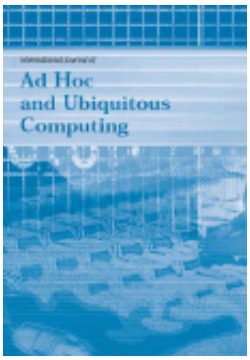

International Journal of Ad Hoc and Ubiquitous Computing

ISSN online: 1743-8233 - ISSN print: 1743-8225
https://www.inderscience.com/ijahuc

Theoretical analysis of biases in TLS encryption scheme Chacha 128

S.K. Karthika, Kunwar Singh

DOI: 10.1504/IJAHUC.2023.10052676

Article History:

Received:	06 December 2021
Last revised:	18 March 2022
Accepted:	18 March 2022
Published online:	16 December 2022

Theoretical analysis of biases in TLS encryption scheme Chacha 128

S.K. Karthika* and Kunwar Singh

Department of Computer Science and Engineering,
National Institute of Technology, Tiruchirappalli,
Tamilnadu, India
Email: karthika231188@gmail.com
Email: kunwar@nitt.edu
*Corresponding author

Abstract: Chacha is a software-oriented stream cipher designed by Bernstein (2008). Chacha is a Salsa variant that is eSTREAM project's finalist candidate. Google added Chacha and a message authentication code to their transport layer security (TLS) and datagram TLS (DTLS) protocols in 2016. Chacha has become an area of interest for cryptanalysis since its adoption by Google. Almost all the existing cryptanalysis is experimental. Experimental cryptanalysis identifies vulnerable areas of a cipher, whereas theoretical analysis helps in the development of possible countermeasures. Differential cryptanalysis is a cryptanalytic technique that helps in discovering distinguishers on stream ciphers. Recently, Dey and Sarkar (2021) have theoretically explored the reason behind distinguishers in Salsa and Chacha 256 stream cipher. Motivated by this work, we have theoretically analysed differential attacks on Chacha 128 (Chacha 256 variant) up to four rounds and we have the bias probabilities. Our theoretical analysis results match the experimental results.

Keywords: transport layer security; stream cipher; Chacha; theoretical analysis; differential cryptanalysis.

Reference to this paper should be made as follows: Karthika, S.K. and Singh, K. (2023) 'Theoretical analysis of biases in TLS encryption scheme Chacha 128', *Int. J. Ad Hoc and Ubiquitous Computing*, Vol. 42, No. 1, pp.47–58.

Biographical notes: S.K. Karthika received her BTech from the Coimbatore Institute of Engineering and Technology, MTech from the University College of Engineering, Trichy Campus. Currently, she is working as a Senior Research Fellow at the National Institute of Technology, Tiruchirappalli, under the project 'Research and Development of Lightweight Stream Ciphers' sponsored by Department of Science and Technology, India. Also, she is pursuing PhD under the guidance of Dr. Kunwar Singh, AP/CSE, National Institute of Technology, Tiruchirappalli. Her area of research is cryptanalysis and Stream ciphers.

Kunwar Singh received his BTech from the IIT Delhi, MTech degree from Jawaharlal University, New Delhi and PhD from the IIT Madras in 2015. Currently, he is an Assistant Professor in Computer Science and Engineering Department at the National Institute of Technology – Tiruchirappalli, India since 2006. His area of research includes public key cryptography, identity-based encryption, lattice-based cryptography, stream ciphers, multi-party computation and blockchain.

This paper is a revised and expanded version of a paper entitled 'Theoretical analysis of biases in Chacha 128-bits' presented at The 5th International Symposium on Mobile Internet Security (MobiSec'21), Jeju Island, Republic of Korea, 7–9 October 2021.

1 Introduction

Stream ciphers are fundamental cryptographic primitives that enable secure communication over insecure channels. A pseudo-random generator is the most important component of any stream cipher encryption. A short random stream, the *secret key* (seed) is fed into the pseudo-random generator, and the output is a long pseudo-random *keystream*. The ciphertext is obtained by bitwise/bytewise XOR of the keystream and the message in the stream cipher encryption phase. When it comes to decryption, keystream is regenerated by the receiver using the secret key, which is then XORed with the ciphertext to get the message. The most difficult aspect of any stream cipher is to create a keystream that is indistinguishable from a random stream. Using the same secret key to encrypt multiple messages

will make it vulnerable to attacks. At the same time, a new secret key for each message is nearly impossible. The use of initialisation vector (IV) is the solution to this key management problem. In a keystream generation, IVs serve as randomisers. Furthermore, IVs are public variables that vary depending on the encryption. Multiple messages can thus be encrypted using the same key but different IVs. A stream cipher's security is based on the assumption that the adversary will be unable to differentiate the keystream created by the stream cipher from a random stream.

When compared to block ciphers, stream ciphers are typically lighter and faster. As a result, stream ciphers are more suited to mobile communication devices with limited speed and memory. In recent years, along with the advancement of the internet, mobile devices have become increasingly important in communication. Mobile communication devices provide wireless connectivity anywhere, allowing users to communicate at any time and from anyplace. Mobile devices are utilised for more than just conversation – they are also used to exchange and transfer data. The development in communication technology has piqued the curiosity of attackers. Chacha is a lightweight stream cipher that Google uses in its transport layer. It is also used in mobile devices to ensure confidentiality. Chacha is now used in cloud computing as well. CloudFare's internet security is supported by Chacha. Chacha is also utilised in wireless sensor networks and the internet of things for network security. Since Chacha stream ciphers are used for TLS, Internet security, and network security, crypt analysts has always been interested in them.

Chacha is a software-oriented stream cipher that is a descendant of Salsa. Bernstein created both Salsa and Chacha in 2005 and in 2008, respectively. Chacha was created to improve the diffusion part of salsa, which had been susceptible to several cryptanalytic attacks. The author also claims that the minimal number of secure rounds for Chacha is smaller than the minimum number of secure rounds for Salsa. The cipher's implementation is simple, with minimal resources and low-cost operations, making it appropriate for use on a variety of architectures. It was created to avoid information leakage by side channel analysis, has a simple and quick key setup, and has a good overall performance.

Experimental cryptanalysis on a property of the cipher helps to pose an attack on the cipher, whereas theoretical cryptanalysis helps us to understand the vulnerability which made the attack possible. Further, theoretical analysis of a cipher can be used to assess the security of any cipher design. The overhead in the theoretical cryptanalysis is the manual computation and it is tedious when we try to exploit distinguishers of higher rounds. To the best of our knowledge, all the existing attacks on Chacha are experimental, and the first theoretical analysis for distinguishers of Chacha on the notion of neutral bits was given by Dey and Sarkar (2020). Recently, the same authors have presented a theoretical analysis on distinguishers of Chacha 256 bits on the notion of differential cryptanalysis (Dey and Sarkar, 2021).

1.1 Contribution

Motivated by the work of Dey and Sarkar (2020, 2021), we have theoretically analysed Chacha 128 up to four rounds and have mathematically computed the biases. We have considered two matrices W and W' each of size 16 words. These matrices W and W' are the same and they differ at only the 18th bit of 15th word. Chacha round functions are applied on these matrices individually up to four rounds. After four rounds, we have computed the probability that these two matrices are the same at a particular bit (bias). The biases observed in round four are as in Table 1. The observed theoretical results are on par with the experimental results.

Table 1 Biases in round 4

Bias probability	*Theoretical result*	*Experimental result*
$\lambda_1^{4a}[19]$	0.9688	0.9669
$\lambda_{16}^{4a}[3]$	0.9688	0.9677
$\lambda_1^{4b}[19]$	0.914	0.9158
$\lambda_{16}^{4b}[9]$	0.875	0.8771

1.2 Paper outline

The paper is organised as follows – preliminaries about Chacha and differential attack in Section 2, general probability results in Section 3, theoretical analysis of Chacha 128 with mathematical proof in Section 4, experimental and theoretical result comparison in Section 5, related work in Section 6 and conclusions in Section 7.

2 Preliminaries

2.1 Chacha

Chacha has a structure similar to that of Salsa with the only difference between them being the core function. Chacha takes a 64 byte input consisting of 16 words, each of size 4 bytes. The 16 words are split into 8 words of key, $\{k_1, k_2, ..., k_8\}$, four words of IV, $\{IV_1, IV_2, IV_3, IV_4\}$, and four constant words, $\{c_1, c_2, c_3, c_4\}$. The Chacha version of being it 128 bits or 256 bits depends on the key type that is chosen. The eight keywords add up to 256 bits and if the initial key is 128 bits, it is to be be padded to itself to make it 256, bits i.e., the keys K_5, K_6, K_7, K_8 are same as K_1, K_2, K_3, K_4 respectively. The words of Chacha are denoted as,

$$\mathrm{W} = \begin{pmatrix} W_1 & W_2 & W_3 & W_4 \\ W_5 & W_6 & W_7 & W_8 \\ W_9 & W_{10} & W_{11} & W_{12} \\ W_{13} & W_{14} & W_{15} & W_{16} \end{pmatrix}$$

$$= \begin{pmatrix} C_0 & C_1 & C_2 & C_3 \\ K_1 & K_2 & K_3 & K_4 \\ K_1 & K_2 & K_3 & K_4 \\ t_0 & t_1 & v_0 & v_1 \end{pmatrix}$$

These words are processed in columns and diagonals. In odd numbered rounds, the columns are processed and in the even numbered rounds, the diagonals are processed. In processing each column and diagonal, a function called 'quarterround' function is employed. The quarterround, column round and diagonal round are denoted as follows.

