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

Aiham Altaher *

Posted Date: 26 July 2024

doi: 10.20944/preprints202406.1179.v2

Keywords: PUF; Improved PUF; ECC; security; Cybersecurity; Authentication; Authorization; Encryption; Decryption doi:10.20944/preprints202406.1179.v2

*Article*

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

**Aiham Altaher** *

School of Engineering at Newcastle University, Newcastle upon Tyne NE1 7RU, England; a.bystrov@ncl.ac.uk; martin.johnston@ncl.ac.uk

* 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).

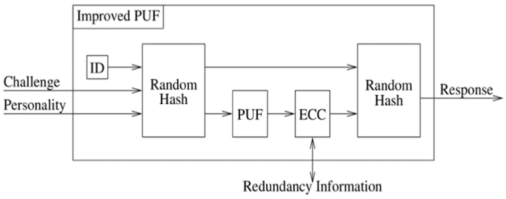


**Figure 1.** Using control to improve a PUF.

### *1.1. The Standard Security System*

The Internet of Things (IoT) commonly uses a standard security system to protect its services. That standard system combines encryption, authentication, and authorization protocols. Begin with encryption protocol that encodes the data traffic to authorise a specific party to access and understand the information. The **encryption** is used to secure the traffic between devices and servers and between devices themselves. The most common encryption protocols used in IoT systems are Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Datagram Transport Layer Security (DTLS) (4) (5). Those protocols proved a high level of security, but they still need development to match the future generation of technology. **Authentication** protocols focus on authorised devices or persons who can access the system for both management and use purposes. That means which devices or persons are permitted to join IoT system. Passwords, digital certificates, and biometric authentication are used with this mechanism in standard security systems. Access control policies specified from authentication protocols may include role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (6) (7). **Authorization** determines appropriate permissions to access the resources they are authorized to use and authenticated before. That means after successfully joined into an IoT system what permissions will provide to devices or users. In summary, authentication verifies the identity of users or devices, while authorization determines what actions or resources those authenticated entities are permitted to access. They are both in responsible to protect system and data from unauthorized access and illegal use. (1) (6) (8) (4).

## 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.

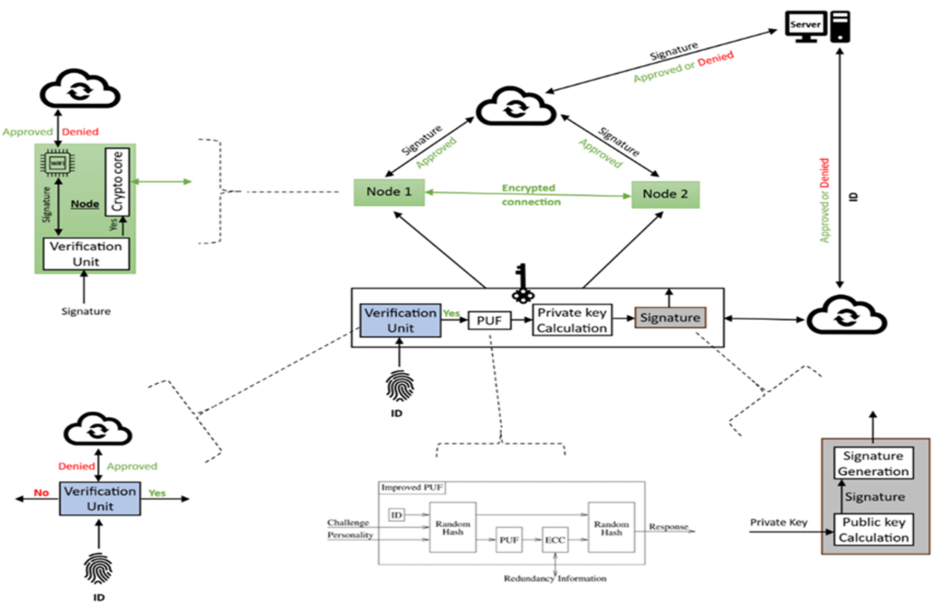


**Figure 2.** The architecture of novel security system.

## 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.

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**:

$$d = \quad R^3 + a^2 + b \, Mod \, p$$

**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.

$$Compute \quad C_1 = [k]G \quad \& \quad C_2 = M + [k]Q$$

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.

