Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105
Volume **9**, Number **2**, May **2024**

Secure E-commerce Payment System Based on Novel SET Network Protocols

Chun-Ming Yu

Department of Information Management
Shanghai Lixin University of Accounting and Finance, Shanghai 201209, China
18801206016@163.com

Xin Jin*

Marketing Department
Chery Automobile Co., Ltd., Wuhu 241000, China
jinx0810@sohu.com

Aaron Feng

Department of Information Engineering
University of Nueva Caceres, Naga 4400, Philippines
je2628@163.com

*Corresponding author: Xin Jin
Received October 25, 2023, revised December 27, 2023, accepted February 10, 2024.

Abstract. *Secure Electronic Transaction (SET) is a secure electronic payment protocol for payments over the Internet. The rapid development of the Internet has led to the development of E-commerce, and the SET protocol has become a key standard in E-commerce transactions. In order to improve the security of E-commerce payments, this work proposes a novel SET network protocol. First, the key modules of a secure E-commerce payment system based on the SET protocol are given. The digital signature module is used to realize double digital signatures by connecting two messages sent to different receivers by improving the digital signature principle to guarantee the payment security of cardholders. The E-commerce recommendation method based on payment encryption is given. Secondly, an improved NAF algorithm is proposed to replace the original private key encryption algorithm for the insufficiency of encryption and decryption algorithms in SET protocol. Finally, the improved NAF algorithm is combined with the Montgomery algorithm to improve the speed, performance and security of the SET protocol. The experimental results show that the improved algorithm possesses smaller time complexity as well as less computational resources compared with the existing algorithm, which further improves the security of the SET protocol.*
Keywords: Network security; E-commerce; SET protocol; payment system; ECC

1. **Introduction.** E-commerce refers to the process of using computer network technology and communication technology to realise the activities of exchanging information and goods within the legally recognised scope [1, 2, 3]. E-commerce can not be carried out smoothly without the development of computer networks. The Internet is a highly open and rapidly developing network, on which there are many unknowable factors, which pose a great threat to Internet-based E-commerce. In order to ensure the security of E-commerce, various measures have been taken, the core of which is the study of secure

E-commerce protocols. Secure E-commerce protocols, are rules that all parties to an electronic transaction must follow [4, 5].

The rise of E-commerce has greatly improved social productivity and promoted the rapid development of the economy; at the same time, the development of E-commerce has also brought about some security problems, especially the electronic payment security problem largely restricts the development of E-commerce, affecting the enthusiasm of the majority of users of online electronic consumption. E-commerce, as an emerging industrial model, is characterised by virtuality, which makes the relationship between people and parties more complex, making the whole transaction system uncertain and prone to cause related security problems [6, 7]. Therefore, E-commerce payment security is a complex issue, how to technically strengthen the security control, so that E-commerce in a safe environment for the healthy development, so that E-commerce can be more widely used [8, 9].

E-commerce is using the Internet as a trading platform. However, the openness of the Internet makes E-commerce face many security problems, such as information eavesdropping, tampering, counterfeiting, and malicious damage, which are also the key factors restricting the flourishing development of E-commerce [10, 11]. How to ensure the security and integrity of information in the transmission process has been the main direction of research, such as data encryption technology, security protocols, security mechanisms, etc [12, 13]. Currently, the main protocol used in E-commerce is SET (Secure Electronic Transaction). SET is an electronic payment model that was proposed in 1997 [14, 15]. SET is widely used because it provides mutual authentication between customers, merchants and banks and uses techniques such as data encryption and digital signatures to ensure authentication, confidentiality, integrity and non-repudiation of data.

The SET protocol has been recognised by the IETF (Internet Engineering Task Force) standards and has become a de facto industry standard [16]. The SET protocol mainly adopts a combination of symmetric and asymmetric encryption algorithms to ensure the integrity and consistency of the data and to achieve the transaction of the anticounterfeiting, the symmetric algorithm generally uses DES encryption algorithm, and the asymmetric encryption algorithm generally uses RSA encryption algorithm. SET protocol is a typical implementation under PKI (Public Key Infrastructure) [17], mainly used in B2C commerce mode to guarantee the security of information. Although the SET protocol is highly secure, it still has some shortcomings, such as low implementation efficiency and the need for repeated authentication of transaction parties. The client software must be downloaded and installed once again each time a user switches computers in order to make transactions, which is quite inconvenient for the cardholder. Therefore, developing and enhancing the SET protocol is crucial to addressing the security issues with E-commerce.

