Refined Linear Approximations for ARX Ciphers and Their Application to ChaCha

Yurie Okada[1][0009−0003−1859−2067], Atsuki Nagai[2], and Atsuko Miyaji[1][0000−0001−8822−5287]

[1] Graduate School of Engineering, The University of Osaka, Japan
yurie.okada@cy2sec.comm.eng.osaka-u.ac.jp, miyaji@comm.eng.osaka-u.ac.jp
[2] KDDI CORPORATION, Japan
at-nagai@kddi.com

Abstract. ARX-based ciphers such as Salsa20 and ChaCha achieve high performance using only modular addition, rotation, and XOR. While ARX constructions are widely deployed in practice, linear and differential-linear cryptanalysis often reveal non-negligible biases in their reduced-round variants. Previous work has shown that a 7-round distinguisher on ChaCha is feasible, requiring about 2^{214} operations and relying on a linear approximation with a theoretical bias of 2^{-53}. However, such theoretical approximations significantly deviate from experimental observations. In this work, we resolve these discrepancies by introducing new fundamental linear approximations for two consecutive additions over three independent variables. We rigorously derive the exact probabilities of these approximations, demonstrating that the conventional independence assumption leads to systematic errors in bias estimation. Applying our theorem to ChaCha, we refine the probabilities of key approximations used in previous attacks. Our refined estimates closely match experimentally observed biases, reducing the gap between theory and practice. These results provide a more accurate foundation for future differential-linear cryptanalysis of ChaCha and other ARX-based designs.

Keywords: ARX · Piling-up Lemma · ChaCha · linear approximation

1 Introduction

ARX Ciphers. In today's advanced information society, symmetric-key cryptography plays a vital role in securing digital communications, transactions, and data exchanges, thereby protecting both stored and transmitted data. Among symmetric primitives, stream ciphers such as Salsa20 [3] and ChaCha [10] have been widely deployed in hardware and software products, making them especially important in practice.

Two common design paradigms for stream and block ciphers are Substitution-Permutation Networks (SPNs) and ARX (Addition, Rotation, XOR) structures. ARX ciphers rely solely on modular addition, bitwise rotation, and exclusive OR, achieving both simplicity and efficiency. Modular addition introduces non-linearity, while rotation enhances diffusion. ARX constructions are appealing

for their high performance and resistance to many standard cryptanalytic techniques; however, they may exhibit noticeable biases in differential and linear approximations, particularly in reduced-round instances.

In the cryptanalysis of ARX designs, linear approximations of additions are fundamental. For estimating linear biases, Wallén's method [15] for analyzing carry propagation in modular addition is essential. In particular, the following linear approximations [15, 6] are frequently used:

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

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

For more advanced analysis, partial linear approximations in lower rounds are combined into longer approximations across several rounds, where Matsui's Piling-up Lemma [12] is often applied. This approach constructs theoretical estimates of linear biases by combining local approximations and then validates them against experimental measurements. It is crucial that theoretical bias estimates closely reflect empirical values. For example, Nyberg et al. [13] refined the bias estimation of linear approximations in the ARX cipher SNOW 2.0, and more generally, similar refinements have been investigated for block ciphers [14].

Related Works on ChaCha. ChaCha [10], proposed by Bernstein in 2008 as a redesign of Salsa20, was later adopted by the Internet Engineering Task Force (IETF) for TLS 1.3, establishing itself as a cornerstone of secure communications. Compared to its predecessor, ChaCha provides better diffusion and stronger resistance to cryptanalysis. Numerous security analyses have since been carried out. Table 1 summarizes the number of rounds, time complexity, and data complexity of existing distinguishers and key-recovery attacks.

Theoretical bias estimates are used to derive complexities in [4, 5], whereas experimental bias measurements are employed in [6, 7, 17, 2]. In parallel, key-recovery attacks based on Probabilistic Neutral Bits (PNBs) [1] have been explored. These have been enhanced through techniques such as syncopation, optimized right-pair search strategies [16, 2, 4, 5, 8], and more recently bit puncturing [9], which reduces complexity by selectively omitting state bits.

The first application of differential-linear cryptanalysis to ChaCha was introduced by Maitra et al. [4], who analyzed its internal structure and proposed a distinguisher by transforming one-bit output differences into multi-bit XOR expressions. This line of research was extended by Coutinho et al. [5], who incorporated two-bit output differences to construct more effective linear approximations and demonstrated an improved 6-round attack using theoretical bias estimation. Later works [6, 7, 2, 17] extended the number of covered rounds by leveraging experimentally observed biases in partial approximations. Notably, [7] presented a 7-round distinguisher with complexity 2^{214}, which remains the best known against ChaCha. However, although discrepancies between theoretical and experimental bias values have been pointed out, no prior work has attempted to refine the theoretical estimates themselves.

To illustrate these discrepancies in more detail, consider the attack structure of [7]. It combines differential cryptanalysis over rounds 1–3 with linear crypt-

Table 1. Time and data complexity of attacks against reduced-round ChaCha

Rounds	Time	Data	Type	Linear Round	References
4	2^{6}	2^{6}	Distinguisher	-	[4]
4.5	2^{12}	2^{12}	Distinguisher	-	[4]
5	2^{16}	2^{16}	Distinguisher	(3,5)	[4]
6	2^{116}	2^{116}	Distinguisher	(3,6)	[4]
	2^{75}	2^{75}	Distinguisher	(3,6)	[5]
	2^{51}	2^{51}	Distinguisher	(3,6)	[6]
	$2^{127.5}$	$2^{37.5}$	Key Recovery	-	[4]
	$2^{102.2}$	2^{56}	Key Recovery	-	[5]
	$2^{61.4}$	2^{51}	Key Recovery	-	[9]
	$2^{57.4}$	$2^{55.7}$	Key Recovery	-	[9]
7	2^{224}	2^{224}	Distinguisher	(3,7)	[6]
	2^{214}	2^{214}	Distinguisher	(3,7)	[7]
	$2^{120.9}$	$2^{120.9}$	Distinguisher	(4,7)	[17]
	$2^{237.7}$	2^{96}	Key Recovery	-	[4]
	$2^{231.9}$	2^{50}	Key Recovery	-	[5]
	$2^{218.92}$	$2^{87.18}$	Key Recovery	-	[8]
	$2^{216.9}$	$2^{68.9}$	Key Recovery	-	[16]
	$2^{210.3}$	$2^{103.3}$	Key Recovery	-	[16]
	$2^{210.68}$	$2^{110.81}$	Key Recovery	-	[2]
	$2^{148.2}$	$2^{127.7}$	Key Recovery	-	[9]
	$2^{154.2}$	$2^{102.9}$	Key Recovery	-	[9]
7.25	$2^{244.85}$	$2^{93.24}$	Key Recovery	-	[8]
7.5	$2^{251.54}$	$2^{251.54}$	Distinguisher	(3.5,7.5)	[2]

analysis over rounds 3–7. To describe the resulting approximations, we use the following notation: the jth bit of the ith word in the mth round is denoted by $x_{i,j}^{(m)}$, the jth bit of the ith word in the $(\frac{s}{2})^{\text{th}}$ round by $x_{i,j}^{[s]}$, and the XOR of bits $j_1, j_2, \cdots, j_n$ of word i by $x_i[j_1, j_2, \cdots, j_n]$. The linear approximation for rounds 3–7 (Eq. (3)) consists of the approximation for rounds 3–6 (Eq. (4)) and that for rounds 6–7.

$$
\begin{aligned}
x_{3,0}^{[6]} \oplus x_{4,0}^{[6]} = {} & x_0^{[14]}[0,3,4,7,8,11,12,14,15,18,20,27,28] \\
& \oplus x_1^{[14]}[0,5,7,8,10,14,15,16,22,23,24,25,27,30,31] \oplus x_2^{[14]}[7,9,10,16,19,25,26] \\
& \oplus x_3^{[14]}[6,7,8,24] \oplus x_4^{[14]}[0,2,3,5,18,22,23,27] \oplus x_5^{[14]}[1,2,9,10,13,14,18,21,22,25,29] \\
& \oplus x_6^{[14]}[0,2,3,7,10,11,13,14,19,22,23,25,27,31] \oplus x_7^{[14]}[1,2,13,25,26,30,31] \\
& \oplus x_8^{[14]}[8,11,13,20,25,27,28,30,31] \oplus x_9^{[14]}[2,3,6,7,11,14,15,18,23,27] \\
& \oplus x_{10}^{[14]}[0,3,4,6,8,12,13,14,18,20,23,25,27,28] \\
& \oplus x_{11}^{[14]}[6,14,15,18,19,23,24,27] \oplus x_{12}^{[14]}[3,4,6,11,13,22,23,24,26,27,30,31] \\
& \oplus x_{13}^{[14]}[1,2,6,7,8,13,14,16,18,20,22,23,24,25,26]
\end{aligned}
$$

$$\oplus\, x_{14}^{[14]}[0,7,13,14,15,16,17,18,23,24] \oplus x_{15}^{[14]}[16,25,26]. \tag{3}$$

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

Then, the approximations over rounds 6–7 are further classified into Groups I–IV in the below.

