x_{c,i}^{[s]} \oplus x_{d,i}^{[s]}$$

Compared with the previous works, the proposed approach is simpler to understand and to use. They also claimed that the proposed approach is possible to derive most of the linear approximations (if not all) of previous works. They demonstrated the effectiveness of their approach by giving an improved linear approximation for 4-round ChaCha with correlation 2^{-53}, while the previous linear approximation for 4-round ChaCha presented at EUROCRYPT 2021 [14] holds with correlation 2^{-55}. In Sect. 3, we will introduce a new framework of deriving linear approximations for ChaCha. To confirm the effectiveness of our new framework, we will further improve the correlation from 2^{-53} to -2^{-50}.

3 A New Framework of Deriving Linear Approximations for ChaCha

At ASIACRYPT 2022, Coutinho et al. [13] presented two different lemmas (i.e., **Lemma 4** and **Lemma 5**), to expand the sums $x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]}$ and $x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]}$, respectively. This brings up a question, i.e., which is the better choice. Generally, **Lemma 5** seems a better rule than **Lemma 4**, since it contains fewer active bits than **Lemma 4**, which usually results into a higher correlation. However, this is not absolute. Since the adjacent bits are always expanded together and should be counted as one, it is possible to cancel some active bits (see [12] for a

complete example). Therefore, they concluded that the best rule will be the one that results in other bits being canceled. When deriving linear approximations for ChaCha, both **Lemma 4** and **Lemma 5** should be considered. The key is how to use these two lemmas. Coutinho et al. did not give an approach to tackle this problem in [13]. In this section, we aim at addressing this open problem. To do so, a new rule to expand the bits $x_{a,i}^{[s-1]}$ and $x_{c,i}^{[s-1]}$ $(i > 0)$ will be introduced, and then a new framework of deriving linear approximations for ChaCha will be proposed. The new rule to expand the bits $x_{a,i}^{[s-1]}$ and $x_{c,i}^{[s-1]}$ is given by the following lemma.

Lemma 6. *For one active input bit in subround $s-1$ and multiple output bits in subround s, the following linear approximations hold with probability $\frac{1}{2}\left(1-\frac{1}{2}\right)$ for the SRF with rotation distances r_1 and r_2 when $i > 0$*

$$\begin{aligned} x_{a,i}^{[s-1]} &= x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{a,i-1}^{[s]} \\ x_{c,i}^{[s-1]} &= x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus x_{c,i-1}^{[s]} \end{aligned}$$

Proof. By the round function of ChaCha, we have $x_{a,i}^{[s]} = x_{a,i}^{[s-1]} \oplus x_{b,i}^{[s-1]} \oplus \Theta_i\left(x_a^{[s-1]}, x_b^{[s-1]}\right)$ and $x_{b,i+r_2}^{[s]} = x_{b,i}^{[s-1]} \oplus x_{c,i}^{[s]}$, and then

$$\begin{aligned} & x_{a,i}^{[s-1]} \oplus x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{a,i-1}^{[s]} \\ =& x_{a,i}^{[s-1]} \oplus x_{a,i}^{[s-1]} \oplus x_{b,i}^{[s-1]} \oplus \Theta_i\left(x_a^{[s-1]}, x_b^{[s-1]}\right) \oplus x_{b,i}^{[s-1]} \oplus x_{c,i}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{a,i-1}^{[s-1]} \oplus x_{b,i-1}^{[s-1]} \\ & \oplus \Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) \\ =& x_{a,i-1}^{[s-1]} \oplus x_{b,i-1}^{[s-1]} \oplus \Theta_i\left(x_a^{[s-1]}, x_b^{[s-1]}\right) \oplus \Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) \end{aligned}$$

Considering $\Theta_i\left(x_a^{[s-1]}, x_b^{[s-1]}\right) = x_{a,i-1}^{[s-1]} \cdot x_{b,i-1}^{[s-1]} \oplus \Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right)\left(x_{a,i-1}^{[s-1]} \oplus x_{b,i-1}^{[s-1]}\right)$, then we have

$$\begin{aligned} & \Pr\left(x_{a,i}^{[s-1]} \oplus x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{a,i-1}^{[s]} = 0\right) \\ =& \Pr\left(x_{a,i-1}^{[s-1]} \oplus x_{b,i-1}^{[s-1]} \oplus x_{a,i-1}^{[s-1]} \cdot x_{b,i-1}^{[s-1]} = 0 | \Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) = 0\right) \cdot \\ & \Pr\left(\Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) = 0\right) + \\ & \Pr\left(x_{a,i-1}^{[s-1]} \cdot x_{b,i-1}^{[s-1]} \oplus 1 = 0 | \Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) = 1\right) \cdot \Pr\left(\Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) = 1\right) \\ =& \frac{1}{4}\Pr\left(\Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) = 0\right) + \frac{1}{4}\Pr\left(\Theta_{i-1}\left(x_a^{[s-1]}, x_b^{[s-1]}\right) = 1\right) \\ =& \frac{1}{2}\left(1-\frac{1}{2}\right) \end{aligned}$$

Therefore, the linear approximation $x_{a,i}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{a,i-1}^{[s]}$ holds with probability $\frac{1}{2}\left(1-\frac{1}{2}\right)$.

By the round function of ChaCha, we have $x_{c,i}^{[s]} = x_{c,i}^{[s-1]} \oplus x_{d,i}^{[s]} \oplus \Theta_i\left(x_c^{[s-1]}, x_d^{[s]}\right)$, and then

$$
\begin{aligned}
& x_{c,i}^{[s-1]} \oplus x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus x_{c,i-1}^{[s]} \\
=& x_{c,i}^{[s-1]} \oplus x_{c,i}^{[s-1]} \oplus x_{d,i}^{[s]} \oplus \Theta_i\left(x_c^{[s-1]}, x_d^{[s]}\right) \oplus x_{d,i}^{[s]} \oplus x_{c,i-1}^{[s-1]} \oplus x_{d,i-1}^{[s]} \oplus \Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right) \\
=& x_{c,i-1}^{[s-1]} \oplus x_{d,i-1}^{[s]} \oplus \Theta_i\left(x_c^{[s-1]}, x_d^{[s]}\right) \oplus \Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right)
\end{aligned}
$$

Considering $\Theta_i\left(x_c^{[s-1]}, x_d^{[s]}\right) = x_{c,i-1}^{[s-1]} \cdot x_{d,i-1}^{[s]} \oplus \Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right)\left(x_{c,i-1}^{[s-1]} \oplus x_{d,i-1}^{[s]}\right)$, then we have

$$
\begin{aligned}
& \Pr\left(x_{c,i}^{[s-1]} \oplus x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus x_{c,i-1}^{[s]} = 0\right) \\
=& \Pr\left(x_{c,i-1}^{[s-1]} \oplus x_{d,i-1}^{[s]} \oplus x_{c,i-1}^{[s-1]} \cdot x_{d,i-1}^{[s]} = 0 | \Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right) = 0\right) \cdot \\
& \Pr\left(\Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right) = 0\right) + \\
& \Pr\left(x_{c,i-1}^{[s-1]} \cdot x_{d,i-1}^{[s]} \oplus 1 = 0 | \Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right) = 1\right) \cdot \Pr\left(\Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right) = 1\right) \\
=& \frac{1}{4} \Pr\left(\Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right) = 0\right) + \frac{1}{4} \Pr\left(\Theta_{i-1}\left(x_c^{[s-1]}, x_d^{[s]}\right) = 1\right) \\
=& \frac{1}{2}\left(1 - \frac{1}{2}\right)
\end{aligned}
$$

Therefore, the linear approximation $x_{c,i}^{[s-1]} = x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus x_{c,i-1}^{[s]}$ holds with probability $\frac{1}{2}\left(1 - \frac{1}{2}\right)$. □

It is important to note that **Lemma 3** and **Lemma 6** expand the same bits, i.e., $x_{a,i}^{[s-1]}$ and $x_{c,i}^{[s-1]}$, **Lemma 4** and **Lemma 5** expand the same sums, i.e., $x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]}$ and $x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]}$. Different choices naturally result in different linear approximations. Now, we provide a systematic three-case framework called *Mixderive* to find linear approximations for ChaCha. In this new framework, these four lemmas are utilized to derive linear approximations in a mixed mode, rather than utilized individually. This is the most significant difference between *Mixderive* and the approach proposed at ASIACRYPT 2022.

Without loss of generality, given some active input bits in subround $s-1$, then the multiple output bits in subround s can be derived by the following three cases.

Case 1: Expanding the bits $x_{b,i}^{[s-1]}, x_{d,i}^{[s-1]}, x_{a,0}^{[s-1]}$ ***and*** $x_{c,0}^{[s-1]}$ ***by Lemma 1 and Lemma 2 directly***

- If the bit $x_{b,i}^{[s-1]}$ or $x_{d,i}^{[s-1]}$ is active in subround $s-1$, then it should be directly expanded to multiple output bits in subround s by **Lemma 1**. Similarly, if the bit $x_{a,0}^{[s-1]}$ or $x_{c,0}^{[s-1]}$ is active in subround $s-1$, then it should be directly expanded to multiple output bits in subround s by **Lemma 2**.

Case 2: Expanding the bit $x_{a,i}^{[s-1]}$ ***or*** $x_{c,i}^{[s-1]}$ $(i > 0)$ ***by Lemma 3 and Lemma 6 respectively***

– If the bit $x_{a,i}^{[s-1]}$ or $x_{c,i}^{[s-1]}$ $(i > 0)$ is active in subround $s-1$, then two different expansions in subround s are obtained by **Lemma 3** and **Lemma 6**, respectively.

Case 3 : Expanding the sum $x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]}$ ***or*** $x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]}$ $(i > 0)$ ***by Lemma 4 and Lemma 5 respectively***

– If the sum $x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]}$ or $x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]}$ $(i > 0)$ is active in subround $s-1$, then two different expansions in subround s are obtained by **Lemma 4** and **Lemma 5**, respectively.

Using the three cases above, all possible options to expand $x_{a,i}^{[s-1]}$, $x_{c,i}^{[s-1]}$, $x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]}$ and $x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]}$ $(i > 0)$ can be exhausted. Thus, the derived results by *Mixderive* undoubtedly will cover the derived results by the approach proposed at ASIACRYPT 2022. In the following section, the improved linear approximations for ChaCha will confirm that our new framework is better than the known one.

4 Improved Linear Approximations for ChaCha

In this section, we will provide improved linear approximations for 3.5- and 4-round ChaCha obtained by the new framework *Mixderive* to confirm its effectiveness.

