Homomorphic Encryption with Enhanced Elliptic Curve for Mobile Wireless Network Security

Mohsin Ali[1], Nurgul Nalgozhina[1], Olzhas Tasmagambetov[2], and Yerzhan N Seitkulov[2]

[1] *International Information Technology University, Manas St. 34/1, Almaty, 050040, Kazakhstan*
[2] *L.N. Gumilyov Eurasian National University, Satpayev St. 2, Astana, 010000, Kazakhstan*

Abstract

With the rapid development of wireless networks, security and accessibility are two crucial issues in device-to-device (D2D) transmission. These networks are typically created for data morality and confidentiality. They could easily acquire wireless sensor nodes because of their design. Additionally, the group's operational nodes are the most alluring to attackers. Therefore, research on data aggregation security is crucial in order to address this security threat. To secure data aggregation in sensor networks in this situation, a number of encryption techniques with high communication overhead have been proposed. We have developed the Secure Information Sharing protocol (SeIS), which stands out for using homomorphic encryption.

We choose Elliptic Curve Cryptography (ECC) curve 25519 with a general discrete-logarithm algorithm for optimization in order to distinguish participants who are exchanging data with other parties by keeping track of the current state of wireless devices and to identify function by key trace communication among User Devices (UD) and other developed nodes. We use advanced AES operations for performance evaluation because they have a shorter computational time, very little communication overhead, and a small increase in calculation that is negligible compared to correspondence costs, which increases the network's lifespan. Additionally, on a 1.50 GHz microprocessor, one elliptic curve point can be multiplied in just 2.623 seconds.

Keywords

Secure Information Sharing protocoL, Elliptic Curve Cryptography, generic discrete-logarithm, Authentication, Privacy, AES

1. Introduction

Wireless sensor networks have captured significant research attention in recent years due to their widespread solicitations in numerous home and commercial applications [1]. A wireless sensor network is constructed using a number of base stations and small sensor devices with constrained battery life, memory, bandwidth, and processor power. The network's lifespan is harmed by the energy consumption of these devices' communication [25]. Energy needed for communication [35] is especially much more advanced than the energy needed for calculation [2]. As a result, a technique that significantly slows down communication movement [3] in wireless sensor networks has been proposed to reduce the volume of data packets that are communicated through sensor nodes. Security in wireless sensor networks is a crucial issue [24].

Unreliable results could result from malicious aggregation carried out by a compromised aggregator node. according to the discussion in. [4] As a result, sensor data at intermediate nodes are more exposed.

Proceedings of the 7th International Conference on Digital Technologies in Education, Science and Industry (DTESI 2022), October 20–21, 2022, Almaty, Kazakhstan

EMAIL: m.farhad@iitu.edu.kz (Mohsin Ali); n.nalgozhina@iitu.edu.kz (Nurgul Nalgozhina); 5999452@mail.ru (Olzhas Tasmagambetov); yerzhan.seitkulov@gmail.com (Yerzhan N Seitkulov)
ORCID: 0000-0001-9737-3273 (Mohsin Ali); 0000-0003-0254-8670 (Nurgul Nalgozhina); 0000-0003-1120-5741 (Olzhas Tasmagambetov); 0000-0002-5172-8339 (Yerzhan N Seitkulov)

Data packets are encrypted once and only decrypted at the base station in an end-to-end or concealed data aggregation scheme [37]. Homomorphism-based cryptosystems are employed for this privacy [26]. These cryptosystems directly process the ciphertexts, reducing communication overhead and security flaws at intermediate nodes [27]. Furthermore, Priyadharshini, T. [36] previously presented a key distribution scheme, but it cannot be used for decentralised D2D communication. To ensure message confidentiality and generate a shared session key for encryption, we have suggested the secure information sharing protocol (SeIS).

The recipient is expected to send a crucial piece of information to the evolved node B (eNB) in order to decode the facts; as a result, performing acceptance is not rejected, which is a crucial aspect of the proposed protocol. We choose the Elliptic Curve Cryptography (ECC) curve 25519 to optimise the algorithm. This paper makes two main contributions: 1) During configuration, we provide a SeIS protocol in wireless transmission environments to distribute the property among the customers in a morally and secretively manner across end-to-end encoding. Additionally, the receiver can alert the manager to the incident by authenticating signatures and reporting a response. As a result, the false information might not reach other customers.

1.1. Contribution

- We create a register table in eNB (Evolved Node B) in favour of unbounded-voyage identification to improve the accessibility of SeIS protocol at the key allotment stage. The register table is also in use, suggesting the artificial individuality to the associated original individuality to ensure monitorability.
- We use the curve 25519 optimal expansion field for quick multiplication and quick inversion in order to optimise the security features.

1.2. Paper Organization

The rest of this article's description is as follows: In Section 2, a structure model is presented. Section 3 provides background information and an explanation of the suggested protocol's fundamentals. The intended protocol is generated and listed in Section 4; Section 5 also includes a security analysis. The suggested protocol's implementation is evaluated in Section 6 using thorough simulations. A case study is presented in Section 7 and this paper is concluded in Section 8.

2. System Model

We look at the method used to connect devices in a wireless network. Through wireless networks, consumers can access their profiles, which can be used to foster customer authenticity. Wireless is typically used to distribute media components among communal networks, but some UEs can recognise the nodes and gather these communications. As a result, rather than speaking with a cellular base station, another person can immediately communicate with those UEs to obtain sensitive information. We look at a three-layer calm stratified framework. Sensing layer quiet with a variety of surveillance tools are used to collect data first, which is then transferred to a set of entrances that combine the collected data before sending it over the internet to a centre for implementation.

