A Novel Security System Using a Physical Unclonable Framework with Modified Elliptic Curve Cryptography Algorithm.

Aiham Altaher *, Alex Bystrov, Martin Johnston

Posted Date: 18 June 2024

doi: 10.20944/preprints202406.1179.v1

Keywords: PUF, Improved PUF, ECC, security, Cybersecurity, Authentication, Authorization, Encryption, Decryption.

Article

A Novel Security System Using a Physical Unclonable Framework with Modified Elliptic Curve Cryptography Algorithm

Aiham Altaher *, Alex Bystrov and Martin Johnston

School of Engineering at Newcastle University, Newcastle upon Tyne NE1 7RU, England
* Correspondence: a.altaher2@newcastle.ac.uk

Abstract: A Physical Unclonable Framework (PUF) is a detached hardware component or, the structural arrangement of hardware that provides natural variations in the physical parts of semiconductor devices to generate unique and unpredictable identifiers based on challenging-to-replicate. In this case, PUFs are giving us a tool to utilize these variations to create an unclonable identifier for your device. PUFs generate a response, or a unique pattern based on the physical characteristics of the device, and this response is difficult to predict or duplicate. This study aims to introduce a PUK device to provide security research on the Internet of Things technology. The elliptic curve cryptography algorithm was modified with an advanced equation to calculate a private key and K value. In this study, a PUF device will be employed with a modified elliptic curve cryptography algorithm on a novel security system to be used in current and future communication technology.

Keywords: PUF; improved PUF; ECC; security; cybersecurity; authentication; authorization; encryption; decryption

1. Introduction

Physical Unclonable Framework (PUFs) was improved before to enhance the performance of PUFs and bolstered the security. A control was added to the silicon PUF that for raise the level of security up and make it more reliable and stronger. That technique makes the system harder for potential adversary to break. Figure (1) below shows the PUF block improvement. It contains four different units, beginning with a random hash function before the PUF. It becomes the first barrier to defense in front of the adversary from performing a "chosen challenge attack," preventing him from selecting the challenges and then easily extracting the parameters. To settle noisy physical measurements and convert them into consistent responses, an Error Correction Code (ECC) was used and placed after the PUF directly. Finally, the random hash function is placed again as the last unit to make the outputs composite function and that will add another level of security and make the adversary's task even harder (1) (2) (3).

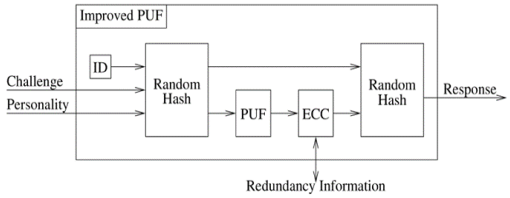

Figure 1. Using control to improve a PUF.

 doi:10.20944/preprints202406.1179.v1

2. A Novel Security System on the Internet of Things

A security research plan includes using the improved PUF to build a novel security system. Moreover, Improved Elliptic Curve Cryptography (ECC) algorithm will be used on this modern system. That system is designed to be a robust and reliable strategy. Figure (2) illustrates that system architecture and shows how that system works. The key (Authority Device) is a significant component of this system. It consists of four different units, beginning with a verification unit. As a part of that unit, a fingerprint will be utilized to verify the key device by sending it with the device's MAC address to the server over the internet for authentication purposes. The key (AD) status will change to active once the server provides its approval. The company should update the server with a list of clients who are permitted to use the devices. The improved PUF unit will start working when the status shows active. The response of the improved PUF unit will contain an advanced unclonable random number, which will be used in the next step to generate the private key based on the improved ECC algorithm. The signature unit is the final part of this design; it contains a method to calculate the public key from the private key and employ it in the next step to generate the signature. The node should receive the signature from the (AD) key and needs to verify it by transmitting it to the server over the internet. Upon the node receiving authorization from the server, the crypto-core unit will start establishing the channel and finding the neighbour. Once the neighbor is detected that means his status is active, both of neighbors will start encrypting and decrypt the traffic using an improved ECC algorithm. The neighbors' discovery is a significant task in building the neighbor list and save it in the node registration field. That list is essential for a multi-nodes system. Figure (2) shows and illustrates the architecture of that security system.

