IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 December 2023, accepted 15 January 2024, date of publication 22 January 2024, date of current version 29 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3356868

RESEARCH ARTICLE

Higher-Order Differential-Linear Cryptanalysis of ChaCha Stream Cipher

NASRATULLAH GHAFOORI AND ATSUKO MIYAJI, (Member, IEEE)
Graduate School of Engineering, Osaka University, Suita, Osaka 565-0871, Japan

Corresponding author: Nasratullah Ghafoori (ghafoori@cy2sec.comm.eng.osaka-u.ac.jp)

This work was supported in part by the Japan Society for Promotion of Science (JSPS) KAKENHI under Grant JP21H03443, and in part by the SECOM Science and Technology Foundation.

ABSTRACT This paper studies the advanced methodologies of differential cryptanalysis with a particular emphasis on higher-order differentials and higher-order differential-linear cryptanalysis, along with their application to the ChaCha stream cipher. The study focuses on the impact of higher-order differential cryptanalysis on different rounds of the ChaCha stream cipher and analyzes how the cipher resists higher-order differential cryptanalysis. Additionally, we apply higher-order differential-linear cryptanalysis to target the reduced rounds of the ChaCha stream cipher, achieving reduced time complexity compared with existing studies. Furthermore, we introduce the first-ever higher-order differential-linear attack on ChaCha 6 and ChaCha 7 with $2^{39.07}$ and $2^{135.07}$ time complexity, respectively. We substantially enhanced the attack complexity by a margin of $2^{11.93}$ on ChaCha 6 and $2^{31.82}$ on ChaCha 7. Moreover, for the first time, we report significantly larger higher-order differential biases of ChaCha, which were previously unknown for internal rounds beyond 3.5 rounds. Furthermore, this research reveals new linear approximations of certain bits from the 4th to the 6th and 7th rounds, thereby reducing the complexity of the distinguisher attack on the 5.5th, 6th, and 7th rounds of ChaCha.

INDEX TERMS Higher-order differential cryptanalysis, differential-linear cryptanalysis, symmetric cryptography, ChaCha, stream cipher.

I. INTRODUCTION

Given today's modern age of computing, symmetric ciphers are playing a crucial role in the security of digital communications, transactions, data exchange, and more. It helps us encrypt data at rest and data in transit. In symmetric cryptography, many algorithms are used as stream and block ciphers. Among stream ciphers, Salsa20 [1] and ChaCha [2] are particularly critical ciphers that have been deployed in a wide range of hardware and software products.[1,2] Substitution-permutation networks (often referred to as SPNs) and Addition, Rotation, and XoR (ARX) operations are applied to design the stream and block ciphers. ARX involves three basic operations: modular addition, constant distance left and right rotations, and bitwise exclusive OR. The security of ARX-based ciphers mainly depends on modular addition, whereas rotation helps ciphers increase the diffusion. ARX ciphers have several exciting advantages, such as fast performance, simple algorithms, and resistance to many attacks, including algebraic and timing attacks. Although ARX-based ciphers with fewer rounds are susceptible to differential and linear attacks, the differential bias and linear correlation significantly decrease as the number of rounds increases. In April 2005, Daniel J. Bernstein introduced the Salsa20 [1] stream cipher, which was followed by ChaCha [2] in January 2008. These ciphers were specifically designed to offer a high level of security with 256-bit protection against key-recovery attacks. In addition, both ciphers have a variant of 128 key bits. Salsa20, particularly its 20-round version was submitted by its designer to the ECRYPT Stream Cipher Project [4] also known as eSTREAM to position it as a candidate for stream ciphers suitable for software applications requiring high throughput and hardware applications constrained by resource limitations.

[1] https://ianix.com/pub/chacha-deployment.html

[2] https://ianix.com/pub/salsa20-deployment.html

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

The eSTREAM portfolio was finalized in September 2008 and Salsa20/12 a 12-round version of Salsa20 was designated as one of the finalists for the eSTREAM software portfolio. ChaCha also has a 12-round variant. However, JP-Aumasson [3] proposed reducing ChaCha's rounds from the original 20 to 8 asserting that this modification does not compromise its security. This reduction would result in a significant speed increase of approximately 2.5 times.

A. MOTIVATION

ChaCha stream cipher has demonstrated resilience against first-order differential cryptanalysis. However, it remains untested against variations of differential cryptanalysis techniques, specifically higher-order differential cryptanalysis. This can potentially render ChaCha susceptible to the variations of differential cryptanalysis. For instance, the COCONUT98 [8] block cipher was initially invulnerable to first-order differential cryptanalysis, yet succumbed to a variant known as the Boomerang attack proposed by David Wagner [9]. Acknowledging this precedent, we aim to conduct a rigorous higher-order differential attack on ChaCha. This investigation aims to assess ChaCha's robustness against the variations of differential cryptanalysis, thus contributing to a comprehensive understanding of its security strengths and potential vulnerabilities. We have extensively explained that recent studies have not explored the resilience of ChaCha against higher-order differential and higher-order differential linear cryptanalysis. Consequently, the study field lacks a clear understanding of ChaCha security against higher-order differential and higher-order differential linear attacks. This paper aims to bridge this gap by conducting an in-depth examination and application of higher-order differential and higher-order differential linear cryptanalysis on ChaCha stream ciphers. The objective of this study is to uncover vulnerabilities within the ChaCha stream cipher concerning higher-order differentials and to report novel biases in various rounds.

B. OUR CONTRIBUTIONS

The key points presented in this paper are outlined as follows:

- We comprehensively explore higher-order differential (second-order and third-order) cryptanalysis of the ChaCha stream cipher and report new higher-order differential biases for ChaCha 3, ChaCha 3.5, and ChaCha 4. The median bias for the mentioned three rounds is 0.00002. The details are presented in Tables 6 and 7, respectively.
- We report new $\mathcal{ID}, \mathcal{OD}$ positions for higher-order differential cryptanalysis of ChaCha. Where $\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]}$ and $\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]} \oplus X^{(0)}_{13,[31]}$ are used as $\mathcal{ID}$ positions for the second and third order differentials, respectively. The $\mathcal{OD}$ positions vary. Please refer to Tables 6 and 7.
- We present a new linear approximation of the ChaCha stream cipher. We report the linear approximation from the 4th rounds to the 6th round with probability $1/2^2$. Please refer to Lemma 6.
- We presented an attack on ChaCha 6 and ChaCha 7 which enhanced the attack complexity by a margin of $2^{11.93}$ on ChaCha 6 and $2^{31.82}$ on ChaCha 7.
- This paper delineates a distinguisher attack on ChaCha 5.5, ChaCha 6, and ChaCha 7 offering improved attack complexity compared with existing studies. The new complexities are listed in Table 9.
- Our findings reveal significant higher-order differential-linear biases for various versions of ChaCha. Specifically, we observed a bias of $2^{-17.53}$ for ChaCha 5.5, $2^{-19.5}$ for ChaCha 6, and an exceptional bias of $2^{-67.5}$ for ChaCha 7.

C. ORGANIZATION OF THIS PAPER

The rest of this paper is organized as follows. Section II provides an overview of existing studies on ChaCha stream cipher security including differential cryptanalysis, linear cryptanalysis, and higher-order differential-linear cryptanalysis which is the primary adversary model for this research. Section III, presents the results obtained from our cryptanalysis approach applied to ChaCha. Finally, Section IV concludes this research and suggests potential future directions.

II. RELATED WORK

This section highlights principal cryptanalysis studies on ChaCha stream ciphers over the last 14 years. To make it easier to understand the research background, we structured this section according to the types of cryptanalysis rather than the chronological order in which the researchers conducted their work. We divided the cryptanalysis of ChaCha into three types. 1) single-bit differential cryptanalysis, 2) differential-linear cryptanalysis, and 3) higher-order differential cryptanalysis. In addition, we explained the past studies' findings, attack approaches, essential proofs, and ideas to better position our work in this research field.

A. NOTATIONS

Throughout this paper, we have used the following notations.

B. SPECIFICATION OF CHACHA

Bernstein introduced ChaCha to improve the diffusion properties of its predecessor, Salsa20. ChaCha updates its state matrix by performing four additions, four XOR operations, and four rotations with a notable difference being that ChaCha updates each word twice instead of once compared to Salsa20. ChaCha adheres to the same fundamental design principles as Salsa20, utilizing 32-bit word units and starting with an initial state of 512 bits. This initial state includes four constant words (c1 = 0×61707865, c2 = 0×3320646e, c3 = 0×79622d32, c4 = 0×6b206574), a 256-bit key, and four nonce words as inputs. ChaCha functions as an iterative stream cipher

TABLE 1. Notations.

Notation	Description
X	A 4 × 4 ChaCha matrix consisting of 16 words.
$X^{(0)}$	The initial state matrix of ChaCha
$X'^{(0)}$	The associate matrix with a single bit difference at $x_{i,j}$ position
$X^{(R)}$	The matrix after ChaCha R rounds
$X^{(r)}$	The matrix after ChaCha r rounds where $R > r$
$x_i^{(R)}$	The $i-th$ word of state matrix $X^{(R)}$
$\Theta(x,y)$	Carry function of the sum $x+y$
$\mathcal{ID}$	Input difference
$\mathcal{OD}$	output difference
$Pr(E)$	Probability of occurrence of an event E
$x_{i,j}^{(R)}$	The $j-th$ bit of $i-th$ word of matrix $X^{(R)}$
$x+y$	The word-wise addition of word x and y
$x-y$	The word-wise subtraction of word x and y
$x \oplus y$	Bit-wise XOR operation of the word x and y
$x \lll n$	The left rotation of word x by n bits
Δx	The XOR difference of word x and x'
ε_d	Differential bias
ε_L	Linear bias
$\varepsilon_d \cdot \varepsilon_L^2$	Differential-Linear bias
γ_i	The neutrality measure of ith key bit
ChaCha n	The n round of ChaCha stream cipher

employing 20 rounds of operations. In each round, the state of ChaCha denoted as the ith state undergoes modification via a set of operations referred to as a quarter-round (QR), which involves four input words (x_a, x_b, x_c, x_d). For ChaCha, the initial state matrix is as follows:

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

The ChaCha round function involves four simultaneous executions of the quarter-round function. A vector $(x_a^{(r)}, x_b^{(r)}, x_c^{(r)}, x_d^{(r)})$ within the internal state matrix $X^{(r)}$ is modified by performing the following computations sequentially:

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

where:

- The subscripts indicate the positions and rounds.
- $\oplus$ represents the bitwise XOR operation.
- $\lll$ represents a left rotation by a specified number of bits.