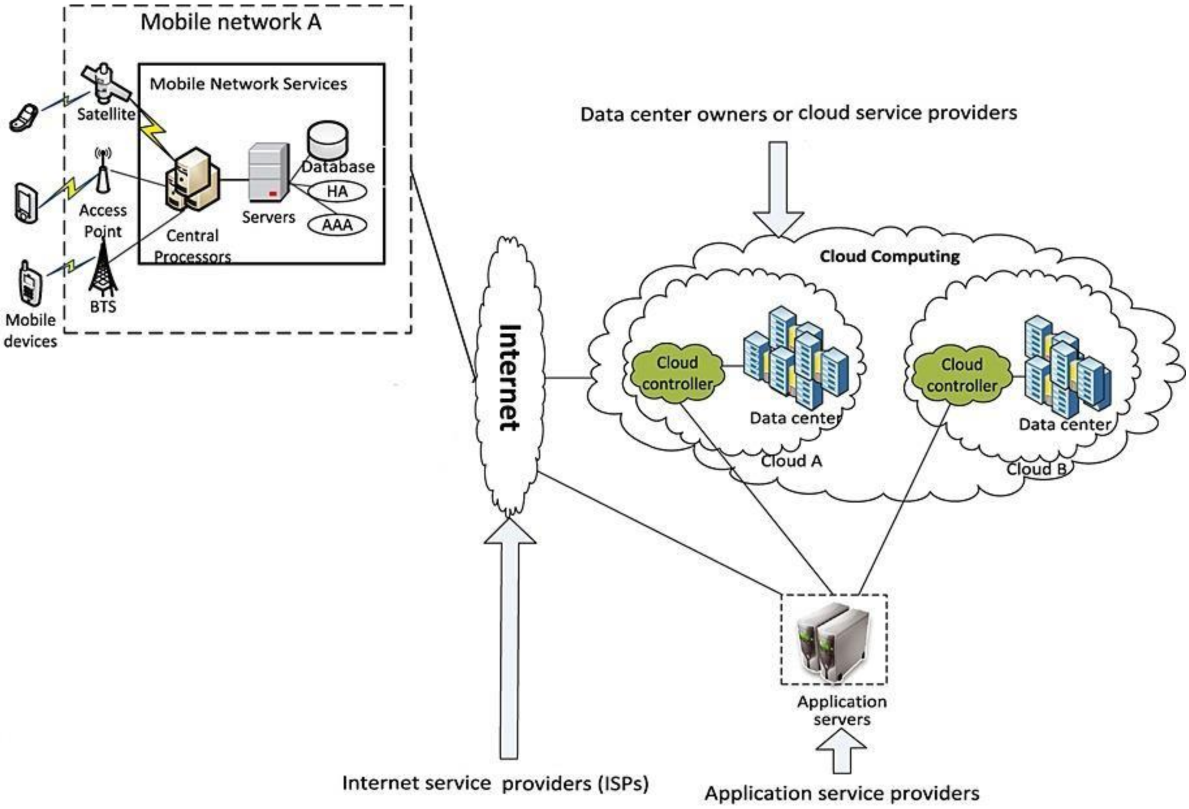

Figure 1: Structure prototype for media components broadcast

The application layer needs suitable judgments as per data evaluation outcome.

Table 1
Symbols and Explanations

Symbols	Explanations
eNB	Evolved Node B
TA	Trust Authority
WNS	Wireless Network Server
UE	User Equipment
RID	Real Identity of Entity
PID	Pseudo-identity of Entity
$H_0(\cdot), H_1(\cdot)$	Hash Secure Function
X_i, x_i	Public and Private Key of Entity
$Enc_{sk}(\cdot), Dec_{sk}(\cdot)$	Encryption and Decryption Algorithm
‖	String Concatenation
P	Base Point of Elliptic Curve
n	Integer Order of P

The procedure includes of TA, eNB, WNS and UE.

TA: Sharing public key for existents, and producing the secure boundaries.

eNB: Combining mobile UEs and wireless network server.

WNS: Supplying customers communal benefits as well as communications allotments over wireless network.

UE: Illustrating the individual user equipment.

The detailed model will be given in the later section with security analysis.

3. Preliminaries

Our proposed method is based on bilinear pairing and Diffle-Hellman key exchange (DHKE). As a result, we examine and explain in detail here. (See [22] for a more in-depth explanation.).

3.1. Bilinear Coupling

Let $G1$ and $G2$ be two cyclic accumulative sets produced by $g1$ and $g1$ appropriately.

Therefore, the bilinear map $\hat{e}$: $G1 \times G1 \rightarrow G2$ gratifying the subsequent characteristics, 1) Bilinear: for the entire P, $Q \in G1$ and $\forall a$, $b \in Z*$, where $Z* = \{x \in Z | 0 \leq x < q,\ gcd(x, q) = 1\}$. We have

q q

$\hat{e}(aP, bQ) = \hat{e}(P, Q)ab$.

2) Symmetric: $\hat{e}(P, Q) = \hat{e}(Q, P)$.

3)Non-degeneracy:$\forall P, Q \in G1$, we have $\hat{e}(P, Q) = 1G2$ if $P = 1G1$ or $Q = 1G1$.

4) Measurable: an effective algorithm to determine $\hat{e}(P, Q)$.

As explained in [5], suchlike a permissible map might be built through the adjusted Weil of Tate pairing over elliptic curve as well as a 160-bit prime order q is supposed to achieve an 80-bit security level. In our chosen curve 25519, a 255-bit integer might be separate into 4 or 8 or 10 or 12 parts to adapt the capabilities of various processors to collect 128 bit security level; an optimal expansion field is linked to a specific number of fragments.

3.2. Paillier Homomorphic Encryption

The cipher text of message $m1$ and $m2$ can smoothly identify the decrypted solution of $Encsk$ $(m1)$ $\cdot Encsk$ $(m2)$ is similar to the decrypted communication $Encsk$ $(m1 + m2)$. This assumes the adjunct conclusion about dual various plain texts possible to acquire through formerly relevant coded texts, instead of combining system collectively within plain texts prior to encrypt. Such characteristic will be completely utilized among the biography identical procedure.

4. Proposed Protocol

To protect information during wireless transmission, we propose a secure information sharing protocol that combines the advantages of symmetric and public key cryptography. To achieve the goal of protection in wireless transmission, we investigate unite PKI-supported signature as symmetric key encryption. Entity verification and data influence are accomplished through the use of digital signatures. Symmetric key cryptography may be used as an option to ensure data privacy.

4.1. System Initialization

System Parameter origination: TA produces the system parameter assembling (q, $g1$, $g2$, $G1$, $G2$, $\hat{e}$), as well as two unique manner hash functions $H0$: $\{0,1\}* \rightarrow Z*$, $H1$: $\{0,1\}* \rightarrow G$. Moreover, TA chooses individual secure symmetric encryption algorithm $Encsk$ $(\cdot)$ as well as an Elliptic Curve $E(a, b)$. Ultimately, the system parameters is being released,

$$params = (q, g1, g2, G1, G2, \hat{e}, H0, H1, Encsk\ (\cdot), P, n) \qquad (1)$$

Suppose m detecting items maintaining $\{si\}m$ detected principles and desiring to convey authorities through utilization essence across a distributed network of intelligent equipments. Suggested elliptic curve arguments are submitted in NSA suite B cryptology [6]. A planning operation should maintain the strategy of this additive homomorphic characteristic, through supplement of two plaintexts ($s1$ + $s2$) designed for the sake of adjunct of their identical elliptic curve items $M1 + M2 = f(s1) + f(s_2)$. We utilized the mapping operation explained in [7] which plots an integer $i \in F_p$ for the sake ofitem iG acquired through summing the creator point G to independently i periods.

