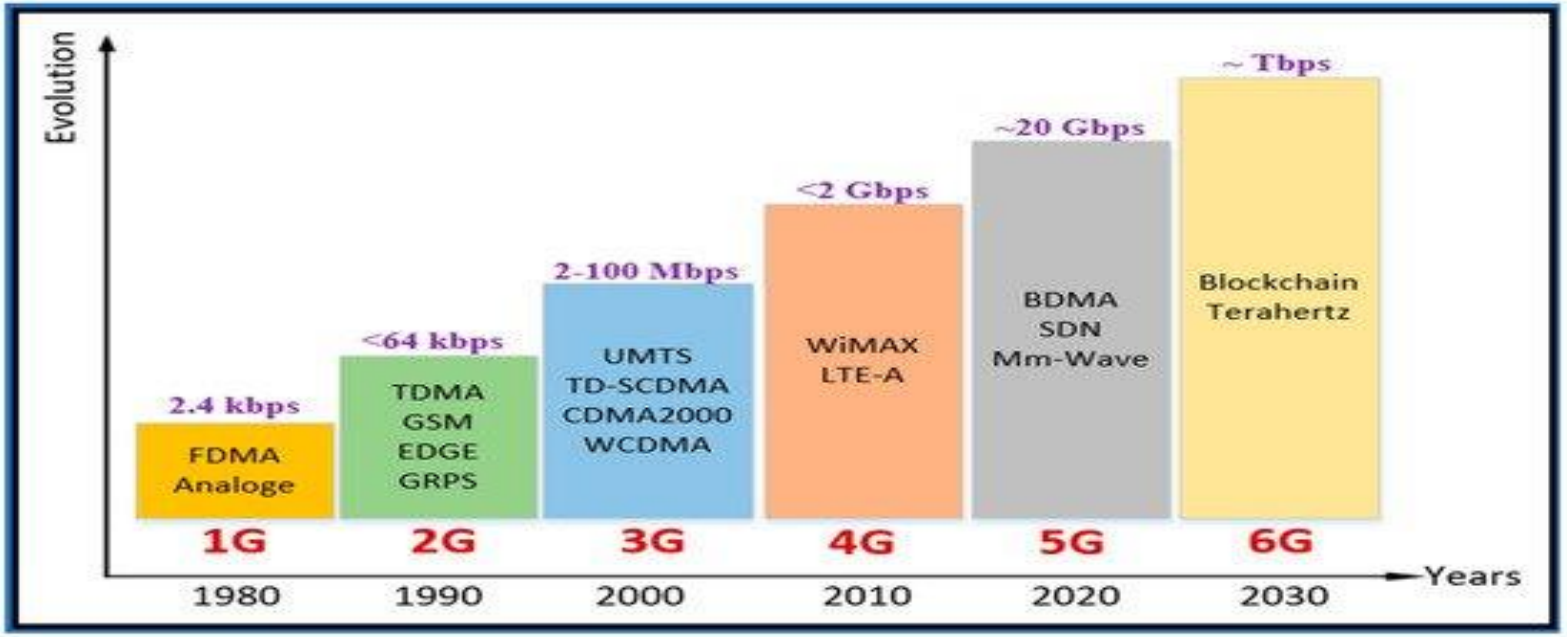
# Encryption Algorithms for Data Security in 4G and 5G Networks

**Khalid Fadhil Jasim**
**Department of Computer Science**
**Cihan University-Erbil, KRG, Iraq**
khalid.jassim@cihanuniversity.edu.iq

# Outlines

- Introduction
- Analysis of AES-CTR Cipher
- Analysis of SNOW 3G Cipher
- Analysis of ZUC Cipher
- Discussion
- Conclusions

# Introduction



# Introduction

- **5G** networks **support** several **services** (e.g. **smart networks**, **data networks using block chain, communication between cars**, Unmanned Aerial Vehicles (UAV), mobile fog computing…)
- **5G relied** on technologies like **Dynamic Adhoc Wirless Net.** (DAWN), **Heterogeneous Nets.** (HetNet), **Multi radio access** (MultiRAT) and the Multiple input Multiple Output (MIMO).
- In addition, **5G** is expected to **offer frequency bandwidth** (**1.8 up to 2.6 GHz**, may be improved to 30 - 300 GHz), and to support **data transmissions** with **( ~ 20 Gbps)**.