For rounds with odd numbers, designated as column rounds, the quarter-round operation is performed on four column vectors: $(x_0^{(r)}, x_4^{(r)}, x_8^{(r)}, x_{12}^{(r)})$, $(x_1^{(r)}, x_5^{(r)}, x_9^{(r)}, x_{13}^{(r)})$, $(x_2^{(r)}, x_6^{(r)}, x_{10}^{(r)}, x_{14}^{(r)})$, and $(x_3^{(r)}, x_7^{(r)}, x_{11}^{(r)}, x_{15}^{(r)})$. In contrast, for even numbered rounds, known as diagonal rounds, the quarter-round operation is applied to the following four diagonal vectors: $(x_0^{(r)}, x_5^{(r)}, x_{10}^{(r)}, x_{15}^{(r)})$, $(x_1^{(r)}, x_6^{(r)}, x_{11}^{(r)}, x_{12}^{(r)})$, $(x_2^{(r)}, x_7^{(r)}, x_8^{(r)}, x_{13}^{(r)})$, and $(x_3^{(r)}, x_4^{(r)}, x_9^{(r)}, x_{14}^{(r)})$. To compute a 512-bit keystream block, we sum the initial state $X^{(0)}$ with the state after the final round $X^{(R)}$, where R represents the last round. The original ChaCha version comprises 20 rounds, and the notation ChaCha20/R denotes a reduced round variant of ChaCha. It is worth noting that the round function of ChaCha is reversible, meaning that an input vector $(x_a^{(r+1)}, x_b^{(r+1)}, x_c^{(r+1)}, x_d^{(r+1)})$ in the internal state matrix $X^{(r+1)}$ can be retraced by sequentially computing the following steps:

$$\begin{cases} x_{b'''}^{(r)} = x_b^{(r+1)} \lll 25, & x_{b''}^{(r)} = x_{b'''}^{(r)} \oplus x_c^{(r+1)}, \\ x_{c'}^{(r)} = x_c^{(r+1)} - x_d^{(r+1)}, & x_{d'''}^{(r)} = x_d^{(r+1)} \lll 24, \\ x_{d''}^{(r)} = x_{d'''}^{(r)} \oplus x_a^{(r+1)}, & x_{a'}^{(r)} = x_a^{(r+1)} - x_{b''}^{(r)}, \\ x_{b'}^{(r)} = x_{b''}^{(r)} \lll 20, & x_b^{(r)} = x_{b'}^{(r)} \oplus x_{c'}^{(r)}, \\ x_c^{(r)} = x_{c'}^{(r)} - x_{d''}^{(r)}, & x_{d'}^{(r)} = x_{d''}^{(r)} \lll 16, \\ x_d^{(r)} = x_{d'}^{(r)} \oplus x_{a'}^{(r)}, & x_a^{(r)} = x_{a'}^{(r)} - x_b^{(r)} \end{cases} \quad (2)$$

C. SINGLE-BIT ATTACKS

In 2008, Aumasson et al. [5] introduced a significant cryptanalysis attack on the reduced rounds of both Salsa20 and ChaCha. Aumasson et al. [5] proposed a differential attack based on the concept of Probabilistic Neutral Bits (PNB). The concept of PNB involves dividing secret key bits into two groups: m for significant key bits and n for non-significant key bits. The key bits neutrality measure is used as a threshold to distinguish between these groups. The sizes of subsets m and n have a significant impact on the attack complexity. Aumasson's research on ChaCha 7 revealed an attack with a time complexity of 2^{248} and data complexity of 2^{27}. Subsequently, nearly all cryptanalysis techniques have been iteratively improved and followed Aumasson's approach. Shi et al. [6] introduced the notions of the Column Chaining distinguisher (CCD) and Probabilistic Neutral Vector (PNV). These concepts were applied to target ChaCha 7, resulting in an attack with time complexity of $2^{246.5}$ and data complexity of 2^{27}. In 2015, Maitra et al. [7] revisited the concept of Probabilistic Neutral Bits (PNBs) and provided insights into specific parameters aimed at reducing the complexity of existing attacks. Their research successfully achieved a key search with a complexity of $2^{247.2}$. In 2016 Maitra et al. [10] introduced a chosen IV attack strategy applicable to Salsa20 and Chacha stream ciphers. In this context, they proposed an attack on ChaCha 7, characterized by a time complexity of approximately $2^{238.94}$ and a data complexity of roughly $2^{23.89}$. In 2017, Dey and Sarkar [13] enhanced the attack on Salsa20 by incorporating additional PNBs. Furthermore, Sabyasachi Dey [13] conducted an attack on ChaCha 7, resulting in a time complexity of approximately $2^{235.2}$. In 2021, Miyashita et al. [15] employed PNB-focused differential cryptanalysis on the ChaCha stream cipher. Their method introduced an attack on ChaCha 7.25 rounds, with a time complexity of $2^{255.62}$ and a data complexity of $2^{48.36}$. Ghafoori et al. [24] applied Miyashita's approach to Salsa20 ChaCha. Ghafoori enhanced the key recovery attack on ChaCha 7.25 with a complexity of approximately $2^{254.011}$. Thus far, all of the aforementioned attacks have utilized single-bit differential cryptanalysis.

D. DIFFERENTIAL-LINEAR ATTACK

In 2016, Choudhuri and Maitra [12] revolutionized Salsa20 and ChaCha cryptanalysis using differential-linear techniques [33]. Their groundbreaking work introduced new linear approximations for these ciphers resulting in an attack on ChaCha 7 with time complexity $2^{237.65}$, data complexity $2^{31.6}$. In 2020, Coutinho et al. [21] improved the work proposed in [12] and attacked ChaCha 6 and ChaCha 7 with $2^{102.2}$ operation and a $2^{231.9}$ operation respectively. In 2020, Coutinho et al. [34] introduced a novel method known as Continuous Diffusion Analysis (CDA) which can be used to examine the diffusion characteristics of the ChaCha stream cipher. In 2021, Coutinho et al. [22] derived a new linear approximation and reported a noteworthy attack on ChaCha 6 which had a complexity of 2^{51}, and a key recovery attack on ChaCha 7, characterized by a complexity of $2^{228.51}$. In 2021, Beierle et al. [14] introduced a framework for differential linear adversaries in the context of ARX ciphers. Within this framework, an attack on ChaCha 7 was presented featuring a time complexity of $2^{230.86}$ and a data complexity of $2^{48.83}$. In 2022, Dey and Sabyasachi [16] enhanced the field of differential-linear cryptanalysis. They proposed an attack on ChaCha 7 with a time complexity of 2^{221} and a data complexity of 2^{90}. In addition, Dey et al. [36] revisited Cryptanalysis on ChaCha from Crypto 2020 and Eurocrypt 2021. Furthermore, Dey et al. [35] recently introduced an attack on ChaCha 7.25 which displayed a complexity of $2^{244.85}$. Subsequently, Niu et al. [17] presented an improved differential-linear distinguisher designed for four rounds of ChaCha. In 2023, Coutinho et al. [18] introduced a distinguisher attack with 2^{214} operations on ChaCha 7 and reported a new linear approximation for the Chacha subround. Following this, Dey et al. [19] reported a $2^{99.48}$ operations attack on ChaCha 6. Afterward, Wang et al. [20] reported an attack with $2^{210.3}$ operations and $2^{103.3}$ data on ChaCha 7, a $2^{244.9}$ operations and $2^{104.9}$ data on ChaCha 7.5 rounds. In 2023, Bellini et al. [23] studied differential-linear cryptanalysis and introduced a key recovery attack on ChaCha 7 with complexity $2^{206.8}$ and a distinguisher attack on ChaCha 7 and ChaCha 7.5 with complexity $2^{166.89}$ and $2^{251.54}$, respectively. In 2023, Dey et al. [38] introduced distinguisher attack on ChaCha 7 with complexity 2^{207} and a distinguisher attack on ChaCha 7.25 with complexity 2^{231}. For a better understanding of the existing attacks on ChaCha, we present the key recovery attack in Table 2 and distinguisher attacks in Table 3.

E. HIGHER ORDER DIFFERENTIAL-LINEAR ATTACK

Kai [37] introduced a differential-linear attack on ChaCha 3.5, ChaCha 4, and ChaCha 4.5 with the bias of $1/2$, $2^{-1.19}$, and $2^{-4.81}$, respectively. In existing studies on the security analysis of ChaCha, it is clear that all the attacks presented so far have focused only on single-bit differential or single-bit differential-linear attacks. Consequently, there is a noticeable lack of research on higher-order differential and higher-order differential-linear attacks on ChaCha. Our research will further explore the field of higher-order differential-linear cryptanalysis to assess the security of the ChaCha stream cipher against a significant adversary model.

TABLE 2. Overview of the most effective key recovery attack on a 256-bit key of ChaCha.

Attack	Target	Time	Data	Ref
Differential	ChaCha 6	2^{139}	2^{30}	[5]
D-Linear	ChaCha 6	$2^{127.5}$	$2^{37.5}$	[12]
D-Linear	ChaCha 6	$2^{77.4}$	2^{58}	[14]
Differential	ChaCha 6	2^{136}	2^{28}	[6]
D-Linear	ChaCha 6	$2^{102.2}$	2^{56}	[21]
Differential	ChaCha 7	2^{248}	2^{27}	[5]
D-Linear	ChaCha 7	$2^{237.7}$	2^{96}	[12]
D-Linear	ChaCha 7	$2^{230.86}$	$2^{48.8}$	[14]
D-Linear	ChaCha 7	$2^{221.95}$	$2^{48.83}$	[16]
Differential	ChaCha 7	$2^{231.63}$	$2^{49.58}$	[15]
Differential	ChaCha 7	$2^{210.3}$	$2^{103.3}$	[20]
Differential	ChaCha 7	$2^{206.8}$	$2^{110.81}$	[23]
Differential	ChaCha 7.25	$2^{255.62}$	$2^{48.36}$	[15]
Differential	ChaCha 7.25	$2^{254.011}$	$2^{51.81}$	[24]
Differential	ChaCha 7.25	$2^{244.85}$	$2^{93.24}$	[35]
Differential	ChaCha 7.25	$2^{242.9}$	$2^{125.8}$	[20]

TABLE 3. Summary of best distinguisher attacks on ChaCha.

Attack	Target Round	Time	Data	Ref
D-Linear	ChaCha 4	2^{6}	2^{6}	[12]
D-Linear	ChaCha 5	2^{16}	2^{16}	[12]
D-Linear	ChaCha 5.5	$2^{35.07}$	$2^{35.07}$	This work
D-Linear	ChaCha 6	2^{116}	2^{116}	[12]
D-Linear	ChaCha 6	2^{51}	2^{51}	[22]
D-Linear	ChaCha 6	$2^{39.07}$	$2^{39.07}$	This work
D-Linear	ChaCha 7	2^{224}	2^{224}	[22]
D-Linear	ChaCha 7	2^{214}	2^{214}	[18]
Differential	ChaCha 7	2^{207}	2^{207}	[38]
D-Linear	ChaCha 7	$2^{166.89}$	$2^{166.89}$	[23]
D-Linear	ChaCha 7	$2^{135.07}$	$2^{135.07}$	This work
Differential	ChaCha 7.5	2^{231}	2^{231}	[38]
D-Linear	ChaCha 7.5	$2^{251.54}$	$2^{251.54}$	[23]

F. CRYPTANALYSIS METHODS: A COMPARATIVE REVIEW

In this section, we provide a thorough explanation of the primary cryptographic techniques. We explain differential cryptanalysis, linear cryptanalysis, differential-linear attack, and higher-order differential adversary model.

1) DIFFERENTIAL CRYPTANALYSIS

Biham and Shamir [26] initially introduced differential cryptanalysis as a framework for assessing the security of DES-like cryptosystems. Over time, it has evolved into a primary method for analyzing the security of block ciphers, stream ciphers, and hash functions. It is a chosen plain text attack that attempts to track the probability of and input different $\mathcal{ID}$ to an output difference $\mathcal{OD}$. At its core, this cryptanalysis method aims to exploit the $\mathcal{ID}$ propagation through n rounds in a cipher to find bias. It observes how an $\mathcal{ID}$ changes in the initial state lead to corresponding changes in the $\mathcal{OD}$. Cryptanalysts can use this information to perform key recovery attacks. The *XOR* operation computes the difference. Attackers aim to find the $\mathcal{ID}$ and $\mathcal{OD}$ denoted by Δ_x and Δ_z or alternatively as α and β, respectively. Limpa [27] examined the XOR differential probability of addition denoted as xdp^{+} and the additive differential probability of XOR expressed as $adp^{\bigoplus}$. The differential probability (DP) concerning modulo 2^n addition shows the likelihood that the input difference affects the resulting output difference.

$$\begin{aligned} DP^{+}(\delta) &= DP^{+}(\alpha, \beta \mapsto \delta) \\ &:= P_{x,y}\left[(x+y) \oplus ((x \oplus \alpha) + (y \oplus \beta)) = \delta\right] \end{aligned} \tag{3}$$

The inputs denoted by x and y have a size of n. In this study, we refer to the initial state matrices of ChaCha as ChaCha X and a modified copy of the initial state matrix with a single-bit difference as ChaChaX'. The interconnected states following R rounds are labeled as X^R and X'^R. Furthermore, we also examine the intermediate rounds of the ChaCha cipher, which we denote as X^r and X'^r where $R > r$. The differential bias of the ChaCha stream cipher after a specific round r is calculated as follows:

$$\Pr\left(\Delta_p^{(r)}[q] = 1 \mid \Delta_i^{(0)}[j] = 1\right) = \frac{1}{2}(1 + \varepsilon_d) \tag{4}$$

Here, ε_d represents the bias of $\mathcal{OD}$. When key bits are randomly generated, we determine ε_d^* as the median value of ε_d [5].

Proposition 1 [29]: The probability of a differential (a, b) is the probability that the first derivative of a function $f(x)$ at point a takes the value b when x is uniformly random.

