New Cryptanalysis of ZUC-256 Initialization Using Modular Differences

Fukang Liu[1], Willi Meier[3], Santanu Sarkar[4], Gaoli Wang[5], Ryoma Ito[2], Tananori Isobe[1,2]

[1]University of Hyogo, Hyogo, Japan

[2]NICT, Tokyo, Japan

[3]FHNW, Windisch, Switzerland

[4]Indian Institute of Technology Madras, Chennai, India

[5]East China Normal University, Shanghai, China

FSE 2023

Overview

ZUC-256

- based on ZUC-128
- 256-bit security for 5G
- version history: 2018 (v1), 2021 (v2), 2023 (v3)
- one of the 3GPP 256-bit Confidentiality and Integrity Algorithms for the Air interface (Nov. 2022)

Impact of this work [latest comments by SAGE]

*So it does not directly translate into an attack on ZUC-256 as a whole. *** initialisation phase are only achieved with a very tight margin. *** and our recommendation is that this number be increased from 32(+1) to 48(+1).*

[Specification of the 256-bit air interface algorithms, Nov., 2022]
`www.3gpp.org/Liaisons/Incoming_LSs/S3-meeting.htm`

Round Function

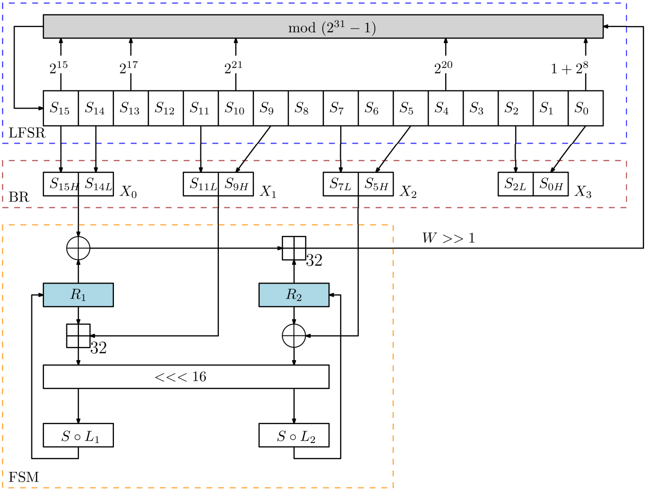


Figure: State update at the initialization phase of ZUC-256 (33 rounds)

Round Function: BR

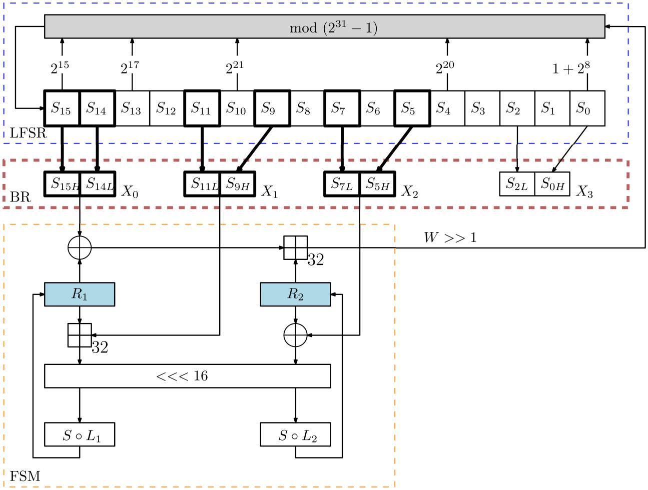
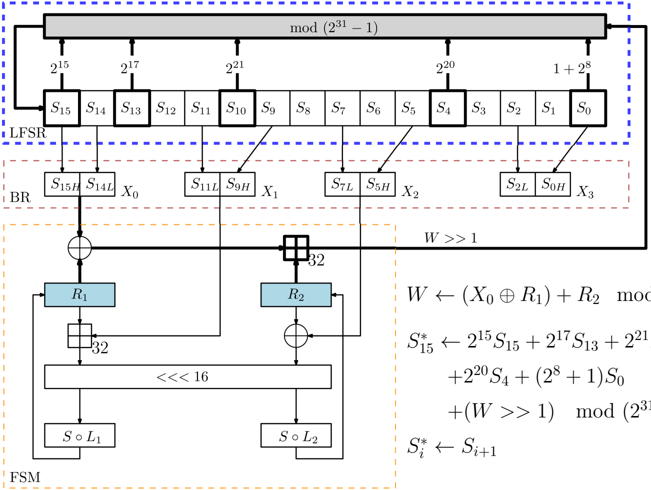


