Analysis of Confidentiality Algorithms in Different Mobile Generations

Khalid Fadhil Jasim
International Islamic University Malaysia
IIUM Cyber Security Malaysia Center for Cyber Space Security, Kuala Lumpur, Malaysia
Cihan University-Erbil, Erbil, Iraq
khalid.jassim@yahoo.com

Imad Fakhri Al-Shaikhli
Department of Computer Science, KICT
International Islamic University Malaysia
IIUM Cyber Security Malaysia Center for Cyber Space Security,
Kuala Lumpur, Malaysia
imadf@iium.edu.my

Abstract

In past years, a variety of Mobile technology generations have been adopted in mobile communication systems. Various sensitive information (e.g. emails, bank transactions, voice calls, ...) was exchanged via the mobile systems. The protection of information confidentiality became a serious problem for the customers of these systems. Security solutions such as confidentiality cipher algorithms proposed to protect the transmissions in different mobile generations. The proposed cipher algorithms like A5/1 cipher, SNOW 3G cipher, ZUC cipher, and AES cipher were designed for securing mobile systems. This paper provides analysis study of operations and specifications for these cipher algorithms, and investigating the cryptanalysis methods which can be employed to attack these cipher algorithms.

Keywords: Mobile Generations; Cipher Algorithms; A5/1Cipher; SNOW3G Cipher; ZUC Cipher; AES Cipher; Cryptanalysis Attacks.

Introduction

In previous years, the researchers and industrials achieved massive advancement in Mobile communication and information technologies. Mobile technologies performed growing success and progress in different mobile generations. In this context, first generation systems (1G) appeared in (1980s), these analog systems presented voice calls without any protection. Shukla et al. [1] provided comparative study on various mobile generations, for instance, Mobile (1G) adopted cell signals with analog transmissions, offered expensive and less heavy devices. The standards in (1G) included Advanced Mobile Phone System (AMPS) and European Total Access Communication Systems (ETACS). The channel bandwidth was (30 KHz) in AMPS

DOI: 10.24086/cuesj.si.2017.n1a11

system. Some problems pointed out in Mobile (1G) such as low capacity, without security, and poor quality in voice calls. Second generation systems deployed in (1990s), these systems relied on digital communication, some standards like Global System for Mobile communication (GSM), and services supported by these systems included (e- mails, SMS messages, and digital faxes).

In Mobile (2G), Some important standards used like (CDMA, the Code Division Multiple Access technique) and (TDMA, the Time Division Multiple Access technique). The channel bandwidth in this generation was (30-200 KHz) and data rate transmission was (64 kbps) [2].

In (2000s), third generation with Universal Mobile Telecommunication System standards (3G-UMTS) was introduced. The (3G) systems adopted the technology of Mobile Broadband, delivered variety of mobile services (e.g. Internet with high speed access, multimedia applications, video conferencing via mobile nets, and digitized voice calls). Mobile (3G) presented features with enhancements (i.e. data transmissions with high speed, raised capacity of data and voice, supported packet data for networks). For example, Mobile (3G) with standards (CDMA2000, EV-DO) offered transmission data rate from (3.1 Mbps) to (14.7Mbps), and the standards (HSPA, WCDMA) supported transmission rate from (14.4 Mbps) up to (63+ Mbps) [3].

Also, fourth generations systems was developed in (2010s) with faster broadband technology, based on some standards like Long Term Evolution technology (LTE). The (4G-LTE) systems presented some services for mobile networks customers, in which involved (Mobile Web Access, IP telephone services , Mobile TVs with HD technology, and Services of Cloud Computing). In mobile LTE technology the frequency bandwidth was (1.4-20 MHz), the peak of transmission rate reached (100 Mbps up to 326.4Mbps) for downlink transmissions, and for uplink transmissions was (50 Mbps). Multiple antenna techniques (i.e. Beam forming, Spatial Division Multiple Access, and MIMO) have been used in Mobile LTE. Using of Multiple antenna techniques led to increase transmission rates, capacity of voice and data, and improved the efficiency in mobile (4G-LTE) systems [4].

In mobile technology there was a demand for high data transmission and new wireless mobile applications with enhanced features. Thus, researches have been started in fifth mobile (5G) generations and it is expected that (5G) will be adopted around (2020). In mobile (5G), the researches focused on improving worldwide wireless web (wwww), provide voice services via IP (VOIP), and Dynamic Adhoc Net (DAWN). The new features include data bandwidth (1Gbps and high), single unified standard, Multiple Access (CDMA and BDMA), core network (Internet), switching (All packet). Also, this generation provides broad band services (e.g. internet, voice, video streaming), and virtual private Net (VPN, Networks) is supported in (5G)[5,6].

