Enhancement of Elgamal Cryptosystem; A Review

Paul Arhin and George Aggrey
Department of Computer Science & I.T, University of Cape Coast, Private Mail Bag, CC-123-1749, Cape Coast, Ghana
parhin@ucc.edu.gh, gaggrey@ucc.edu.gh

Keywords: ElGamal Cryptosystem, Hybrid Encryption, Hardware Enhancement, Software Enhancement.

Abstract: This article reviews a large body of research on optimizing the ElGamal cryptosystem for increased hardware and software efficiency. Areas of effort identified in the research include, hardware acceleration, hybrid systems combining ElGamal with symmetric cryptosystems, software advancements through adjustments to mathematical difficulties, and hybrids with other asymmetric cryptosystems. There is a clear demonstration that hybrid systems that combine ElGamal with symmetric encryption and software improvement through adjustments to the mathematical difficulties are highly impactful with about 95% score based on the amount of research done in the area. This indicates the significance of these domains for the further evolution of the ElGamal cryptosystem. Hybrid systems which seek to combine Elgamal with symmetric cryptosystems, such as AES, has become a very crucial area that needs a high level of concentration. This ensures both high level of security and greater enhancement to the time complexity. Through these changes, performances were improved and computational overhead were decreased by optimizing the underlying mathematical operations and combining Elgamal with other symmetric algorithms. The article proposes ChaCha20-Poly1305 as a potential for further improvement in hybrid encryption.

1 INTRODUCTION

Taher ElGamal created the ElGamal cryptosystem in 1985, and it is a foundation of public-key cryptography [1]. Because of its durability and reliance on the computationally challenging discrete logarithm issue, it is commonly used for secure key exchange and digital signatures [2]. The ElGamal cryptosystem has undergone a number of improvements throughout time to increase its security, effectiveness, and application.

These improvements, which address a variety of issues like performance optimization, attack resistance, and platform and application adaptation, have been made using both hardware and software. Specialized hardware has been utilized over the years to help improve the efficiency and security of the ElGamal cryptosystem [3].

Using Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) to speed up cryptographic procedures are two notable initiatives in this field [3][4][5].

The goal of these implementations is to achieve low power consumption and high processing speed, which are essential for real-time applications and situations with limited resources, such as Internet of Things devices [6]. There has been a great advancement in the use of software to improve ElGamal cryptosystem [7]. Many of these enhancements entail applying mathematical adjustments to the fundamental algorithm, including streamlining the procedures of key creation, encryption, and decryption [8].

These improvements are meant to boost the cryptosystem's effectiveness and strengthen its defences against cryptographic assaults. The creation of hybrid encryption systems that combine ElGamal with other cryptographic algorithms to make use of their unique advantages is another example of software upgrades [9][10]. A good way of improving Elgamal efficiency has been through the use of asymmetric hybrids, which combine ElGamal with other public-key cryptosystems like RSA or ECC (Elliptic Curve Cryptography) [11][12].

The integration of various encryption layers in these hybrids improves security. A number of attempts have concentrated on merging ElGamal with symmetric encryption techniques, which provide further security advantages and fast data encryption [13]. The high computational and mathematical requirements of the Elgamal cryptosystem have significantly impacted its effectiveness. Complex

mathematical operations are required for key generation, encryption, and decryption, which can be time- and resource-consuming [14].

As a result, there is a need to increase its efficiency using a variety of techniques, such as hybrid approaches, algorithmic optimizations, and hardware acceleration. Although ElGamal has undergone substantial development, more research needs to be done in integrating alternative symmetric algorithms in conjunction with ElGamal for a more efficient cryptosystem.

2 ELGAMAL CRYPTOSYSTEM

The Elgamal cryptosystem, a widely used public-key cryptosystem scheme is dependent on the difficulty of computing discrete logarithms over finite fields [2].

It is a public key encryption scheme which means the public key is shared and used for encryption whiles the secret or private key is kept secret and used for decryption.

Like other cryptosystems, the Elgamal cryptosystem involves three stages: Key Generation, Encryption and Decryption [2][3]. Figure 1 illustrates this process.