$Encryption$: After dispatching a bunch application, the gateway arbitrarily chooses a from FP and announce her public key aG. Every detection element i, in occupancy about a detected measure $Si \in FP$, chooses a arbitrary $ri \in FP$ and estimates the pair $(riG, Mi + ri(aG))$ where $Mi = f(Si)$. This couple of items are the encryption of si, which is utilizing the elliptic bend elgamal cryptographic system.

Individually such two elements relate about elliptic curve E as well as contains two counterparts x and y of the volume of the modulus p (e.g. 255 bits). Such couple of thing is encoding of si, which is utilized elliptic curve elgamal cryptographic system. By this point squeezing methods, besides of x align, just single additional bit is needed for illustrate the y align (whereas here is merely two remedies for Weirstrass formula to illustrates the curve), consequent within a element of length $1 + log2p$ segments. Therefore for describe $Enc(si)$, we integrate the two points to acquire a ciphertext Ci of length $2(1 + log2p)$ bits. We notice $Ci = Enc(si)$.

$Distribution$: Next to encoding, every detection item i allocates the acquired ciphertext Ci to n intelligent targets utilizing $a(k, n)$ Shamir secret distribution method. Next, the item i haphazardly picks a polynomial Pi in Fq were q remains a bigger prime compare to encoded contents, e.g. 328 segments as p of length 163 bits. A polynomial Pi is the extent of $k - 1$ and over steady collaborative the ciphertext Ci. Thus item i allocates allowances to n nodes as $\{Pi(Id(j))\}n$, where $P(Id(j))$ i becomes dividend, obtained through entity j (among community attributive $Id(j)$) based on detection element i. Through utlizing identifiers we ensure that portions obtained along with a mixing entity j are assessments of various polynomials at the identical index $Id(j)$, that permits their association.

$Combination$: Every object j merges the m segments, obtained from detecting elements form a macro- portion $Q_j = \sum_{i=1}^{m} P_i(Id(j))$. Such macro-portion Q_j is further the analysis of the super polynomial $Q = \sum_{i=1}^{m} P_i$ at $Id(j)$, $Q(Id(j))$. After that Q_j is transferred to the portal for furthur dispatch them to the monitoring center across the Internet. After obtaining k shares $\{Q(Id(j))\}_{j=1}^{k}$, gateway interposes them to retrieve the brilliant polynomial Q holding as steady factor of the sum of ciphertexts $\sum_{i=1}^{m} C_i$. Utlizing this complete accumulative homomorphic attribute of the encryption system which is explained in (1), this aggregate might be decrypted to the summation of plaintexts $\sum_{i=1}^{m} S_i$.

Server Registration: The $Server$ records to eNB through RID_{WNS}. TA first estimates $PID_{WNS} = H_0(RID_{WNS})$, and makes the Paillier encryption public key and private key (PK, SK) for $Server$. Next the pair (PK, SK) will be safely delivered to $Server$. TA release PK to the system.

User Enrollment: A calculates $PID_i = H_0(RID_i)$ while UE_i enrolls to the method with RID_i. Next TA arbitary choices an integer $x_i \in Z_q^*$ while the private key of UE_i as well as settles the public key $X_i = g_1^{x_i}$. The combination (X_i, x_i) transmit to UE_i through the safe channel. Additionally, TA establish the vital private key x_0, and public key $X_0 = g_1^{x_0}$.

4.2. User Enrollment Corresponding in WNS

UE_i and UE_j individually present their enrollment solicit to the WNS through safe channel. UE_i transfers the message $\{PID_i \parallel (I_i)_{PK} \parallel |I_i| \parallel Li \parallel T_i\}$, wherever (I_i) PK is encoded through the Paillier homomorphic algorithm. PID_i becomes artificial - individuality of UE_i. $|I_i|$ is the complete concern figure of UE_i based on concern TABLE 2. I_i and I_j describe the concern vector of consumer i and j. Moreover, L_i illustrates the user's geographical position. T_i is the instants. Through all substances enlisted within the framework the WNS decides an authenticity among consumers:

1) WNS calculates $(I_{ij})_{PK}$=$(I_i)_{PK} \cdot (I_j)_{PK}$, since we referred earlier, in this Paillier homomorphic encryption, I_{ij} presents the summation effect for two consumers' concern vectors. WNS be able to decrypt $(I_{ij})_{PK}$ by utlizing own Paillier private key.

Table 2
Concern Index Table

Entity	Index 1	Index 2	Index 3	…	Index n-1	Index n
UE_i	0	1	1	…	1	1
UE_j	1	1	1	…	0	1

$|I_{ij}|$ indicate the ordinary benefit about UE_i as well as UE_j. Thus, an equation uniformity record might be measured as below,

$$S(i,j) = \frac{|I_{ij}|}{\sqrt{|I_i| \cdot |I_j|}} \tag{2}$$

2) The attachments might be numerical from the alliances [8].

4.3. Secure Information Sharing Protocol

Based on above mention, the highest reliable contestant in $SeIS$ may be identified through their reliability. The complete method of $SeIS$ is explained as follows.

1) The consumer arbitary selects $d_j \in [1, n-1]$ those needs to obtain the details in wireless network and estimates $Q_j = d_j P$. After that he transfers the wishing message $\{PID \parallel Q_j \parallel h(M) \parallel T_j \parallel HMAC_{xj}(\cdot)\}$ over eNB. Indicate such $h(M)$ becomes exponent of media substance M.

2) During obtaining communication from UE_j , eNB initially verifies the morality of this message as well as the consumer's uniqueness. Next dispatches the asking message to WNS in favour of investigating a conveing applicant as per Table 3. Later, WNS refunds the trustworthiness Cr_{ij} of candidate. eNB selects $d_0 \in [1, n-1]$ and calculates $Q_0 \in [1, n-1]$ as well as estimates $Q_0 = d_0 P \cdot$ eNB produces the sign of the claimed media substance as well as the share key K_{0j} through UE_j .