4.1 Improved Linear Approximation for 3.5-Round ChaCha

At EUROCRYPT 2021, Coutinho and Souza [14] presented a linear approximation for 3.5-round ChaCha with correlation 2^{-47}. Now, we will provide an improved linear approximation for 3.5-round ChaCha obtained by *Mixderive*. The new linear approximation will be given by **Lemma 8**. Before introducing it, a linear approximation for 2.5-round ChaCha is given by the following lemma, as it will be used in the proof of **Lemma 8**.

Lemma 7. *The following linear approximation for 2.5-round ChaCha holds with probability* $\frac{1}{2}\left(1 - \frac{1}{2^8}\right)$:

$$\begin{aligned} x_{5,0}^{(3.5)} =& x_0^{(6)}[0] \oplus x_2^{(6)}[0,6,7,23] \oplus x_3^{(6)}[0,8,16,19,24] \oplus x_4^{(6)}[7,15] \oplus x_5^{(6)}[13] \oplus \\ & x_7^{(6)}[7,14,19] \oplus x_8^{(6)}[7,12] \oplus x_9^{(6)}[0,7,8,18,19] \oplus x_{10}^{(6)}[0,6,25,26] \oplus \\ & x_{13}^{(6)}[0,31] \oplus x_{14}^{(6)}[0,6,7,15,18,19,24,27] \oplus x_{15}^{(6)}[0,8,26] \end{aligned}$$

Proof. By **Lemma 1** and **Lemma 2**, we have

$$x_{5,0}^{(3.5)} = x_{5,7}^{(4)} \oplus x_{10,0}^{(4)} = x_{5,19}^{(4.5)} \oplus x_{9,7}^{(4.5)} \oplus x_{10,0}^{(4.5)} \oplus x_{14,0}^{(4.5)}$$

with probability 1.

Next, we expand $x_{9,7}^{(4.5)}$ with **Lemma 6** and other three active bits with **Lemma 1** and **Lemma 2** to obtain

$$\begin{aligned}&x_{5,19}^{(4.5)} \oplus x_{9,7}^{(4.5)} \oplus x_{10,0}^{(4.5)} \oplus x_{14,0}^{(4.5)}\\ =&x_2^{(5)}[0] \oplus x_5^{(5)}[26] \oplus x_9^{(5)}[6,7,19] \oplus x_{10}^{(5)}[0] \oplus x_{13}^{(5)}[7] \oplus x_{14}^{(5)}[0,8]\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2}\right)$.

After then, we expand $x_9^{(5)}[6,7]$ with **Lemma 5** and $x_{9,19}^{(5)}$ with **Lemma 6** to get

$$\begin{aligned}&x_2^{(5)}[0] \oplus x_5^{(5)}[26] \oplus x_9^{(5)}[6,7,19] \oplus x_{10}^{(5)}[0] \oplus x_{13}^{(5)}[7] \oplus x_{14}^{(5)}[0,8]\\ =&x_2^{(5.5)}[0,7] \oplus x_3^{(5.5)}[0,8] \oplus x_5^{(5.5)}[6] \oplus x_7^{(5.5)}[12] \oplus x_8^{(5.5)}[0] \oplus x_9^{(5.5)}[7,18,19] \oplus\\ &x_{10}^{(5.5)}[0,26]\, x_{13}^{(5.5)}[23] \oplus x_{14}^{(5.5)}[7,16,19,24] \oplus x_{15}^{(5.5)}[0]\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^2}\right)$.

Then, we expand $x_9^{(5.5)}[18,19]$ with **Lemma 4**, $x_{2,7}^{(5.5)}, x_{3,8}^{(5.5)}, x_{10,26}^{(5.5)}$ with **Lemma 6** and $x_{9,7}^{(5.5)}$ with **Lemma 3** to obtain

$$\begin{aligned}&x_2^{(5.5)}[0,7] \oplus x_3^{(5.5)}[0,8] \oplus x_5^{(5.5)}[6] \oplus x_7^{(5.5)}[12] \oplus x_8^{(5.5)}[0] \oplus x_9^{(5.5)}[7,18,19] \oplus\\ &x_{10}^{(5.5)}[0,26] \oplus x_{13}^{(5.5)}[23] \oplus x_{14}^{(5.5)}[7,16,19,24] \oplus x_{15}^{(5.5)}[0]\\ =&x_0^{(6)}[0] \oplus x_2^{(6)}[0,6,7,23] \oplus x_3^{(6)}[0,8,16,19,24] \oplus x_4^{(6)}[7,15] \oplus x_5^{(6)}[13] \oplus x_7^{(6)}[7,14,19] \oplus\\ &x_8^{(6)}[7,12] \oplus x_9^{(6)}[0,7,8,18,19] \oplus x_{10}^{(6)}[0,6,25,26] \oplus x_{13}^{(6)}[0,31] \oplus\\ &x_{14}^{(6)}[0,6,7,15,18,19,24,27] \oplus x_{15}^{(6)}[0,8,26]\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^5}\right)$.

By the Piling-up Lemma, we can combine these linear relations to get **Lemma 7** with probability $\frac{1}{2}\left(1-\frac{1}{2^8}\right)$. □

Computational Result 1. *The linear approximation of **Lemma 7** holds computationally with* $\varepsilon_{\text{Lemma 7}} = -2^{-6.84}$. *This correlation was verified using* 2^{36} *random samples.*

Lemma 8. *The following linear approximation for 3.5-round ChaCha holds with probability* $\frac{1}{2}\left(1-\frac{1}{2^{41}}\right)$:

$$
\begin{aligned}
x_{5,0}^{(3.5)} =& x_0^{(7)}[0,6,7,12] \oplus x_1^{(7)}[8,15,16,19,31] \oplus \\
& x_2^{(7)}[0,2,3,5,6,8,11,14,15,16,18,19,22,24,25,26,27,31] \oplus \\
& x_3^{(7)}[10,15,19,25,26] \oplus x_4^{(7)}[2,7,19,26] \oplus x_5^{(7)}[0,5,6,7] \oplus \\
& x_6^{(7)}[1,2,9,10,19,22,30,31] \oplus x_7^{(7)}[3,11,19,22,23,26,27,31] \oplus \\
& x_8^{(7)}[11,15,19,27] \oplus x_9^{(7)}[7,8,13,18,19,25,30,31] \oplus \\
& x_{10}^{(7)}[2,3,7,12,15,24,25,27] \oplus x_{11}^{(7)}[0,4,7,8,12,14,19,20,28] \oplus \\
& x_{12}^{(7)}[0,11,12,20] \oplus x_{13}^{(7)}[0,12,13,16,19,23,24,27] \oplus \\
& x_{14}^{(7)}[1,2,6,8,10,11,13,14,16,19,23,24,25,26,30,31] \oplus \\
& x_{15}^{(7)}[8,13,14,16,18,23]
\end{aligned}
$$

Proof. We start from the linear approximation of **Lemma 7** and expand the linear approximation one more round. Since we are transitioning from round 6 to 7, we have $(a,b,c,d) \in \{(0,4,8,12),(1,5,9,13),(2,6,10,14),(3,7,11,15)\}$. Therefore, we can divide the right-hand side of **Lemma 7** into 4 distinct groups :

Group I: $x_0^{(6)}[0], x_4^{(6)}[7,15], x_8^{(6)}[7,12]$
Group II: $x_5^{(6)}[13], x_9^{(6)}[0,7,8,18,19], x_{13}^{(6)}[0,31]$
Group III: $x_2^{(6)}[0,6,7,23], x_{10}^{(6)}[0,6,25,26], x_{14}^{(6)}[0,6,7,15,18,19,24,27]$
Group IV: $x_3^{(6)}[0,8,16,19,24], x_7^{(6)}[7,14,19], x_{15}^{(6)}[0,8,26]$

For Group I, we first expand $x_{8,12}^{(6)}$ with **Lemma 6** and $x_{8,7}^{(6)}$ with **Lemma 3** to get

$$
\begin{aligned}
& x_0^{(6)}[0] \oplus x_4^{(6)}[7,15] \oplus x_8^{(6)}[7,12] \\
=& x_0^{(6.5)}[0] \oplus x_4^{(6.5)}[12,19,27] \oplus x_8^{(6.5)}[0,11,12,15] \oplus x_{12}^{(6.5)}[6,7,12]
\end{aligned}
$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^2}\right)$.

Next, we expand $x_8^{(6.5)}[11,12]$ with **Lemma 4** and $x_{8,15}^{[13]}$ with **Lemma 3** to obtain

$$
\begin{aligned}
& x_0^{(6.5)}[0] \oplus x_4^{(6.5)}[12,19,27] \oplus x_8^{(6.5)}[0,11,12,15] \oplus x_{12}^{(6.5)}[6,7,12] \\
=& x_0^{(7)}[0,6,7,12] \oplus x_4^{(7)}[2,7,19,26] \oplus x_8^{(7)}[11,15,19,27] \oplus x_{12}^{(7)}[0,11,12,20]
\end{aligned}
$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^2}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$
\begin{aligned}
& x_0^{(6)}[0] \oplus x_4^{(6)}[7,15] \oplus x_8^{(6)}[7,12] \\
=& x_0^{(7)}[0,6,7,12] \oplus x_4^{(7)}[2,7,19,26] \oplus x_8^{(7)}[11,15,19,27] \oplus x_{12}^{(7)}[0,11,12,20]
\end{aligned} \tag{3}
$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^4}\right)$.

For Group II, we first expand $x_9^{[12]}[7,8], x_9^{[12]}[18,19]$ with **Lemma 5** to get

$$\begin{aligned}&x_5^{(6)}[13]\oplus x_9^{(6)}[0,7,8,18,19]\oplus x_{13}^{(6)}[0,31]\\=&x_1^{(6.5)}[0,31]\oplus x_5^{(6.5)}[25]\oplus x_9^{(6.5)}[0,8,13,19]\oplus x_{13}^{(6.5)}[0,8,15,16,19]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^2}\right)$.

Next, we expand $x_{9,8}^{(6.5)}, x_{9,19}^{(6.5)}$ with **Lemma 6** and $x_{1,31}^{(6.5)}, x_{9,13}^{(6.5)}$ with **Lemma 3** to obtain

$$\begin{aligned}&x_1^{(6.5)}[0,31]\oplus x_5^{(6.5)}[25]\oplus x_9^{(6.5)}[0,8,13,19]\oplus x_{13}^{(6.5)}[0,8,15,16,19]\\=&x_1^{(7)}[8,15,16,19,31]\oplus x_5^{(7)}[0,5,6,7]\oplus x_9^{(7)}[7,8,13,18,19,25,30,31]\oplus\\&x_{13}^{(7)}[0,12,13,16,19,23,24,27]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned}&x_5^{(6)}[13]\oplus x_9^{(6)}[0,7,8,18,19]\oplus x_{13}^{(6)}[0,31]\\=&x_1^{(7)}[8,15,16,19,31]\oplus x_5^{(7)}[0,5,6,7]\oplus x_9^{(7)}[7,8,13,18,19,25,30,31]\oplus\\&x_{13}^{(7)}[0,12,13,16,19,23,24,27]\end{aligned}\tag{4}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^6}\right)$.

