Evaluation key generator of Multiple Asymmetric methods in Wireless Sensor Network (WSNs)

Evaluation key generator of Multiple Asymmetric methods in Wireless Sensor Network (WSNs)

Aseel Hamoud Hamza[1], Saif M. Kh. Al-Alak[2]

Department of Computer Science, College of Science for Women, University of Babylon, Hillah, Iraq

aseel.hamoud@uobabylon.edu.iq
saif.shareefy@gmail.com

Abstract. The wireless sensor network (WSNs) is constructed with a combination of the sensor nodes and the sink nodes. WSNs applied in many applications. The Security in WSNs is necessary because of limitations of storage, computing capacity, power use. Encryption is one of the most important tools utilized to supply the security services for WSNs. Asymmetric and symmetric encryption algorithm can be utilized in the WSNs structure to supply the security. The asymmetric key encryption algorithm gives a higher level of the security, but compared to symmetric key encryption, that causes extra sensor overhead. In this research KCMA method used to generate chains key of twelve experiments of the algorithms (ECC, RSA, ELGamal). These chains merged with hash function SHA2 and XOR. Diehard test was utilized in all experiments to evaluate the randomness of the secret key generated, and show it's more security system. SHA2 was the best as compared with XOR. Also, the work evaluated the performance (time) for the system and throughput network.

Keywords. ECC, RSA, ELGamal, WSNs, randomness, KCMA, SHA2.

1. Introduction

Sensor networks be composed of hundreds of self-organizing, low cost ,low power wireless nodes prevailed to observe the environment[1]. Sensor nodes capture information from an environment, process data and transfer it over radio signals. In sensitive WSNs applications like as enemy line monitoring or border area surveillance, the security protocols that supply confidential data transfer from sensor nodes to the base station should be utilized. However, the low processor and radio capabilities of the sensor nodes do not permit for the application of the traditional security protocols in the sensor networks [2]. The security is generally accomplished through encryption in WSNs. Encryption protects data through encryption and decryption. It composes of two classes: asymmetric and symmetric encryption, where one key is utilized to achieve the security process in the symmetric method and to various keys are utilized in the asymmetric method. Several encryption algorithms are suggested for security. Encryption algorithms work with key creation that guarantees message confidentiality.

The last years have known about the evolution of novel, more energy-effective encryption algorithms and give the same security threshold as traditional algorithms like as RSA [3, 4]. The Elliptic Curve

Encryption (ECC) [10] is one of these novel algorithms and is the most promising in terms of energy and time consuming, making it very attractive for encrypting data in WSNs. The ECC provides equal security with smaller key sizes, providing memory, computational and energy for restricted wireless devices [4] [9]. On the other hand, Elgamal was developed in 1984 by Taher ElGamal. It is an asymmetric key technique-based D-H key interchange. ELGAMAL encoding can be described on any periodic group G. Security depends on G problem related to the calculation of discrete logarithms [4] [9]. The rapid generalized encryption of long messages and the rate of data extending have the biggest advantages of this technique . The prime restriction in ELGAMAL is a random condition and a slower speed [5] [2].

The security is a very important issue in the WSN, especially with the development of science and computers ,the researchers attempted to provide security by generating chains secret key, the randomness of these keys generated are low, so in this work suggested Key Chain Multiple Asymmetric (KCMA) method to increase randomness and improve the confidentiality of the system. The key chains generate through twelve experiments evaluate with Diehard test. The time and throughput network for the chains generated was calculated in the Java programming language. Also, the complexity of the algorithms is illustrated.

The rest of the paper as follows: The WSNs are explained in the Section 1. The related work is highlighted in the Section 2. The proposed research is explained in the Section 3. The Measures Metrics and result is illustrated in the Section 4. The complexity of an algorithm is explained in the section 5. And, the Section 6 concludes the paper.

2. Related work:

The work related to researchers who work in this field:

The search In [6], the research suggests an algorithm based on complementary subtraction 1 to represent numerical multiplication in numerical multiplication which provides a lower Hamming weight and significantly improves the computational efficiency of numerical multiplication .In this paper, used a hybrid cryptosystem asymmetric RSA and El-gamal algorithm , improve performance and the security will be relay on throughput and encryption time , decryption time [7]. This paper has shown increase the security system by using the protocol MKP which use two series of ECC algorithm to generate secret keys. It gives the authentication , since it has multiple key and work in parallel mode, that increase the throughput and the performance of the system ,and decrease the run-time, also it save the energy[8]. (Palanisamy and Chellappan 2011) suggested RSA -CRT technology is enhanced in secure routing and gives functional management of keys that use the best encryption / decryption to authenticate broadcast messages. The suggested technique will resist attacks on the WSN network layer and will minimize overhead for communications, and energy node consumption, and storage space [9].This paper [10] implemented ECC and RSA over Sun SPOTs . Its transmit the light reading, time and capacity of the available battery. Initially charged the battery, then computed time taken by every technique to discharge the battery to detect which technique exhausts minimal battery. In the same conditions RSA exhausts, power more than ECC. [11] in this paper used two system RSA and ECC,and discover that ECC is more suitable as compared to RSA, because of low CPU consuming, low memory use and shorter key size as compared to the RSA.