Furthermore, stream ciphers and block ciphers algorithms have been proposed as confidentiality ciphers algorithms to ensure the security in different mobile communication systems. The A5/1 stream cipher algorithm was developed to protect users of mobile systems (2G-GSM) and prevent eavesdropping operations against these systems [7]. SNOW 3G is stream cipher algorithm represented the core confidentiality algorithm (UEA2), used as encryption algorithm in mobile phone systems (3G-UMTS). Design of SNOW 3G depends on register LFSR, Finite State Machine(FSM), and registers (R1, R2, and R3). Fault cryptanalysis can be used against SNOW 3G, in which the cryptanalyst may inject fault values in certain positions (S_i) of LFSR during keystream generation mode. In this case, the cryptanalyst needs (22) fault values and (200) words of output keystream, then tries to extract values of keystream [8]. The stream cipher algorithm ZUC was designed to be adopted in confidentiality algorithm (EEA3-128), integrity algorithm (IEA3-128), and represented essential encryption in mobile systems (4G-LTE, Long Term Evolution mobile technology). Structure of ZUC relies on register LFSR, bit reorganization (BR), and non linear f-function. In initialization mode, ZUC cipher algorithm is loaded with values from IV key and secret key (K). In key stream operation mode the ZUC cipher produces words of key stream (Z). The key stream words used in encryption and decryption operation for packets of data in downlink and uplinks transmissions (i.e. in 4G-LTE devices) [9]. Additionally, AES cipher algorithm was block cipher algorithm and employed in mobile technology (4G-LTE). It was identified as (EEA2) confidentiality algorithm and (EIA2) integrity algorithm to achieve data confidentiality and integrity. The EEA2 algorithm was based on AES block cipher, in which it operates with 128-bit key and counter operation mode (AES-128 with CTR mode). During data encryption with bock cipher algorithm (AES in CTR mode), the plaintext (PT) data divided into (128-bit) blocks, these blocks of (PT) are XORED with key stream blocks of AES cipher then produce blocks of encrypted data [10].

The paper organized as follows. Section II provides specification of A5/1 cipher algorithm and Guess and Determine cryptanalysis against this cipher algorithm. Description and operations of SNOW 3G cipher algorithm and Differential cryptanalysis attacks presented in section III. Section IV focuses on analysis components of ZUC cipher and Algebraic cryptanalysis attacks against this cipher. Versions of AES block ciphers, operations, descriptions, and Meet-in-the-Middle with biclique cryptanalysis for AES ciphers are presented in section V. Section VI provides analysis summery of confidentiality cipher algorithms and cryptanalysis techniques. Finally, some conclusions of this research are offered in last section VII.

A5/1 Cipher Algorithm

The A5/1 cipher algorithm was designed to protect the voice calls transmitted through GSM mobile communications. A5/1 was adopted as confidentiality algorithm in second generation mobile technology (2G- GSM) [11]. Also, A5/1 relied on stream cipher technique, the structure consists of (3) Linear Feedback Shift Registers (R1[19-bits], R2[22-bits], and R3[23-bits]). The secret key involves 64-bits (Kc with 64 bits). The feedback function of register R1 computed from positions (13, 16, 17, and 18), register R2 calculated from positions (20 and 21), and R3 from positions (7, 20, 21, and 22). The movement of three registers based on stop and go technique, so bit position (8) controls clock of R1, bit position (10) controls clock of R2, and position (10) controls R3. The 3 registers are clocked , then keystream (KS) is generated according to the following equation:

$$KS= R1[18] \oplus R2[21] \oplus R3[22] \quad (1)$$

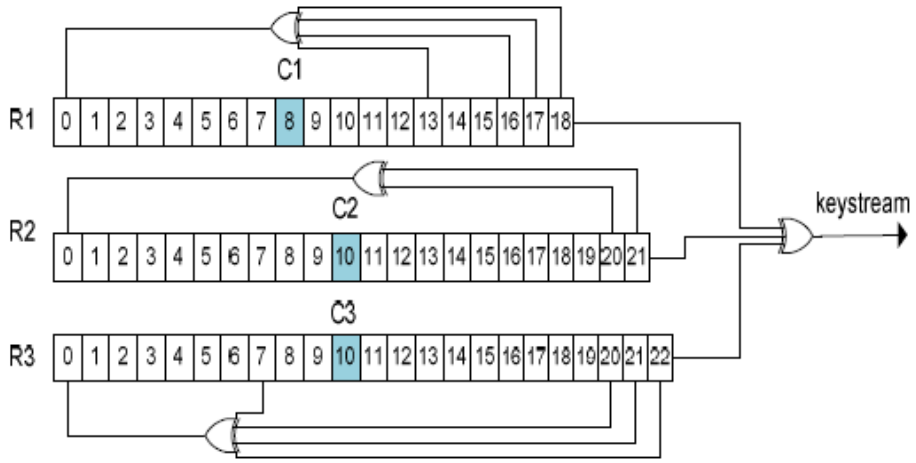

Fig. 1: A5/1 Cipher

The key stream generator is moved (224) steps and produce two blocks (BLOCK1 with 114-bits and BLOCK2 with 114-bits), represent the key stream (KS). The first part of key stream (BLOCK1) is adopted in the encryption of uplink transmission, the second part (BLOCK2) is used in decryption of downlink transmission (in Mobile Station Side). Moreover, BLOCK1 of key stream is used to decrypt uplink transmission and BLOCK2 to encrypt downlink transmission (in Network Side) [11].

Guess and Determine cryptanalysis attack may be used in cryptanalysis of A5/1 cipher algorithm. In 1994, Anderson[12] suggested this method to attack A5/1 algorithm, in which he proposed to guess the initial state (19- bits) of register R1, 22-bits of R2, and 11-bits of R3. The attacker will search (2^{52}, where 19+22+11=52) cases to determine the correct unknown bits of R3.

Cryptanalysis attack against this cipher was proposed by Golic [13]. In this attack, a system of linear equations were constructed then tried to solve the set of (64x64 linear equations). The complexity of this attack was (2^{40}). First, half of initial values for registers (R1, R2, and R3) have been guessed, then the remaining initial values of these registers will be determined based on information extracted from known-keystream (KS, Equation 1).

Mahalanobis & Shah [14] presented an improved version of Guess and Determine cryptanalysis to attack A5/1 cipher. The average complexity of this attack method was required ($2^{48.5}$, search for possible cases). The attack is started by guessing (19-bits) of register R1, then the initial values of registers (R1 and R2) will be determined in next steps of the attack. It is assumed that (64-bits) of keystream are available for cryptanalyst. Also, the attack included Determination Phase and Post Processing Phase. In Determination Phase, the cryptanalyst tries to guess the values of (R1) and then identifies the values of (R1 and R2). Where, in Post Processing Phase, the A5/1 cipher is moved and produce outputs (i.e. stream of bits). The outputs are compared with the available (64-bits) of keystream, If the outputs matching with keystream then the initial values of registers (R1, R2, and R3) represent the values of secret key.

Snow 3G Cipher Algorithm

The SNOW 3G cipher algorithm was developed by (ETSI/SAGE) and it was adopted as confidentiality cipher algorithm in third generation of mobile technology (3G- UMTS) . This stream cipher algorithm depends on secret key (K with 128-bits) and Initial vector key (IV with 128-bits). The design of SNOW 3G involves Linear Feedback Shift Register (LFSR, with length 16 32-bit words, $s_0, s_1, \ldots, s_{15}$), finite state machine (FSM, with 3 registers R1, R2and R3, each of 32-bit), and substitution boxes (S-boxes S1 and S2, each with 32-bit input and 32-bit output). The positions (s_5 and s_{15}) of LFSR are used as input to FSM to update the components of FSM (e.g. at clock t) as follows[15]:

$$R_1^t = R_2^{t-1} \boxplus (R_3^{t-1} \oplus s_5^{t-1})$$

$$R_2^t = S_1(R_1^{t-1}) \qquad R_3^t = S_2(R_2^{t-1})$$
$$F^t = (s_{15}^t \boxplus R_1^t) \oplus R_2^t$$

Differential cryptanalysis attacks can be used to analyze SNOW 3G cipher [16]. In this method, it is noticed that if there is no feedback from (FSM) to (LFSR), during initialization operations (clock No.1 to clock No. 32), and the cryptanalyst gained information about pair of (IV keys). Then this cipher algorithm can be attacked and crypt analyzed by using differential method (with known IV), the required complexities of this attack are (2^{57}) for the time and (2^{33}) for data of keystream. In case there is a feedback (from FSM to LFSR), the same attack's method can be adopted in cryptanalysis of 16 rounds from 33 rounds during initialization process of this cipher.

