Journal of Intelligent & Fuzzy Systems 39 (2020) 8237–8247
DOI:10.3233/JIFS-189144
IOS Press

A secured signcryption scheme for e-payment system using hyper elliptic curve

Malathi Devarajan* and N. Sasikaladevi
School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, India

Abstract. With the growing trend of Communication Technologies (ICT), buying goods through online has been increased drastically. Besides, e-payment makes online purchase easier and made our daily life more convenient. However, there exists a user privacy and data security issue in conventional e-payment systems. Thus, a hyper elliptic curve based signcryption scheme is proposed to achieve reduced computational cost. Because, most of the payment is processed on resource constraint devices like smart phone, hence an energy efficient e-payment system is in requisite. In order to ensure user authenticity, an aadhaar number (unique identity) is used to generate signcryption key. The proposed signcryption scheme can be implemented in real-time applications like e-payment system to ensure confidentiality, privacy, authenticity and integrity. The security of the system is validated through a simulation tool – AVISPA (Automated Validation of Internet Security Protocols and Applications). Further, the resistivity against various cryptographic attacks was analyzed informally and also the computational cost is estimated and compared with other related schemes.

Keywords: E-payment system, signcryption, hyper elliptic curve, security analysis, cybersecurity

1. Introduction

With the growing progress of communication technologies, buying goods through online has been amplified drastically. Consumers tend to save their shopping time and money by paying bills and purchasing goods through online using e-payment method. Though e-payment makes daily life easier and convenient, security and privacy are the major concerns. On the other hand, a good e-payment system should guarantee user anonymity, privacy protection, fair exchange, double spending prevention and dispute resolution along with other security requirements. Thus developing secure e-payment scheme is considered as a significant factor for e-commerce.

An anonymous payment method based on blind signatures was first proposed by Chaum [1] in 1983, after that many e-payment methods were proposed [2–5]. Despite, e-payment system relies mostly on resource constraint devices like mobile phone, thus employing complex techniques to secure e-payment system is less efficient. To reduce computational cost and storage space, Zheng [6] first established the concept of signcryption scheme. It performs digital signature and encryption in single process to achieve confidentiality, integrity and authenticity. It significantly reduces the computational overhead as it performs two cryptographic operations at a single step. Following Zhengs' signcryption scheme, many e-payment methods has been proposed using signcryption algorithms based on elliptic curve cryptosystem and bilinear pairing [7]. But bilinear pairing algorithms are computationally heavy and ECC based signcryption algorithm fails to achieve public verifiability and forward secrecy [8].

*Corresponding author. Malathi Devarajan, School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, India. E-mail: malathipuducherry@gmail.com.

Later, Yang et al. [9] proposed the payment system using authenticated encryption method. But Heydari et al. [10] analyzed Yang et al.'s method and said that just by knowing the public parameters; an attacker can impersonate the customer. Later, Chaudhry et al. [11] also reveals that Yang et al.'s approach is susceptible to impersonation attack and presented an improved electronic payment system. They claimed that their system resists all known attacks and provides 66% less computational cost when compared to Yang et al.'s approach. But, Kang et al. [12] stated that Chaudhry et al.'s approach lacks user anonymity, dispute resolution and fairness properties. So they developed an enhanced e-payment scheme by combining authenticated encryption and verifiably encrypted signature scheme which resists impersonation attack.

To alleviate the aforementioned limitations, we aim to design an efficient signcryption method for e-payment system using hyper elliptic curve. It uses user's aadhaar number to generate signcryption key. Though authentication and identity verification plays a vital role in providing high security, it is a time-consuming process. Thus a 12-digit aadhaar number is used to design a signcryption scheme. It contains users' demographic details and stored in a smart card as QR code [13, 14]. And hyper elliptic curve is used to provide low computational cost which suits well for resource constraint environment like e-payment system [15]. To validate the enhanced performance of the e-payment system, comparison is made with existing state-of-the-art protocols.

1.1. The key contributions

The key contributions of the work are given as follows

- A secure signcryption scheme using hyper elliptic curve cryptosystem is proposed for e-payment system with user's aadhaar number.
- Security of the projected e-payment method is validated using the simulation tool - AVISPA and showed that the protocol satisfies the defined authentication and privacy goals.
- Further, security requirements were analyzed informally and improved performance was assessed in comparison with other existing schemes.

The remainder of the work is structured as follows: the technical background of hyper elliptic curve together with signcryption scheme, e-payment system and its security requirements are defined for clear understanding of the scheme in section 2,. The proposed hyper elliptic curve based signcryption method and its application in e-payment system is presented in section 3 and 4. Informal security analyses were made in section 5, while the simulation results obtained using AVISPA tool is presented to confirm the security of the proposed scheme in section 6. The comparison of performance evaluation in terms of computational cost is given in the 7th section. Finally, section 8 summarizes the work with future directions.

2. Technical background

In the section, we present the technical background of hyper elliptic curve cryptosystem, definition of signcryption, e-payment system and its security requirements for clear understanding of the proposed scheme.