3. The Proposed Research:

The objective of the research is building a strong WSNs security system and improve the performance of the system. The work suggested a Key Chain of Multiple Asymmetric (KCMA) method. At first, the base station sends initial values (A0, B0) to the specific nodes for the purpose of utilizing them in the proposed method as shown in Figure no. (1). The base station encrypts initial values of the public key of each destination node before transferring.

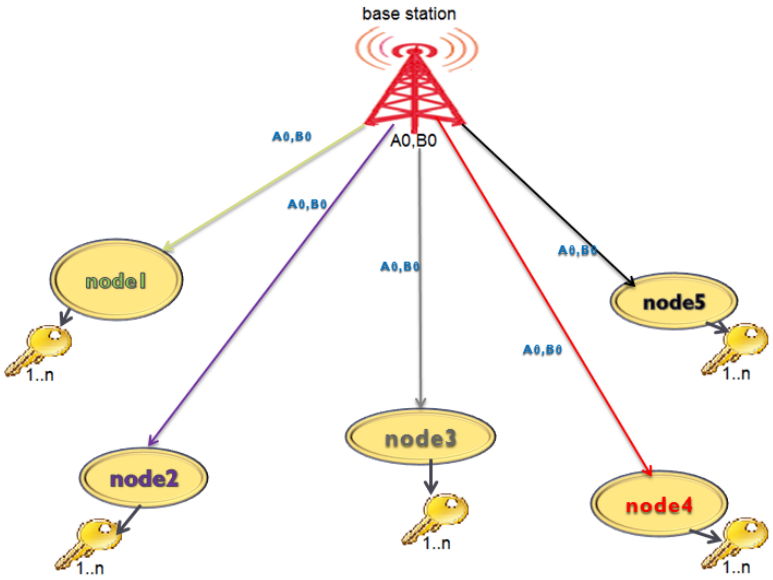


Figure 1. Base station generates public key to the nodes

The KCMA method uses the initial values (A0, B0) to generate two different chains off of the keys: A0, Al,..., A; B0,B1,...,Bm , as shown in fig no (2)

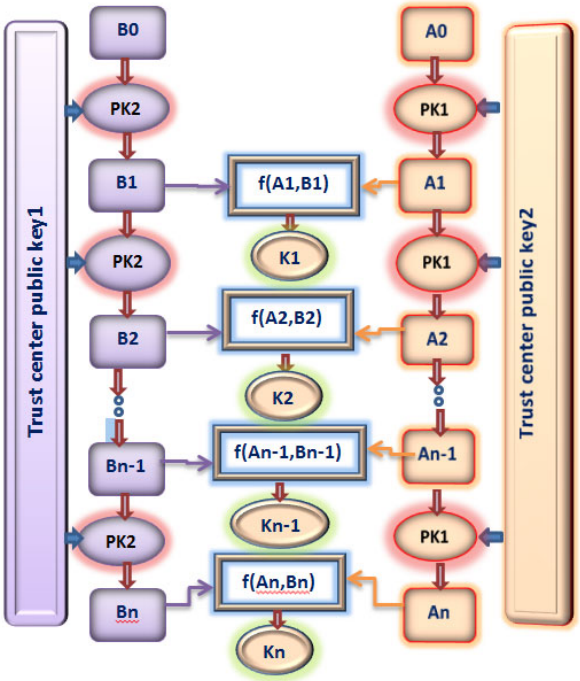


Figure 2. Diagram of the suggested KCMA method generates two chains of keys

To generate the elements in each chain, the asymmetric algorithms are used as in the following Eq.1 and Eq.2:

Ai=PK1en (TK1, Ai-1) (1) 0< I <n

Bi=PK2en (TK2, Bi-1) (2) 0< I <n

Where:

PK1en = the first algorithm, PK2en = the second algorithm.