2.1 Key Generation

The key generation process starts with the selection of a large prime number p, and then choosing a suitable generator g and then randomly selecting a private key x, and computing the public key h using the relation $h = g^x \bmod p$. The public key becomes (p, g, h) and the private key (x). This forms the foundation for secure communication during the encryption and decryption procedures.[3].

2.2 Encryption Process

In the Encryption process, the sender gets access to the recipients' public key (p, g, h) generated in the key generation stage. To encrypt the message m, the plaintext is converted into an integer such that, $0 \leq m < p$. A random integer y is chosen for the encryption. $c1$ is then computed as $c_1 = g^y \bmod p$, c_2 is computed as $c_2 = m \cdot h^y \bmod p$. The resulting ciphertext is the pair; Ciphertext (c_1, c_2) [2][3].

2.3 Decryption Process

In the decryption process, the recipient first receives the ciphertext, Ciphertext (c_1, c_2). The receiver then computes the shared secret s as $s = c_1^x \bmod p$. The modular inverse of s (s^{-1}) is computed by the recipient such that $s \cdot s^{-1} \equiv 1 \bmod p$. The recipient then goes ahead to derive the original message, $m = c_2 \cdot s^{-1} \bmod p$. The plain text is then derived.[3]

3 PERFORMANCE CHALLENGES OF ELGAMAL

Despite being widely used, the ElGamal cryptosystem has a number of significant performance issues.

The traditional Elgamal Cryptosystem is noted for its inefficiency in encrypting large message sizes. This is due to its inherent message expansion. This results in a ciphertext that is bigger than the size of the plaintext, roughly a double of the plaintext [15][16]. This will require more storage, more bandwidth and longer processing times.

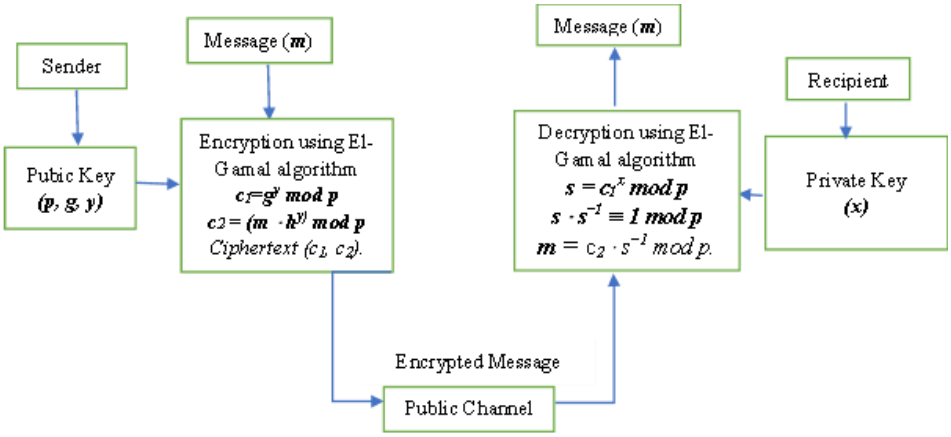

Figure 1: ElGamal Cryptosystem Procedure.

The computational complexity of key generation and the encryption/decryption procedures frequently reduces the efficiency of the cryptosystem. This is particularly troublesome for real-time applications with big databases [17].

The traditional ElGamal cryptosystem is dependent on the discrete logarithm problem. This makes it vulnerable to advancements in quantum computing capabilities. ElGamal's security presumptions might be broken by quantum algorithms [17][18].

4 ENHANCEMENTS OF ELGAMAL

According to [19], The ElGamal cryptosystem's resistance to attacks by quantum algorithms has been strengthened by the application of matrix ideas in key pair creation, making it appropriate for lower prime numbers and enhancing its security against brute-force attacks. This was done by using a square matrix as the private key to improve resistance against quantum logarithms attacks. With larger matrix sizes, there is a higher security against brute force attacks. Elliptic Curve Cryptography (ECC) was employed to upgrade ELGAMAL encryption scheme for better security.