Table 3
Authenticity Table

Entity	$\boldsymbol{PID_1}$	…	$\boldsymbol{PID_i}$	…	$\boldsymbol{PID_i}$
PID_1	NAN	…	Cr_{1i}	…	Cr_{1n}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
PID_i	Cr_{i1}	$\cdots$	NAN	$\cdots$	Cr_{in}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
PID_n	Cr_{n1}	$\cdots$	Cr_{ni}	$\cdots$	NAN

3) eNB dispatches message $\{Q_0 \parallel \sigma_1 \parallel Cr_{ij} \parallel HMAC_{x0}(\cdot)\}$ to UE_j, where σ is the sign of desired media substance signed by eNB. UE_j verifies the signature of eNB as well as produces the share key for obtaining the decryption key. To notify UE_i, eNB transmits message $\{PID_j \parallel Q_j \parallel Q_0 \parallel \sigma_1 \parallel Cr_{ij} \parallel HMAC_{x0}(\cdot)\}$ to him. Therefore UE_i might dispatch the media content to UE_j .

4) Obtained the message from eNB, UE_i confirms the fairness of the communication through verifying $HMAC_{x0}(\cdot)$ and σ_1. Next UE_i chooses $d_i \in [1, n-1]$ and calculates $Q_i = d_i P$ as key clue for UE_j. UE_i calculates the exchange key $K_{ij} = d_i Q_j$ and encrypts records M. Thereafter, UE_i produces the sign σ_2 of the message. Next he transfers the communication $\{PID_i \parallel PID_j \parallel m \parallel Cr_{ij} \parallel T_i \parallel HMAC_{xi}(\cdot)\}$ to UE_j. UE_i choices $y_i \in [1, n-1]$ and calculates Y_i after produces distribute key K_{0i} through eNB. UE_i utilizes K_{0i} to encrypt $Q_i' = Enc_{K_{0i}}(Q_i)$. Lastly, UE_i transmits the communication $\{PID_i \parallel PID_j \parallel \sigma_2 \parallel Q_i' \parallel Y_i \parallel T_i \parallel HMAC_{xi}(\cdot)\}$ to eNB.

5) eNB controls the fairness and sign over the obtained message from UE_i. Afterwards produces the share key K_{0i} that is utilized to decode the message $Q_i = Dec_{K_{0i}}(Q_i')$. additionally, eNB re-encrypts

$Q_i'' = Enc_{K_{0j}}(Q_i)$ as well as transfers message to UE_j . UE_j decrypts $Q_i = Dec_{K_{0j}}(Q_i'')$ and produces $K_{ij} = d_j Q_i$. So, the required matter may be decrypted.

5. Security analysis

Here we will indicate in what way $SeIS$ can join through the security provisions. The assessment demonstrated in this way.

5.1. Privacy and Reliability

Through data broadcast, the novel message M are protected by suitable encoding algorithm $Encsk(\cdot)$. After getting the shared key information may be decrypted on time. Although acceptor cannot decipher the message even if he gets the clue until he gets the other one from eNB.

Assuming that attender receives two key indications Qj and Qi, the distribute key Kij may be secured in accordance with the $ECDLP$ presumptions whereas the private key dj or di even may not be extract. So, the data secrecy may be obtained. In addition, $HMAC(\cdot)$ is utilized to deliver data morality and information verification avoiding the message from individual-in-the-central attack. For supply the authorization and validity, the genuine matter M had been approved by eNB before broadcast. So, the reliable influence of actual content may be demonstrated through checking $\sigma 1$.

5.2. Suggested Protocol Assures Specific Authentication

Unique Authentication is applied among the UE and eNB as well as within the UEs. While UE and eNB interchange message among themselves, the individual verification is conducted through the regular cellular transmission. Moreover, the eNB validates the participation with monitoring though the RID matches among the false recognition in the member register Table 3.

Normally, the verification in wireless communication systems is carried out through the authentication of the signature $\sigma 2$. Before transmitting the information to other equipment, the communicator is pretended to build a signature upon its false individuality as well as the recipient be able to authenticate the signature to verify the false character of the transmitter.

5.3. Supply Non-rejection

Non-rejection technique is both sender and recipient be liable for the communication they delivered. The formalities may offer non- rejection through verifying the sign $\sigma 1$ or $\sigma 2$, such signatures indicate whether communicator utilizes the private key which one TA has designated to sign the message. Moreover, recipient may authenticate the signature through utilizing this public key from sender. Through certifying the sign, the recipient may follow if the communicator is within the framework or not.

5.4. Joint Validation

Validation is usually applied among two various attendees in one period. In $SeIS$, eNB require to verify the user's genuine individuality RID (e.g. SIM card digit) to validates its accuracy. The verification among UE and eNB is carried out through verifying the authenticity of signature $\sigma 1$ or $\sigma 2$. Every transmission loop needs the sender to produce a digital signature in favor of the message he dispatch. Therefore, the protocol can produce cooperative validation.

5.5. The Suggested Protocol is Strong to Unbounded Attacks

Unrestricted attacks are acquired against legal through maintaining a register table in the eNB and renewed after each record circulation incident. Through mention to the element share frequency in the table, it is simple to determine the people who sets in minimum attempt on exchange data among else.

5.6. Strength

The system's power is established over coated security is accepted, those intervals the method is as significantly difficult as smashes a portal cryptography cover extended among the elliptic curve cryptography cover. Assume an attacker needs to enter a controlled variable s i; first, he wants to recognise only k items holding portions in favour of matching ciphertext C i; then, he wants to decode the acquired ciphertext. We are currently concentrating on the strength of the next stage. Therefore, we presume k negotiated nodes for combine as well as determine to expose distinct tiny - dividends through insertion and desire to build the polynomial Pi as well as therefore retrieve the ciphertext Ci.

Consequently, they achieve a pair $Ci = (riG, Mi + ri(aG))$.

To get M, the assaulter, who is presumed to recognize together G as well as the public key aG, desires to search this private key ri for calculate riG and $ri(aG)$ and therefore deduct the first phrase among twin from the alternate to receive M. Though searching the private key ri measures to work out $S = riG$ especially recognised in term of the elliptic curve discrete logarithm problem $ECDLP$ also considered as additional inflexible compare to parallel Discrete Logarithm Problem DLP through restricted areas. The $ECDLP$ is developed like this:

5.7. Analog of Discrete Logarithm Problem on Elliptic Curve EC-DLP

Suppose E is an elliptic curve determined on Fp. Provided two elements in the elliptic curve $S, T \in E$, identify d so that $S = d \cdot T$.