TK1, TK2: trust center public keys that are different keys.
The keys are calculated using the hash function (f) as shown in the following Eq.3:
Keyi= f (Ai,Bi) (3) 1< i <n
Where F represents hash function XOR or SHA2

The algorithm (1) shows the suggested KCMA method with two group key generator model.

algorithm (1) : KCMA (two sets)

1. Input: Ai,Bi:key groups pk 1,pk2;created public keys
2. Output: Ki; proposed created keys
3. Begin
4. for i= 1 to n
5. Ai= PK1 (Ai-1,pk1)
6. Bi= PK2 (Bi-1,pk2)
7. Ki= f (Ai,Bi)
8. Endfor
9. End

4. Measured Metrics

This section demonstrated some important measures for the evaluation of the proposed KCMA method, this measure can be illustrated as follows:

4.1. Randomness test

The randomness of the output is one of the significant factors in measuring the security of any algorithm. The search implements diehard tests. Diehard (*develop by Marsaglia*) is a battery of statistical tests for measuring the quality of a random number generator. They include: (Birthday spacing's test, Overlapping 5-permutation test, Binary rank matrices test, Bitstream test, OPSO, OQSO & DNA test, Count-the-1's test, Parking lot test, Minimum distance test, 3D spheres test, Squeeze test, Overlapping sums test, Runs *test*, *Craps test)[12]* .These tests are p-values that dividing the range to three region : safe, doubt, and failure area. These regions can be defined by this following limits: $0.1 < p\text{-value} \leq 0.25$ or $0.75 \leq p > < 0.9$ lies in the Doubt region. $0 < p\text{-value} \leq 0.1$ or $0.9 \leq p\text{-value} \leq 1$ located in the failure region . $0.25 < p\text{-value} < 0.75$ located in a safe region [13].

4.2. The evaluation of the time generating

Java programming language (NetBeans IDE 8.2) is used to measure the performance (time) in millisecond for the chains generated by the twelve experiments that used in the proposed method. Five different keys (100,200,300,400,500), are used in computations. The charts of the figures and the comparison were done by using the Excel program. The experiments are done under Windows 7, Core 7,… CPU =2.80GH, Memory=4096MB RAM.

4.3. Network throughput

Throughput is the amount of the data transferred in a unit of the time. Moreover, the node throughput is the rate of the data transported through the simulation time as described in Eq. (4). The throughput network is the throughput rate of all nodes on the number of the nodes as shown in Eq. (5) [14]

$$T\_N = Data/Time \ldots (4)$$

Where T_N: the node's throughput, Data: the amount of the transferred data, and Time: the time simulation.

$$T\_Net = \Sigma\, T\_Ni \,/\, No\_Node,\ No\_Node \leq i \geq 1 \ldots . (5)$$

Where T_Net: network throughput, T_Ni: node's throughput, and No_Node: number of nodes.

5. The Result of the test:

5.1. Randomness test

The test was performed on the twelve experiments of the asymmetric method described in the following table (1).

Table 1. the twelve experiments of the asymmetric method

No	Exper.1	Exper.2	FUNCTION	
			XOR	SHA2
1	ECC1	ECC2	TWOECC_XOR	TWOECC_SHA2
2	RSA1	RSA2	TWORSA_XOR	TWORSA_SHA2
3	ELGamal1	ELGamal2	TwoELGamal _XOR	TwoELGamal _SHA2
4	ECC	RSA	ECC_RSA_XOR	ECC_RSA_SHA2
5	ECC	ELGamal	ECC_ELGamal_XOR	ECC_ELGamal_SHA2
6	RSA	ELGamal	RSA_ ELGamal_XOR	RSA_ ELGamal_SHA2

The work file that size (11) MB was used as a measure to test the randomness of suggested research. The randomness of the twelve experiments is illustrated in Figures below:

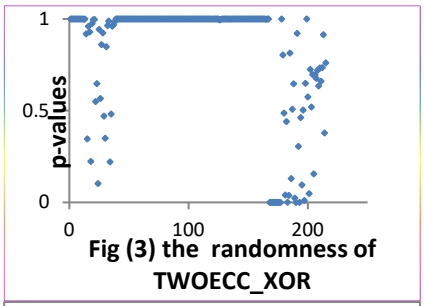


Fig (3) the randomness of TWOECC_XOR

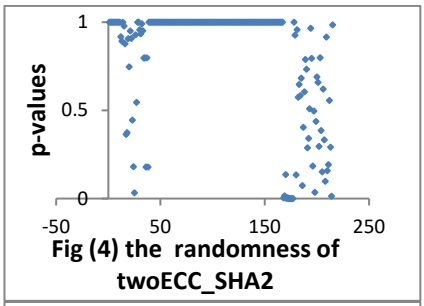


Fig (4) the randomness of twoECC_SHA2

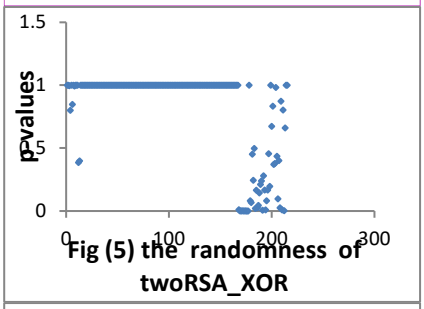


Fig (5) the randomness of twoRSA_XOR

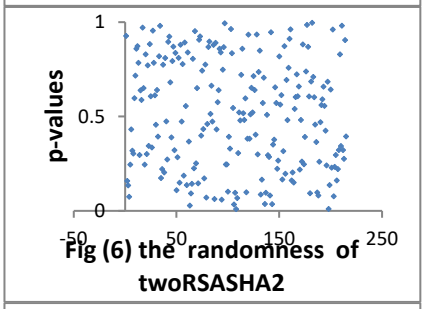


Fig (6) the randomness of twoRSASHA2

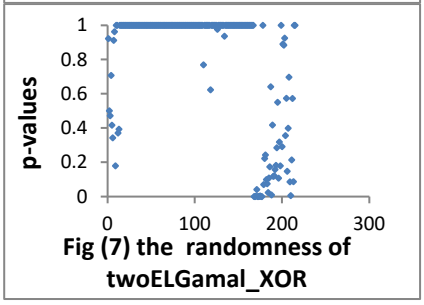


Fig (7) the randomness of twoELGamal_XOR

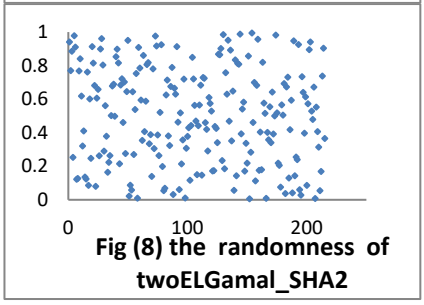


Fig (8) the randomness of twoELGamal_SHA2

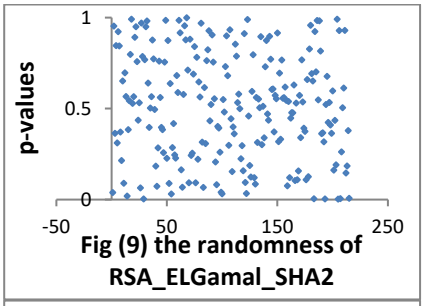


Fig (9) the randomness of RSA_ELGamal_SHA2

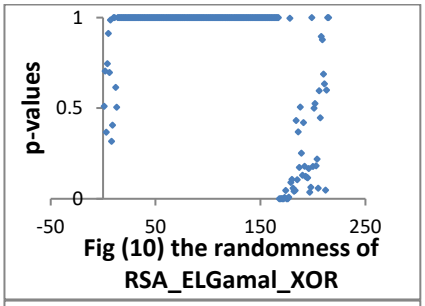


Fig (10) the randomness of RSA_ELGamal_XOR

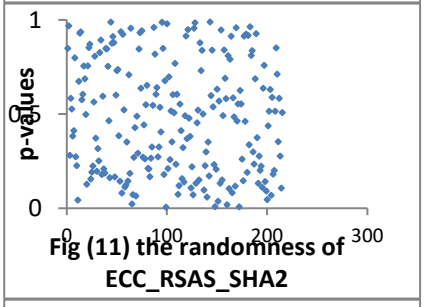


Fig (11) the randomness of ECC_RSAS_SHA2

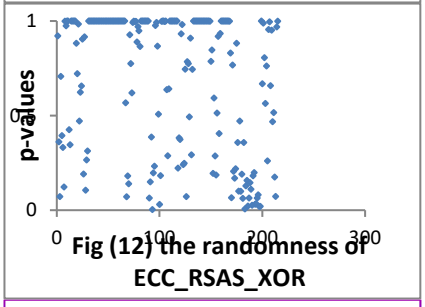


Fig (12) the randomness of ECC_RSAS_XOR

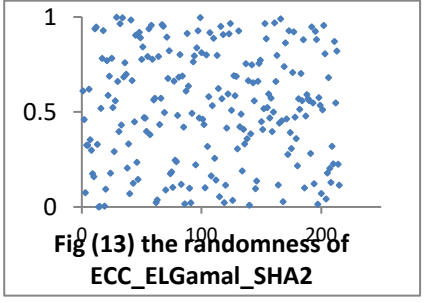


Fig (13) the randomness of ECC_ELGamal_SHA2

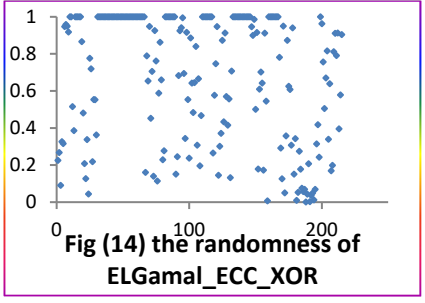
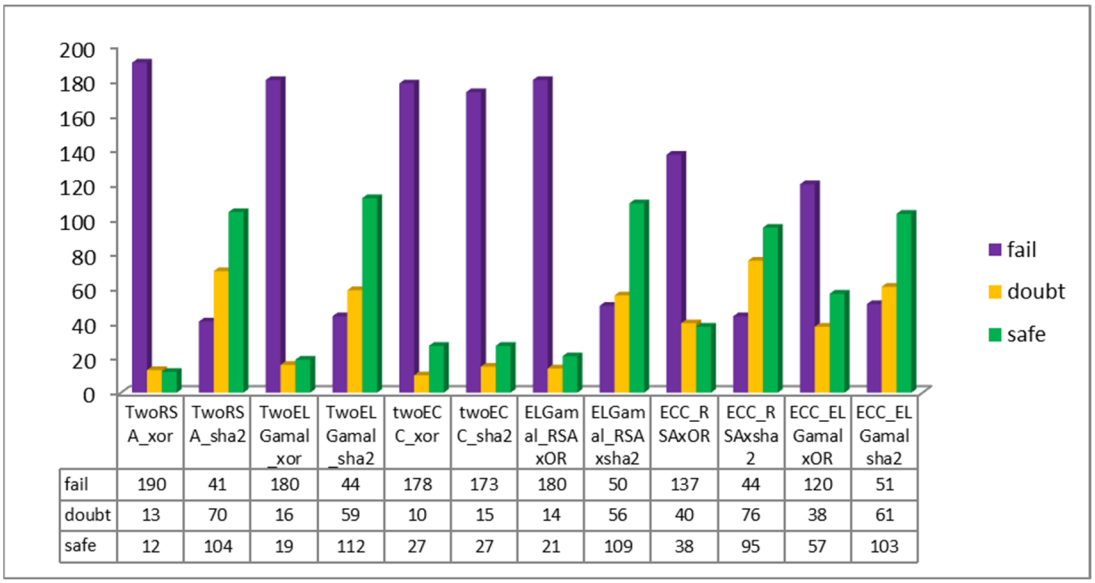


Fig (14) the randomness of ELGamal_ECC_XOR