2.1.1 Quarterround

The quarterround takes a 4-word sequence as input and outputs a 4-word sequence. If $W = (W_1, W_2, W_3, W_4)$ is the input to the quarterround, then quarterround (W) is defined as,

$$\begin{aligned} W_1 &= W_1 + W_2; & W_4 &= ((W_4 \oplus W_1) \lll 16) \\ W_3 &= W_3 + W_4; & W_2 &= ((W_2 \oplus W_3) \lll 12) \\ W_1 &= W_1 + W_2; & W_4 &= ((W_4 \oplus W_1) \lll 8) \\ W_3 &= W_3 + W_4; & W_2 &= ((W_2 \oplus W_3) \lll 7) \end{aligned}$$

2.1.2 Columnround

Let the input to the column round function be $W = (W_1, W_2, ..., W_{16})$. The column round for the 16-word Chacha matrix is defined as,

$$\begin{aligned} (S_1, S_5, S_9, S_{13}) &= quarterround(W_1, W_5, W_9, W_{13}) \\ (S_2, S_6, S_{10}, S_{14}) &= quarterround(W_2, W_6, W_{10}, W_{14}) \\ (S_3, S_7, S_{11}, S_{15}) &= quarterround(W_3, W_7, W_{11}, W_{15}) \\ (S_4, S_8, S_{12}, S_{16}) &= quarterround(W_4, W_8, W_{12}, W_{16}) \end{aligned}$$

2.1.3 Diagonalround

Let the input to the diagonal round function be $W = (W_1, W_2, ..., W_{16})$. The diagonal round for the 16-word Chacha matrix is defined as,

$$\begin{aligned} (S_1, S_6, S_{11}, S_{16}) &= quarterround(W_1, W_6, W_{11}, W_{16}) \\ (S_2, S_7, S_{12}, S_{13}) &= quarterround(W_2, W_7, W_{12}, W_{13}) \\ (S_3, S_8, S_9, S_{14}) &= quarterround(W_3, W_8, W_9, W_{14}) \\ (S_4, S_5, S_{10}, S_{15}) &= quarterround(W_4, W_5, W_{10}, W_{15}) \end{aligned}$$

2.2 Differential attack

Differential attack is a technique that involves changing one or more bits of the input and observing its effect on the output. The changes in the input are traced, which aids in the identification of distinguishers for specific rounds. This is commonly referred to as a chosen-plaintext attack. The attacker has access to the public value of the input, i.e., the IV is accessible to the adversary. A theoretical analysis of a differential attack on Chacha 128 is presented in this study. The following is the concept of the analysis: Two 16-word sequences, W and W', are used, with W' differing by one bit from W. Each word is made up of 32 bits, numbered 0 to 31. In the fifteenth word of W', the difference is presented at the 18th bit. This means that when W and W' are XORed, the result will have only the 18th bit of the 15th word as 1. Both these word sequences are subjected to the Chacha round functions and the differences are traced. W and W' are compared after a specified number of rounds. This method is repeated for different random inputs. We compared 2^{21} random inputs in this study. The probabilities of the outputs' similarity are compared and analysed. If the probability is more than 0.5, the output is regarded distinguishable, and thus proving the non-randomness of the cipher. In general, differential attacks observe changes in the ciphertext which occurred due to changes in the plaintext and thereby obtain a distinguisher. This distinguisher is further exploited to recover the key or the plaintext.

Differential attack using multiple bit differences in the plaintext can also be performed. Multiple bit changes in the plaintext will lead to higher diffusion in the ciphertext, thereby making it difficult to trace the changes in the ciphertext.

3 Probabilistic results

3.1 Basic notations

The following are the notations used in this paper,

1 W_i denotes a word with number i

2 $W_i[n]$ indicates n^{th} bit of W_i

3 $W_i^r[n]$ indicates n^{th} bit of W_i at round r

4 $Pr[E]$ denotes the probability of occurrence of an event E

5 let $\lambda_w[n] = Pr(W[n] = W'[n])$ denote the event that n^{th} bit of W and W' are equal

6 let $\bar{\lambda}_w[n] = Pr(W[n] \neq W'[n])$ denote the event that n^{th} bit of W and W' are different

7 let $\Phi(W[n], k)$ denote the event that for any pair of words (W, W'), the bits from n to k are complemented exactly

8 let $\bar{\Phi}(W[n], k)$ denote the event that for any pair of words (W, W'), the bits from n to k are complemented at the least.

3.2 Proved results

Herewith we have stated a lemma and two theorems which will be used in Chacha analysis.

Lemma 1: Let X and Y be two independently chosen random 32 bit numbers. Let Y' be a 32 bit number that differs exactly at one bit position (let it be n) as to Y. Consider $Z = X + Y \mod 2^{32}$ and $Z' = X + Y' \mod 2^{32}$. Now, for any $k \geq 0$ such that $n + k \leq 31$, the probability that Z and Z' differ at $(n+k)^{\text{th}}$ bit is $\frac{1}{2^k}$.

The proof of this Lemma is available in Dey and Sarkar (2017).

Theorem 1: Let X and Y be two independently chosen random single bit numbers. Let X' and Y' be two single bit numbers such that $Pr(X = X') = p$ and $Pr(Y = Y') = q$. Let $Z = X + Y$ and $Z' = X' + Y'$. Then the probability that $Pr(Z = Z')$ is given as

$$pq + (1-p)(1-q) \text{ if } c = c'$$
$$p(1-q) + q(1-p) \text{ if } c \neq c'$$

where c is the carry generated in word Z and c' is the carry generated in word Z'.

Theorem 2: Let X and Y be two independently chosen random $n-bit$ numbers. Let X' and Y' be two $n-bit$ numbers such that $Pr(X[n] = X'[n]) = p_i$ and $Pr(Y[n] = Y'[n]) = q_i$ for $0 \leq n \leq 31$. Let $c[n]$ be the carry generated at position n in $Z = X + Y$ and $c'[n]$ be the carry generated at position n in $Z' = X' + Y'$. Then,

$$Pr\left(c_{i+1} \neq c'_{i+1}\right) = Pr\left(c_i \neq c'_i\right) \cdot \left(1 - p - q + \frac{3pq}{2}\right) + Pr\left(c_i = c'_i\right) \frac{(1-pq)}{2}$$

Theorems 1 and 2 are proved in Dey and Sarkar (2020).

4 Theoretical analysis of Chacha 128

The input to Chacha 128 is 16 words where eight words are key bits, four words are IVs and four words are constant values. To make a 8-word (256 bits) keystream, the 4-word (128 bits) keystream is added to itself. Consider two input matrices $W = (W_1, W_2, ..., W_{16})$ and $W' = (W'_1, W'_2, ..., W'_{16})$. Here the matrices W and W' are same and they only differ at the 18th bit of 15th word. The difference is given at 18th bit of the fifteenth word and the biases are observed up-to four rounds of Chacha 128. In Chacha quarterrounds, each word is updated twice. Therefore, for ease of understanding, here in this paper we denote the first update as 'a' and the second update as 'b'. Example, consider the word W_1 is subjected to two quarterround updates in round 2. The output of first update is denoted as W_1^{2a} and the output of second update is denoted as W_1^{2b}.

4.1 Observations of round 1

The Chacha core function is applied to the input matrices W and W', where there is a single bit difference between the two matrices at the 18th bit of the 15th word. Round 1 is done in a column-by-column fashion. Because there is a change in column 3 (15th word), the differences can only be seen in that column. The first, second, and fourth columns have not been changed. The following are the changed words in column 3 at the end of round 1:

- The first quarterround of column 3 is,

  $$W_3'^{1a} = W_3'^0 + W_7'^0; W_{15}'^{1a} = (W_{15}'^0 \oplus W_3'^{1a}) \lll 16$$

  The initial difference set up at bit position 18 of $W_{15}'^0$ will reflect in bit position 2 of $W_{15}'^{1a}$ after XOR and left rotation by 16 bits. Thus, at the end of the first quarterround, $W_{15}'^{1a}[2]$ has a change.

- The second quarterround of column 3 is,

  $$W_{11}'^{1a} = W_{11}'^0 + W_{15}'^{1a}; W_7'^{1a} = (W_7'^0 \oplus W_{11}'^{1a}) \lll 12$$

  The change in bit position $W_{15}'^{1a}[2]$ will cause a change in $W_{11}'^{1a}[2]$ after the addition. This change will further reflect in $W_7'^{1a}[14]$ after the XOR and 12-bit left rotation. Thus, at the end of second quarterround, the changes are at $W_{11}'^{1a}[2]$ and $W_7'^{1a}[14]$.

- The third quarterround of column 3 is,

  $$W_3'^{1b} = W_3'^{1a} + W_7'^{1a}; W_{15}'^{1b} = (W_{15}'^{1a} \oplus W_3'^{1b}) \lll 8$$

  The change in bit position $W_7'^{1a}[14]$ causes a change in $W_3'^{1b}[14]$ after the addition. The difference at $W_3'^{1b}[14]$, along with the difference in $W_{15}'^{1a}[2]$ will reflect in $W_{15}'^{1b}[22]$ and $W_{15}'^{1b}[10]$ respectively after the XOR and 8-bit left rotation. At the end of this quarterround, the changes are at $W_3'^{1b}[14]$, $W_{15}'^{1b}[10]$ and $W_{15}'^{1b}[22]$.