As the majority of symmetric ciphers are designed by iterating cryptographically weak functions. If the attacker can predict the output difference with a higher probability, the probabilistic success rate of the attack increases as well. The basic idea of differential cryptanalysis can be generalized to higher-order differentials where more than two pairs of inputs to the cipher function can be used to recover the secret key. Next, we explain the basic concept of higher-order differential cryptanalysis.

2) HIGHER-ORDER DIFFERENTIAL CRYPTANALYSIS

Lai [29] introduced the concept of higher-order derivatives for multi-variable functions. Lai explored a potential extension of first-order differential cryptanalysis by considering higher-order derivatives. Inspired by boomerang and differential-linear cryptanalysis, Biham et al. [11] investigated various combined attack techniques. These methods encompass differential-bilinear, higher-order differential-linear (HDL), and boomerang attacks. Now, let us revisit the fundamental definitions.

Definition 1 [29]: Consider two Abelian groups, denoted as $(S, +)$ and $(T, +)$. For function $f : S \mapsto T$, the derivatives of f at a specific point $a \in S$ are defined as follows:

$$\Delta_a f(x) = f(x+a) - f(x)$$

The ith derivative of the function f at the point $(a_1, a_2, \ldots, a_i)$ is defined as:

$$\Delta^{(i)}_{a_1,\ldots,a_i} f(x) = \Delta_{a_i}(\Delta^{(i-1)}_{a_1,\ldots,a_{i-1}} f(x))$$

where $\Delta^{(i-1)}_{a_1,\ldots,a_{i-1}} f(x)$ is the $(i-1)$th derivative of f at $(a_1, \ldots, a_{i-1})$. The 0th derivative of $f(x)$ was defined as $f(x)$ itself.

For $i = 2$, we have

$$f(x + a_1 + a_2) = \Delta^{(2)}_{a_1,a_2} f(x) + \Delta_{a_1} f(x) + \Delta_{a_2} f(x) + f(x).$$

Proposition 2 [29]:

$$f(x + a_1 + a_2 + \ldots + a_n) = \Sigma_{i=0}^{n} \Delta^{(i)}_{a_{j_1},\ldots,a_{j_i}} f(x)$$

Proposition 3 [29]: For any function $f : F_2^n \mapsto F_2^m$. The $n-th$ derivative of f is a constant. if $f : F_2^n \mapsto F_2^m$ is invertible, then $(n-1)-th$ derivative of f is a constant.

Proposition 4 [29]: Let $deg(f)$ represent the nonlinear degree of a multi-variable polynomial function $f(x)$. Thus, it holds that $deg(\Delta_a f(x)) \leq deg(f(x)) - 1$.

Proposition 5 [29]: The derivatives of a Boolean function remain consistent, regardless of the order in which differentiation is performed. That is, for any permutation $p(j)$ of index j, the derivatives remain the same.

$$\Delta^{(i)}_{a_1,\ldots,a_i} f(x) = \Delta^{(i)}_{a_{p(1)},\ldots,a_{p(i)}} f(x)$$

Knudsen [30] proposed higher-order differential cryptanalysis based on higher derivatives. The higher-order differential adversary model attacks the cipher based on the generalization of differential cryptanalysis. Knudsen proposed applications of truncated and higher-order differentials and showed that some ciphers that are secure against differential cryptanalysis are vulnerable to higher-order differential cryptanalysis. Many researchers have applied higher-order differential cryptanalysis to evaluate the security of various ciphers. In 2011, Duan and Lai [31] introduced a framework for higher-order differentials and demonstrated that higher-order differential cryptanalysis is based on higher-order derivatives of Boolean functions. Zhu et al. [32] worked on a cryptanalysis tool to examine the security of Boolean algebra-based block ciphers. Zhu proposed an algorithm to expedite cryptanalysis. Shi [6] applied second-order differential cryptanalysis to Salsa20 and ChaCha stream ciphers. Shi defined a second-order differential as follows: Let X be the initial state matrix, and X_1, X_2, and X_3 be associated state matrices with a single bit input difference $[\Delta_{ij}^{(0)}] = 1$ in X_1, a single bit input difference $[\Delta_{mn}^{(0)}] = 1$ in X_2 and double bit input difference $[\Delta_{ij}^{(0)}] = 1$, $[\Delta_{mn}^{(0)}] = 1$ respectively. According to Shi [6] $(i-m)^2 + (j-m)^2 = 0$ should not hold. The single-bit output difference $[\Delta_{pq}^{(r)}] = 1$ after r internal rounds can be computed as follows:

$$[\Delta_p^{(r)}]_q = [X_p^{(r)}]_q \oplus [X_{1,p}^{(r)}]_q \oplus [X_{2,p}^{(r)}]_q \oplus [X_{p+1}^{(r)}]_q \tag{5}$$

while the second-order input difference is dented by:

$$([X_p^{(r)}]_q | X_i^{(0)}]_j, [X_m^{(0)}]_n)$$

The forward bias ε_d is calculated as

$$\Pr\big([\Delta_p^{(r)}]q = 1 | [\Delta_i^{(0)}]_j, [\Delta_m^{(0)}]_n\big) = \frac{1}{2}(1 + \varepsilon_d) \tag{6}$$

3) LINEAR CRYPTANALYSIS

Linear Cryptanalysis introduced by Matsui [28], initially served as an adversarial model to assess the security of the DES cipher. Like its differential counterpart, linear cryptanalysis is a chosen plaintext attack that assumes that the attacker can select a set of plaintexts, whether predetermined or random and their corresponding outputs. In this adversary model, the focus is on utilizing the statistical characteristics of linear approximations between the plaintext and ciphertext. By identifying these linear connections, attackers can obtain crucial key information. The fundamental concept revolves around approximating a portion of the cipher's operation through bitwise manipulation with mod-2 (specifically, the exclusive OR operation denoted as $\oplus$). This expression has the following structure:

$$X_{t_1} \oplus X_{t_2} \cdots \oplus X_{t_u} \oplus Y_{v_1} \oplus Y_{v_2} \cdots \oplus Y_{v_z} = 0 \tag{7}$$

where the X_t is the tth bit of input vector $X = [X_1, X_2, \ldots]$ and Y_v is the vth bit of input vector $Y = [Y_1, Y_2, \ldots]$. The equation 7 represents the exclusive-OR of t input bits and v output bits. In linear cryptanalysis, the method identifies expressions similar to those mentioned in equation 7 that give either a high or low probability. If a cipher shows a pattern in which the equation holds or does not hold with a high probability, the cipher lacks effective randomness. If we can obtain the linear approximation of a cipher with $[Pr = 1]$, then the cipher has disastrous weaknesses. Surprisingly, some specific bit positions in the ChaCha stream cipher could be approximated with a probability of 1. This is discussed in Lemma 2. To combine the linear bias of different rounds of a cipher we use Lemma 3 of [28] called (Piling-up Lemma) and define it in Lemma 1.

Lemma 1 [28]: Let X_i $(1 \leq i \leq n)$ be an independent random variable whose values are zero with probability p_i or 1 with probability $1 - p_i$. Then the probability that $X_1 \oplus X_2 \cdot \cdots \oplus X_n = 0$ is

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

With Lemma 1 in mind, it can be stated that the increased number of rounds in a cipher enhances its security compared to when reduced rounds are used.

4) DIFFERENTIAL-LINEAR CRYPTANALYSIS

The differential-linear attack [33] shares similarities with traditional differential or linear attacks. Any difference between these attack methodologies primarily stems from the implementation approach to identify weaknesses within the cipher. The main idea behind the differential-linear adversary model is to combine the differential bias and the linear correlations.

The initial strategy of avoiding lengthy differentials and linear approximations seemed promising for safeguarding the cipher against certain attacks. However, it became apparent that exploiting shorter characteristics and approximations could still compromise its security. Langford's [33] introduction of the differential-linear cryptanalysis (DL technique) in 1994 highlighted a breakthrough: when a cipher E can be deconstructed as a cascade $E = E_2 \cdot E_1$, combining a differential probability of E_1 with a biased linear approximation of E_2 effectively distinguishes the entire cipher E. This technique proved successful in various ciphers. The procedure for the DL attack is as follows: Let E be a cipher. We write E as the composition of two sub-ciphers, $E1$ and $E2$, where $E1$ covers m rounds of the main cipher and $E2$ covers l rounds of the main cipher. We can write it $E = E_2 {\cdot} E_1$ see Fig 1. To attack cipher E with the differential-linear cryptanalysis method, we apply the differential cryptanalysis on E_1 and linear cryptanalysis on E_2 to cover the m and l rounds of the cipher. For E_1 we insert an input different $\mathcal{ID}$ $\Delta X^{(0)}$ in the initial states of sub-cipher E_1 and obtain the output difference $\mathcal{OD}$ $\Delta X^{(m)}$ after m rounds. Subsequently, we apply linear cryptanalysis to E_2 using masks Γ_m and Γ_{out}. We aim to find linear approximations for the remaining l rounds of cipher E. Using this method, we can create a differential-linear distinguisher that covers all $m + l$ rounds of cipher E. In some cases, we divide the cipher into three parts $E = E_3 \cdot E_2 \cdot E_1$ [14] where E_1 and E_2 cover the differential part and $E3$ covers the linear part. For the differential-linear analysis of ChaCha, consider matrices $X^{(r)}$ and $X'^{(r)}$ with their differentials denoted as $\Delta X^{(r)} = X^{(r)} \oplus X'^{(r)}$. Let $\Delta^{(r)} i[j]$ represent the difference between individual words at the jth bit of the ith word after r internal rounds computed as $x^{(r)} i[j] \oplus x_i'^{(r)}[j]$. Let $\mathcal{L}$ be the set of bits and let σ and σ' be linear combinations of bits within $\mathcal{J}$ defined as $\sigma = \left(\bigoplus_{(i,[j]) \in \mathcal{J}} x_{i,[j]}^{(r)}\right)$ and $\sigma' = \left(\bigoplus_{(i,[j]) \in \mathcal{J}} x'^{(r)} i, [j]\right)$. The linear combination ΔX is then expressed as $\Delta X = \left(\bigoplus (i, [j]) \in \mathcal{J} \Delta x_{i,[j]}^{(r)}\right)$ combining σ and σ'. The differential bias ε_d is calculated using $Pr\left[\Delta\sigma = 0 | \Delta X^{(0)}\right] = \frac{1}{2}(1 + \varepsilon_d)$. Through linear cryptanalysis, we can establish new relationships between the initial state and the state after the target round $R > r$. Specifically, let ρ and ρ' represent the linear combinations of bits in $\mathcal{J}$ after R rounds defined as $\rho = \left(\bigoplus_{(i,[j])\in\mathcal{J}} x_{i,[j]}^{(R)}\right)$ and $\rho' = \left(\oplus_{(i,[j])\in\mathcal{J}} x'^{(R)} i, [j]\right)$. The linear combination $\Delta\rho$ is then formed as $\Delta\rho = \left(\oplus(i,[j]) \in \mathcal{J}\Delta x_{i,[j]}^{(R)}\right)$. The probability that σ equals ρ is given by $Pr\left[\sigma = \rho\right] = \frac{1}{2}(1 + \varepsilon_L)$ where ε_L denotes linear correlation. Given that, our objective is to determine the bias, denoted by γ such that

$$Pr[\Delta_\rho = 0] = Pr[\rho \oplus \rho' = 0] = \frac{1}{2}(+\gamma).$$

$$\begin{aligned} Pr[\Delta_\sigma = \Delta_\rho] &= Pr[\sigma = \rho] \cdot Pr[\sigma' = \rho'] \\ &\quad + Pr[\sigma = \bar{\rho}] \cdot Pr[\sigma' = \bar{\rho}'] \\ &= \frac{1}{2}(1+\varepsilon_L) \cdot \frac{1}{2}(1+\varepsilon_L) \\ &\quad + \frac{1}{2}(1-\varepsilon_L) \cdot \frac{1}{2}(1-\varepsilon_L) = \frac{1}{2}(1+\varepsilon_L^2) \end{aligned}$$

Afterwards,

$$\begin{aligned} Pr[\Delta_\rho = 0] &= Pr[\Delta_\sigma = 0] \cdot Pr[\Delta_\sigma = \Delta_\rho] \\ &\quad + Pr[\Delta_\sigma = 1] \cdot Pr[\Delta_\sigma = \overline{\Delta_\rho}] \\ &= \frac{1}{2}(1+\varepsilon_d) \cdot \frac{1}{2}(1+\varepsilon_L^2) + \frac{1}{2}(1-\varepsilon_d) \cdot \frac{1}{2}(1-\varepsilon_L^2) \\ &= \frac{1}{2}(1+\varepsilon_d \cdot \varepsilon_L^2) \quad [12] \end{aligned}$$

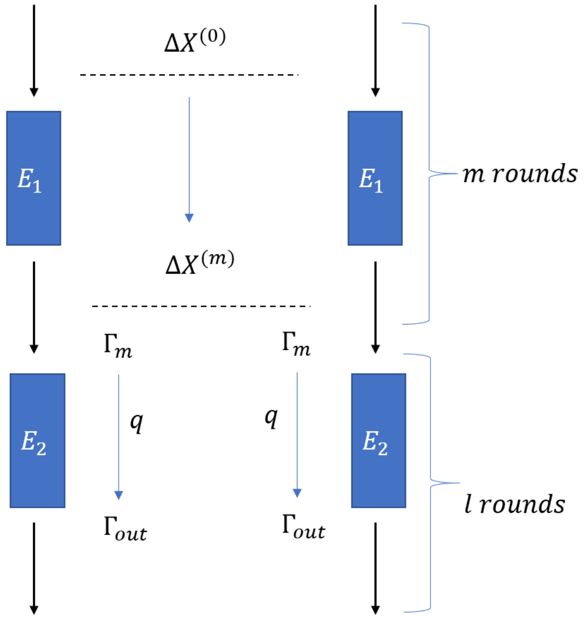


FIGURE 1. Differential-linear cryptanalysis.