Group I

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

Group II

$$\begin{aligned} & x_1^{[12]}[0,6,7,11,12,22,23] \oplus x_{5,7}^{[12]} \oplus x_9^{[12]}[0,6,12,26] \oplus x_{13}^{[12]}[0,14,15,24,26,27] \\ & = x_1^{[14]}[0,5,7,8,10,14,15,16,22,23,24,25,27,30,31] \\ & \quad \oplus x_5^{[14]}[1,2,9,10,13,14,18,21,22,25,29] \oplus x_9^{[14]}[2,3,6,7,11,14,15,18,23,27] \\ & \quad \oplus x_{13}^{[14]}[1,2,6,7,8,13,14,16,18,20,22,23,24,25,26] \end{aligned}$$

Group III

$$\begin{aligned} & x_2^{[12]}[0,6,7,8,16,18,19,24] \oplus x_6^{[12]}[7,13,14,19] \oplus x_{10,0}^{[12]} \oplus x_{14}^{[12]}[8,25,26] \\ & = x_2^{[14]}[7,9,10,16,19,25,26] \oplus x_6^{[14]}[0,2,3,7,10,11,13,14,19,22,23,25,27,31] \\ & \quad \oplus x_{10}^{[14]}[0,3,4,6,8,12,13,14,18,20,23,25,27,28] \\ & \quad \oplus x_{14}^{[14]}[0,7,13,14,15,16,17,18,23,24] \end{aligned}$$

Group IV

$$\begin{aligned} & x_7^{[12]}[6,7,14,15,26] \oplus x_{11}^{[12]}[6,7] \oplus x_{15,24}^{[12]} \\ & = x_3^{[14]}[6,7,8,24] \oplus x_7^{[14]}[1,2,13,25,26,30,31] \oplus x_{11}^{[14]}[6,14,15,18,19,23,24,27] \\ & \quad \oplus x_{15}^{[14]}[16,25,26] \end{aligned}$$

Significant discrepancies between theoretical and experimental biases have been observed for Eq. (4) and Groups I–III [7, 6]. Theoretical biases for Eq. (4) and Groups I, II, and III are estimated at 2^{-8}, 2^{-12}, 2^{-14}, and 2^{-15}, respectively. In contrast, the corresponding experimental values are $2^{-7.17}$, $2^{-11.70}$, $2^{-12.31}$, and $2^{-12.813}$ [6, 7]. These partial approximations were first introduced in [6], with Groups II and III later refined in [7]. Nevertheless, even after these refinements, a substantial gap between theoretical and experimental biases remains.

Our First Contribution: Fundamental Linear Approximation. To resolve the discrepancies discussed above, we introduce new fundamental linear approximations beyond Eqs. (1) and (2).

These approximations apply not only to ChaCha but also more broadly to ARX-based ciphers. In particular, we consider two consecutive additions of three variables x, y, z, namely $x+y$ and $(x+y)+z$, as illustrated in Fig. 1. From this setting we derive three new linear relations:

$$\Theta_i(x,y) \oplus \Theta_i(x+y,z) = x_{i-1} \oplus z_{i-1}, \tag{5}$$

$$\Theta_{i-1}(x,y) \oplus \Theta_i(x,y) \oplus \Theta_{i-1}(x+y,z) \oplus \Theta_i(x+y,z) = 0, \tag{6}$$

$$\Theta_i(x,y) \oplus \Theta_{i-1}(x,y) \oplus \Theta_i(x+y,z) = z_{i-1}. \tag{7}$$

The properties of these relations are summarized as follows:

1. Eq. (5): The XOR of the i-th carries of the two consecutive additions equals $x_{i-1} \oplus z_{i-1}$.
2. Eq. (6): The XOR of the four carries at positions $i-1$ and i in both additions equals zero.
3. Eq. (7): The XOR of the two carries at positions $i-1$ and i in the first addition and the i-th carry in the second addition equals z_{i-1}.

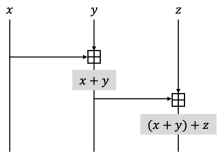

Fig. 1. Addition of three independent elements

In existing approaches, the probabilities that Eqs. (5)–(7) hold were computed as follows:

$$\Pr[\text{Eq. (5)}] = \Pr[\text{Eq. (6)}] = \Pr[\text{Eq. (7)}] = \tfrac{1}{2}\left(1 + \tfrac{1}{4}\right). \tag{8}$$

However, since these two consecutive additions are not independent, the use of the piling-up lemma causes discrepancies between the experimental and theoretical biases. This work rigorously derives the *exact* theoretical probabilities of Eqs. (5)-(7), summarized in the following theorem.

Theorem 1. *Let x, y, and z be independent variables. For the i-th carry in the binary additions $x+y$ and $(x+y)+z$, the following holds for all $i \geq 1$:*

$$\Pr[\text{Eq. (5)}] = \tfrac{2}{3} - \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1} \approx \tfrac{2}{3} = \tfrac{1}{2}\left(1 + \tfrac{1}{3}\right), \quad i \gg 1, \tag{9}$$

$$\Pr[\text{Eq. (6)}] = \tfrac{2}{3} - \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1} \approx \tfrac{2}{3} = \tfrac{1}{2}\left(1 + \tfrac{1}{3}\right), \quad i \gg 1, \tag{10}$$

$$\Pr[\text{Eq. (7)}] = \tfrac{7}{12} + \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1} \approx \tfrac{7}{12} = \tfrac{1}{2}\left(1 + \tfrac{1}{6}\right), \quad i \gg 1. \tag{11}$$

Our Second Contribution: Application to ChaCha. We now return to the discrepancies observed in the distinguisher attack against ChaCha in [7]. By applying Theorem 1 to Eq. (4) and Groups I–IV, we obtain refined probabilities for the corresponding linear approximations, as given in the following lemmas.

Lemma 1. *The probability that Eq. (4) holds for rounds 3–6 is*

$$\Pr[\text{Eq. (4)}] = \tfrac{1}{2}\left(1 + \tfrac{1}{2^{6}\cdot 3}\right).$$

Lemma 2. *The probabilities that* Group I − III *hold are*

$$\Pr[\text{Group I}] = \tfrac{1}{2}\left(1 + \tfrac{1}{2^{7}\cdot 3^{3}}\right), \quad \Pr[\text{Group II}] = \tfrac{1}{2}\left(1 + \tfrac{1}{2^{6}\cdot 3^{4}}\right), \quad \Pr[\text{Group III}] = \tfrac{1}{2}\left(1 + \tfrac{1}{2^{8}\cdot 3^{3}}\right).$$

Combining Lemmas 1 and 2 with Group IV from [6, 7], we refine the bias of Eq. (3), as presented in Theorem 2. Since no discrepancy was observed between the experimental and theoretical values for Group IV, no further refinement was necessary.

Theorem 2. *The probability that Eq. (3) holds for rounds 3–7 is*

$$\Pr[\text{Eq. (3)}] = \tfrac{1}{2}\left(1 + \tfrac{1}{2^{31}\cdot 3^{11}}\right) \approx \tfrac{1}{2}\left(1 + \tfrac{1}{2^{48.43}}\right).$$

Table 2 compares our refined theoretical biases with experimental results and with the existing estimates in [7]. The experiments were conducted by ourselves, and the error is calculated as (experimental value − theoretical value)/theoretical value. The results show that our refined probabilities match the experimental biases significantly more closely than the earlier theoretical estimates.

Table 2. Comparison of theoretical and experimental linear biases and errors between [7] and this work

Round		Experimental	[7]		This work	
			Theoretical	Error	Theoretical	Error
3–6	Eq. (4)	$2^{-7.17}$	2^{-8}	0.781	$2^{-6}\cdot 3^{-1} \approx 2^{-7.58}$	0.336
6–7	Group I	$2^{-11.70}$	2^{-12}	0.232	$2^{-7}\cdot 3^{-3} \approx 2^{-11.75}$	0.039
	Group II	$2^{-12.28}$	2^{-14}	2.304	$2^{-6}\cdot 3^{-4} \approx 2^{-12.34}$	0.045
	Group III	$2^{-12.84}$	2^{-15}	3.473	$2^{-8}\cdot 3^{-3} \approx 2^{-12.75}$	−0.057

The structure of this paper is as follows. Section 2 introduces linear approximations for ARX-based ciphers, the differential-linear cryptanalysis that forms the basis of this study, and the structure of ChaCha. Section 3 reviews existing linear approximations of ChaCha. Section 4 presents and proves a new theorem on carries in non-independent additions of three variables. Section 5 applies this theorem to the linear approximations of ChaCha derived in [7]. Finally, Section 6 concludes the paper.

2 Preliminary

This section provides background for this work. We first review the fundamental linear approximations and their integration in ARX ciphers, then discuss differential-linear cryptanalysis, and finally describe the structure of ChaCha. Table 3 summarizes the notations used in this paper.