Pollard's rho method [11] is the most well-known method for solving the discrete log problem using a set of elliptic curve elements on the area of numerals cluster. Despite the fact that the new NSA (National Security Agency) cryptographic criteria [6] recommend using 256-bit elliptic curve cryptography ECC, [12] states that due to more time, 160-bit ECC may be securely implemented. This fractional time will work out the ECDLP concurrently through the tiny key lengths that are concerned (tiny ciphertexts) in order to defend our choice of elliptic curve cryptography ECC over RSA. In [13], the authors compare ECC and RSA to provide security levels against the required key sizes.

5.8. Compromise Tolerance

This section focuses on the method's settlement flexibility, which removes the capability from that application overlay to properly rebuild this addition result among the negotiated nodes. We need to indicate during the previous segment which is aggregate of supervised variables and whether k appropriate to n massive-portions are obtained, assuming the number of negotiated nodes is less than *n*-*k*. The following concept offers the possibility of a successful renovation.

6. Performance evaluation

Herein portion, we assess an execution of SeIS during provisions of calculation expense. As UE is restricted for calculation skill, the usages shows a realistic method.

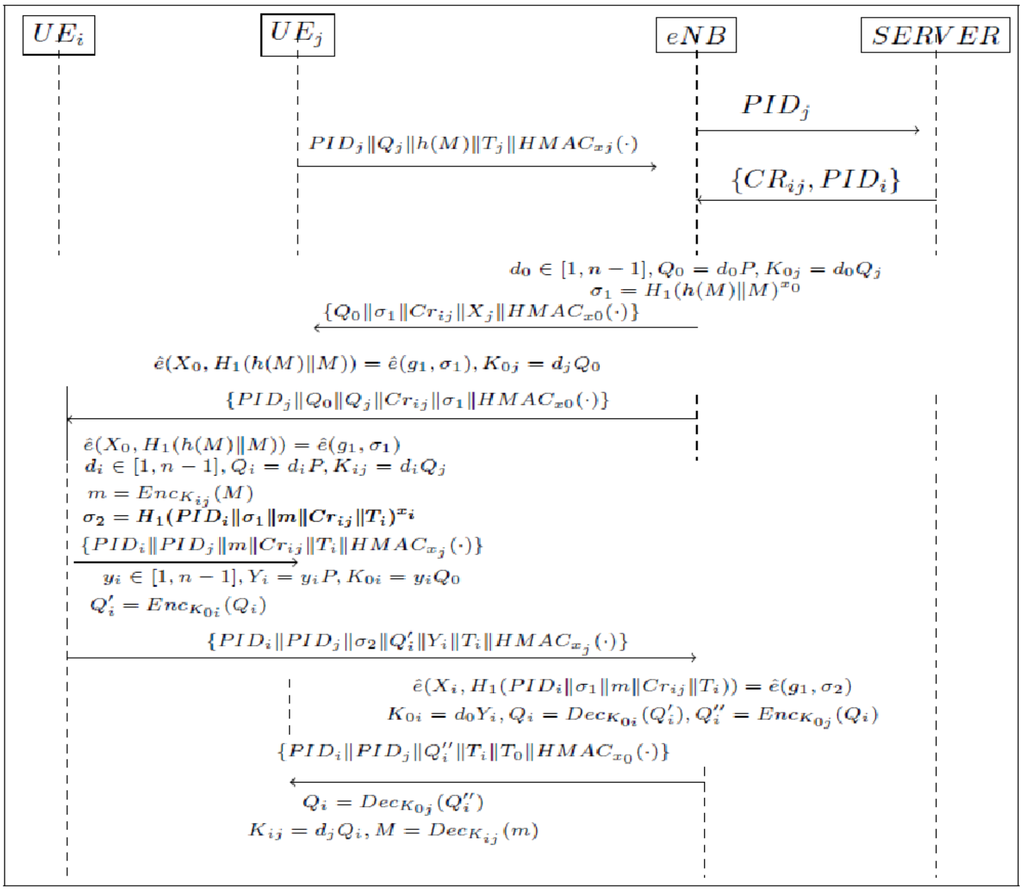
UE_i
UE_j
eNB
$SERVER$
PID_j
$PID_j\|Q_j\|h(M)\|T_j\|HMAC_{xj}(\cdot)$
$\{CR_{ij}, PID_i\}$
$d_0 \in [1, n-1], Q_0 = d_0P, K_{0j} = d_0Q_j$
$\sigma_1 = H_1(h(M)\|M)^{x_0}$
$\{Q_0\|\sigma_1\|Cr_{ij}\|X_j\|HMAC_{x0}(\cdot)\}$
$\hat{e}(X_0, H_1(h(M)\|M)) = \hat{e}(g_1, \sigma_1), K_{0j} = d_jQ_0$
$\{PID_j\|Q_0\|Q_j\|Cr_{ij}\|\sigma_1\|HMAC_{x0}(\cdot)\}$
$\hat{e}(X_0, H_1(h(M)\|M)) = \hat{e}(g_1, \sigma_1)$
$d_i \in [1, n-1], Q_i = d_iP, K_{ij} = d_iQ_j$
$m = Enc_{K_{ij}}(M)$
$\sigma_2 = H_1(PID_i\|\sigma_1\|m\|Cr_{ij}\|T_i)^{x_i}$
$\{PID_i\|PID_j\|m\|Cr_{ij}\|T_i\|HMAC_{x_j}(\cdot)\}$
$y_i \in [1, n-1], Y_i = y_iP, K_{0i} = y_iQ_0$
$Q_i' = Enc_{K_{0i}}(Q_i)$
$\{PID_i\|PID_j\|\sigma_2\|Q_i'\|Y_i\|T_i\|HMAC_{x_j}(\cdot)\}$
$\hat{e}(X_i, H_1(PID_i\|\sigma_1\|m\|Cr_{ij}\|T_i)) = \hat{e}(g_1, \sigma_2)$
$K_{0i} = d_0Y_i, Q_i = Dec_{K_{0i}}(Q_i'), Q_i'' = Enc_{K_{0j}}(Q_i)$
$\{PID_i\|PID_j\|Q_i''\|T_i\|T_0\|HMAC_{x_0}(\cdot)\}$
$Q_i = Dec_{K_{0j}}(Q_i'')$
$K_{ij} = d_jQ_i, M = Dec_{K_{ij}}(m)$

Figure 2: Secure Information Sharing Protocol

Additionally bilinear pairing, elliptic curve point aggregation as wll as encryption or decryption process take a major part. Thus, we examine just these exercise in $SeIS$ during contrasting among another associated method. In article [14], the performance time of various activities was evaluated on 3 GHz processor. The functioning time is 4.5 ms in favor of one bilinear pairing as well as 0.6 ms in order to numerical performance. This executing period of one AES in favour of 64 Bytes is 0.984 μs that was evaluated on 1.8 GHz processor [15]. So we may roughly compute the functional period of one AES for data M through L bytes on 1.50 GHz processor. This is almost $((0.984 \times 1.8)/1.50 \times L/64 = 1.9L \times 10^{-5}ms)$ based on the article [16]. In addition to the execution peiod of single elliptic curve point multiplication need around 1.8 ms over 3 GHz microprocessor, this specific calculation period is demonstrated on Table 4.