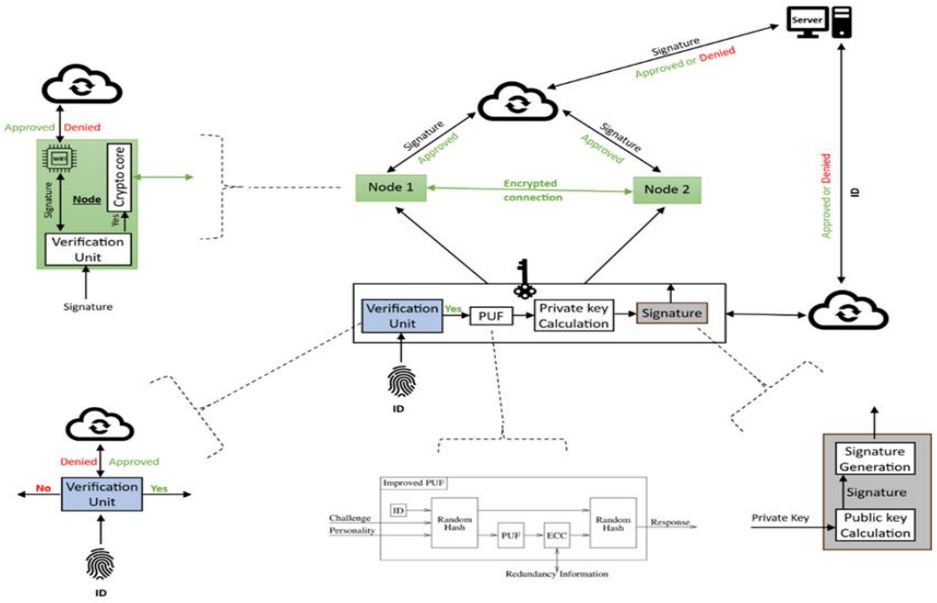

Figure 2. The architecture of novel security system.

3. Modified Elliptic Curve Cryptography Algorithm.

On the improved PUF device, a cryptography algorithm will be implemented to support the study problem with an exceptional solution. This algorithm will encrypt the traffic with an extremely low latency compared with other lightweight cryptography algorithms. It was developed based on an Elliptic Curve Cryptography algorithm to support the internet of things with a significantly fast and modern method. A lower processing time will definitely reduce the power consumption, and that will save a lot of money. It has ten separate steps to encrypt and decrypt the message. Steps three and five are designed and developed to provide a higher level of security while maintaining the speed feature.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 June 2024 doi:10.20944/preprints202406.1179.v1

The following are the novel cryptography algorithm steps:

- **Step 1.** Mapping the message on the curve.
- **Step 2.** Generate all the points based on the first point (point doubling & point adding).
- **Step 3.** Calculate the **private key**:
  $d = R^3 + a^2 + b \; Mod \; p$
  R: Random number comes from PUF device
  a, b Two elements on the curve.
  p: Specifying the finite field F_p
- **Step 4.** Calculate the public key,
  Public key = d * *Generator point*.
- **Step 5.** Calculate K value:
  $K = R^3 + a^2 + b \; Mod \; p$
- **Step 6.** Apply the encryption equation.
  Compute $C_1 = [k]G$ & $C_2 = M + [k]Q$
  G: Generator Point
  M: Plaintext.
  Q: Public key
- **Step 7.** Send that ciphertext to the destination.
- **Step 8.** Receive that ciphertext.
- **Step 9.** Apply the decryption equation.
  $M = C_2 - [d]C_1$
- **Step 10.** Mapping the message back.