### *3.1. Full Educational Example*

In this example we are going to encrypt message **M={B}** using modified elliptic curve algorithm with an improved PUF device. Use the following element values:

$$y^2 = x^3 + 2x + 2\ (Mod\ 17)$$

**P=17**

**a = 2 & b = 2**

$$G(x_1, y_1) = (5, 1)$$

**n = 19**

**h = 1**

The solution:

**Step 1.** Encoding the Plaintext & Mapping the message on the curve

Let's assume {B} character equal { 11 } in ASCII table

Choose integer k as auxiliary base parameter {20}

Compute x = m * k + 1 = 11 * 20 + 1 = 221

Compute $y^2 = x^3 + ax + b\ (Mod\ P)$

y2 = (221)3 + [2*221] + 2 Mod 17

y2= 4

The message mapped on the curve on point (221, 4)

Step 2. Generating the Points

G (5, 1) → $1G(X_{1G}, Y_{1G})$

2G = G + G we have to apply a point doubling method

$$\lambda = \frac{3x_{1G}^2 + a}{2y_{1G}} = \frac{3 * 5^2 + 2}{2 * 1} = \frac{77}{2} = 77 * 2^{-1} = 81\ Mod\ 17 = 13$$

$$2^{-1} \to 2 * X = 1\ mod\ 17$$

X is a number between {1; n-1} And when multiply it with 2 mod 17 will equal 1

Solution: X=9 because (2 * 9) mod 17 = 1 → $\lambda = (9 * 9) mod\ 17 = 13$

$$x_{2G} = \lambda^2 - 2x_{1G} = 13^2 - (2 * 5) = 16 - 10 = 6\ Mod\ 17 = 6$$

$$y_{2G} = \lambda\,(x_{1G} - x_{2G}) - y_{1G} = 13(5 - 6) - 1 = -14\ Mod\ 17 = 3$$

2G= (6,3)

Now we have 1G (5,1) & 2G(6,3) → Let's generate 3G Note. 1G != 2G

3G = 1G + 2G → $3P = (x_{2G}, y_{2G}) + (x_{3G}, y_{3G})$ Where $3G = (x_{3G}, y_{3G})$

if 1G != 2G → $\lambda = \frac{y_{2G} - y_{1G}}{x_{2G} - x_{1G}} = \frac{3-1}{6-5} = \frac{2}{1} = 2$

$$x_{3G} = \lambda^2 - x_{1G} - x_{2G} = 2^2 - 5 - 6 = -7\ mod\ 17 = 10\ \ y_{3G} = \lambda\,(x_{1G} - x_{3G}) - y_{1G} = 2(5 - 10) - 1 = -11\ mod\ 17 = 6$$

3G= (10,6) And thus we can calculate all the points,

1G= (5, 1)
2G= (6, 3)
3G= (10, 6)
4G= (3, 1)
5G= (9, 16)
6G= (16, 13)
7G= (0, 6)

8G= (13, 7)
9G= (7, 6)
10G= (7, 11)
11G= (13, 10)
12G= (0, 11)
13G= (16, 4)
14G= (9, 1)

15G= (3, 16)
16G= (10, 11)
17G= (6, 14)
18G= (5, 16)
19G= Ɵ

Total Points = n - 1 = 19 - 1 = 18 points

**Step 3.** Calculate private key.

Sending a challenge to PUF device to generate an advanced random number. Once the random number is ready, the algorithm can calculate the private number.

$$d = \boldsymbol{R}^3 + \boldsymbol{a}^2 + \boldsymbol{b}\ \boldsymbol{Mod}\ \boldsymbol{p}$$

R: Random number comes from PUF device

$\boldsymbol{a}, \boldsymbol{b}$ Two elements on the curve.

$\boldsymbol{p}$: Specifying the finite field $\boldsymbol{F_p}$

Next step is Generate the public key:

**Step 4.** Calculating the public key:

Random number (d) in the interval [1; n - 1].

Compute Q = d G. where.

Q: Public Key

d: Private key

G: Generator Point

Let's specify a private key d For Example d=5.

Q=5G → (9, 16) It is a public key.

