On the Linear Distinguishing Attack against ZUC-256 Stream Cipher

ZUC Design Team

Chinese Academy of Sciences
contact email: martin_zhangbin@hotmail.com

Abstract. At FSE 2020, a linear distinguishing attack is presented against the ZUC-256 stream cipher based on the 32-bit word with a data/time complexity of about $2^{236.38}$. In this paper, we re-evaluate the complexity of this attack and discuss the applicability of such a distinguishing attack in 5G application scenarios, where each keystream frame is limited to 20000, and up to 2^{32} bits. To assure a high success probability close to 1, it is shown that the precise time complexity of the distinguishing attack is $2^{253.93}$ basic operations with a data complexity of $2^{241.38}$ bits keystream, which is far beyond the keystream length limit in 5G application settings in the single-frame setting. Besides, we also consider the multiple-frame scenario where a long keystream could be formed by concatenating many short keystream frames generated from different (Key, IV) pairs. We show that even in such a strong model of distinguishing attacks, the reported bias will not exist in 5G application scenarios and the linear distinguishing attack will not work due to the fact that the long linear combination relation derived from the polynomial multiple of the LFSR in ZUC-256 over $\mathrm{GF}(2^{31}-1)$, which has been verified in experiments. It is concluded that the ZUC-256 stream cipher offers the full 256-bit security in 5G application scenarios.

Keywords: ZUC-256, 256-bit security, Linear distinguishing attack.

1 Introduction

ZUC-128 stream cipher [2] is the core of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 and 128-EIA3 international standard. With the development of the communication and computing technology, there is an emerging need for the new core stream cipher in the upcoming 5G applications which offers 256-bit security. To be highly compatible with the current 128-bit version, ZUC-256 stream cipher, which is a successor of the previous ZUC-128 stream cipher, is introduced in the beginning of 2018 [5]. The new ZUC-256 stream cipher differs from ZUC-128 only in the initialization phase and in the message authentication codes (MAC) generation phase, other aspects are all the same as the previous ZUC-128 algorithm, including the keystream generation phase. This design choice is required by the industrial domain, and is an advantage from the practical application point of view.

At FSE 2020, a linear distinguishing attack is presented by some researchers from Lund University in [3]. It is based on the new spectral analysis of the finite state machine (FSM) part and a new linear combination cancellation technique to deal with the arithmetic LFSR relation in ZUC-256 design. While normal cryptanalysis against common stream ciphers cannot be directly applied to ZUC-256, the new generic techniques could be applied to deal with the large linear approximations which is interesting in theory. Although this is only a linear distinguishing attack which requires a very long keystream and a high data/time complexity of $2^{236.38}$, it is of academic interest in the sense that in 5G applications, the long keystream could be formed by concatenating many short keystream frames so that the attack could be mounted to restore 1 bit information. In this paper, we first re-evaluate the time complexity of the linear distinguishing attack and show that the precise time complexity is $2^{253.93}$ basic operations to have a success probability very close to 1, with a data complexity of $2^{241.38}$ keystream bits. Thus, in the single-frame setting where a long keystream is available to the adversary, this distinguishing attack is out of the range of interest because the keystream frame length is limited to 20000, and up to 2^{32} keystream bits at most in 5G applications. Then, we consider the strong model of distinguishing attacks where a long keystream could be formed by concatenating many short keystream frames, and show that even in this setting, it is impossible to launch the linear distinguishing attack as described in [2]. The reason is that the linear combination relation required by the linear distinguishing attack is too long so that the biased combination could not be constructed even in the multiple-frame setting. We theoretically prove a necessary condition to launch a linear distinguishing attack in the multiple-frame setting, and present some experimental results on Brivium-B, and a reduced version of ZUC-256 to validate our results. It is concluded that ZUC-256 stream cipher could offer the full 256-bit security in 5G applications scenarios.

This paper is structured as follows. In Section 2, we give the detailed description of the keystream generation phase in ZUC-256 stream cipher that is relevant to our analysis. Then the re-evaluation of the data/time complexity of the linear distinguishing attack is presented in Section 3, and theoretical analysis of the multiple-frame linear distinguishing attack is provided in Section 4 with the corresponding experimental results on Brivium-B and the reduced version of ZUC-256. Finally, some conclusions are drawn in Section 5.

2 The Description of ZUC-256 Stream Cipher

In this section, we will present the detailed description of the keystream generation phase in ZUC-256 stream cipher. The following notations will be used herein.