4. The Authority Device (AD)

The key device, known as the Authority Device (AD), is the main component of the security system designed to secure the Internet of Things or any other communication system. Improved-PUF and improved-ECC algorithm were the two novel components used in the development side on the AD device. Both those parts are working to provide an exceptional solution for the study proposal. To highlight the AD procedures, the following figure (3) illustrates the procedure steps:

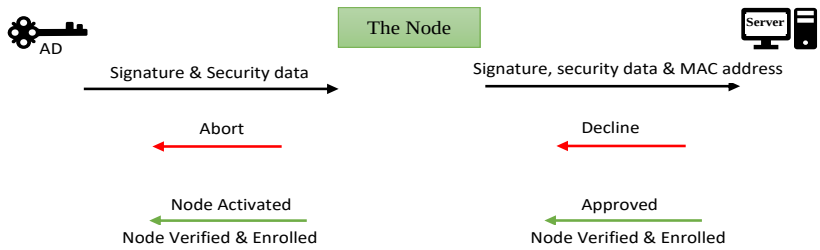

Figure 3. The AD device for node verification and enrolment.

The node verification and Enrolment method requires three different devices to achieve it. Begin with the AD device by sending the signature, and public key to the server by VPN tunnel over the internet and transmitting that confidential data with the private key to the node directly; The node

 doi:10.20944/preprints202406.1179.v1

will then create VPN tunnel with the server over the internet to transmit that confidential data with it is MAC address for authentication purposes. The server will respond after checking the data center to find the node's MAC address and check other security data then will reply with a refusal or approval. Once the node gets approval the status will switch to active before beginning to look for neighbors.

4.1. The Authority Device Structure

A novel structure was invented to build the AD device up to provide an exceptional protection layer on the modern security system. Initially, the company will install the task statements using the input port. These statements will contain all system data, including the technical engineer ID and company identity, the tunnel configuration for each system part, and the protocols required to operate the system network. On the other hand, the output port will be used to send that information to destination nodes. The following are the components of that security device:

1- Improved PUF device: This device was developed in the last decade to generate an advance, unclonable random number for each challenge to calculate the private key using the improved ECC algorithm. That number is significantly important on this innovative system. Because it provides an additional layer protection.

2- Decommission unit: This unit's task is destroying the whole motherboard with all other components by sending high voltage suddenly. This unit is acting in an emergency only when the AD devices is lost or intentionally hidden. It activates directly from the server or automatically once the task statement period has expired. The direct order comes from the server when the technical engineer inform his manager of the missing device; Otherwise, he should promptly return the AD device back to company once his mission has finished immediately. because if not the decommission unit will be activated from itself once the mission period has expired. For the security purposes the decommission unit will destroy all the device's parts if the device does not return safely to company at the appropriate time.

3- Fingerprint reader: This unit provides an additional protection layer on the system. The unit's task is preventing intruder to use the AD device. Therefore, this device should verify the engineer identification first before begin activating all nodes in the system.

4- Central Processing Unit CPU: It is the processor which is essential to processing the system instructions to drive the whole device. Basically, the CPU is the main crucial integrated circuitry chip in all devices. Control unit with arithmetic logical unit working together to interpreting the most of device commands.

5- Storage units: Random Access Memory RAM is significant part to store the security info comes from the solid-state drive or storage on it before transmitting it to nodes system. Read only memory task is storing the system essential instructions.

6- Power supply unit PSU: It is the unique power source which is needed to operate the motherboard and all other the AD device parts.

7- Cooling system: That system's mission is preserving the temperature in the desired range to prevents overheating on the device which generated by electronic components. Furthermore, the cooling system works to enhance device performance by removing overheating, which let the system operating at higher speed.

8- Wi-Fi network: Wireless Fidelity is a significant part in this system using to associate AD device with the server by VPN tunnel which will be created over the internet. Figure (4) displays the AD device structure and shows all the device parts.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 June 2024 doi:10.20944/preprints202406.1179.v1