- The fourth quarterround of column 3 is,

  $$W_{11}'^{1b} = W_{11}'^{1a} + W_{15}'^{1b}; W_7'^{1b} = (W_7'^{1a} \oplus W_{11}'^{1b}) \lll 7$$

  The changes in $W_{11}'^{1a}[2]$, $W_{15}'^{1b}[10]$ and $W_{15}'^{1b}[22]$ causes a change in $W_{11}'^{1b}[2]$, $W_{11}'^{1b}[10]$ and $W_{11}'^{1b}[22]$ respectively after the addition. These changes will reflect in $W_7'^{1b}[21]$, $W_7'^{1b}[9]$, $W_7'^{1b}[17]$ and $W_7'^{1b}[29]$ correspondingly after the XOR and 7-bit left rotation.

  At the end of round 1, the changes are at $W_3'^{1b}[14]$, $W_7'^{1b}[9]$, $W_7'^{1b}[17]$, $W_7'^{1b}[21]$, $W_7'^{1b}[29]$, $W_{11}'^{1b}[2]$, $W_{11}'^{1b}[10]$, $W_{11}'^{1b}[22]$, $W_{15}'^{1b}[10]$ and $W_{15}'^{1b}[22]$.

4.2 Observations of round 2

Theorem 3: In the first and second quarterround of diagonal 1,

1 $Pr(W_1^{2a} = W_1'^{2a}) = 1$

2 $Pr(W_{16}^{2a} = W_{16}'^{2a}) = 1$

3 $Pr(W_{11}^{2a}[2, 10, 22] = W_{11}'^{2a}[2, 10, 22]) = 0$

4 $Pr(W_6^{2a}[2, 14, 22] = W_6'^{2a}[2, 14, 22]) = 0.$

Proof: The first quarterround of diagonal 1 is,

$$W_1'^{2a} = W_1'^1 + W_6'^1; W_{16}'^{2a} = (W_{16}'^1 \oplus W_1'^{2a}) \lll 16$$

Parts 1, 2: The words involved in this quarterround did not exhibit any change at the end of round 1 and as a result $Pr(W_1^{2a} = W_1'^{2a}) = 1$ and $Pr(W_{16}^{2a} = W_{16}'^{2a}) = 1$.

The second quarterround of diagonal 1 is,

$$W_{11}'^{2a} = W_{11}'^{1b} + W_{16}'^{2a}; W_6'^{2a} = (W_6'^1 \oplus W_{11}'^{2a}) \lll 12$$

Parts 3, 4: The changes in bit positions 2, 10 and 22 of $W_{11}'^{1b}$ will cause a difference in the same bit positions of $W_{11}'^{2a}$ after the addition. Thus, $Pr(W_{11}^{2a}[2, 10, 22] = W_{11}'^{2a}[2, 10, 22]) = 0$. The differences at $W_{11}'^{2a}[2, 10, 22]$ will reflect in bit positions 14, 22 and 2 of $W_6'^{2a}$ respectively. Therefore, $Pr(W_6^{2a}[2, 14, 22] = W_6'^{2a}[2, 14, 22]) = 0$. □

Theorem 4: At the end of third quarterround of diagonal 1,

1 $Pr(W_1^{2b}[2, 14, 22] = W_1'^{2b}[2, 14, 22]) = 0$

2 $Pr(W_1^{2b}[0, 1] = W_1'^{2b}[0, 1]) = 1$

3 $Pr(W_{16}^{2b}[10, 22, 30] = W_{16}'^{2b}[10, 22, 30]) = 0$

4 $Pr(W_{16}^{2b}[8, 9] = W_{16}'^{2b}[8, 9]) = 1.$

Proof: The third quarterround of diagonal 1 is,

$$W_1'^{2b} = W_1'^{2a} + W_6'^{2a}; W_{16}'^{2b} = (W_{16}'^{2a} \oplus W_1'^{2b}) \lll 8$$

Parts 1, 2: There is a change in bits 2, 14 and 22 of $W_6'^{2a}$ (from Theorem 3) and there are no changes in $W_1'^{2a}$ (from Theorem 3). The changes are received by bits 2, 14 and 22 of $W_1'^{2b}$ after the addition. Thus, $Pr(W_1^{2b}[2, 14, 22] = W_1'^{2b}[2, 14, 22]) = 0$. During addition, the changes in bits 2, 14 and 22 may propagate to the left with probability $\frac{1}{2^k}$ according to Lemma 1. This implies that there could be a change in bits 3 to 13, 15 to 21 and 23 to 31. The only bits that are unchanged are 0 and 1. Thus $Pr(W_1^{2b}[0, 1] = W_1'^{2b}[0, 1]) = 1$.

Parts 3, 4: During XOR operation, the changes in bits 2, 14 and 22 of $W_1'^{2b}$ are reflected in bits 2, 14 and 22 of the XOR output. When the XOR output is subjected to 8-bit left rotation, the changes are moved to bit positions 10, 22 and 30, respectively. Therefore, $Pr(W_{16}^{2b}[10, 22, 30] = W_{16}'^{2b}[10, 22, 30]) = 0$. The unchanged bits 0,1 in $W_1'^{2b}$ will move to bit positions 8 and 9. Therefore, $Pr(W_{16}^{2b}[8, 9] = W_{16}'^{2b}[8, 9]) = 1$. □

Theorem 5: At the end of fourth quarterround of diagonal 1,

1 $Pr(W_{11}^{2b}[10, 22] = W_{11}'^{2b}[10, 22]) = 1$

2 $Pr(W_{11}^{2b}[2, 30] = W_{11}'^{2b}[2, 30]) = 0$

3 $Pr(W_6^{2b}[9] = W_6'^{2b}[9]) = 1$

4 $Pr(W_6^{2b}[5, 21, 29] = W_6'^{2b}[5, 21, 29]) = 0$

Proof: The fourth quarterround of diagonal 1 is,

$$W_{11}'^{2b} = W_{11}'^{2a} + W_{16}'^{2b}; W_6'^{2b} = (W_6'^{2a} \oplus W_{11}'^{2b}) \lll 7$$

Parts 1, 2: There are changes in bits 2, 10 and 22 of $W_{11}'^{2a}$ (from Theorem 3) and in bits 10, 22 and 30 of $W_{16}'^{2b}$ (from Theorem 4). It could be observed that bits 10 and 22 of both the operands in the addition have change. When these are added, the bit values in positions 10 and 22 of $W_{11}'^{2b}$ will be same as that of W_{11}^{2b}. Therefore, $Pr(W_{11}^{2b}[10, 22] = W_{11}'^{2b}[10, 22]) = 1$. The changes in remaining bits $W_{11}'^{2a}[2]$ and $W_{16}'^{2b}[30]$ will be reflected in bits 2 and 30 of W_{11}^{2b}. Thus, $Pr(W_{11}^{2b}[2, 30] = W_{11}'^{2b}[2, 30]) = 0$.

Parts 3, 4: There are changes in bits 2, 14 and 22 of $W_6'^{2a}$ (from Theorem 3) and in bits 2 and 30 of $W_{11}'^{2b}$. It could be observed that bit 2 of both the operands in the XOR operation have change. When these are XORed, the bit value in position 2 of XOR output in W' will be same as that of XOR output of W. This result is received by bit 9 of $W'^{2b}[9]$ after 7-bit left rotation. Therefore, $Pr(W_6^{2b}[9] = W_6'^{2b}[9]) = 1$. The changes in remaining bits 14, 22 and 30 of the XOR output will be reflected in bits 21, 29 and 5 of W_6^{2b} respectively. Thus, $Pr(W_6^{2b}[5, 21, 29] = W_6'^{2b}[5, 21, 29]) = 0$. □

Theorem 6: At the end of first quarterround of diagonal 2,

1 $Pr(W_2^{2a}[9, 7, 21, 29] = W_2'^{2a}[9, 7, 21, 29]) = 0$

2 $Pr(W_2^{2a}[0 - 8] = W_2'^{2a}[0 - 8]) = 1$

3 $Pr(W_{13}^{2a}[5, 13, 25, 26] = W_{13}'^{2a}[5, 13, 25, 26]) = 0$

4 $Pr(W_{13}^{2a}[16 - 24] = W_{13}'^{2a}[16 - 24]) = 1$

Proof: The first quarterround of diagonal 2 is,

$$W_2'^{2a} = W_2'^1 + W_7'^1; W_{13}'^{2a} = (W_{13}'^1 \oplus W_2'^{2a}) \lll 16$$

Parts 1, 2: at the end of round 1, $W_7'^1$ had changes in bit positions 9, 17, 21 and 29. These changes, after the addition is received by bits 9, 17, 21 and 29 of $W_2'^{2a}$. Therefore, $Pr(W_2^{2a}[9, 7, 21, 29] = W_2'^{2a}[9, 7, 21, 29]) = 0$. After addition, the change in bit 9, 17, 21 and 29 may propagate to the left with probability $\frac{1}{2^k}$ according to Lemma 1. This implies that there could be a change in bits 10 to 16, 18 to 20 , 22 to 28 and 30, 31 respectively. The unaltered bits are 0 to 8. Thus, $Pr(W_2^{2a}[0 - 8] = W_2'^{2a}[0 - 8]) = 1$.

