Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3239–3248
DOI : 10.47974/JDMSC-2811

Mathematical modeling and security analysis of a lightweight cryptographic encryption algorithm for resource-constrained IoT devices

Ramesh Kumar [@]
Department of Electronics & Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Satya Narayan [†]
Department of Computer Science and Engineering
Engineering College Ajmer
Ajmer 305002
Rajasthan
India

Shashank Tripathi [§]
Department of Electrical Engineering
K K Wagh Institute of Engineering Education and Research
Nashik 422003
Maharashtra
India

Ashish Kumar Singh [‡]
Department of Electronics and Communication Engineering
Graphic Era (Deemed to be University)
Dehradun 248002
Uttarakhand
India

[@] *E-mail:* Ramesh.meena@jaipur.manipal.edu; rameshkumarmeena@gmail.com
[†] *E-mail:* satya.tazi@ecajmer.ac.in
[§] *E-mail:* satripathi@kkwagh.edu.in
[‡] *E-mail:* ashishkrsinghiitbhu@gmail.com

Gagandeep Berar *
Department of Computer Science and Engineering
Chitkara Institute of Engineering & Technology
Chitkara University
Rajpura 140401
Punjab
India

Abstract

This potential has sparked significant interest across industries and in academic circles. IoT evolving into a versatile utility, offering advanced capabilities in sensing, acting, communicating, controlling, and extracting valuable insights from vast amounts of data. However, there's a big challenge: IoT devices often have limited computing power, memory, and battery life, which creates a major hurdle for security. To tackle this, our research introduces a new, energy-efficient, and lightweight cryptographic approach. It's based on the ElGamal algorithm, specifically adapted for these resource-constrained IoT devices. In this study uses the ElGamal algorithm for key generation, encryption, and decryption. We've also included a comparative performance analysis using MATLAB, pitting our approach against RSA and Paillier algorithms. By employing an 8-bit manipulation technique, our proposed method significantly reduces power and memory consumption, making it ideal for energy-limited IoT applications. The results clearly show that our solution performs better in terms of power usage, memory requirements, and processing time, demonstrating its effectiveness for securing IoT devices.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cryptography, Internet of things (IoT), Lightweight, Encryption, Decryption, Security.*

1. Introduction

IoT has indeed gone viral in the recent past and it is due to the fact that we are now able to access cheap and dependable wireless sensors [1-2]. IoT is being used in any type of engineering project and is allowing devices to communicate with each other over the internet. Nonetheless, a source of actual concern is that cyber-attacks potentially cause havoc in industrial systems [3]. In case of wrong information being relayed to the main computer, it may cause a few ugly decisions since analysis of the data will be faulty. This is why it is necessary to address this issue of security. The study is dedicated to the development of a method of sending and receiving (encrypt and decrypt) of information that all these various IoT devices transmit through the air safely [1-3].

Symmetric key cryptography is widely used in hardware with significant resource limitations. The fundamental blocks of a cryptographic system designed for IoT devices [4]. It highlights key security aspects such as confidentiality, ensuring that data is not accessible to unauthorized parties, and

* *E-mail:* **gagandeep2913@gmail.com (Corresponding Author)**

integrity and authentication, where robust security measures are implemented to verify the authenticity of users before granting access to the data [5-6].

2. Literature Review

A power diffusion strategy based on NASH bargaining arrangements is proposed to efficiently exploit the most challenging-to-reach nodes [7]. Additionally, current receiver wire technologies are reviewed, and an optimal design is suggested for maximizing energy extraction from low-power RF signals. By employing these methods, battery-powered sensor nodes can achieve the desired goals of extended lifespan, reduced overall costs, high performance, transmission coverage, and reliability [8-10].

In the context of the Internet of Things simplified cryptographic techniques are explored [11]. This review compares several block cipher versions and discusses a series of safety measures, including light cryptographic techniques. The advanced encryption pattern is identified as an effective security solution for IoT devices with resource restriction. The authors in [9], [12-13] focus on IoT devices with minimal resources, such as RFID tags, sensors, and smart cards, which can be challenging to secure under these conditions.