When compared to normal ELGAMAL encryption, the suggested technique improves security and speed in both encryption and decryption duties while maintaining an extended cipher text size. It improves security and elapsed time in both encryption and decryption tasks over the conventional ELGAMAL encryption approach. A. Niemi and J. Teuhola [20] conducted a thorough study seeking to enhance Elgamal. The goal of the study is to improve the security of the Elgamal cryptosystem by using Burrows-Wheeler post-transformation with effective clustering and interpolative coding. This will boost the security of the Elgamal public-key algorithm.

An enhanced version of Elgamal was also developed by Hussein et al [15] for image encryption and decryption enhancement. The suggested method performs excellently across a range of assessment measures when tested on four distinct color photos. An improved ElGamal cryptosystem was used for image encryption, image decryption, and key pair generation in the methodology. To facilitate encryption and decryption, random bytes were created and pixels and generated bytes were subjected to an XOR process. Four color photos were used to test the approach, and the results were good.

For IoT devices, Mohan et al in 2020 [6] developed an improved Elgamal cryptosystem for secure Data Transfer in IoT networks. The updated ElGamal cryptosystem increases transmission efficiency while maintaining security levels comparable to the original. The study suggests a public-key cryptosystem (PKEIE) that is based on ElGamal and is effective in addressing issues such massive message encryption, integrity, authentication, non-malleability, and semantic security. With this approach, data of any size can be encrypted, something that the old ElGamal cryptosystem was not able to do. The suggested technique integrates integrity, authentication, and encryption using a single algorithm, making it appropriate for Internet of Things networks when compared to other ElGamal variant schemes based on security levels and performance. A. Pandey et al (2020) [21] proposed a methodology, which includes breaking down group ring elements into matrices over base rings, applying linear algebra techniques, and creating a cryptanalytic algorithm to effectively break the ElGamal-like cryptosystem put forth by Saba Inam and Rashid Ali. The security of the plan against selected ciphertext attacks (IND-CCA) and selected plaintext assaults (IND-CPA) is also examined by the authors. The authors enhanced the method of cryptanalysis, proved that Saba and Rashid's ElGamal cryptosystem was insecure, and created a cryptanalytic assault that might compromise the system.

An improved Exponential Elgamal Encryption Scheme with Additive Homomorphism was proposed by Zhou et al [22] in 2022. The process comprised evaluating the security of the established ElGamal encryption scheme, putting forth the exponential ElGamal system as a new encryption strategy, and verifying the effectiveness and security of the new scheme. When chosen plaintext was used as an attack vector, the ElGamal encryption technique was not sufficiently secure. The proposed enhanced Elgamal cryptosystem achieved a higher security.

Ranasinghe et al [23] presented a work on the generalization of the Elgamal public-key cryptosystem. The methodology is based on a proposal for an extension of the original ElGamal system that uses modular exponentiation twice during encryption and incorporates the prime factorization of the plaintext to improve the encryption process. The scheme’s encryption mechanism is enhanced.

Owolabi et al [24] also proposed a hybrid system of Elgamal and Blowfish with the focus of enhancing efficiency and security. The goal of the research is to increase encryption/decryption performance and data security of ElGamal by integrating the Blowfish and ElGamal cryptosystems. The result is the achievement of a more secure encryption technique with faster encryption and decryption speeds compared to the standalone El-Gamal algorithm.

Another work that combined Elgamal with another Symmetric algorithm, 3DES was conducted by Rachmawati et al [25] in the year 2018. The work explored a hybrid cryptographic strategy to address security concerns in data exchange over the internet by utilizing the asymmetric ElGamal algorithm and the symmetric Triple DES algorithm. Using a hybrid cryptography approach, the study combined the asymmetric ElGamal algorithm with the symmetric Triple DES algorithm. Triple DES, which requires three 56-bit keys, was utilized for both encryption and decryption. The Triple DES keys were encrypted using ElGamal, which uses a public key for encryption and a private key for decryption. Text files ending in.txt were the messages that needed to be encrypted.