Parts 3, 4: After the XOR of $W_{13}'^1$ and $W_2'^{2a}$, the changes in bits 9, 17, 21 and 29 of $W_2'^{2a}$ will reflect in the XOR result and will move to bit positions 25, 26, 5 and 13 respectively after 16-bit left rotation. This makes $Pr(W_{13}^{2a}[5, 13, 25, 26] = W_{13}'^{2a}[5, 13, 25, 26]) = 0$. The unaltered bits 0 to 8 of $W_2'^{2a}$ will move to bit positions 16 to 24 after 16-bit left rotation. Therefore, $Pr(W_{13}^{2a}[16 - 24] = W_{13}'^{2a}[16 - 24]) = 0$. □

Theorem 7: At the end of second quarterround of diagonal 2,

1 $Pr(W_{12}^{2a}[5, 13, 25, 26] = W_{12}'^{2a}[5, 13, 25, 26]) = 0$

2 $\lambda_7^{2a}[21] = 0.0625$

3 $\lambda_7^{2a}[29] = 0.0625$

4 $\lambda_7^{2a}[9] = 0.125$

5 $Pr(W_7^{2a}[1,5,6,17,25] = W_7'^{2a}[1,5,6,17,25]) = 0.$

Proof: The second quarterround of diagonal 2 is,

$$W_{12}'^{2a} = W_{12}'^{1} + W_{13}'^{2a}; W_7'^{2a} = (W_7'^{1} \oplus W_{12}'^{2a}) \lll 12$$

Part 1: From Theorem 6, we have changes in bit positions 5, 13, 25 and 26 of $W_{13}'^{2a}$. After addition with $W_{12}'^{1}$ (no changes so far), these changes reflect in bit positions 5, 13, 25 and 26 of $W_{12}'^{2a}$. These changes may propagate to the left with probability $\frac{1}{2^k}$ according to Lemma 1. Therefore, $Pr(W_{12}^{2a}[5,13,25,26] = W_{12}'^{2a}[5,13,25,26]) = 0$.

Parts 2–5: From round 1 we have changes in bit positions 9, 17, 21 and 29 of $W_7'^{1}$ and from previous proof, we have changes in bit positions 5, 13, 25 and 26 of $W_{12}'^{2a}$. Also, it is known that there may be changes in bits 6 to 12, 14 to 24 and 27 to 31 of $W_{12}'^{2a}$ (Lemma 1). From this, we have,

$$\bar{\lambda}_{12}^{2a}[9] = \frac{1}{2^{(9-5)}} = 0.0625$$

This implies, $\lambda_{12}^{2a}[9] = 1 - 0.0625 = 0.9375$ and let $p = 0.9375$. Also, we know $\lambda_7^1[9] = 0$ and let $q = 0$. By applying Theorem 1,

$$\lambda_{XOR}[9] = pq + (1-p)(1-q) = 0.0625$$

This result, after the 12-bit left rotation, is received by bit 21 of $W_7'^{2a}$. Thus, $\lambda_7^{2a}[21] = 0.0625$. Similarly, it can be proved for $\lambda_7^{2a}[29] = 0.0625$ and $\lambda_7^{2a}[9] = 0.125$. The remaining changes in bits 5, 13, 25 and 26 of $W_{12}'^{2a}$ and bit 21 of $W_7'^{1}$ are shifted to bit positions 17, 25, 5, 6 and 1 respectively. Thus, $Pr(W_7^{2a}[1,5,6,17,25] = W_7'^{2a}[1,5,6,17,25]) = 0$. □

Theorem 8: In the third quarterround of diagonal 2,

1 $\lambda_2^{2b}[9] = 0.875$

2 $\lambda_2^{2b}[21] = 0.9375$

3 $\lambda_2^{2b}[29] = 0.9375$

4 $Pr(W_2^{2b}[1,5,6,7,17,25] = W_2'^{2b}[1,5,6,7,17,25]) = 0$

Proof: The addition part in third quarterround of diagonal 2 is,

$$W_2'^{2b} = W_2'^{2a} + W_7'^{2a}$$

From Theorem 7, we have $\lambda_7^{2a}[21] = 0.0625$, $\lambda_7^{2a}[29] = 0.0625$ and $\lambda_7^{2a}[9] = 0.125$. Let these values be p_{21}, p_{29} and p_9 respectively. From Theorem 6, we have $\lambda_2^{2a}[21] = 0$, $\lambda_2^{2a}[29] = 0$ and $\lambda_2^{2a}[9] = 0$. Let these values be q_{21}, q_{29} and q_9 respectively. Applying Theorem 1,

$$\lambda_{Sum}[21] = p_{21}q_{21} + (1-p_{21})(1-q_{21}) = 0.9375$$

This result applies to 21st bit of $W_2'^{2b}$. Therefore, $\lambda_2^{2b}[21] = 0.9375$. Similarly it can be proved for $\lambda_2^{2b}[29] = 0.9375$ and $\lambda_2^{2b}[9] = 0.875$. The remaining changes in bit positions 1, 5, 6, 17, 25 of $W_7'^{2a}$ (from Theorem 7) and bit 7 of $W_2'^{2a}$ (from Theorem 6) are received by bits 1, 5, 6, 7, 17 and 25 of $W_2'^{2b}$. Thus, $Pr(W_2^{2b}[1,5,6,7,17,25] = W_2'^{2b}[1,5,6,7,17,25]) = 0$. □

Theorem 9: At the end of third quarterround of diagonal 2,

1 $Pr(W_{13}^{2b}[13] = W_{13}'^{2b}[13]) = 1$

2 $Pr(W_{13}^{2b}[1] = W_{13}'^{2b}[1]) = 1$

3 $\lambda_{13}^{2b}[17] = 0.875$

4 $\lambda_{13}^{2b}[29] = 0.9375$

5 $\lambda_{13}^{2b}[5] = 0.9375$

6 $Pr(W_{13}^{2b}[2,9,14,15,21,25] = W_{13}'^{2b}[2,9,14,15,21,25]) = 0$

Proof: The XOR and left rotation part in third quarterround of diagonal 2 is,

$$W_{13}'^{2b} = (W_{13}'^{2a} \oplus W_2'^{2b}) \lll 8$$

Parts 1, 2: There are changes in bit positions 5 and 25 of $W_{13}'^{2a}$ and $W_2'^{2b}$ from Theorems 6 and 8, respectively. This implies that, in the XOR of $W_{13}'^{2a}$ and $W_2'^{2b}$, the bits 5 and 25 differ in both the operands. When both the operands have change in the same bit, the result of W' will be same as that of W in this operation. This result, when rotated in left by 8 bits, will move to bit positions 13 and 1 respectively. Thus, $Pr(W_{13}^{2b}[13] = W_{13}'^{2b}[13]) = 1$ and $Pr(W_{13}^{2b}[1] = W_{13}'^{2b}[1]) = 1$.

Parts 3–5: From Theorem 8, we have $\lambda_2^{2b}[9] = 0.875$, $\lambda_2^{2b}[21] = 0.9375$ and $\lambda_2^{2b}[29] = 0.9375$. This result in $W_2'^{2b}$, after the XOR with $W_{13}'^{2a}$(No change in bits 9, 21 and 29), will reflect in bits 9, 21 and 29 of the XOR result. After 8-bit left rotation, these get shifted to positions 17, 29 and 5 respectively. Therefore, $\lambda_{13}^{2b}[17] = 0.875$, $\lambda_{13}^{2b}[29] = 0.9375$ and $\lambda_{13}^{2b}[5] = 0.9375$.

Part 6: There are changes in bit positions 1, 6, 7 and 17 of $W_2'^{2b}$ (from Theorem 8) and 13, 26 of $W_{13}'^{2a}$ (from Theorem 6). These changes after XOR and 8-bit left rotation, reflect in the bit positions 9, 14, 15, 25, 21 and 2 of $W_{13}'^{2b}$ respectively. Thus, $Pr(W_{13}^{2b}[2,9,14,15,21,25] = W_{13}'^{2b}[2,9,14,15,21,25]) = 0$. □

Theorem 10: In the fourth quarterround of diagonal 2,

1 $Pr(W_{12}^{2b}[25] = W_{12}'^{2b}[25]) = 1$

2 $\lambda_{12}^{2b}[5] = 0.0625$

3 $\lambda_{12}^{2b}[17] = 0.875$

4 $\lambda_{12}^{2b}[29] = 0.9375$

5 $Pr(W_{12}^{2b}[2,9,13,14,15,21,26] = W_{12}'^{2b}[2,9,13,14,15,21,26]) = 0$

Proof: The addition part in fourth quarterround of diagonal 2 is,

$$W'^{2b}_{12} = W'^{2a}_{12} + W'^{2b}_{13}$$

Part 1: There is a change in bit position 25 of both W'^{2a}_{12} and W'^{2b}_{13} from Theorem 7 and Theorem 9 respectively. Change in same bit position of both the operands in addition will produce a result in W' that is same as that of W. Therefore, $Pr(W^{2b}_{12}[25] = W'^{2b}_{12}[25]) = 1$.

Parts 2–4: From Theorem 7, we have $\lambda^{2a}_{12}[5] = 0$. So let $p = 0$. From Theorem 9, we have $\lambda^{2b}_{13}[5] = 0.9375$. Let this be $q = 0.9375$. Applying Theorem 1,

$$\lambda_{Sum}[5] = pq + (1-p)(1-q) = 0.0625$$

This result reflects in 5th bit of W'^{2b}_{12}. Thus, $\lambda^{2b}_{12}[5] = 0.0625$. From Theorem 9, we have $\lambda^{2b}_{13}[17] = 0.875$ and $\lambda^{2b}_{13}[29] = 0.9375$. This reflects in the 17th and 29th bit of W'^{2b}_{12}. Therefore, $\lambda^{2b}_{12}[17] = 0.875$ and $\lambda^{2b}_{12}[29] = 0.9375$.