3. Methodology

3.1 *ElGamal Algorithm*

ElGamal cryptography is a public-key cryptosystem that provides encryption and digital signatures based on the challenge of solving discrete logarithms. The algorithm consists of three primary components: key generation, encryption, and decryption [14-17].

For Key Generation to choose a large prime p and a primitive root g modulo p. And select a private key x randomly from the set $\{1,2,\dots,p-2\}$. With Compute the public key:

$$y = g^x mod p \tag{1}$$

The public key is the tuple (p, g, y), and the private key is x.

For Encryption, Choose a random integer k from $\{1,2,\dots,p-2\}$. And Compute the shared secret:

$$s = y^k mod p \tag{2}$$

Given a plaintext message m (represented as an integer modulo p), compute the ciphertext pair:

$$c_1 = g^k mod p, c_2 = m \cdot s mod p \tag{3}$$

For Decryption, Recompute the shared secret using the private key and Recover the plaintext:

$$s = c_1^x mod p \tag{4}$$

$$m = c_2 \cdot s^{-1} mod p \tag{5}$$

where s^{-1} is the modular inverse of s modulo p.

The Elgamal algorithm has a workflow as shown in Figure 1. This algorithm is based on the operation of the public encryption, which is the asymmetrical key encryption, in order to have the safe two-part communication.

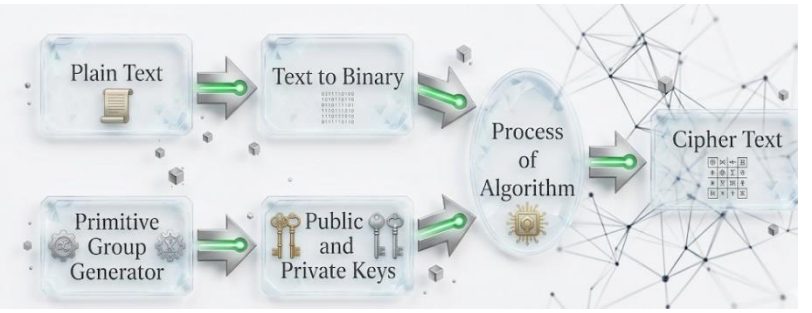

Figure 1

Process flow of EIGamal algorithm

To illustrate this, we can take an example of two users denoted by user-1 and user-2 who are willing to switch the data safely by the use of Elgamal technique. Their steps to follow to gain safe communication are as specified below.

A). Step 1: Generation of Public and Private Key.

User-1 first selects a large integer and a cyclic group which we will refer to as x. They then choose two of these from this group, B and C. The value A is stored in the form of the private key that is stored for subsequent use. Suppose that Gbe is a cyclic group with generator F. Select two elements $B, C \in G$ such that a defined group operation satisfies:

$$f(B, C) = 1 \tag{6}$$

User-1 generates the key parameter as

$$F_m = B^C \tag{7}$$

Thus, the Public Key and Private Key

$$PK = (F, B, C) \tag{8}$$

$$SK = A \tag{9}$$

where A is kept secret by User-1.

B). Step 2: Data Encryption by User-2

User-2 uses the public key of User-1 in order to encrypt a message. It consists of choosing certain settings, including a cyclic group p value, which on processing by a given function produces 1 - replicating the first steps of User-1. The encryption step finishes with multiplying this output with a variable/ Z, to obtain the ciphertext: bp, Z × bap. User-2 picks a parameter p in the cyclic group, G. First compute

$$p_w = B^p \tag{10}$$

Then evaluate B^C, and B^{Ap} and The ciphertext is produced as

$$C = (B^p,\ Z \times B^{Ap}) \tag{11}$$

Where Z = message value and C = ciphertext pair.

C). Step 3: Decrypting the Message by User-1.