# Introduction (Cont.)

- 4th generations (**4G**) of mobile networks **introduced in (2010)**.
- **4G** networks presented **services** (e.g. **Voice calls via IP** telephony, **Web Access via Mobile devices**, **Cloud Computing** applications, and Mobile HD-TV technology)
- **4G** networks relied on 2 **standards :** Worldwide Interoperability for Microwave Access (**WiMAX**) & Long Term Evolution (**LTE**).
- **4G-LTE** supported **frequency bandwidth** (**1.4-20 MHz**).
- Data transmissions, **bit rate** was (**< 2 Gbps**) .

# Introduction (Cont.)

- **In terms** of **communication security,** the **5G and 4G** networks relied on cryptographic systems to encrypt and **protect** the **exchanged data** between **base stations** and **mobile phones.**
- In this context, **5G and 4G** networks **relied** on **security** encryption **algorithms AES-CTR, SNOW 3G, and ZUC.**

# Analysis of AES-CTR Cipher

- **AES block cipher** included **three versions:**
- **AES-128 with 10 rounds**, **AES-192 with 12 rounds**, and **AES-256 with 14 rounds**.
- Each round: adopts **4** mathematical **transformations** (**SubBytes**, **ShiftRows**, **MixColumns**, and **AddRoundKey** operations)
- **AES-128 with counter mode (AES-CTR)** was **adopted** for confidentiality and integrity algorithms (EEA2 & EIA2) in the mobile generations (**4G-LTE**) and for **5G** generation.

# Analysis of AES-CTR Cipher(Cont.)

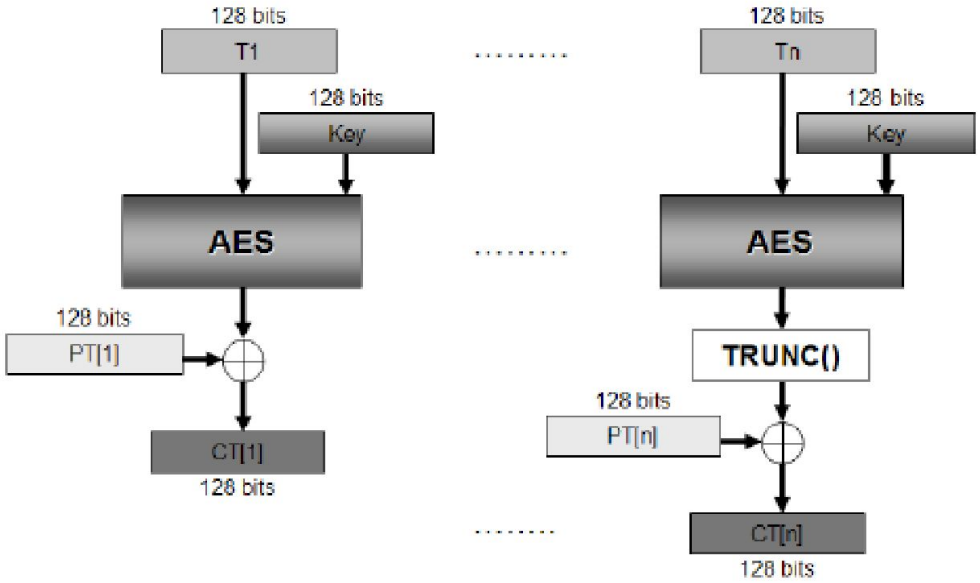



Figure 1: AES-CTR with Encryption/Decryption.

# Analysis of AES-CTR Cipher(Cont.)

- **Weaknesses: Improved Impossible Differential Cryptanalysis** attack can be implemented **against AES** cipher.
- This cryptanalysis **attack against AES-128** (with **7 Rounds**) requires **data complexity** ($2^{105}$ ), **time complexity** ($2^{106.88}$ )
- **In Initialization phase**, AES-CTR **requires 128-bit secret key** (K) and **counter block** (**T of 128-bit**, IV key).
- **Weaknesses: Counter block T** (IV key) **sent without protection.**

# Analysis of SNOW 3G Cipher

- **SNOW 3G** cipher **adopted** for the **security** of (**4G-LTE**) (128-EEA1 and 128-EIA1) LTE systems and proposed for (**5G**) network security.
- The **structure based** on **two parts:**
- **First**, **LFSR register** of 16 stages (S0, S1, S2, S3, … S15).
- **Second**, **FSM** with **3 registers (R1, R2, and R3**) and 2 Substitution boxes (**Sbox(S1) & Sbox(S2)**) (Figure 2)