As suggested by the reviewer to verify the signature for each obtained instruction, this will accept 3 times bilinear pairing. For the sake of acquire the digital signature the algorithms through decline of 19% and 29% of numerical procedure with 6 times symmetric encryption to ensure the secrecy. Therefore, the complete calculational period of our protocol is achieved. Through contrast with another associated protocol, the benefits of our protocol is indicated. In $SeIS$ protocol, the complete calculational period is intended in addition we contrast with $SeCD$ protocol [17]. Though we demonstrated in Table 5.

Table 4
Computational Time of Various Executions

Notation	Description	Time(ms)
T_p	One pairing time	$4.5ms$
T_{pm}	One point multiplication time	$1.8ms$
T_n	One exponential time	$0.6ms$
T_a	One AES time	$1.9L \times 10^{-5}ms$

Table 5

Computational Duration Comparison

	Computational Time
SeIS	$1.5T_p + 4T_{pm} + 2Tn + 3Ta$
SeCD	$14T_p + 38T_n + T_a$

Whereas T_p requires the much computational time.

6.1. Computational complexity

Our chosen curve is Curve 25519 and the curve equation is $y^2 = x^3 + 486662x^2 + x \ mod(p)$. Where $mod(p)$ is established by $3 < p \leqslant 2^{255} - 19$, with a established-point of $x = 9$ is a Montgomery curve. Specify p is the prime $2^{255} - 19$. Identify F_p as the prime field $Z/p = Z/(2^{255} - 19))[\sqrt{2}]$. Specify $A = 486662$. Indicate that $486662^2 - 4$ is not a square in F_p. Define E as elliptic curve $y^2 = x^3 + Ax^2 + x$ over F_p. Identify a function $X_0 : E(F_{p^2}) \rightarrow F_{p^2}$ in this way: $X_0(\infty) = 0$; $X_0(x, y) = x$. Specify a function $X: E(F_{p^2}) \rightarrow \infty \cup F_{p^2}$ in this way: $X(\infty) = \infty$; $X(x, y) = x$.

Currently we state that, specified $n \in 2^{254} + 80{,}1{,}2{,}3\ldots, 2^{251} - 1$, $q \in F_p$ and the curve 25519 operation generates s, there is a unique integer $s \in 0{,}1{,}2{,}3\ldots, 2^{255} - 20$ with the pursuing attribute: $s = X_0(nQ)$ for all $Q \in E(F_{p^2})$ so that $X_0(Q) = q$ mod $2^{255} - 19$. Lastly, curve $25519(n, q)$ is determined as $\underline{s}$. A 255-bit integer may be divided through 4 or 8 or 10 or 12 fragments to adapt the capacity of different processors; an optimal extension field is connected to a particular number of portions. Prime $2^{255} - 19$ tracks the status: authority of 2 preserve time in field activities (as in, e.g, [18], with no impact on (presumed) security level.

Quick x-coordinate point addition on our chosen elliptic curve $y^2 = x^3 + 486662x^2 + x$; describes speedy x-coordinate scalar multiplication, i.e., quick estimation of curve 25519. Our evaluated $X(nQ)$ for each $n \in 2^{254} + 8\{0,1\ldots, 2^{251} - 1\}$ with 255 doublings and 255 additions beginning from $X(Q); X(0); X(Q)$. At the initial and final some repetitions might be easy. The last $X(nQ)$, as another X values, is described as a segment x/z. We examine $X_0(nQ) = xz^{p-2}$ utilizing a direct series of 254 squarings and 11 multiplications [19]. These actions contain of determined - point multiplication, scalar multiplication, point expansion, point doubling, augmentative reverse and confirmation. Faz-Hernández et al. [30] as well as Chou [31] utlized progressed curve activities in comparatively much strong CPUs through improve direction which is unable to provided by 8-bit CPUs. For this reason our effort's CPU price is little upper than Faz-Hernández et al. (2019) as well as Chou (2015). This is perceptible that our suggested method applies effective curve procedure in making 128-bit encryption keys. Table 7 summarizes contrast our encryption execution with available methods wherever the procedures applied identical curve forms (Montgomery) as well as hardware (AVR class) to create encrypted keys through 160-bit area. The methods endorsed various libraries as well as characteristics to enhance encoded keys' safety and execution. Liu et al. [32] utlized optimal prime field (OPF) library to enhance scalar multiplication method and match over past performance with Gallant-Lambert-Vanstone [20] method over twisted Edward curves.

Table 6

Curve execution comparability for 128-bit key origination

Work	**Applied area**	**Curve**	**Key Generation**
Oliveira et al [28]	Teensy 3.1 @ 48 MHz	ECqDSA	614 (pa + pd)
Fujii and Aranha [29]	ARM Cortex	Ed25519 & Ed448	353 (pa + pd)
Faz-Hernández et al. [30]	Intel Haswell	X25519& X448	18pa + 12pd
Our work	ATmega 16	Curve 25519	25pa + 48 pd

Table 7

Encryption time comparability with available method on 160-bit field

Techniques	Support feature	Hardware	Execution Time (ET)	RAM
Düll et al. [33]	Assembly	ATmega 2560	14.15 s	510 Bytes
Liu et al. [32]	OPF lib	ATmega 128	5.53 s	n/a
Moosavi et al. [34]	IPI /LSFR PRNG	ATmega 128L	3 s	n/a
Our work	OPF lib	ATmega 16	2.623 s	812 Bytes

The execution proficiency of ECC trusts upon computing a established-point or scalar-point multiplication, provide this outcome points x, y. Execution price of scalar multiplication mostly relies over two curve process i.e., PA (Point Addition) and PD (Point Doubling). Curve 25519 is quicker and be able to resist timing, boundary passage, twists over curve, stairs and numerical attacks (Dong et al. 2018). In our suggested technique, we obtain only 160-bit security which the cost-effective in source restrained independent IoT equipment. We present superior execution in encrypting 128-bit keys. It may be finalized suchlike our effort produced 128-bit encrypted keys through inexpensive inner memory usage and permitted 8-bit $CPUs$ in performing elliptic curve supported strong adjacent encryption.