Table 3. Notation

Notation	Description
$+$	32-bit modular addition
$\oplus$	bitwise XOR
$\lll i$	rotation by i bits to the left
$X^{(r)}$	state matrix after application of r round functions
$X^{[s]}$	state matrix after application of $\frac{s}{2}$ round functions
$x_{i,j}^{(r)}$	j^{th} bit of ith word in the rth round
$x_i^{(r)}[j_1, j_2, \cdots, j_n]$	bitwise XOR of $x_{i,j_1}^{(r)}$, $x_{i,j_1}^{(r)}$, $\cdots$ and $x_{i,j_n}^{(r)}$
$x_{i,j}^{[s]}$	j^{th} bit of ith word in the $\frac{s}{2}{}^{th}$ round
b *w.p.* a	b with probability a

2.1 A Review of Differential-Linear Cryptanalysis

Differential-linear cryptanalysis builds on linear approximations by describing an addition $x + y$ of two numbers as a combination of XOR and carry, $\Theta(x, y)$:

$$x + y = x \oplus y \oplus \Theta(x, y). \tag{12}$$

The i-th bit of $\Theta(x, y)$ is denoted by $\Theta_i(x, y)$, with $\Theta_0(x, y) = 0$. Fundamental linear approximations such as Eqs. (1) and (2) are frequently used in constructing linear relations. To extend these into multi-round linear approximations, the following lemma is commonly applied to combine several approximations.

Lemma 3 (Piling-up Lemma (Lemma 3 of [12])).
Let $X_i (1 \le i \le n)$ be independent random variables taking value 0 with probability p_i and 1 with probability $1 - p_i$. Then $\Pr[X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0]$ *is*

$$\tfrac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \left(p_i - \tfrac{1}{2}\right).$$

Differential-linear cryptanalysis, proposed by S. Langford and M.E. Hellman in 1994 [11], is a two-step technique that combines differential analysis with linear approximations:

STEP 1: Perform a differential analysis between input and output differences.
STEP 2: Identify linear approximations holding on the output difference from STEP 1 and apply linear analysis.

The differential-linear bias is defined as follows. Let σ and σ' denote linear combinations of two states $X(0)$ and $X'(0)$ after r rounds of transformation. Similarly, let ρ and ρ' denote linear combinations of two states after R rounds of transformation, where $r < R$:

$$\Delta\sigma = \sigma \oplus \sigma' = \bigoplus_u \Delta x^{(r)}_{p_u,q_u}, \quad \rho = \bigoplus_v x^{(R)}_{p_v,q_v}, \quad \rho' = \bigoplus_v x'^{(R)}_{p_v,q_v}.$$

Here, p_u and q_u indicate the word and bit positions of differing bits in σ and σ', while p_v and q_v indicate positions of terms involved in the linear approximation.

The differential bias ϵ_d and the linear bias ϵ_L are defined as

$$\Pr[\Delta\sigma = 0] = \tfrac{1}{2}(1+\epsilon_d), \qquad \Pr[\sigma = \rho] = \tfrac{1}{2}(1+\epsilon_L).$$

The differential-linear bias after R rounds, γ, can then be computed as

$$\begin{aligned}\Pr[\Delta\rho = 0] &= \Pr[\Delta\sigma = 0]\cdot\Pr[\Delta\sigma = \Delta\rho] + \Pr[\Delta\sigma = 1]\cdot\Pr[\Delta\sigma = \bar{\Delta}\rho] \\ &= \tfrac{1}{2}(1+\epsilon_d)\cdot\tfrac{1}{2}(1+\epsilon_L^2) + \tfrac{1}{2}(1-\epsilon_d)\cdot\tfrac{1}{2}(1-\epsilon_L^2) \\ &= \tfrac{1}{2}(1+\epsilon_d\cdot\epsilon_L^2),\end{aligned}$$

using the relation

$$\Pr[\Delta\sigma = \Delta\rho] = \Pr[\sigma=\rho]\cdot\Pr[\sigma'=\rho'] + \Pr[\sigma=\bar{\rho}]\cdot\Pr[\sigma'=\bar{\rho}'] = \tfrac{1}{2}(1+\epsilon_L^2).$$

Thus, the resulting differential-linear bias is given by $\gamma = \epsilon_d \cdot \epsilon_L^2$.

2.2 Structure of ChaCha

ChaCha utilizes three operations: 32-bit modular addition, bitwise exclusive OR (XOR), and shift rotation. A single word consists of 4 bytes, and an initial state matrix is constructed from 16 words derived from the secret key, block counter, nonce, and constants. Each round consists of four QuarterRound functions, which process four words at a time. The words in the 4×4 matrix are processed either column-wise or diagonally, with the pattern repeating every two rounds. The initial state matrix of ChaCha is give as follows:

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

which takes four predefined constants $c_0 = 0x61707865, c_1 = 0x3320646e, c_2 = 0x79622d32, c_3 = 0x6b206574$, 256-bit key $k_0 \sim k_7$, 96-bit nonce $v_0 \sim v_2$ and 32-bit counter t_0. The QuaterRound Function (QRF) has the following operations denoted by $QR_{ChaCha}(x_a^{(m)}, x_b^{(m)}, x_c^{(m)}, x_d^{(m)})$ (See Figure 2.):

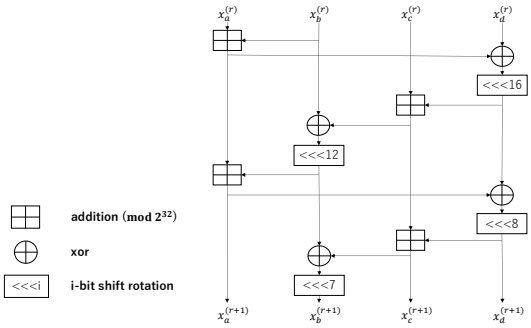

Fig. 2. One QR_{ChaCha}

$$\begin{cases} x_{a'}^{(m)} = x_a^{(m)} + x_b^{(m)}; x_{d'}^{(m)} = x_d^{(m)} \oplus x_{a'}^{(m)}; x_{d''}^{(m)} = x_{d'}^{(m)} \lll 16; \\ x_{c'}^{(m)} = x_c^{(m)} + x_{d''}^{(m)}; x_{b'}^{(m)} = x_b^{(m)} \oplus x_{c'}^{(m)}; x_{b''}^{(m)} = x_{b'}^{(m)} \lll 12; \\ x_a^{(m+1)} = x_{a'}^{(m)} + x_{b''}^{(m)}; x_{d'''}^{(m)} = x_{d''}^{(m)} \oplus x_a^{(m+1)}; x_d^{(m+1)} = x_{d'''}^{(m)} \lll 8; \\ x_c^{(m+1)} = x_{c'}^{(m)} + x_d^{(m+1)}; x_{b'''}^{(m)} = x_{b''}^{(m)} \oplus x_c^{(m+1)}; x_b^{(m+1)} = x_{b'''}^{(m)} \lll 7; \end{cases} \tag{13}$$

Using Eq. (12), the QRF Eq. (13) can be rewritten as follows:

$$\begin{aligned} x_{b,i}^{(m-1)} &= x_{b,i+19}^{(m)} \oplus x_c^{(m)}[i, i+12] \oplus x_{d,i}^{(m)} \oplus \Theta_i(x_{c'}^{(m-1)}, x_d^{(m)}), \\ x_{a,i}^{(m-1)} &= x_{a,i}^{(m)} \oplus x_b^{(m)}[i+7, i+19] \oplus x_{c,i+12}^{(m)} \oplus x_{d,i}^{(m)} \\ &\quad \oplus \Theta_i(x_{c'}^{(m-1)}, x_d^{(m)}) \oplus \Theta_i(x_a^{(m-1)}, x_b^{(m-1)}) \oplus \Theta_i(x_{a'}^{(m-1)}, x_{b''}^{(m-1)}), \\ x_{c,i}^{(m-1)} &= x_{a,i}^{(m)} \oplus x_{c,i}^{(m)} \oplus x_d^{(m)}[i, i+8] \oplus \Theta_i(x_{c'}^{(m-1)}, x_d^{(m)}) \oplus \Theta_i(x_c^{(m-1)}, x_{d''}^{(m-1)}), \\ x_{d,i}^{(m-1)} &= x_a^{(m)}[i, i+16] \oplus x_{b,i+7}^{(m)} \oplus x_{c,i}^{(m)} \oplus x_{d,i+24}^{(m)} \oplus \Theta_i(x_{a'}^{(m-1)}, x_{b''}^{(m-1)}). \end{aligned} \tag{14}$$

There are two types of rounds, column-round and diagonal-round correspond to the odd and even round, respectively. In the column-round, the following four QRF is applied: $QR_{ChaCha}(x_0^{(m)}, x_4^{(m)}, x_8^{(m)}, x_{12}^{(m)})$, $QR_{ChaCha}(x_1^{(m)}, x_5^{(m)}, x_9^{(m)}, x_{13}^{(m)})$, $QR_{ChaCha}(x_2^{(m)}, x_6^{(m)}, x_{10}^{(m)}, x_{14}^{(m)})$ and $QR_{ChaCha}(x_3^{(m)}, x_7^{(m)}, x_{11}^{(m)}, x_{15}^{(m)})$. In the diagonal-round, the following four QRF is applied: $QR_{ChaCha}(x_0^{(m)}, x_5^{(m)}, x_{10}^{(m)}, x_{15}^{(m)})$, $QR_{ChaCha}(x_1^{(m)}, x_6^{(m)}, x_{11}^{(m)}, x_{12}^{(m)})$, $QR_{ChaCha}(x_2^{(m)}, x_7^{(m)}, x_8^{(m)}, x_{13}^{(m)})$, and $QR_{ChaCha}(x_3^{(m)}, x_4^{(m)}, x_9^{(m)}, x_{14}^{(m)})$. The keystream block Z is generated by 32-bit addition of $X^{(0)}$ and $X^{(20)}$. $X^{(20)}$ is obtained by alternately repeating column-round and diagonal-round. Then, the ciphertext c is obtained by XOR operation of the keystream Z and the plaintext m: $Z = X^{(0)} + X^{(20)},\ c = Z \oplus m$.