1.1. **Related Work.** The current asymmetric encryption system used by the SET protocol is the RSA cryptosystem. the SET protocol requires a 2048-bit key for the Certificate Authority (CA) and a 1024-bit key for organisations other than the CA [18].

With the development of science and technology, the processing and computing speed of computers is getting faster and faster, resulting in the time spent on decomposing factors is getting shorter and shorter, which has gradually threatened the security of the current 1024-bit key. In order to solve this problem, there are two methods [19, 20]: one is to improve the RSA cryptosystem, increase the key length and try to speed up its computing speed; the second is to find a new cryptosystem that can replace RSA. Currently, Elliptic curve cryptosystem (ECC) has become a strong contender to replace RSA, and ECC has been gradually regarded as the best public key cryptosystem other than RSA cryptosystem, and has already posed a strong challenge to RSA cryptosystem,

and is expected to become the next generation public key cryptosystem standard. This work focuses on the possibility of ECC cryptosystems in SET protocol applications.

The security of ECC is based on the elliptic curve discrete logarithm problem. Compared with RSA cryptosystem, ECC cryptosystem is able to use shorter keys to achieve the same security, and it is usually considered that a 160-bit elliptic curve key is able to have the same security strength as a 1024-bit key of RSA algorithm, and this proportionality will be bigger and bigger with the increase of the key length, so it has a better resistance to attack [21, 22]. Moreover, shorter keys also bring advantages such as faster computing speed, smaller storage space, lower bandwidth requirements, and better flexibility. It makes elliptic curve cryptosystems extremely suitable in various environments especially in space resource constrained environments, thus ECC is more advantageous for applications in E-commerce, wireless communication and other fields.

The current research related to ECC has two main aspects: one is the research on secure elliptic curve generation, mainly how to quickly find a large number of secure elliptic curves is a hot research topic; the other is how to quickly implement ECC, i.e., the research on the ECC scalar multiplication algorithm. Kavitha [23] explored the problem of achieving secure communication in wireless sensor networks and introduced an ECC-based based ECC with efficient implementation to ensure efficient secure communication in a limited resource environment. For how to implement efficient and scalable ECC in IoT, Noori et al. [24] proposed a novel curve selection method based on ECC scalar algorithm to improve the computational efficiency. Also, a fast decoding method based on algebraic curve coding is proposed to reduce the decoding cost. By applying these optimisation methods to ECC in IoT, the computational and communication efficiency of IoT devices can be improved. To address the bottlenecks in conventional ECC processors, Kalaiarasi et al. [25] proposed an improved ECC processor architecture for digital signature applications to increase cryptographic processing speed and circuit area efficiency. A new modulo-multiplication algorithm is introduced that reduces the use of multipliers by using techniques such as addition, subtraction and shift operations, thus increasing the processing speed. In addition, the paper introduces a new parallel arithmetic structure that allows multiple modulo multiplication operations to be computed in parallel, further improving processing efficiency.

1.2. **Motivation and contribution.** The most time-consuming part of ECC is the operation of the scalar multiplication algorithm, which is also the main research direction to improve the performance of ECC, and the improvement of the scalar multiplication algorithm plays an important role in the fast application of ECC. In order to further improve the security and reduce the computational resources of ECC, this work improves the ECC. The main innovations and contributions of this work include:

(1) The key modules of a secure e-commerce payment system based on SET protocol are given. The digital signature module is used to realize double digital signatures by connecting two messages sent to different receivers by improving the digital signature principle to guarantee the payment security of cardholders. An E-commerce recommendation method based on payment encryption is given.

(2) Aiming at the deficiencies of the encryption and decryption algorithms in the SET protocol, an improved ECC is proposed for replacing the original private key encryption algorithm to improve the speed, performance and security of the SET protocol. On the basis of Non-Adjacent Form (NAF) [26] scalar algorithm, it is improved and combined with Montgomery scalar algorithm, called Montgomery & NAF.

2. **The SET protocol and how it works.**

2.1. **Introduction to the SET protocol.** There are two main problems to be solved in the technical aspects of the design of E-commerce systems: one is the accuracy of message delivery and the other is the security of message delivery. The former is well solved by the message exchange protocol, while the latter is a problem to be studied at present. For this reason, the SET1.0 standard was born through the unremitting efforts of all parties. Since its launch, this standard has been supported by many vendors such as IBM, Netscape, Microsoft, Oracle and recognised by IETF standards, and has become the B2C industry standard.