For Group III, we first expand $x_2^{(6)}[6,7], x_{10}^{(6)}[25,26]$ with **Lemma 4** and $x_{2,23}^{(6)}, x_{10,6}^{(6)}$ with **Lemma 3** to get

$$\begin{aligned}&x_2^{(6)}[0,6,7,23]\oplus x_{10}^{(6)}[0,6,25,26]\oplus x_{14}^{(6)}[0,6,7,15,18,19,24,27]\\=&x_2^{(6.5)}[15,18,19,23,24,27]\oplus x_6^{(6.5)}[2,3,12,18,19]\oplus x_{10}^{(6.5)}[7,22,23,25,26]\oplus\\&x_{14}^{(6.5)}[0,2,3,5,6,8,11,16,22,23,25,26,31]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

Next, we expand $x_2^{(6.5)}[18,19], x_2^{(6.5)}[23,24], x_{10}^{(6.5)}[25,26]$ with **Lemma 4**, $x_{10}^{(6.5)}[22,23]$ with **Lemma 5**, $x_{2,15}^{(6.5)}$ with **Lemma 6** and $x_{2,27}^{(6.5)}, x_{10,7}^{(6.5)}$ with **Lemma 3** to obtain

$$\begin{aligned}&x_2^{(6.5)}[15,18,19,23,24,27]\oplus x_6^{(6.5)}[2,3,12,18,19]\oplus x_{10}^{(6.5)}[7,22,23,25,26]\oplus\\&x_{14}^{(6.5)}[0,2,3,5,6,8,11,16,22,23,25,26,31]\\=&x_2^{(7)}[0,2,3,5,6,8,11,14,15,16,18,19,22,24,25,26,27,31]\oplus\\&x_6^{(7)}[1,2,9,10,19,22,30,31]\oplus x_{10}^{(7)}[2,3,7,12,15,24,25,27]\oplus\\&x_{14}^{(7)}[1,2,6,8,10,11,13,14,16,19,23,24,25,26,30,31]\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^7}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned} & x_2^{(6)}[0,6,7,23] \oplus x_{10}^{(6)}[0,6,25,26] \oplus x_{14}^{(6)}[0,6,7,15,18,19,24,27] \\ =& x_2^{(7)}[0,2,3,5,6,8,11,14,15,16,18,19,22,24,25,26,27,31] \oplus \\ & x_6^{(7)}[1,2,9,10,19,22,30,31] \oplus x_{10}^{(7)}[2,3,7,12,15,24,25,27] \oplus \\ & x_{14}^{(7)}[1,2,6,8,10,11,13,14,16,19,23,24,25,26,30,31] \end{aligned} \tag{5}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^{11}}\right)$.

For Group IV, we first expand $x_{3,16}^{(6)}, x_{3,19}^{(6)}, x_{3,24}^{(6)}$ with **Lemma 6** and $x_{3,8}^{(6)}$ with **Lemma 3** to get

$$\begin{aligned} & x_3^{(6)}[0,8,16,19,24] \oplus x_7^{(6)}[7,14,19] \oplus x_{15}^{(6)}[0,8,26] \\ =& x_3^{(6.5)}[15,16,18,19,23,24,26] \oplus x_7^{(6.5)}[4,12,20,26,28] \oplus \\ & x_{11}^{(6.5)}[0,8,14,16,24] \oplus x_{15}^{(6.5)}[10,16,24] \end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^4}\right)$.

Next, we expand $x_3^{(6.5)}[15,16]$ with **Lemma 4**, $x_3^{(6.5)}[18,19], x_3^{(6.5)}[23,24]$ with **Lemma 5**, $x_{3,26}^{(6.5)}, x_{11,8}^{(6.5)}, x_{11,16}^{(6.5)}$ with **Lemma 6** and $x_{11,14}^{(6.5)}, x_{11,24}^{(6.5)}$ with **Lemma 3** to obtain

$$\begin{aligned} & x_3^{(6.5)}[15,16,18,19,23,24,26] \oplus x_7^{(6.5)}[4,12,20,26,28] \oplus \\ & x_{11}^{(6.5)}[0,8,14,16,24] \oplus x_{15}^{(6.5)}[10,16,24] \\ =& x_3^{(7)}[10,15,19,25,26] \oplus x_7^{(7)}[3,11,19,22,23,26,27,31] \oplus \\ & x_{11}^{(7)}[0,4,7,8,12,14,19,20,28] \oplus x_{15}^{(7)}[8,13,14,16,18,23] \end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^8}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned} & x_3^{(6)}[0,8,16,19,24] \oplus x_7^{(6)}[7,14,19] \oplus x_{15}^{(6)}[0,8,26] \\ =& x_3^{(7)}[10,15,19,25,26] \oplus x_7^{(7)}[3,11,19,22,23,26,27,31] \oplus \\ & x_{11}^{(7)}[0,4,7,8,12,14,19,20,28] \oplus x_{15}^{(7)}[8,13,14,16,18,23] \end{aligned} \tag{6}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^{12}}\right)$.

Finally, using the Piling-up Lemma we obtain **Lemma 8** by combining the result from **Lemma 7** and Eqs. (3)-(6), which leads to a correlation of $-2^{-(8+4+6+11+12)} = -2^{-41}$. □

Computational Result 2. *The linear approximation of Eq. (3) and Eq. (5) holds computationally with* $\varepsilon_{L_0} = 2^{-14.20}$. *This correlation was verified using* 2^{36} *random samples.*

Computational Result 3. *The linear approximation of Eq. (4) holds computationally with* $\varepsilon_{L_1} = 2^{-5.17}$*. This correlation was verified using* 2^{36} *random samples.*

Computational Result 4. *The linear approximation of Eq. (6) holds computationally with* $\varepsilon_{L_2} = 2^{-10.77}$*. This correlation was verified using* 2^{36} *random samples.*

Using the Piling-up Lemma and **Computational Results 1-4**, the linear approximation of **Lemma 8** holds computationally with correlation $\varepsilon_{Lemma\ 8} = -2^{-(6.84+14.20+5.17+10.77)} = -2^{-36.98}$.

4.2 Improved Linear Approximation for 4-Round ChaCha

At EUROCRYPT 2021, Coutinho and Souza [14] presented a linear approximation for 4-round ChaCha with correlation 2^{-55}. Soon after, Coutinho et al. [13] gave an improved linear approximation for 4-round ChaCha with correlation 2^{-53} at ASIACRYPT 2022. Now, we will provide a new linear approximation for 4-round ChaCha obtained by *Mixderive*. It will be given by **Lemma 10**. Before introducing this lemma, a linear approximation for 3-round ChaCha is given by the following lemma, as it will be used in the proof of **Lemma 10**.

Lemma 9. *The following linear approximation for 3-round ChaCha holds with probability* $\frac{1}{2}\left(1 - \frac{1}{2^8}\right)$:

$$\begin{aligned} x_{3,0}^{(3)} \oplus x_{4,0}^{(3)} =& x_0^{(6)}[0,16] \oplus x_1^{(6)}[0,6,7,12,23] \oplus x_2^{(6)}[0,7,8,16,18,19,24] \oplus \\ & x_4^{(6)}[7,13,19] \oplus x_5^{(6)}[7] \oplus x_6^{(6)}[7,14,19] \oplus x_7^{(6)}[6,7,14,15,26] \oplus \\ & x_8^{(6)}[0,7,8,19,31] \oplus x_9^{(6)}[0,6,12,26] \oplus x_{10}^{(6)}[0] \oplus x_{11}^{(6)}[7] \oplus \\ & x_{12}^{(6)}[0,12,20,31] \oplus x_{13}^{(6)}[0,15,24,26,27] \oplus x_{14}^{(6)}[8,25,26] \oplus x_{15}^{(6)}[24] \end{aligned}$$

Proof. By **Lemma 1** and **Lemma 2**, we directly have

$$\begin{aligned} x_{3,0}^{(3)} \oplus x_{4,0}^{(3)} &= x_{3,0}^{(3.5)} \\ &= x_{3,0}^{(4)} \oplus x_{4,7}^{(4)} \oplus x_{9,0}^{(4)} \\ &= x_{3,0}^{(4.5)} \oplus x_{7,12}^{(4.5)} \oplus x_{11,0}^{(4.5)} \oplus x_{4,19}^{(4.5)} \oplus x_{8,7}^{(4.5)} \oplus x_{9,0}^{(4.5)} \oplus x_{13,0}^{(4.5)} \end{aligned}$$

with probability 1.

Next, we expand $x_{8,7}^{(4.5)}$ with **Lemma 6** and other six active bits with **Lemma 1** and **Lemma 2** to get

$$\begin{aligned} & x_{3,0}^{(4.5)} \oplus x_{4,19}^{(4.5)} \oplus x_{7,12}^{(4.5)} \oplus x_{8,7}^{(4.5)} \oplus x_{9,0}^{(4.5)} \oplus x_{11,0}^{(4.5)} \oplus x_{13,0}^{(4.5)} \\ =& x_1^{(5)}[0] \oplus x_3^{(5)}[0] \oplus x_4^{(5)}[26] \oplus x_7^{(5)}[7,19] \oplus x_8^{(5)}[6,7,19] \oplus \\ & x_9^{(5)}[0] \oplus x_{11}^{(5)}[12] \oplus x_{12}^{(5)}[7] \oplus x_{13}^{(5)}[0,8] \oplus x_{15}^{(5)}[0] \end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2}\right)$.

After then, we expand $x_8^{(5)}[6,7]$ with **Lemma 5**, $x_{11,12}^{(5)}$ with **Lemma 6** and $x_{8,19}^{(5)}$ with **Lemma 3** to obtain

$$\begin{aligned}
&x_1^{(5)}[0] \oplus x_3^{(5)}[0] \oplus x_4^{(5)}[26] \oplus x_7^{(5)}[7,19] \oplus x_8^{(5)}[6,7,19] \oplus \\
&x_9^{(5)}[0] \oplus x_{11}^{(5)}[12] \oplus x_{12}^{(5)}[7] \oplus x_{13}^{(5)}[0,8] \oplus x_{15}^{(5)}[0] \\
=&x_0^{(5.5)}[0] \oplus x_1^{(5.5)}[0,7] \oplus x_2^{(5.5)}[0,8] \oplus x_3^{(5.5)}[0] \oplus \\
&x_4^{(5.5)}[6,12] \oplus x_6^{(5.5)}[12] \oplus x_7^{(5.5)}[19,31] \oplus \\
&x_9^{(5.5)}[26] \oplus x_{11}^{(5.5)}[0,11,12] \oplus x_{12}^{(5.5)}[12,23] \oplus \\
&x_{13}^{(5.5)}[7,16,18,19,24] \oplus x_{14}^{(5.5)}[0] \oplus x_{15}^{(5.5)}[16]
\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^3}\right)$.