- Denote the integer modular addition by $\boxplus$, i.e., for $0 \leq x < 2^{32}$ and $0 \leq y < 2^{32}$, $x \boxplus y$ is the integer addition mod 2^{32}.
- Denote the integer addition modulo $2^{31} - 1$ by $x + y \bmod 2^{31} - 1$ for $1 \leq x \leq 2^{31} - 1$ and $1 \leq y \leq 2^{31} - 1$.

- Denote the bitwise exclusive OR by $\oplus$.
- Denote the bit string concatenation by $\|$.
- Denote the bitwise logic OR by $|$.
- $K = (K_{31}, K_{30}, ..., K_2, K_1, K_0)$, the 256-bit secret key used in the ZUC-256 where K_i for $0 \leq i \leq 31$ are 8-bit bytes.
- $IV = (IV_{24}, IV_{23}, ..., IV_{17}, IV_{16}, IV_{15}, \ldots, IV_1, IV_0)$, the 184-bit initialization vector used in the ZUC-256 where IV_i for $0 \leq i \leq 16$ are 8-bit bytes and IV_i for $17 \leq i \leq 24$ are 6-bit string occupying the 6 least significant bits of a byte.
- d_i for $0 \leq i \leq 15$ are the 7-bit constants used in the ZUC-256 stream cipher.
- $\lll$, the left rotation of a 64-bit operand, $x \lll n$ means $((x \ll n) \mid (x \gg (64 - n)))$.

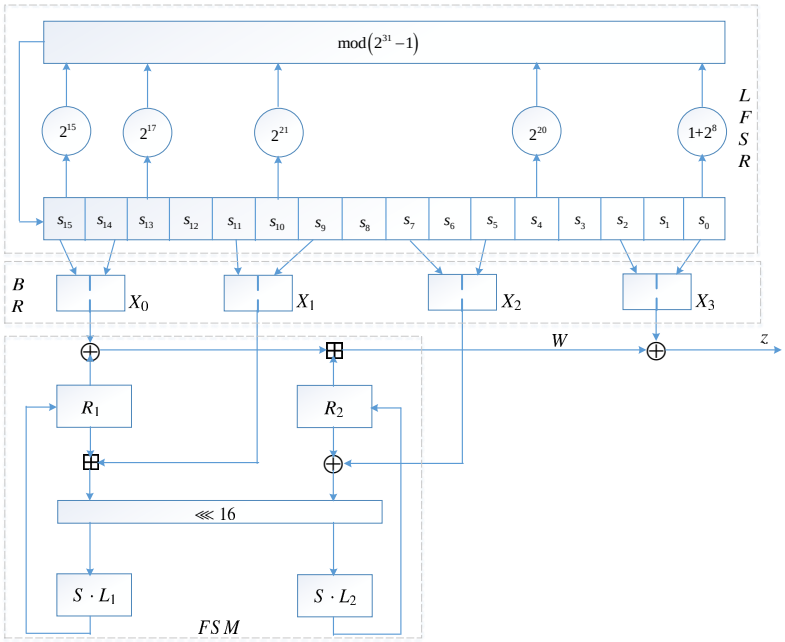

Fig. 1. The keystream generation phase of the ZUC-256 stream cipher

As depicted in Fig.1, there are 3 parts involved in ZUC-256: a 496-bit linear feedback shift register (LFSR) defined over the field GF($2^{31} - 1$), consisting of 16 31-bit cells $(s_{15}, s_{14}, ..., s_2, s_1, s_0)$ defined over the set $\{1, 2, ..., 2^{31} - 1\}$; a bit reorganization layer (BR), which extracts the content of the LFSR to form 4 32-bit words, (X_0, X_1, X_2, X_3), used in the following finite state machine (FSM); there are two 32-bit words R_1 and R_2 used as the memory in the FSM.

There are $32 + 1 = 33$ rounds of initialization in the ZUC-256 and after it, the keystream generation phase begins which output a 32-bit keystream word at each step. Now we specify the relevant subroutines one-by-one.

LFSRWithworkMode()

1. $s_{16} = 2^{15} \cdot s_{15} + 2^{17} \cdot s_{13} + 2^{21} \cdot s_{10} + 2^{20} \cdot s_4 + (1 + 2^8) \cdot s_0 \mod(2^{31} - 1)$
2. if $s_{16} = 0$ then set $s_{16} = 2^{31} - 1$
3. $(s_{16}, s_{15}, \cdots, s_2, s_1) \rightarrow (s_{15}, s_{14}, \cdots, s_1, s_0)$.