ZUC Cipher Algorithm

The ZUC cipher algorithm is developed in china to be used as confidentiality and integrity algorithms (128-EEA3 and 128-EIA3 respectively) for the security of fourth generation mobile technology (Mobile 4G-LTE). The design of ZUC relied on three main parts: linear feedback register (LFSR), bit reorganization part, and the (f) as nonlinear function [17]. The initial input keys for this cipher involve initial vector key (IV with 128-bits) and secret key (K with 128-bits). The LFSR includes 16 stages ($s_0, s_1, \ldots, s_{15}$, where each stage s_i consists of 31-bits). The bit reorganization part consists of four (32-bits) words (X0, X1, X2, and X3) and defined as follows:

$X0 = S_{15}H \parallel S_{14}L$; (where H is leftmost (16 bits) of word S_{15} from LFSR and $\parallel$ is concatenation)

$X1 = S_{11}L \parallel S_9H$; (where L is rightmost (16 bits) of word S_{11} from LFSR)

Where the symbol ($\boxplus$) is addition modulo 2^{32} and ($\oplus$) is bit wise exclusive OR. Also, at the beginning of cipher algorithm operation, the LFSR initialized with values from IV key and secret key (K), the FSM is started with initial values (R1=R2=R3=0). The cipher algorithm runs (33 clocks), then the (32-bit) word of keystream (Z^t) is produced (e.g. at clock t) as shown:

$$z^t = s_0^t \oplus F^t \tag{2}$$

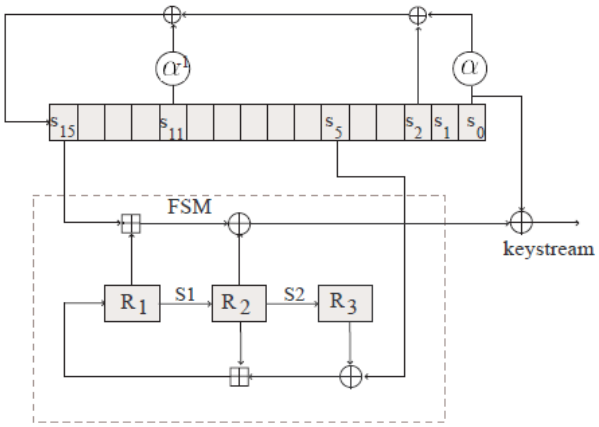

Fig. 2: SNOW 3G Cipher

$$X2 = S7L \parallel S5H;$$

$$X3 = S2L \parallel S0H.$$

The words (X1 and X2) are employed as inputs to function (f), in which to update registers (R1 and R2). The remaining words (X0 and X3) adopted in computation of keystream (Z).

Moreover, the function (f) relies on two registers (R1 [32-bits], and R2 [32-bits]), two words (W1 and W2), and (32x32 bits) Substitution box S (S-box S):

W= (X0 $\oplus$ R1) $\boxplus$ R2; ($\oplus$is exclusive OR, $\boxplus$ is addition mod 232) W1 = R1 $\boxplus$ X1; W2 = R2 $\oplus$ X2;

R1=S-Box S(L1 (W1L $\parallel$ W2H)); (where L is rightmost (16 bits) of word W1)

R2=S-Box S(L2 (W2L $\parallel$ W1H)). (where H is leftmost (16 bits) of word W1)

The linear transformations L1 and L2 , used in function (f), is computed as shown:

$$L1(X)=X \oplus (X <<< 2) \oplus (X <<< 10) \oplus (X$$

$$<<<18) \oplus (X <<< 24),$$

L2(X)=X $\oplus$ (X <<< 8) $\oplus$ (X <<< 14) $\oplus$ (X <<<22) $\oplus$ (X <<< 30). (where X <<< n , is the n-bit cyclic shift of 32-bit word X to the left).

During the keystream generation mode, ZUC cipher algorithm produces (32-bits) word of keystream (Z^t, at clock t) as follows:

$$Z^t = ((X_0^t \oplus R_1^t) + R_2^t) \oplus X_3^t \quad (3)$$

The sequence of keystream words are adopted in encryption and decryption processes for transmitted data via mobile communications.