	TwoRSA_xor	TwoRSA_sha2	TwoELGamal_xor	TwoELGamal_sha2	twoECC_xor	twoECC_sha2	ELGamal_RSAxOR	ELGamal_RSAxsha2	ECC_RSAxOR	ECC_RSAxsha2	ECC_ELGamalxOR	ECC_ELGamalsha2
fail	190	41	180	44	178	173	180	50	137	44	120	51
doubt	13	70	16	59	10	15	14	56	40	76	38	61
safe	12	104	19	112	27	27	21	109	38	95	57	103

Figure 15. p-value of twelve experiments

It is clear from the figure the p-value safe increase when using the SHA2, therefore it is outperformed in achieving the security with the comparison to XOR, and the (TwoRSA_SHA2, TwoELGamal_SHA2, ELGAMAL_RSA_SHA2, ECC_RSA_SHA2, ECC_ELGamal_SHA2") were the highest security levels of the experiments.

5.2. Time generating of the ECC methods

To calculate the time in five cases of the key (100,200,300,400,500), when using two ECC _XOR, it consumes the longer time of use it with SHA2, the time consumption of ECC_RSA and ECC_ELGamal when used them with XOR spent more time when used them with SHA2, but ECC_ELGamal is the least time consuming, as shown in Figure No. (16).