Bitreorganization()

1. $X_0 = s_{15H} \parallel s_{14L}$
2. $X_1 = s_{11L} \parallel s_{9H}$
3. $X_2 = s_{7L} \parallel s_{5H}$
4. $X_3 = s_{2L} \parallel s_{0H}$,

where s_{iH} is the high 16 bits of the cell s_i and s_{jL} is the low 16 bits of the cell s_j.

$F(X_0, X_1, X_2)$

1. $W = (X_0 \oplus R_1) \boxplus R_2$
2. $W_1 = R_1 \boxplus X_1$
3. $W_2 = R_2 \oplus X_2$
4. $R_1 = S(L_1(W_{1L} \parallel W_{2H}))$
5. $R_2 = S(L_2(W_{2L} \parallel W_{1H}))$,

where $S = (S_0, S_1, S_0, S_1)$ is the 4 parallel S-boxes which are the same as those used in the previous ZUC-128 and L_1 and L_2 are the two MDS matrices used in the ZUC-128. The ZUC-256 stream cipher generates a 32-bit keystream word at each time instant.

KeystreamGeneration()

1. Bitreorganization( )
2. $Z = F(X_0, X_1, X_2) \oplus X_3$
3. LFSRWithworkMode().

ZUC-256 generates from 20000-bit keystream to 2^{32}-bit keystream for each frame, after that a key/IV re-synchronization is performed with the key/constants fixed and the IV changing into a new value, then the new keystream frame is generated.

As specified in [5], *the security claim of the ZUC-256 stream cipher is the 256-bit security in the 5G application setting.* For the forgery attacks on the authentication part, the security level is the same as the tag size and the IV is not allowed to be re-used. If the tag verification failed, no output should be generated.

3 Re-evaluation of the Complexity in the Distinguishing Attack

In this section, we will make a re-evaluation of the complexity aspects of the linear distinguishing attack in [3] in the number of basic operations, i.e., the bit logical and/bit xor. We will not give a detailed review of the 32-bit word based linear distinguisher here. Please see the original paper for the details.

Since the linear distinguisher exploits the Squared Euclidean Imbalance (SEI) of $2^{236.38}$, we first recall the following Theorem according to [1].

Theorem 1. *Let $Z_1, Z_2, \ldots, Z_n$ be the iid (independent and identified distribution) random variables over the alphabet set $\boldsymbol{Z}$ of distribution D, D_0 and D_1 be two distributions of same support which are close to each other, and n be the number of samples of the best distinguisher between $D = D_0$ or $D = D_1$. Let d be a real number such that*

$$n = \frac{d}{\sum_{z \in \boldsymbol{Z}} \frac{\epsilon_z^2}{p_z}} \approx \frac{d}{2D(D_0 \| D_1)},$$

where $p_z = Pr_{D_1}[z]$ and $p_z + \epsilon_z = Pr_{D_0[z]}$. Then the overall probability of error is $P_e = \Phi(-\frac{\sqrt{d}}{2})$ with $\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{1}{2}u^2} du$, and $D(D_0 \| D_1)$ is the relative entropy between two distributions D_0 and D_1.

Theorem 1 shows that to have a high distinguishing success probability, the $\frac{1}{D(D_0 \| D_1)}$ data complexity is not enough. The following Table shows the correspondence according to Theorem 1. In the following, we will utilize Theorem 1

Table 1. The correspondence between d and the success distinguishing probability

d	1	2	4	8	16	32	64
success prob.	0.691462	0.76025	0.841345	0.92135	0.97725	0.997661	0.999968

and Table 1 to compute the time complexity of the word-based distinguishing attack.

First note that before actually launching the linear distinguisher, the adversary should first collect this amount of keystream and then compute the statistic from the keystream to finally make a decision. In the ZUC-256 case, the adversary should first collect $O(2^{236.38})$ 32-bit keystream words and then utilize the long linear combination of the following form

$$M\sigma[Z^{t_1} \oplus Z^{t_2} \oplus Z^{t_3} \oplus Z^{t_4}] \oplus [Z^{t_1+1} \oplus Z^{t_2+1} \oplus Z^{t_3+1} \oplus Z^{t_4+1}],$$

where $t_1 \leq t_2 \leq t_3 \leq t_4$ and the t_is are the 4 time instants derived from the polynomial multiple of the LFSR in ZUC-256 with $t_4 \approx 2^{167}$ and the matrix M

is as follows.