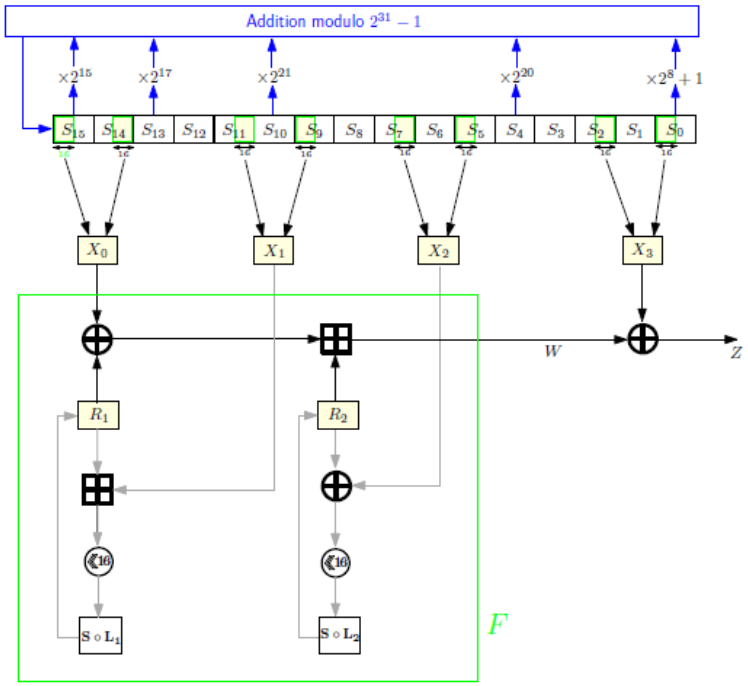

Fig. 3: ZUC Cipher

Algebraic cryptanalysis method may be adopted to attack ZUC cipher. In this attack, the cryptanalyst tries to find indirect relation between bits sequence of keystream (Z) and internal state of this cipher algorithm. It will be considered that the non linear filter function as combiner function. The inputs to combiner function include four words (X0, X1, X2, and X3) extracted from LFSR, and the output is 32-bits word of keystream (Z with 32-bits). To establish a relation between the four inputs and the one output, a matrix is constructed, in which to simulate the combiner. Matrix columns involve monomials (128-bits of four inputs and 32- bits of outputs Z to combiner function), and Matrix rows include four input words (X0, X1, X2, and X3). This method

of attack can be used to solve the system of equations and extract secret key (initial state of LFSR) of ZUC cipher with keystream data (2^{97}) and complexity of needed operations (2^{282}) [18,19].

AES Cipher Algorithm

Advanced Encryption Standard Algorithm (AES) is classified as block cipher and operates on data block of size (128-bits). The encryption operations based on secret keys with size (128-bit, 192-bit, or 256-bit). According to size of keys, there are three versions of AES ciphers (i.e. AES-128 bit with 10 rounds, AES-192 bit with 12 rounds, and AES-256 bit with 14 rounds). Moreover, the AES-128 bit with 10 rounds was employed as confidentiality and integrity algorithms (128-bit EEA2 and 128-bit EIA2 respectively). These two algorithms represented the second set of algorithms in fourth generation of Long Term Evolution in mobile systems technology (Mobile 4G-LTE technology)[20].

In AES-128 bit, the main encryption and decryption operations are applied on state array with size (4x4 bytes as 2 dimension matrix). The input plaintext (128-bits), is represented as 16 bytes, and arranged in state array (4x4 bytes). Each round of AES-128 (10 rounds in AES-128) adopts four mathematical operations on state array:

1. **Sub Bytes Operation(SB):** represents nonlinear mathematical transformation, in which it applies the substitution box (S-Box) on all the 16 (bytes), which already exist in state array (4x4 matrix of input plain bytes).

2. **Shift Rows Operation(SR):** denotes linear mathematical transformation, the target of this operation is to rotate the row number (i, ith row) of state array by value (i-bytes) to left direction, where (i=0,1,2,3).

3. **Mix Columns Operation(MC):** also, this operation represented linear mathematical transformation, in which each column of state array is multiplied by constant array (4x4 matrix of constant bytes) and the math operations defined in the field ($GF(2^8)$).

4. **Add Round Key Operation:** the AES-128 bit depends on 10 rounds, therefore the 16 bytes of state array, in round number (i), are XORED with 16 bytes of related round key (RK_i).

Furthermore, The AES-128 cipher relies on secret key with (128-bits), and key schedule procedure used to produce (11) round sub keys (Round Key-0, Round Key-1, ...

, Round Key-10). First round key is extracted from secret key bytes, then each of remaining round keys (RKi , where i=1,2, …,10) produced depending on its predecessors sub round keys (RKi-1).

In addition, Meet-in-the-Middle cryptanalysis is a technique which can be employed to attack block ciphers [21]. Biclique cryptanalysis technique proposed to attack hash functions family (SHA-2 family, Skein-512 hash function) . Also, Biclique technique can be adopted to attack different versions of AES block cipher. The idea of Biclique cryptanalysis against AES cipher is based on the Biclique concept presented in [22].