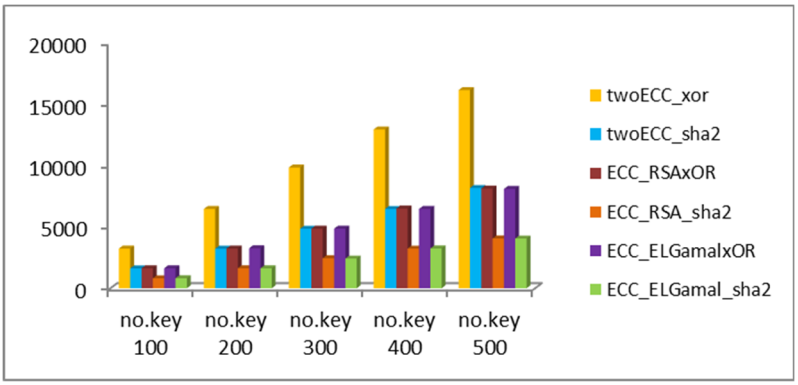


Figure 16. The time generating of the ECC methods

5.3. Time generating of the RSA methods

In the five cases of no. of the keys (100,200,300,400,500), we notice that the use of TwoRSA with XOR takes longer time than when used with SHA2, as well as ELGamal_RSA _ XOR consume time more than four ELGamal_RSA _ SHA2, as shown in the figure no. (17).

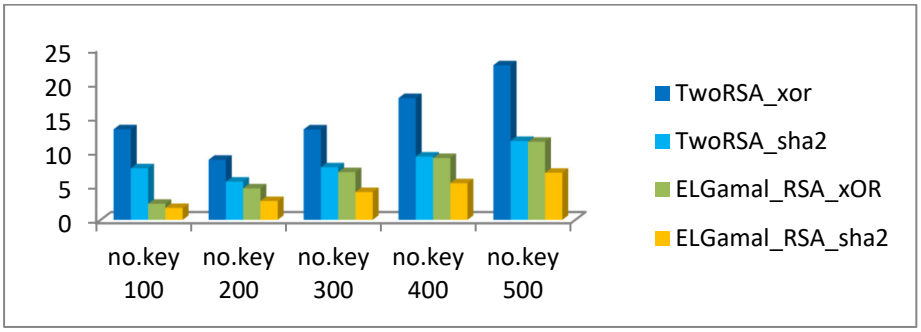


Figure 17. The time generating of the RSA methods

5.4. Time generating of the ELGamal methods

From the figure no. (18) below, we have shown in the five statuses of the number of keys (100,200,300,400,500) that TwoELGamal_XOR is less time consumption than TwoELGamal_SHA2.

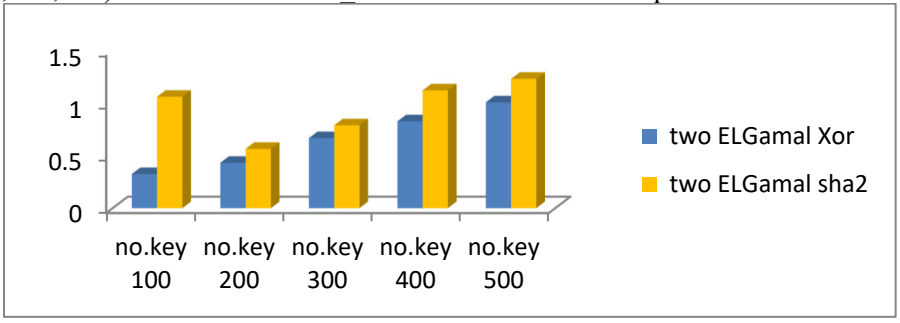


Figure 18. the time generating of the ELGamal methods

5.5. Throughput of the ECC based KCMA methods

From the figure (19), to measure throughput of five keys (100,200,300,400,500), the chart illustrates the high throughput network in the key (100), and network's throughput is less in the key number (500). The ECC_ELGAMAL_SHA2 is higher throughput, and TwoECC_XOR is a lower throughput network in this chart.