2.1. Hyper elliptic curve cryptosystem (HECC)

The hyper elliptic curve is the generalized form of elliptic curve whose security depends on the problem of solving discrete logarithmic problem in the jacobian curve [16]. HECC has higher efficiency, shorter key size and superior than other public key cryptosystems [17, 18]. Let C be a hyper elliptic curve of F_q, where F_q is a finite field, then C is defined as follows

$$y^2 + h(x)\, y = f(x)$$

where $h(x)$ is a polynomial of degree less than or equal to g and $f(x)$ is a monic polynomial of degree less than or equal to $2g + 1$. Unlike elliptic curve points, HEC points don't form a group. The finite sum of HEC points makes a divisor D and is characterized in the Mumford form as follows

$$D = (u(x), v(x)) = \left\{ \sum_{i=0}^{g} x^i u_i \sum_{i=0}^{g-1} x^i v_i \right\}$$

Divisors form the Jacobian group $J_c\left(F_q\right)$ and finding an integer $k \in F_q$ from D_2, such that $D_2 = k * D_1$ provided D_1 and D_2 is defined as HEC discrete logarithmic problem [19]. HECC requires a group order of size $q \geq 2^{80}$ and the NIST recommended key size of HECC is 80 bits whereas for ECC, it is 160 bits and it is 1024 bits for Rivest-Shamir-Adlemann cryptosystem.

2.2. Signcryption

A primitive cryptographic operation which performs both encryption and digital signature at the same time is defined as signcryption. It ensures message confidentiality, user authenticity, forward secrecy, non-repudiation and integrity [20]. Traditionally, authentication and confidentiality were achieved individually by means of signature and encryption. But, it takes more energy, time and computational process as it performs two operations simultaneously at both ends [21, 22]. Unfortunately, it doesn't suits for resource constraint environment like e-payment system. Then in 1997, Zheng et al. [23] first introduced the concept of signcryption where encryption and signature takes place at a single place. It reduces the computational cost, storage space and processing time. In signcryption, sender generates the key and sends the ciphertext along with signature to the receiver. Upon getting the message, unsigncrypter generates the same key for decryption and also verifies the signature at the same time [24–26].

2.3. E-payment system

An electronic payment process assists transaction of digital money from one person to another. The objective of any e-payment system is to afford a platform for online purchase and secured digital payment. It should ensure user anonymity, privacy protection, fair exchange, double spending prevention and dispute resolution. Customer, merchant, and bank are the three main entities of e-payment system. If any dispute rises and any of the participating entity complaints about the dispute then trusted authority involve resolving the disputes. The framework of e-payment system is illustrated in Fig. 1.

In general, e-payment system consists of buying, paying, exchange, transfer and dispute resolution phases to complete one transaction. Before performing a transaction, both customer and merchant should register with respective bank server and opens an account to take advantage of an e-payment system. Then they requisite to produce key pair - private and public key for further transactions. Explanation on each phase is defined as follows:

- **Buying phase:** A customer who wishes to buy goods should initiate the payment process by downloading goods' information and price details from merchants' website and requests the bank for voucher.

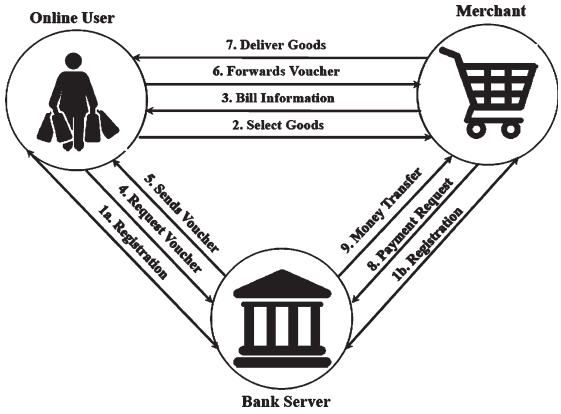

Fig. 1. Architecture of E-payment system.

- **Paying phase:** Upon receiving the voucher, the bank checks the validity of voucher and legitimacy of customer. If holds, then deducts the requested amount from customers' account and deposited in temporary amount for some arbitrary time. And also sends the voucher to customer specifying the expiry date.
- **Exchanging phase:** After receiving the voucher, customer sends the order request message with the voucher to merchant. After verifying the voucher and customer legality, merchant delivers the product. The session is declined, if any of the party is proved as unauthorized by other party.
- **Transferring phase:** After successful exchange of goods and voucher, merchant forwards the voucher to respective bank. Then bank releases the money from temporary account and deposited the same in merchants' account before the end of expiry date.
- **Dispute resolution phase:** It takes place when a dispute arises and requested by any of the participating entity. In such case, trusted authority helps to resolve the dispute.

2.4. Security requirements of E-payment system

During the payment process, information is transmitted over unsecure channel. So, it necessitates robust cryptographic mechanism for secure communications. The most important security requirements for payment process such as mutual authentication, user anonymity, non-repudiation, integrity, confidentiality, forward secrecy and public verifiability should be satisfied along with low computational complexity and communication overhead. Important security