Figure: Step 1: update on BR

Round Function: LFSR



$$W \leftarrow (X_0 \oplus R_1) + R_2 \mod (2^{32})$$

$$S_{15}^* \leftarrow 2^{15}S_{15} + 2^{17}S_{13} + 2^{21}S_{10} + 2^{20}S_4 + (2^8+1)S_0 + (W >> 1) \mod (2^{31}-1)$$

$$S_i^* \leftarrow S_{i+1}$$

Round Function: FSM

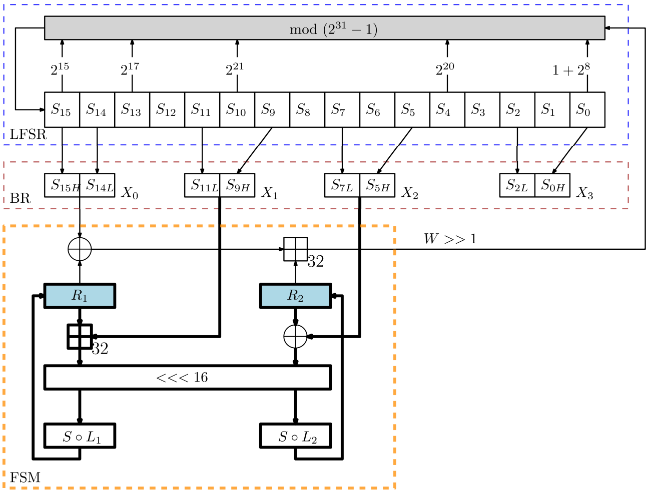


Figure: Step 3: update on FSM

Keystream

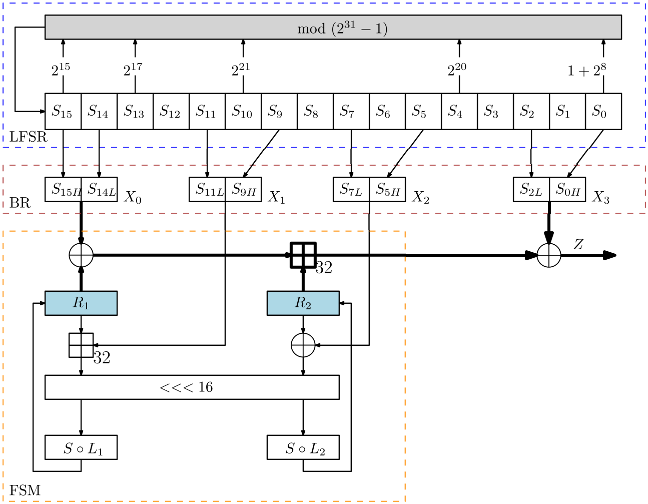


Figure: The first keystream word

Some Features

The round function looks complex:

- modular addition: modulo $p = 2^{31} - 1$ [LFSR layer]
- modular addition: modulo 2^{32} [LFSR/FSM layers]
- XOR ($\oplus$), logical shift ($\gg$) [LFSR/FSM layers]
- truncation, composition [BR layer]
- 8-bit S-boxes over $\mathbb{F}_2^8$ [FSM layer]
- 32-bit linear transforms over $\mathbb{F}_2^{32}$ [FSM layer]

It looks difficult to analyze the security.