Finally, we expand $x_{11}^{(5.5)}[11,12]$ with **Lemma 5**, $x_{1,7}^{(5.5)}$ with **Lemma 6** and $x_{9,26}^{(5.5)}, x_{2,8}^{(5.5)}$ with **Lemma 3** to get

$$\begin{aligned}
&x_0^{(5.5)}[0] \oplus x_1^{(5.5)}[0,7] \oplus x_2^{(5.5)}[0,8] \oplus x_3^{(5.5)}[0] \oplus x_4^{(5.5)}[6,12] \oplus x_6^{(5.5)}[12] \oplus \\
&x_7^{(5.5)}[19,31] \oplus x_9^{(5.5)}[26] \oplus x_{11}^{(5.5)}[0,11,12] \oplus x_{12}^{(5.5)}[12,23] \oplus \\
&x_{13}^{(5.5)}[7,16,18,19,24] \oplus x_{14}^{(5.5)}[0] \oplus x_{15}^{(5.5)}[16] \\
=&x_0^{(6)}[0,16] \oplus x_1^{(6)}[0,6,7,12,23] \oplus x_2^{(6)}[0,7,8,16,18,19,24] \oplus x_4^{(6)}[7,13,19] \oplus \\
&x_5^{(6)}[7] \oplus x_6^{(6)}[7,14,19] \oplus x_7^{(6)}[6,7,14,15,26] \oplus x_8^{(6)}[0,7,8,19,31] \oplus \\
&x_9^{(6)}[0,6,12,26] \oplus x_{10}^{(6)}[0] \oplus x_{11}^{(6)}[7] \oplus x_{12}^{(6)}[0,12,20,31] \oplus \\
&x_{13}^{(6)}[0,15,24,26,27] \oplus x_{14}^{(6)}[8,25,26] \oplus x_{15}^{(6)}[24]
\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^4}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain **Lemma 9** with probability $\frac{1}{2}\left(1-\frac{1}{2^8}\right)$. □

Computational Result 5. *The linear approximation of* ***Lemma 9*** *holds computationally with* $\varepsilon_{\text{Lemma 9}} = -2^{-7.17}$. *This correlation was verified using* 2^{36} *random samples.*

Lemma 10. *The following linear approximation for 4-round ChaCha holds with probability* $\frac{1}{2}\left(1-\frac{1}{2^{50}}\right)$:

$$\begin{aligned}x_{3,0}^{(3)} \oplus x_{4,0}^{(3)} =& x_0^{(7)}[0,4,8,11,12,18,20,28,30] \oplus x_1^{(7)}[0,5,7,8,10,15,16,24,25,26,27,31] \oplus \\ & x_2^{(7)}[9,10,16,19,23,26] \oplus x_3^{(7)}[7,8,23,24] \oplus x_4^{(7)}[0,2,3,23,26,27] \oplus \\ & x_5^{(7)}[2,9,10,14,21,22] \oplus x_6^{(7)}[3,7,11,19,23,25,27,30,31] \oplus \\ & x_7^{(7)}[1,2,13,25,26,31] \oplus x_8^{(7)}[8,13,15,19,20,25,27,28,30,31] \oplus \\ & x_9^{(7)}[2,3,6,7,14,15,22,23,26,27] \oplus x_{10}^{(7)}[0,4,8,12,14,18,20,23,28] \oplus \\ & x_{11}^{(7)}[6,14,15,18,19,24,27] \oplus x_{12}^{(7)}[4,7,13,15,23,24,26,27,30,31] \oplus \\ & x_{13}^{(7)}[1,2,5,6,7,8,13,14,16,18,20,22,23,24,25,26] \oplus \\ & x_{14}^{(7)}[0,13,14,15,16,17,18,23,24] \oplus x_{15}^{(7)}[14,16,25,26]\end{aligned}$$

Proof. We start from the linear approximation of **Lemma 9** and expand the linear approximation one more round. Since we are transitioning from round 6 to 7, we have $(a,b,c,d) \in \{(0,4,8,12),(1,5,9,13),(2,6,10,14),(3,7,11,15)\}$. Therefore, we can divide the right-hand side of **Lemma 9** into 4 distinct groups :

Group I: $x_0^{(6)}[0,16], x_4^{(6)}[7,13,19], x_8^{(6)}[0,7,8,19,31], x_{12}^{(6)}[0,12,20,31]$
Group II: $x_1^{(6)}[0,6,7,12,23], x_5^{(6)}[7], x_9^{(6)}[0,6,12,26], x_{13}^{(6)}[0,15,24,26,27]$
Group III: $x_2^{(6)}[0,7,8,16,18,19,24], x_6^{(6)}[7,14,19], x_{10}^{(6)}[0], x_{14}^{(6)}[8,25,26]$
Group IV: $x_7^{(6)}[6,7,14,15,26], x_{11}^{(6)}[7], x_{15}^{(6)}[24]$

For Group I, we first expand $x_8^{(6)}[7,8]$ with **Lemma 5**, $x_{8,31}^{(6)}, x_{0,16}^{(6)}$ with **Lemma 6** and $x_{8,19}^{(6)}$ with **Lemma 3** to obtain

$$\begin{aligned}& x_0^{(6)}[0,16] \oplus x_4^{(6)}[7,13,19] \oplus x_8^{(6)}[0,7,8,19,31] \\ =& x_0^{(6.5)}[12,16,20,31] \oplus x_4^{(6.5)}[12,19,25,27,28,31] \oplus \\ & x_8^{(6.5)}[7,8,13,15,16,30,31] \oplus x_{12}^{(6.5)}[0,4,8,15,16,18,19,28,31]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

After then, we expand $x_8^{(6.5)}[15,16], x_8^{(6.5)}[30,31]$ with **Lemma 4**, $x_8^{(6.5)}[7,8]$ with **Lemma 5**, $x_{0,12}^{(6.5)}, x_{0,16}^{(6.5)}, x_{0,20}^{(6.5)}, x_{0,31}^{(6.5)}$ with **Lemma 6** and $x_{8,13}^{(6.5)}$ with **Lemma 3** to get

$$\begin{aligned}& x_0^{(6.5)}[12,16,20,31] \oplus x_4^{(6.5)}[12,19,25,27,28,31] \oplus \\ & x_8^{(6.5)}[7,8,13,15,16,30,31] \oplus x_{12}^{(6.5)}[0,4,8,15,16,18,19,28,31] \\ =& x_0^{(7)}[0,4,8,11,12,18,20,28,30] \oplus x_4^{(7)}[0,2,3,23,26,27] \oplus \\ & x_8^{(7)}[8,13,15,19,20,25,27,28,30,31] \oplus x_{12}^{(7)}[4,7,13,15,23,24,26,27,30,31]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^8}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned} & x_0^{(6)}[0,16] \oplus x_4^{(6)}[7,13,19] \oplus x_8^{(6)}[0,7,8,19,31] \oplus x_{12}^{(6)}[0,12,20,31] \\ =& x_0^{(7)}[0,4,8,11,12,18,20,28,30] \oplus x_4^{(7)}[0,2,3,23,26,27] \oplus \\ & x_8^{(7)}[8,13,15,19,20,25,27,28,30,31] \oplus \\ & x_{12}^{(7)}[4,7,13,15,23,24,26,27,30,31] \end{aligned} \tag{7}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^{12}}\right)$.

For Group II, we first expand $x_1^{(6)}[6,7]$ with **Lemma 5**, $x_{1,12}^{(6)}$ with **Lemma 6** and $x_{1,23}^{(6)}, x_{9,6}^{(6)}, x_{9,12}^{(6)}, x_{9,26}^{(6)}$ with **Lemma 3** to obtain

$$\begin{aligned} & x_1^{(6)}[0,6,7,12,23] \oplus x_5^{(6)}[7] \oplus x_9^{(6)}[0,6,12,26] \oplus x_{13}^{(6)}[0,15,24,26,27] \\ =& x_1^{(6.5)}[7,11,12,15,23,24,26,27] \oplus x_5^{(6.5)}[2,3,12,24] \oplus \\ & x_9^{(6.5)}[6,22,23,26] \oplus x_{13}^{(6.5)}[0,5,6,8,10,12,16,25,26,31] \end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^6}\right)$.

After then, we expand $x_9^{(6.5)}[22,23]$ with **Lemma 4**, $x_1^{(6.5)}[11,12], x_1^{(6.5)}[23,24], x_1^{(6.5)}[26,27]$ with **Lemma 5**, $x_{1,7}^{(6.5)}$ with **Lemma 6** and $x_{9,6}^{(6.5)}, x_{9,26}^{(6.5)}, x_{1,15}^{(6.5)}$ with **Lemma 3** to get

$$\begin{aligned} & x_1^{(6.5)}[7,11,12,15,23,24,26,27] \oplus x_5^{(6.5)}[2,3,12,24] \oplus \\ & x_9^{(6.5)}[6,22,23,26] \oplus x_{13}^{(6.5)}[0,5,6,8,10,12,16,25,26,31] \\ =& x_1^{(7)}[0,5,7,8,10,15,16,24,25,26,27,31] \oplus \\ & x_5^{(7)}[2,9,10,14,21,22] \oplus x_9^{(7)}[2,3,6,7,14,15,22,23,26,27] \oplus \\ & x_{13}^{(7)}[1,2,5,6,7,8,13,14,16,18,20,22,23,24,25,26] \end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^8}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned} & x_1^{(6)}[0,6,7,12,23] \oplus x_5^{(6)}[7] \oplus x_9^{(6)}[0,6,12,26] \oplus x_{13}^{(6)}[0,15,24,26,27] \\ =& x_1^{(7)}[0,5,7,8,10,15,16,24,25,26,27,31] \oplus \\ & x_5^{(7)}[2,9,10,14,21,22] \oplus x_9^{(7)}[2,3,6,7,14,15,22,23,26,27] \oplus \\ & x_{13}^{(7)}[1,2,5,6,7,8,13,14,16,18,20,22,23,24,25,26] \end{aligned} \tag{8}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^{14}}\right)$.