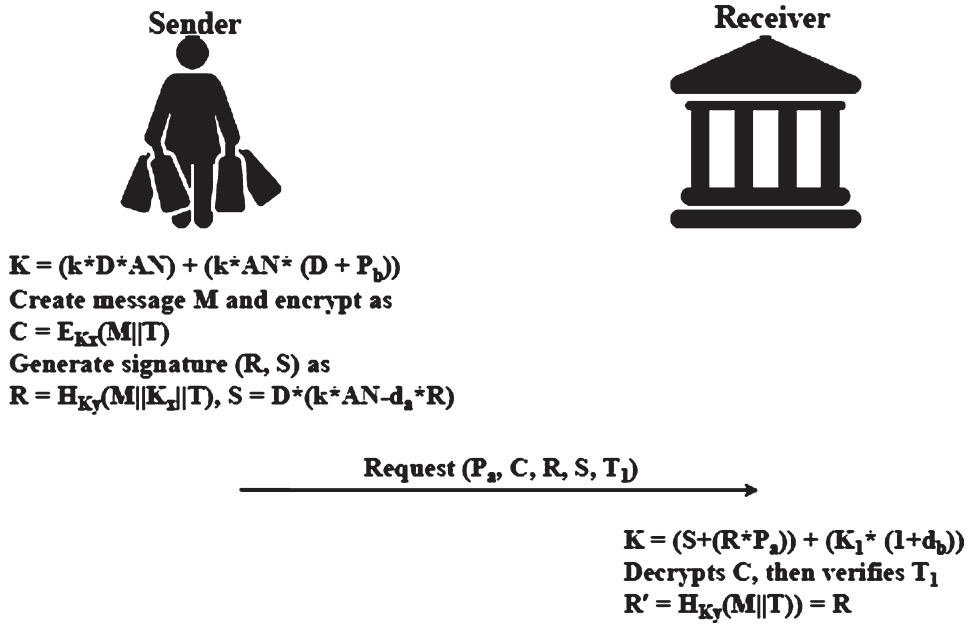

Fig. 2. The proposed Signcryption Scheme.

requirements to be considered are as follows:

- **Mutual authentication:** Participants like customer, merchant and bank should authenticate each other for successful e-transaction.
- **Confidentiality:** Each participant should know only their desired information other than public parameters and must be hidden from others.
- **Anonymity:** The original identity of participants and goods information should kept secret and cannot be obtained from any message.
- **Integrity:** At any cause, the message cannot be modified or altered by an adversary.
- **Non-repudiation:** No participants should refuse their participation or communication.
- **Forward secrecy:** Past or future secret key should be secret and cannot be predicted, though long term secret key is revealed.
- **Prevent double spending:** The system only allows the payment voucher to be used once.

3. The proposed signcryption approach

The secured signcryption approach is designed using hyper elliptic curve and utilized for E-payment application to ensure confidentiality, authentication, forward secrecy and other security requirements with reduced communication and computational cost. The proposed signcryption scheme is explained in the following subsections with verification phase and correctness of generated key. The scheme utilizes users' aadhaar number to generate signcryption key. Figure 2 depicts the proposed signcryption scheme with key generation and verification.

3.1. Initialization phase

At first, the system administrator published the public parameters i.e. hyper elliptic curve C over the finite field F_q, where q is the large prime number, D is the divisor of C, H is the one-way hash function and E/D be the symmetric key cryptosystem. Let d_a be the signcrypters' private key, then his public key is computed as $P_a = d_a * D$. Similarly, the private and public key pair of unsigncrypter is d_b and $P_b = d_b * D$.

3.2. Signcryption

If the signcrypter wishes to communicate securely with unsigncrypter and he also knows the public key of unsigncrypter means, then signcryption has to be performed. For that, signcrypter selects a random number $k \in F_q$ and takes his Aadhaar number (AN) to generate the secret key K as follows:

Step 1. Signcrypter chooses the random integer $k \in \{1, \ldots, q-1\}$ to generate the key

$K = K_1 + K_2$ where $K_1 = AN^*D^*k$ and $K_2 = k^*AN^*(D + P_b)$.

Step 2. Now mapping function φ is used to convert the divisor K into its corresponding integer $(K_x,\ K_y)$.

Step 3. Then generate the ciphertext c and signature $(R,\ S)$ as $C = E_{k_x}(m, T)$, $R = H_{k_y}(m\,||K_x||\,T)$ and $S = (k^*AN - d_a{}^*R)\,^*D$, where T is the timestamp.

Step 4. Finally, the tuple (C, R, S, T) is communicated to the unsigncrypter for verification.

3.3. Verification phase

In receipt of signcrypted tuple (C, R, S, T), unsigncrypter verifies the signature and authenticates the signcrypter as follows:

Step 1. Unsigncrypter uses the public parameters and received signcrypted tuple to generate secret key K as $K = K_1 + K_2$ where $K_1 = S + (R^*P_a)$ and $K_2 = K_1(1 + d_b)$.

Step 2. Now mapping function φ is used to convert the divisor K into its corresponding integer $(K_x,\ K_y)$.

Step 3. Then K_x is used for decryption process and retrieves the message as $(m, T) = D_{K_x}(C)$ and verifies the validity of timestamp T.

Step 4. If T is valid, then unsigncrypter computes R' and checks $R' = H_{K_y}(m \parallel K_x \parallel T) = R$, if holds, then he believes that the message is really sent by the valid signcrypter, else unsigncrypter discards the session.