# Analysis of SNOW 3G Cipher(Cont.)

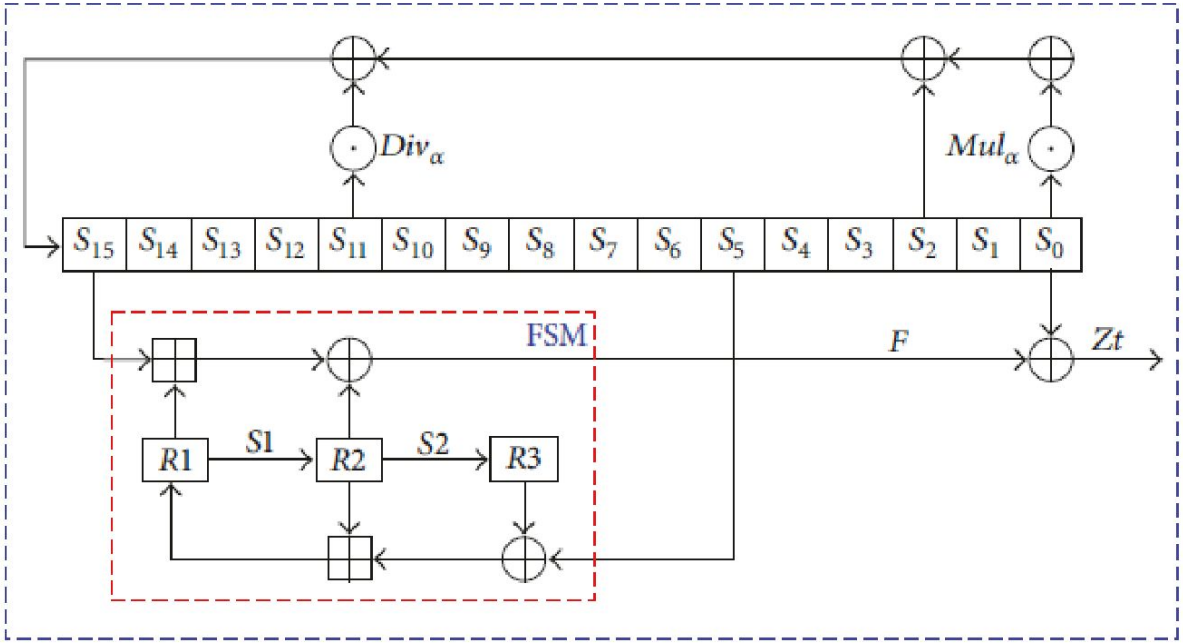



Figure 2: Structure of SNOW 3G Stream Cipher

# Analysis of SNOW 3G Cipher(Cont.)

- **Chosen IV cryptanalysis** technique can be adopted to **attack SNOW 3G** cipher.
- **Choosing IV attack** of **(18) steps** needs **data complexity** ($2^{57}$) and **time complexity** ($2^{53}$).
- **In initialization** operations, **secret key (K)** words (**K0, K1, K2, and K3**). **IV key** 32-bit words (**IV0, IV1, IV2, and IV3).**
- **Weaknesses** have been identified:
- **Length** of **secret key**(**128-bit**) was **less than** the **length** of **LFSR** register(**512-bit**).

# Analysis of SNOW 3G Cipher(Cont.)

- For instance, the same 32-bit **K0 used in:**

  LFSR_S8 = **K0 XOR** 0xffffffff; and

  LFSR_S0 =**K0 XOR** 0xffffffff).

- **Length** of **IV key** (**128-bit**) was **less than** the length of **LFSR** register (**512-bit**), used in positions:

  LFSR_S9 = K1 XOR 0xffffffff XOR **IV3**;

# Analysis of ZUC Cipher

- **ZUC cipher** constructed basically with **three layers.**
- **First layer:** the **LFSR** register, 16 stages (S0, S1, S2, S3, … S15).
- **Second layer, Bit Reorganization** (BR), 4 words (X0, X1, X2, X3)
- **Third layer: function (F)**, 2 (32-bit) **registers (R1 & R2)**,

  and 2 substitution boxes (**S-box S0 & S-box S1**).