For Group III, we expand $x_2^{(6)}[7,8], x_2^{(6)}[18,19]$ with **Lemma 5** and $x_{2,16}^{(6)}, x_{2,24}^{(6)}$ with **Lemma 6** to get

$$\begin{aligned}&x_2^{(6)}[0,7,8,16,18,19,24] \oplus x_6^{(6)}[7,14,19] \oplus x_{10}^{(6)}[0] \oplus x_{14}^{(6)}[8,25,26]\\ =&x_2^{(6.5)}[0,15,16,19,23,24,25,26] \oplus x_6^{(6.5)}[4,12,19,20,26,28] \oplus\\ &x_{10}^{(6.5)}[7,8,14,16,24] \oplus x_{14}^{(6.5)}[0,9,10,24]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

After then, we expand $x_2^{(6.5)}[23,24]$ with **Lemma 4**, $x_{10}^{(6.5)}[7,8], x_2^{(6.5)}[15,16], x_2^{(6.5)}[25,26]$ with **Lemma 5** and $x_{2,19}^{(6.5)}, x_{10,14}^{(6.5)}, x_{10,16}^{(6.5)}, x_{10,24}^{(6.5)}$ with **Lemma 3** to obtain

$$\begin{aligned}&x_2^{(6.5)}[0,15,16,19,23,24,25,26] \oplus x_6^{(6.5)}[4,12,19,20,26,28] \oplus\\ &x_{10}^{(6.5)}[7,8,14,16,24] \oplus x_{14}^{(6.5)}[0,9,10,24]\\ =&x_2^{(7)}[9,10,16,19,23,26] \oplus x_6^{(7)}[3,7,11,19,23,25,27,30,31] \oplus\\ &x_{10}^{(7)}[0,4,8,12,14,18,20,23,28] \oplus x_{14}^{(7)}[0,13,14,15,16,17,18,23,24]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^8}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned}&x_2^{(6)}[0,7,8,16,18,19,24] \oplus x_6^{(6)}[7,14,19] \oplus x_{10}^{(6)}[0] \oplus x_{14}^{(6)}[8,25,26]\\ =&x_2^{(7)}[9,10,16,19,23,26] \oplus x_6^{(7)}[3,7,11,19,23,25,27,30,31] \oplus\\ &x_{10}^{(7)}[0,4,8,12,14,18,20,23,28] \oplus x_{14}^{(7)}[0,13,14,15,16,17,18,23,24]\end{aligned} \tag{9}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^{12}}\right)$.

For Group IV, we first expand $x_{11,7}^{(6)}$ with **Lemma 6** to get

$$\begin{aligned}&x_7^{(6)}[6,7,14,15,26] \oplus x_{11}^{(6)}[7] \oplus x_{15}^{(6)}[24]\\ =&x_3^{(6.5)}[24] \oplus x_7^{(6.5)}[6,18,19,26,27] \oplus x_{11}^{(6.5)}[14,15,26] \oplus x_{15}^{(6.5)}[7,8]\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2}\right)$.

After then, we expand $x_{11}^{(6.5)}[14,15]$ with **Lemma 4**, $x_{3,24}^{(6.5)}$ with **Lemma 6** and $x_{11,26}^{(6.5)}$ with **Lemma 3** to obtain

$$\begin{aligned}&x_3^{(6.5)}[24] \oplus x_7^{(6.5)}[6,18,19,26,27] \oplus x_{11}^{(6.5)}[14,15,26] \oplus x_{15}^{(6.5)}[7,8]\\ =&x_3^{(7)}[7,8,23,24] \oplus x_7^{(7)}[1,2,13,25,26,31] \oplus x_{11}^{(7)}[6,14,15,18,19,24,27] \oplus\\ &x_{15}^{(7)}[14,16,25,26]\end{aligned}$$

with probability $\frac{1}{2}\left(1-\frac{1}{2^3}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned} & x_7^{(6)}[6,7,14,15,26] \oplus x_{11}^{(6)}[7] \oplus x_{15}^{(6)}[24] \\ =& x_3^{(7)}[7,8,23,24] \oplus x_7^{(7)}[1,2,13,25,26,31] \oplus \\ & x_{11}^{(7)}[6,14,15,18,19,24,27] \oplus x_{15}^{(7)}[14,16,25,26] \end{aligned} \tag{10}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

Finally, using the Piling-up Lemma we obtain **Lemma 10** by combining the result from **Lemma 9** and Eqs. (7)-(10), which leads to a correlation of $-2^{-(8+12+14+12+4)} = -2^{-50}$. □

Computational Result 6. *The linear approximation of Eq. (7) and Eq. (10) holds computationally with* $\varepsilon_{L_3} = 2^{-15.77}$*. This correlation was verified using* 2^{38} *random samples.*

Computational Result 7. *The linear approximation of Eq. (8) holds computationally with* $\varepsilon_{L_4} = 2^{-12.47}$*. This correlation was verified using* 2^{36} *random samples.*

Computational Result 8. *The linear approximation of Eq. (9) holds computationally with* $\varepsilon_{L_5} = 2^{-10.59}$*. This correlation was verified using* 2^{36} *random samples.*

Using the Piling-up Lemma and **Computational Results 5-8**, the linear approximation of **Lemma 10** holds computationally with correlation $\varepsilon_{\text{Lemma 10}} = -2^{-(7.17+15.77+12.47+10.59)} = -2^{-46}$.

4.3 Comparisons with the Known Linear Approximations for ChaCha

We summarize the improved linear approximations for ChaCha in Table 3, together with the known linear approximations for ChaCha. The computational results of each linear approximation are also listed in Table 3. For 3.5-round ChaCha, we have obtained an improved linear approximation with correlation 2^{-41}, while the known linear approximation has a correlation of 2^{-47} presented at EUROCRYPT 2021 [14]. For 4-round ChaCha, we have obtained an improved linear approximation with correlation 2^{-50}, which is better than the known linear approximations presented at EUROCRYPT 2021 [14] and ASIACRYPT 2022 [13], respectively. These improvements confirm the effectiveness of our new framework *Mixderive*.

5 New Linear Approximations for 2- and 2.5-Round ChaCha

In this section, we will provide new linear approximations for 2- and 2.5-round ChaCha obtained by our new framework *Mixderive*. These two new linear ap-

Table 3. Linear approximations for 3.5- and 4-round ChaCha.

Rounds	Input	Theoretical correlation	Computational result	Ref.
3.5	$x_{5,0}^{(3.5)}$	2^{-47}	$2^{-42.3}$	[14]
		-2^{-41}	$-2^{-36.98}$	**This paper**
4	$x_{3,0}^{(3)} \oplus x_{4,0}^{(3)}$	2^{-55}	$2^{-50.42}$	[14]
		2^{-53}	$2^{-47.99}$	[13]
		-2^{-50}	-2^{-46}	**This paper**

proximations will be used to construct differential-linear distinguishers for 7- and 7.5-round ChaCha, respectively.

5.1 New Linear Approximation for 2-Round ChaCha

The new linear approximation for 2-round ChaCha that will be used to construct differential-linear distinguisher for 7-round ChaCha is given by the following lemma.

Lemma 11. *The following linear approximation for 2-round ChaCha holds with probability* $\frac{1}{2}\left(1+\frac{1}{2^{24}}\right)$:

$$\Gamma^{(5)} = \Gamma_0^{(7)}$$

where $\Gamma^{(5)} = x_2^{(5)}[0] \oplus x_6^{(5)}[7,19] \oplus x_{10}^{(5)}[12] \oplus x_{14}^{(5)}[0]$ *and*

$$\begin{aligned}\Gamma_0^{(7)} =& x_0^{(7)}[2,3,7,11,19,22,23] \oplus x_1^{(7)}[16] \oplus x_2^{(7)}[0,8,11,12,24] \oplus \\ & x_3^{(7)}[0,3,4,6,7,12,16,20,27,28,30,31] \oplus x_4^{(7)}[14,18,19,31] \oplus \\ & x_5^{(7)}[7] \oplus x_6^{(7)}[7,13,19,25,30,31] \oplus x_7^{(7)}[2,3,6,7,22,23,26,27] \oplus \\ & x_8^{(7)}[11,12,24,] \oplus x_{10}^{(7)}[18,23,24,26] \oplus x_{11}^{(7)}[20,27,28] \oplus \\ & x_{12}^{(7)}[6,7,10,11,19,20,30,31] \oplus x_{13}^{(7)}[0,8,24] \oplus \\ & x_{14}^{(7)}[0,5,6,11,12,16,19,20,25,26] \oplus x_{15}^{(7)}[0,3,4,6,7,11,12,14,16,18,19,30,31]\end{aligned}$$

Proof. We first expend $x_6^{(5)}[7,19], x_{14,0}^{(5)}$ with **Lemma 1**, $x_{2,0}^{(5)}$ with **Lemma 2** and $x_{10,12}^{(5)}$ with **Lemma 3** to obtain

$$\begin{aligned}& x_2^{(5)}[0] \oplus x_6^{(5)}[7,19] \oplus x_{10}^{(5)}[12] \oplus x_{14}^{(5)}[0] \\ =& x_2^{(5.5)}[0] \oplus x_3^{(5.5)}[0] \oplus x_6^{(5.5)}[19,31] \oplus x_7^{(5.5)}[12] \oplus x_8^{(5.5)}[0] \oplus \\ & x_{10}^{(5.5)}[12] \oplus x_{11}^{(5.5)}[7,19] \oplus x_{14}^{(5.5)}[16] \oplus x_{15}^{(5.5)}[11,12]\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2}\right)$.

After then, we expend $x_{10,12}^{(5.5)}, x_{11,7}^{(5.5)}, x_{11,19}^{(5.5)}$ with **Lemma 3** to get

$$\begin{aligned}
&x_2^{(5.5)}[0] \oplus x_3^{(5.5)}[0] \oplus x_6^{(5.5)}[19,31] \oplus x_7^{(5.5)}[12] \oplus x_8^{(5.5)}[0] \oplus \\
&x_{10}^{(5.5)}[12] \oplus x_{11}^{(5.5)}[7,19] \oplus x_{14}^{(5.5)}[16] \oplus x_{15}^{(5.5)}[11,12] \\
=&x_0^{(6)}[11,12] \oplus x_2^{(6)}[0] \oplus x_3^{(6)}[0,16] \oplus x_4^{(6)}[7] \oplus x_6^{(6)}[6,26] \oplus \\
&x_7^{(6)}[7,19] \oplus x_8^{(6)}[12] \oplus x_9^{(6)}[0] \oplus x_{10}^{(6)}[12] \oplus x_{11}^{(6)}[7,31] \oplus \\
&x_{12}^{(6)}[6,7,18,19] \oplus x_{13}^{(6)}[0] \oplus x_{14}^{(6)}[24] \oplus x_{15}^{(6)}[11,12,19,20]
\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^3}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned}
\Gamma^{(5)} =&x_0^{(6)}[11,12] \oplus x_2^{(6)}[0] \oplus x_3^{(6)}[0,16] \oplus x_4^{(6)}[7] \oplus x_6^{(6)}[6,26] \oplus \\
&x_7^{(6)}[7,19] \oplus x_8^{(6)}[12] \oplus x_9^{(6)}[0] \oplus x_{10}^{(6)}[12] \oplus x_{11}^{(6)}[7,31] \oplus \\
&x_{12}^{(6)}[6,7,18,19] \oplus x_{13}^{(6)}[0] \oplus x_{14}^{(6)}[24] \oplus x_{15}^{(6)}[11,12,19,20]
\end{aligned} \tag{11}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