For allocation, it includes in calculation the stocks of n groups, with every share containing of a $k-1$ extent polynomial assessment at a component in the restricted area F_q. This was displayed in [23], such assessments be able to performed in $O(k(log_2\ k)^2)$ arithmetic actions of expense $O((log_2\ q)^2)$ individually.

When encryption and distribution are executed through detecting items, union is the just action executed through transfer items. This includes in counting m stocks to pattern a macro-share through every supplement of expence $O(log_2\ q)$, ensuing in a complexity of $m \times O(log_2\ q)$. We may communicate entire expenses with conditions of p whereas $log_2\ q = 2(1 + log_2\ p)$.

B. Communication Cost

Within allocation, a detection element transfers shares to n various nodes through every portion of measure $log_2 q$ ensuing in $nlog_2 q$ conveyed bits. Within composite, every smart apparatus accepts stocks from m detecting elements ruling to $mlog_2 q$ obtained bits, merges system into single comprehensive - part that is a component of F_q and therefore of length $log_2 q$ bits. Such comprehensive - part is therefore dispatched to the entrance. As provision for a 328-bit prime q, whether we examine acceptance as well as communication of estimate charges, we receive a bandwidth operating expense of $328n$ bits transmitted through a detecting element, and $328(m + 1)$ bits interchanged through a transferal equipment.

Table 8

Computation and Communication Overheds

Computation		Communication		
Encryption	$\frac{45}{2} \Vert p \Vert^3$	Detecting object		$2n. \Vert p \Vert$
Distribution	$2k. \Vert k \Vert^2. \Vert p \Vert^2$	Forwarding object	received	$2m. \Vert p \Vert$
Combination	$2m \Vert p \Vert$		transmitted	$2 \Vert p \Vert$

It is clear that for the engaged parameters, wherever we presumed $\Vert q \Vert = 2 \Vert p \Vert$, the key size $\Vert p \Vert$ is the volume of 160 or 256 bits, although this remain of parameters ((k, n) in favour of private exchange as well as m in favour of the amount of controlled variables) be organized of twenty like utmost within this technique that certifies the high spirits through this method additionally its fitness in favour of assets restrained intelligent items.

7. Case study

In this section, we will apply a homomorphic encryption supported protocol to a Smart Network scheme. The computational complexity of the proposed protocol is investigated across strong ECC supported 160 bit low-cost security to source restricted wireless equipment. The curve 25519 is used to provide fast performance when producing private keys using the OPF library. The proposed method in terms of performance time (clock cycles) involves encryption of 128-bit keys to generate encoded keys over a 160-bit field. To improve scaler multiplication, we used the optimal prime field (OPF) library. The information on the voltage usage of each zone is gathered, pre-processed, and sent via fixed gateways to a service location via internet determination.

These accumulated data are examined for a variety of purposes, such as broadcast administration, remote apparatus supervision, and so on. As a result, these data will be mostly used to change the status of forwarded spirits. If the circumference of the gateway is not used to overcome such an entrance, the entrance will not transmit the details into focus. To carry out such a procedure, the gateway needs to calculate the total utilised strength across the boundary, which is entirely relevant to internal usage stages. Elliptic curve cryptography implementations in wireless equipment are available events and deficiencies. Wireless equipment is limited for stream/block cypher methods that require 32-bit computation power and a large storage capacity. As a result, quickCPUs and modern encoding algorithms (which require additional storage and clock periods) can be used smoothly.

The main goal of our effort is to use the OPF library for relevant arithmetic estimations in order to maintain roughly identical security levels and strong encrypted blocks using an 8-bit CPU that only used 1-2 Kbytes of RAM. The OPF library enabled us to quickly implement curve actions in order to generate 128-bit keys and large arbitrary prime integers. Because of the in advance calculation approach, our novel protocol performed faster within encryption and provided low-cost 160-bit security. The action must be carried out without jeopardising the secrecy and confidentiality of the consumers' private data.

8. Conclusion

We have proposed the secure information sharing protocol (SeIS) for wireless transmission. The protocol is carefully set up to achieve the desired results, with the exception of adding to the load on cellular networks. The suggested protocol is suitable for wireless communication's secure information-sharing strategy. Each node in the network is able to communicate with legitimate attendees. For general brute attack, a thorough security evaluation had been introduced. The performance indicates that SeIS has less computational time than the efficiency evaluation, which had been fully estimated. To enable secure and effective association of various detected variables without displaying all of them, the suggested method accumulates homomorphic encryption through a gateway for confidential exchange.

Through a flexible gateway and private distribution, the strategy benefits from both basic security and small-scale elliptic curve cryptography. We focus on the paper by allowing for secrecy and integrity among the updated data, even though validation is a crucial area to focus on in our best effort. In our upcoming work, we'll demonstrate secure data sharing between devices that doesn't require the use of an eNB. We'll also study more general and complex application setups where the service time isn't actually present, and we'll make use of how mobility affects security in D2D transmission.

9. Acknowledgements

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. BR18574045).

10.References

[1] A. Razaque, and S. S. Rizvi, Secure data aggregation using access control and authentication for wireless sensor networks, Computers & security 70 (2017) 532-545.

[2] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, Confidentiality and integrity for data aggregation in WSN using homomorphic encryption, Wireless Personal Communications 80.2 (2015) 867-889.

[3] K.A. Shim, Ch.-M. Park, A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks, IEEE transactions on parallel and distributed systems, 26.8 (2014) 2128-2139.

[4] J. L. Fernández-Alemán, C. S. Inmaculada, P. Á. O. Lozoya, and A. Toval, Security and privacy in electronic health records: A systematic literature review, Journal of biomedical informatics 46.3 (2013) 541-562, 2013.

[5] A. Razaque, V. Alexandrov, M. Almiani, B. Alotaibi, M. Alotaibi, and A. Al-Dmour, Comparative Analysis of Digital Signature and Elliptic Curve Digital Signature Algorithms for the Validation of QR Code Vulnerabilities, in Proceedings of the 2021 Eighth International Conference on Software Defined Systems, SDS, IEEE, 2021, pp. 1-7.