$$M = \begin{pmatrix} \texttt{0x26dad00b} & \texttt{0x5de94454} & \texttt{0x3bdfdb0d} & \texttt{0x1423c42f} & \texttt{0xc4f35585} & \texttt{0x1f22e504} \\ \texttt{0xeb07cc1e} & \texttt{0x3633b301} & \texttt{0x11b4bca3} & \texttt{0x6f23b103} & \texttt{0x912adb7d} & \texttt{0x6a058e9e} \\ \texttt{0x67d4ef5a} & \texttt{0xdd0830b6} & \texttt{0xee579099} & \texttt{0x9af30192} & \texttt{0x455d8a7b} & \texttt{0x22133144} \\ \texttt{0x7fb935a8} & \texttt{0x4d923b96} & \texttt{0xc0c9967e} & \texttt{0x99db94fc} & \texttt{0x442f1154} & \texttt{0x17994e1f} \\ \texttt{0x08d2662e} & \texttt{0xccc8fe9c} & \texttt{0x994d8fb8} & \texttt{0xfba4f0dc} & \texttt{0x462d2a69} & \texttt{0x373306ed} \\ \texttt{0x91282e11} & \texttt{0x9b82d788} & & & & \end{pmatrix}$$

From [3], the 32×32 binary matrix M is given as a vector of 32-bit integers, where $M_{i,j}$ for $0 \leq i, j \leq 31$ is derived as $M_{i,j} = \lfloor \frac{M[i]}{2^j} \rfloor \bmod 2 = (M[i] >> j)$ & $0x1$.

Thus, the adversary will first compute a large amount of 32-bit vectors by the matrix multiplication of $M_{32\times 32}$ with the actual keystream words, repeat this process at the 4 specified time instants, and xor the resultant 32-bit words together to have the desirable statistic. The time complexity of this process is as follows.

$$d \cdot (32 \cdot (32 \cdot \frac{1}{2} + \log_2 32 + 1) \cdot 2^2 + (\log_2 4 + 1) \cdot 32 \cdot 2) \cdot 2^{236.38}.$$

When $d = 64$, the time complexity is around $2^{253.93}$ basic operations, which is really marginal for the 256-bit security. The concrete correspondence between the time complexity and d is shown in Table 2. Note that if table-lookup is used to replace the basic operations in some data unit, the numerical number will be decreased to some factor, but not to much and the complexity unit will be the time cost for one table-lookup of the specified data unit.

Table 2. The correspondence between d and the time complexity

d	1	2	4	8	16	32	64
Time comp.	$2^{247.93}$	$2^{248.93}$	$2^{249.93}$	$2^{250.93}$	$2^{251.93}$	$2^{252.93}$	$2^{253.93}$

4 Multiple-frame Linear Distinguishing Attack

In this section, we will consider a very strong model for linear distinguishing attacks, where a long keystream is obtained by concatenating many short keystream frames generated from different (Key, IV) pairs and show that even in such a strong model, the presented linear distinguishing against ZUC-256 will not work due to the long linear combination relation needed in the attack, which is impossible to get for ZUC-256 in 5G application scenarios.

4.1 Theoretical Analysis

Theorem 2. *Let $Z = Z_1, Z_2, \ldots, Z_n$ be the keystream words generated by some stream cipher over the alphabet set $\boldsymbol{Z}$ and let $\bigoplus_{i=0}^{L-1} \alpha_i Z_i$ $(\alpha_{L-1} \neq 0)$ be the statistic with some bias $\triangle(Z)$ and no shorter linear combination $\bigoplus_{i=0}^{L'-1} \alpha'_i Z_i$ $(\alpha'_{L'-1} \neq 0)$ with $L' < L$ is detected to have a bias. Consider the multiple-frame scenario where a long keystream*

of length $n = \frac{d}{\triangle(Z)}$ *is formed by concatenating many short frames with frame length* $f < L$*, then there will be no bias detected in such a scenario; if* $f \geq L$*, then the bias* $\triangle(Z)$ *will be detected in such a keystream.*

Proof. Regard each keystream word Z_i in Z as a random variable, then according to the assumption that there is no shorter statistic $\bigoplus_{i=0}^{L'-1} \alpha'_i Z_i$ with $L' < L$ to have a detected bias, the target statistic $\bigoplus_{i=0}^{L-1} \alpha_i Z_i$ is of length L. If $f < L$, then the adversary cannot construct the biased quantity $\bigoplus_{i=0}^{L-1} \alpha_i Z_i$ from only one keystream frame, and at least two consecutive keystream frames are needed to construct the desirable quantity. In the latter case, the result will have no bias according to the assumption and the fact that the variables coming from different initialized states are independent. On the other hand, if $f \geq L$, at least one biased statistic quantity could be constructed successfully from two consecutive keystream frames, thus the final result will be some realizations of a series of biased quantities. □