Now, we start from the linear approximation of Eq. (11) and expand the linear approximation one more round. Since we are transitioning from round 6 to 7, we have $(a,b,c,d) \in \{(0,4,8,12),(1,5,9,13),(2,6,10,14),(3,7,11,15)\}$. Therefore, we can divide the right-hand side of Eq. (11) into 4 distinct groups :

Group I: $x_0^{(6)}[11,12], x_4^{(6)}[7], x_8^{(6)}[12], x_{12}^{(6)}[6,7,18,19]$
Group II: $x_9^{(6)}[0], x_{13}^{(6)}[0]$
Group III: $x_2^{(6)}[0], x_6^{(6)}[6,26], x_{10}^{(6)}[12], x_{14}^{(6)}[24]$
Group IV: $x_3^{(6)}[0,16], x_7^{(6)}[7,19], x_{11}^{(6)}[7,31], x_{15}^{(6)}[11,12,19,20]$

For Group I, we first expand $x_{8,12}^{(6)}$ with **Lemma 3** and $x_0^{(6)}[11,12]$ with **Lemma 5** to get

$$\begin{aligned}
&x_0^{(6)}[11,12] \oplus x_4^{(6)}[7] \oplus x_8^{(6)}[12] \oplus x_{12}^{(6)}[6,7,18,19] \\
=&x_0^{(6.5)}[6,7,12,18,19] \oplus x_4^{(6.5)}[19,24] \oplus x_8^{(6.5)}[7] \oplus x_{12}^{(6.5)}[2,3,11,12,22,23]
\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^2}\right)$.

Next, we expand $x_{0,12}^{(6.5)}, x_{8,7}^{(6.5)}$ with **Lemma 3** and $x_0^{(6.5)}[6,7], x_0^{(6.5)}[18,19]$ with **Lemma 5** to get

$$\begin{aligned}
&x_0^{(6.5)}[6,7,12,18,19] \oplus x_4^{(6.5)}[19,24] \oplus x_8^{(6.5)}[7] \oplus x_{12}^{(6.5)}[2,3,11,12,22,23] \\
=&x_0^{(7)}[2,3,7,11,19,22,23] \oplus x_4^{(7)}[14,18,19,31] \oplus x_8^{(7)}[11,12,24] \oplus \\
&x_{12}^{(7)}[6,7,10,11,19,20,30,31]
\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned} & x_0^{(6)}[11,12] \oplus x_4^{(6)}[7] \oplus x_8^{(6)}[12] \oplus x_{12}^{(6)}[6,7,18,19] \\ =& x_0^{(7)}[2,3,7,11,19,22,23] \oplus x_4^{(7)}[14,18,19,31] \oplus \\ & x_8^{(7)}[11,12,24] \oplus x_{12}^{(7)}[6,7,10,11,19,20,30,31] \end{aligned} \tag{12}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^6}\right)$.

For Group II, we first expand $x_{13,0}^{(6)}$ with **Lemma 1** and $x_{9,0}^{(6)}$ with **Lemma 2** to get

$$x_9^{(6)}[0] \oplus x_{13}^{(6)}[0] = x_1^{(6.5)}[0] \oplus x_9^{(6.5)}[0] \oplus x_{13}^{(6.5)}[0,16]$$

with probability 1.

Next, we expand $x_{13}^{(6.5)}[0,16]$ with **Lemma 1** and $x_{1,0}^{(6.5)}, x_{9,0}^{(6.5)}$ with **Lemma 2** to obtain

$$x_1^{(6.5)}[0] \oplus x_9^{(6.5)}[0] \oplus x_{13}^{(6.5)}[0,16] = x_1^{(7)}[16] \oplus x_5^{(7)}[7] \oplus x_{13}^{(7)}[0,8,24]$$

with probability 1.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$x_9^{(6)}[0] \oplus x_{13}^{(6)}[0] = x_1^{(7)}[16] \oplus x_5^{(7)}[7] \oplus x_{13}^{(7)}[0,8,24] \tag{13}$$

with probability 1.

For Group III, we first expand $x_{2,0}^{(6)}$ with **Lemma 2** and $x_{10,12}^{(6)}$ with **Lemma 3** to get

$$\begin{aligned} & x_2^{(6)}[0] \oplus x_6^{(6)}[6,26] \oplus x_{10}^{(6)}[12] \oplus x_{14}^{(6)}[24] \\ =& x_2^{(6.5)}[0,24] \oplus x_6^{(6.5)}[6,12,18] \oplus x_{10}^{(6.5)}[0,6,12,26] \oplus x_{14}^{(6.5)}[8,11,12] \end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2}\right)$.

Next, we expand $x_{2,0}^{(6.5)}, x_{10,0}^{(6.5)}$ with **Lemma 2** and $x_{2,24}^{(6.5)}, x_{10,6}^{(6.5)}, x_{10,12}^{(6.5)}, x_{10,26}^{(6.5)}$ with **Lemma 3** to obtain

$$\begin{aligned} & x_2^{(6.5)}[0,24] \oplus x_6^{(6.5)}[6,12,18] \oplus x_{10}^{(6.5)}[0,6,12,26] \oplus x_{14}^{(6.5)}[8,11,12] \\ =& x_2^{(7)}[0,8,11,12,24] \oplus x_6^{(7)}[7,13,19,25,30,31] \oplus x_{10}^{(7)}[18,23,24,26] \oplus \\ & x_{14}^{(7)}[0,5,6,11,12,16,19,20,25,26] \end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^4}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned} & x_2^{(6)}[0] \oplus x_6^{(6)}[6,26] \oplus x_{10}^{(6)}[12] \oplus x_{14}^{(6)}[24] \\ =& x_2^{(7)}[0,8,11,12,24] \oplus x_6^{(7)}[7,13,19,25,30,31] \oplus \\ & x_{10}^{(7)}[18,23,24,26] \oplus x_{14}^{(7)}[0,5,6,11,12,16,19,20,25,26] \end{aligned} \tag{14}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^5}\right)$.

For Group IV, we first expand $x_{3,0}^{(6)}$ with **Lemma 2** and $x_{3,16}^{(6)}, x_{11,7}^{(6)}, x_{11,31}^{(6)}$ with **Lemma 3** to get

$$\begin{aligned}
&x_3^{(6)}[0,16] \oplus x_7^{(6)}[7,19] \oplus x_{11}^{(6)}[7,31] \oplus x_{15}^{(6)}[11,12,19,20] \\
=&x_3^{(6.5)}[0,11,12,16,19,20] \oplus x_7^{(6.5)}[12,19,27,28,31] \oplus \\
&x_{11}^{(6.5)}[0,15,16,19,31] \oplus x_{15}^{(6.5)}[3,4,6,7,27,28,30,31]
\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^3}\right)$.

Next, we expand $x_{3,16}^{(6.5)}, x_{11,19}^{(6.5)}, x_{11,31}^{(6.5)}$ with **Lemma 3**, $x_{11}^{(6.5)}[15,16]$ with **Lemma 4** and $x_3^{(6.5)}[11,12], x_3^{(6.5)}[19,20]$ with **Lemma 5** to obtain

$$\begin{aligned}
&x_3^{(6.5)}[0,11,12,16,19,20] \oplus x_7^{(6.5)}[12,19,27,28,31] \oplus \\
&x_{11}^{(6.5)}[0,15,16,19,31] \oplus x_{15}^{(6.5)}[3,4,6,7,27,28,30,31] \\
=&x_3^{(7)}[0,3,4,6,7,12,16,20,27,28,30,31] \oplus x_7^{(7)}[2,3,6,7,22,23,26,27] \oplus \\
&x_{11}^{(7)}[20,27,28] \oplus x_{15}^{(7)}[0,3,4,6,7,11,12,14,16,18,19,30,31]
\end{aligned}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^6}\right)$.

By the Piling-up Lemma, we can combine these linear relations to obtain

$$\begin{aligned}
&x_3^{(6)}[0,16] \oplus x_7^{(6)}[7,19] \oplus x_{11}^{(6)}[7,31] \oplus x_{15}^{(6)}[11,12,19,20] \\
=&x_3^{(7)}[0,3,4,6,7,12,16,20,27,28,30,31] \oplus x_7^{(7)}[2,3,6,7,22,23,26,27] \oplus \\
&x_{11}^{(7)}[20,27,28] \oplus x_{15}^{(7)}[0,3,4,6,7,11,12,14,16,18,19,30,31]
\end{aligned} \tag{15}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^9}\right)$.

Finally, using the Piling-up Lemma we obtain **Lemma 11** by combining Eqs. (11)-(15), which leads to a correlation of $2^{-(4+6+0+5+9)} = 2^{-24}$. □

Computational Result 9. *The linear approximation of Eq. (11) holds computationally with $\varepsilon_{L_6} = 2^{-3.58}$. This correlation was verified using 2^{36} random samples.*

Computational Result 10. *The linear approximation of Eqs. (12) and (14) holds computationally with $\varepsilon_{L_7} = 2^{-9.44}$. This correlation was verified using 2^{36} random samples.*

Computational Result 11. *The linear approximation of Eq. (15) holds computationally with $\varepsilon_{L_8} = 2^{-7.95}$. This correlation was verified using 2^{36} random samples.*

Using the Piling-up Lemma, the linear approximation of **Lemma 11** holds computationally with correlation $\varepsilon_{Lemma\ 11} = 2^{-(3.58+9.44+7.95)} = 2^{-20.97}$.

5.2 New Linear Approximation for 2.5-Round ChaCha

The new linear approximation for 2.5-round ChaCha that will be used to construct differential-linear distinguisher for 7.5-round ChaCha is given by **Lemma 13**. To complete the proof of **Lemma 13**, a linear approximation for 2-round ChaCha presented in [5] is used. It is given by the following lemma.