Part 5: There are changes in bit positions 2, 9, 14, 15 and 21 in W'^{2b}_{13} (from Theorem 9) and changes in bit positions 13 and 26 in W'^{2a}_{12} (from Theorem 7). These reflect in bit positions 2, 9, 13, 14, 15, 21 and 26 of W'^{2b}_{12}. Thus, $Pr(W^{2b}_{12}[2, 9, 13, 14, 15, 21, 26] = W'^{2b}_{12}[2, 9, 13, 14, 15, 21, 26]) = 0$. □

Theorem 11: At the end of fourth quarterround of diagonal 2,

1 $\lambda^{2b}_{7}[12] = 0.9375$
2 $\lambda^{2b}_{7}[16] = 0.875$
3 $\lambda^{2b}_{7}[28] = 0.9375$
4 $\lambda^{2b}_{7}[4] = 0.1171$
5 $\lambda^{2b}_{7}[24] = 0.125$
6 $Pr(W^{2b}_{7}[0, 1, 8, 9, 13, 20, 21, 22] = W'^{2b}_{7}[0, 1, 8, 9, 13, 20, 21, 22]) = 0.$

Proof: The XOR and left rotation part in third quarterround of diagonal 2 is,

$$W'^{2b}_{7} = (W'^{2a}_{7} \oplus W'^{2b}_{12}) \lll 7$$

Parts 1–5: From Theorem 7, we have $\lambda^{2a}_{7}[5] = 0$ and from Theorem 10 we have $\lambda^{2a}_{12}[5] = 0.0625$. Let these values be denoted as $p = 0$ and $q = 0.0625$. Applying Theorem 1,

$$\lambda_{XOR}[5] = pq + (1-p)(1-q) = 0.9375$$

This result is received by bit 12 of W'^{2b}_{7} after 7-bit left rotation. Therefore, $\lambda^{2b}_{7}[12] = 0.9375$.

From Theorem 7, we have $\lambda^{2a}_{7}[9] = 0.125$ and from Theorem 10, we have $\lambda^{2a}_{12}[9] = 0$. Let these values be denoted as $p = 0.125$ and $q = 0$. Applying Theorem 1,

$$\lambda_{XOR}[9] = pq + (1-p)(1-q) = 0.875$$

This result is received by bit 16 of W'^{2b}_{7} after 7-bit left rotation. Thus, $\lambda^{2b}_{7}[16] = 0.875$. Similarly it can be proved for other parts.

Part 6: From Theorem 7, we have changes in bits 1, 6, 25 of W'^{2a}_{7} and from Theorem 10 we have changes in bits 2, 13, 14, 15, 26 of W'^{2b}_{12}. These changes, after XOR and 7-bit left rotation, shifts to bit positions 8, 13, 0 and 9, 20, 21, 22, 1 respectively. Thus, $Pr(W^{2b}_{7}[0, 1, 8, 9, 13, 20, 21, 22] = W'^{2b}_{7}[0, 1, 8, 9, 13, 20, 21, 22]) = 0$. □

Theorem 12: At the end of first quarterround of diagonal 3,

1 $Pr(W^{2a}_{3}[14] = W'^{2a}_{3}[14]) = 0$
2 $Pr[\Phi(W'^{2a}_{3}[14 + k])] = \frac{1}{2^k}$ for $1 \leq k \leq 17$
3 $\lambda^{2a}_{3}[18] = 0.9375$
4 $\lambda^{2a}_{3}[19] = 0.9688$
5 $\lambda^{2a}_{3}[20] = 0.9844$
6 $Pr(W^{2a}_{14}[30] = W'^{2a}_{14}[30]) = 0$
7 $\lambda^{2a}_{14}[2] = 0.9375$
8 $\lambda^{2a}_{14}[3] = 0.9688$
9 $\lambda^{2a}_{14}[4] = 0.9844.$

Proof: The first quarterround of diagonal 3 is,

$$W'^{2a}_{3} = W'^{1}_{3} + W'^{1}_{8}; W'2a_{14} = (W'^{1}_{14} \oplus W'^{2a}_{3}) \lll 16$$

Parts 1, 2: At the end of round 1 , there was a change at bit position 14 of W'^{1}_{3} and there was no change in W'^{1}_{8}. During addition of W'^{1}_{3} and W'^{1}_{8}, the change in $W'^{1}_{3}[14]$ will reflect in the 14th bit of the addition result and it may propagate to the left with probability $\frac{1}{2^k}$ (Lemma 1).

Parts 3–5: Using the above result, we have,

$$\bar{\lambda}^{2a}_{3}[18] = \frac{1}{2^{(18-14)}} = 0.0625$$

Therefore, $\lambda^{2a}_{3}[18] = 1 - 0.0625 = 0.9375$

$$\bar{\lambda}^{2a}_{3}[19] = \frac{1}{2^{(19-14)}} = 0.0312$$

Therefore, $\lambda^{2a}_{3}[19] = 1 - 0.0312 = 0.9688$

$$\bar{\lambda}^{2a}_{3}[20] = \frac{1}{2^{(20-14)}} = 0.0156$$

Therefore, $\lambda^{2a}_{3}[20] = 1 - 0.0156 = 0.9844$

Parts 6–9: The changes in bits 14, 18, 19 and 20 of W'^{2a}_{3} will reflect in the XOR result and will move to bit positions 30, 2, 3 and 4 of W'^{2a}_{14} respectively. □

Theorem 13: At the end of second quarterround of diagonal 3,

1 $\lambda_9^{2a}[4] = 0.9763$

2 $Pr(W_9^{2a}[30] = W_9'^{2a}[30]) = 0$

3 $\lambda_8^{2a}[16] = 0.9763$

4 $Pr(W_8^{2a}[10] = W_8'^{2a}[10]) = 0$

Proof: The second quarterround of diagonal 3 is,

$$W_9'^{2a} = W_9'^1 + W_{14}'^{2a}; W_8'^{2a} = (W_8'^1 \oplus W_9'^{2a}) \lll 12$$

Part 1: From Theorem 12, we have $\lambda_{14}^{2a}[2] = 0.9375$, $\lambda_{14}^{2a}[3] = 0.9688$ and $\lambda_{14}^{2a}[4] = 0.9844$. Let these values be denoted as, $p_2 = 0.9375$, $p_3 = 0.9688$ and $p_4 = 0.9844$. There are no changes observed so far in bits 2, 3 and 4 of $W_9'^1$. Therefore, $\lambda_9^1[2] = 1$, $\lambda_9^1[3] = 1$and $\lambda_9^1[4] = 1$. Let these values be denotes as $q_2 = 1$, $q_3 = 1$ and $q_4 = 1$. During addition of $W_9'^1$ and $W_{14}'^{2a}$, we consider only the bits 2, 3, 4 and ignore the carry generated from the previous bit 1. Therefore, $Pr(c[2] = c'[2]) = 1$. Using Theorem 2, compute $Pr(c[3] = c'[3])$ as,

$$\begin{aligned} Pr(c[3] = c'[3]) &= 1 - Pr(c[2] \neq c'[2]) \\ &= 1 - 0.0156 = 0.9844 \end{aligned}$$

Similarly,

$$\begin{aligned} Pr(c[4] = c'[4]) &= 1 - Pr(c[3] \neq c'[3]) \\ &= 1 - 0.0083 = 0.9917 \\ Pr(c[4] \neq c'[4]) &= 0.0083 \end{aligned}$$

Let $Sum[4] = W_9^1[4] + W_{14}^{2a}[4]$ and $Sum'[4] = W_9'^1[4] + W_{14}'^{2a}[4]$. Now,

$$\begin{aligned} \lambda_{Sum}[4] &= Pr(Sum[4] = Sum'[4]) \\ &= Pr(c[4] = c'[4]) \\ &\quad Pr((Sum[4] = Sum'[4])|(c[4] = c'[4])) \\ &\quad + Pr(c[4] \neq c'[4]) \\ &\quad Pr((Sum[4] = Sum'[4])|(c[4] \neq c'[4])) \end{aligned}$$

Using Theorem 1, we can find $Pr((Sum[4] = Sum'[4])|(c[4] = c'[4])) = 0.9844$ and $Pr((Sum[4] = Sum'[4])| \ (c[4] \neq c'[4])) = 0.0156$. Substituting these values to find $\lambda_{Sum}[4] = Pr(Sum[4] = Sum'[4])$, we get $\lambda_{Sum}[4] = 0.9763$. This will reflect in the 4th bit of $W_9'^{2a}$. Thus, $\lambda_9^{2a}[4] = 0.9763$.

Part 2: The change in 30th bit of $W_{14}'^{2a}$ will reflect in $W_9'^{2a}$ after the addition. Thus, $Pr(W_9^{2a}[30] = W_9'^{2a}[30]) = 0$.