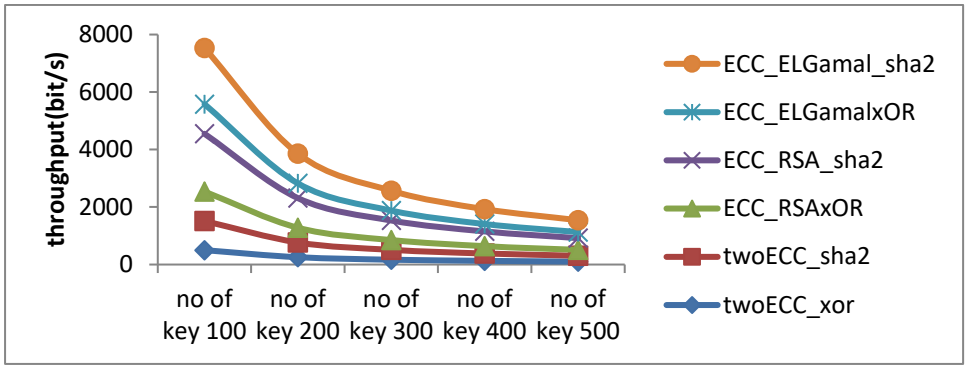


Figure 19. the throughput network of ECC

5.6. Throughput of the RSA based KCMA methods

The throughput of RSA based KCMA method of number keys (100,200,300,400,500), from chart, notice the number of keys (500) is less throughput than the number of keys (100). The method TwoRSA_XOR is a high throughput network, and TwoRSA_SHA2 is the least throughput of this the chart. As shown in figure no. (20)

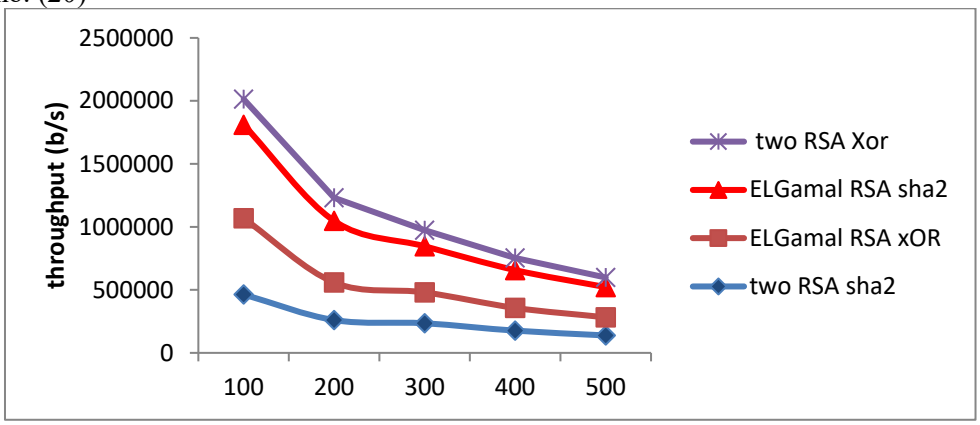


Figure 20. Throughput of the RSA based KCMA methods

5.7. Throughput of the ELGamal based KCMA methods

The throughput of Two_ELGamal_XOR is less than Two_ELGamal_SHA2, as shown in a figure no. (21).

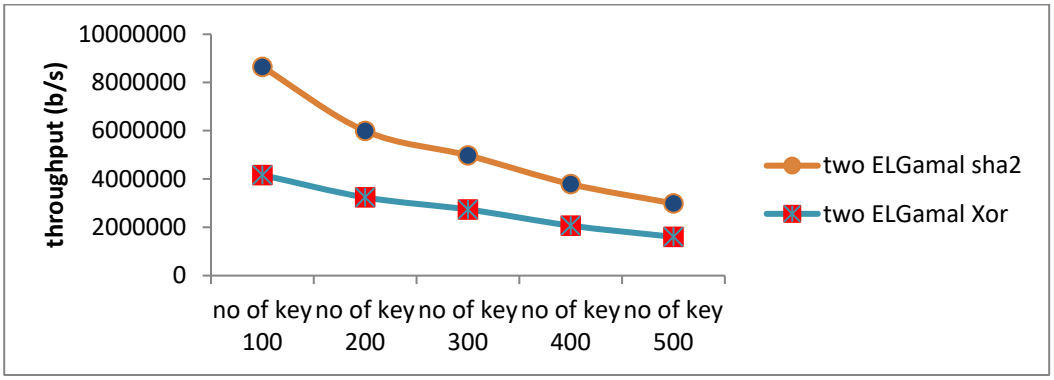


Figure 21. Throughput of the ELGamal based KCMA methods

6. Time Complexity

Time complexity is a mathematical complexity that describes the amount of the time it gets to run an algorithm. The complexity of the algorithm is classified according to the kind of function that appears in the large notation (O). For instance, a time complexity algorithm is linear time algorithm and a time complexity algorithm for constant is polynomial algorithm [15]. The problems of integer factorization of algorithm RSA permit algorithms which run in sub-exponential time [16]. according to [17]complexity of RSA refer to is (o(log(n)3)). With regard to El-Gamal encryption system is based on the discrete logarithm problem at Zp*,. It is necessary that different random integers k be utilized to encrypt various messages[18]. The time complexity of El-Gamal cryptosystem is (o(log(n)3) [17]. The complexity of ECC "difficult to break it" is equal to resolving problem of the discrete logarithm. Find discrete logarithm of one item in elliptic will not help locate the logarithm of any another item[19]. The time complexity of ECC is equal to(o√n)[20].