In Biclique cryptanalysis, first the function (f) is defined as function that transforms internal state (S) of block cipher to output ciphertext (C):

$$f_K(S) = C \tag{4}$$

Here, function f is connected the input (2^d) of internal states (S_j), (2^d) ciphertext (C_i), and (2^{2d}) cipher keys (K[i,j]. Thus, Biclique with (d-dimension) is defined by three elements, [{C_i}, {S_j}, {K[i,j]}]:

$$C_i = f_{K[i,j]}(S_j) \text{ for all } i,j \in \{0,\ldots,2^d-1\} \tag{5}$$

In this cryptanalysis attack, Biclique attack can be performed according to the following steps:

- The cryptanalyst tries to partition the space of cipher key (K) for groups (K[i,j], matrix with 2^dx2^d dimensions), and Encryption of block cipher (E) is assumed as two sub ciphers (E=f ◦g).
- The cryptanalyst creates structure which includes possible ciphertexts (2^d of C_i), intermediate possible states (2^d of S_j), according to group of cipher keys (K[i,j]), and such that decipherment of ciphertext (C_i) leads to the state (S_j) of the block cipher.

$$\forall i,j : S_j \xrightarrow[f]{K[i,j]} C_i$$

 The cryptanalyst performs the decryption operations on possible ciphertexts (C_i), based on secret cipher keys (Ksecret), then producing the possible plaintexts (2^d of P_i).

$$C_i \xrightarrow[e^{-1}]{\text{decryption oracle}} P_i$$

 The Secret key (Ksecret) is identified, when it leads to transform state (S_j) to plaintext (P_i), and it is one of the cipher keys (K[i,j]) under tests.

$$\exists i,j : P_i \xrightarrow[g]{K[i,j]} S_j$$

As a results, to recover the key of AES-128 bit (for 8- round from 10), the requirements involved complexity of memory with (2^8), complexity of data is (2^{88}), and complexity of computations ($2^{125.34}$). The requirements for AES-192 bit (9-round from 12) included complexity of memory with (2^8), complexity of data is (2^{80}), and complexity of computations ($2^{188.8}$). With respect to AES-256 bit (9-round from 14), the complexity of memory was (2^8), complexity of data was (2^{120}), and complexity of computations ($2^{251.92}$) [23].

Discussion

The analysis summary of Cipher algorithms and cryptanalysis techniques (shown in TABLE 1 and TABLE 2) are follows:

 The cipher algorithms (A5/1, SNOW 3G, and ZUC) are adopted design of stream ciphers, where AES relied on design of block ciphers.

 The structure of A5/1 algorithm was simple, consists of 3 LFSRs and function with (XORs operations).

 The structures of SNOW 3G and ZUC Ciphers were more complicated adopted different components (e.g. LFSR [16 words], FSM, memory registers Rs, Non linear functions, and S-boxes), in which enhanced the security for these ciphers.

 The structure of AES relied on three versions (AES-128 with 10 rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds). Each round

depends on Sub Bytes , Shift Row, Mix Column, and Add Round Key operations, S-boxes as well. Different number of rounds, the four operations, variety of keys (128-bits, 192-bits, and 256-bits), were made AES block cipher with better security over three mentioned stream ciphers.

- Moreover, A5/1 cipher used to secure (2G-GSM) Mobile systems, SNOW 3G for security of (3G- UMTS) Mobile systems, ZUC and AES ciphers in (4G-LTE) Mobile systems.

- Various Cryptanalysis techniques can be used to attack these cipher algorithms. Guess and Determine adopted to attack A5/1 cipher. The cryptanalyst targets to guess (19 bits) of register R1, using (64-bits) of keystream, and tries to identify values of registers R2 and R3. This attack requires, complexity computations ($2^{48.5}$), data complexity (2^{6}). To attack initial key with brute force it is required complexity computations (2^{64}).

- Differential cryptanalysis used to attack SNOW 3G cipher. The IV key (128-bit) used in SNOW 3G during encryption operations, and it is transmitted via communication channels. Thus, the cryptanalyst can use differential method with known information of IV keys, focused on pairs of IVs and steps of keystream generation (clock-1 to clock-32). This type of cryptanalysis against SNOW 3G, needs complexity computation (2^{57}), and data complexity (2^{33}) for the keystream. Also, the secret key K with (128-bit) in this cipher, and the required complexity is (2^{128}) for brute force attack.

- Algebraic cryptanalysis can be applied to attack ZUC cipher. In this method, the non liner function treated as combiner function. Four (32-bit) words (X0, X1, X2, and X3) are taken from register LFSR, used as inputs to combiner function, then (32-bit) keystream (Z) represents output of this combiner function. Matrix is created based on (128-bits) of the four inputs and (32-bits) of (Z) keystream. Thus, the cryptanalyst tries to solve system of equations, then reveals values of secret key K (i.e. 128 bits used to initialize register LFSR). To perform this attack, the needed data complexity is (2^{97}) for keystream, and computations complexity is (2^{282}). Brute force attack required (2^{128}) computation complexity based on (128-bits) of secret key.