3.4. Correctness

Proof 1.
$$\begin{aligned} K_1 &= S + \left(R^*P_a\right) \\ &= D^*\left(k^*AN - d_a{}^*R\right) + R^*P_a \\ &= D^*k^*AN - D^*d_a{}^*R + R^*P_a \\ &= D^*k^*AN = K_1 \end{aligned}$$

Proof 2.
$$\begin{aligned} K_2 &= K_1(1 + d_b) \\ &= D^*k^*AN(1 + d_b) \\ &= k^*AN(D + P_b) = K_2 \end{aligned}$$

Table 1
Notations utilized in the proposed method

Notation	Meaning
C	Hyper elliptic curve over F_q
F_q	Finite field
Q	Prime number
D	Divisor
K	Random integer
AN	Aadhaar number
K	Session key
d_a, d_b and d_m	Private key of customer, bank and merchant
P_a, P_b and P_m	Public key of customer, bank and merchant
(R, S)	Signature
T	Timestamp
$H()$	Hash function
E/D	Encryption/Decryption
M	Message

4. The proposed signcryption method and its application in E-payment system

The proposed signcryption scheme which is designed using HEC cryptosystem assures authenticity and confidentiality at the same time. Accordingly, it can be explored in e-payment system to offer secure transactions. In general, e-payment system consists of initialization, buying, paying, exchange, transfer and dispute resolution phases. In addition, each participants i.e. merchant and customer should register and open their accounts in the respective bank before the transaction begins. Table 1 presents the notations utilized in the proposed signcryption method and Fig. 3 depicts the sequence of e-payment system with proposed signcryption scheme and each phase is explained in detail in the subsequent sections.

4.1. Initialization phase

During initialization, the system generates public parameters like hyper elliptic curve C, divisor D and symmetric key encryption and decryption method. Each user selects private key d_i and generates its corresponding public key as $P_i = d_i{}^*D$. At last, public parameters are made available publicly, while the private keys are kept secret.

4.2. Buying phase

When the customer wishes to buy some goods, he/she first collects the goods' information *GI* from the merchants' website. Then generates payment message as follows and sends to the bank requesting payment voucher. This phase is described as follows:

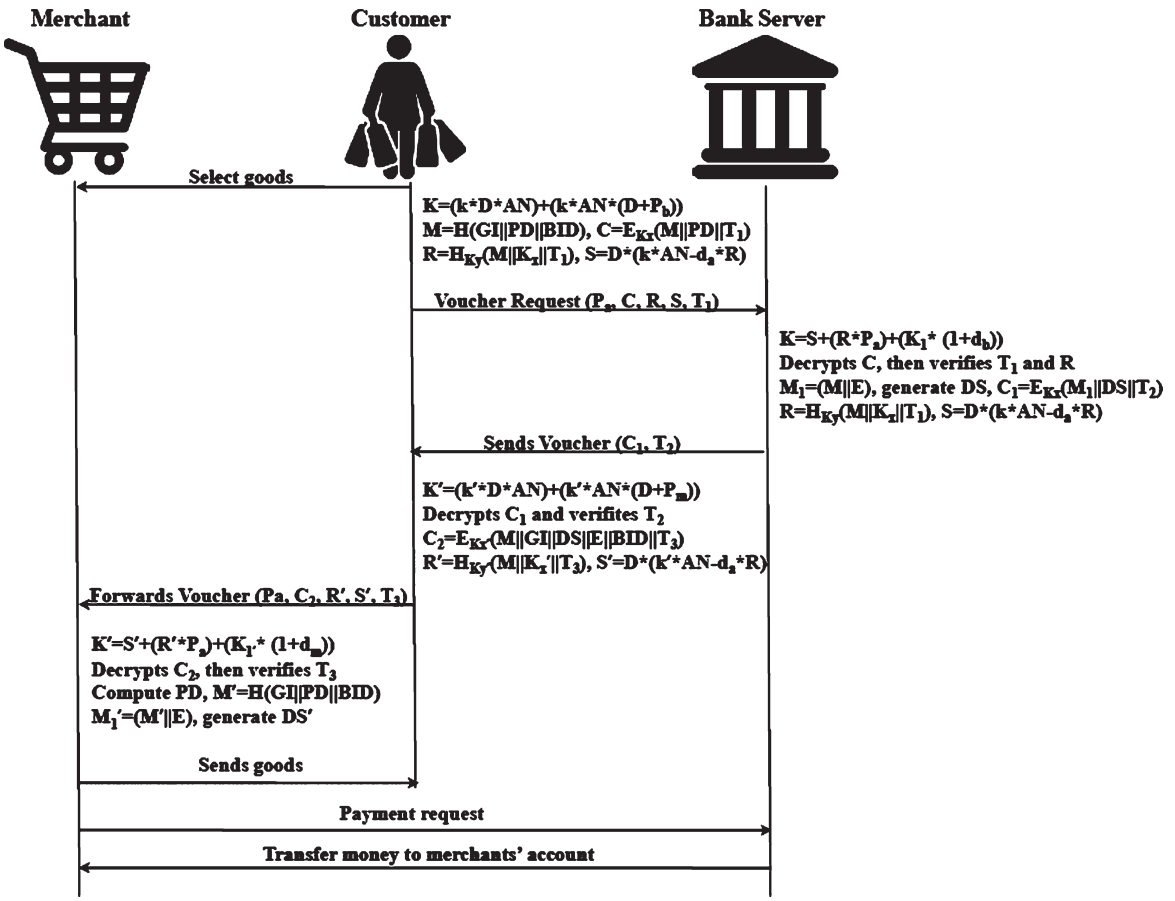

Fig. 3. Proposed e-payment system.

Step 1. Customer collects the goods information $GI = \{(G_1, P_1), (G_2, P_2), \cdots (G_n, P_n)\}$ from merchant's website and price details $PD = \sum_{i=1}^{n} price_i$.