The differential-linear correlation is calculated as $Pr\left[\Delta\rho = 0|\Delta X^{(0)}\right] = \frac{1}{2}(1 + \varepsilon_d \cdot \varepsilon_L^2)$, with $\varepsilon_d \cdot \varepsilon_L^2$ representing the differential-linear bias. The complexity of the distinguisher is determined as $\mathcal{O}\left(\frac{1}{\varepsilon_d^2 \cdot \varepsilon_L^4}\right)$. Typically, a minimum of $\mathcal{O}\left(\frac{1}{pq^2}\right)$ samples are required to differentiate between two events, where one event has a probability of p and the other event has a significantly smaller probability of q. In the context of the Differential-Linear adversary model, the assumption of randomness pertains to the independence between the sub-ciphers E_1 and E_2.

5) PROBABILISTIC NEUTRAL BITS

As discussed in Section II, the concept of Probabilistic Neutral Bits (PNB) enables us to partition the set of key bits into two distinct subsets, which we refer to as the significant key bits subset denoted as m, and the non-significant key bits subset denoted as n, where the relationship is expressed as $m = 256 - n$. To discern between these two sets, the PNB concept emphasizes assessing the impact of each key bit on the output of the ChaCha function, which we refer to as $\mathcal{OD}$ in this context. This influence of key bits on the output is termed the neutral measure. In this study, we incorporate the PNB concept into our approach to select the output differential positions denoted as $\mathcal{OD}$. Our objective was to identify those $\mathcal{OD}$ positions where the influence of key bits on the cipher's output is reduced after specific rounds.

The neutral measure associated with the key bit position γ_i concerning $\mathcal{OD}$ is defined as γ_κ. Specifically, it quantifies the probability that altering the key bit κ at position γ_i will not affect $\mathcal{OD}$. This probability is expressed as $\frac{1}{2}(1 + \gamma_\kappa)$.

According to [5], the following singular cases of the neutral measure exist:

- When $\gamma_k = 1$: it signifies that $\mathcal{OD}$ is unaffected by the ith key bit, which implies that it is non-significant.
- When $\gamma_k = 0$: it implies that $\mathcal{OD}$ is statistically independent of the ith key bit, making it significant.
- $\gamma_k = -1$: This indicates a linear dependence of $\mathcal{OD}$ on the ith key bit.

To accomplish this goal for the higher order differential attack, we developed the Algorithm 1.

G. LINEAR CRYPTANALYSIS OF CHACHA

In this section, we present the existing linear approximation of the ChaCha stream cipher proposed in previous studies. The author in [12] studied the ChaCha quarter-round function at the bit level. In 2021, Coutinho [22] changed the notation and defined a new linear approximation. For a better understanding, we follow Coutinho's notation. We review the bitwise representation of the ChaCha quarter-round function as follows.

$$x'^{(m-1)}_{a,i} = x^{(m-1)}_{a,i} \oplus x^{(m-1)}_{b,i} \oplus \Theta_i(x^{(m-1)}_a, x^{(m-1)}_b) \tag{8}$$

$$x'^{(m-1)}_{d,i+16} = x^{(m-1)}_{d,i} \oplus x'^{(m-1)}_{a,i} \tag{9}$$

$$x'^{(m-1)}_{c,i} = x^{(m-1)}_{c,i} \oplus x'^{(m-1)}_{d,i} \oplus \Theta_i(x^{(m-1)}_c, x'^{(m-1)}_d) \tag{10}$$

$$x'^{(m-1)}_{b,i+12} = x^{(m-1)}_{b,i} \oplus x'^{(m-1)}_{c,i} \tag{11}$$

$$x^{(m-1)}_{a,i} = x'^{(m-1)}_{a,i} \oplus x'^{(m-1)}_{b,i} \oplus \Theta_i(x'^{(m-1)}_a, x^{(m-1)}_b) \tag{12}$$

$$x^{(m)}_{d,i+8} = x'^{(m-1)}_{d,i} \oplus x^{(m)}_{a,i} \tag{13}$$

$$x^{(m)}_{c,i} = x'^{(m-1)}_{c,i} \oplus x^{(m-1)}_{d,i} \oplus \Theta_i(x'^{(m-1)}_c, x^{(m)}_d) \tag{14}$$

$$x^{(m)}_{b,i+7} = x'^{(m-1)}_{b,i} \oplus x^{(m)}_{c,i} \tag{15}$$

Upon reversing these equations, we obtain:

$$x'^{(m-1)}_{b,i} = x^{(m)}_{b+7} \oplus x^{(m)}_{c,i} \tag{16}$$
$$x'^{(m-1)}_{c,i} = x^{(m)}_{c,i} \oplus x^{(m)}_{d,i} \oplus \Theta_i(x'^{(m-1)}_{c}, x^{(m)}_{d}) \tag{17}$$
$$x'^{(m-1)}_{d,i} = x^{(m)}_{a,i} \oplus x^{(m)}_{d,i+8} \tag{18}$$
$$x'^{(m-1)}_{a,i} = x^{(m)}_{a,i} \oplus x^{(m)}_{b,i+7} \oplus x^{(m)}_{c} \oplus \Theta_i(x'^{(m-1)}_{a}, x'^{(m-1)}_{b}) \tag{19}$$
$$x^{(m-1)}_{b,i} = \mathcal{L}^{(m)}_{b,i} \oplus \Theta_i(x'^{(m-1)}_{c}, x^{(m)}_{d}) \tag{20}$$
$$x^{(m-1)}_{c,i} = \mathcal{L}^{(m)}_{c,i} \oplus \Theta_i(x'^{(m-1)}_{c}, x^{(m)}_{d}) \oplus \Theta_i(x^{(m-1)}_{c}, x'^{(m-1)}_{d}) \tag{21}$$
$$x^{(m-1)}_{d,i} = \mathcal{L}^{(m)}_{d,i} \oplus \Theta_i(x'^{(m-1)}_{a}, x'^{(m-1)}_{b}) \tag{22}$$
$$x^{(m-1)}_{a,i} = \mathcal{L}^{(m)}_{a,i} \oplus \Theta_i(x'^{(m-1)}_{a}, x'^{(m-1)}_{b}) \oplus \Theta_i(x'^{(m-1)}_{c}, x^{(m)}_{d}) \oplus \Theta_i(x^{(m-1)}_{a}, x^{(m-1)}_{b}) \tag{23}$$

where

$$\mathcal{L}^{m}_{a,i} = x^{m}_{a,i} \oplus x^{m}_{b,i+7} \oplus x^{m}_{b,i+19} \oplus x^{m}_{c,i+12} \oplus x^{m}_{d,i} \tag{24}$$
$$\mathcal{L}^{m}_{b,i} = x^{m}_{b,i+19} \oplus x^{m}_{c,i} \oplus x^{m}_{c,i+12} \oplus x^{m}_{d,i} \tag{25}$$
$$\mathcal{L}^{m}_{c,i} = x^{m}_{a,i} \oplus x^{m}_{c,i} \oplus x^{m}_{d,i} \oplus x^{m}_{d,i+8} \tag{26}$$
$$\mathcal{L}^{m}_{d,i} = x^{m}_{a,i} \oplus x^{m}_{a,i+16} \oplus x^{m}_{b,i+7} \oplus x^{m}_{c,i} \oplus x^{m}_{d,i+24} \tag{27}$$

Lemma 2 [12]: In the least significant bit (LSB) positions, the quarter-round function enables us to set $i = 0$ and accurately approximate the linear correlation from $m-1$ and m round with a probability of 1. Let

$$\Delta A^{(m)} = \Delta x^{(m)}_{\alpha,0} \oplus \Delta x^{(m)}_{\beta,7} \oplus \Delta x^{(m)}_{\beta,19} \oplus \Delta x^{(m)}_{\gamma,12} \oplus \Delta x^{(m)}_{\delta,0}, \tag{28}$$
$$\Delta B^{(m)} = \Delta x^{(m)}_{\beta,19} \oplus \Delta x^{(m)}_{\gamma,0} \oplus \Delta x^{(m)}_{\gamma,12} \oplus \Delta x^{(m)}_{\delta,0}, \tag{29}$$
$$\Delta C^{(m)} = \Delta x^{(m)}_{\delta,0} \oplus \Delta x^{(m)}_{\gamma,0} \oplus \Delta x^{(m)}_{\delta,8} \oplus \Delta x^{(m)}_{\alpha,0}, \tag{30}$$
$$\Delta D^{(m)} = \Delta x^{(m)}_{\delta,24} \oplus \Delta x^{(m)}_{\alpha,16} \oplus \Delta x^{(m)}_{\alpha,0} \oplus \Delta x^{(m)}_{\gamma,0} \oplus \Delta x^{(m)}_{\beta,7}. \tag{31}$$

Then, the following equations for four biases hold:

$$\left|\varepsilon(A^{(m)})\right| = \left|\varepsilon(x^{(m-1)}_{\alpha}[0])\right|,$$
$$\left|\varepsilon(B^{(m)})\right| = \left|\varepsilon(x^{(m-1)}_{\beta}[0])\right|,$$
$$\left|\varepsilon(C^{(m)})\right| = \left|\varepsilon(x^{(m-1)}_{\gamma}[0])\right|, \text{ and}$$
$$\left|\varepsilon(D^{(m)})\right| = \left|\varepsilon(x^{(m-1)}_{\delta}[0])\right|.$$

where these relations are divided into two cases depending on m,

1) If m is an odd number:

$$(\alpha, \beta, \gamma, \delta) \in \{(0, 4, 8, 12), (1, 5, 9, 13), (2, 6, 10, 14), (3, 7, 11, 15)\},$$

2) If m is an even number:

$$(\alpha, \beta, \gamma, \delta) \in \{(0, 5, 10, 15), (1, 6, 11, 12), (2, 7, 8, 13), (3, 4, 9, 14)\}.$$

For the proof, please refer to [12]

Lemma 3 [12]: To obtain the linear approximation of a half round of ChaCha, [12] defined the following lemma:

$$x^{(m)}_{a,i} = x^{(m+0.5)}_{a,i} \oplus x^{(m+0.5)}_{b,i+12} \oplus x^{(m+0.5)}_{c,i} \oplus C^{1}_{\text{carry},i} \tag{32}$$
$$x^{(m)}_{b,i} = x^{(m+0.5)}_{b,i+12} \oplus x^{(m+0.5)}_{c,i} \tag{33}$$
$$x^{(m)}_{c,i} = x^{(m+0.5)}_{c,i} \oplus x^{(m+0.5)}_{d,i} \oplus C^{2}_{\text{carry},i} \tag{34}$$
$$x^{(m)}_{d,i} = x^{(m+0.5)}_{d,i+16} \oplus x^{(m+0.5)}_{a,i} \tag{35}$$

Remarkably, we observe that the bias of variables such as $x^{(m)}_{b[i]}$ and $x^{(m)}_{d[i]}$ can be derived from round $m+0.5$ without any reduction in their value for all i. While the word positions $x^{(m)}_{b[i]}$ and $x^{(m)}_{d[i]}$ can be extended to a half round with probability 1 for all bit positions. However, the case is not the same as $x^{(m)}_{a[i]}$ and $x^{(m)}_{c[i]}$ which occur with probability < 1. Hence, we explain the following Lemma for the half-round extension of $x^{(m)}_{a[i]}$ and $x^{(m)}_{c[i]}$.