We also use the SubRound Function (SRF) [7], defined as follows:

$$\begin{aligned}(x_a^{[s]}, x_b^{[s]}, x_c^{[s]}, x_d^{[s]}) = SR(x_a^{[s-1]}, x_b^{[s-1]}, x_c^{[s-1]}, x_d^{[s-1]}, r_1, r_2),\\ x_a^{[s]} = x_a^{[s-1]} + x_b^{[s-1]}, x_d^{[s]} = (x_d^{[s-1]} \oplus x_a^{[s]}) \lll r_1,\\ x_c^{[s]} = x_c^{[s-1]} + x_d^{[s]}, x_b^{[s]} = (x_b^{[s-1]} \oplus x_c^{[s]}) \lll r_2.\end{aligned} \tag{15}$$

The SRF Eq. (15) is transformed as follows:

$$\begin{aligned}x_{b,i}^{[s-1]} = x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]},\ x_{c,i}^{[s-1]} = x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus \Theta_i(x_c^{[s-1]}, x_d^{[s]}),\\ x_{d,i}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{d,i+r_1}^{[s]},\ x_{a,i}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus \Theta_i(x_a^{[s-1]}, x_b^{[s-1]}).\end{aligned} \tag{16}$$

Two SRFs correspond to One QRF, $X(s) = X[2s]$.

3 Related Works on Linear Approximation for ChaCha

This section reviews the linear approximations related to the proof of the 3–7 round linear approximation improved in Section 5, as well as linear approximations derived from the structure of SRF and the $m-1$-round single-bit and m-round multi-bit linear approximations in [7], [4], and [6]. Using Eqs. (1), (2), and (14),the following Lemma 4 is derived.

Lemma 4. (*Lemma 9 of [4] combined with Lemma 6 of [6]*) *For one active input bit in round $m-1$ and multiple active output bits in round $m \geq 1$, the following holds for $i > 0$.*

$$x_{b,i}^{(m-1)} = x_{b,i+19}^{(m)} \oplus x_{c,i}^{(m)} \oplus x_{c,i+12}^{(m)} \oplus x_{d,i}^{(m)} \oplus x_{d,i-1}^{(m)},\ w.p. \tfrac{1}{2}\left(1+\tfrac{1}{2}\right), \tag{17}$$

$$\begin{aligned}x_{a,i}^{(m-1)} = {} & x_{a,i}^{(m)} \oplus x_{b,i+7}^{(m)} \oplus x_{b,i+19}^{(m)} \oplus x_{c,i+12}^{(m)} \oplus x_{d,i}^{(m)}\\ & \oplus x_{b,i+6}^{(m)} \oplus x_{b,i+18}^{(m)} \oplus x_{c,i+11}^{(m)} \oplus x_{d,i-1}^{(m)},\ w.p. \tfrac{1}{2}\left(1+\tfrac{1}{2^3}\right),\end{aligned} \tag{18}$$

$$\begin{aligned}x_{c,i}^{(m-1)} = {} & x_{a,i}^{(m)} \oplus x_{c,i}^{(m)} \oplus x_{d,i}^{(m)} \oplus x_{d,i+8}^{(m)} \oplus x_{a,i-1}^{(m)}\\ & \oplus x_{d,i+7}^{(m)} \oplus x_{d,i-1}^{(m)},\ w.p. \tfrac{1}{2}\left(1+\tfrac{1}{2^2}\right),\end{aligned} \tag{19}$$

$$\begin{aligned}x_{d,i}^{(m-1)} = {} & x_{a,i}^{(m)} \oplus x_{a,i+16}^{(m)} \oplus x_{b,i+7}^{(m)} \oplus x_{c,i}^{(m)}\\ & \oplus x_{d,i+24}^{(m)} \oplus x_{c,i-1}^{(m)} \oplus x_{b,i+6}^{(m)},\ w.p. \tfrac{1}{2}\left(1+\tfrac{1}{2}\right).\end{aligned} \tag{20}$$

The following Lemma 5 is a reformulation of Lemmas 5-7 from [7], based on Eqs. (1) and (2).

Lemma 5. (*Lemma 5-7 of [7]*) *For one or two active input bits in subround $s-1$ and multiple output bits in subround s, the following linear approximations hold with probability $\frac{1}{2}(1+\frac{1}{2})$ with rotation distances r_1 and r_2, when $i > 0$.*

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

$$
\begin{aligned}
&x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]} = x_{c,i}^{[s]} \oplus x_{d,i}^{[s]} \oplus x_{c,i-1}^{[s]} \oplus x_{d,i-1}^{[s]},\\
&x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]} \oplus x_{a,i-1}^{[s]} \oplus x_{b,i+r_2-1}^{[s]} \oplus x_{c,i-1}^{[s]}, \quad (21)\\
&x_{c,i}^{[s-1]} \oplus x_{c,i-1}^{[s-1]} = x_{c,i}^{[s]} \oplus x_{d,i}^{[s]},\\
&x_{a,i}^{[s-1]} \oplus x_{a,i-1}^{[s-1]} = x_{a,i}^{[s]} \oplus x_{b,i+r_2}^{[s]} \oplus x_{c,i}^{[s]}.
\end{aligned}
$$

Some linear approximations in Lemma 9 of [6] are represented in the following Lemma 6, which combines each two or more $(m-1)$-round to m-round linear approximations into each one linear equation.

Lemma 6. (*Lemma 9 of [6]*) *For multiple active input bits in round $m-1$ and multiple output bits in round m, the following linear approximations hold with probability $\frac{1}{2}(1+\frac{1}{2^k})$.*

$$
\begin{aligned}
&x_a^{(m-1)}[i-1,i] \oplus x_{b,i}^{(m-1)}\\
&= x_a^{(m)}[i-1,i] \oplus x_b^{(m)}[i+6,i+7,i+18] \oplus x_c^{(m)}[i,i+11] \oplus x_d^{(m)}[i-2,i-1] \ (k=3),\\
&x_a^{(m-1)}[i-1,i] \oplus x_{c,i}^{(m-1)}\\
&= x_b^{(m)}[i+6,i+7,i+18,i+19] \oplus x_c^{(m)}[i,i+11,i+12] \oplus x_d^{(m)}[i-2,i-1,i+7,i+8] \ (k=4),\\
&x_a^{(m-1)}[i-1,i] \oplus x_{b,i}^{(m-1)} \oplus x_{c,i}^{(m-1)}\\
&= x_a^{(m)}[i-2,i] \oplus x_b^{(m)}[i+6,i+7,i+18] \oplus x_c^{(m)}[i-1,i,i+11] \oplus x_d^{(m)}[i+6,i+7] \ (k=3),\\
&x_a^{(m-1)}[i-1,i]\\
&= x_a^{(m)}[i-1,i] \oplus x_b^{(m)}[i+6,i+7,i+18,i+19] \oplus x_c^{(m)}[i+11,i+12] \oplus x_d^{(m)}[i-1,i] \ (k=3).
\end{aligned}
$$

The computational complexity of 2^{214} in [7] is derived from the bias of the linear approximation for rounds 3–6 and four partial linear approximations for rounds 6–7, categorized into Groups I–IV. The linear approximation for rounds 3–6 is described in Lemma 7 (originally Lemma 10 in [6]). The four partial linear approximations corresponding to Groups I–IV are given in Lemmas 8. The combined linear approximation for rounds 3–7 is then described in Lemma 9 (originally Lemma 8 in [7]).

Lemma 7. (*Lemma 10 of [6]*)
The probabilities for the linear approximation for 3-6 rounds is as follows:

$$\Pr[\text{Eq. (4)}] = \tfrac{1}{2}\left(1+\tfrac{1}{2^8}\right). \quad (22)$$

Lemma 8. *(Lemma 8 of [7] and Lemma 11 of [6])*
The probabilities for the linear approximations in Groups $\mathrm{I}-\mathrm{IV}$ *are as follows:*

$$
\begin{aligned}
\Pr[\text{Group I}] &= \tfrac{1}{2}\left(1+\tfrac{1}{2^{12}}\right), \ \Pr[\text{Group II}] = \tfrac{1}{2}\left(1+\tfrac{1}{2^{14}}\right),\\
\Pr[\text{Group III}] &= \tfrac{1}{2}\left(1+\tfrac{1}{2^{15}}\right), \ \Pr[\text{Group IV}] = \tfrac{1}{2}\left(1+\tfrac{1}{2^{4}}\right).
\end{aligned}
$$

Lemma 9. (*Lemma 8 of [7]*)
The probability for the linear approximations for 3–7 rounds is as follows:

$$\Pr[\text{Eq. (3)}] = \tfrac{1}{2}\left(1+\tfrac{1}{2^{53}}\right) \quad (23)$$

4 Newly Derived Foundamental Linear Approximations for ARX Ciphers

Analysis of stream ciphers often begins with approximations of a single addition of two elements such as Eqs (1) and (2) in Section 1. Not only approximations of a single addition but also those of two consecutive additions $x+y$ and $(x+y)+z$ of three elements x, y, and z, (as shown in Fig. 1), such as Eqs. (5)–(7), which hold for all $i \geq 1$, are frequently used in stream ciphers. For example, in [6, 7], both Eq. (4) and Groups I-III rely on Eqs. (5)–(7). Eq. (4) and Group III use Eq. (5); Group I uses Eqs.(5) and (7); and Group II uses Eqs.(5) and (6). Interestingly, the probabilities of these three equations are equal to Eq. (8) when they are evaluated by applying Lemma 3 under the assumption that the two additions are independent. In this section, we refine the linear approximations in Theorem 1 without relying on Lemma 3.