The main contents of SET protocol are: (1) Application of encryption algorithm; (2) Certificate and its object format; (3) Purchase and its object format; (4) Payment and its object format; (5) Message protocol between each participant.SET protocol adopts the following technological means: symmetric encryption, asymmetric encryption, MD5 algorithm, digital certificates, digital signatures, double digital signatures, digital envelopes and other technologies. The confidentiality of data is ensured by using symmetric and asymmetric key encryption. Data integrity and non-repudiation is ensured through the use of digital signatures, MD5 algorithms. Authentication of the parties involved in the transaction through digital certificates. The transaction participants of the SET protocol include the cardholder, the merchant, the issuing bank, the acquiring bank, the payment gateway, and the CA, as shown in Figure 1. The protocol specifies the definition of the type of transaction parties and the format of the message during processing. Before both parties send a message, the consumer, merchant and payment gateway must authenticate each other's identity through the authentication centre to ensure that the other party's identity is authentic and reliable.

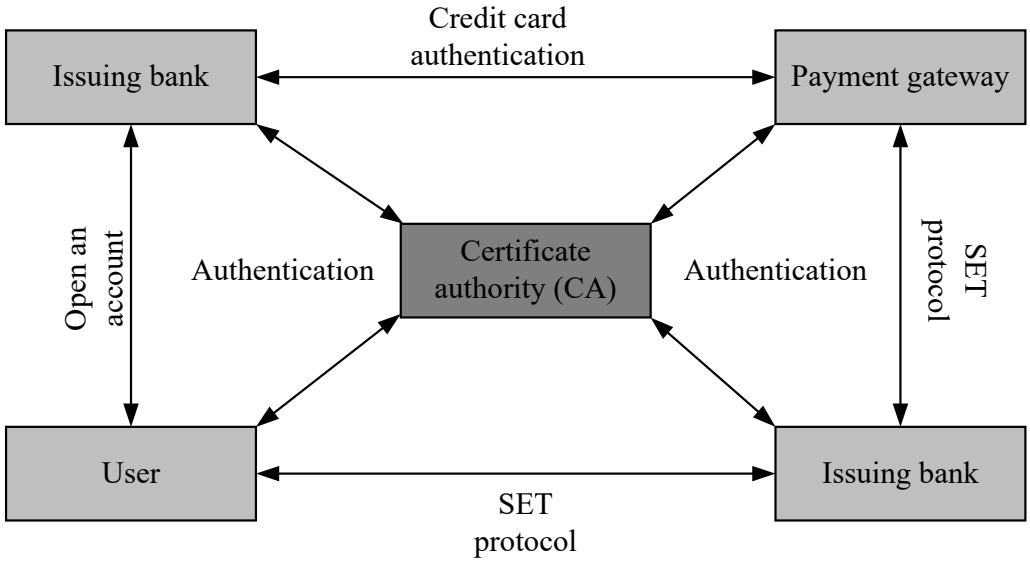

Figure 1. Working principle of SET protocol

2.2. **Process of the SET protocol.** In order to ensure that the information is not modified during transmission, it is necessary to encrypt the information sent. There are many ways to classify cryptographic encryption algorithms according to different criteria, among which the most common classification is according to the key method, which is divided into symmetric key encryption algorithm and asymmetric key encryption algorithm. The workflow of the SET protocol is shown below [27]:

(1) The customer sends a purchase request to the merchant.

(2) The merchant sends a catalogue listing to the customer.

(3) If the customer agrees to purchase, digitally sign the Order OI (Order Instruction): $OI' = Dskc\ (OI)$ and send the signed Order OI' to the merchant.

(4) The merchant decrypts the order OI using its private key: $OI = E_{pxc}(OI')$, thus determining that the order was sent by the customer. The merchant digitally signs its own certificate $CerM$, the payment gateway's certificate $CerP$, and the payment request Pay: $Y = DsKM(CerM, CerP, Pay)$ and sends Y to the customer.

(5) The customer receives Y, decrypts $Y : (CerM, CerP, Pay) = EPKM(Y)$, confirms that Y is from the merchant and the identity of the payment gateway. The customer generates a Payment Instruction (PI) according to the payment request and digitally signs $PI : PI' = Dskc(PI)$. The system randomly generates a symmetric key K, which the customer uses to encrypt PI: $PI' = E_K(PI')$.

