Design hybrid encryption system based on E0 algorithm and A5/3 algorithm in the encryption process

[1]Nibras Hadi Jawad, [2]Sameer Hameed Abdulshaheed Muosaa

1University of Al-Qadisiyah - College of Education- Al-Qadisiyah- Iraq/nibras.hadi@qu.edu.iq

2 Technical University of Al-Furat Al-Awsat - Engineering Technical College-Najaf/sameer.h.sh@etcn.edu.iq

Received:- 13/12/2016 Accepted:-31/1/2017

Abstract

The purpose of this paper is to create the safer hybrid system ,the more secure and fast , by the merge A5/3 algorithm with E0 algorithm, so as to produce bluetooth algorithm relies on block cipher. Some modifications were done on both algorithms in order to correspond the work of each algorithm with other, that would speed up the labor of the algorithm in the calculation of the total time-spent and increases the complexity, which increases in the algorithm security.

Key word: Simulation, E0, A5/3 algorithms, hybrid, SIMULINK.,kasumi

Physical Classification QA75.- 76.95

.

1. Introduction

In communications, GSM networks are relying on the A5/X algorithm in the telecommunications and data transmitted encryption process[1] [2], A5/X algorithm in the first issue have been adopted on the principle of stream cipher producing single bit at a time where it developed in subsequent releases to rely on block cipher with work the principle of stream cipher, which produces 228 bits at a time, with the increase in execution time a bit, but with the general account the percentage of time with production between release first ratio and the third, we find that the general rate of client time with the quantity of bits delivered much better in the third form of the discharge the first [3]. A5/3 depends on the kasumi encryption algorithm; it is a block system based on the work entrances key size of 128-bit and 64-bit data size, it comes as a result of counter blocks calculation algorithm[4]. E0 algorithm based on the principle stream cipher and contains a total of four registers which is 128, in addition to its based on the complexity mechanism to complex the output registered [5].

We propose a hybrid algorithm relies in its work on mixing A5/3 algorithm and E0 algorithm, so as to produce Bluetooth algorithm relies on block cipher that would speed up the job of the algorithms and increment the algorithm complexity and the difficulty of breaking it.

The order of This paper is as follows. In section2 the Literature review was given. In section3 what is the A5/3 algorithm and E0 algorithm. In section4 simulation the implementation of the A5/3 and E0 . In section5 description of proposed system. In section6 results analysis was given with using "statistical test" and section7 the important conclusion and future work.

2. Literature review

- **Kitsos P., at el…. (2004)** [6] presented in this paper hardware implementations of the 64-bit kasumi block cipher. The proposed usage bolster both encryption and decryption operation opposed to the previously published executions. Two different VLSI usage (the first uses pipeline technique, and the second uses feedback logic). By using internal round and external round pipelining technique significant throughput improvement is accomplished. The main accomplishes throughput value equivalent to 3584 Mbps at 56 MHz, and the second accomplishes throughput 432 Mbps at 54 MHz.
- **Vrentzos E., at el…. (2006)** [7] in this paper presented a VLSI parameterized implementation that applies in both A5/3 & A5/4 encryption algorithms. The fundamental preferred standpoint of the proposed execution is that backings variable key length from 64 to 128 bits. the external key length input In case A5/3 has 64 bits while in the key length of the A5/4 is 128 bits. The other awesome favorable position of the proposed execution is the lessening of region. It gives adaptability as it can be utilized as a part of numerous applications with any key length from 64 to 128 piece. The proposed framework achieves a data throughpout up to 166Mbps in a maximium frequency of 130MHz.
- **Rasmi P S, Varghese P. (2011)** [8] present a " hybrid cryptographic system" that joins both the "symmetric key algorithm", which utilizes the properties of a circle and asymmetric key algorithm of RSA with CRT. The asymmetric algorithm is RSA with CRT which improves the performance of the essential RSA

