Cryptanalysis of Reduced Round ChaCha – New Attack & Deeper Analysis[1]

Fast Software Encryption - 2023, Beijing, China

Sabyasachi Dey[1], **Hirendra Kumar Garai[1]**, Subhamoy Maitra[2]

[1]Department of Mathematics, BITS Pilani, Hyderabad Campus, Hyderabad, 500078, India,

[2]Applied Statistics Unit, Indian Statistical Institute, Kolkata, 700108, India

[1]Dey, S., Garai, H. K., Maitra, S. (2023). Cryptanalysis of Reduced Round ChaCha – New Attack Deeper Analysis. IACR Transactions on Symmetric Cryptology, 2023(1), 89–110. https://doi.org/10.46586/tosc.v2023.i1.89-110

20 March 2023

Introduction

- Symmetric cipher is of two types :
  1. Block cipher - A block of plaintext is encrypted at a time.
  2. Stream cipher - Key-stream generated from a key is XORed with plaintext in encryption.
- ARX is a popular design scheme. Easy to implement and fast performance.
- FEAL (1970) was the first cipher that used ARX scheme.
- **ChaCha** is a stream cipher that uses ARX design (2008).

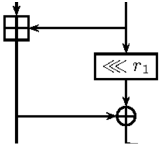


Figure: ARX design

Structure of ChaCha (Keystream generation algorithm)

- *Output*: 512-bit key-stream.
- Key stream generation algorithm takes a 256-bit **Key (k)**, 128-bit **Constant(c)**, and 128-bit **Initial vectors (v, t) / attacker controlled inputs**.
- They are stored in the following matrix form:

$$X = \begin{pmatrix} X_0 & X_1 & X_2 & X_3 \\ X_4 & X_5 & X_6 & X_7 \\ X_8 & X_9 & X_{10} & X_{11} \\ X_{12} & X_{13} & X_{14} & X_{15} \end{pmatrix}_{4\times 4} = \begin{pmatrix} constant & constant & constant & constant \\ key & key & key & key \\ key & key & key & key \\ input & input & input & input \end{pmatrix}_{4\times 4}$$

ChaCha *Round* function

- **ChaCha** *round* functions invertibly transforms the state X through 20 rounds.
- Each **ChaCha** *round* is constructed with following *ARX* functions which updates vector (a, b, c, d) to (a'', b'', c'', d'') :

$$
\begin{aligned}
a' &= a \boxplus b; & d' &= ((d \oplus a') \lll 16); \\
c' &= c \boxplus d'; & b' &= ((b \oplus c') \lll 12); \\
a'' &= a' \boxplus b'; & d'' &= ((d' \oplus a'') \lll 8); \\
c'' &= c' \boxplus d''; & b'' &= ((b' \oplus c'') \lll 7);
\end{aligned}
\tag{1}
$$

- In odd numbered rounds the **column** vectors of X are updated:

$$\begin{pmatrix} x_0 \\ x_4 \\ x_8 \\ x_{12} \end{pmatrix}, \begin{pmatrix} x_1 \\ x_5 \\ x_9 \\ x_{13} \end{pmatrix}, \begin{pmatrix} x_2 \\ x_6 \\ x_{10} \\ x_{14} \end{pmatrix}, \begin{pmatrix} x_3 \\ x_7 \\ x_{11} \\ x_{15} \end{pmatrix}$$

- In even numbered rounds the **diagonal** vectors of X are updated:

$$\begin{pmatrix} x_0 \\ x_5 \\ x_{10} \\ x_{15} \end{pmatrix}, \begin{pmatrix} x_1 \\ x_6 \\ x_{11} \\ x_{12} \end{pmatrix}, \begin{pmatrix} x_2 \\ x_7 \\ x_8 \\ x_{13} \end{pmatrix}, \begin{pmatrix} x_3 \\ x_4 \\ x_9 \\ x_{14} \end{pmatrix}$$

- The final keystream Z is given by:

$$Z = X \boxplus X^{(20)},$$

  $X^{(20)}$ is the state after 20 **ChaCha** rounds.

- In **ChaCha** cipher, one can reverse back from round r to round $r-1$ by reversing the ARX operations.

Attacks on ChaCha

- Type of cryptanalysis : Mostly of differential-linear. A single differential $(\mathcal{ID}, \mathcal{OD})$ is used.
- One of the prominent attack technique: *Probabilistic Neutral Bits* (PNB's) based attack[2].
- [3]The claimed complexity of most successful attack before our attack on **6 round ChaCha**: $2^{104.68}$.