The results show that, the Triple DES algorithm takes longer to encrypt and decrypt messages with larger volumes. The Triple DES and ElGamal algorithms require more time to encrypt data than to decrypt it. Still on hybrid of Elgamal with Symmetric algorithms, Rani et al [26] in their paper, “Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal”, presented a hybrid cryptographic algorithm combining Elgamal and AES that enhances performance over using them alone.

This is done to improve the security, encryption/decryption time, and throughput. The new hybrid algorithm that integrates AES and Elgamal was implemented with the Java programming language, and the performance analysis conducted. The results indeed showed that, the hybrid algorithm that was designed to decrease the time of encryption and decryption and increase throughput indeed performed far better than the individual algorithms.

A proposed hybrid system that integrates the symmetric Hill Cipher 3*3 and the asymmetric Elgamal to secure instant messaging for Android was thoroughly conducted by Rachmawati et al (2019) [27].

5 RESULT AND ANALYSIS

Upon reviewing a number of articles on the improvement and enhancement of the Elgamal cryptosystem to yield better efficiency in both hardware and software, notable results were recognized in the modification of the Elgamal cryptosystem in several ways. These ways include Software enhancement through modifications to the mathematical complexities of Elgamal, Hardware enhancement, Hybrid Enhancement involving Elgamal and other asymmetric systems and Hybrid enhancement involving Elgamal and symmetric algorithms.

Software improvements are highly impactful with about 95% of research done in this area. This have mostly concentrated on altering the ElGamal algorithm's mathematical complexity and hybrid systems involving Elgamal and symmetric algorithms as well as Elgamal and other Asymmetric algorithms. in order to increase its effectiveness and security. Through these changes, performances were improved and computational overhead were decreased by optimizing the underlying mathematical operations.

These enhancements typically involve optimizing algorithms, reducing computational complexity, and improving security measures. Other studies have also looked into using hardware acceleration to increase the ElGamal cryptosystem's speed and efficiency. ElGamal is becoming more feasible for resource-constrained environments and high-throughput applications as implementations utilizing FPGAs and other hardware accelerators have shown notable increases in processing performance.

6 CONCLUSIONS

Given the benefits of symmetric algorithms for increasing efficiency, it is noteworthy that Google's high-speed symmetric algorithm, ChaCha20-Poly1305 [28], has received little to no attention thus far. A strong contender for improving the ElGamal cryptosystem, ChaCha20-Poly1305 has exceptional performance and security characteristics. Even though ChaCha20-Poly1305 has a lot of potential, the literature review points to a gap in its integration with ElGamal, indicating an area that has not yet been thoroughly investigated but has the potential to significantly increase encryption efficiency and speed.

Furthermore, the integration of AI technology is still not fully utilized in efforts to identify the greatest speed enhancements in Elgamal cryptosystem. With the development of AI, there is a significant possibility to improve security procedures, anticipate weaknesses, and optimize operations. ElGamal cryptosystem has not been fully optimized by using AI applications in hardware, including Tensor Processing Units (TPUs), and software. Should this research gap be filled, it has the potential to greatly advance the field of cryptography technologies as AI integration in software enhancements as well as hardware accelerators is lacking.

Subsequent investigations ought to concentrate on merging ChaCha20-Poly1305 with ElGamal in order to create a hybrid cryptosystem that blends ElGamal's strong security with ChaCha20-Poly1305's fast performance. It should also investigate AI methods to improve security protocols [29], optimize encryption procedures, and anticipate future flaws in the ElGamal cryptosystem [30].

It is also crucial to include AI technologies into software programs and hardware accelerators like TPUs in order to obtain better encryption efficiency and performance. By filling in these gaps, the study can make a substantial contribution to the creation of an ElGamal cryptosystem that is more effective and safer while using the most recent developments in symmetric encryption and artificial intelligence.

REFERENCES

[1] H. Hajaje et al., “CPC-H2: Convolution Power-based Cryptosystem and Digital Signature,” 2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1–7, 2021, [Online]. Available: https://doi: 10.1109/CCECE53047.2021.9569033

[2] R. Ranasinghe and P. Athukorala, "A generalization of the ElGamal public-key cryptosystem," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, pp. 2395–2403, 2021. [Online]. Available: https://doi: 10.1080/09720529.2020.1857902.