- **Sean L. , at el…. (2012)** [9] provides new step in proposed algorithm to avoid the weak, used some famous algorithms to encrypt a data. created new algorithm to provide security issue and time constraint of operation then combine AES using multiplexing of keys, Improvement in DES key size and blowfish algorithm. present both the encryption and decryption that supports in real time application.
- **Ravindra Kumar Gupta, Parvinder Singh (2013)** [10] a new hybrid concept is proposed by analyzing the principle of the hybrid cryptography based on the combination of symmetric and message digesting. In proposed concept designed a new symmetric encryption algorithm and combine with SHA-1 message digesting function to provide hybrid nature. the proposed system will try to improve exiting problem. In proposed system symmetric key will use series of logical functions like xor function, circular Shift (Right, Left), Feastel function and these operations are time efficient operation as compared to mathematical operation for providing confidentiality and authentication.
- **Komal R., at el…. (2013)** [11] proposed a hybrid encryption algorithm based on "AES and RSA" to enhance the security of data transmission in "Bluetooth communication E0". In the proposed hybrid encryption algorithm, instead of the" E0 encryption", "AES algorithm", known for of its higher efficiency in block encryption is used for data transmission and "RSA algorithm "is used for the encryption of the AES key due to its key management advantages. Thus the dual protection using "AES and RSA algorithm "will make the data transmission using Bluetooth more secure. And, the hybrid encryption algorithm provides a very easy and convenient technique for the encryption of transmitted data.
- **Prakash K. , Saeed Q. (2014)** [12] This research study proposes Hybrid Encryption System using new public key algorithm and private key algorithm. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. propose a provably two way secured data encryption framework. This framework has two diverse encryption encryption algorithms have been used both in the Encryption and decryption sequence.

3. The A5/3 algorithm and E0

A5/3 encryption algorithm is a binary key stream generator [13] [14] which used to encryption and decryption blocks of data under (confidentiality key or security key) KC [15] for conversations on GSM mobile phons. Its structure is very fast doing and based on the "kasumi algorithm" [16]. kasumi is a block cipher that produce a" 64 bits output" from a "64 bits input" under the control of a "128 bits key" [14]. These algorithms use kasumi in a form of output feedback mode as a key stream generator, the inputs to the algorithm are given from count number (22 bits) and Kc (64 bits). The output from the "GSM A5/3 algorithm " is twice of "114 bits" (namely two blocks) key stream strings, one is used for "uplink encryption / decryption" and the other is used for "downlink encryption / decryption"[14]. The definition of the function is by mapping the "GSM A5/3" inputs onto the inputs of the "core function KGCORE" and mapping the output of "KGCORE" onto the outputs of "GSM A5/3".

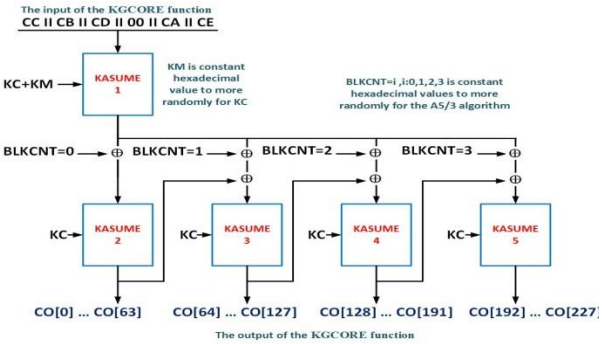
The define of the input [13] :

"CA[0]..CA[7] = (0 0 0 0 1 1 1 1)"
"CB[0]..CB [4] = (0 0 0 0 0)"
"CC[0]..CC [9] = (0 0 0 0 0 0 0 0 0 0)"
"CC[10]..CC[31]=(COUNT[0]..COUNT[21])""
CD[0] = (0)"
"CE[0]..CE[15] =(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)"
"CKi[0]..CKi[KLN-1] =(KC[0] ⊕KM[0]….
KC[KLN-1] ⊕KM[KLN-1])"
"Length = 228" Apply "KGCORE" to these inputs to derive the "output CO[0]..CO[227]".