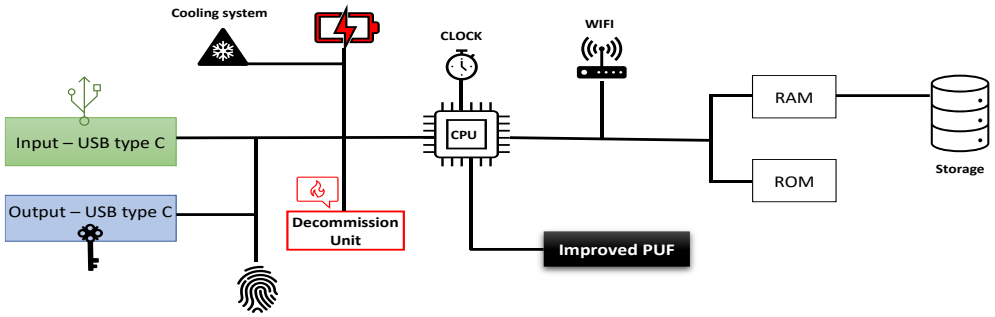

Figure 4. The Authority Device structure.

5. The Node Device

The node device is described as a physical object that is embedded with an interface consisting of sensors, software, and other modern components. That device should be associated with his neighbors and have direct connections to server over the internet. The purpose of that is to achieve centralized management by working as a team and to get benefit from the modern technology features to provide the highest service quality. Cellular networks, traffic light systems, smart automobiles, kitchen appliances, thermostats, CCTV systems, etc. are all becoming sophisticated objects when employing embedded interfaces with them to connect people, processes, and things. In summary, when the interface or embedded system installed on the standard node, it will convert to smart things, and that is the exact definition of the internet of things.

5.1. The Node Structure

The node is divided into two sections. The first section is an ordinary or standard part, such as any typical appliance, for example. The second section is the smart side, which converts the standard node into a smart device. The interface is an electronic device that contains sensors, processing units, storage, and a wireless chip for data exchange. The sensor's task is to read the physical environment or system outcomes to let the admin decide to take a specific action when it needs to. There are a wide range of sensors, each designed to recognize specific input types. A motion sensor, gas sensor, temperature sensor, pressure sensor, humidity sensor, photodetector, and biometric reader are a few common instances. They are necessary for creating intelligent devices with advanced control systems. The interface side should be supported by a power source and cooling system, which are essential to operating the system. For saving the system's instructions and store the data, storage units are also necessary to build this system up. Figure (5) shows the node structure and differentiate between the interface part and standard node part.

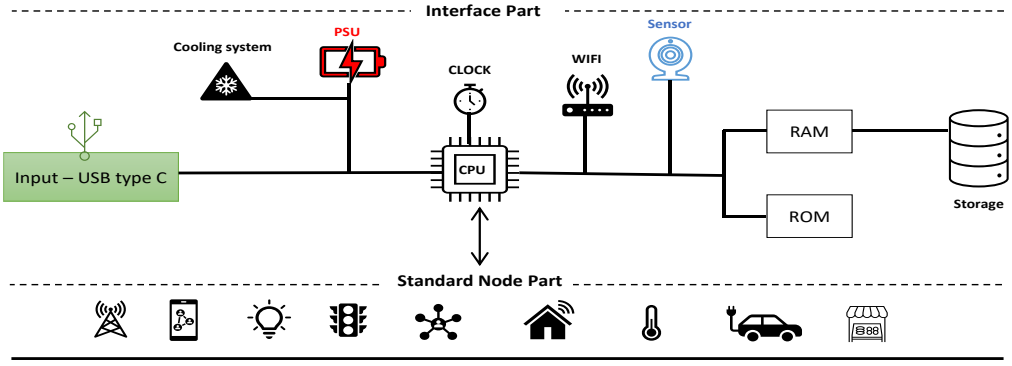

Figure 5. The node structure.

 doi:10.20944/preprints202406.1179.v1

5.2. The Node Neighborhood

The node list consists of all the nodes in the whole topology. That list will be created as soon as the node status indicates that it is active. In this stage node 1 will be appointed as a master node from the server. The master node will send an acknowledgement message to all activated nodes via a wireless fidelity network. Once the destination node gets the ACK message, it will reply with its name and MAC address to the master node. The first action will be creating the channel before starting to encrypt the traffic using the improved ECC algorithm equation. On the other site, node 2 will start decrypting the traffic after accepting the channel request from the master node. At the same time, node 2 could send back encrypted data to the master node or to any other node in the same domain. The master node and all others should use the Improved ECC algorithm to decrypt the data is coming from authenticated neighbour nodes in the same topology. Figure (6) illustrates how the master node was appointed and shows the steps from creating the channel to encrypting and decrypting the traffic.