4.1 Proof of Theorem 1

This subsection provides a proof of Theorem 1. We now rigorously derive the exact theoretical probabilities of Eqs. (5)–(7) in Theorem 1. S

Eqs. (9), (10), and (11) all rely on $\Pr[\Theta_i(x,y) \oplus \Theta_i(x+y,z) = 0]$. Define $F_i(x,y,z) := \Theta_i(x,y) \oplus \Theta_i(x+y,z)$; we prove by induction that

$$q_i = \Pr[F_i(x,y,z) = 0] \ = \frac{2}{3} \cdot \left(\frac{1}{4}\right)^i + \frac{1}{3} \quad (i \geq 0). \tag{24}$$

Note that $1 - q_i = \Pr[F_i(x,y,z) = 1]$. Table 4 shows the combinations of $(\Theta_i(x,y), \Theta_i(x+y,z))$ and (x_i, y_i, z_i) for which $\Theta_{i+1}(x,y) \oplus \Theta_{i+1}(x+y,z) = 0$ holds. For example, when $(\Theta_i(x,y), \Theta_i(x+y,z)) = (0,1)$, the cases $(x_i, y_i, z_i) = (0,0,0)$ and $(1,1,1)$ satisfy $\Theta_{i+1}(x,y) \oplus \Theta_{i+1}(x+y,z) = 0$.

Table 4. Combinations of $(\Theta_i(x,y), \Theta_i(x+y,z))$ and (x_i, y_i, z_i) that satisfy $\Theta_{i+1}(x,y) \oplus \Theta_{i+1}(x+y,z) = 0$

$(\Theta_i(x,y), \Theta_i(x+y,z))$	(x_i, y_i, z_i)
(0,0)	(0,0,0), (0,0,1), (0,1,0), (1,0,0)
(0,1)	(0,0,0), (1,1,1)
(1,0)	(0,0,0), (1,1,1)
(1,1)	(0,1,1), (1,0,1), (1,1,0), (1,1,1)

We first prove the case $i = 0$. Since no carry occurs from $i = 0$, we always have $(\Theta_0(x,y), \Theta_0(x+y,z)) = (0,0)$. Therefore, we obtain $q_0 = 1 = \frac{2}{3} + \frac{1}{3}$; thus Eq. (24) holds for $i = 0$.

Next, assume Eq. (24) holds for some $i \geq 0$. We prove the case $i+1$ by considering separately $F_i(x,y,z) = 0$ and $F_i(x,y,z) = 1$. When $F_i(x,y,z) = 0$, i.e. $(\Theta_i(x,y), \Theta_i(x+y,z)) \in \{(0,0),(1,1)\}$, Table 4 shows there are 8 cases

with $F_{i+1}(x,y,z) = 0$. When $F_i(x,y,z) = 1$, i.e. $(\Theta_i(x,y), \Theta_i(x+y,z)) \in \{(0,1),(1,0)\}$, Table 4 shows there are 4 cases with $F_{i+1}(x,y,z) = 0$. Hence,

$$\begin{aligned} q_{i+1} &= q_i \cdot \Pr[F_{i+1}(x,y,z) = 0 \mid F_i(x,y,z) = 0] \\ &\quad +(1-q_i) \cdot \Pr[F_{i+1}(x,y,z) = 0 \mid F_i(x,y,z) = 1] \\ &= q_i \cdot \tfrac{8}{16} + (1-q_i) \cdot \tfrac{4}{16} = \tfrac{1}{4} + \tfrac{1}{4} q_i = \tfrac{2}{3} \cdot \left(\tfrac{1}{4}\right)^{i+1} + \tfrac{1}{3}. \end{aligned}$$

Thus, Eq. (24) also holds for $i+1$, and by induction, it holds for all $i \geq 0$.

Using q_i, we prove Eqs. (9), (10), and (11). Table 5 shows the combinations of $(\Theta_{i-1}(x,y), \Theta_{i-1}(x+y,z), x_{i-1}, y_{i-1}, z_{i-1})$ that satisfy Eqs. (5), (6), and (7). For the i-th bit, we derive the probability that each equation holds by consider-

Table 5. Combinations of $(\Theta_{i-1}(x,y), \Theta_{i-1}(x+y,z))$ and $(x_{i-1}, y_{i-1}, z_{i-1})$ with Eqs. (5), (6), and (7)

	$(\Theta_{i-1}(x,y), \Theta_{i-1}(x+y,z))$	$(x_{i-1}, y_{i-1}.z_{i-1})$
Eq. (5)	(0,0)	(0,0,0), (0,1,0), (0,1,1), (1,1,0)
	(0,1)	(0,0,0), (0,0,1), (0,1,1), (1,0,0), (1,1,0), (1,1,1)
	(1,0)	(0,0,0), (0,0,1), (0,1,1), (1,0,0), (1,1,0), (1,1,1)
	(1,1)	(0,0,1), (1,0,0), (1,0,1), (1,1,1)
Eq. (6)	(0,0)	(0,0,0), (0,0,1), (0,1,0), (1,0,0)
	(0,1)	(0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0)
	(1,0)	(0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0)
	(1,1)	(0,1,1), (1,0,1), (1,1,0), (1,1,1)
Eq. (7)	(0,0)	(0,0,0), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,1)
	(0,1)	(0,0,0), (0,0,1), (1,0,1), (0,1,1)
	(1,0)	(0,0,0), (0,0,1), (0,1,1), (1,0,1)
	(1,1)	(0,0,0), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,1)

ing separately the cases $F_{i-1}(x,y,z) = 0$ and $F_{i-1}(x,y,z) = 1$.

Eq. (9). We determine the probability that Eq. (5) holds for $i \geq 1$. When $F_{i-1}(x,y,z) = 0$, i.e. $(\Theta_{i-1}(x,y), \Theta_{i-1}(x+y,z)) \in \{(0,0),(1,1)\}$, Table 5 shows that there are 8 cases that satisfy Eq. (5). When $F_{i-1}(x,y,z) = 1$, i.e. $(\Theta_{i-1}(x,y), \Theta_{i-1}(x+y,z)) \in \{(0,1),(1,0)\}$, Table 5 shows that there are 12 cases that satisfy Eq. (5). From the above results and the previously derived q_i, the probability that Eq. (5) holds can be obtained as follows.

$$\begin{aligned} \Pr[\text{Eq. (5)}] &= q_{i-1} \cdot \Pr[\text{Eq. (5)} \mid F_{i-1}(x,y,z) = 0] \\ &\quad +(1-q_{i-1}) \cdot \Pr[\text{Eq. (5)} \mid F_{i-1}(x,y,z) = 1] \\ &= q_{i-1} \cdot \tfrac{8}{16} + (1-q_{i-1}) \cdot \tfrac{12}{16} = \tfrac{3}{4} - \tfrac{1}{4} q_{i-1} = \tfrac{2}{3} - \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1} \end{aligned}$$

Eq. (10). We determine the probability that Eq. (6) holds for $i \geq 1$. When $F_{i-1}(x,y,z) = 0$, Table 5 shows that there are 8 cases that satisfy Eq. (6). When $F_{i-1}(x,y,z) = 1$, Table 5 shows that there are 12 cases that satisfy Eq. (6). From

the above results and q_i, the probability that Eq. (6) holds can be obtained as follows.

$$\begin{aligned}\Pr[\text{Eq. (6)}] &= q_{i-1} \cdot \Pr[\text{Eq. (6)} \mid F_{i-1}(x,y,z) = 0] \\ &\quad +(1-q_{i-1}) \cdot \Pr[\text{Eq. (6)} \mid F_{i-1}(x,y,z) = 1] \\ &= q_{i-1} \cdot \tfrac{8}{16} + (1-q_{i-1}) \cdot \tfrac{12}{16} = \tfrac{3}{4} - \tfrac{1}{4} q_{i-1} = \tfrac{2}{3} - \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1}\end{aligned}$$

Eq. (11). We determine the probability that Eq. (7) holds for $i \geq 1$. When $F_{i-1}(x,y,z) = 0$, Table 5 shows that there are 12 cases that satisfy Eq. (7). When $F_{i-1}(x,y,z) = 1$, Table 5 shows that there are 8 cases that satisfy Eq. (7). From the above results and q_i, the probability that Eq. (7) holds can be obtained as follows.

$$\begin{aligned}\Pr[\text{Eq. (7)}] &= q_{i-1} \cdot \Pr[\text{Eq. (7)} \mid F_{i-1}(x,y,z) = 0] \\ &\quad +(1-q_{i-1}) \cdot \Pr[\text{Eq. (7)} \mid F_{i-1}(x,y,z) = 1] \\ &= q_{i-1} \cdot \tfrac{12}{16} + (1-q_{i-1}) \cdot \tfrac{8}{16} = \tfrac{1}{2} + \tfrac{1}{4} q_{i-1} = \tfrac{7}{12} + \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1} \square\end{aligned}$$

The following corollary is obtained in the same manner as Theorem 1, by generalizing the right-hand sides of Eqs. (5) and (7).