The define of the output:

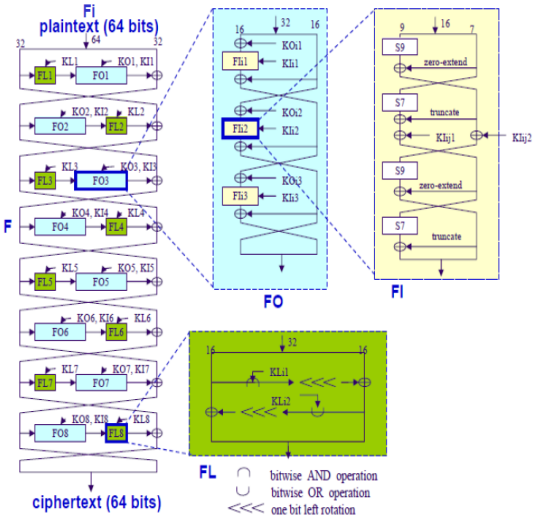
"Block1[0]..Block1[113]=(CO[0]…CO[113])"
"Block2[0]..Block2[113]=(CO[114]…CO[22)"

Illustrate the "diagram of A5/3", look in the Fig. (1).



Figure(1). the diagram of A5/3 generator

a. **"Kasumi** is a block cipher produces a 64 bits" output taken from a "64 bits" inpuot working under the control of a "128 bits key". festal cipher used in this algorithm with "8 rounds" with associaeted subkeys "(KL, KI and KO) of CK". It operates on a "64 bits" data block and uses a "128 bits key" [17]. Its "8 rounds" are shown in Figure (2). Each" kasumi" operator uses" FL and FO funections". In each odd round of kasumi operator uses" Ri=FO(FL(Li1, KLi), KOi, KIi)" function and for each even round uses "Ri=FL(FO(Li1, KOi, KIi), KLi)". The "FL and FO algorithms" based on no. of iteration round with substitutions "S.Boxes" [13]. Illustrate the component of kasumi, see in Fig. (2).



Figure(2). the component of kasumi

b. **E0**: The bluetooth E 0 algorithm is a special case of a combination generator . It consists of four LFSRs; the total length is "128 bits" ,and a "nonlinear combiner function" with "four bits memory" . In the manufacturing process an initial key is stored into the Bluetooth chip. The four LFSR and the four memory bits are initializid by the key, an address , a " random number and clockiing bits". The purpose of the "clocking bits" is to guarantee that the system cannot be run many times with the same initialezation to reveal the bits of the key [18].

4. Simulation of A5/3 and E0

We had previously simulated two algorithms separately in previous research [19] [20] , This is a brief explanation of the simulation process:

a. SIMULINK [21] is used in the simulation of all component of "A5/3" In the simulation process of "A5/3 algorithm" and no code was used in the simulation process but only blocks in SIMULINK.

The simulation process of A5/3 algorithm divided to two levels, first level is simulation of kasumi algorithm which it consists of four sections, each section was simulated and then assembled all the

sections to produce kasumi algorithm. the second level is simulation of A5/3 algorithm using kasumi algorithm which was simulated in the first level.

In the Figure (3) shows the simulation of A5/3 algorithm using SIMULINK , and we note that the input to the A5/3 algorithm depends on two of the subsystem blokes, the first subsystem block is relating to the inputs KGCORE function, , the second subsystem block (KC+KM) is relating to the input of cipher key KC mixed with the KM to increase the random of the KC, these inputs will depend on kasumi algorithm in terms of its work it will give values to the private block kasumi, to continue link algorithm using five blocks from kasumi algorithm. The output of A5/3 algorithm is divided to blokes with same size and the values that we have obtained from the output stored in a separate two blokes of files. When run a simulation as mentioned above , A5/3 algorithm will give two blocks with length 114 bits for each block in the same time, With the variables used in the simulation encryption algorithm were stable, in terms of inputs (Kc, Cn).