**Step 5.** Calculate K value:

Sending a challenge to PUF device to generate an advanced random number. Once the random number is ready, the algorithm can calculate the K value.

$$K = \boldsymbol{R}^3 + \boldsymbol{a}^2 + \boldsymbol{b}\ \boldsymbol{Mod}\ \boldsymbol{p}$$

**Step 6.** Applying the encryption equation:

Compute $\boldsymbol{C_1} = [\boldsymbol{k}]\boldsymbol{G}$ & $\boldsymbol{C_2} = \boldsymbol{M} + [\boldsymbol{k}]\boldsymbol{Q}$

G: Generator Point

M: Plaintext.

Q: Public key

$$Ciphertext\ (C_1, C_2)$$

$$C_1 = [k]P$$

$$C_2 = M + [k]Q$$

-Let's assume k ∈ [1; n-1] Let's say k= 13

P is the base point (5, 1).

Q is the public key (9, 16).

M is the message mapped on the curve (221, 4).

$$\boldsymbol{C_1} = \boldsymbol{13}(\boldsymbol{5}, \boldsymbol{1}) = (\boldsymbol{16}, \boldsymbol{14})$$

$$\boldsymbol{C_2} = (\boldsymbol{221}, \boldsymbol{4}) + [\boldsymbol{13}](\boldsymbol{9}, \boldsymbol{16}) = (\boldsymbol{7}, \boldsymbol{8})$$

$$\boldsymbol{Ciphertext}\ \left((\boldsymbol{16}, \boldsymbol{14}), (\boldsymbol{7}, \boldsymbol{8})\right)$$

**Step 7 & 8** will be transmitting & receiving the ciphertext to the destination.

**Step 9.** Applying the decryption equation:

$$\boldsymbol{M} = \boldsymbol{C_2} - [\boldsymbol{d}]\boldsymbol{C_1}$$

$$\boldsymbol{M} = (7, 8) - [5](16.14)$$

$$\boldsymbol{M} = (\boldsymbol{221}, \boldsymbol{4})$$

**Step 10.** Mapping the message back

It is the last step, map the point back by computing (x - 1) / K

K=20, x =221

(221 – 1) / 20 = 11

Decoding the plaintext by ASCII code 11 = '**B**' for example.

## 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:

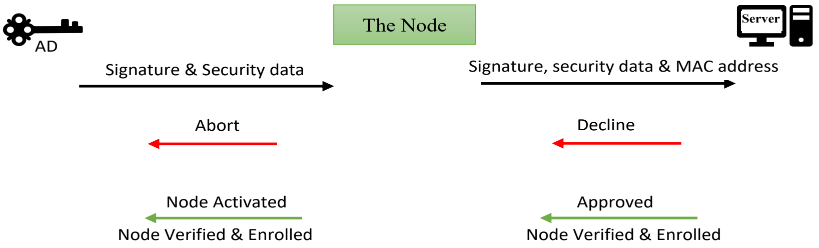


**Figure 3.** The AD device for node verification and enrolment.

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 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.

doi:10.20944/preprints202406.1179.v2

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.