Attack Scenario

Question1

Can we find an input difference such that there are nonrandom properties in ΔS_i^t after t clocks?

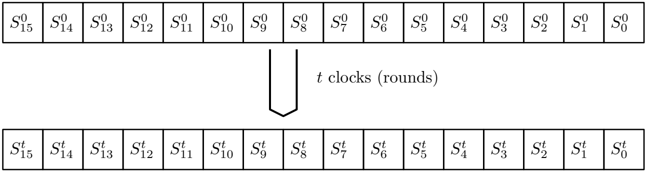


Figure: The t-round attack

Attack Scenario

A Shortcut ($\Delta S_{15}^{t-15} = \Delta S_{15}^{t}$)

Can we find an input difference such that there are nonrandom properties in ΔS_{15}^{t-15} after $t - 15$ clocks? How to detect the nonrandom properties of ΔS_{15}^{t-15}?

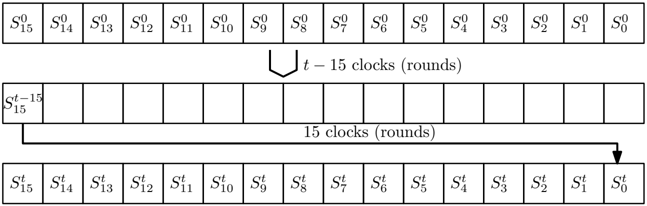


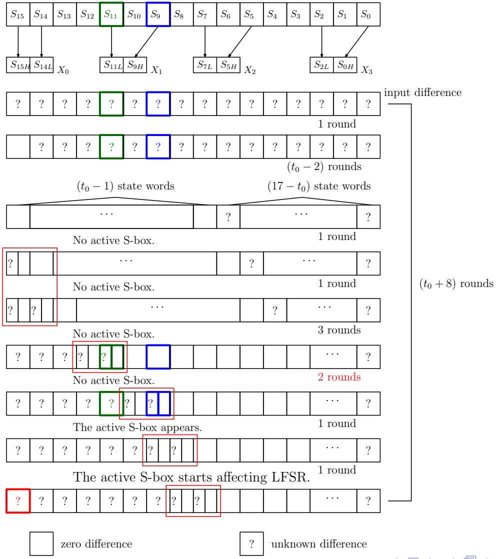
Figure: The t-round attack

Finding the Input Difference

The general idea:

- Construct equations such that the active S-boxes appear as late as possible.
- Allow active S-boxes to appear at the first few rounds, but the difference transitions can hold with probability 1 by controlling IV.
- Solve the corresponding equations.

A Critical Observation to Attack More Rounds



A Critical Observation

A critical observation

It is possible to extend the attack for 2 additional rounds if we have a suitable input difference.

When $\delta S_{15}^{t_0} \neq 0$ for the first time, we should make

$$\delta S_{15}^{t_0}{}_L \in \{0, \mathtt{0xffff}\},$$
$$\delta S_{15}^{t_0+1}{}_L \in \{0, \mathtt{0xffff}\}.$$

Then, it is possible to attack $t_0 + 6 + 2 + 15 = t_0 + 23$ rounds.

Equations when $t_0 = 8$ for ZUC-256

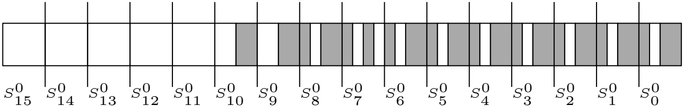


Figure: The illustration of the input difference (marked in gray).