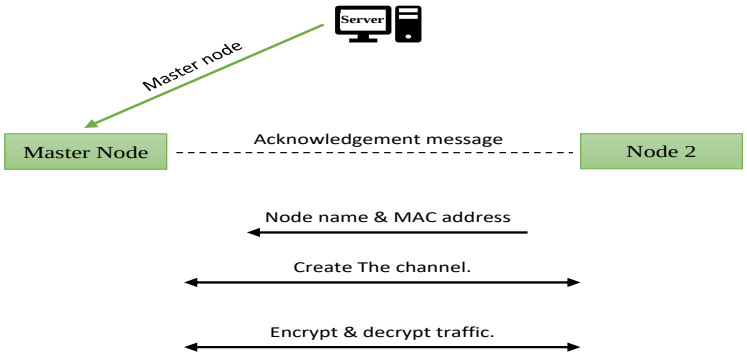

Figure 6. Create the channel and encrypt the traffic.

5.3. The Node Decommission

Removing the node from one of its neighbourhoods is known as decommissioning node task. The server is in responsible of the neighbour list configuration. That means when remove node 1 for example from the data centre in the server, it will be deleted from itself after the node gets the first update message from the server. The update message receives from the server once every minute. Reactivate node 1 again needs to update the data centre in the sever first then reauthenticate the node from beginning. That means it needs AD device again to get new signature to verify the node and create a new channel for rebuild the neighbour list and enrol itself with the neighbourhood. Figure (7) explains that how the decommission task happened and shows reactivate node steps with sequence.

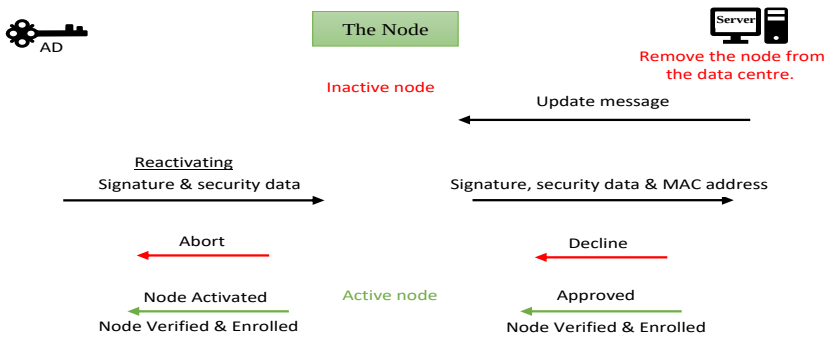

Figure 7. Decommission and reauthentication task.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 June 2024 doi:10.20944/preprints202406.1179.v1

5.4. Multiple Nodes System

The multiple nodes system can be defined simply as those nodes that operate across multiple domains. That system has the mutual part between neighborhoods for cooperating and coordinating purposes. There are two main categories of topologies. First, independent neighborhood: that kind of topology does not have any mutual nodes or any connection with other domains, such as the Internet of Things, installed in the same location as home or station, for instance. Secondly, multiple neighborhoods that have mutual nodes associating the domains together. Figure (8) shows those topologies.

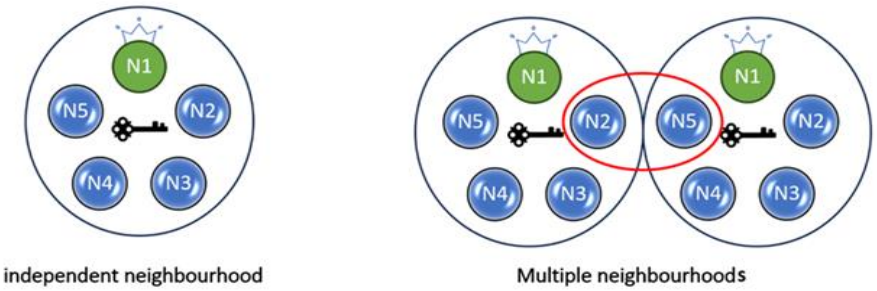

Figure 8. Topologies type.