Parts 3 ,4: The change in 4th and 30th bit of $W_9'^{2a}$ will reflect in bit positions 16 and 10 of $W_8'^{2a}$ respectively. □

Theorem 14: In the third quarterround of diagonal 3,

1 $Pr(W_3^{2b}[10, 14] = W_3'^{2b}[10, 14]) = 0$

2 $\lambda_3^{2b}[18] = 0.9375$

3 $\lambda_3^{2b}[19] = 0.9688$

4 $\lambda_3^{2b}[20] = 0.9844$

5 $\lambda_3^{2b}[16] = 0.7381$

Proof: The addition part of third quarterround of diagonal 3 is,

$$W_3'^{2b} = W_3'^{2a} + W_8'^{2a}$$

Part 1: From Theorems 12 and 13, we know that bits 14 and 10 of $W_3'^{2a}$ and $W_8'^{2a}$ change respectively. These changes reflect in bit positions 10 and 14 of the addition result.

Parts 2–4: From Theorem 12, we have $\lambda_3^{2a}[18] = 0.9375$, $\lambda_3^{2a}[19] = 0.9688$ and $\lambda_3^{2a}[20] = 0.9844$. These reflect in the addition result at the same bit positions.

Part 5: From Theorem 13, we have $\lambda_8^{2a}[16] = 0.9763$. Let this value be denoted as $p = 0.9763$. When $W_3'^{2a}$ and $W_8'^{2a}$ are added, the change in $W_3'^{2a}[14]$ may propagate to the left with probability $\frac{1}{2^k}$. Therefore,

$$\bar{\lambda}_3^{2b}[16] = \frac{1}{2^{(16-14)}} = 0.25$$

This implies,

$$\lambda_3^{2b} = 1 - \bar{\lambda}_3^{2b} = 0.75$$

Let this value be denoted as $q = 0.75$. Applying Theorem 1,

$$\lambda_3^{2b}[16] = pq + (1-p)(1-q) = 0.7381$$

□

Theorem 15: At the end of third quarterround of diagonal 3,

1 $Pr(W_{14}^{2b}[6, 18, 22] = W_{14}'^{2b}[6, 18, 22]) = 0$

2 $\lambda_{14}^{2b}[10] = 0.9375$

3 $\lambda_{14}^{2b}[11] = 0.9688$

4 $\lambda_{14}^{2b}[12] = 0.9844$

5 $\lambda_{14}^{2b}[24] = 0.7381$

6 $\lambda_{14}^{2b}[26] = 0.9375$

7 $\lambda_{14}^{2b}[27] = 0.9688$

8 $\lambda_{14}^{2b}[28] = 0.9844.$

Proof: The XOR and shift part in the third quarterround of diagonal 3 is,

$$W_{14}'^{2b} = (W_{14}'^{2a} \oplus W_{13}'^{2b}) \lll 8$$

There are changes in bit 30 of $W_{14}'^{2a}$ (from Theorem 12) and in bits 10 and 14 of $W_{13}'^{2b}$ (from Theorem 14). These changes, after the XOR and 8-bit left rotation, move to

bit positions 6, 18 and 22 respectively. The result of bit positions 2, 3 and 4 in $W_{14}^{\prime 2a}$ (from Theorem 12) move to bit positions 10, 11 and 12 of $W_{14}^{\prime 2b}$ respectively after XOR and 8-bit left rotation. The result in bit positions 16, 18, 19, 20 in $W_{13}^{\prime 2b}$ (from Theorem 14) move to bit positions 24, 26, 27, 28 respectively after XOR and 8-bit left rotation. □

Theorem 16: In the fourth quarterround of diagonal 3,

1 $Pr(W_9^{2b}[6,8,22,30] = W_9^{\prime 2b}[6,8,22,30]) = 0$
2 $\lambda_9^{2b}[4] = 0.9763$
3 $\lambda_9^{2b}[10] = 0.9375$
4 $\lambda_9^{2b}[11] = 0.9688$
5 $\lambda_9^{2b}[12] = 0.9844$
6 $\lambda_9^{2b}[24] = 0.7381$
7 $\lambda_9^{2b}[26] = 0.9375$
8 $\lambda_9^{2b}[27] = 0.9688$
9 $\lambda_9^{2b}[28] = 0.9844.$

Proof: The addition part in fourth quarterround of diagonal 3 is,

$$W_9^{\prime 2b} = W_9^{\prime 2a} + W_{14}^{\prime 2b}$$

There are changes in bit position 30 of $W_9^{\prime 2a}$ (from Theorem 13) and in bit positions 6, 8 and 22 of $W_{14}^{\prime 2b}$ (from Theorem 15). These will reflect in bit positions 6, 8, 22 and 30 of $W_9^{\prime 2b}$. The results of bit position 4 in $W_9^{\prime 2a}$ (from Theorem 13) and bit positions 10 to 12, 24, 26 to 28 in $W_{14}^{\prime 2b}$ (from Theorem 15) will be received by same bit positions of $W_9^{\prime 2b}$. □

Theorem 17: At the end of fourth quarterround of diagonal 3,

1 $Pr(W_8^{2b}[5,13,15,29] = W_8^{\prime 2b}[5,13,15,29]) = 0$
2 $\lambda_8^{2b}[11] = 0.9763$
3 $\lambda_8^{2b}[18] = 0.9688$
4 $\lambda_8^{2b}[19] = 0.9844$
5 $\lambda_8^{2b}[23] = 0.9763$
6 $\lambda_8^{2b}[31] = 0.7381$
7 $\lambda_8^{2b}[1] = 0.9375$
8 $\lambda_8^{2b}[2] = 0.9688$
9 $\lambda_8^{2b}[3] = 0.9844$
10 $\lambda_8^{2b}[17] = 0.0625$

Proof: The XOR and left shift part in fourth quarterround of diagonal 3 is,

$$W_8^{\prime 2b} = (W_8^{\prime 2a} \oplus W_9^{\prime 2b}) \lll 7$$

There are changes in bit positions 6, 8, 22 and 30 of $W_9^{\prime 2b}$ (from Theorem 16). These changes move to bit positions 13, 15, 29 and 5 of $W_8^{\prime 2b}$ respectively after XOR and 7-bit left rotation. The result of bit 16 in $W_8^{\prime 2a}$ (from Theorem 13) moves to bit position 23 of $W_8^{\prime 2b}$. Similarly the results of bit positions 4, 11, 12, 24, 26, 27, 28 of $W_9^{\prime 2b}$ (from Theorem 16) moves to bit positions 11, 18, 19, 31, 1, 2, 3 of $W_8^{\prime 2b}$ respectively.

From Theorem 13, we have $\lambda_8^{2a}[10] = 0$ and from Theorem 16, we have $\lambda_9^{2b}[10] = 0.9375$. Let these values be $p = 0$ and $q = 0.9375$. Applying Theorem 1,

$$\lambda_8^{2b}[10] = pq + (1-p)(1-q) = 0.0625$$

□

Theorem 18: In the first quarterround of diagonal 4,

1 $Pr(W_4^{2a} = W_4^{\prime 2a}) = 1$
2 $Pr(W_{15}^{2a}[6,16] = W_{15}^{\prime 2a}[6,16]) = 0.$

Proof: The first quarterround of diagonal 4 is,

$$W_4^{\prime 2a} = W_4^{\prime 1} + W_5^{\prime 1}; W_{15}^{\prime 2a} = (W_{15}^{\prime 1} \oplus W_4^{\prime 2a}) \lll 16$$

From round 1 results, we know that there are no changes in the words $W_4^{\prime 1}$ and $W_5^{\prime 1}$. Therefore, there are no changes in W and W' after the addition part. Thus, $Pr(W_4^{2a} = W_4^{\prime 2a}) = 1$. From round 1, there were changes in bits 10 and 22 of $W_{15}^{\prime 1}$. This change, after the XOR with $W_4^{\prime 2a}$ and rotation by 16 bits, reflects in the bit positions 16 and 6 respectively of the output. Therefore, $Pr(W_{15}^{2a}[6,16] = W_{15}^{\prime 2a}[6,16]) = 0$. □

Theorem 19: In the second quarterround of diagonal 4,

1 $Pr(W_{10}^{2a}[6,16] = W_{10}^{\prime 2a}[6,16]) = 0$
2 $Pr(W_{10}^{2a}[0-5] = W_{10}^{\prime 2a}[0-5]) = 1$
3 $Pr(W_5^{2a}[8,18] = W_5^{\prime 2a}[8,18]) = 0$
4 $Pr(W_5^{2a}[7-12] = W_5^{\prime 2a}[7-12]) = 1.$

Proof: The second quarterround of diagonal 4 is,

$$W_{10}^{\prime 2a} = W_{10}^{\prime 1} + W_{15}^{\prime 2a}; W_5^{\prime 2a} = (W_5^{\prime 1} \oplus W_{10}^{\prime 2a}) \lll 12$$

From Theorem 18, it is evident that there are changes in bit positions 6 and 16 of $W_{15}^{\prime 2a}$. Also, from results of round 1 we know that there are no changes in $W_{10}^{\prime 1}$. After the addition of $W_{10}^{\prime 1}$ and $W_{15}^{\prime 2a}$, changes are reflected in bit positions 6 and 16 of $W_{10}^{\prime 2a}$. Therefore, $Pr(W_{10}^{2a}[6,16] = W_{10}^{\prime 2a}[6,16]) = 0$. These changes may propagate to their left with probability $\frac{1}{2^\kappa}$ (according to Lemma 1). The bits that are unchanged after the addition are in positions 0 to 5. Thus, $Pr(W_{10}^{2a}[0-5] = W_{10}^{\prime 2a}[0-5]) = 1$. The changes in bits 6 and 16 of $W_{10}^{\prime 2a}$ reflects in bit positions 18 and 28 respectively after the XOR and 12-bit left rotation. Therefore, $Pr(W_5^{2a}[8,18] = W_5^{\prime 2a}[8,18]) = 0$. The unchanged bits in bit positions 0 to 5 of $W_{10}^{\prime 2a}$ are unchanged after the XOR with $W_5^{\prime 1}$ and 12-bit left rotation. Thus, $Pr(W_5^{2a}[7-12] = W_5^{\prime 2a}[7-12]) = 1$. □