Step 2. Then selects the random integer k and takes his aadhaar number to compute the secret key $K = K_1 + K_2$, where $K_1 = k^*D^*AN$ and $K_2 = k^*AN\,(D + P_b)$.

Step 3. Here, mapping function φ is applied on K to convert the divisor into its corresponding integer value $K = \left(K_x, K_y\right)$ which is used further for encryption and hash function.

Step 4. Now customer creates the payment information $M = H\,(GI\,||PD||\,BID)$, where PD is price details, GI is goods information, and BID is the bank identity.

Step 5. Finally, customer encrypts the message and price as $C = E_{K_x}\,(M||PD \parallel T_1)$ and produces the signature (R, S) as $R = H_{K_y}\,(M \parallel K_x \parallel T_1)$, $S = D^*\,(k^*AN - d_a{}^*R)$, then sends the message (P_a, C, R, S, T_1) to the respective bank requesting the voucher.

4.3. Paying phase

Once the bank obtains the payment voucher request from the customer, it verifies the legitimacy of requester and validity of time stamp. After successful verification, bank deducts the quoted amount from customers' account and transfers it into temporary account. Further, bank produces the digital signature DS and replays back to customer as:

Step 1. The bank establishes the key $K = K_1 + K_2$ from $K_1 = S + (R^*P_a)$ and $K_2 = K_1{}^*\,(1 + d_b)$. Then mapping function φ is applied on K to obtain $\left(K_x, K_y\right)$.

Step 2. The bank decrypts the ciphertext C and verifies the timestamp T_1 and checks

the correctness of $R^* = H_{K_y}(M \parallel K_x \parallel T_1) = R$. If holds, then bank continues the session, else rejects it. And it deducts the amount quoted in the *PD* from customers' account and deposited in temporary account.

Step 3. Now, bank sets the expiry date E and creates the message $M_1 = \{M||E\}$. After that digital signature *DS* is produced with private key d_b, and then stores the tuple $\{DS,\ M\}$ for future reference.

Step 4. In final, bank generates the ciphertext $C_1 = E_{K_x}(M_1 \parallel DS \parallel T_2)$ and sends the message (C_1, T_2) to the respective customer.

Step 5. In receipt of the tuple (C_1, T_2), customer confirms the validity of timestamp T_2 and decrypts the message C_1 to get *DS* and *E*.

4.4. Exchange phase

After getting the voucher from the bank, customer forwards it to merchant for goods delivery. Merchant verifies the digital signature using banks' public key and sends the goods to the customer and voucher to the bank for transaction if validity of *DS* holds as follows:

Step 1. Customer selects the random integer k' to compute $K'_1 = k' * AN * D$, $K'_2 = k' * AN * (D + P_m)$ and $K' = K'_1 + K'_2$.

Step 2. Then mapping function is utilized to change the divisor K' to its corresponding integer values $\left(K'_x, K'_y\right)$.

Step 3. Now customer encrypts the information as $C_2 = E_{K'_x}(M\,||GI||\,DS\,||E||\,BID||T_3)$ and generates the signature $\left(R', S'\right)$ as $R' = H_{K'_y}\left(M \parallel K'_x \parallel T_3\right)$, $S' = D^* \left(k' * AN - d_a * R\right)$. Then sends the tuple $\left(P_a, C_2, R', S', T_3\right)$ to merchant.

Step 4. Now the merchant computes $K' = K'_1 + K'_2$ as $K'_1 = S' + \left(R' * P_a\right)$ and $K'_2 = K'_1 * (1 + d_m)$ and converts K' into integer values using mapping function φ to get $\left(K'_x, K'_y\right)$.

Step 5. With the help of K'_x, merchant decrypts C_2 and gets $D_{K'_x}(C_2) = (M\,||GI||\,DS\,||E||\,BID||T_3)$ and verifies the validity of T_3.

Step 6. If it holds, then computes $PD' = \sum_{i=1}^{n} price_i$ and $M' = H(GI\,||PD||\,BID)$ for the received goods information, and also generates the digital signature DS' with the public key of bank.

Step 7. If the computed DS' matches with the received *DS*, then merchant verifies the integrity of the message as $R'' = H_{K'_y}\left(M' \parallel K'_x \parallel T_3\right) = R'$.

Step 8. Finally, merchant sends the ordered goods to customer and maintains the tuple $\{DS, M\}$ in their database to avoid double spending.

4.5. Transfer phase

In transfer phase, before the date expires merchant forwards the voucher to the bank. Then bank credits the quoted amount into merchants' account and removes the entry from its database. The customer can request the bank to cancel the transaction, if he does not collect the ordered goods on time or before the expected time or if any dispute arise. In this scenario, the bank credits the money back to customers' account and clears temporary account.

4.6. Dispute resolution phase

If suppose the customer doesn't receive the ordered goods correctly or merchant doesn't receive the proper payment voucher, then complaint can be raised by them and resolve the disputes with the help of trusted authority.

Case 1. What if customer does not collect the ordered goods correctly?
In this case, the customer needs to prove that the received goods are not satisfactory. For that, he needs to disclose the goods information and price, he used for order placement. If received good doesn't meet the requirements of ordered good, then customer wins the case. Since the scheme ensures mutual authentication, other than merchant no one can generate and utilize that key.