6. The System Reliability and Integrity

This system is designed to provide a high level of security and accurate reliability by integrating the comprehensive security keys and passwords in the AD device. This technique will guarantee that all the confidential information is saved away from anyone including the company's engineers and any other employees or managers. The fundamental concept behind this system is that it provides less confidence to all the company's engineers and staff avoiding any potential corruption or leakage of sensitive information. That technique will completely secure the services and provide extraordinary security. In addition, the AD device will safely store the tunnel establishment settings out of the human's reach, which are required to build the VPN tunnel across the internet between the nodes and the servers. Initially, the node will extract the tunnel policy from the AD device and then begin to install the tunnel automatically. That technique will be explained in the following subsections in full detail.

6.1. The System Reliability Features

The Authority Device AD is an electronic hardware device consisting of microsystem chips, sensors, and improved PUF with memories and suitable storage to store sensitive information such as tunnel policy and cryptography algorithm keys. That sophisticated architecture will raise the service to a significant level. The flowing Figure (9) explains those features.

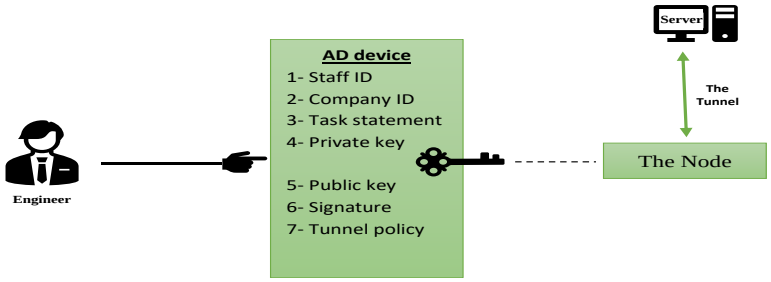

Figure 9. The AD device contains secret info.

In this structure, the technical engineer does not have any access to secret info or even has ability to verify its authenticity. As mentioned in section 2 The Authority Device (AD), the AD device needs

 doi:10.20944/preprints202406.1179.v1

to be authenticated with the server before its status shows as active. A VPN tunnel should be created to participate in and synchronize the sensitive data with the server. That tunnel should be established across the internet to transmit confidential information such as staff identification, company identification, keys, signature, tunnel policy, and even task statement with the server. That statement contains the company's permission with a specific date, time, and engineer's ID to achieve the task at the exact time and location. Moreover, serial numbers for all nodes should be provided in the task statement by the company for reliability purposes. That is why the technical engineers do not have any ability to access on secret information. The AD device's responsibility is to calculate the private key using the improved PUF outcome as an important element with an improved ECC algorithm. The public key will generate then to produce the signature. The tunnel policy should be stored in the AD device from the company to be used next in the node to create a VPN tunnel between the node and the server across the internet.

6.2. The Authority Device, Decommission Unit

The AD device is the core component in this system because it contains all the system's secret info, such as private key, which is why it is significantly important. In case of losing or missing the AD device, the decommission unit in the device will activate by the server's direct request to destroy all secret data and hardware circuits. That will be achieved by sending an emergency order to the AD device to erase all confidential information in the memory units. Figure (10) shows that method and explain how and when that emergency action will take.