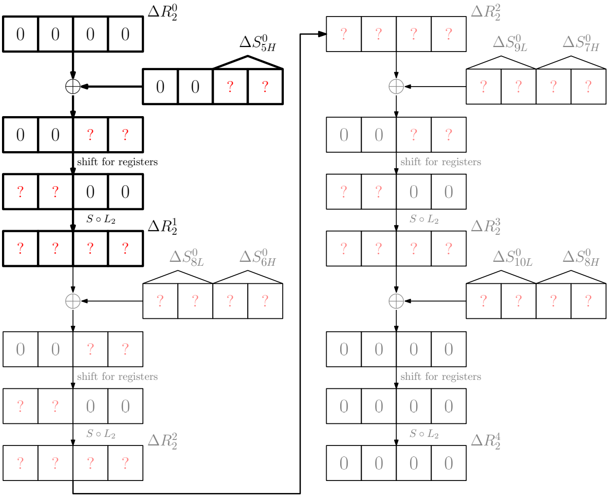
Clock 1:

$$\begin{aligned} 2^{21} \cdot \delta S_{10}^0 \boxplus 2^{20} \cdot \delta S_4^0 \boxplus 257 \cdot \delta S_0^0 &= 0, \\ \Delta S_{5H}^0 &\neq 0, \\ \Delta S_{7L}^0 &= 0, \\ \Delta S_{9H}^0 &= 0. \end{aligned}$$

Effect: $\delta S_{15}^1 = 0$, $\Delta R_1^1 = 0$, $\Delta R_2^1 \neq 0$.

Equations when $t_0 = 8$ for ZUC-256

Illustration for the FSM at the 1st clock:



Equations when $t_0 = 8$ for ZUC-256

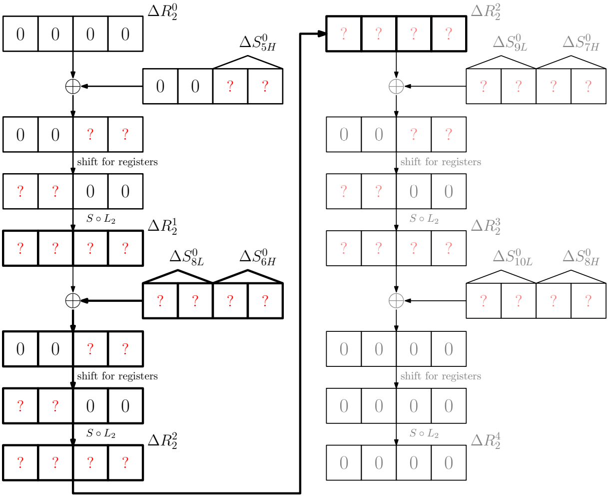
Clock 2:

$$\begin{aligned}((R_2^1 \oplus \Delta R_2^1) \gg 1) \boxminus (R_2^1 \gg 1) \boxplus 2^{20} \cdot \delta S_5^0 \boxplus 257 \cdot \delta S_1^0 &= 0, \\ \Delta S_{8L}^0 &= \Delta R_{2H}^1, \\ \Delta S_{10H}^0 &= 0.\end{aligned}$$

Effect: $\delta S_{15}^2 = 0$, $\Delta R_1^2 = 0$, $\Delta R_2^2 \neq 0$.

Equations when $t_0 = 8$ for ZUC-256

Illustration for the FSM at the 2nd clock:



Equations when $t_0 = 8$ for ZUC-256

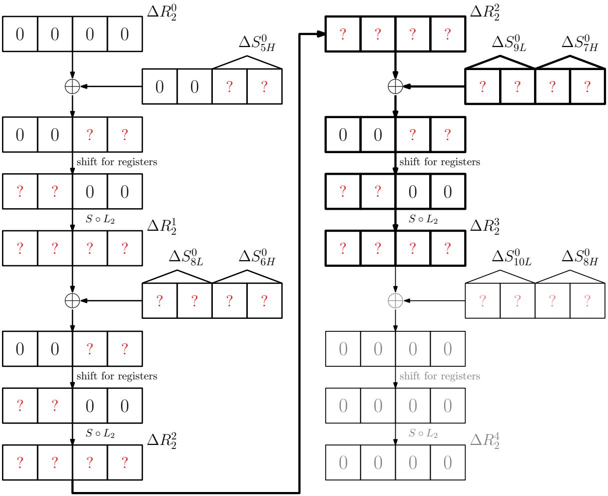
Clock 3:

$$\begin{aligned}((R_2^2 \oplus \Delta R_2^2) \gg 1) \boxminus (R_2^2 \gg 1) \boxplus 2^{20} \cdot \delta S_6^0 \boxplus 257 \cdot \delta S_2^0 &= 0, \\ \Delta S_{9L}^0 &= \Delta R_{2H}^2.\end{aligned}$$