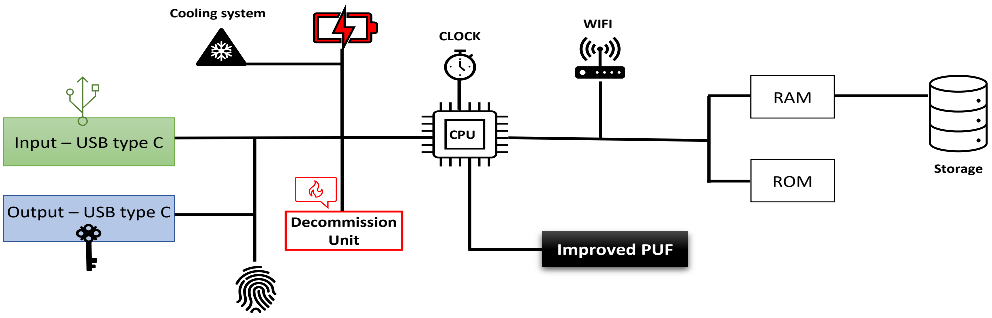


**Figure 4.** The Authority Device structure.

## 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.

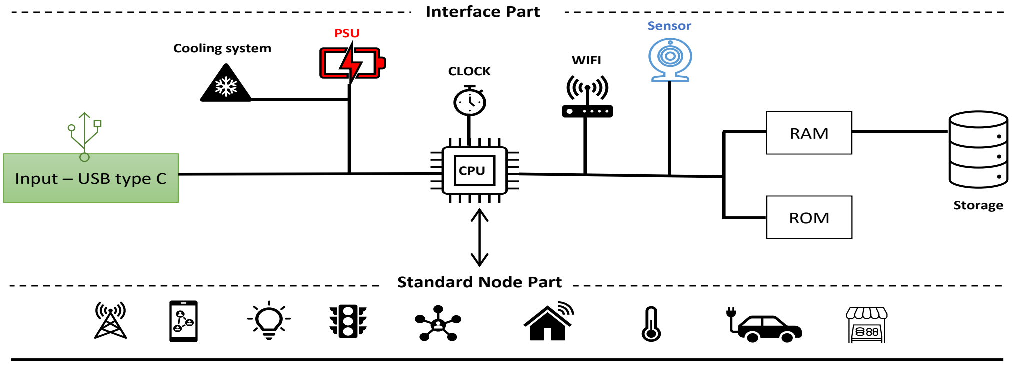


**Figure 5.** The node structure.

### 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.

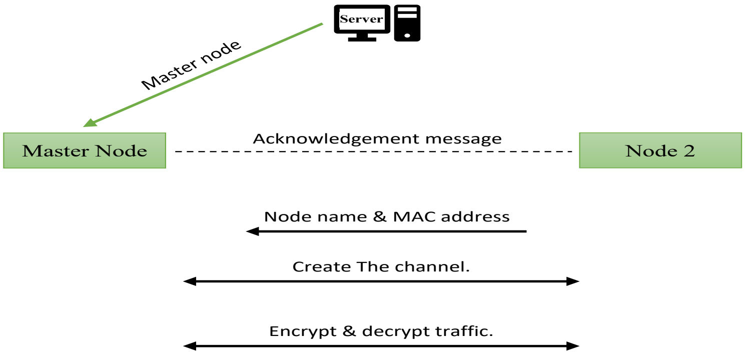


**Figure 6.** Create the channel and encrypt the traffic.

### 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.

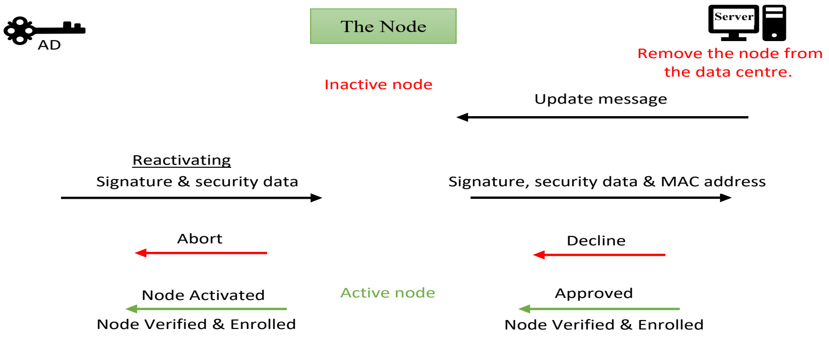


**Figure 7.** Decommission and reauthentication task.

*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.