Lemma 4 [18]: When $i = 0$ the following linear approximations are valid with a probability of 1, considering a single active input bit in half round $m-1$ and multiple output bits in half round $m + 0.5$.

$$x^{(m)}_{c,i} = x^{(m+0.5)}_{c,i} \oplus x^{(m+0.5)}_{d,i} \tag{36}$$
$$x^{(m)}_{a,i} = x^{(m+0.5)}_{a,i} \oplus x^{(m+0.5)}_{b,i+7} \oplus x^{(m+0.5)}_{c,i} \tag{37}$$

When $i > 0$ the following linear approximations are valid with a probability of $1/2(1 + 1/2)$ considering a single active input bit in half round $m - 1$ and multiple output bits in half round m.

$$x^{(m)}_{c,i} = x^{(m+0.5)}_{c,i} \oplus x^{(m+0.5)}_{d,i} \oplus x^{(m+0.5)}_{d,i-1} \tag{38}$$
$$x^{(m)}_{a,i} = x^{(m+0.5)}_{a,i} \oplus x^{(m+0.5)}_{b,i+7} \oplus x^{(m+0.5)}_{c,i} \oplus x^{(m+0.5)}_{b,i+6} \oplus x^{(m+0.5)}_{c,i-1} \tag{39}$$

Lemma 5 [12]: When there is a single active input bit in round $m - 1$ and multiple active output bits in round m the following statement holds for $i > 0$:

$$x^{(m-1)}_{b,i} = x^{(m)}_{b,i+19} \oplus x^{(m)}_{c,i+12} \oplus x^{(m)}_{d,i} \oplus x^{(m)}_{c,i} \oplus x^{(m)}_{d,i-1}, \quad \text{W.P.} \frac{1}{2}\left(1 + \frac{1}{2}\right), \tag{40}$$
$$x^{(m-1)}_{a,i} = x^{(m)}_{a,i} \oplus x^{(m)}_{b,i+7} \oplus x^{(m)}_{b,i+19} \oplus x^{(m)}_{c,i+12} \oplus x^{(m)}_{d,i} \oplus x^{(m)}_{b,i+18} \oplus x^{(m)}_{c,i+11} \oplus x^{(m)}_{d,i-2} \oplus x^{(m)}_{d,i+6}, \quad \text{W.P.} \frac{1}{2}\left(1 + \frac{1}{2^4}\right), \tag{41}$$
$$x^{(m-1)}_{c,i} = x^{(m)}_{d,i} \oplus x^{(m)}_{c,i} \oplus x^{(m)}_{d,i+8} \oplus x^{(m)}_{a,i} \oplus x^{(m)}_{a,i-1} \oplus x^{(m)}_{d,i+7} \oplus x^{(m)}_{d,i-1}, \quad \text{W.P.} \frac{1}{2}\left(1 + \frac{1}{2^2}\right), \tag{42}$$
$$x^{(m-1)}_{d,i} = x^{(m)}_{d,i+24} \oplus x^{(m)}_{a,i+16} \oplus x^{(m)}_{a,i} \oplus x^{(m)}_{c,i} \oplus x^{(m)}_{b,i+7} \oplus x^{(m)}_{c,i-1} \oplus x^{(m)}_{b,i+6}, \quad \text{W.P.} \frac{1}{2}\left(1 + \frac{1}{2}\right), \tag{43}$$

Using Lemma 2, we can obtain a linear approximation for one round of ChaCha with (probability 1). In contrast, Lemma 5 provides a linear approximation with less than perfect certainty (probability < 1). Notably, equations 41 and 42 corresponding to words ‘A’ and ‘C,’ have lower probabilities of occurrence. The choice of words can significantly affect the overall complexity of an attack. Hence, it is advisable to avoid using these words.

H. HIGHER-ORDER DIFFERENTIAL-LINEAR ATTACK ON CHACHA

To provide a clearer understanding of higher-order differential cryptanalysis, we begin by introducing Kai's work on higher-order differential-linear cryptanalysis [37]. Kai studied higher-order differential-linear attacks from an algebraic perspective. Kai introduced a higher-order differential-linear distinguisher for several internal rounds of ChaCha. Kai first experimented to find high-biased second-order DL with a single bit $\mathcal{OD}$ and then appended the 1.5-round deterministic linear approximation. The 3.5-round $2nd$ order higher-order differential-linear holds with bias close to $\frac{1}{2}$. Kai used the $\Delta X^{(0)}_{12[0]} \oplus \Delta X^{(0)}_{14[0]}$ as $\mathcal{ID}$ position and the $\mathcal{OD}$ was selected as $\Delta X^{(2)}_{8,[0]}$

$$X^{(2)}_{8,[0]} = X^{3.5}_{0,[0]} \oplus X^{3.5}_{0,[8]} \oplus X^{3.5}_{3,[0]} \oplus X^{3.5}_{4,[12]} \oplus X^{3.5}_{9,[0]} \oplus X^{3.5}_{11,[0]} \oplus X^{3.5}_{12,[0]} \oplus X^{3.5}_{15,[16]} \oplus X^{3.5}_{15,[24]} \quad (44)$$

Kai found a 4-round 2nd order HDL with a bias of approximately $2^{-1.19}$. The $\Delta X^{(0)}_{13[16]} \oplus \Delta X^{(0)}_{14[0]}$ was used as $\mathcal{ID}$ position, and the $\mathcal{OD}$ was selected as $\Delta X^{(2.5)}_{8,[0]}$.

$$X^{(2.5)}_{8,[0]} = X^{4}_{1,[0]} \oplus X^{4}_{1,[16]} \oplus X^{4}_{2,[0]} \oplus X^{4}_{6,[7]} \oplus X^{4}_{8,[0]} \oplus X^{4}_{11,[0]} \oplus X^{4}_{12,[24]} \oplus X^{4}_{13,[0]} \oplus X^{4}_{13,[8]} \quad (45)$$

For ChaCha 4.5 rounds, Kai reported a 2nd-order differential-linear bias of approximately $2^{-4.81}$. The $\Delta X^{(0)}_{14[12]} \oplus \Delta X^{(0)}_{15[15]}$ was used as $\mathcal{ID}$ positions, and the $\mathcal{OD}$ was selected as $\Delta X^{(3)}_{8,[0]}$. The 1.5-round linear approximation occurred with probability 1/2

$$X^{(3)}_{8,[0]} = X^{4.5}_{0,[0]} \oplus X^{4.5}_{0,[8]} \oplus X^{4.5}_{1,[0]} \oplus X^{4.5}_{5,[12]} \oplus X^{4.5}_{9,[0]} \oplus X^{4.5}_{11,[0]} \oplus X^{4.5}_{12,[16]} \oplus X^{4.5}_{12,[24]} \oplus X^{4.5}_{15,[0]} \quad (46)$$

Kai combined the initial 3-round 2nd-order HDL approximation with a subsequent 1.5-round linear approximation, resulting in a 4-round 2nd-order HDL distinguisher with an approximately equal bias $2^{-4.81}$. The biases observed in the second-order DL distinguishers for these three versions surpassed those of all prior DL distinguishers. Owing to these notably higher biased approximations, it is possible to enhance the distinguishing attacks on ChaCha 3.5, ChaCha 4, and ChaCha 4.5.

III. HIGHER-ORDER DIFFERENTIAL-LINEAR CRYPTANALYSIS OF CHACHA

In this section, we comprehensively present the result of our proposed higher-order differential-linear attack on ChaCha stream cipher. We explore higher-order differential cryptanalysis on ChaCha and the resultant bias from higher-order differential attacks. To enhance attacks on ChaCha, we combine linear attacks with higher-order differentials.

A. PROPOSED CRYPTANALYSIS FEATURES

This section describes the features of our proposed attack, emphasizing the key strategies that augment its effectiveness.

- The method we used primarily relies on a higher-order differential basis, differing from previous ChaCha attacks that heavily depended on a first-order differential bias. This change in approach allowed us to explore the 4th round of the ChaCha stream cipher using a more verifiable higher-order differential bias. Subsequently, enhanced the attack complexity by a margin of $2^{11.93}$ on ChaCha 6 and $2^{31.82}$ on ChaCha 7.
- To increase the success probability of the attack, we used the median bias ε^{*}_{d}. We primarily utilized the 4th round forward bias which is generated as a result of higher-order differential cryptanalysis. The ChaCha stream cipher maintains a consistent median bias across the 3rd, 3.5th, and 4th rounds under higher-order differential cryptanalysis. Exploiting this vulnerability in the ChaCha QR function enabled us to focus on the 4th round which significantly reduced the complexity of the attack. Please refer to Table 6 and 7.
- We applied specific strategies to select multiple $\mathcal{ID}$ and $\mathcal{OD}$ positions. For $\mathcal{ID}$ positions, we employ the Hamming Weight technique to reduce the number of possible $\mathcal{ID}$s. Unlike approaches outlined in section II, which either randomly select the $\mathcal{ID}$ position or result from exhaustive searches, our method bypasses exhaustive search or random selection of $\mathcal{ID}$ positions. This approach resulted in a higher bias due to the Hamming Weight technique in the selection process, consequently enhancing the attack. Please refer to Subsection III-B.
- The selection of the $\mathcal{OD}$ position relies on a neutrality measure computed across 256 key bit positions concerning each $\mathcal{OD}$. To support this selection process, we developed Algorithm 1. This algorithm facilitates the identification of an optimal $\mathcal{OD}$ position with a higher bias. The $\mathcal{OD}$ positions exhibiting a higher neutral measure contribute to a more favorable bias, consequently reducing the complexity of the attack. Our experimental outputs validated this analysis. Please refer to Tables 4, 5, 6, 7 as well as Figs 2 and 3.
- While many existing attacks rely on linearity correlation to decrease attack complexity, often targeting either the 3rd or 3.5th round of differentials. We focused on enhancing the attack primarily through the differential aspect rather than the linear aspect. As a result, we pursued the verified bias of the 4th round. Although the attack primarily centers on differential analysis using 4 rounds, we included 2 rounds of linear approximation,

further enhancing the attack's efficiency. Please refer to Subsection III-C.

- We treat the differential and linear components of the attack as two separate ciphers. This implies that the linear component, which is constructed on the output of the differential part, remains unaffected by the differential analysis.