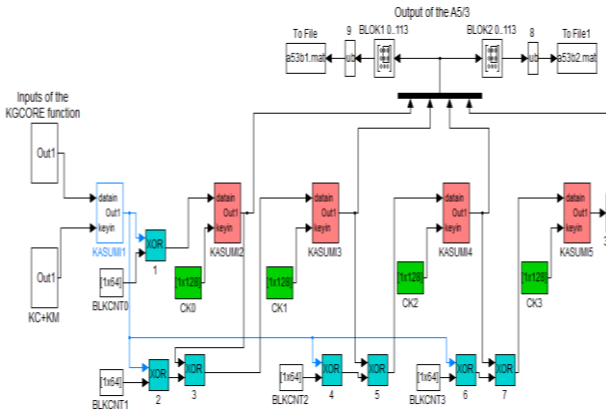


Figure (3). simulation of A5/3 algorithm.

b. Simulate of E0 with used SIMULINK divided into two levels, first level is simulation of registers which it consists of four registers. The second level is simulation of subsystem Ct , mixing the output of two levels to produce the output of Zt.

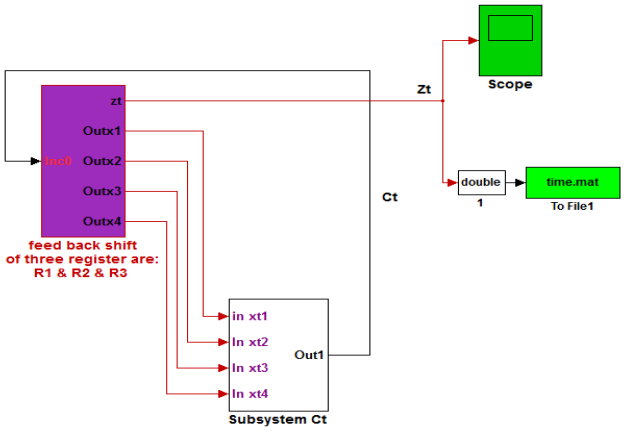
5. The Proposed System

Take advantages of the previous works and the efforts that have been made in the Bluetooth algorithm as part of a new framework**,** we have proposed work hybrid algorithm depends in its work on the mixing of A5/3 algorithm and E0 algorithm, so as to produce an Bluetooth algorithm operating principle of block cipher to give a stronger and faster key than the original design, the output key will be much more complex than the output key from the original algorithms.

Construction depends on the original algorithms with the addition of some modifications and changes in two algorithms to adapt work with each other, so as every algorithm has its own style and characteristic work.

The proposed algorithm is to two parts:

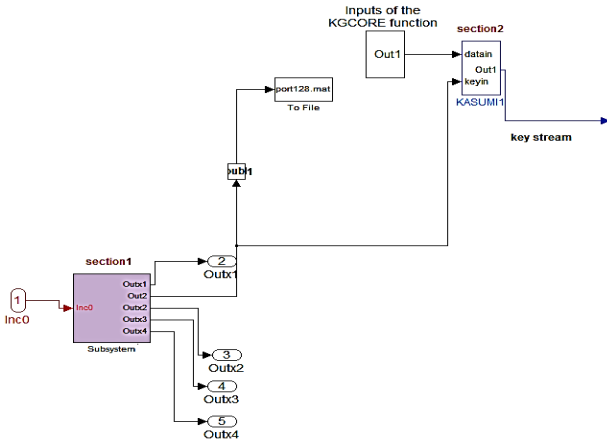
1. The "first part" relating to the geniration of the encryption key, which in turn is composed of two sections, see in fig.(4)**:**



Figure(4): proposed system

A- partial system that contains four recorders, which are input value comes from the second part subsystem Ct to increase complexity, which mixes with the recorders randomly, giving the initial value of the four recorders, will be directed by this section is 128 bits to be the

entrance to the section of the second, see in fig.(5).