User-1 computes the shared value using B^{Ap} Then the plaintext message is recovered as

$$Z = \frac{Z \times B^{Ap}}{B^{Ap}} \tag{12}$$

Thus,

$$Z = \frac{C_2}{B^{Ap}} \tag{13}$$

Where,

$$C = (C_1, C_2) = (B^p, Z \times B^{Ap}) \tag{14}$$

3.2. *Mathematical Model of EIGamal Algorithm*

The ElGamal algorithm is a public-key encryption method that leverages the properties of discrete logarithms in a finite field. Here is the mathematical formulation and execution process for the ElGamal algorithm.

For Key Generation, Choose a large prime number p and a generator g of the cyclic group $\mathbb{Z}_p^*$. To Select a private key

$$a \in \{1,2, \dots, p-2\} \tag{15}$$

Compute the public key

$$A = g^a mod p \tag{16}$$

Where Public key is (p, g, A) and Private key is a.

Form Encryption, Convert the message into an integer m such that $0 \leq m < p$, Choose a random integer $k \in \{1,2, \dots, p-2\}$, Compute the first ciphertext component

$$c_1 = g^k mod p \tag{17}$$

Compute the second ciphertext component

$$c_2 = m \cdot A^k mod p \tag{18}$$

with Ciphertext

$$C = (c_1, c_2) \tag{19}$$

For Decryption, Recover the plaintext using the private key a:

$$m = c_2 \cdot (c_1^a)^{-1} mod p \tag{20}$$

where $(c_1^a)^{-1}$, is the modular multiplicative inverse of c_1^a modulo p.

The security of the ElGamal encryption scheme hinges on the computational difficulty of solving the discrete logarithm problem within the cyclic group Zp. Specifically, given the parameters p, g, and A, deriving the private key a remains a formidable challenge due to this underlying problem.

4. Results and Discussion

Evaluating ElGamal cryptography for IoT devices requires assessing its compatibility with IoT's specific constraints. One of the issues is that encryption and decryption processes of ElGamal are computationally intensive because they implement modular operations, which could be a serious challenge to hardware with low capacity in the Internet of Things.

The three algorithms are compared using Table 1 analysis with several parameters. ElGamal algorithm is faster than RSA, ECC, and Paillier in transfer rate, and it is more efficient with small and lightweight key size which is in line with our research findings. ElGamal is more successful in these aspects, but RSA and Paillier are more flexible and have larger key sizes that are useful in a broader range of applications.

Table 1

Parameters for Comparison of Algorithms Metric

S. No.	Parameters	ElGamal Algorithm	RSA Algorithm	Paillier Algorithm	ECC Algorithm
1	Frequency	250 MHz	200 MHz	500 MHz to 2 GHz	100 MHz to GHz
2	Throughput	7.5 Gbps	5 Gbps	0.128 Gbps	1.5 Gbps.
3	Area	12,000 gates	20,000 gates	10,000 to 100,000 gates	10,000 to 100,000 gates
4	Key Size	256 bits	2048 bits	2048 to 4096 bits	256-bit keys
5	Power Consumption	200 mW	400 mW	100 mW	384-bit keys

From the results presented in Figures 2, 3, 4, 5, and 6, the ElGamal method demonstrated superior performance compared to RSA, ECC and Paillier in terms of encryption time.