Algorithm 1 Computing Neutrality Measure of Key Bits Concerning the $\mathcal{OD}$ Position

```
Require: Random($X$) and associate states ($X_1, X_2, X_3$) and counter $T = 0$
Ensure: The $\mathcal{OD}$ position where the key bits generate the best average neutral measure given higher-order differentials.
    1. Generate random keywords $k = (k_0, \ldots, k_7)$.
    2. Decide $\mathcal{ID}$ $\Delta_{12}^{(0)}[15]$, $\Delta_{13}^{(0)}[20]$, $\Delta_{14}^{(0)}[21]$ and compute new initial states $X_1^{(0)} = X^{(0)} \oplus \Delta_{12}^{(0)}[15]$, $X_2^{(0)} = X^{(0)} \oplus \Delta_{13}^{(0)}[20]$ and $X_3^{(0)} = X^{(0)} \oplus \Delta_{12}^{(0)}[15] \oplus \Delta_{13}^{(0)}[20] \oplus \Delta_{14}^{(0)}[21]$.
    3. From the initial states $(X^{(0)}, X_1^{(0)}, X_2^{(0)}, X_3^{(0)})$, compute the states after $r = 4$ rounds $(X^{(4)}, X_1^{(4)}, X_2^{(4)}, X_3^{(4)})$ and the final states $(X^{(7)}, X_1^{(7)}, X_2^{(7)}, X_3^{(7)})$.
    4. From $(X^{(4)}, X_1^{(4)}, X_2^{(4)}, X_3^{(4)})$ compute output differentials $\mathcal{OD}$ $\Delta^{(4)}4[0] = X^{(4)}4[0] \oplus X_1^{(4)}4[0] \oplus X_2^{(4)}4[0] \oplus X_3^{(4)}4[0])$.
    5. From the final states $(X^{(7)}, X_1^{(7)}, X_2^{(7)}, X_3^{(7)})$ obtain the key-stream $Z = X^{(0)} + X^{(7)}$, $Z_1 = X_1^{(0)} + X_1^{(7)}$, $Z_2 = X_2^{(0)} + X_2^{(7)}$ and $Z_3 = X_3^{(0)} + X_3^{(R)}$.
    6. Complement a key bit $\kappa$ ($\kappa \in \{0, \ldots, 255\}$) and compute new initial states $\overline{X}^{(0)}, \overline{X_1}^{(0)}, \overline{X_2}^{(0)}, \overline{X_3}^{(0)}$ from initial states $(X^{(0)}, X_1^{(0)}, X_2^{(0)}, X_3^{(0)})$.
    7. Compute the states $(Y^{(4)}, Y_1^{(4)}, Y_2^{(4)}, Y_3^{(4)})$ with $Z - \overline{X}^{(0)}, Z_1 - \overline{X_1}^{(0)}, Z_2 - \overline{X_2}^{(0)}, Z_3 - \overline{X_3}^{(0)}$ as inputs to the inverse round function of ChaCha.
    8. Derive the output differentials $\Gamma^{(4)}4[0] = Y^{(4)}4[0] \oplus Y_1^{(4)}4[0] \oplus Y_2^{(4)}4[0] \oplus Y_3^{(4)}4[0]$ for all possible choices of 4 and 0.
    9. If $\Delta_4^{(4)}[0] = \Gamma_4^{(4)}[0]$ increment the $T$.
    10. Divide the sum of $T$ by the key trial and $\mathcal{ID}$ samples to obtain the probability of each key bit concerning $\Delta_4^{(4)}[0]$.
```

B. $\mathcal{ID}$, $\mathcal{OD}$ SELECTION APPROACHES

This subsection introduces novel $\mathcal{ID}$, $\mathcal{OD}$ positions associated with higher-order differentials. Our research approach selects the $\mathcal{OD}$ positions depending on two interconnected methodologies. First, we aimed to narrow down the possible $\mathcal{OD}$ positions from a pool of 512 possibilities to two selections (i.e., word B and D). To achieve this, we focused on identifying $\mathcal{OD}$ positions based on the structure of the ChaCha quarter-round function and the linear approximation lemmas of ChaCha. Our primary focus here was on $\mathcal{OD}$ positions th at produce an increased number of least significant bits when the bit position is set to zero ($i = 0$). Next, we validate the selected position using Algorithm 1 to extensively search the $\mathcal{OD}$ positions yielding the highest count of probabilistic neutral bits concerning the lth-order differential. For an in-depth discussion on PNBs, please refer to Section II and [5]. The algorithm was executed for both the $2nd$ and $3rd$-order differentials, targeting the $7th$, $7.25th$, and $7.5th$ rounds including respective internal and reverse rounds. The findings and conclusions derived from these experiments are consolidated in Tables 4 and 5 and visually represented in Figs 2 and 3. In these visual representations, the horizontal X-axis illustrates the position of $\mathcal{OD}$ bits where the vertical y-axis indicates the neutrality measure of the key bits. As observed, there is a decrease in the neutrality measure of the key bits when transitioning from lth order differentials to $l + 1$ order differentials. This observation suggests that when using a higher-order differential-linear approach in a key recovery attack based on the PNB concept the number of reverse rounds required for a successful attack should be lower than that required for a first-order differential attack. Additionally, higher-order differential-linear cryptanalysis enables the attacker to target a higher number of forward rounds, thereby addressing the weakness of lower reverse rounds when using this technique.

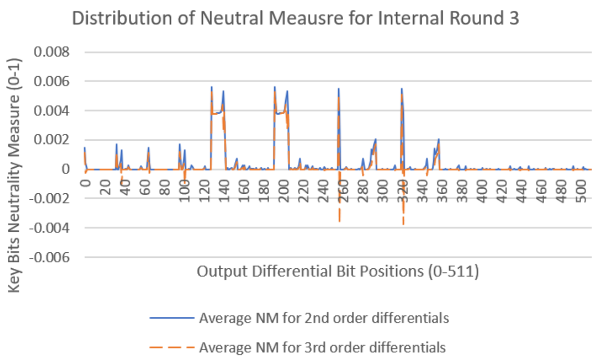


FIGURE 2. Distribution of NM for 2nd Order vs. 3rd order at round 7.

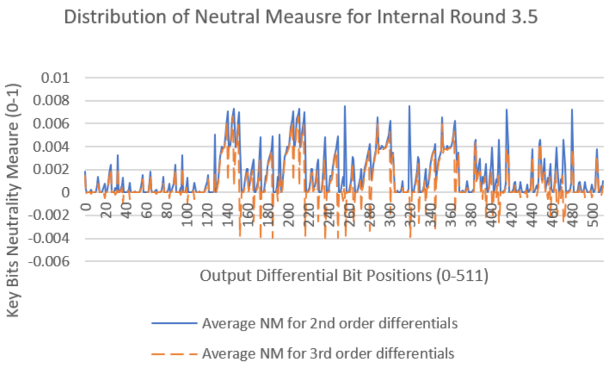


FIGURE 3. Distribution of NM for 2nd order vs. 3rd order at round 7.

Considering the nature of differential-linear attacks on ChaCha, our focus remains on $\mathcal{OD}$ positions at the 0th

TABLE 4. Best average neutral measure given 2*nd*-order differentials.

Target Round	Internal Rounds	$\mathcal{ID}$	$\mathcal{OD}$	Highest Average NM
7	3	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]}$	$\Delta X^{(3)}_{4,[0]}$	0.00561
7	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]}$	$\Delta X^{(3.5)}_{8,[0]}$	0.00755
7	4	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]}$	$\Delta X^{(4)}_{4,[0]}$	0.01449
7.25	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]}$	$\Delta X^{(3.5)}_{6,[19]}$	0.00729
7.5	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]}$	$\Delta X^{(3.5)}_{6,[6]}$	0.00393
7.75	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]}$	$\Delta X^{(3.5)}_{8,[0]}$	0.00185

TABLE 5. Best average neutral measure given 3*rd*-order differentials.

Target Round	Internal Rounds	$\mathcal{ID}$	$\mathcal{OD}$	Highest Average NM
7	3	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]} \oplus X^{(0)}_{14,[21]}$	$\Delta X^{(3)}_{4,[0]}$	0.00526
7	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]} \oplus X^{(0)}_{14,[21]}$	$\Delta X^{(3.5)}_{6,[18]}$	0.00667
7	4	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]} \oplus X^{(0)}_{14,[21]}$	$\Delta X^{(4)}_{0,[0]}$	0.01198
7.25	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]} \oplus X^{(0)}_{14,[21]}$	$\Delta X^{(3.5)}_{6,[18]}$	0.00663
7.5	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]} \oplus X^{(0)}_{14,[21]}$	$\Delta X^{(3.5)}_{6,[6]}$	0.00391
7.75	3.5	$\Delta X^{(0)}_{12,[15]} \oplus \Delta X^{(0)}_{13,[20]} \oplus X^{(0)}_{14,[21]}$	$\Delta X^{(3.5)}_{4,[7]}$	0.0.0001

TABLE 6. ChaCha 2nd-order bias.

$\mathcal{ID}$	$\mathcal{OD}$	ε_d	$\lvert\varepsilon_d *\rvert$
$\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]}$	$\Delta X^{(4)}_{4,[0]}$	0.000096	0.000021
$\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]}$	$\Delta X^{(3.5)}_{8,[0]}$	0.000103	0.00002
$\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]}$	$\Delta X^{(3)}_{4,[0]}$	0.00021	0.000021

TABLE 7. ChaCha 3rd-order bias.

$\mathcal{ID}$	$\mathcal{OD}$	$\lvert\varepsilon^*_d\rvert$
$\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]} \oplus \Delta X^{(0)}_{13,[31]}$	$\Delta X^{(4)}_{0,[0]}$	0.000021
$\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]} \oplus \Delta X^{(0)}_{13,[31]}$	$\Delta X^{(3.5)}_{6,[18]}$	0.00002
$\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]} \oplus \Delta X^{(0)}_{13,[31]}$	$\Delta X^{(3)}_{4,[0]}$	0.00002

bit. Consequently, we disregard all other positions where $i > 0$. From Tables 4 and 5, we selected the $\mathcal{OD}$ position $\Delta X^{(4)}_{4,[0]}$ to attack ChaCha 7 given its better neutrality measure compared the other positions. For the higher-order differentials, identifying $\mathcal{ID}$ positions is challenging. An exhaustive search is not an optimal solution. Considering the 2*nd*-order differential we would have 8128 possible $\mathcal{ID}$ positions when selecting two $\mathcal{ID}s$ at a time from a set of 128 possible $\mathcal{ID}s$. Because a brute-force search over the 8128 possible bit combinations is neither feasible nor optimal. We used the Hamming Weight strategy to select pairs of two bits in the case of 2nd-order differentials, allowing us to look at the forward differential ε_d. We attempted to find the Hamming weight of the ChaCha matrix with the $\mathcal{ID}$ in the initial state after the first, second, and third rounds. Interestingly, the ChaCha quarter-round function (Equation 1) evenly propagates the difference, regardless of the $\mathcal{ID}$ position. This was a different case for the Salsa20 stream cipher. In which the Salsa20 matrix hamming weight after specific rounds was affected by the $\mathcal{ID}$ position. The average change in the Hamming Weight of the ChaCha matrix after each round was 18.21%.

TABLE 8. ChaCha matrix hamming weight after specific rounds.

Rounds	HM	Percentage of Changes
1	10	2.14 %
2	63	12.5%
3	204	40.03%

As shown in Table 8, the $\mathcal{ID}$ position does not significantly affect the Hamming Weight which in turn may not have a notable impact on the forward differential. As a result, we have selected $\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]}$ as the input differential positions to calculate the second-order differential, and $\Delta X^{(0)}_{12,[0]} \oplus \Delta X^{(0)}_{13,[0]} \oplus \Delta X^{(0)}_{13,[31]}$ as the input differential positions to search the third-order differential bias of ChaCha. We ran an experiment [3] with a complexity of 2^{40} to search for the 2nd and third-order differentials. Our findings are summarized as follows. To distinguish between two events generated by a random number generator and ChaCha, we require $\mathcal{O}(\frac{1}{pq^2})$ random numbers. Consequently, a maximum of 2^{32} random values were required to distinguish the biases reported in Tables 6 and 7. The results in Tables 6 and 7 show that the highest bias represented by ε_d varies for each position. However, the absolute median bias denoted as $|\varepsilon^*_d|$ remains the same for both second and third-order biases. We also examine the biases at $\Delta X^{(3.5)}6[0]$, $\Delta X^{(3.5)}8[0]$, and $\Delta X^{(3.5)}11[0]$ for the second-order differential. For third-order differentials, we evaluated the biases at the $\Delta X^{(3.5)}15[0]$, $\Delta X^{(3.5)}6[0]$, $\Delta X^{(3.5)}11[0]$ and $\Delta X^{(3.5)}9[0]$ positions. The results match those reported in Tables 6 and 7. The

[3] We used the Maximum Length (M-Sequence) random number generator for our experiment. The Intel(R) Xeon(R) CPU E7-4830 v4 @ 2.00GHz was used to execute the experiment.

complexity of the attack given the second-order and third-order differential cryptanalysis will be $2^{31.07}$ for a 3.5 round of ChaCha. Hence, we need to utilize linear cryptanalysis to enhance the attack on the higher rounds of ChaCha.