Corollary 1 *Let x, y, and z be independent variables. For the i-th carry in the binary additions $x+y$ and $(x+y)+z$, the following relations hold for all $i \geq 1$:*

$$\Pr[\Theta_i(x,y) \oplus \Theta_i(x+y,z) = \alpha \oplus \beta] = \tfrac{2}{3} - \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1}, \tag{25}$$

$$\Pr[\Theta_i(x,y) \oplus \Theta_{i-1}(x,y) \oplus \Theta_i(x+y,z) = \gamma] = \tfrac{7}{12} + \tfrac{1}{6} \cdot \left(\tfrac{1}{4}\right)^{i-1}. \tag{26}$$

where $(\alpha,\beta) \in \{(x_{i-1},y_{i-1}),(x_{i-1},z_{i-1}),(y_{i-1},z_{i-1})\}$ and $\gamma \in \{x_{i-1},y_{i-1},z_{i-1}\}$.

4.2 Experiment

To experimentally verify Theorem 1, we evaluated the probabilities that Eqs. (5)–(7) hold by performing 10,000 trials of additions of 10–bit values x, y, z. Table 6 shows the theoretical probabilities, the experimental probabilities, and the experimental errors, all rounded to four decimal places.

Similarly, Corollary 1 was verified experimentally in the same manner. In this case, Eqs. (25) and (26) were tested separately, each corresponding to the right-hand side expressions (one of which coincides with Theorem 1). Table 7 compares the theoretical and experimental probabilities of Corollary 1, again showing values rounded to four decimal places.

In all cases, the experimental errors were negligible, confirming the correctness of both Theorem 1 and Corollary 1.

5 Application of Theorem 1 to the ChaCha Permutation

In this section, we refine the theoretical biases of the 3–7 round linear approximations used in [7] by applying Theorem 1, with the goal of reducing the discrepancies between theoretical and experimental values shown in Table 2.

Table 6. Probabilities of Eqs. (5)–(7) in Theorem 1: theory, experiment, and error

Eq.		i								
		1	2	3	4	5	6	7	8	9
(5)	Theoretical	0.5	0.625	0.6563	0.6641	0.6660	0.6665	0.6666	0.6667	0.6667
	Experimental	0.4997	0.6196	0.6583	0.668	0.663	0.6629	0.6728	0.6697	0.6754
	Error	-0.0006	-0.0086	0.0031	0.0059	-0.0045	-0.0054	0.0093	0.0046	0.0131
(6)	Theoretical	0.5	0.625	0.6563	0.6641	0.6660	0.6665	0.6666	0.6667	0.6667
	Experimental	0.4926	0.6164	0.6599	0.6594	0.6712	0.6651	0.6623	0.6597	0.6577
	Error	-0.0148	-0.0138	0.0056	-0.0070	0.0078	-0.0021	-0.0065	-0.0104	-0.0134
(7)	Theoretical	0.75	0.625	0.5938	0.5859	0.5840	0.5835	0.5834	0.5833	0.5833
	Experimental	0.7478	0.6403	0.5915	0.5823	0.5911	0.5828	0.5777	0.5923	0.5820
	Error	-0.0029	0.0245	-0.0038	-0.0062	0.0122	-0.0012	-0.0097	0.0154	-0.0023

Table 7. Probabilities of Eqs. (25) and (26) in Corollary 1: theory, experiment, and error

Eq.	RHS		i								
			1	2	3	4	5	6	7	8	9
(25)	$(\alpha \oplus \beta)$	Theoretical	0.5	0.625	0.6563	0.6641	0.6660	0.6665	0.6666	0.6667	0.6667
	$x_{i-1} \oplus y_{i-1}$	Experimental	0.5081	0.6132	0.6572	0.6671	0.6677	0.6652	0.6721	0.6673	0.6709
		Error	0.0162	-0.0189	0.0014	0.0046	0.0025	-0.0020	0.0082	0.0010	0.0064
	$y_{i-1} \oplus z_{i-1}$	Experimental	0.5014	0.6270	0.6564	0.6665	0.6743	0.6669	0.6594	0.6685	0.6630
		Error	0.0028	0.0032	0.0002	0.0037	0.0124	0.0006	-0.0108	0.0028	-0.0055
(26)	γ	Theoretical	0.75	0.625	0.5938	0.5859	0.5840	0.5835	0.5834	0.5833	0.5833
	x_{i-1}	Experimental	0.7485	0.6326	0.5940	0.5878	0.5797	0.5840	0.5766	0.5739	0.5944
		Error	-0.0020	0.0122	0.0004	0.0032	-0.0073	0.0009	-0.0116	-0.0162	0.0190
	y_{i-1}	Experimental	0.7536	0.6238	0.5818	0.5918	0.5894	0.5764	0.5762	0.5868	0.5840
		Error	0.0048	-0.0019	-0.0201	0.0100	0.0093	-0.0122	-0.0123	0.0059	0.0011

First, the 3–7 round linear approximation is divided into the 3–6 round linear approximation Eq. (4) and the 6–7 round linear approximations Groups I-IV. It is known that Group IV does not exhibit any discrepancy. Next, Eq. (4) is further separated into the 3–5 round and 5–6 round approximations. By comparing their theoretical and experimental values, we found that Eq. (27), corresponding to the 5–6 round approximation, causes discrepancies. Similarly, by decomposing Groups I–III into finer sub-approximations, we identified the following equations as sources of discrepancies: Eqs. (28)–(30) in Group I, Eqs. (31)–(34) in Group II, and Eqs. (35)-(37) in Group III. For these equations, Theorem 1 is applied to derive more precise theoretical biases.

$$x_{11,12}^{[10]} = x_{1}^{[12]}[11,12] \oplus x_{11,12}^{[12]} \oplus x_{12}^{[12]}[11,12,19,20], \tag{27}$$

$$x_{0,16}^{[12]} = x_{0,16}^{[14]} \oplus x_{4}^{[14]}[2,3,22,23] \oplus x_{8}^{[14]}[27,28] \oplus x_{12}^{[14]}[15,16], \tag{28}$$

$$x_{4,7}^{[12]} \oplus x_{8}^{[12]}[7,8] = x_{0}^{[14]}[7,8] \oplus x_{4,26}^{[14]} \oplus x_{8}^{[14]}[8,19] \oplus x_{12}^{[14]}[7,8,15,16], \tag{29}$$

$$x_{8,31}^{[12]} = x_{0}^{[14]}[30,31] \oplus x_{8,31}^{[14]} \oplus x_{12}^{[14]}[6,7,30,31], \tag{30}$$

$$x_1^{[12]}[11,12] \oplus x_{9,12}^{[12]} = x_{1,11}^{[14]} \oplus x_5^{[14]}[18,19,31] \oplus x_9^{[14]}[11,12,24] \oplus x_{13}^{[14]}[19,20], \tag{31}$$

$$x_1^{[12]}[22,23] = x_1^{[14]}[22,23] \oplus x_5^{[14]}[9,10,29,30] \oplus x_9^{[14]}[2,3] \oplus x_{13}^{[14]}[22,23], \tag{32}$$

$$x_1^{[12]}[6,7] \oplus x_{5,7}^{[12]} \oplus x_{9,6}^{[12]} = x_1^{[14]}[5,7] \oplus x_5^{[14]}[13,14,25] \oplus x_9^{[14]}[6,7,18] \oplus x_{13}^{[14]}[13,14], \tag{33}$$

$$x_{9,26}^{[12]} = x_1^{[14]}[25,26] \oplus x_{9,26}^{[14]} \oplus x_{13}^{[14]}[1,2,25,26], \tag{34}$$

$$x_{2,16}^{[12]} = x_{2,16}^{[14]} \oplus x_6^{[14]}[2,3,22,23] \oplus x_{10}^{[14]}[27,28] \oplus x_{14}^{[14]}[15,16], \tag{35}$$

$$x_2^{[12]}[6,7] \oplus x_{6,7}^{[12]} = x_{2,7}^{[14]} \oplus x_6^{[14]}[13,14] \oplus x_{10}^{[14]}[6,7], \tag{36}$$

$$x_2^{[12]}[18,19] \oplus x_{6,19}^{[12]} = x_{2,19}^{[14]} \oplus x_6^{[14]}[25,26] \oplus x_{10}^{[14]}[18,19]. \tag{37}$$

Eqs. (27)–(37) are obtained as compositions of linear approximations for two consecutive additions, as illustrated in Fig. 1. Table 8 shows, for each approximation, the two underlying linear approximations of additions, together with the corresponding fundamental linear approximations Eqs. (9), (10), and (11) in Theorem 1.

Accordingly, for the compositions of these dependent linear approximations, we apply Theorem 1, whereas for the compositions of independent approximations, we use Lemma 3. The resulting probabilities that Eqs. (27)–(37) hold are presented in Lemma 10.