Effect: $\delta S_{15}^3 = 0$, $\Delta R_1^3 = 0$, $\Delta R_2^3 \neq 0$.

Equations when $t_0 = 8$ for ZUC-256

Illustration for the FSM at the 3rd clock:



Equations when $t_0 = 8$ for ZUC-256

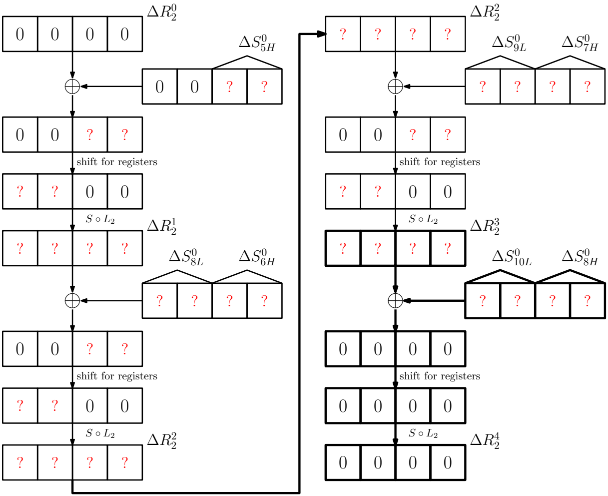
Clock 4:

$$\begin{aligned}((R_2^3 \oplus \Delta R_2^3) \gg 1) \boxminus (R_2^3 \gg 1) \boxplus 2^{20} \cdot \delta S_7^0 \boxplus 257 \cdot \delta S_3^0 &= 0,\\ \Delta S_{10L}^0 &= \Delta R_{2H}^3,\\ \Delta S_{8H}^0 &= \Delta R_{2L}^3.\end{aligned}$$

Effect: $\delta S_{15}^4 = 0$, $\Delta R_1^4 = 0$, $\Delta R_2^4 = 0$.

Equations when $t_0 = 8$ for ZUC-256

Illustration for the FSM at the 4th clock:



Equations when $t_0 = 8$ for ZUC-256

Clock 5:

$$
\begin{aligned}
2^{20} \cdot \delta S_8^0 \boxplus 257 \cdot \delta S_4^0 &= 0, \\
\Delta S_{9H}^0 &= 0.
\end{aligned}
$$

Effect: $\delta S_{15}^5 = 0$, $\Delta R_1^5 = 0$, $\Delta R_2^5 = 0$.

Equations when $t_0 = 8$ for ZUC-256

Clock 6:

$$\begin{aligned} 2^{20} \cdot \delta S_9^0 \boxplus 257 \cdot \delta S_5^0 &= 0, \\ \Delta S_{10H}^0 &= 0. \end{aligned}$$

Effect: $\delta S_{15}^6 = 0$, $\Delta R_1^6 = 0$, $\Delta R_2^6 = 0$.

Clock 7:

$$2^{20} \cdot \delta S_{10}^0 \boxplus 257 \cdot \delta S_6^0 = 0.$$

Effect: $\delta S_{15}^7 = 0$.