Case 2. What if merchant does not receive the valid or proper payment voucher?
If suppose the corresponding bank rejects the voucher and refuses to pay the merchant or customer holds the payment

process, then trusted authority enters and checks the validity of payment voucher to resolve the dispute. Though, it is not possible because only the respective bank can generate the *DS* with its private key and customer cannot alter it.

5. Security analysis

The proposed signcryption method resists various cryptographic attacks such as impersonation attack, outsider attack, identity theft, replay attack, server spoofing and man-in-the-middle attack. The security of signcryption method relies mainly on the complexity of breaking HEC discrete logarithmic problem. Let D_1 and D_2 be two divisors, where $D_2 = k * D_1$, then finding k provided D_1 and D_2 is not feasible. It also satisfies all the aforementioned security requirements and thus suits well for e-payment application. The discussion on resistance against each attack is presented in the following subsections.

5.1. Impersonation attack

Suppose an attacker tries to impersonate customer, it is difficult for him to do so, because an attacker generated symmetric key $K = (K_x, K_y)$ won't match with the key generated by the merchant. This is due to the fact that an adversary is in need of customers' private key d_a to compute $S = D^*(k^*AN - d_a{}^*R)$ and merchant needs his own private key d_m to compute the symmetric key $K = (K_x, K_y)$.

5.2. Identity theft attack

It is difficult to perform identity theft attack in the proposed scheme. Because, though an attacker gets the aadhaar number and some other information of the customer, he is not able to impersonate the customer as the scheme does not require any such information for authentication and verification.

5.3. Man-in-the-middle attack

Let us assume that an intruder seizes the payment information (P_a, C_2, R', S', T_3) and he wishes to get the goods from the merchant. He tries to change the timestamp T_3 and sends the modified information to the merchant. While checking the validity of the timestamp T_3 obtained by decrypting the ciphertext $C_2 = E_{K'_x}(M||DS||E||GI||BID||T_3)$, receiver discovers that the received message is invalid as it fails to match with received timestamp T_3. Accordingly, the proposed method resists man-in-the-middle attack.

5.4. Outsider attack

Suppose an intruder intercepts the message from unsecure communication channel and tries to get the information from ciphertext C. For that he needs to generate the key $K = (K_x, K_y)$ and fails as it is difficult to achieve K_x due to the difficulty of breaking HEC discrete logarithmic problem. By this way, the proposed method resists outsider attack.

5.5. Replay attack

Though an attacker intercepts any message transmitted between sender and receiver, he is not able to pretend like a legitimate user. This is because, every message contains the timestamp T and the session is aborted by the receiver if there is no freshness in the received timestamp.

5.6. Server spoofing attack

Let us assume that an intruder wishes to act as a legal bank server, he needs to generate proper K_x to compute the ciphertext $C_1 = E_{K_x}(M_1 \parallel DS \parallel T_2)$ to send (C_1, T_2) to customer. But it is not feasible to do so because an attacker is not aware of banks' private key d_b.

5.7. Achieves security requirements

The proposed signcryption method assures significant security requirements such as mutual authentication, privacy prevention, user anonymity, double spending protection and non-repudiation as follows:

- **Authentication:** By verifying the correctness of timestamp T and K_x from $R = H_{K_y}(M \parallel K_x \parallel T)$, the proposed scheme achieves authenticity. Because only an authorized user can generate the key (K_x, K_y) and verifies the message with that key.
- **Anonymity:** The user anonymity is preserved in this signcryption scheme. Though the customer uses his aadhaar number to generate the key (K_x, K_y), the same is not used in other side i.e. by bank or merchant to generate the same

key. So the merchant does not recognize who the buyer is.

- **Confidentiality:** Since the message is communicated over channel after applying symmetric key encryption method, an intruder needs to know $(K_x,\ K_y)$ and $\left(K'_x,\ K'_y\right)$ to get the information. But this is difficult to generate the symmetric key as it is computed using the aadhaar number and private keys of sender and receiver. Without knowing this secret information, an attacker cannot able to decrypt the ciphertext which ensures the confidentiality of transmitting messages.
- **Double spending protection:** Double spending is prevented by keeping the tuple DS, M in its database by bank till the payment completes successfully. Once the payment process completes, the bank deletes the entry.
- **Integrity:** The proposed scheme ensures message integrity, because other than legitimate user no one can generate (K_x, K_y) due to HEC discrete logarithmic problem. Without knowing the symmetric key, an attacker cannot modify the message.
- **Non-repudiation:** The signcryption scheme is designed in a way that none of the participant can refuse their participation. Because, if any dispute arises, then trusted authority will engage to resolve the dispute by checking the communication and participation of users.
- **Privacy protection:** The buying information i.e. goods information GI and price details PD i.e. $M = H(GI||PD||BID)$ are protected from bank and other outsiders with the help of one-way hash function.

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/sign.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 4.00s
 visitedNodes: 648 nodes
 depth: 11 plies
```

Fig. 4. OFMC result.

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
 /home/span/span/testsuite/results/sign.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
 Analysed  : 4 states
 Reachable : 4 states
 Translation: 0.13 seconds
 Computation: 0.00 seconds
```

Fig. 5. CL-AtSe result.

6. AVISPA: simulation results

The widely accepted automated security analysis tool AVISPA is utilized for protocol validation. The tool contains 4 different back-end checkers such as CL-AtSe checker, OFMC checker, TA4SP checker and SATMC checker for automatic analysis and the protocol is specified in High Level Protocol Specification Language (HLPSL). The HLPSL2IF helps to translate the protocol in low level language from high level language called IF (Intermediate Format).