[6] M. Almiani, A. Razaque, T. Aidja, and A. Al-Dmour, Context-aware latency reduction protocol for secure encryption and decryption, International Journal of High Performance Computing and Networking 12.3 (2018) 251-260.

[7] J. M. Adler, W. Dai, R. L. Green, and C. A. Neff, Computational details of the vote here homomorphic election system, in: Proc. Ann. Intl Conf. Theory and Application of Cryptology and Information Security, ASIACRYPT, 2000.

[8] X. Wang, M. Chen, Zh. Han, D. O. Wu, and T. T. Kwon, TOSS: Traffic offloading by social network service-based opportunistic sharing in mobile social networks, in: Proceedings of the IEEE Conference on Computer Communications, IEEE INFOCOM 2014, IEEE, 2014, pp. 2346-2354.

[9] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.), Handbook of elliptic and hyperelliptic curve cryptography, CRC press, 2005 p. 32.

[10] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.). Handbook of elliptic and hyperelliptic curve cryptography, CRC press, 2005, p. 480.

[11] J. M. Pollard, Monte Carlo methods for index computation ($modp$), Mathematics of computation, 32.143 (1978) 918-924.

[12] J. Bos, M. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery, On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography, No. REP_WORK, 2009.

[13] D. Mahto, D. A. Khan, and D. K. Yadav, Security analysis of elliptic curve cryptography and RSA, in: Proceedings of the World Congress on Engineering, 1, 2016, pp. 419-422.

[14] A. J. Augusto, M. Scott, and R. Dahab, Implementing cryptographic pairings over Barreto-Naehrig curves, in: Proceedings of the International Conference on Pairing-Based Cryptography, Springer, Berlin, Heidelberg, 2007, pp. 197-207.

[15] D. He, J. Bu, S. Zhu, S. Chan, and Ch. Chen, Distributed access control with privacy support in wireless sensor networks, IEEE Transactions on wireless communications, 10.10 (2011) 3472-3481.

[16] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks, IEEE Transactions on Vehicular Technology, 65.4 (2015) 2659-2672.

[17] Y. Hao, J. Tang, and Y. Cheng, Secure cooperative data downloading in vehicular ad hoc networks, IEEE Journal on Selected Areas in Communications, 31.9 (2013) 523-537.

[18] A. Bender, G. Castagnoli, On the implementation of elliptic curve cryptosystems, MR 91d:11154, 16 (1990) 186–192.

[19] D. J. Bernstein, Curve25519: new Diffie-Hellman speed records, in: Proceedings of the International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, 2006, pp. 207-228.

[20] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.) Handbook of elliptic and hyperelliptic curve cryptography, CRC press, 2005.

[21] J. Girao, D. Westhoff, and M. Schneider, CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks, In IEEE International Conference on Communications, 5 (2005) 3044-3049.

[22] D. Boneh, and M. Franklin, Identity-based encryption from the Weil pairing, in: Proceedings of the Annual International Cryptology Conference, Springer, Berlin, Heidelberg, 2001, pp. 213-229.

[23] H.-T. Kung, Fast evaluation and interpolation, Carnegie-Mellon University, Department of Computer Science, 1973.

[24] R. Rahim, S. Murugan, S. Priya, S. Magesh, and R. Manikandan, Taylor based grey wolf optimization algorithm (TGWOA) for energy aware secure routing protocol, International Journal of Computer Networks and Applications (IJCNA), 7.4 (2020) 93-102.

[25] R. Sahu, S. Sharma, and M. A. Rizvi, ZBLE: zone based leader election energy constrained AOMDV routing protocol, International Journal of Computer Networks and Applications, 6.3 (2019) 39-46.

[26] F. Farokhi, I. Shames, and N. Batterham, Secure and private control using semi-homomorphic encryption, Control Engineering Practice, 67 (2017) 13-20.

[27] Zh. Zhang, P. Cheng, J. Wu, and J. Chen, Secure state estimation using hybrid homomorphic encryption scheme, IEEE Transactions on Control Systems Technology, 29.4 (2020) 1704-1720.

[28] T. Oliveira, J. López, H. Hışıl, A. Faz-Hernández, and F. Rodríguez-Henríquez, How to (pre-) compute a ladder, in: Proceedings of the International Conference on Selected Areas in Cryptography, Springer, Cham, 2017, pp. 172-191.

[29] H. Fujii, and D. F. Aranha, Curve25519 for the Cortex-M4 and beyond, in: Proceedings of the International Conference on Cryptology and Information Security in Latin America, Springer, Cham, 2017, pp. 109-127.

[30] A. Faz-Hernández, J. López, and R. Dahab, High-performance implementation of elliptic curve cryptography using vector instructions, ACM Transactions on Mathematical Software (TOMS), 45.3 (2019) pp.1-35.

[31] Ch.-H. Yang, Ch.-W. Chou, Ch.-Sh. Hsu, and Ch.-E. Chen, A systolic array based GTD processor with a parallel algorithm, IEEE Transactions on Circuits and Systems I: Regular papers, 62.4, (2015) 1099-1108.

[32] Zh. Liu, X. Huang, Zh. Hu, M. K. Khan, H. Seo, and L. Zhou, On emerging family of elliptic curves to secure internet of things: ECC comes of age, IEEE Transactions on Dependable and Secure Computing, 14.3 (2016) 237-248.

[33] M. Düll, B. Haase, G. Hinterwälder, M. Hutter, C. Paar, A. H. Sánchez, and P. Schwabe, High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers, Designs, Codes and Cryptography, 77.2 (2015) 493-514.

[34] S.R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, Cryptographic key generation using ECG signal, in: Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2017, pp. 1024-1031.

[35] F. Hendaoui, H. Eltaief, and H. Youssef, UAP: A unified authentication platform for IoT environment, Computer Networks, 188 (2021) 107811.

[36] T. Ch. Priyadharshini, and D. M. Geetha, Efficient Key Management System Based Lightweight Devices in IoT, Intelligent Automation and Soft Computing, 31.3 (2022) 1793-1808.

[37] L. Wang, Zh. Li, M. Chen, A. Zhang, J.-W. Cui, and B. Zheng, Secure content sharing protocol for D2D users based on profile matching in social networks, in: Proceedings of the 9th International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 2017, pp. 1-5.