C. LEVERAGING LINEAR CRYPTANALYSIS

The enhancement of higher-order differential cryptanalysis with linear cryptanalysis relies on the complementary strengths inherent in these two techniques. Here's how:

- Linear cryptanalysis can be used to identify linear structures within the cipher. These structures can then be exploited to simplify the differential analysis of the cipher [28], [33].
- Higher-order differential cryptanalysis often involves complex computations due to the large number of text differences that need to be considered (i.e., based on the differential order $\mathcal{L}$). Attacking the higher number of rounds with higher-order differential cryptanalysis will be computationally infeasible. By using linear approximations, the attack rounds can be further improved and overall the complexity of these computations can be significantly reduced. Refer to Algorithm 1 for practical understanding.
- The success of higher-order differential cryptanalysis depends on the probability of certain differential patterns occurring. Linear cryptanalysis can improve overall probabilities by identifying and exploiting linear relations between the plaintext, ciphertext, and key bits [33].
- While higher-order differential cryptanalysis is less effective against ciphers with high algebraic degrees [39], linear cryptanalysis can be used to analyze the linear components of these ciphers. This allows for a more thorough analysis of the cipher potentially leading to a more efficient attack.
- Some ciphers including the ChaCha stream cipher are resistant to attacks using just differential cryptanalysis and its variations. However, these ciphers are vulnerable when multiple techniques are employed together. By combining linear cryptanalysis and higher-order differentials, cryptanalysts can explore a wider range of possibilities to find weaknesses in the cipher

Given the outlined facts, our approach involved conducting a higher-order differential-linear attack on the ChaCha cipher. Subsection III-D offers a comprehensive explanation of integrating the linear segment within our proposed attack strategy.

D. NEW LINEAR APPROXIMATIONS

We based our attack on the following analysis: Given the existing studies and the absence of higher-order differential cryptanalysis on ChaCha, we sought to exploit the advantages of higher-order differentials and integrate them with linear cryptanalysis to target the reduced rounds of the ChaCha stream cipher. As demonstrated in Tables 6 and 7, the higher-order differential bias of the ChaCha stream cipher consistently yielded the same bias across different internal rounds (i.e., $r = 3, 3.5,$ and 4). The ChaCha design leads to this specific vulnerability in its structure. To the best of our knowledge, previous studies have focused on a differential analysis of 3.5 internal rounds of ChaCha and have reported linear approximations for only 2.5 rounds. No study has reported a differential-linear bias of 4 rounds. Considering the structure of differential attacks, increasing the number of internal rounds will help us to attack a higher number of rounds and consequently reduce the complexity of the final attack. Additionally, in alignment with Lemma 1, increasing the number of linear approximations decreases linear correlation. With this understanding, we used the 4th round of differential bias in ChaCha in conjunction with 2 rounds of linear approximation. For this purpose, we selected the $\mathcal{OD}$ position $\Delta x^{(4)}_{4,0}$ corresponds to the word B in ChaCha matrix and verified it with Algorithm 1. To extend the $\Delta x^{(4)}_{4,0}$ to the 5th round and get the linear approximation with probability 1, we used the Lemma 2.

Lemma 6: The following linear approximation from 4th to 6th rounds of ChaCha holds with probability $\frac{1}{2}(1+\frac{1}{2^2})$

$$\begin{aligned}\Delta x^{(4)}_{4[0]} = {} & \Delta x^{(6)}_{1[0]} \oplus \Delta x^{(6)}_{2[0,11,12]} \oplus \Delta x^{(6)}_{4[6]} \oplus \Delta x^{(6)}_{6[7]} \oplus \Delta x^{(6)}_{8[0,12]} \\ & \oplus \Delta x^{(6)}_{9[19,31]} \oplus \Delta x^{(6)}_{11[0]} \oplus \Delta x^{(6)}_{12[8]} \oplus \\ & \Delta x^{(6)}_{13[0,8,11,12,19,20]} \oplus \Delta x^{(6)}_{14[18,19]} \\ & \text{W.P. } \frac{1}{2}\left(1+\frac{1}{2^2}\right) \end{aligned} \tag{47}$$

Proof: At first, we extend from 4th round to 5th round with probability 1. For this purpose, we use the Lemma 2 and the approximation for the word B given the position of $\mathcal{OD}$ $\Delta x^{(4)}_{4[0]}$

$$\begin{aligned}\Delta x^{(m-1)}_{b[i]} &= \Delta x^{(m)}_{b[19]} \oplus \Delta x^{(m)}_{c[12]} \oplus \Delta x^{(m)}_{d[0]} \oplus \Delta x^{(m)}_{c[0]} \\ \Delta x^{(4)}_{4[0]} &= \Delta x^{(5)}_{4[19]} \oplus \Delta x^{(5)}_{8[12]} \oplus \Delta x^{(5)}_{12[0]} \oplus \Delta x^{(5)}_{8[0]} \\ & \text{W. P. } 1\end{aligned}$$

As the linear extension comes with the probability 1 in this case, $\varepsilon^*_d \cdot \varepsilon^2_l = \varepsilon^*_d$ and $\varepsilon^*_d \cdot \varepsilon^2_l = 2^{-15.5}$. Next, we would like to extend the linear approximation from the 5th round to the 5.5th round. For this purpose, we use the Lemma 3. Given the 5th round linear extension, all the expressions could be extended with probability 1 except $\Delta x^{(5)}_{8[12]}$ as it's in position C of the input vector to ChaCha quarter-round function. As a result, we use the Lemma 4 to extend the $\Delta x^{(5)}_{8[12]}$ to $\Delta x^{(5.5)}_{8[12]}$ with probability 1/2 and Lemma 3 to extend the remaining expressions to half round with probability 1.

$$\Delta x^{(5)}_{4[19]} = \Delta x^{(5.5)}_{4[31]} \oplus \Delta x^{(5.5)}_{9[19]} \text{ with probability } 1 \tag{48}$$

$$\begin{aligned}\Delta x^{(5)}_{8[12]} = {} & \Delta x^{(5.5)}_{8[12]} \oplus \Delta x^{(5.5)}_{13[12]} \oplus \Delta x^{(5.5)}_{13[11]} \\ & \text{with probability } \frac{1}{2}\end{aligned} \tag{49}$$

$$\Delta x^{(5)}_{12[0]} = \Delta x^{(5.5)}_{12[0]} \oplus \Delta x^{(5.5)}_{1[0]} \text{ with probability } 1 \tag{50}$$

$$\Delta x^{(5)}_{8[0]} = \Delta x^{(5.5)}_{8[0]} \oplus \Delta x^{(5.5)}_{13[0]} \text{ with probability } 1 \tag{51}$$

Consequently,

$$\Delta x^{(4)}_{4[0]} = \Delta x^{(5.5)}_{1[0]} \oplus \Delta x^{(5.5)}_{4[31]} \Delta x^{(5.5)}_{8[0,12]} \oplus \Delta x^{(5.5)}_{9[19]} \oplus \Delta x^{(5.5)}_{12[0]} \oplus \Delta x^{(5.5)}_{13[11,12,0]} \text{W.P. } \frac{1}{2}. \tag{52}$$

As a result, we can get the distinguisher and differential-linear bias for ChaCha 5.5 as $\varepsilon_d^* \cdot \varepsilon_l^2 = 2^{-18.53}$. The attack complexity ChaCha 5.5 is presented in Table 9. The higher-order differential biases of ChaCha 4 rounds were reported in Table 6. Next, we will extend the linear approximation from ChaCha 5.5 to ChaCha 6 rounds. For this purpose, we deploy the Lemma 3 for word positions in B and D which can be extended with probability 1. For the word positions in A and C, we use the Lemma 4 with probability $1/2(1 + 1/2)$.

$$\Delta x^{(5.5)}_{4[31]} = \Delta x^{(6)}_{4[6]} \oplus \Delta x^{(6)}_{9[31]} \text{ With Probability 1} \tag{53}$$

$$\Delta x^{(5.5)}_{9[19]} = \Delta x^{(6)}_{9[19]} \oplus \Delta x^{(6)}_{14[19]} \oplus \Delta x^{(6)}_{14[18]} \text{W.P. } \frac{1}{2}\left(1 + \frac{1}{2}\right) \tag{54}$$

$$\Delta x^{(5.5)}_{8[12]} = \Delta x^{(6)}_{8[12]} \oplus \Delta x^{(6)}_{13[12]} \oplus \Delta x^{(6)}_{13[11]} \text{W.P. } \frac{1}{2}\left(1 + \frac{1}{2}\right)$$

$$\Delta x^{(5.5)}_{13[12]} = \Delta x^{(6)}_{2[12]} \oplus \Delta x^{(6)}_{13[20]} \text{ With Probability 1} \tag{55}$$

$$\Delta x^{(5.5)}_{12[0]} = \Delta x^{(6)}_{1[0]} \oplus \Delta x^{(6)}_{12[8]} \text{With Probability 1} \tag{56}$$

$$\Delta x^{(5.5)}_{1[0]} = \Delta x^{(6)}_{1[0]} \oplus \Delta x^{(6)}_{6[7]} \oplus \Delta x^{(6)}_{11[0]} \text{ With Probability 1} \tag{57}$$

$$\Delta x^{(5.5)}_{8[0]} = \Delta x^{(6)}_{8[0]} \oplus \Delta x^{(6)}_{13[0]} \text{With Probability 1} \tag{58}$$

$$\Delta x^{(5.5)}_{13[0]} = \Delta x^{(6)}_{2[0]} \oplus \Delta x^{(6)}_{13[8]} \text{With Probability 1} \tag{59}$$

$$\Delta x^{(5.5)}_{13[11]} = \Delta x^{(6)}_{2[11]} \oplus \Delta x^{(6)}_{13[19]} \text{With Probability 1} \tag{60}$$

As a result, the term $\Delta x^{(6)}_{1[0]}$ would be removed and we get the following linear approximation with probability $1/2(1 + 1/2^2)$ from ChaCha 4 rounds to ChaCha 6. To the best of our knowledge, this is the first and best linear approximation reported for two rounds so far. The attack complexity is summarized in Table 9.

$$\Delta x^{(4)}_{4[0]} = \Delta x^{(6)}_{2[0,11,12]} \oplus \Delta x^{(6)}_{4[6]} \oplus \Delta x^{(6)}_{6[7]} \Delta x^{(6)}_{8[0,12]} \oplus \Delta x^{(6)}_{9[19,31]} \oplus \Delta x^{(6)}_{11[0]} \oplus \oplus \Delta x^{(6)}_{12[8]} \oplus \Delta x^{(6)}_{13[0,8,11,12,19,20]} \oplus \Delta x^{(6)}_{14[18,19]} \text{W.P.} \frac{1}{2}\left(1 + \frac{1}{2^2}\right). \tag{61}$$

Given the obtained linear probability and the $2nd$-order differential bias, the complexity of the attack on ChaCha 6 is reported in Table 9. The complexities in Table 9 are computed based on absolute median bias $|\varepsilon_d^*| = 0.000021$. Extending the linear approximation to the 7th round introduces the issue of significant bits. In the case of ChaCha, when setting $i = 0$, we get the linear approximation of the least significant bits with probability 1. Consequently, the computational cost is mainly influenced by the significant bits variables. The computation cost involves counting the occurrences of significant bits variables and the frequency of their appearances in the form (Variable Type, Number of Significant Bits Occurrences). Considering the linear approximation from 4th round to 6th round, the number of significant variables is $2, 2, 3, 8$ for the word A, B, C, D respectively which are denoted as $(x_a, 2), (x_b, 2), (x_c, 3), (x_d, 8)$. Using the probability of Lemma 5 which defines the probability of each word extension when $i > 1$ and Lemma 6, the linear correlation can be computed as $\varepsilon_L = \frac{1}{2^{2+2\cdot4+2\cdot1+3\cdot2+8\cdot1}}$. This leads to a 7 rounds distinguisher with complexity of $2^{135.07}$ and a differential-linear bias $|\varepsilon_d^*| \cdot \varepsilon_L^2 = 2^{-67.5}$. The ChaCha 7th round distinguisher and differential-linear bias are summarized in Table 9. If we compute the complexity of the attack with the highest bias $\varepsilon_d = 0.000096$, the complexity of the final attack can be reduced. The attacks presented in Lemma 6 are the best attacks presented on 5.5, 6, and 7 rounds of ChaCha. This is the first-ever higher-order differential-linear attack on ChaCha 5.5 ChaCha 6 and ChaCha 7 with the complexity of $2^{35.07}$, $2^{39.07}$ and $2^{135.07}$ time complexity, respectively. We improved the attack complexity by $2^{11.93}$ on ChaCha 6 and $2^{31.82}$ on ChaCha 7. Table 3 has summarized the results.