In order to assess the security features of e-payment system, the protocol is implemented in HLPSL code and then both CL-AtSe and OFMC back-end checkers were executed. The back-end checkers analysis the protocol and outputs the result as either safe or unsafe. It also states whether there is a problem in the protocol and what kind of problem it is. From the simulation results shown in Figs. 4 and 5, it is observed that the system is safe and attains defined security targets.

7. Performance analysis

The computational cost of the signcryption scheme proposed for e-payment system is determined and compared with other related schemes. Let us assume

Table 2
Comparative analysis of computational cost and execution time

	Buying phase	Paying phase	Exchange phase	Total cost	Execution time
Yang et al. [9]	$3T_{PM}+1T_H+1T_E$	$1T_{PM}+2T_D+1T_E$	$4T_{PM}+1T_E+1T_D+1T_H$	$8T_{PM}+3T_E+3T_D+2T_H$	≈17.8402ms
Chaudhry et al. [11]	$1T_I+1T_{PM}+1T_H+1T_E$	$1T_{PA}+2T_{PM}+1T_D+1T_E$	$2T_D+1T_I+3T_{PM}+1T_E+1T_{PA}+1T_H$	$2T_I+6T_{PM}+2T_H+3T_E+3T_D+2T_{PA}$	≈13.4458ms
Heydari et al. [10]	$1T_I+1T_{PM}+1T_H+1T_E$	$2T_{PM}+1T_{PA}+1T_I+2T_D+1T_E$	$2T_I+3T_{PM}+1T_E+1T_{PA}+1T_D+1T_H$	$4T_I+6T_{PM}+2T_H+3T_E+3T_D+2T_{PA}$	≈13.4458ms
Kang et al. [12]	$1T_I+1T_{PM}+1T_H+1T_E$	$2T_{PM}+1T_{PA}+1T_D+1T_E$	$2T_D+3T_{PM}+1T_E+1T_H+1T_{PA}+1T_I$	$2T_I+6T_{PM}+2T_H+3T_E+2T_{PA}+3T_D$	≈13.4458ms
Kumar et al. [28]	$4T_{PM}+1T_{PA}+2T_H+1T_E$	$2T_{PM}+1T_H+1T_{PA}+2T_D+1T_E$	$6TP_M+3T_H+2T_{PA}+1T_E+1T_D$	$12T_{PM}+4T_{PA}+6T_H+3T_E+3T_D$	≈26.8686ms
Proposed	$2T_{DA}+2T_{DM}+1T_H+1T_{KH}+1T_E$	$2T_{DA}+3T_{DM}+1T_{KH}+1T_E+2T_D$	$5T_{DM}+4T_{DA}+1T_E+1T_H+2T_{KH}+1T_D$	$8T_{DA}+10T_{DM}+2T_H+4T_{KH}+3T_E+3T_D$	≈11.2958ms

that the time taken to perform elliptic curve and hyper elliptic curve arithmetic operations be

- T_E: Symmetric encryption
- T_D: Symmetric decryption
- T_H: One way hash function
- T_{KH}: Keyed hash function
- T_{PM}: EC point multiplication
- T_{PA}: EC point addition
- T_{DM}: HEC divisor multiplication
- T_{DA}: HEC divisor addition

According to Kilinc and Yanik [27], the time taken for one-way hash function is 0.0023 ms, 0.0046 ms for keyed hash function, 2.226 for point multiplication, 0.0288 ms for point addition and 0.0046 ms for symmetric encryption or decryption on Intel Core i3-6100U, 2.3 GHz processor, 2048 MB of RAM and Ubuntu 12.04.1 LTS 64 bit operating system. The divisor arithmetic consumes half the cost of point arithmetic as it uses lesser key size. The computational cost of related approach is given in Table 2 for comparison with the computational cost of proposed approach. It is observed that proposed method consumes less computational cost than other schemes. Thus our scheme is sufficient enough to use in resource constraint environment like e-payment system.

8. Conclusion

Essential security requirements can be achieved by implementing proposed signcryption method. Its security relies on hardness of solving hyper elliptic curve discrete logarithmic problem. It also reduces the computational cost as it accomplishes confidentiality and authentication in single step, while the reduced computational cost achieved also compared with other schemes. Further, it resists man-in-the-middle, replay, server spoofing, impersonation and other attacks. In order to demonstrate that, informal security analyses were carried out against all possible attacks.

Besides, the proposed scheme is appropriate for resource constrained applications like e-payment system. The security verification of the proposed scheme is performed using widely accepted protocol validation tool, AVISPA. The simulation results obtained demonstrates the safety of protocol and its achievement on specified goals. It also ensures confidentiality and authenticity, protects privacy and prevents double spending.

Acknowledgments

The authors are grateful to Science and Engineering Research Board (SERB), Department of Science and Technology, New Delhi, for the financial support under ECR grant (ECR/2017/000679/ES).

References

[1] D. Chaum, Blind signatures for untraceable payments, In *Advances in Cryptology (pp. 199–203). Springer*, Boston, MA. (1983).

[2] S.J. Lin and D.C. Liu, An incentive-based electronic payment scheme for digital content transactions over the Internet, *Journal of Network and Computer Applications* **32**(3) (2009), 589–598.