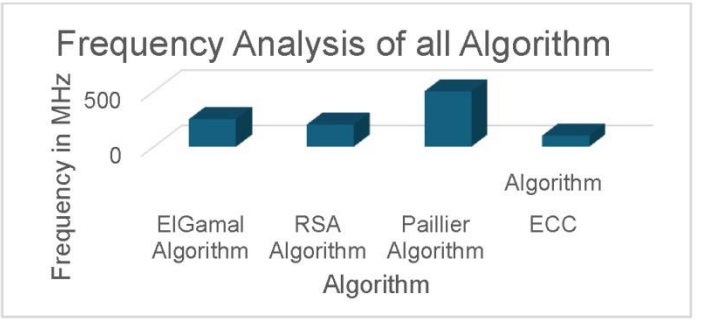

Figure 2

Comparison of Frequency of Algorithm Process

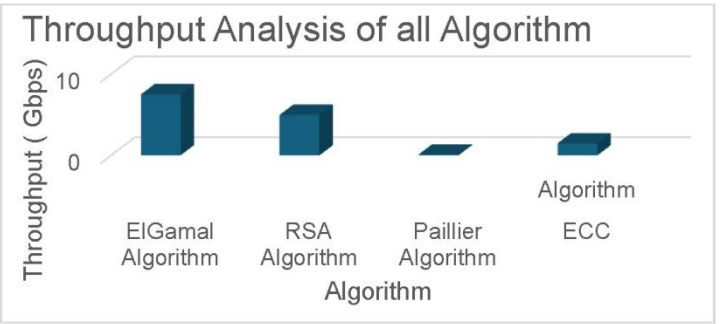

Figure 3
Throughput of All Algorithm Process

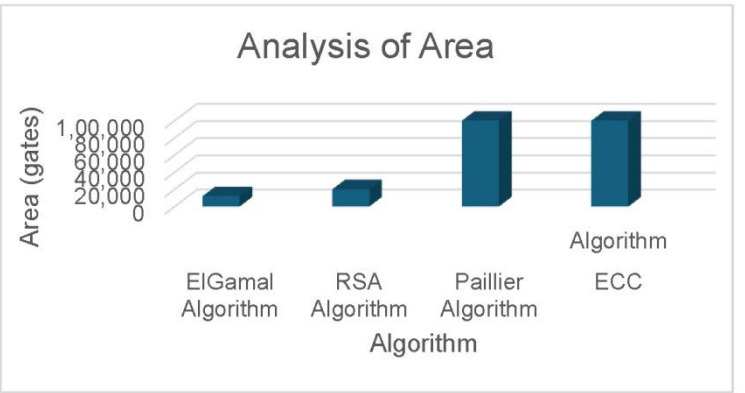

Figure 4
Analysis of Area of the All Algorithm Process

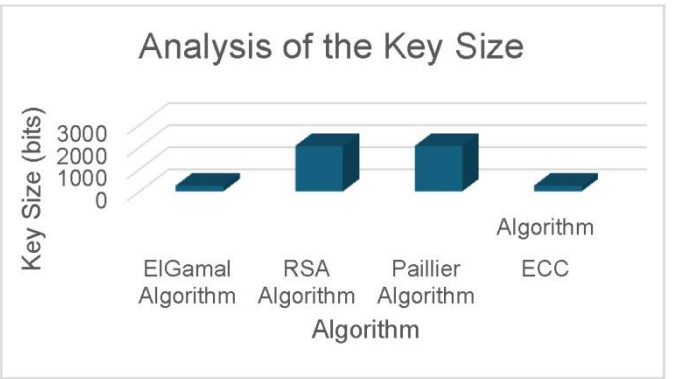

Figure 5
Analysis of the Key Size of All Algorithm Processes

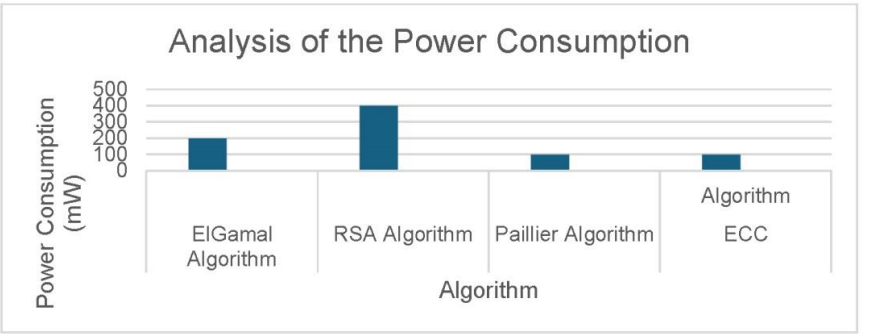

Figure 6
The Power Consumption of All Algorithm Processes

5. Conclusion

The current paper offers a lightweight and more energy-efficient ElGamal encryption approach. This algorithm exploits the difficulty of discrete logarithms in a cyclic group through the combination of asymmetric key encryption with two-party communication using the public-key cryptography. Using text data, the proposed algorithm was properly tested and tested using modern methods of analysis. In our findings, there is evident better throughput and area performance with very low delay in the proposed approach. This ElGamal encryption scheme of ciphertext block encryption is well appropriate to secure real-time applications due to its lightweight nature and high-security measures. This encompasses such critical usages as e-money transactions, different authentication mechanisms, timestamping, and popular messaging applications as WhatsApp and others.