[2] J.-P. Aumasson, S. Fischer, S. Khazaei, W. Meier, and C. Rechberger. New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba. Fast Software Encryption 2008

[3] M. Coutinho and T. C. S. Neto. New Multi-bit Differentials to Improve Attacks Against ChaCha. IACR Cryptol. ePrint Arch., page 350, 2020. https: //eprint.iacr.org/2020/350.

Correction of the complexity formula

- The formula to compute complexity was given by Aumasson et. al:

$$2^m \cdot N + 2^{k-\alpha}, \text{ where } m \text{ is very very bigger than } \alpha \quad (2)$$

The updated form is given by Dey et. al[4]:

$$2^m \cdot N + 2^{k-\alpha} + 2^{k-m} \quad (3)$$

k = Total number of key-bits, m = Number of non-PNBs, $2^{-\alpha}$ = False alarm probability. N = Data complexity.

- Using the existing attacks, the runtime complexity can not go below $2^{k/2}$.

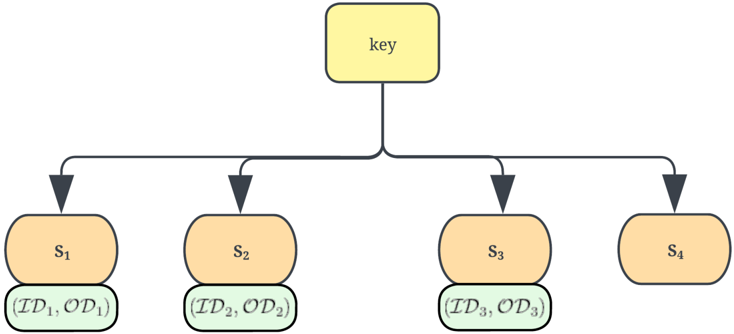
[4] S. Dey, H. K. Garai, S. Sarkar, and N. K. Sharma. Revamped Differential-Linear Cryptanalysis on Reduced Round ChaCha. Advances in Cryptology - EUROCRYPT 2022

Updated complexities of the existing attacks

Attack	# PNB	Complexity	
		Claimed	Actual
[1]	147	2^{139}	2^{147}
[4]	136	2^{136}	2^{139}
[2]	159	$2^{131.40}$	2^{159}
[2]	161	$2^{129.53}$	2^{161}
[2]	166	$2^{127.5}$	2^{166}
[3]	210	$2^{102.2}$	2^{210}
[3]	212	$2^{104.68}$	2^{212}

Table: Corrected complexities of certain previous key-recovery attacks on 6-round ChaCha and our improved result.

Multiple $(\mathcal{ID}, \mathcal{OD})$ approach:
Preprocessing stage:



Data collection:

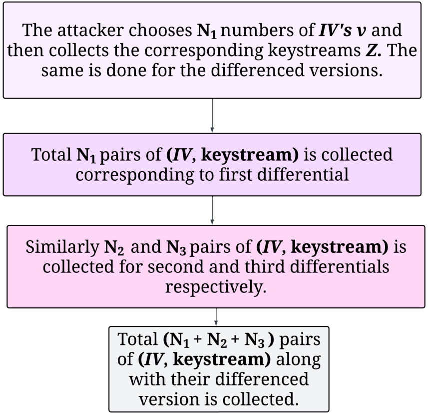


Figure: Data collection

Key recovery:

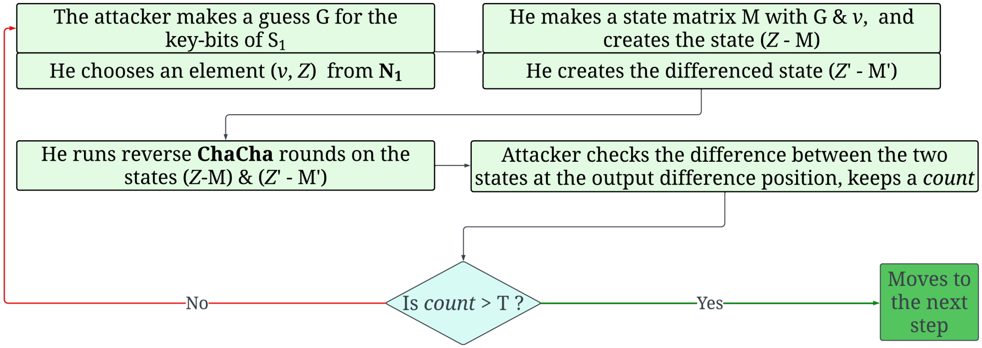


Figure: S_1 recovery

- Now he has the correct values for the $|S_1|$ key-bits. Leaving those key bits as it is, he searches $|S_2|$ key bits as similar as before.
- After getting the key-bits of S_2 correct he recovers the key-bits of S_3 similarly.
- Lastly the $|S_4|$ key-bits are searched exhaustively.