Equations when $t_0 = 8$ for ZUC-256

Clock 8:

$$(257 \cdot \delta S_7^0)[15:0] \quad \in \quad \{0, \texttt{0xffff}\}.$$

Effect: $\delta S_{15L}^8 \in \{0, \texttt{0xffff}\}.$

Clock 9:

$$(2^{15} \cdot (257 \cdot \delta S_7^0) \boxplus 257 \cdot \delta S_8^0)[15:0] \quad \in \quad \{0, \texttt{0xffff}\}.$$

Effect: $\delta S_{15L}^9 \in \{0, \texttt{0xffff}\}.$

Equations when $t_0 = 7$ for ZUC-256-v2

The equations at Clock 1 to Clock 6 are the same.

Clock 7:

$$(2^{20} \cdot \delta S_{10}^{0} \boxplus 257 \cdot \delta S_{6}^{0})[15:0] \quad \in \quad \{0, \texttt{0xffff}\}.$$

Effect: $\delta S_{15L}^{7} \in \{0, \texttt{0xffff}\}$.

Clock 8:

$$(2^{15} \cdot (2^{20} \cdot \delta S_{10}^{0} \boxplus 257 \cdot \delta S_{6}^{0}) \boxplus 257 \cdot \delta S_{7}^{0})[15:0] \quad \in \quad \{0, \texttt{0xffff}\}.$$

Effect: $\delta S_{15L}^{8} \in \{0, \texttt{0xffff}\}$.

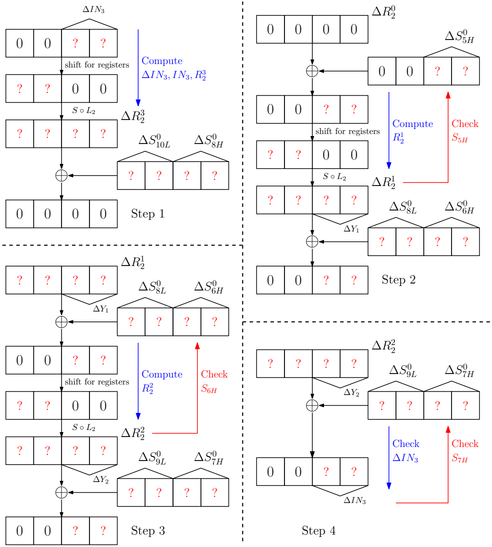
Clock 9: no more constraints.

Solving the Complex Equations

The general guess-and-determine procedure:

1. Pick a solution to the modular differences $(\delta S_0^0, \delta S_4^0, \delta S_8^0, \delta S_{10}^0, \delta S_6^0, \delta S_7^0)$ that does not contradict the equations.
2. Compute the set of XOR differences $\mathrm{SET}_{\Delta S_{6H}^0}$, $\mathrm{SET}_{\Delta S_{7H}^0}$, $\mathrm{SET}_{\Delta S_{10L}^0}$, $(\mathrm{SET}_{\Delta S_{8H}^0}, \mathrm{SET}_{\Delta S_{8L}^0})$.
3. Pick a solution to δS_9^0 and compute $\delta S_5^0 = 257^{-1} \cdot (p \boxminus 2^{20} \cdot \delta S_9^0)$.
4. Compute $\mathrm{SET}_{\Delta S_{9L}^0}$ and $\mathrm{SET}_{\Delta S_{5H}^0}$.
5. Only $(\delta S_1^0, \delta S_2^0, \delta S_3^0)$ are unknown. Determine them to make $\Delta R_1^4 = 0$, $\Delta R_2^4 = 0$. [Depth-first search & MITM]