# Analysis of ZUC Cipher(Cont.)

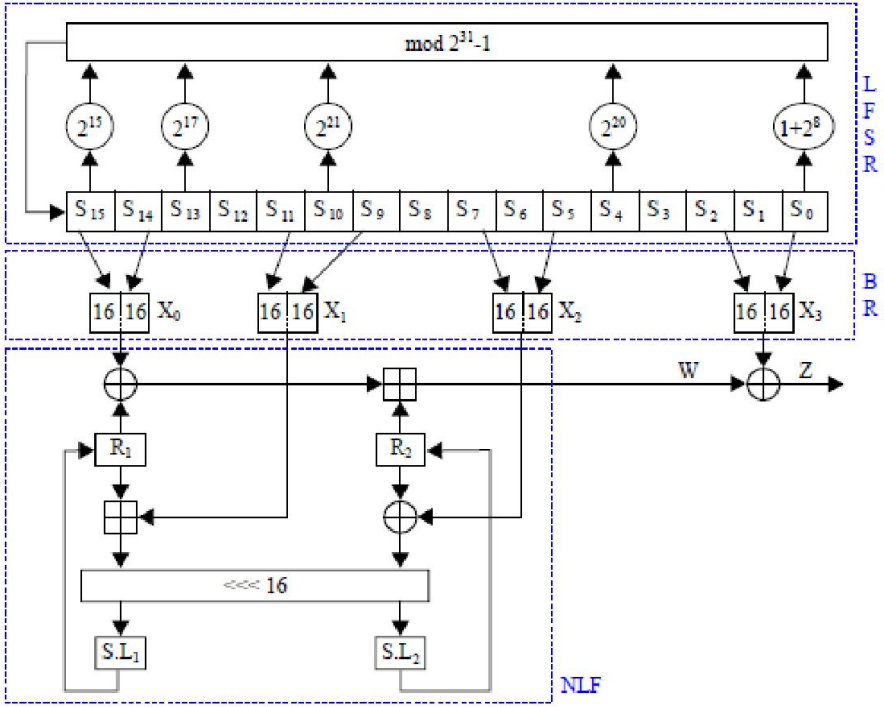



Figure 3: ZUC Cipher .

# Analysis of ZUC Cipher(Cont.)

- **Differential cryptanalysis** can be used to attack the ZUC cipher.
- The method needs to **test** ( $2^{13.3}$ ) values of **IV keys** pairs, it was found that **one of** the ($2^{15.4}$ ) values of keys there were **identical** values from **keystreams**.
- **In initialization phase**, **LFSR** register requires **secret key** bytes **(K0, K1, K2, … , K15)**, fixed values (**d[16]: d0, d1, d2, … , d15**) and **IV key** bytes (**IV0, IV1, IV2, … , IV15**).
- For Example: **LFSR_S0 = (K0 ‖ d0 ‖ IV0); …**

# Analysis of ZUC Cipher(Cont.)

- **Weaknesses** were pinpointed :
- The bytes of **IV key** are **sent without protection.**
- ZUC cipher **depends** on **constants of d[16]:**
  **do= 0x44D7,** d1=0x26BC, … , **d15= 0x47AC.**
- **Length** of **secret key** (**128-bit**), **less than** of **LFSR** (**496-bit**).
- Therefore, **Brute force** attack **reduced** from **($2^{496}$)** to **($2^{128}$)**, which **decrease security** of **ZUC** cipher.

# Conclusions

- This **research concentrated** on analysis and investigation the features of **4G and 5G** technologies.
- **AES-CTR, SNOW 3G and ZUC** ciphers were used for the **security** of **4G and 5G** generations.
- **Security Weaknesses** found :
- **In AES-CTR , Counter block** is sent **without protection**, **Improved Impossible Differential Cryptanalysis** attack (with 7 Rounds).
- **In SNOW 3G, IV** is sent **without protection,**

# Conclusions (cont.)

- **In ZUC , IV key** is sent **without protection,**

  **depends** on **constants** of **d[16],**

  **Differential cryptanalysis** can be used to **attack ZUC** cipher.
- **Therefore**, **we proposed** to:
- **Increase** the **lengths** of initialization keys (**Counter Block, IV and K)**
- **Use encrypted IV keys,**
- **Use variable** values for **d[],** in which **to enhance the security** of **these cipher algorithms.**

# THANK YOU