Complexity of our attack

$(\mathcal{ID}, \mathcal{OD})$	Key-bits that are not PNB	Data
$((12, 6), (1, 0))$	$58(S_1)$	$2^{41.67}(N_1)$
$((13, 6), (2, 0))$	$56(S_2)$	$2^{34.26}(N_2)$
$((14, 6), (3, 0))$	$50(S_3)$	$2^{30.32}(N_3)$

Here $|S_4| = 92$.
The runtime complexity formula for this attack is

$$2^{|S_1|} \cdot N_1 + 2^{|S_2|} \cdot N_2 + 2^{|S_3|} \cdot N_3 + 2^{|S_4|} \tag{4}$$

which after putting the value becomes $\approx 2^{99.48} < 2^{256/2}$.

Why ToyChaCha ?

- The complexity formula, success probability uses many statistical assumption which is not experimentally verified.
- The attacks on the original **ChaCha** cipher is impossible to demonstrate till date.

Structure of cipher

- The 128-bit input to the Toy**ChaCha** is arranged in 4×4 matrix, where each entry is of 8-bit.
- The Toy**ChaCha** uses a 64-bit key.
- The *round* function is accordingly adjusted.

Results on ToyChaCha

Parameter	Attack of Aumasson et. al		Attack of Maitra	
	Theory	Experiment	Theory	Experiment
Data	378	378	185	185
Complexity for significant bits	$2^{24.56}$	$2^{23.56}$	$2^{24.53}$	$2^{23.47}$
False alarm Complexity	2^{21}	$2^{18.18}$	2^{21}	$2^{17.59}$
Complexity for PNBs	2^{16}	$2^{15.01}$	2^{15}	$2^{13.99}$
Total Complexity	$2^{24.67}$	$2^{23.60}$	$2^{24.65}$	$2^{23.50}$
Success probability	$\geqslant 0.50$	0.9981	$\geqslant 0.50$	0.9971
Pr_{fa}	$\leqslant 0.00049$	0.00034	$\leqslant 0.00049$	0.00015

Table: Comparison of theoretical claim and experimental results of the implemented attack on 3.5 round Toy**ChaCha**

Multiple $(\mathcal{ID}, \mathcal{OD})$ attack on ToyChaCha

Complexity	Single $(\mathcal{ID}, \mathcal{OD})$			Multiple $(\mathcal{ID}, \mathcal{OD})$	
	Theory (Aumasson et. al)	Theory (Dey et. al)	Experiment	Theory	Experiment
Data	95	95	95	94	94
Recover S_1	$2^{14.56}$	$2^{14.56}$	$2^{13.51}$	$2^{14.56}$	$2^{13.51}$
Recover S_2	-	-	-	$2^{14.56}$	$2^{13.51}$
Recover S_3	-	-	-	$2^{14.56}$	$2^{13.5}$
False alarm	2^{-8}	2^{-8}	0	0	0
Recover PNB	0	2^{24}	$2^{23.01}$	2^{8}	$2^{6.95}$
Total	$2^{14.56}$	2^{24}	$2^{23.01}$	$2^{16.15}$	$2^{15.1}$

Table: Comparison of theory and experiments for 3-round attack using multiple $(\mathcal{ID}, \mathcal{OD})$ and single $(\mathcal{ID}, \mathcal{OD})$

Reference

[1] J. Aumasson, S. Fischer, S. Khazaei, W. Meier, and C. Rechberger.

New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba.

Fast Software Encryption, 15th International Workshop, Lausanne, Switzerland, Revised Selected Papers, 5086:470–488, 2008.

https://doi.org/10.1007/978-3-540-71039-4_30.

[2] A. R. Choudhuri and S. Maitra.

Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha.

IACR Trans. Symmetric Cryptol., 2016(2):261–287, 2016.

https://doi.org/10.13154/tosc.v2016.i2.261-287.

[3] M. Coutinho and T. C. S. Neto.

New Multi-bit Differentials to Improve Attacks Against ChaCha.

IACR Cryptol. ePrint Arch., page 350, 2020.

https://eprint.iacr.org/2020/350.

[4] Z. Shi, B. Zhang, D. Feng, and W. Wu.

Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha.

Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, Revised Selected Papers, 7839:337–351, 2012.

https://doi.org/10.1007/978-3-642-37682-5_24.

Dhonnobad !!

(Thank You)