References

[1] V. Annepu and A. Rajesh, "Implementation of an efficient artificial bee colony algorithm for node localization in unmanned aerial vehicle assisted wireless sensor networks," *Wireless Pers. Commun.*, vol. 114, no. 3, pp. 2663–2680 (2020).

[2] V. Annepu and A. Rajesh, "An unmanned aerial vehicle aided node localization using an efficient multilayer perceptron neural network in wireless sensor networks," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 11551–11663 (2020).

[3] V. Annepu, A. Rajesh, and K. Bagadi, "Radial basis function-based node localization for unmanned aerial vehicle-assisted 5G wireless sensor networks," *Neural Comput. Appl.*, vol. 33, no. 19, pp. 12333–12346 (2021), doi: 10.1007/s00521-021-06033-4.

[4] V. Annepu, D. R. Sona, C. V. Ravikumar, K. Bagadi, M. Alibakhshikenari, A. A. Althuwayb, B. Alali, M. A. Alzamil, J. Nebhen, and E. Limiti, "Review on unmanned aerial vehicle assisted sensor node localization in wireless networks: Soft computing approaches," *IEEE Access,* vol. 10, pp. 132875–132894 (2022).

[5] N. K. Vaegae, K. K. Pulluri, K. Bagadi, and O. O. Oyerinde, "Design of an efficient distracted driver detection system: Deep learning approaches," *IEEE Access,* vol. 10, pp. 116087–116097 (2022).

[6] K. Bagadi, C. V. Ravikumar, M. Alibakhshikenari, N. Challa, A. Rajesh, S. Aïssa, I. Dayoub, F. Falcone, and E. Limiti, "Precoded large scale multi-user-MIMO system using likelihood ascent search for signal detection," *Radio Sci.*, vol. 57, no. 12, Art. no. e2022RS007573 (Dec. 2022), doi: 10.1029/2022RS007573.

[7] T. K. Goyal, V. Sahula, and D. Kumawat, "Energy efficient lightweight cryptography algorithms for IoT devices," *IETE J. Res.,* vol. 68, no. 3, pp. 1722–1735 (2022).

[8] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison, and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193 (2021).

[9] I. K. Duna, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for Internet of insecure things: A survey," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, pp. 475–481 (2019).

[10] W. J. Okello, Q. Liu, F. A. Siddiqui, and C. Zhang, "A survey of the current state of lightweight cryptography for the Internet of Things," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, pp. 292–296 (2017).

[11] V. Rao and K. V. Prema, "A review on lightweight cryptography for Internet-of-Things based applications," *J. Ambient Intell. Humaniz. Comput.,* vol. 12, pp. 8835–8857 (2021).

[12] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "HIGHT: A new block cipher suitable for low-resource device," in *Cryptographic Hardware and Embedded Systems—CHES 2006, Lecture Notes Comput. Sci.*, vol. 4249, Berlin, Germany: Springer, pp. 46–59 (2006).

[13] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next generation lightweight cryptography for smart IoT devices: Implementation,

challenges and applications," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, pp. 707–710 (2019).

[14] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *J. Cyber Secur. Technol.*, vol. 1, nos. 3–4, pp. 187–201 (2017).

[15] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers," *Cryptology ePrint Archive*, Rep. 2013/404 (2013).

[16] R. Joshi, P. Mathur, A. K. Gupta, S. Singh, V. Paliwal, and S. Nayar, "Mathematical modeling of intelligent system for predicting effectiveness of premenstrual syndrome," *J. Interdiscip. Math.*, vol. 26, no. 3, pp. 551–562 (2023).

[17] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1473–1486 (2025).

Received January, 2026