[3] S. Kim and R. Kyung, "Study on Modified Public Key Cryptosystem Based on ElGamal and Cramer-Shoup Cryptosystems," 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 280–284, 2023, [Online]. Available: https://doi: 10.1109/CCWC57344.2023.10099297.

[4] A. Kurd and N. Besli, "Analysis of the Cryptography Methods for Design of Crypto-Processor," 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), pp. 1–7, 2020, [Online]. Available: https://doi: 10.1109/HORA49412.2020.9152929.

[5] S. Guilley, L. Sauvage, J. Danger, T. Graba, and Y. Mathieu, "Evaluation of Power-Constant Dual-Rail Logic as a Protection of Cryptographic Applications in FPGAs," 2008 Second International Conference on Secure System Integration and Reliability Improvement, pp. 16–23, 2008, [Online]. Available: https://doi: 10.1109/SSIRI.2008.31.

[6] M. Mohan, M. Kavithadevi, and J. V., "Improved ElGamal Cryptosystem for Secure Data Transfer in IoT Networks," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 295–302, 2020, [Online]. Available: https://doi: 10.1109/I-SMAC49090.2020.9243407.

[7] H. I. Hussein and W. M. Abduallah, "An efficient ElGamal cryptosystem scheme," International Journal of Computers and Applications, vol. 43, pp. 1088–1094, 2019, [Online]. Available: https://doi: 10.1080/1206212X.2019.1678799.

[8] G. Kim and S. Li, "Decryption speed up of ElGamal with composite modulus," PLoS ONE, vol. 15, 2020, [Online]. Available: https://doi: 10.1371/journal.pone.0240248.

[9] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, and R. Odarchenko, "Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems," 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), pp. 229–233, 2018, [Online]. Available: https://doi: 10.1109/MSNMC.2018.8576289.

[10] D. Rachmawati, M. A. Budiman, and M. I. Wardhono, "Hybrid Cryptosystem for Image Security by Using Hill Cipher 4x4 and ElGamal Elliptic Curve Algorithm," 2018 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), pp. 49–54, 2018, [Online]. Available: https://doi: 10.1109/COMNETSAT.2018.8684121.

[11] M. Enriquez, D. W. Garcia, and E. R. Arboleda, "Enhanced Hybrid Algorithm of Secure and Fast Chaos-based, AES, RSA and ElGamal Cryptosystems," Indian Journal of Science and Technology, vol. 10, pp. 1–14, 2017, [Online]. Available: https://doi: 10.17485.IJST.2017.V10I27.105001.

[12] M. Bie, W. Li, T. Chen, L. Nan, and D. Yang, "An energy-efficient reconfigurable asymmetric modular cryptographic operation unit for RSA and ECC," Frontiers of Information Technology & Electronic Engineering, vol. 23, pp. 134–144, 2022, [Online]. Available: https://doi: 10.1631/FITEE.2000325

[13] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An Image Encryption Method Based on Elliptic Curve ElGamal Encryption and Chaotic Systems," IEEE Access, vol. 7, pp. 38507–38522, 2019, [Online]. Available: https://doi: 10.1109/ACCESS.2019.2906052.

[14] P. Sharma, S. Sharma, and R. Dhakar, "Modified Elgamal Cryptosystem Algorithm (MECA)," 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011), pp. 439–443, 2011, [Online]. Available: https://doi: 10.1109/ICCCT.2011.6075141.

[15] H. I. Hussein, R. J. Mstafa, A. Mohammed, and Y. M. Younis, "An Enhanced ElGamal Cryptosystem for Image Encryption and Decryption," 2022 International Conference on Computer Science and Software Engineering (CSASE), pp. 337–342, 2022, [Online]. Available: https://doi: 10.1109/CSASE51777.2022.9759643.

[16] M. Hwang, C. Chang, and K. Hwang, "An ElGamal-Like Cryptosystem for Enciphering Large Messages," IEEE Transactions on Knowledge and Data Engineering, vol. 14, pp. 445–446, 2002, [Online]. Available: https://doi: 10.1109/69.991728.