Lemma 12 (Linear Trail 4 in [5]). *The following linear approximation for 2-round ChaCha holds with probability* $\frac{1}{2}\left(1+\frac{1}{2^{24}}\right)$:

$$\Gamma^{(5)} = \Gamma_1^{(7)}$$

where

$$\begin{aligned}\Gamma_1^{(7)} =& x_0^{(7)}[2,3,7,19,22,23] \oplus x_1^{(7)}[16] \oplus x_2^{(7)}[0,8,12,23,24] \oplus \\ & x_3^{(7)}[0,3,4,6,7,11,12,16,20,28,31] \oplus x_4^{(7)}[14,19,31] \oplus \\ & x_5^{(7)}[7] \oplus x_6^{(7)}[7,13,19,25,31] \oplus x_7^{(7)}[2,3,6,7,22,23,26,27] \oplus \\ & x_8^{(7)}[12,24] \oplus x_{10}^{(7)}[18,24,25,26] \oplus x_{11}^{(7)}[20,27,28] \oplus \\ & x_{12}^{(7)}[6,7,10,11,19,20,30,31] \oplus x_{13}^{(7)}[0,8,24] \oplus x_{14}^{(7)}[0,5,6,11,12,16,20,26] \oplus \\ & x_{15}^{(7)}[0,4,7,11,12,14,16,18,19,31]\end{aligned}$$

As shown in [5], the linear approximation of **Lemma 12** holds computationally with $\varepsilon_{Lemma\ 12} = 2^{-21.11}$. Based on **Lemma 12**, the new linear approximation for 2.5-round ChaCha is given by the following lemma.

Lemma 13. *The following linear approximation for 2.5-round ChaCha holds with probability* $\frac{1}{2}\left(1+\frac{1}{2^{46}}\right)$:

$$\Gamma^{(5)} = \Gamma^{(7.5)}$$

where

$$\begin{aligned}\Gamma^{(7.5)} =& x_0^{(7.5)}[0,3,4,11,12,14,16,18,23,31] \oplus x_1^{(7.5)}[6,7,10,11,16,19,20,30,31] \oplus \\ & x_2^{(7.5)}[12] \oplus x_3^{(7.5)}[4,5,6,7,26,28,31] \oplus x_4^{(7.5)}[0,7,8,10,12,16,19,23,24,26,27,28] \oplus \\ & x_5^{(7.5)}[3,15,18,30,31] \oplus x_6^{(7.5)}[5,11,19,25,27,28,31] \oplus \\ & x_7^{(7.5)}[2,3,4,6,7,12,14,15,18,20,23,24] \oplus x_8^{(7.5)}[0,2,3,6,8,11,22,23,26,27] \oplus \\ & x_9^{(7.5)}[0,4,7,11,12,14,15,16,20,27,28,30] \oplus x_{10}^{(7.5)}[3,6,19,23,24,26] \oplus \\ & x_{11}^{(7.5)}[7,13,15,16,19,20,25,27,28,31] \oplus x_{12}^{(7.5)}[3,4,14,15,19,20,22,23,26,28] \oplus \\ & x_{13}^{(7.5)}[8,11,12,16,23] \oplus x_{14}^{(7.5)}[0,4,10,16,21,22,27,28] \oplus \\ & x_{15}^{(7.5)}[0,2,3,15,16,17,18,20,24,26,27,28,30]\end{aligned}$$

Proof. We start from the linear approximation of **Lemma 12** and expand the linear approximation 0.5 more round. Since we are transitioning from round 7

to 7.5, we have $(a,b,c,d) \in \{(0,5,10,15),(1,6,11,12),(2,7,8,13),(3,4,9,14)\}$. Therefore, we can divide the linear mask $\Gamma_1^{(7)}$ into 4 distinct groups :

Group I: $x_0^{(7)}[2,3,7,19,22,23], x_5^{(7)}[7], x_{10}^{(7)}[18,24,25,26], x_{15}^{(7)}[0,4,7,11,12,14,16,18,19,31]$
Group II: $x_1^{(7)}[16], x_6^{(7)}[7,13,19,25,31], x_{11}^{(7)}[20,27,28], x_{12}^{(7)}[6,7,10,11,19,20,30,31]$
Group III: $x_2^{(7)}[0,8,12,23,24], x_7^{(7)}[2,3,6,7,22,23,26,27], x_8^{(7)}[12,24], x_{13}^{(7)}[0,8,24]$
Group IV: $x_3^{(7)}[0,3,4,6,7,11,12,16,20,28,31], x_4^{(7)}[14,19,31], x_{14}^{(7)}[0,5,6,11,12,16,20,26]$

For Group I, we expand $x_{0,7}^{(7)}, x_{0,19}^{(7)}, x_{10,18}^{(7)}, x_{10,26}^{(7)}$ with **Lemma 3**, $x_0^{(7)}[2,3], x_0^{(7)}[22,23]$ with **Lemma 5** and $x_{10}^{(7)}[24,25]$ with **Lemma 4** to get

$$\begin{aligned} & x_0^{(7)}[2,3,7,19,22,23] \oplus x_5^{(7)}[7] \oplus x_{10}^{(7)}[18,24,25,26] \oplus \\ & x_{15}^{(7)}[0,4,7,11,12,14,16,18,19,31] \\ =& x_0^{(7.5)}[0,3,4,11,12,14,16,18,23,31] \oplus x_5^{(7.5)}[3,15,18,30,31] \oplus \\ & x_{10}^{(7.5)}[3,6,19,23,24,26] \oplus \\ & x_{15}^{(7.5)}[0,2,3,15,16,17,18,20,24,26,27,28,30] \end{aligned} \tag{16}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^7}\right)$.

For Group II, we expand $x_{1,16}^{(7)}, x_{11,20}^{(7)}$ with **Lemma 3** and $x_{11}^{(7)}[27,28]$ with **Lemma 4** to obtain

$$\begin{aligned} & x_1^{(7)}[16] \oplus x_6^{(7)}[7,13,19,25,31] \oplus x_{11}^{(7)}[20,27,28] \oplus \\ & x_{12}^{(7)}[6,7,10,11,19,20,30,31] \\ =& x_1^{(7.5)}[6,7,10,11,16,19,20,30,31] \oplus x_6^{(7.5)}[5,11,19,25,27,28,31] \oplus \\ & x_{11}^{(7.5)}[7,13,15,16,19,20,25,27,28,31] \oplus \\ & x_{12}^{(7.5)}[3,4,14,15,19,20,22,23,26,28] \end{aligned} \tag{17}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^3}\right)$.

For Group III, we expand $x_{2,8}^{(7)}, x_{2,12}^{(7)}, x_{8,12}^{(7)}, x_{8,24}^{(7)}$ with **Lemma 3** and $x_2^{(7)}[23,24]$ with **Lemma 5** to get

$$\begin{aligned} & x_2^{(7)}[0,8,12,23,24] \oplus x_7^{(7)}[2,3,6,7,22,23,26,27] \oplus \\ & x_8^{(7)}[12,24] \oplus x_{13}^{(7)}[0,8,24] \\ =& x_2^{(7.5)}[12] \oplus x_7^{(7.5)}[2,3,4,6,7,12,14,15,18,20,23,24] \oplus \\ & x_8^{(7.5)}[0,2,3,6,8,11,22,23,26,27] \oplus x_{13}^{(7.5)}[8,11,12,16,23] \end{aligned} \tag{18}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^5}\right)$.

For Group IV, we expand $x_{3,16}^{(7)}, x_{3,20}^{(7)}, x_{3,28}^{(7)}, x_{3,31}^{(7)}$ with **Lemma 3** and $x_3^{(7)}[3,4]$, $x_3^{(7)}[6,7], x_3^{(7)}[11,12]$ with **Lemma 5** to obtain

$$\begin{aligned} & x_3^{(7)}[0,3,4,6,7,11,12,16,20,28,31] \oplus x_4^{(7)}[14,19,31] \oplus \\ & x_{14}^{(7)}[0,5,6,11,12,16,20,26] \\ =& x_3^{(7.5)}[4,5,6,7,26,28,31] \oplus \\ & x_4^{(7.5)}[0,7,8,10,12,16,19,23,24,26,27,28] \oplus \\ & x_9^{(7.5)}[0,4,7,11,12,14,15,16,20,27,28,30] \oplus \\ & x_{14}^{(7.5)}[0,4,10,16,21,22,27,28] \end{aligned} \tag{19}$$

with probability $\frac{1}{2}\left(1+\frac{1}{2^7}\right)$.

Finally, using the Piling-up Lemma we obtain **Lemma 13** by combining the result from **Lemma 12** and Eqs. (16)-(19), which leads to a correlation of $2^{-(24+7+3+5+7)} = 2^{-46}$. □

Computational Result 12. *The linear approximation of Eqs. (16)-(18) holds computationally with $\varepsilon_{L_9} = 2^{-14.25}$. This correlation was verified using 2^{36} random samples.*

Computational Result 13. *The linear approximation of Eq. (19) holds computationally with $\varepsilon_{L_{10}} = 2^{-6.81}$. This correlation was verified using 2^{36} random samples.*

Using the Piling-up Lemma, the linear approximation of **Lemma 13** holds computationally with correlation $\varepsilon_{Lemma\ 13} = 2^{-(21.11+14.25+6.81)} = 2^{-42.17}$.

6 Improved Differential-Linear Distinguishers for ChaCha256

In this section, we propose improved differential-linear distinguishers for 7- and 7.5-round ChaCha256, based on our new linear approximations for 2- and 2.5-round ChaCha proposed above.

6.1 Improved Differential-Linear Distinguisher for 7-Round ChaCha256

At FSE 2023, Bellini et al. [5] presented a 4-round differential-linear distinguisher $\Delta^{(1)} \to \Gamma^{(5)}$ with correlation $2^{-34.15}$, which is obtained by combining a 2-round differential-linear distinguisher $\Delta^{(1)} \to \Gamma_0^{(3)}$ with correlation $2^{-30.15}$ and a 2-round linear approximation $\Gamma_0^{(3)} \to \Gamma^{(5)}$ with correlation 2^{-2}, where

$$\begin{aligned} \Delta^{(1)} &= x_3^{(1)}[5,25] \oplus x_7^{(1)}[12,28] \oplus x_{11}^{(1)}[21,25] \oplus x_{15}^{(1)}[13,21] \\ \Gamma_0^{(3)} &= x_2^{(3)}[0,3,4] \oplus x_7^{(3)}[0,4,20] \oplus x_8^{(3)}[19,20] \oplus x_{13}^{(3)}[4] \\ \Gamma^{(5)} &= x_2^{(5)}[0] \oplus x_6^{(5)}[7,19] \oplus x_{10}^{(5)}[12] \oplus x_{14}^{(5)}[0] \end{aligned}$$

At FSE 2024, Xu et al. [30] found that the intermediate linear mask $\Gamma_0^{(3)}$ at round 3 can be replaced by other 15 intermediate linear masks $\Gamma_1^{(3)}, \cdots, \Gamma_{15}^{(3)}$. More details about these intermediate linear masks are given in Appendix. By considering differential-linear hull, an improved 4-round differential-linear distinguisher $\Delta^{(1)} \to \Gamma^{(5)}$ with correlation $2^{-32.2}$ was proposed in [30].