[3] L. Zhang, F. Zhang, B. Qin and S. Liu, Provably-secure electronic cash based on certificateless partially-blind signatures *Electronic Commerce Research and Applications* **10**(5) (2011), 545–552.

[4] Y.C. Yen, T.C. Wu, N.W. Lo and K.Y. Tsai, A Fair-Exchange E-Payment Protocol For Digital Products With Customer Unlinkability, *KSII Transactions on Internet & Information Systems* **6**(11) (2012).

[5] X. Chen, J. Li, J. Ma, W. Lou and D.S. Wong, New and efficient conditional e-payment systems with transferability, *Future Generation Computer Systems* **37** (2014), 252–258.

[6] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption)« cost (signature) +cost (encryption). In *Annual international cryptology conference (pp. 165–179). Springer, Berlin*, Heidelberg. (1997).

[7] A.K. Singh, A review of elliptic curve based signcryption schemes, *International Journal of Computer Applications* **102**(6) (2014).

[8] V. Rajasekar, J. Premalatha and K. Sathya, An Efficient Signcryption Scheme for Secure Authentication using Hyper Elliptic Curve Cryptography and Keccak Hashing, *International Journal of Recent Technology and Engineering* **8**(3) (2019), 1593–1598.

[9] J.H. Yang, Y.F. Chang and Y.H. Chen, An efficient authenticated encryption scheme based on ECC and its application for electronic payment, *Information Technology and Control* **42**(4) (2013), 315–324.

[10] M. Heydari, S. Sadough, S.A. Chaudhry, M. Sabzinejad Farash and M.R. Aref, An Improved Authentication Scheme for Electronic Payment Systems in Global Mobility Networks, *Information Technology and Control* **44**(4) (2015), 387–403.

[11] S.A. Chaudhry, M.S. Farash, H. Naqvi and M. Sher, A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography, *Electronic Commerce Research* **16**(1) (2016), 113–139.

[12] B. Kang, D. Shao and J. Wang, A fair electronic payment system for digital content using elliptic curve cryptography, *Journal of Algorithms & Computational Technology* **12**(1) (2018), 13–19.

[13] K. Prakasha, B. Muniyal and V. Acharya, Automated user authentication in wireless public key infrastructure for mobile devices using Aadhar card, *IEEE Access* **7** (2019), 17981–18007.

[14] K.N. Mishra, AAdhar based smartcard system for security management in South Asia. In *2016 International Conference on Control, Computing, Communication and Materials (ICCCCM) (pp. 1–6)*. IEEE. (2016).

[15] S. Ullah, X.Y. Li and L. Zhang, A review of signcryption schemes based on hyper elliptic curve, In *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM) (pp. 51–58)*. IEEE. (2017).

[16] I. Ullah, N.U. Amin, M. Naeem, H. Khattak, S.J. Khattak and H. Ali, A Novel Provable Secured Signcryption Scheme PSSS: A Hyper-Elliptic Curve-Based Approach, *Mathematics* **7**(8) (2019), 686.

[17] N. Koblitz, A family of jacobians suitable for discrete log cryptosystems, In *Conference on the Theory and Application of Cryptography (pp. 94–99). Springer*, New York, NY. (1988).

[18] P. Kumar, A. Singh and A.D. Tyagi, Implementation of Hyperelliptic Curve Based Signcryption Approach, *International Journal of Scientific and Engineering Research* **4**(7) (2013).

[19] A. Sadat, R. Ahmad, I. Ullah, H. Khattak and S. Ullah, Multi Receiver Signcryption Based On Hyper Elliptic Curve Cryptosystem, *J Appl Environ Biol Sci* **7**(12) (2017), 194–200.

[20] A. Braeken and P. Porambage, ASEC: anonym signcryption scheme based on EC operations, *International Journal of Computer Applications* **5**(7) (2015), 90–96.

[21] X.W. Zhou, Improved Signcryption Schemes Based on Hyper-elliptic Curves Cryptosystem, In *Applied Mechanics and Materials (Vol. 20, pp. 546–552). Trans Tech Publications Ltd*. (2010).

[22] Y. Zheng and H. Imai, How to construct efficient signcryption schemes on elliptic curves, *Information Processing Letters* **68**(5) (1998), 227–233.

[23] Y. Zheng, Signcryption and its applications in efficient public key solutions, In *International Workshop on Information Security (pp. 291–312). Springer, Berlin, Heidelberg*, (1997).

[24] S.A. Ch and N. Amin, Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem, In *8th International Conference on High-capacity Optical Networks and Emerging Technologies (pp. 244–247). IEEE*. (2011).

[25] S.A. Ch and M. Sher, Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem, In *International Conference on Information Systems, Technology and Management (pp. 135–142). Springer, Berlin, Heidelberg* (2012).

[26] S.A. Ch, M. Sher, A. Ghani, H. Naqvi and A. Irshad, An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography, *Multimedia Tools and Applications* **74**(5) (2015), 1711–1723.

[27] H.H. Kilinc and T. Yanik, A survey of SIP authentication and key agreement schemes, *IEEE Communications Surveys & Tutorials* **16**(2) (2013), 1005–1023.

[28] R. Kumar, S.K. Pal and A. Yadav, Elliptic curve based authenticated encryption scheme and its application for electronic payment system, *International Journal of Computing Science and Mathematics* **9**(1) (2018), 90–101.