[17] T. Prantl et al., "Performance Evaluation for a Post-Quantum Public-Key Cryptosystem," 2021 IEEE International Performance, Computing, and Communications Conference (IPCCC), pp. 1–7, 2021, [Online]. Available: https://doi: 10.1109/IPCCC51483.2021.9679412.

[18] J. Jianwei, H. Wang, H. Zhang, S. Wang, and J. Liu, "Cryptanalysis of an ElGamal-Like Cryptosystem Based on Matrices Over Group Rings," Communications in Computer and Information Science, 2018, [Online]. Available: https://doi: 10.1007/978-981-13-5913-2_16.

[19] Maxrizal, S. Irawadi, and Sujono, "Discrete Logarithmic Improvement for ElGamal Cryptosystem Using Matrix Concepts," 2020 8th International Conference on Cyber and IT Service Management (CITSM), pp. 1–5, 2020, [Online]. Available: https://doi: 10.1109/CITSM50537.2020.9268832.

[20] A. Niemi and J. Teuhola, "Burrows-Wheeler post-transformation with effective clustering and interpolative coding," Software: Practice and Experience, vol. 50, pp. 1858–1874, 2020, [Online]. Available: https://doi: 10.1002/spe.2873.

[21] A. Pandey, I. Gupta, and D. Singh, "Improved cryptanalysis of a ElGamal Cryptosystem Based on Matrices Over Group Rings," Journal of Mathematical Cryptology, vol. 15, pp. 266–279, 2020, [Online]. Available: https://doi: 10.1515/jmc-2019-0054.

[22] R. Zhou and Z. Lin, "An Improved Exponential ElGamal Encryption Scheme with Additive Homomorphism," 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), pp. 25–27, 2022, [Online]. Available: https://doi: 10.1109/ICBCTIS55569.2022.00017

[23] R. Ranasinghe and P. Athukorala, "A generalization of the ElGamal public-key cryptosystem," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, pp. 2395–2403, 2021, [Online]. Available: https://doi: 10.1080/09720529.2020.1857902.

[24] O. Y. Owolabi, P. B. Shola, and M. B. Jibrin, "Improved Data Security System Using Hybrid Cryptosystem," International Journal of Scientific Research in Science, Engineering and Technology, vol. 3, pp. 90–93, 2017. [Online]. Available: [Online]. Available: https://www.academia.edu/89014842/Improved_Data_Security_System_Using_Hybrid_Cryptosystem

[25] D. Rachmawati, A. Harahap, and R. N. Purba, "A hybrid cryptosystem approach for data security by using triple DES algorithm and ElGamal algorithm," IOP Conference Series: Materials Science and Engineering, vol. 453, 2018, [Online]. Available: https://doi: 10.1088/1757-899X/453/1/012018

[26] S. Rani and H. Kaur, "Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal," International Journal of Advanced Research in Computer Science, vol. 8, pp. 254–258, 2017, [Online]. Available: https://doi: 10.26483/ijarcs.v8i3.2990.

[27] D. Rachmawati, A. Sharif, and Ericko, "Hybrid Cryptosystem Combination Algorithm Of Hill Cipher 3x3 and Elgamal To Secure Instant Messaging For Android," Journal of Physics: Conference Series, vol. 1235, 2019, [Online]. Available: https://doi: 10.1088/1742-6596/1235/1/012074

[28] J. P. Degabriele et al., "The Security of ChaCha20-Poly1305 in the Multi-User Setting," Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021. [Online]. Available: https://doi: 10.1145/3460120.3484814

[29] Li, B., Feng, Y., Xiong, Z., Yang, W., & Liu, G. (2021). "Research on AI Security Enhanced Encryption Algorithm of Autonomous IoT Systems." Information Sciences, vol. 575, pp. 379-398. [Online]. Available: https://doi: 10.1016/J.INS.2021.06.016

[30] Blackledge, J., & Mosola, N. (2020). "Applications of Artificial Intelligence to Cryptography." Transactions on Machine Learning and Artificial Intelligence, vol. 8, pp. 21-60. [Online]. Available: https://doi: 10.14738/tmlai.83.8219.