- Meet-in-the-Middle with Biclique techniques used to attack (3) versions AES cipher. These attacks depend on sequence of steps. First, the space of secret ciphering key divided to groups and treated as matrix (K[i,j],with $2^{d}x2^{d}$ dimensions), block cipher encryption (E) with two sub ciphers (f and g). Next, establish structure

involves possible ciphertexts (2^d of C_i), possible states (2^d of S_i), based on group of keys, decryption of ciphertext to produce state (S_i). Then, decryption applied on possible ciphertexts (C_i), using secret keys(Ksecret), and generating possible plaintexts (2^d of P_i). For instance in AES-128, the data complexity is (2^{88}), and complexity of computations ($2^{125.34}$). But in AES-256, the data complexity is (2^{120}), and complexity of computations ($2^{251.92}$).

Table 1. Cipher algorithms and mobile generations

Cipher Algorithms	Type of Cipher Design	Components of Cipher Algorithm	Encryption/ Decryption Keys	Mobile Generations
A5/1	Stream Cipher	-LFSR1[18-bits], LFSR2[21-bits], LFSR3[22-bits] -Function(with 2 XORs)	-K(64-bits) -IV(22-bits)	Mobile(2G-GSM)
SNOW 3G	Stream Cipher	-LFSR[16, 32-bits words] -FSM -Registers R1[32-bits], R2[32-bits], R3[32-bits] -S-Boxes (S1, S2)	-K(128-bits) -IV(128-bits)	Mobile(3G-UMTS)
ZUC	Stream Cipher	-LFSR[16, 31-bits words] -Bit Reorganization (X0, X1, X2, X3) -Non linear Function -Registers R1[32-bits], R2[32-bits] -S-Boxes (S0, S1)	-K(128-bits) -IV(128-bits)	Mobile(4G-LTE)
AES	Block Cipher	-State array (4x4 bytes) -Sub Bytes Operation (SB) -Shift Row Operation (SR) -Mix Column Operation (MC) -Add Round Key Operation (AK)	-K(128-bits) -K(192-bits) -K(256-bits) -IV(128-bits)	Mobile(4G-LTE)

Table 2. Cryptanalysis of Ciphe algorithms

Cipher Algorithms	Type of Cryptanalysis Attack	Computations Complexity Of Attack	Data Complexity Of Attack	Complexity Of Brute Force Attack
A5/1	Guess and Determine Cryptanalysis	$2^{48.5}$	2^6	2^{64}
SNOW 3G	Differential Cryptanalysis	2^{57}	2^{33}	2^{128}
ZUC	Algebraic Cryptanalysis	2^{282}	2^{97}	2^{128}
AES	Biclique Cryptanalysis, Based on Meet-in-the-Middle Attack	-AES-128, $2^{125.34}$ - AES-192, $2^{188.8}$ - AES-256, $2^{251.92}$	-AES-128, 2^{88} - AES-192, 2^{80} - AES-256, 2^{120}	-AES-128, 2^{128} - AES-192, 2^{192} - AES-256, 2^{256}

Conclusion

This paper introduced analysis study of confidentiality cipher algorithms in different mobile technology generations. First generation (Mobile 1-G) was without protection. Second generation (2G-GSM) relied on A5/1 cipher algorithm. A5/1 cipher possessed simple design (3 LFSRs, XORs operations) and offered weak protection. Third generation (3G-UMTS) adopted SNOW3G cipher for data protection and authenticity. SNOW3G involved rigid design, more secure, with various components (LFSRs, FSM, Registers, and S-boxes). Fourth generation (4G-LTE) employed ZUC and AES ciphers for integrity and confidentiality algorithms. ZUC cipher included secure design, based on different components (LFSRs, Bit Reorganization, non linear function, Registers, and S-boxes). AES cipher was with 3 versions (AES-128 with 10 rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds). In AES ciphers, the rounds relied on different mathematical transformations (Sub Bytes , Shift Row, Mix Column, Add Round Key operations, and S-boxes). In addition, there was research progress efforts on fifth mobile generations (5G), it is still under research, the researches focused on improving worldwide wireless web, and enhance wireless mobile features. it is expected that (5G) will be presented around (2020).

Finally, this paper investigated some cryptanalysis techniques (Guess and Determine for A5/1 cipher, Differential cryptanalysis for SNOW 3G cipher, Algebraic cryptanalysis for ZUC cipher, and Meet-in-the-Middle with Biclique techniques for 3 versions of AES cipher).