TABLE 9. Our proposed attack complexities.

Target	$\mathcal{OD}$	$\lvert\varepsilon_d^*\rvert$	$\lvert\varepsilon_d^*\rvert \cdot \varepsilon_L^2$	Complexity
5.5	$\Delta X^{(4)}_{4,[0]}$	0.000021	$2^{-17.5}$	$2^{35.07}$
6	$\Delta X^{(4)}_{4,[0]}$	0.000021	$2^{-19.5}$	$2^{39.07}$
7	$\Delta X^{(4)}_{4,[0]}$	0.000021	$2^{-67.5}$	$2^{135.07}$

IV. CONCLUSION

In this study, we investigated higher-order differential and higher-order differential-linear cryptanalysis and its application to the ChaCha stream cipher. We report the first-ever higher-order differential and higher-order differential-linear biases of different rounds of ChaCha. We also present attacks on ChaCha 5.5, ChaCha 6, and ChaCha 7. We significantly improved the attack complexities of ChaCha 6 and ChaCha 7. Our proposed attack on ChaCha 6 with a complexity of $2^{39.07}$ and on ChaCha 7 with a complexity of $2^{135.07}$ are the best-known attacks on reduced rounds of ChaCha stream ciphers. This is the first detailed study of higher-order differential linear cryptanalysis on ChaCha and we believe that the attack has the potential to become an important adversary model to analyze the security of different ciphers.

REFERENCES

[1] D. J. Bernstein, "The Salsa20 family of stream ciphers," in *New Stream Cipher Designs: The eSTREAM Finalists*. Cham, Switzerland: Springer, 2008, pp. 84–97.

[2] D. J. Bernstein, "ChaCha, a variant of Salsa20," in *Proc. Workshop Rec. SASC*, 2008, vol. 8, no. 1, pp. 3–5.

[3] J.-P. Aumasson, "Too much crypto," Cryptol. ePrint Arch., Paper 2019/1492, 2019. [Online]. Available: https://eprint.iacr.org/2019/1492

[4] *ECRYPT Stream Cipher Project*. Accessed: Aug. 19, 2023. [Online]. Available: https://www.ecrypt.eu.org/stream/

[5] J. P. Aumasson, S. Fischer, S. Khazaei, W. Meier, and C. Rechberger, "New features of Latin dances: Analysis of Salsa, ChaCha, and Rumba," in *Proc. 15th Int. Workshop FSE*, Lausanne, Switzerland. Cham, Switzerland: Springer, Feb. 2008, pp. 470–488.

[6] Z. Shi, B. Zhang, D. Feng, and W. Wu, "Improved key recovery attacks on reduced-round Salsa20 and ChaCha," in *Proc. Inscrypt*. Berlin Springer, 2012, pp. 337–351.

[7] S. Maitra, G. Paul, and W. Meier, "Salsa20 cryptanalysis: New moves and revisiting old styles," in *Proc. 9th Int. Workshop Coding Cryptogr. (WCC)*, A. Canteaut, G. Leurent, and M. Naya-Plasencia, Eds. Paris, France, Apr. 2015.

[8] S. Vaudenay, "Provable security for block ciphers by decorrelation," in *Proc. Annu. Symp. Theor. Aspects Comput. Sci.*, 1998, pp. 249–275.

[9] D. Wagner, "The boomerang attack," in *Proc. Int. Workshop Fast Softw. Encryption*, 1999, pp. 156–170.

[10] S. Maitra, "Chosen IV cryptanalysis on reduced round Chacha and Salsa," *Discrete Appl. Math.*, vol. 208, pp. 88–97, Jul. 2016.

[11] E. Biham, O. Dunkelman, and N. Keller, "New combined attacks on block ciphers," in *Proc. Fast Softw. Encryption (FSE*, in Lecture Notes in Computer Science, vol. 3557. Berlin, Germany: Springer, 2005, pp. 126–144.

[12] A. R. Choudhuri and S. Maitra, "Significantly improved multi-bit differentials for reduced round Salsa and ChaCha," in *Proc. IACR ToSC*, vol. 4, 2016, pp. 261–287.

[13] S. Dey and S. Sarkar, "Improved analysis for reduced round Salsa and Chacha," *Discrete Appl. Math.*, vol. 227, pp. 58–69, Aug. 2017.

[14] C. Beierle, M. Broll, F. Canale, N. David, A. Flórez-Gutiérrez, G. Leander, M. Naya-Plasencia, and Y. Todo, "Improved differential-linear attacks with applications to ARX ciphers," *J. Cryptol.*, vol. 35, no. 4, p. 29, Oct. 2022.

[15] S. Miyashita, R. Ito, and A. Miyaji, "PNB-focused differential cryptanalysis of ChaCha stream cipher," in *Proc. ACISP*, 2022, pp. 1407–1422.

[16] S. Dey, H. K. Garai, S. Sarkar, and N. K. Sharma, "Revamped differential-linear cryptanalysis on reduced round ChaCha," in *Proc. Eurocrypt*, 2022, pp. 86–114.

[17] Z. Niu, S. Sun, Y. Liu, and C. Li, "Rotational differential-linear distinguishers of ARX ciphers with arbitrary output linear masks," in *Proc. ICC*, 2022, pp. 3–32.

[18] M. Coutinho, I. Passos, J. C. G. Vásquez, S. Sarkar, F. L. L. de Mendonça, R. T. de Sousa, and F. Borges, "Latin dances reloaded: Improved cryptanalysis against salsa and ChaCha, and the proposal of Forró," *J. Cryptol.*, vol. 36, no. 3, p. 18, Jul. 2023, doi: 10.1007/s00145-023-09455-5.

[19] S. Dey, H. K. Garai, and S. Maitra, "Cryptanalysis of reduced round ChaCha—New attack & deeper analysis," *ToSC*, vol. 2023, no. 1, pp. 89–110, Mar. 2023.

[20] S. Wang, M. Liu, S. Hou, and D. Lin, "Moving a step of Chacha in syncopated rhythm," in *Proc. ICC*. Cham, Switzerland: Springer, 2023, pp. 273–304.

[21] M. Coutinho and T. C. S. Neto, "New multi-bit differentials to improve attacks against ChaCha," Cryptol. ePrint Arch., Paper 2020/350, 2020. [Online]. Available: https://eprint.iacr.org/2020/350

[22] M. Coutinho and T. C. S. Neto, "Improved linear approximations to ARX ciphers and attacks against ChaCha," in *Proc. 40th Adv. Cryptol.-EUROCRYPT*, vol. 40, Zagreb, Croatia. Cham, Switzerland: Springer, Oct. 2021.

[23] E. Bellini, D. Gerault, J. Grados, R. H. Makarim, and T. Peyrin, "Boosting differential-linear cryptanalysis of ChaCha7 with MILP," *IACR Trans. Symmetric Cryptol.*, vol. 2023, no. 2, pp. 189–223, Jun. 2023, doi: 10.46586/tosc.v2023.i2.189-223.

[24] N. Ghafoori, A. Miyaji, R. Ito, and S. Miyashita, "PNB based differential cryptanalysis of Salsa20 and Chacha," *IEICE Trans. Inf. Syst.*, vol. E106.D, no. 9, pp. 1407–1422, Sep. 2023.

[25] K. Hu, T. Peyrin, Q. Q. Tan, and T. Yap, "Revisiting higher-order differential-linear attacks from an algebraic perspective," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf.* Springer, 2023, pp. 405–435.

[26] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 3–72, May 1991.

[27] H. Lipmaa, J. Wallén, and P. Dumas, "On the additive differential probability of exclusive-or," in *Fast Software Encryption*, vol. 3017, B. Roy and W. Meier, Eds. Berlin, Germany: Springer, 2004, pp. 295–305.

[28] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. EUROCRYPT*, 1993, pp. 386–397.

[29] X. Lai, "Higher order derivatives and differential cryptanalysis," in *Communications and Cryptography: Two Sides of One Tapestry*. Boston, MA, USA: Springer, 1994, pp. 227–233.

[30] L. R. Knudsen, "Truncated and higher order differentials," in *Proc. 2nd Int. Workshop FSE*, vol. 2, Leuven, Belgium. Berlin, Germany: Springer, Dec. 1995, pp. 196–211.

[31] M. Duan and X. Lai, "Higher order differential cryptanalysis framework and its applications," in *Proc. Int. Conf. Inf. Sci. Technol.*, Mar. 2011, pp. 291–297.

[32] B. Zhu, K. Chen, and X. Lai, "Bitwise higher order differential cryptanalysis," in *Proc. 1st Int. Conf. Trusted Syst. INTRUST*, vol. 1, Beijing, China. Berlin, Germany: Springer, Dec. 2010.

[33] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in *Proc. Annu. Int. Cryptol. Conf.*, vol. 14, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 1994.

[34] M. Coutinho, R. T. De Sousa, and F. Borges, "Continuous diffusion analysis," *IEEE Access*, vol. 8, pp. 123735–123745, 2020, doi: 10.1109/ACCESS.2020.3005504.

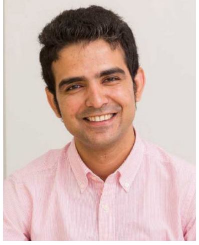
[35] S. Dey, H. K. Garai, S. Sarkar, and N. K. Sharma, "Enhanced differential-linear attacks on reduced round Chacha," *IEEE Trans. Inf. Theory*, vol. 69, no. 8, pp. 5318–5336, Aug. 2023, doi: 10.1109/TIT.2023.3269790.

[36] S. Dey, C. Dey, S. Sarkar, and W. Meier, "Revisiting cryptanalysis on ChaCha from crypto 2020 and Eurocrypt 2021," *IEEE Trans. Inf. Theory*, vol. 68, no. 9, pp. 6114–6133, Sep. 2022, doi: 10.1109/TIT.2022.3171865.

[37] K. Hu and T. Peyrin, "Revisiting higher-order differential (-linear) attacks from an algebraic perspective: Applications to ASCON, GRAIN v1, XOODOO, and ChaCha," in *Proc. 5th NIST Lightweight Cryptogr. Workshop*, 2022.

[38] C. Dey and S. Sarkar, "A new distinguishing attack on reduced round ChaCha permutation," *Sci. Rep.*, vol. 13, p. 13958, Aug. 2023, doi: 10.1038/s41598-023-39849-1.

[39] C. Boura and A. Canteaut, "On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 691–702, Jan. 2013.



NASRATULLAH GHAFOORI received the B.Sc. degree in computer science and the M.Sc. degree in information systems. He is currently pursuing the Ph.D. degree with the Graduate School of Engineering, Osaka University. He primarily conducts research in the field of applied cryptography with Osaka University.

ATSUKO MIYAJI (Member, IEEE) received the B.Sc., M.Sc., and Dr. (Sci.) degrees in mathematics from Osaka University, in 1988, 1990, and 1997, respectively. She was an Associate Professor with the Japan Advanced Institute of Science and Technology (JAIST), in 1998, where she was a Professor, from 2007 to 2023. She has been a Professor with the Graduate School of Engineering, Osaka University, since 2015. She is a fellow of IPSJ. She is a member of the International Association for Cryptologic Research, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, the Mathematical Society of Japan, the Japanese Society for Artificial Intelligence, and Japan Association for Medical Informatics. She received the Young Paper Award of SCIS'93, in 1993, Notable Invention Award of the Science and Technology Agency, in 1997, the IPSJ Sakai Special Researcher Award, in 2002, the Standardization Contribution Award, in 2003, the Award for the Contribution to Culture of Security, in 2007, the General Director of Industrial Science and Technology Policy and Environment Bureau Award, in 2007, DoCoMo Mobile Science Awards, in 2008, Advanced Data Mining and Applications (ADMA 2010) Best Paper Award, Prizes for Science and Technology, the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology, International Conference on Applications and Technologies in Information Security (ATIS 2016) Best Paper Award, the 16th IEEE TrustCom 2017 Best Paper Award, IEICE Milestone Certification, in 2017, the 14th Asia Joint Conference on Information Security (AsiaJCIS 2019) Best Paper Award, Information Security Applications—20th International Conference (WISA 2020) Best Paper Gold Award, IEICE Distinguished Educational Practitioners Award, in 2020, and IEICE Achievement Award, in 2023.