Figure(5):feedback shift register and kasumi

B- The second section consisting of Kasumi algorithm taken from the algorithm A5/3, based on the two entrances: the first comes from the first section of the output, and the second comes from KGCORE function which is a function giving the 64-bit key series depends upon the algorithm in its work, then you'll make another accounts to the key to complex the resulting key largely, producing a block of 228-bit key size, see in fig.(5).

2. The second part subsystem Ct is a complex part, and that is not changing anything of its work, which produces one bit mixed with the first section in the first part with any regesters, see in fig.(4).

6. Results

In this section explain , after implementation of hybrid algorithm with statistical Tests Suite [22] [23].

The results that we have obtained very good and acceptable by using the "statistical tests", the results appear all within the specified domain, For a "significance level of = 0:05". Developed case is non-linear because the key stream generated for all cases the no. of zeros is not equal to the no. of one depending on the "frequency test". The results of random are good.

We have been generating 1000 blocks each one have 228 bits to measure execution time, It is shown that the times of execution hybrid algorithm is ≈ 0.13second, comparison with execution time of each algorithm separately , the execution time of A5/3 is 4 second and the execution time of E0 is 0.2 second, you can see the difference between them.

The tests were to generated key output is generally 128-bit in block , as shown in table (1), in "column Time of computation", the entropy in the hybrid algorithm is good with value 0.0432 , as shown in Table (1), in "column Entropy test". It is noted that all the results of hybrid algorithm the cryptography randomness are good, as shown in Table (1), so hybrid algorithm can be adopted in bluetooth.

Table (1): results of tests

Key length	128
Time of computation	≈ 0.13
Entropy test	0.0432
Binary matrix rank	65
Run test	3.2256
Autocorrelation test	0.5156
Frequency test	3.1250
Serial test	3.3868
Poker test	6.3810

7. Conclusion

A5/3 key stream generated is very fast, easy to implement and also efficient "encryption algorithm" used in communication of developed "GSM networks". E0 a wireless communication technology designed to exchange data over short distances at low power consumption. By integrating two algorithms, we were able to configure a hybrid algorithm operates on the bluetooth data encryption, and it's done on SIMULINK under "MATLAB (R2013a)"

as result obtained in form of graph. We just continue in the use of SIMULINK that become of our experience to use, open ideas and good results obtained from the use of SIMULINK. The hybrid algorithm structure has been easy to implement and fast to do. This paper proposes a high speed , minimum cost hybridkey block algorithms and produce deferent values for each block generated in each time.

We achieved a high speed in generating , production of 128 bit by depending on first block and generation of 128 blocks by depending on the last block for better complexion by comparing the results of the our system with systems " A5/3 algorithm and E0 algorithm" separately.

8. References

1- Magnus G., Kristian H., Espen H. ***Decoding GSM*. Master of Science in Communication Technology**; 2010.

2- Lachu A., Stefano F., Risto M. , Basavaraj P. , Yousuf S. , Sarvesh S. , Srinivas S. ***Getting to Know Wireless Networks and Technology***; 2003.

3- Yu L. ***short Message Service (SMS) Security Solution for Mobile Devices;*** M.Sc. thesis, Naval Postgraduate School, Monterey, California; 2006.

4- Elad B. , Eli B. ***Instant cipher text-only cryptanalysis of GSM encrypted communication.*** citeseerx library; 2004.

5- Panse T. , Kapoor V.***, A Review on Security Mechanism of Bluetooth Communication ,*** International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (2) , 3419-3422 , 2012 .

6- Kitsos P., Galanis M. D. and Koufopavlou O.. "***High-Speed Hardware Implementations of the KASUMI Block Cipher"***, in Proc. of the 2004 IEEE International Symposium on Circuit and Systems ISCAS'04, 2004.

7- Vrentzos E., Kostopoulos G. and Koufopavlou O.. ***Hardware Implementation Of The A5/3 & A5/4 Gsm Encryption Algorithms***; Published by Conference WAC 2006.