(6) The card issuer validates the message to confirm that the customer's account number is valid, and then sends the PI processing result to the payment gateway to transfer the customer's account payment to the merchant's account.

(7) The payment gateway encrypts the payment completed message Msg: $Msg' = D_{SKP}(Msg)$ and sends Msg' to the merchant.

(8) Merchant decrypts Msg': $Msg = E_{PKP}(Msg')$, confirms that it was sent by the merchant, and provides the goods or services to the customer upon completion.

(9) The issuing bank sends a list of purchases to the customer.

The statistics of the number of times the cardholder, merchant, and payment gateway transmit certificates, digitally sign, and encrypt messages during SET transactions are shown in Table 1.

Table 1. Certificate number of passes statistics.

Participant	Number Of Transmissions	Number Of Identifications
Cardholders	1(Cardholder Signature 1)	3(Merchant Signatures 2; Payer Encryption 1)
Businessmen	5(Cardholder Certificate 1; Payer Certificate 1; Encrypted Merchant Certificate 1; Merchant Certificates 2)	3(Cardholder Certificate 1; Encryption Gateway Certificate 1; Signature Gateway Certificate 1)
Payment Gateway	1(Signature Gateway Certificate 1)	3(Cardholder Signature Certificate 1; Encrypted Merchant Certificate 1; Signed Merchant Certificate 1)

3. **Secure e-commerce payment system based on SET protocol.**

3.1. **Double digital signature design.** Based on the workflow of SET protocol, this paper designs a secure e-commerce payment system based on SET protocol.

Dual digital signature is an effective improvement of digital signature by concatenating two messages sent to different receivers. The composition process of dual digital signature is described in detail as follows: firstly, the digests $OIMD$ and $PIMD$ of the cardholder's OI information and PI information are computed, and the two digests are effectively connected to obtain the cardholder's dual information $POMD$; then the cardholder adopts the private key E_{KRC} to encrypt the obtained $POMD$, which means that the dual digital signature is obtained. The calculation of the process is shown below:

$$TS = E_{KRC}\left[F(F(PI)) \parallel F(OI)\right] \tag{1}$$

where E_{KRC} denotes the private key used to represent the cardholder, TS denotes the dual digital signature result; and $F(OI)$ and $F(PI)$ are the encryption results of the OI information and the PI information, i.e., $OIMD$ and $PIMD$, respectively.

After the merchant gets the TS, $PIMD$, OI and the digital certificate from the cardholder, the merchant uses Equation (2) to decode the dual digital signature to obtain the dual data digest $POMD$, and compares the decoding result with the calculation result of Equation (3). If the results are consistent, the dual digital signature signature is judged to be correct, and vice versa the results are inconsistent and the signature is verified to be incorrect.

$$POMD = T_{KUE}[TS] \tag{2}$$

where T_{KUE} is the decoding key. After the payment gateway obtains the dual digital signatures TS, $PIMD$, OI and digital certificates, the decoding formula is used to decode them, and the decoding results are compared with the results of Equation (3) to verify the correctness of the dual digital signature results.

$$\begin{cases} \text{POMD} = F\left(F(\text{PI}) \parallel \text{OIMD}\right) \\ \text{POMD} \neq F\left(F(\text{PI}) \parallel \text{OIMD}\right) \end{cases} \tag{3}$$

In the process of carrying out dual digital signatures for e-commerce payments, if the merchant does not have the cardholder's payment information PI, the payment network cannot obtain the ordering information of the goods, thus indicating that the dual digital signatures used in the model of this paper can guarantee the security of the cardholder's payment.

This paper is based on the implementation of the functions of the payment gateway module in the secure e-commerce payment improvement model of the SET protocol, including the change of various businesses of cardholders and merchants, the query of the account business, and the registration, etc. The CA module is responsible for the issuance of digital certificates and the verification of digital certificates, and the CA module includes the digital authentication and the digital certificate manager.