Table 8. Two Additions where Theorem 1 Applied

Eq.	Two Additions	Applied Equation in Theorem 1
(27)	$x_{11,12}^{[11]} = x_{11,12}^{[10]} + x_{12,12}^{[11]}, x_{11,12}^{[12]} = x_{11,12}^{[11]} + x_{12,12}^{[12]}$	(9)
(28)	$x_{0,16}^{[13]} = x_{0,16}^{[12]} + x_{4,16}^{[12]}, x_{0,16}^{[14]} = x_{0,16}^{[13]} + x_{4,16}^{[13]}$	(9)
(29)	$x_{8,8}^{[13]} = x_{8,8}^{[12]} + x_{12,8}^{[13]}, x_{8,8}^{[14]} = x_{8,8}^{[13]} + x_{12,8}^{[14]}$	(11)
(30)	$x_{8,31}^{[13]} = x_{8,31}^{[12]} + x_{12,31}^{[13]}, x_{8,31}^{[14]} = x_{8,31}^{[13]} + x_{12,31}^{[14]}$	(9)
(31)	$x_{1,12}^{[13]} = x_{1,12}^{[12]} + x_{5,12}^{[12]}, x_{1,12}^{[14]} = x_{1,12}^{[13]} + x_{5,12}^{[13]}$	(9)
(32)	$x_{1,23}^{[13]} = x_{1,23}^{[12]} + x_{5,23}^{[12]}, x_{1,23}^{[14]} = x_{1,23}^{[13]} + x_{5,23}^{[13]}$	(10)
(33)	$x_{1,7}^{[13]} = x_{1,7}^{[12]} + x_{5,7}^{[12]}, x_{1,7}^{[14]} = x_{1,7}^{[13]} + x_{5,7}^{[13]}$	(10)
(34)	$x_{9,26}^{[13]} = x_{9,26}^{[12]} + x_{13,26}^{[13]}, x_{9,26}^{[14]} = x_{9,26}^{[13]} + x_{13,26}^{[14]}$	(9)
(35)	$x_{2,16}^{[13]} = x_{2,16}^{[12]} + x_{6,16}^{[12]}, x_{2,16}^{[14]} = x_{2,16}^{[13]} + x_{6,16}^{[13]}$	(9)
(36)	$x_{2,7}^{[13]} = x_{2,7}^{[12]} + x_{6,7}^{[12]}, x_{2,7}^{[14]} = x_{2,7}^{[13]} + x_{6,7}^{[13]}$	(9)
(37)	$x_{2,19}^{[13]} = x_{2,19}^{[12]} + x_{6,19}^{[12]}, x_{2,19}^{[14]} = x_{2,19}^{[13]} + x_{6,19}^{[13]}$	(9)

Lemma 10. Eqs. (27) − (37) *hold with the following probabilities.*

$$\Pr[\text{Eq. (27)}] = \tfrac{1}{2}\left(1+\tfrac{1}{3}\right), \quad \Pr[\text{Eq. (28)}] = \tfrac{1}{2}\left(1+\tfrac{1}{6}\right), \quad \Pr[\text{Eq. (29)}] = \tfrac{1}{2}\left(1+\tfrac{1}{6}\right),$$
$$\Pr[\text{Eq. (30)}] = \tfrac{1}{2}\left(1+\tfrac{1}{3}\right), \quad \Pr[\text{Eq. (31)}] = \tfrac{1}{2}\left(1+\tfrac{1}{6}\right), \quad \Pr[\text{Eq. (32)}] = \tfrac{1}{2}\left(1+\tfrac{1}{6}\right),$$

$\Pr[\text{Eq. (33)}] = \frac{1}{2}\left(1+\frac{1}{6}\right)$, $\Pr[\text{Eq. (34)}] = \frac{1}{2}\left(1+\frac{1}{3}\right)$, $\Pr[\text{Eq. (35)}] = \frac{1}{2}\left(1+\frac{1}{6}\right)$,
$\Pr[\text{Eq. (36)}] = \frac{1}{2}\left(1+\frac{1}{3}\right)$, $\Pr[\text{Eq. (37)}] = \frac{1}{2}\left(1+\frac{1}{3}\right)$.

Proof. For simplicity, we prove only the probability that Eq. (27) holds. The other equations can be proved in the same manner. Consider two linear approximations $x_{11,12}^{[11]} = x_{11,12}^{[10]} + x_{12,12}^{[11]}$ and $x_{11,12}^{[12]} = x_{11,12}^{[11]} + x_{12,12}^{[12]}$, which can be explicitly expressed using carries as follows:

$$x_{11,12}^{[10]} = x_{11,12}^{[11]} \oplus x_{12,12}^{[11]} \oplus \Theta_{12}(x_{11}^{[10]}, x_{12}^{[11]}),$$
$$x_{11,12}^{[11]} = x_{11,12}^{[12]} \oplus x_{12,12}^{[12]} \oplus \Theta_{12}(x_{11}^{[11]}, x_{12}^{[12]}).$$

Combining these two equations, we obtain

$$x_{11,12}^{[10]} = x_{12,12}^{[11]} \oplus x_{11,12}^{[12]} \oplus x_{12,12}^{[12]} \oplus \Theta_{12}(x_{11}^{[10]}, x_{12}^{[11]}) \oplus \Theta_{12}(x_{11}^{[11]}, x_{12}^{[12]}). \quad (38)$$

Since $x_{11}^{[11]} = x_{11}^{[10]} + x_{12}^{[11]}$, we can apply Eq. (9) of Theorem 1 to the carries and obtain

$$\Pr[\Theta_{12}(x_{11}^{[10]}, x_{12}^{[11]}) \oplus \Theta_{12}(x_{11}^{[11]}, x_{12}^{[12]}) = x_{12,11}^{[11]} \oplus x_{12,11}^{[12]}] \approx \frac{1}{2}\left(1+\frac{1}{3}\right). \quad (39)$$

The remaining terms $x_{12,12}^{[11]}$ and $x_{12,12}^{[12]}$ can be further expanded with probability 1 as follows:

$$x_{12,11}^{[11]} = x_{1,11}^{[12]} \oplus x_{12,19}^{[12]}, \quad x_{12,12}^{[11]} = x_{1,12}^{[12]} \oplus x_{12,20}^{[12]}. \quad (40)$$

Finally, by applying Lemma 3 to combine Eqs. (38), (39), and (40), we obtain $\Pr[\text{Eq. (27)}] = \frac{1}{2}\left(1+\frac{1}{3}\right)$. □

Table 9. Biases and Errors before/after refinement of Eqs. (27)–(37)

Round	Group	Eq.	Experimental	[6, 7]		This work	
				Theoretical	Error	Theoretical	Error
5-6	Eq. (4)	(27)	$0.333358 \approx 2^{-1.585}$	2^{-2}	0.333432	$\frac{1}{3}$	0.000074
6-7	Group I	(28)	$0.166536 \approx 2^{-2.586}$	2^{-3}	0.332288	$\frac{1}{6}$	-0.000784
		(29)	$0.166524 \approx 2^{-2.586}$	2^{-2}	-0.333904	$\frac{1}{6}$	-0.000856
		(30)	$0.333272 \approx 2^{-1.585}$	2^{-2}	0.333088	$\frac{1}{3}$	-0.000184
	Group II	(31)	$0.166748 \approx 2^{-2.584}$	2^{-3}	0.333984	$\frac{1}{6}$	0.000488
		(32)	$0.166443 \approx 2^{-2.586}$	2^{-3}	0.331544	$\frac{1}{6}$	-0.001342
		(33)	$0.167328 \approx 2^{-2.579}$	2^{-3}	0.338624	$\frac{1}{6}$	0.003968
		(34)	$0.333313 \approx 2^{-1.585}$	2^{-2}	0.333252	$\frac{1}{3}$	-0.000061
	Group III	(35)	$0.166443 \approx 2^{-2.587}$	2^{-3}	0.331544	$\frac{1}{6}$	-0.001342
		(36)	$0.333374 \approx 2^{-1.585}$	2^{-2}	0.333496	$\frac{1}{3}$	0.000122
		(37)	$0.333618 \approx 2^{-1.584}$	2^{-2}	0.334472	$\frac{1}{3}$	0.000854

Table 9 presents the theoretical values, experimental results, and experimental errors of Eqs. (27)–(37) shown in Lemma 10, together with the results of [6, 7]. From the table, it can be seen that the new Lemma 10 reproduces the experimental results more precisely.