Solving the Complex Equations



Our Result for 31-round ZUC-256

i	δS_i^0	∇S_i^0
0	0x0d80db05	=== nn=n n=== ==== nn=n n=nn ==== =n=n
1	0x7c00fb01	=== =u== ==== ==== nnnn n=nn ==== ==n=
2	0x047f38cb	=== =n== n=== ==== uu== u=== nn== n=nn
3	0x7f8034c3	=== ==== u=== ==== ==nn =n== nn== =n==
4	0x20ff011e	=n= ===n ==== ==== uuuu uuuu ==n= ==u=
5	0x20003fc0	nu0 0001 111n uuuu uu== ==== =u== ====
6	0x10001fe0	00n 1010 0101 1101 nuu= ==== ==u= ====
7	0x00020000	110 1101 0110 1nu0 1=== ==== ==== ====
8	0x7f04fdff	=== unnn ==== =n=n ===u nnn= ==== ====
9	0x7ffffdfb	=== ==== ==== ==== ==== ==uu nnnn nn==
10	0x7ffffefd	=== ==== ==== ==== ==== ===u =unn nnn=
11	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
12	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
13	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
14	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
15	0x00000000	=== ==== ==== ==== ==== ==== ==== ====

$R_2^1 = \texttt{0xc99de9d6}$, $R_2^2 = \texttt{0xb7b8cf96}$, $R_2^3 = \texttt{0xfaf5498c}$

$\Delta R_2^1 = \texttt{0x1e000604}$, $\Delta R_2^2 = \texttt{0x03fc0870}$, $\Delta R_2^3 = \texttt{0x017e1e0a}$

Our Result for 30-round ZUC-256-v2

i	δS_i^0	∇S_i^0
0	0x017f82fd	=== ===n n=== ==== u=== ==nn ==== =u=n
1	0x037f2f49	=== =n== u=== ==== uu=u ===u =n== n==n
2	0x1e00f305	=n= ==u= ==== ==== nnnn ==nn ==== =n=n
3	0x12fff85a	==n ==nn ==== ==== ==== u=== =n=n n=n=
4	0x6c00200f	=u= nn== ==== ==== ==n= ==== ===n ====
5	0x007f00ff	001 110n u000 0101 uuuu uuuu ==== ===u
6	0x0000fe02	001 1101 1101 0001 nnnn nnn= ==== ==n=
7	0x00800000	111 0000 n100 0010 1=== ==== ==== ====
8	0x7e80c13d	nnn nnn= n=== ==== nn=n uuu= uu== ==uu
9	0x00000008	=== ==== ==== ==== ===n uuuu uuuu u===
10	0x7fffefef	=== ==== ==== ==== ==un unnn nnnn ====
11	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
12	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
13	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
14	0x00000000	=== ==== ==== ==== ==== ==== ==== ====
15	0x00000000	=== ==== ==== ==== ==== ==== ==== ====

$R_2^1 = \texttt{0xa21c991b}$, $R_2^2 = \texttt{0xcf1106f0}$, $R_2^3 = \texttt{0x32f0e1e3}$
$\Delta R_2^1 = \texttt{0xdec311a0}$, $\Delta R_2^2 = \texttt{0x1ff810de}$, $\Delta R_2^3 = \texttt{0x3ff0fd01}$

Our Results

Target	Attack Type	Rounds	Time	Data
ZUC-256 initialization	distinguisher	28 (out of 33)	2^{23}	2^{23}
ZUC-256 initialization	distinguisher	31 (out of 33)	2^{29}	2^{29}
ZUC-256-v2 initialization	distinguisher	30 (out of 33)	$2^{39.8}$	$2^{39.8}$
ZUC-256 cipher	key recovery	15 (out of 33)	2^{47}	2^{47}
ZUC-256-v2 cipher	key recovery	14 (out of 33)	2^{58}	2^{58}

Table: Summary of the attacks on ZUC-256 and ZUC-256-v2, where at least 16 key bits are recovered in the key-recovery attacks. All the attacks are in the related-key setting. In addition, when the target is the initialization phase, attackers can access some internal state bits. When the target is the actual cipher, attackers can only access the keystream words.

Conclusion

1. With XOR/signed/modular differences, we can carefully study the difference transitions though the round function of ZUC-256.
2. Security margins seem small (2 and 3 rounds) for this type of distinguishing attack.

In ZUC-256-v3, the number of initialization rounds is increased to 48 rounds, thus a large security margin.