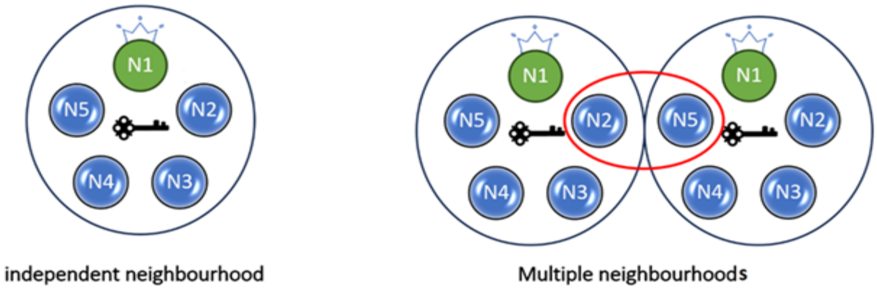


**Figure 8.** Topologies type.

## 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.

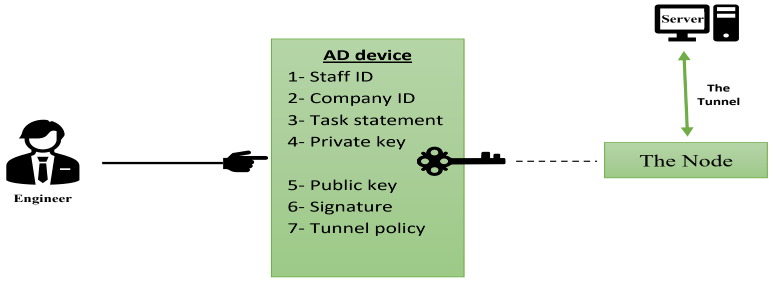


**Figure 9.** The AD device contains secret info.

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 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.

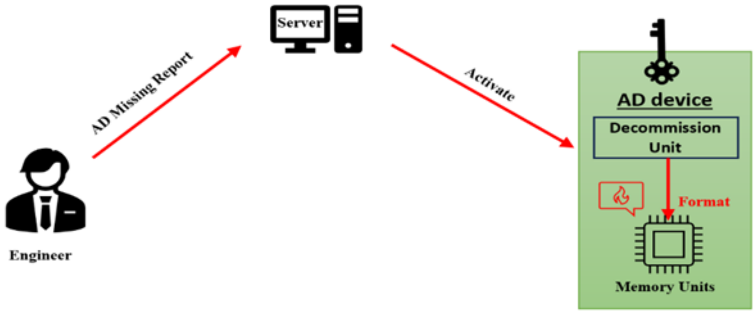


**Figure 10.** Decommission unit task in the AD device.

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.

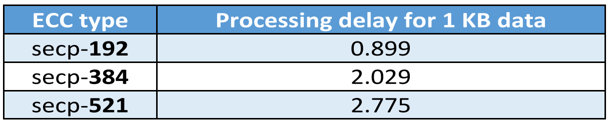
## 7. Implementing the Modified ECC algorithm on Internet of Things

The new security system will employ the improved PUF device with the improved Elliptic Curve Cryptography algorithm 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 to support the internet of things and fifth generation with a significantly fast and modern method. A lower processing time will 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 to provide a higher level of security while maintaining the speed feature.

### *7.1. Applying Elliptic Curve Cryptography algorithm on the Internet of Things*

In this point python was used to apply three different types of ECC algorithms on the system, First, secp-192 this kind of ECC algorithm using 192 bits key length compared to sec-384 which using longer key length. Finally, secp-521 this type has the longest key length in the ECC algorithms. Processing delay values were plotted and registered when the algorithms applied on 1 KB data message, Table (1) shows that results and finding.

**Table 1.** Processing delay values for ECC algorithm.



| ECC type | Processing delay for 1 KB data |
|---|---|
| secp-**192** | 0.899 |
| secp-**384** | 2.029 |
| secp-**521** | 2.775 |

Secp-192 registered the lowest values of processing delay ever because, short key length was utilized on this type on ECC algorithm, the delay values were estimated my seconds, for this type is 0.8 seconds. This value increased gradually when the security level went up when 384 bits key length applied, it shows 2.02 seconds for secp-384 type. The last type is secp-512 shows the top delay value with slight increase to 2.77 seconds after successfully encryption and decryption methods achieved. Figure (11) illustrates that difference.