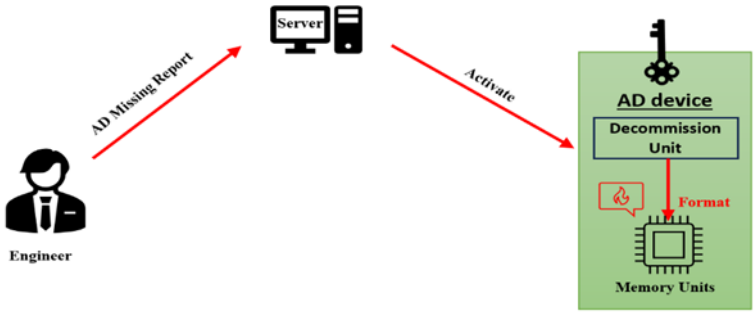

Figure 10. Decommission unit task in the AD device.

Decommission unit could be activated in two conditions only. First by direct order from the server which occurs when the engineer reports the missing device incident to his manager or by remotely connection with the server. Second, once the statement task period has expired. That means the statement task should indicate the expire time precisely, that means the AD device should be returned to the company for security reasons. The decommission unit guarantees that the confidential information will be safe and secure; otherwise, it will be removed before being is exposed.

7. Conclusions

This research provided a novel security system that is recommended for utilization on the Internet of Things technology supporting the current and coming generations. That system works to integrate the secrete keys and passwords into the security hardware device, safely away from any human touch. That technique solved the problem of leaking security information by keeping it inside the AD device and making it impossible to reach, even the technical engineers and company's managers. The traffic was securely encrypted using an asymmetric algorithm. That lightweight algorithm uses a public key concept to encrypt the traffic and a private key for decryption. The ECC algorithm developed a new equation to calculate the private key to utilize it next in the decryption step. Furthermore, this system employed an improved PUF security device feature to support the cryptography algorithm with an advanced unclonable random number to provide the highest level of security.

 doi:10.20944/preprints202406.1179.v1

Funding: Please add: This research was funded by Newcastle University.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Controlled Physical Random Function . Blaise Gassend, Dwaine Clarke, Marten van Dijk † and Srinivas Devadas. 13 Dec. 2002, 18th Annual Computer Security Applications Conference, 2002. Proceedings., pp. 149-160.
2. Goutsos, Konstantinos. Physical Unclonability Framework forthe Internet of Things. The UK - Newcastle : Newcastle University, 2019.
3. KINZA SHAFIQUE, BILAL A. KHAWAJA, FARAH SABIR, SAMEER QAZI, MUHAMMAD MUSTAQIM. Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. s.l. : IEEE Acess, 2020.
4. Analysis of Encryption Algorithms Proposed for Data Security in 4G and 5G Generations. Khalid Fadhil Jasim 1*, Kayhan Zrar Ghafoor2,3, and Halgurd S. Maghdid. 2022. ITM Web of Conferences 42, 01004 (2022).
5. Analysis of Standard Elliptic Curves for the Implementation of Elliptic Curve Cryptography in Resource-Constrained E-commerce Applications. Javed R. Shaikh, Maria Nenova, Georgi Iliev and Zlatka Valkova-Jarvis. Sofia, Bulgaria : s.n., 2017. IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS).
6. Elliptic Curve Cryptosystems. Koblitz, Neal. 1987, MATHEMATICS OF COMPUTATION, Vol. 48, pp. 203-209.
7. Constandinos X. Mavromoustakis, Jordi Mongay Batalla, George Mastorakis. Internet of Things (IoT) in 5G Mobile Technologies. Switzerland : Springer International Publishing Switzerland , 2016.
8. Lightweight and Secure PUF Key Storage Using Limits of Machine Learning. Meng-Day, Yu1, David M'Raihi, Richard Sowell,. 2011, International Association for Cryptologic Research, p. 16.
9. Brown, Daniel R. L. SEC 1: Elliptic Curve Cryptography. s.l. : Standards for Efficient Cryptography, 2009.
10. SEC 2 : Recommended Elliptic Curve Domain Parameters. s.l. : Standards for Efficient Cryptography, 2010.
11. Buckley, Eoin. SEC 4 Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV) - draft 2. s.l. : Standards for Efficient Cryptography, 2014.
12. Silicon Physical Random Functions. Blaise Gassend, Dwaine Clarke, Marten vandijk, and Srinivas Devadas. November 2002. Proceedings of the 9th ACM conference on Computer and communications security.