8- Rasmi P S, Varghese P. , ***A Hybrid Crypto System based on a new Circle -Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications*** International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011.

9- Sean L. , Karthik S. ,Saitheja K. , Abdel-shakour A. , ***Hybrid cryptography using symmetric key encryption;*** ResearchGate, 2012.

10- Ravindra Kumar Gupta, Parvinder Singh, ***A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network***, International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3), 2013.

11- Komal R., Nikita G., Pooja B., Sunil M. ***Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA***. International Journal of Computer Applications (0975 – 8887) Volume 71– No.22, June 2013.

12- Prakash K. , Saeed Q. ***Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm*** MIS Review Vol. 19, No. 2, March (2014).

13- ***Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Design and evaluation report.*** 3rd Generation Partnership Project, TR 55.919**.**

14- 3GPP TS 135.202 Version 7.0.0, ***3rd Generation Partnership Project; Specification of 3GPP confidentiality and integrity algorithms; 3G*** Security,KASUMI Specification, 2007.

15- Jay J., ***Matlab Simulation of Cryptographic Algorithm for mobile Communication***; Published by National conference on Emerging Trends in Information and Communication Technology, 2007.

16- Orr D., Nathan K., and Adi S. ***A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony***; Published by International Association for Cryptologic Research, 2010.

17- Kim H., Choi Y., Kim M.and Ryu H., ***Hardware Implementation of the 3GPP KASUMI Crypto Algorithm;*** in Proc. of

18- the 2002 International Technical

19- Conference on Circuits/Systems,

20- Computers and Communications ITC-CSCC-2002, 2002, pp. 317–320.

21- Bluetooth, S. I. G., ***Bluetooth Core Specification v4.0.*** ; 30 June 2010 Available at https:// www.bluetooth.org .

22- Nibras H. ***Improvement Stream Cipher Type A5/1 Using SIMULINK Environment***;Master of Science in computer Science, university of Babylon, 2014.

23- Sameer H. , ***Evaluation of Bluetooth Security Based on Fuzzy Logic Technique***; Master of Science in computer Science, university of Babylon, 2014.

24- MATLAB/ SIMULINK .***Simulink ® Getting Started Guide***; R2013b, 2013.

25- Dhilal M. ***Security Evaluation of Cryptosystem Based on Information Theory***. Master of Science in computer Science, university of Babylon; 2013.

26- Menezes A. and vanOorschot P., Vanstone S. ***Handbook of Applied Cryptography***; citeseerx library; 1997.

تصميم نظام تشفير هجين بالاعتماد على الخوارزمية A5 / 3 والخوارزمية E0 في عملية التشفير

[1] نبراس هادي جواد [2] سمير حميد عبد الشهيد

1 جامعة القادسية / كلية التربية / nibras.hadi@qu.edu.iq

2 جامعة الفرات الاوسط التقنية / الكلية التقنية الهندسية النجف / sameer.h.sh@etcn.edu.iq

تاريخ الاستلام:- 2016/12/13 تاريخ القبول :- 2017/1/31

الخلاصة

الغرض من هذا البحث هو اقتراح نظام هجين اكثر امنا، وذلك بدمج خوارزمية A5/3 مع خوارزمية E0 ، وذلك لتقديم خوارزمية بلوتوث تعمل بنظام التشفير الكتلي، وذلك باجراء التعديلات على كلا الخوارزميتين لكي يتلائم عمل كل خوارزمية مع الاخرى. سوف نحصل من هذا العمل على خوارزمية يكو ن معدل الوقت المستهلك بشكل عام اسرع من عمل الخوارزميتين كل على حدى ، اضافة الى زيادة تعقيد الخوارزمية مما يزيد من امنيتها.

الكلمات المفتاحية : المحاكاة، خوارزمية A5/3 و E0 ،الهجين، SIMULINL ، خوارزمية كاسومي.