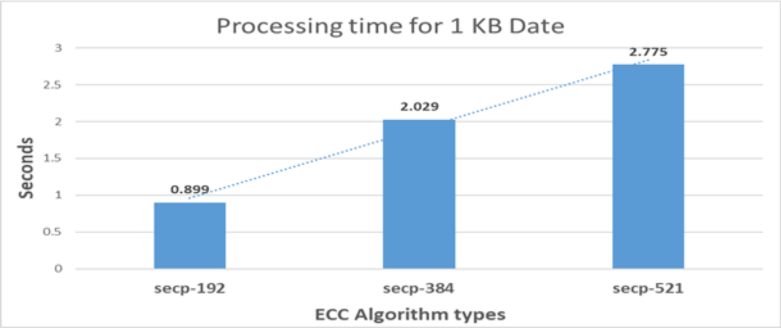


**Figure 11.** Processing delay values for ECC algorithm.

### *7.2. Applying Rivest Shamir Adleman Algorithm on the Internet of Things*

For comparison purposes, three separate types of RSA algorithms were applied to the system using Python. The first type uses 1536 bits key length, second type has 2048 bits key length, the last type of RSA algorithm is RSA-3048 with the longest key length. Indeed, the RSA algorithm has longer key lengths but that will not include in this study for concentration on the short keys length for comparison and educational purposes. All results and finding were recorded and written below on the table (2).

**Table 2.** Processing delay values for RSA algorithm.

| RSA type | Processing delay for 1 KB data |
|---|---|
| RSA-1536 | 4.016 |
| RSA-2048 | 5.996 |
| RSA-3048 | 10.598 |

When the RSA algorithm types were applied on a **1 KB** data message using the python language, the processing delay values estimated by seconds and registered as the flowing results: RSA-1536 algorithm type recorded 4 seconds to complete encryption and decryption steps, this value slightly increased to 5,9 seconds when the security level was raised up by using a 2048-bit key length. RSA-3048 shows the significant rise value to 10,5 seconds after successfully encrypted and decrypted that data message. Consequently, the delay parameter value increases directly with the key length increases. Figure (12) displays that finding.

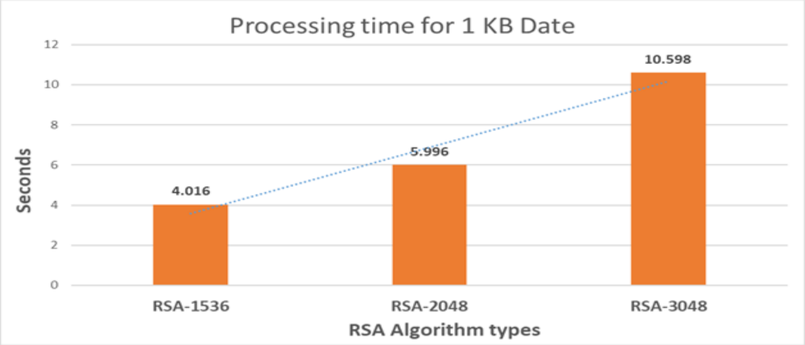


**Figure 12.** Processing delay values for RSA algorithm.

*7.3. The Comparison Results between ECC and RSA Algorithms*

Using Python to apply ECC and RSA to the system shows a clear variation in processing delay values. Figure (13) illustrates this variation.

For both algorithms the processing delay values increased coinciding with increasing key's length. That occurred when the level of security went up, that means the latency time rising up with security level. In this occasion, RSA algorithm was defeated by ECC algorithm, with very low latency time of all ECC types compared with RSA, The **ECC algorithm won** and acquired the speed point against RSA algorithms.

With 192 bits key length, ECC algorithm registered just 0.8 seconds against 4 seconds of RSA-1536. When ECC algorithm increased the level of security, it uses secp-384 the latency time increased slightly to reach 2 seconds only opposite 5.9 seconds when the RSA algorithm used 2048 bits key length. Finally, when the ECC algorithm has used the longest key length, the delay value displayed extremely low indicator compared to RSA-3048, it is 2.7 seconds and 10.5 seconds respectively.