Theorem 2 shows that in the multiple-frame scenario in 5G applications, since each keystream frame is limited to be less than or equal to 2^{32} bits and the exploited linear combination relation is of weight 4 and is of length $O(2^{167})$, thus there will be no bias detected in this setting, or in other words, ZUC-256 will be immune to the linear distinguishing attack in 5G applications.

4.2 Experimental Results

To support the above analysis, some practical experiments have been done to check whether there will be some bias detected under the concrete conditions specified by Theorem 2. We have done experiments on Brivium-B [4] and a reduced version of ZUC-256 to check the validity of Theorem 2. The results are as follows.

Brivium-B Case. Brivium-B is a Trivium-like stream cipher which has a 177-bit internal state, we will not review the detailed description here. It was shown in [4] that Brivium-B has a biased statistic constructed from the generated keystream as $z_0 \oplus z_{15} \oplus z_{27} \oplus z_{30} \oplus z_{42} \oplus z_{99} \oplus z_{108} \oplus z_{177}$ with a bias 2^{-16}. Thus, according to Theorem 2, if a long keystream of length 2^{32} which is generated consecutively from one internal state is available, then there will be some bias detected. Actually, this is indeed the case as verified both in Table 8 of [4] and in our experiments. Furthermore, we have also done experiments to check whether there will be some bias detected in the multiple-frame setting with $f = 1$, $f = 100$ and $f = 175$, it has been observed that there is no bias detected in all of the three cases in tens of times of experiments, which are all in our prediction provided by Theorem 2.

A reduced version of ZUC-256 Case. We have also constructed several reduced versions of ZUC-256 which inherit the design spirit of the actual ZUC-256. Here we only give the corresponding results for one reduced version. In this reduced version, the LFSR feedback polynomial is defined as $P(x) = -x^{16} + x^{13} + 2 \cdot x^6 + x + 2$ over $p = 2^3 - 1 = 7$. There is a polynomial multiple of weight 4 found as $x^{t_1} + x^{t_2} = x^{t_3} + x^{t_4} \mod P(x)$, where $t_1 = 0, t_2 = 43359, t_3 = 29682$ and $t_4 = 107162$. The corresponding keystream words bias is found to be 2^{-17}. Thus, in the experiments we have found that if there is a long keystream of length 2^{37} generated from one initial

state, then there will always be a bias detected; while in the multiple-frame setting with the frame length $f < t_4$, then no matter how long the formed keystream is and whatever the initialized state is generated, there will be no bias detected in the experiments, which have shown the validity of Theorem 2.

5 Conclusions

In this paper, we have re-evaluated the complexity of the linear distinguishing attack at FSE 2020 and discussed the applicability of such a distinguishing attack in 5G application scenarios. The time complexity of the presented linear distinguishing attack is shown to be $2^{253.93}$ basic operations when the success probability is very close to 1, which is marginal to the 256-bit security. It is also shown both in theory and in experiments that even in the multiple-frame linear distinguishing attack setting, such an attack will not work in the considered 5G scenarios. Finally, it is concluded that ZUC-256 offers the full 256-bit security in 5G application settings.

References

1. Baigneres T., Junod P. and Vaudenay S., How Far Can We Go Beyond Linear Cryptanalysis? *Advances in Cryptology–ASIACRYPT'2004*, LNCS vol. 3329, pp. 432-450, 2004.
2. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 and 128-EIA3, Document 4: Design and Evaluation Reprot. `http://www.gsmworld.com/documents/EEA3_EIA3_Design_Evaluation_v1_1.pdf`.
3. Yang J., Johansson T. and Maximov A., Spectral Analysis of ZUC-256, In IACR Transactions on Symmetric Cryptology 2020 (1). pp. 266-288
4. Maximov A., Biryukov A., Two Trivial Attacks on Trivium, *Selected Areas in Cryptography–SAC 2007*, LNCS vol. 4876, pp. 36-55, 2007.
5. ZUC Design Team, The ZUC-256 Stream Cipher, available at `http://www.is.cas.cn/ztzl2016/zouchongzhi/201801/W020180126529970733243.pdf`.