7. Conclusion

Security is one of the most difficult problems in WSNs. In this research, the KCMA method has been proposed to generate a key chain of asymmetrical algorithms. These chains generated from two different algorithms combined with hash function SHA2 and XOR, then it have been tested by Diehard Test, the results shown the randomness increased by using the SHA2, so the system is confidential and secure, as demonstrated by the test the highest security methods were (TwoRSA_SHA2, TwoELGamal_SHA2, RSA_ELGAMAL_SHA2, ECC_RSA_SHA2, ECC_ELGamal_sha2). The time was calculated in the Java language for the generated keys and, shown that the method which used less time consuming were (ECC_RSA_SHA2, ECC_ELGamal_ SHA2, ELGamal_RSA_SHA2, ECC_RSA_SHA2, TwoELGamal_XOR). SHA2 is the best in terms of security and time consumption. The complexity of the RSA and Elgamal were o(log(n)3, and ECC is o√n.

References

[1] Sebastiano, F., L.J. Breems, and K.A. Makinwa, Fully Integrated Radios for Wireless Sensor Networks, in Mobility-based Time References for Wireless Sensor Networks. 2013, Springer. p. 7-37.
[2] Oswald, E., Introduction to elliptic curve cryptography. Institute for Applied Information Processing and Communication, Graz University Technology, 2002.
[3] Gura, N., et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. in International workshop on cryptographic hardware and embedded systems. 2004: Springer.
[4] Wander, A.S., et al. Energy analysis of public-key cryptography for wireless sensor networks. in Third IEEE international conference on pervasive computing and communications. 2005: IEEE.
[5] Shetty, A., K. Shravya, and K. Krithika, A review on asymmetric cryptography RSA and ElGamal algorithm. Int. J. Innovative Res. Comput. Commun. Eng, 2014. 2(5): p. 98-105.

[6] Huang, X., P. Shah, and D. Sharma. Fast algorithm in ECC for wireless sensor network. in Proceedings of the International MultiConference of Engineers and Computer Scientists. 2010.
[7] Patila, R. and V. Kulkarnib, Hybrid Cryptosystem Approach for secure communication. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, 2016: p. 2278-0661.
[8] Al-alak, S., et al., Aes and ecc mixed for zigbee wireless sensor security. computing, 2011. 1: p. 5.
[9] Palanisamy, K., Authenticated broadcast in heterogeneous wireless sensor networks using Chinese remainder theorem algorithm. Journal of Computer Science, 2011. 7(6): p. 849.
[10] Kaur, A., Energy analysis of wireless sensor networks using rsa and ecc encryption method. International Journal of Scientific & Engineering Research, 2013. 4(5): p. 2212.
[11] Eberle, H., et al. A public-key cryptographic processor for RSA and ECC. in Proceedings. 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2004. 2004: IEEE.
[12] Test, R., https://embeddedsw.net/Randomness_Test_Home.html.
[13] Alani, M.M., Testing randomness in ciphertext of block-ciphers using DieHard tests. Int. J. Comput. Sci. Netw. Secur, 2010. 10(4): p. 53-57.
[14] Al-Alak, S., Sowing Seeds Protocol based Key Distribution for Wireless Sensor Network. International Journal of Applied Engineering Research, 2017. 12(24): p. 14882-14888.
[15] Wikipedia, https://en.wikipedia.org/wiki/Time_complexity.
[16] Torres, I., Elliptical curve cryptography-segurança e privacidade em sistemas de armazenamento e transporte de dados. 2007, junho.
[17] HAMAD, S.S. and A. SAGHEER, PUBLIC KEY FULLY HOMOMORPHIC ENCRYPTION. Journal of Theoretical & Applied Information Technology, 2018. 96(7).
[18] Meier, A.V., The elgamal cryptosystem. 2005, June.
[19] Al-Saffar, N.H. and M.R.M. Said, On the Mathematical Complexity and the Time Implementation of Proposed Variants of Elliptic Curves Cryptosystems. International Journal of Cryptology Research, 2013. 4(1): p. 42-54.
[20] Eshghi, F. and A. Zamani, Security Enhancement of Wireless Sensor Networks: A Hybrid Efficient Encryption Algorithm Approach. Information Systems & Telecommunication: p. 177.