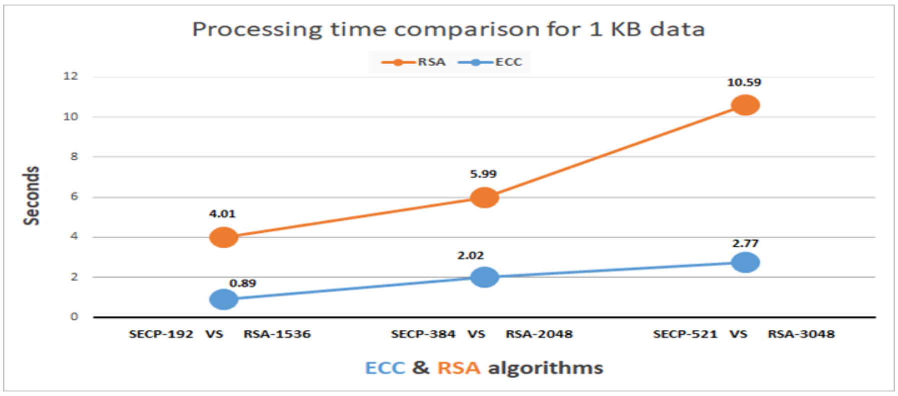


**Figure 13.** Processing time comparison for ECC & RSA.

In conclusion, ECC algorithm is extremely faster than RSA with all keys size. That high speed will support the system with a suitable security protocol to secure the network traffic. However, the weak point notified on the security level of ECC against RSA, Therefore, the recommendation was to solve that defect by developing the algorithm to won on security aspect as well as distinguishing on the speed field. That what was achieved to make the ECC algorithm the best solution for the current and the next generation of technology.

## 8. A Comparison Study between the Standard and the Novel Security System

In this stage, an academic comparison is made between the standard system that is currently being used to support IoT technology and the novel system. The main difference between them is that, while the novel system uses encrypted secret keys, the standard system transmits secret keys in plaintext that is disclosed to company's engineers. Trust in the company's engineers is the main defect that makes the system vulnerable. To solve this problem the novel system uses Zero Trust Network Access (ZTNA) concept to manage the network. Furthermore, the standard system does not use a security device compared to the novel system, which has an AD device supported by an improved Physical Unclonable Framework. The PUF device was used in the novel security system to generate an advanced private key. On the other side, the standard system produces a simple random number to calculate the private keys. For the **encryption** step, the modified ECC algorithm raises the security level compared with any other algorithm, such as RSA. The **authentication** phase with the standard system is achieved manually by adding a username and password to join a new terminal node to the domain system, compared with the automatic authentication task achieved by the AD device. The **authorizations** are accomplished individually with a classic security system, against a centralization technique in the novel system to process them. Moreover, the decommissioning task is performed manually when the system administrators want to remove any terminal nodes. That compared with a central update on the node list on the company's server. Elliptic curve cryptography is a super-fast algorithm compared with another lightweight algorithm, and that was proved in section 7. The system reliability and safety are extremely strong with our novel system because all the confidential data is included in the AD device without any human touch or knowledge, compared with the vulnerable techniques used with the standard systems. Finally, the standard system is significantly slower for the system installation stage because it does not use centralization for management, such as the novel system. All those features pushed that system to be compatible with the current and future generations of technology. The following table (3) shows and explains the difference between the standard system and the novel recommended system for security on the IoT systems.

**Table 3.** The comparison between security systems.

| | Standard system | Novel system |
|---|---|---|
| Secret keys | plaintext | Encrypted |
| System Safety | Trust Engineers | Zero Trust Network Access |
| Hardware component | None | Improved PUF |
| Authority device | None | Yes |
| Key generation method | Good | Advanced |
| Keys distribution | Manually (weak) | Automatically (strong) |
| Encryption | Strong | Advanced |
| Cryptography algorithm type | Ratchet (good) | Modified ECC (advanced) |

| | | |
|---|---|---|
| Authentication | Manually (weak) | Automatically (strong) |
| Authorisation | Individually (weak) | Centrally (strong) |
| Nodes decommission task | Individually (weak) | Centrally (strong) |
| Algorithm speed | Fast | Faster |
| System Reliability | Strong | Advanced |
| System Installation | Slow | Speed |
| System compatibility | Matched with current technology | Matched with current & coming technology |
| Environment | 4G, 5G | 5G & 6G |

## 8. 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.

**Author Contributions:**.

**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. 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. 2. **Goutsos, Konstantinos.** *Physical Unclonability Framework forthe Internet of Things.* The UK - Newcastle : Newcastle University, 2019.
3. 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. 4. *Internet of Things security: A survey.* **Fadele Ayotunde Alabaa, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi.** 2017, Journal of Network and Computer Applications, Vol. 88, pp. 10-28.
5. 5. **András Varga, Rudolf Hornig.** *AN OVERVIEW OF THE OMNeT++ SIMULATION ENVIRONMENT.* Budapest, Hungary : s.n., 2016.
6. 6. **(Ed.), Phillip Rogaway.** *Advances in Cryptology – Crypto 2011.* Santa Barbara, CA, USA : Springer, August 14-18, 2011.
7. 7. **Niels Ferguson, Bruce Schneier, Tadayoshi Kohno.** *Cryptography Engineering: Design Principles and Practical Applications.* s.l. : Wiley 1st edition, March 2010.
8. 8. *Elliptical Curve Cryptography Design Principles.* **J VenkataGiri, Dr. ASR Murty.** 2021. International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT).
9. 9. *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).