The differential-linear distinguisher for 7-round ChaCha256 is composed of three parts. The first part is a 1-round differential trail $\Delta_{in}^{(0)} \to \Delta^{(1)}$, where $\Delta_{in}^{(0)} = \left(\Delta_{15,9}^{(0)}, \Delta_{15,29}^{(0)}\right)$. As shown in [5], this differential trail holds with probability $p = 2^{-7}$. The second part is the 4-round differential-linear distinguisher $\Delta^{(1)} \to \Gamma^{(5)}$ proposed in [30] that holds with correlation $\varepsilon_d = 2^{-32.2}$. The last part is the 2-round linear approximation $\Gamma^{(5)} \to \Gamma_0^{(7)}$ given in Sect. 5, which holds with correlation $\varepsilon_{Lemma\ 11} = 2^{-20.97}$. Thus, the following differential-linear distinguisher for 7-round ChaCha256 holds with a computational complexity of $p^{-2} \cdot \varepsilon_d^{-2} \cdot \varepsilon_{Lemma\ 11}^{-4} \approx 2^{162.28}$.

$$\Delta_{in}^{(0)} \to \Delta^{(1)} \to \Gamma^{(5)} \to \Gamma_0^{(7)}$$

6.2 Improved Differential-Linear Distinguisher for 7.5-Round ChaCha256

The differential-linear distinguisher for 7.5-round ChaCha256 is also composed of three parts. The first and second parts are the same as in the distinguisher for 7-round ChaCha256 above. The last part is the 2.5-round linear approximation $\Gamma^{(5)} \to \Gamma^{(7.5)}$ given in Sect. 5, which holds with correlation $\varepsilon_{Lemma\ 13} = 2^{-42.17}$. Thus, the following differential-linear distinguisher for 7.5-round ChaCha256 holds with a computational complexity of $p^{-2} \cdot \varepsilon_d^{-2} \cdot \varepsilon_{Lemma\ 13}^{-4} \approx 2^{247.08}$.

$$\Delta_{in}^{(0)} \to \Delta^{(1)} \to \Gamma^{(5)} \to \Gamma^{(7.5)}$$

7 Conclusions

In this paper, a new framework of deriving linear approximations for ChaCha called *Mixderive* is proposed. By *Mixderive*, we derive some new linear approximations for ChaCha with higher correlations, and succeed in finding new 2- and 2.5-round linear approximations for ChaCha. Based on these new findings, new differential-linear distinguishers for 7- and 7.5-round ChaCha256 with complexities $2^{162.28}$ and $2^{247.08}$ are proposed, which improve the best known distinguishers by factors of $2^{8.29}$ and $2^{8.14}$, respectively. As far as we know, both cryptanalytic results are the best. The proposed framework *Mixderive* may be applied to other ARX-based ciphers, such as Salsa and Sparx. This is left for future research.

Acknowledgments. The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

Competing interests. The authors have no competing interests to declare that are relevant to the content of this paper.

Data availability statement. Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Funding. This work was supported by the National Natural Science Foundation of China under Grant number 62472439.

References

1. Aumasson, J.P., Fischer, S., Khazaei, S., Meier, W., Rechberger, C.: New features of latin dances: Analysis of salsa, ChaCha, and rumba. In: Fast Software Encryption Workshop. vol. 5086, pp. 470–488 (2008). https://doi.org/https://doi.org/10.1007/978-3-540-71039-4_30
2. Aumasson, J.P., Henzen, L., Meier, W., Phan, C.W.: Sha3 proposal blake (2008), https://api.semanticscholar.org/CorpusID:15020034
3. Beierle, C., Biryukov, A., dos Santos, L.C., Großschädl, J., Perrin, L., Udovenko, A., Velichkov, V., Wang, Q.: Lightweight aead and hashing using the sparkle permutation family. IACR Transactions on Symmetric Cryptology **2020**, 208–261 (Jun 2020). https://doi.org/https://doi.org/10.13154/tosc.v2020.iS1.208-261
4. Beierle, C., Leander, G., Todo, Y.: Improved differential-linear attacks with applications to arx ciphers. Journal of Cryptology **35** (2020). https://doi.org/https://doi.org/10.1007/s00145-022-09437-z
5. Bellini, E., Gerault, D., Grados, J., Makarim, R.H., Peyrin, T.: Boosting differential-linear cryptanalysis of chacha7 with milp. IACR Transactions on Symmetric Cryptology **2023, Issue 2**, 189–223 (2023). https://doi.org/10.46586/tosc.v2023.i2.189-223
6. Bernstein, D.J.: The Salsa20 Family of Stream Ciphers, pp. 84–97. Springer Berlin Heidelberg, Berlin, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68351-3_8
7. Bernstein, D.J.: Chacha, a variant of salsa20. Workshop Record of SASC **8**, 3–5 (2008)
8. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1990). https://doi.org/10.1007/3-540-38424-3_1, invited paper
9. Blondeau, C., Leander, G., Nyberg, K.: Differential-linear cryptanalysis revisited. In: Fast Software Encryption. pp. 411–430. Springer (2014). https://doi.org/10.1007/978-3-662-46706-0_21
10. Choudhuri, A.R., Maitra, S.: Significantly improved multi-bit differentials for reduced round salsa and ChaCha. IACR Transactions on Symmetric Cryptology pp. 261–287 (02 2017). https://doi.org/https://doi.org/10.46586/tosc.v2016.i2.261-287
11. Coutinho, M., Neto, T.C.S.: New multi-bit differentials to improve attacks against chacha. IACR Cryptol. ePrint Arch. **2020**, 350 (2020), https://eprint.iacr.org/2020/350

12. Coutinho, M., Passos, I., VÃąsquez, J.C.G.: Latin dances reloaded: Improved cryptanalysis against salsa and chacha, and the proposal of forró. Journal of Cryptology **36**, 1–57 (2023). https://doi.org/10.1007/s00145-023-09455-5
13. Coutinho, M., Passos, I., VÃąsquez, J.C.G., Sarkar, S., de MendonÃğa, F.L.L., de Sousa, R.T., Borges, F.: Latin dances reloaded: Improved cryptanalysis against salsa and chacha, and the proposal of forró. In: Advances in Cryptology – ASIACRYPT 2022. pp. 256–286. Springer International Publishing, Cham (2022). https://doi.org/https://doi.org/10.1007/978-3-031-22963-3_9
14. Coutinho, M., Souza, T.C.N.: Improved linear approximations to ARX ciphers and attacks against ChaCha. In: Advances in Cryptology – EUROCRYPT 2021. pp. 711–740. Springer International Publishing, Cham (2021). https://doi.org/https://doi.org/10.1007/978-3-030-77870-5_25
15. Dey, S.: Advancing the idea of probabilistic neutral bits: First key recovery attack on 7.5 round chacha. IEEE Transactions on Information Theory **70**(8), 6091–6106 (2024). https://doi.org/10.1109/TIT.2024.3389874
16. Dey, S., Dey, C., Sarkar, S., Meier, W.: Revisiting cryptanalysis on chacha from crypto 2020 and eurocrypt 2021. IEEE Transactions on Information Theory **68**(9), 6114–6133 (2022). https://doi.org/10.1109/TIT.2022.3171865
17. Dey, S., Garai, H.K., Maitra, S.: Cryptanalysis of reduced round ChaCha- new attack and deeper analysis. IACR Transactions on Symmetric Cryptology pp. 89–110 (03 2023). https://doi.org/10.46586/tosc.v2023.i1.89-110
18. Dey, S., Garai, H.K., Sarkar, S., Sharma, N.K.: Revamped differential-linear cryptanalysis on reduced round ChaCha. In: Advances in Cryptology – EUROCRYPT 2022. vol. 13277, pp. 86–114 (05 2022). https://doi.org/10.1007/978-3-031-07082-2_4
19. Dey, S., Garai, H.K., Sarkar, S., Sharma, N.K.: Enhanced differential-linear attacks on reduced round chacha. IEEE Transactions on Information Theory **69**(8), 5318–5336 (2023). https://doi.org/10.1109/TIT.2023.3269790
20. Dey, S., Sarkar, S.: Improved analysis for reduced round salsa and chacha. Discrete Applied Mathematics **227**, 58–69 (2017). https://doi.org/https://doi.org/10.1016/j.dam.2017.04.034
21. Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J., Biryukov, A.: Design strategies for arx with provable bounds: Sparx and lax. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016. pp. 484–513. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
22. Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis. In: Desmedt, Y.G. (ed.) Advances in Cryptology — CRYPTO '94. pp. 17–25. Springer Berlin Heidelberg, Berlin, Heidelberg (1994)
23. Langley, A., Chang, W.T., Mavrogiannopoulos, N., Strömbergson, J., Josefsson, S.: Chacha20-poly1305 cipher suites for transport layer security (tls). Requests For Comment **7905**, 1–8 (2016). https://doi.org/https://doi.org/10.17487/RFC7905
24. Maitra, S.: Chosen IV cryptanalysis on reduced round ChaCha and salsa. Discrete Applied Mathematics **208**, 88–97 (2016). https://doi.org/https://doi.org/10.1016/j.dam.2016.02.020
25. Matsui, M., Yamagishi, A.: A new method for known plaintext attack of feal cipher. In: Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, BalatonfÃijred, Hungary, May 24-28, 1992, Proceedings. Lecture Notes in Computer Science, vol. 658, pp. 81–91. Springer (1992). https://doi.org/10.1007/3-540-47555-9_7

26. Miyashita, S., Ito, R., Miyaji, A.: PNB-focused differential cryptanalysis of ChaCha stream cipher. In: Australasian Conference on Information Security and Privacy (2022). https://doi.org/10.1007/978-3-031-22301-3_3
27. Mouha, N., Mennink, B., Herrewege, A.V., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: An efficient mac algorithm for 32-bit microcontrollers. Lecture Notes in Computer Science **2014**, 306–323 (2014). https://doi.org/https://doi.org/10.1007/978-3-319-13051-4_19
28. Shi, Z., Zhang, B., Feng, D., Wu, W.: Improved key recovery attacks on reduced-round salsa20 and chacha. In: Proceedings of the 15th International Conference on Information Security and Cryptology. pp. 337–351. ICISC'12, Springer-Verlag, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-37682-5_24
29. Wang, S., Liu, M., Hou, S., Lin, D.: Moving a step of ChaCha in syncopated rhythm. In: Advances in Cryptology – CRYPTO 2023. pp. 273–304. Springer Nature Switzerland, Cham (2023). https://doi.org/https://doi.org/10.1007/978-3-031-38548-3_10
30. Xu, Z., Xu, H., Tan, L., Qi, W.: Differential-linear cryptanalysis of reduced round chacha. IACR Transactions on Symmetric Cryptology **2**, 166–189 (2024). https://doi.org/10.46586/tosc.v2024.i2.166-189