4.3 Observations of round 3

Theorem 20: At the end of first quarterround of column 1,

1 $Pr(W_1^{3a}[2,14,22] = W_1'^{3a}[2,14,22]) = 0$

2 $Pr(W_{13}^{3a}[18,30] = W_{13}'^{3a}[18,30]) = 1$

3 $Pr(W_{13}^{3a}[5,6,9,25,31] = W_{13}'^{3a}[5,6,9,25,31]) = 0$

4 $\lambda_{13}^{3a}[1] = 0.875$

5 $\lambda_{13}^{3a}[13] = 0.9375$

6 $\lambda_{13}^{3a}[21] = 0.9375$

Proof: The first quarterround of column 1 is,

$$W_1'^{3a} = W_1'^{2b} + W_5'^{2b}; W_{13}'^{3a} = (W_{13}'^{2b} \oplus W_1'^{3a}) \lll 16$$

Part 1: From Theorem 4 we know that there are changes in bit positions 2, 14 and 22 of $W_1'^{2b}$. These changes reflect in the same bit positions of $W_1'^{3a}$ after the addition.

Parts 2–6: There are changes in bit positions 9, 15, 21 and 25 of $W_{13}'^{2b}$ (from Theorem 9) and bit 22 of $W_1'^{3a}$ (from part 1 of this theorem). These changes, after the XOR and 16-bit left rotation, moves to bit positions 25, 31, 5, 9 and 6 of $W_{13}'^{3a}$ respectively. Also, from Theorem 9 and part 1 result of this theorem, it is evident that the bits at positions 2 and 14 of both $W_{13}'^{2b}$ and $W_1'^{3a}$ have changes. These, when XORed and left shifted by 16 bits, will produce result at bits 18 and 30 that is same as the result in W. Therefore, $Pr(W_{13}^{3a}[18,30] = W_{13}'^{3a}[18,30]) = 1$. From Theorem 9, we have results for bit positions 17, 29 and 5 of $W_{13}'^{2b}$. These results will apply to bit positions 21,1 and 13 of $W_{13}'^{3a}$ respectively. □

Theorem 21: At the end of third quarterround of column 1,

1 $Pr(W_1^{3b}[2,14,22] = W_1'^{3b}[2,14,22]) = 0$

2 $Pr(W_{13}^{3b}[1,7,10,13,14,17,22,30] = W_{13}'^{3b}[1,7,10,13,14,17,22,30]) = 0$

3 $\lambda_{13}^{3b}[9] = 0.875$

4 $\lambda_{13}^{3b}[21] = 0.9375$

5 $\lambda_{13}^{3b}[29] = 0.9375$

Proof: The third quarterround of column 1 is,

$$W_1'^{3b} = W_1'^{3a} + W_5'^{3b}; W_{13}'^{3b} = (W_{13}'^{3a} \oplus W_1'^{3b}) \lll 8$$

Part 1: From Theorem 20, we know that there are changes in bit positions 2, 14 and 22 of $W_1'^{3a}$. These reflect in the same bit positions of $W_1'^{3b}$ after the addition.

Part 2: From part 1, we have changes in bit positions 2, 14 and 22 of $W_1'^{3b}$. Also, from Theorem 20, we have changes in bit positions 5, 6, 9, 25 and 31 of $W_{13}'^{3a}$. These changes, after the XOR of $W_{13}'^{3a}$ and $W_1'^{3b}$ and 8-bit left rotation, reflect in bit positions 10, 22, 30, 13, 14, 17, 1 and 7 respectively.

Parts 3–5: The results of bits 1, 13 and 21 of $W_{13}'^{3a}$ (from Theorem 20) will reflect in bit positions 9, 21 and 29 of $W_{13}'^{3b}$ respectively after the XOR and 8-bit left rotation. □

4.4 Observations of round 4

Theorem 22: At the end of first quarterround of diagonal 1,

1 $Pr(W_1^{4a}[2,14,22] = W_1'^{4a}[2,14,22]) = 0$

2 $\lambda_1^{4a}[17] = 0.875$

3 $\lambda_1^{4a}[18] = 0.9375$

4 $\lambda_1^{4a}[19] = 0.9688$

5 $Pr(W_{16}^{4a}[6,18,30] = W_{16}'^{4a}[6,18,30]) = 0$

6 $\lambda_{16}^{4a}[1] = 0.875$

7 $\lambda_{16}^{4a}[2] = 0.9375$

8 $\lambda_{16}^{4a}[3] = 0.9688$

Proof: The first quarterround of diagonal 1 is,

$$W_1'^{4a} = W_1'^{3b} + W_6'^{3b}; W_{16}'^{4a} = (W_{16}'^{3b} \oplus W_1'^{4a}) \lll 16$$

Parts 1–4: From Theorem 21, we know that bits 2, 14 and 22 of $W_1'^{3b}$ have difference. This difference is received by the same bit positions of $W_1'^{4a}$ during addition. After the addition, the changes in the mentioned bit positions may propagate to the left with probability $\frac{1}{2^k}$ (Lemma 1). This implies,

$$\bar{\lambda}_1^{4a}[17] = \frac{1}{2^{(17-14)}} = 0.125$$

Therefore, $\lambda_1^{4a}[17] = 1 - 0.125 = 0.875$

$$\bar{\lambda}_1^{4a}[18] = \frac{1}{2^{(18-14)}} = 0.0625$$

Therefore, $\lambda_1^{4a}[18] = 1 - 0.0625 = 0.9375$

$$\bar{\lambda}_1^{4a}[19] = \frac{1}{2^{(19-14)}} = 0.0312$$

Therefore, $\lambda_1^{4a}[19] = 1 - 0.0312 = 0.9688$.

Parts 5–8: During the XOR and left rotation by 16 bits, the changes observed in part 1 will shift to bit positions 18, 30 and 6 of $W_{16}'^{4a}$ respectively. Also, the results of bits 17, 18 and 19 of $W_1'^{4a}$ will apply to bit positions 1, 2 and 3 respectively after XOR and 16-bit left rotation. □

Theorem 23: At the end of third quarterround of diagonal 1,

1 $Pr(W_1^{4b}[2,14,22] = W_1'^{4b}[2,14,22]) = 0$

2 $\lambda_1^{4b}[19] = 0.914$

3 $Pr(W_{16}^{4b}[6,14,22,26,30] = W_{16}'^{4b}[6,14,22,26,30]) = 0$

4 $\lambda_{16}^{4b}[9] = 0.875$

5 $\lambda_{16}^{4b}[11] = 0.9375$

6 $\lambda_{16}^{4b}[27] = 0.914$

7 $\lambda_{16}^{4b}[10] = 0.0625$.

Proof: The third quarterround of diagonal 1 is,

$$W_1'^{4b} = W_1'^{4a} + W_6'^{4a}; W_{16}'^{4b} = (W_{16}'^{4a} \oplus W_1'^{4b}) \lll 8$$

Part 1: There is difference in bit positions 2, 14 and 22 of $W_1'^{4a}$ (from Theorem 22). These differences are received by same bit positions of $W_1'^{4b}$ after the addition.

Part 2: From Theorem 22, we have $\lambda_1^{4a}[17] = 0.875$, $\lambda_1^{4a}[18] = 0.9375$ and $\lambda_1^{4a}[19] = 0.9688$. Let these values be denoted as $p_{17} = 0.875$, $p_{18} = 0.9375$ and $p_{19} = 0.9688$. Assuming that there are no differences in the same bit positions of $W_6'^{4a}$, let $q_{17} = 1$, $q_{18} = 1$ and $q_{19} = 1$. During the addition of $W_1'^{4a}$ and $W_6'^{4a}$, we consider only the bits 17, 18, 19 and ignore the carry generated from the previous bit 16. Therefore, $Pr(c[17] = c'[17]) = 1$. Using Theorem 2, compute $Pr(c[18] = c'[18])$ as,

$$\begin{aligned} Pr(c[18] = c'[18]) &= 1 - Pr(c[17] \neq c'[17]) \\ &= 1 - 0.0625 = 0.9375 \end{aligned}$$

Similarly,

$$\begin{aligned} Pr(c[19] = c'[19]) &= 1 - Pr(c[18] \neq c'[18]) \\ &= 1 - 0.0584 = 0.9416 \\ Pr(c[19] \neq c'[19]) &= 0.0584 \end{aligned}$$

Let $Sum[19] = W_1^{4a}[19] + W_6^{4a}[19]$ and $Sum'[19] = W_1'^{4a}[19] + W_6'^{4a}[19]$. Now,

$$\begin{aligned} \lambda_{Sum}[19] &= Pr(Sum[19] = Sum'[19]) \\ &= Pr(c[19] = c'[19]) \\ &\quad Pr((Sum[19] = Sum'[19])|(c[19] = c'[19])) \\ &\quad + Pr(c[19] \neq c'[19]) \\ &\quad Pr((Sum[19] = Sum'[19])|(c[19] \neq c'[19])) \end{aligned}$$

Using Theorem 1, we can find $Pr((Sum[19] = Sum'[19])|(c[19] = c'[19])) = 0.9688$ and $Pr((Sum[19] = Sum'[19])|\ (c[19] \neq c'[19])) = 0.0312$. Substituting these values to find $\lambda_{Sum}[19] = Pr(Sum[19] = Sum'[19])$, we get $\lambda_{Sum}[19] = 0.914$. This will reflect in the 19th bit of $W_1'^{4b}$. Thus, $\lambda_1^{4b}[19] = 0.914$.