10. 10. 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).
11. 11. *Elliptic Curve Cryptosystems.* **Koblitz, Neal.** 1987, MATHEMATICS OF COMPUTATION, Vol. 48, pp. 203-209.
12. 12. **Constandinos X. Mavromoustakis, Jordi Mongay Batalla, George Mastorakis.** *Internet of Things (IoT) in 5G Mobile Technologies.* Switzerland : Springer International Publishing Switzerland , 2016.
13. 13. *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.
14. 14. **Brown, Daniel R. L.** *SEC 1: Elliptic Curve Cryptography.* s.l. : Standards for Efficient Cryptography, 2009.
15. 15. —. *SEC 2 : Recommended Elliptic Curve Domain Parameters.* s.l. : Standards for Efficient Cryptography, 2010.
16. 16. **Buckley, Eoin.** SEC 4 Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV) - draft 2. s.l. : Standards for Efficient Cryptography, 2014.
17. 17. *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.
18. 18. *Implementation of ElGamal Elliptic Curve Cryptography Over Prime Field Using C.* **Debabrat Boruah, Monjul Saikia.** India : s.n., 2014. ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.
19. 19. *The State of Elliptic Curve Cryptography.* **NEAL KOBLITZ, ALFRED MENEZES, SCOTT VANSTONE.** 2000, Kluwer Academic Publishers, Boston. Manufactured in The Netherlands, Vol. 19, pp. 173–193.
20. 20. *Towards 5G Security Analysis against Null Security Algorithms Used in Normal Communication.* **Run Zhang,1 WenAn Zhou ,1 and Huamiao Hu2.** 2021, Hindawi Security and Communication Networks, p. 15.
21. 21. **Buckley, Eoin.** *SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate draft - 1.* s.l. : Standards for Efficient Cryptography, 2013.
22. 22. *AES, DES, and RSA: A Comprehensive Study on Data Security Mechanisms.* **Kapoor, Aditya.** 2018, IJCAM Research Consultant, Indore , India, p. 9.
23. 23. **Maletsky, Kerry.** *RSA vs ECC Comparasion for Embedded system.* s.l. : Microchip, 2020.
24. 24. **Shaheen, Mai Helmy.** Hybrid Encryption Algorithms Over Wireless Communication Channels. Oxon : A SCIENCE PUBLISHERS BOOK, 2022.
25. 25. Advances in Security Technology, Security Analysis of "A Novel Elliptic Curve Dynamic Access Control System". **Haeng-kon Kim, Tai-hoon Kim, Akingbehin Kiumi.** China : s.n., 2008. International Conference SecTech.
26. 26. *Cryptographic Analysis of DES and RSA Algorithm Using the AVISPA Tool andWSN.* **Shailendra Singh Gaur, Megha Gupta, and Gautam Gupta.** 2021, Proceedings of 3rd International Conference on Computing Informatics and Networks, Vol. 167.
27. 27. **Tom St Denis, Simon Johnson.** *Cryptography for Developers.* s.l. : Syngress, 2006.
28. 28. **Sumit Singh Dhanda, Brahmjit Singh, and Poonam Jindal.** *Elliptic Curve Cryptography: A Software Implementation.* India : Department of Electronics and Communication Engineering, National Institute of Technology, 2021.
29. 29. *Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography.* **Padma Bh, D.Chandravathi , P.Prapoorna Roja.** 2010, (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, p. 05.
30. 30. **Burt Kaliski, Terry S. Arnold,.** *IEEE Standard Specifications for Public-Key Cryptography.* New York : American National Standards Institute, 2000.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideavs, methods, instructions or products referred to in the content.