Proof of Lemma 1

Eq. (4) is constructed by combining Eq. (27) with the following two linear approximations:

$$
\begin{aligned}
&x_{3,0}^{[6]} \oplus x_{4,0}^{[6]} \\
&= x_{1,0}^{[10]} \oplus x_{3,0}^{[10]} \oplus x_{4,26}^{[10]} \oplus x_{7}^{[10]}[7,19] \oplus x_{8}^{[10]}[7,19] \oplus x_{9,0}^{[10]} \oplus x_{11,12}^{[10]} \\
&\quad \oplus x_{12}^{[10]}[6,7] \oplus x_{13}^{[10]}[0,8] \oplus x_{15,0}^{[10]}, \ w.p.\ \tfrac{1}{2}\left(1+\tfrac{1}{2}\right), \qquad (41) \\
&x_{1,0}^{[10]} \oplus x_{3,0}^{[10]} \oplus x_{4,26}^{[10]} \oplus x_{7}^{[10]}[7,19] \oplus x_{8}^{[10]}[7,19] \oplus x_{9,0}^{[10]} \\
&\oplus x_{11,12}^{[10]} \oplus x_{12}^{[10]}[6,7] \oplus x_{13}^{[10]}[0,8] \oplus x_{15,0}^{[10]} \\
&= x_{0}^{[12]}[0,16] \oplus x_{1}^{[12]}[0,6,7,22,23] \oplus x_{2}^{[12]}[0,6,7,8,16,18,19,24] \\
&\quad \oplus x_{4}^{[12]}[7,13,19] \oplus x_{5,7}^{[12]} \oplus x_{6}^{[12]}[7,13,14,19] \oplus x_{7}^{[12]}[6,7,14,15,26] \\
&\quad \oplus x_{8}^{[12]}[0,7,8,19,31] \oplus x_{9}^{[12]}[0,6,12,26] \oplus x_{10,0}^{[12]} \oplus x_{11}^{[12]}[6,7,12] \\
&\quad \oplus x_{12}^{[12]}[0,30,31] \oplus x_{13}^{[12]}[0,14,15,24,26,27] \\
&\quad \oplus x_{14}^{[12]}[8,25,26] \oplus x_{15,24}^{[12]}, \ w.p.\ \tfrac{1}{2}\left(1+\tfrac{1}{2^5}\right). \qquad (42)
\end{aligned}
$$

By experiments, we confirmed that Eq. (41) and Eq. (42) incur no experimental error (i.e., their empirical correlations match the stated values), whereas the only source of experimental deviation in the construction is Eq. (27). By Lemma 10, the correlation contributed by Eq. (27) is $\frac{1}{3}$. Under the (standard) independence assumptions required by Lemma 3, the overall correlation of $2^{-1} \cdot 2^{-5} \cdot \frac{1}{3} = \frac{1}{2^6 \cdot 3}$. Therefore, Pr[Eq. (4)] $= \frac{1}{2}\left(1+\frac{1}{2^6 \cdot 3}\right)$, which proves the claim. □

Proof of Lemma 2

For simplicity, we prove only the probability that Group I holds. Groups I is constructed by combining Eqs. (28)-(30) with the following linear approximation:

$$
\begin{aligned}
&x_{0,0}^{[12]} \oplus x_{4}^{[12]}[7,13,19] \oplus x_{8}^{[12]}[0,19] \oplus x_{12}^{[12]}[0,11,12,19,20,30,31] \\
&= x_{0}^{[14]}[0,3,4,11,12,14,15,16,18,20,27,28,30,31] \\
&\quad \oplus x_{4}^{[14]}[0,5,18,26,27] \oplus x_{8}^{[14]}[11,13,19,20,25,30] \\
&\quad \oplus x_{12}^{[14]}[3,4,8,11,13,22,23,24,26,27] \ w.p.\ \tfrac{1}{2}\left(1+\tfrac{1}{2^5}\right), \qquad (43)
\end{aligned}
$$

By experiments, we confirmed that Eq. (43) incur no experimental error, whereas the onlysource of experimental deviation in the construction is Eqs. (28)-(30). By Lemma 10, Eqs. (28), (29), and (30) contribute correlations of $\frac{1}{6}$, $\frac{1}{6}$, and $\frac{1}{3}$, respectively. Under the independence assumptions required by Lemma 3, the overall correlation of $2^{-5} \cdot \frac{1}{6} \cdot \frac{1}{6} \cdot \frac{1}{3} = \frac{1}{2^7 \cdot 3^3}$. Therefore, Pr[Group I] $= \frac{1}{2}\left(1+\frac{1}{2^7 \cdot 3^3}\right)$, which proves the claim. □

Proof of Theorem 2
The linear approximation in Theorem 2 consists of the partial linear approximations Eq. (4) and Groups I–IV. By applying Lemma 3 to combine Eq. (4) and Groups I–III refined in Lemmas 1 and 2 with the remaining approximations including Group IV in Lemma 8, we derive Theorem 2.

6 Conclusion

In this paper, we addressed the discrepancies between theoretical and experimental bias estimates in the linear and differential-linear cryptanalysis of ARX-based ciphers, with a particular focus on ChaCha. We introduced new fundamental linear approximations for two consecutive additions over three independent variables and rigorously derived their exact probabilities. Our analysis demonstrated that the conventional assumption of independence between consecutive additions introduces systematic errors, leading to theoretical values that diverge significantly from experimental measurements.

By applying our theorem to ChaCha, we refined the probabilities of key linear approximations used in existing distinguishers. In particular, we improved the theoretical estimates of Eq. (4) and Groups I–III, which had shown large deviations in previous work. Our refined approximations yield theoretical biases that are much closer to the experimental results, thereby reducing the gap between theory and practice. This not only strengthens the validity of existing attacks but also provides a more reliable framework for evaluating the security of ChaCha against differential-linear cryptanalysis.

The results presented here demonstrate the importance of carefully analyzing dependencies in ARX-based designs and highlight that seemingly small refinements in bias estimation can lead to a significant improvement in the accuracy of cryptanalytic evaluations. Future work includes applying the proposed framework to other ARX ciphers, such as Salsa20 and variants of ChaCha, as well as exploring its integration into key-recovery scenarios. We believe that the methodology developed in this paper will serve as a solid foundation for further advances in the cryptanalysis of ARX-based primitives.

Acknowledgements This work is partially supported by JSPS KAKENHI Grant Number JP21H03443 and SECOM Science and Technology Foundation.

References

1. Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, and Christian Rechberger. New features of latin dances: analysis of Salsa, ChaCha, and Rumba. In *Fast Software Encryption: 15th International Workshop, FSE 2008*, pages 470–488. Springer, 2008.
2. Emanuele Bellini, David Gerault, Juan Grados, Rusydi H Makarim, and Thomas Peyrin. Boosting differential-linear cryptanalysis of ChaCha7 with MILP. *IACR Transactions on Symmetric Cryptology*, 2023.

3. Daniel J Bernstein. Salsa20 specification. *eSTREAM Project algorithm description, http://www. ecrypt. eu. org/stream/salsa20pf. html*, 2005.
4. Arka Rai Choudhuri and Subhamoy Maitra. Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha. *IACR Transactions on Symmetric Cryptology*, 2016(2):261–287, 2016.
5. Murilo Coutinho and TC Souza Neto. New multi-bit differentials to improve attacks against ChaCha. *Cryptology ePrint Archive*, 2020.
6. Murilo Coutinho and Tertuliano C. Souza Neto. Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha. In *Advances in Cryptology - EUROCRYPT 2021*, volume 12696, pages 711–740. Springer, 2021.
7. Murilo Coutinho, Iago Passos, Juan C Grados Vásquez, Santanu Sarkar, Fábio LL de Mendonça, Rafael T de Sousa Jr, and Fábio Borges. Latin Dances Reloaded: Improved Cryptanalysis Against Salsa and ChaCha, and the Proposal of Forró. *Journal of Cryptology*, 36(3):18, 2023.
8. Sabyasachi Dey, Hirendra Kumar Garai, Santanu Sarkar, and Nitin Kumar Sharma. Enhanced differential-linear attacks on reduced round chacha. *IEEE Transactions on Information Theory*, 69(8):5318–5336, 2023.
9. Antonio Flórez-Gutiérrez and Yosuke Todo. Improved Cryptanalysis of ChaCha: Beating PNBs with Bit Puncturing. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 15061 of *Lecture Notes in Computer Science*, pages 427–457. Springer, 2025.
10. Daniel J.Bernstein. ChaCha, a variant of Salsa20. In *In Workshop Record of SASC*, volume 8, pages 3–5, 2008.
11. Susan K. Langford and Martin E. Hellman. Differential-Linear cryptanalysis. In *In Advances in Cryptology - CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 17–25. Springer, 1994.
12. Mitsuru Matsui. Linear Cryptanalysis Method for DES cipher. In *Advances in Cryptology - EUROCRYPT '93,*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.
13. Kaisa Nyberg and Johan Wallén. Improved linear distinguishers for SNOW 2.0. In *Fast Software Encryption*, volume 4047 of *Lecture Notes in Computer Science*, pages 144–162. Springer, 2006.
14. Andrea Röck and Kaisa Nyberg. Exploiting linear hull in Matsui' s algorithm 1 (extended version). *Cryptology ePrint Archive*, 2011.
15. Johan Wallén. Linear Approximations of Addition Modulo 2^n. In *Fast Software Encryption*, volume 2887 of *Lecture Notes in Computer Science*, pages 261–273. Springer, 2003.
16. Shichang Wang, Meicheng Liu, Shiqi Hou, and Dongdai Lin. Moving a step of ChaCha in Syncopated Rhythm. In *Advances in Cryptology – CRYPTO 2023*, volume 14083 of *Lecture Notes in Computer Science*, pages 273–304. Springer, 2023.
17. Ryo Watanabe, Nasratullah Ghafoori, and Atsuko Miyaji. Improved Differential-Linear Cryptanalysis of Reduced Rounds of ChaCha. In *International Conference on Information Security Applications*, volume 14402 of *Lecture Notes in Computer Science*, pages 269–281. Springer, 2023.