Part 3: There is difference in bit positions 14 and 22 of $W_1'^{4b}$ (from part 1). Also, there are differences at bit positions 6, 18 and 30 of $W_{16}'^{4a}$ (from Theorem 22). These changes are received by bit positions 22, 30, 14, 26, 6 of $W_{16}'^{4b}$ respectively after XOR and 8-bit left rotation.

Parts 4–6: There are results for bit positions 1,3 of $W_{16}'^{4a}$ (from Theorem 22) and result for bit 19 of $W_1'^{4b}$ (from part 2). These are received by bit positions 9, 11 and 27 of $W_{16}'^{4b}$ respectively.

Part 7: From Theorem 22, we have $\lambda_{16}^{4a}[2] = 0.9375$. Also, from part 1 of this theorem we have $\lambda_1^{4b}[2] = 0$. Let these values be denoted as $p = 0.9375$ and $q = 0$. Applying Theorem 1,

$$\lambda_{XOR}^{4b}[2] = pq + (1-p)(1-q) = 0.0625$$

This result moves to bit position 10 of $W_{16}'^{4b}$ after 8-bit left rotation. Thus, $\lambda_{16}^{4b}[10] = 0.0625$. □

5 Theoretical and experimental result comparison

We have compared the theoretical results obtained in this work with the experimental results. In Section 4, we have theoretically analysed Chacha 128 with probability. The theoretical results are compared with the experimental results. For experimental verification, we took random combinations of IVs and applied Chacha round function to it. Also, for the same set of random combinations with one bit input difference, we applied Chacha round function and observed the output differences at each round. The probabilities of the output difference at the end of every round were computed. The experiments were conducted with 2^{21} random sets of IVs and the results were computed using probabilistic methods. We have depicted the results of each bit of the words up-to 4 decimal digits. The comparative results are shown in Table 2. Table 2 shows that the theoretical analysis is on par with the experimental results. The theoretical analysis was performed up to four rounds in this work. For higher rounds, the diffusion was more and therefore it was increasingly difficult to track the changes.

Table 2 Theoretical and experimental result comparison

Bias probability	*Theoretical result*	*Experimental result*
$\lambda_7^{2a}[9]$	0.125	0.129
$\lambda_2^{2b}[9]$	0.875	0.881
$\lambda_{13}^{2b}[29]$	0.9375	0.9481
$\lambda_{12}^{2b}[5]$	0.0625	0.0684
$\lambda_7^{2b}[4]$	0.1171	0.1189
$\lambda_3^{2a}[19]$	0.9688	0.9701
$\lambda_{14}^{2a}[4]$	0.9844	0.9840
$\lambda_9^{2a}[4]$	0.9763	0.9757
$\lambda_8^{2a}[16]$	0.9763	0.9759
$\lambda_3^{2b}[16]$	0.7381	0.7596
$\lambda_{14}^{2b}[27]$	0.9688	0.9523
$\lambda_9^{2b}[28]$	0.9844	0.9838
$\lambda_8^{2b}[17]$	0.0625	0.0649
$\lambda_{13}^{3a}[13]$	0.9375	0.9395

Table 2 Theoretical and experimental result comparison (continued)

Bias probability	*Theoretical result*	*Experimental result*
$\lambda_{13}^{3b}[9]$	0.875	0.8774
$\lambda_{1}^{4a}[19]$	0.9688	0.9669
$\lambda_{16}^{4a}[3]$	0.9688	0.9677
$\lambda_{1}^{4b}[19]$	0.914	0.9158
$\lambda_{16}^{4b}[9]$	0.875	0.8771

6 Related work

To the best of our knowledge, the first ever attack on Chacha was done by Aumasson et al. (2008). Their attack is inspired by correlation analysis and the notion of neutral bits. The idea is to perform a single bit differential cryptanalysis and to observe the correlation in the output bits. The authors have attacked a 6- and 7-round Chacha. Later Ishiguro et al. (2011), improved the single bit differential cryptanalysis by Aumasson et al. (2008) to a double bit differential cryptanalysis and have attacked a 8-round Chacha. In Shi et al. (2012), a new distinguisher called chaining distinguisher was used to recover the key from Chacha. Maitra (2016) proposed chosen IV cryptanalysis on Chacha which is claimed to be better than the previous attacks. Later, Choudhuri and Maitra (2016), for the first time, showed how to choose output bit combinations theoretically to improve biases in Chacha. In Dey and Sarkar (2017), the authors presented an algorithm to probabilistically construct neutral bits which can be further exploited to find distinguishers. Improved cryptanalytic techniques were suggested by Deepthi and Singh (2017, 2019). In CRYPTO 2020, Beierle et al. (2020) have recovered key bits in 6-round Chacha with time complexity $2^{77.4}$ and 7-round Chacha with time complexity $2^{230.86}$.

Some more distinguishing attacks on literature include probabilistic neutral bits (PNB)-based attack, chaining distinguishers, impact of differential attack on add, rotate, XOR (ARX) operations and chosen IV attack. The differential characteristics in ARX operations and its application in stream cipher salsa was given by Mouha and Preneel (2013). Distinguishing attacks by choosing optimal parameters were introduced by Maitra et al. (2015).

7 Conclusions

Chacha is a lightweight stream cipher used by Google and in cloud computing for transport layer security and internet security respectively. In this work, we have theoretically analysed the differential attack on Chacha stream cipher. Most of the cryptanalytic works in literature are focused on experimental analysis. Very few are done in a theoretical aspect. Theoretical analysis of differential attacks helps in identifying the reason for biases in the cipher. Also, theoretical analysis of an attack provides an insight into designing a cipher that resists the attacks. We have theoretically analysed 128 bit Chacha and have recorded the biases caused by differences in input using probability. We have mathematically proved the biases up-to 4 rounds of Chacha 128 and have compared it with experimental results. This proves that, the stream cipher 128-bit Chacha has observable biases up to round 4 and that thereby it has a distinguisher in round 4. The theoretical results are confirmed with the experimental results. In future, this mathematical analysis can be extended to further rounds to theorise in the light of the existing experimental results.

References

Aumasson, J-P., Fischer, S., Khazaei, S., Meier, W. and Rechberger, C. (2008) 'New features of Latin dances: analysis of Salsa, ChaCha, and Rumba', *International Workshop on Fast Software Encryption*, pp.470–488.

Beierle, C., Leander, G. and Todo, Y. (2020) 'Improved differential-linear attacks with applications to ARX ciphers', *Annual International Cryptology Conference*, pp.329–358.

Bernstein, D.J. (2008) 'ChaCha, a variant of Salsa20', *Workshop Record of SASC*, Vol. 8, pp.3–5

Choudhuri, A.R. and Maitra, S. (2016) 'Significantly improved multi-bit differentials for reduced round Salsa and ChaCha', *IACR Transactions on Symmetric Cryptology*, pp.261–287.

Deepthi, K.K.C. and Singh, K. (2017) 'Cryptanalysis of Salsa and ChaCha: revisited', *International Conference on Mobile Networks and Management*, pp.324–338.

Deepthi, K.K.C. and Singh, K. (2019) 'Cryptanalysis for reduced round Salsa and ChaCha: revisited', *IET Information Security*, Vol. 13, No. 6, pp.591–602.

Dey, S. and Sarkar, S. (2017) 'Improved analysis for reduced round Salsa and Chacha', *Discrete Applied Mathematics*, Vol. 227, pp.58–69.

Dey, S. and Sarkar, S. (2020) 'Proving the biases of Salsa and ChaCha in differential attack', *Designs, Codes and Cryptography*, Vol. 88, No. 9, pp.1827–1856.

Dey, S. and Sarkar, S. (2021) 'A theoretical investigation on the distinguishers of Salsa and ChaCha', *Discrete Applied Mathematics*, Vol. 302, pp.147–162.

Ishiguro, T., Kiyomoto, S. and Miyake, Y. (2011) 'Latin dances revisited: new analytic results of Salsa20 and ChaCha', *International Conference on Information and Communications Security*, pp.255–266.

Maitra, S. (2016) 'Chosen IV cryptanalysis on reduced round ChaCha and Salsa', *Discrete Applied Mathematics*, Vol. 208, pp.88–97.

Maitra, S., Paul, G. and Meier, W. (2015) 'Salsa20 cryptanalysis: new moves and revisiting old styles', *International Workshop on Coding and Cryptography, WCC2015*.

Mouha, N. and Preneel, B. (2013) *Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20*, Cryptology ePrint Archive, Report 2013/328.

Shi, Z., Zhang, B., Feng, D. and Wu, W.(2012) 'Improved key recovery attacks on reduced-round Salsa20 and ChaCha', *International Conference on Information Security and Cryptology*, pp.337–351.