References

[1] S. Shukla, V. Khare, S Garg, and P. Sharma, “Comparative Study of 1G , 2G , 3G and 4G,” Journal of Engineering, Computers & Applied Sciences (JEC&AS), vol. 2, no. 4, pp. 55–63, 2013.

[2] M. R. Bhalla and A. V. Bhalla, “Generations of Mobile Wireless Technology: A Survey,” International Journal of Computer Applications, vol. 5, no. 4, pp. 26–32, 2010.

[3] M. La Polla, F. Martinelli, and D. Sgandurra, “A Survey on Security for Mobile Devices,” IEEE Communications Surveys & Totorials, pp. 1–26, 2012.

[4] F. Rezaei, M. Hempel, and H. Sharif, “A comprehensive performance analysis of LTE and Mobile WiMAX,” 8th Int. Wirel. Commun. Mob. Comput. Conf., pp. 939–944, Aug. 2012.

[5] Garsha Sai Nitesh and Ashna Kakkar, “Generations of Mobile Communication ,” International Journal of Advanced Research in Computer Science and Software Engineering 6 (3), March - 2016, pp. 320-324.

[6] Priyanka Jain and Rajendra Singh Yadav, "A Comparative Study of Different Generations of Communication Networks," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Special Issue 3, November 2016.

[7] E. Biham & O. Dunkelman, "Cryptanalysis of the A5/1 GSM stream cipher," In Indocrypt'00., 2000.

[8] B. Debraize and I. M. Corbella, "Fault analysis of the stream cipher snow 3G," in Fault Diagnosis and Tolerance in Cryptography - Proceedings of the 6th International Workshop, FDTC 2009, pp. 103–110.

[9] S. Traboulsi, N. Pohl, J. Hausner, A. Bilgic, and V. Frascolla, "Power analysis and optimization of the ZUC stream cipher for LTE- Advanced mobile terminals," in 2012 IEEE 3rd Latin American Symposium on Circuits and Systems, LASCAS 2012 - Conference Proceedings.

[10] G. Orhanou, S. El Hajji, and Y. Bentaleb, "EPS AES-based confidentiality and integrity algorithms: Complexity study," in International Conference on Multimedia Computing and Systems - Proceedings, 2011.

[11] M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, "Breaking the GSM A5/1 cryptography algorithm with rainbow Tables and high-end FPGAs," in Proceedings - 22nd International Conference on Field Programmable Logic and Applications, FPL 2012, pp. 747–753.

[12] R. Anderson, "A5 (was: Hacking digital phones) ," Newsgroup Communication, 1994.

[13] J. Golic, "Cryptanalysis of alleged A5 stream cipher," In Eurocrypt'97, pp. 239-255, 1997.

[14] A. Mahalanobis and J. Shah, "An Improved Guess-and-Determine Attack on the A5 / 1 Stream Cipher," Journal of Computer and Information Science, vol. 7, no. 1, pp. 115–124, 2014.

[15] ETSI/SAGE, "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2," Document 2: SNOW 3G Specification, version 10.0.0, 2011.

[16] Biryukov, Priemuth-Schmid and Zhang, "Differential Resynchronization Attacks on Reduced Round SNOW 3G," ICETE 2010, CCIS 222, pp. 147–157, 2012.

[17] P. Kitsos, et al., "An FPGA Implementation of the ZUC Stream Cipher," 14th Euromicro conference on Digital System Design (DSD 2011), Oulu, Finland, Sep. 2011.

[18] N. T. Courtois and W. Meier, "Algebraic Attacks on Stream Ciphers with Linear Feedback," In E. Biham, editor, Advances in cryptology EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science, pages 345 - 359, 2003.

[19] M. Al Mashrafi, "A different algebraic analysis of the ZUC stream cipher," In Proceedings of the 4th International Conference on Security of Information and Networks, ACM, Macquarie Graduate School of Management, Sydney, NSW, pp. 191-198, 2011.

[20] G. ORHANOU, S. EL HAJJI, Y. BENTALEB and J. LAASSIRI, "EPS Confidentiality and Integrity mechanisms Algorithmic Approach," IJCSI, International Journal of Computer Science Issues, Vol. 7, Issue 4, No 4, July 2010.

[21] Huseyin Demirci and Ali Aydin Selcuk, "A meet-in-the-middle attack on 8-round AES," In FSE'08, volume 5086 of Lecture Notes in Computer Science, pages 116–126, 2008.

[22] Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva, "Bicliques for preimages: attacks on Skein-512 and the SHA-2 family," Available at http://eprint.iacr.org/2011/286.pdf, 2011.

[23] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES," ASIACRYPT 2011, pp. 344-371, 2011.