3.2. **E-commerce recommendation based on payment encryption.** E-commerce payment and traditional payment mode has a certain similarity between the size of its similarity can be expressed by the degree of affiliation. If its similarity is $T(a)$, the value of personalisation in e-commerce is W_i. The step of encryption of e-commerce information is designed for execution, and the specific encryption rule parameter calculation steps are as follows:

$$f(x) = \max T(a) \cdot \log\left(\frac{1}{2}(R - W_i)\right) \tag{4}$$

In order to avoid problems such as loss and leakage of user information, on the basis of the above algorithm, further information encryption processing is carried out and a vulnerability detection execution step is added, if the vulnerability feature value in the encryption process is ϕ and the collection value is L, the data feature normalisation is carried out according to the collection result, and the normalisation computation process is shown as follows:

$$\delta = \ln\varphi \frac{f\left(x\right) - 1}{\sum L\left[\max G\left(a\right) - \min G\left(a\right)\right]} \tag{5}$$

where $\max G(a)$ and $\min G(a)$ represent the maximum and minimum values of the vulnerability in the process of information e-security payment, respectively. Based on the above calculation steps for e-commerce information encryption vulnerability detection, The ACCESS data management structure is used to preprocess the core network management data C_1, detailed list data C_m, platform data C_3, complaint data C_4 and other related data to achieve the analysis and management of user value and user perception

data.

$$\lambda = \delta \sum_{m=0}^{\infty} [C_1 + C_m + C_3 + C_4]/n \tag{6}$$

where m denotes the value of the detail data C_m in the range $(0, +\infty)$.

E-commerce personalized recommendation system for the analysis of user value and user perception, the main algorithms used are big data analysis algorithms, including hierarchical analysis and clustering threshold method. Based on the above two algorithms for e-commerce payment affiliation is calculated, let the number of times V appears in the profile of commodity M on the feature n affiliation can be expressed as:

$$\eta = \lambda - \frac{M}{V} + 1 \tag{7}$$

In order to better widen the gap between commodity payment affiliations and highlight the importance of e-payment features, a larger weight is assigned to some of the features α_n, and the value of the affiliation relationship on each feature is F. Then the e-payment security value is calculated in the following way as shown below:

$$S_i = \sum_{n=0}^{\infty} \alpha_n \eta \oplus F_n \tag{8}$$

4. **Montgomery & NAF based SET protocol.**

4.1. **Basic concepts of ECC.** ECC is a cryptographic principle based on the discrete logarithmic problem in the domain of elliptic curves. The principle of ECC focuses on the discrete logarithmic problem on appropriately chosen elliptic curves. Under the same security conditions, the encryption and decryption problems can be solved using smaller parameters in ECC as compared to DSA & RSA cryptosystems. Combined with the above analysis, we can conclude that ECC has the following advantages: relatively shorter key lengths are used; smaller digital certificates and digital signatures, and faster computing speed.

The commonly used elliptic curve finite domains mainly include: prime number domain $GF(p)$ and binary domain $GF(2^m)$. Among them, the elements in the binary domain are easier to achieve parallel addition, subtraction, multiplication and other operations in the computer, and thus elliptic curve cryptosystems often choose the binary domain for hardware encryption. The non-singular elliptic curve E on the binary domain $GF(2^m)$ is shown as follows:

$$y^2 + xy = x^3 + ax^2 + b \tag{9}$$

where a, b are elements in $GF(2^m)$ and $b \neq 0$.

The curve also contains an infinity point denoted by O as an additive unit element of a point on the curve. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, be two points on E and $P_1 \neq -P_2$, then $P_3 = P_1 + P_2 = (x_3, y_3)$.

(1) $P_1 \neq P_2$

$$\begin{cases} \lambda = (y_2 + y_1)/(x_2 + x_1) \\ x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \end{cases} \tag{10}$$

(2) $P_1 = P_2$

$$\begin{cases} \lambda = y_1/x_1 + x_1 \\ x_3 = \lambda + \lambda + a \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \end{cases} \tag{11}$$

In ECC, the encryption and decryption processes require the public key protocol to perform elliptic curve computation, the process is as follows: choose a base domain F_q, and define a point P of prime order on the elliptic curves E and F on this domain. The coordinates of the point P are denoted by (x_p, y_p). The domain elements a and b in the finite domain F_q are pre-set parameters of the elliptic curve. When the system is built each user will generate the corresponding key individually.

By analysing the elliptic curve key exchange process, it can be seen that if the encryption and decryption speed is to be improved, improving the efficiency of the number multiplication of points is the most central element. So we further analyse the computation of the elliptic curve number multiplication operation required by the encryption and decryption process of ECC as follows:

$$Q = kP = \underbrace{P + ... + P}_{k} \tag{12}$$

where P is a point on the elliptic curve, $k = (a_{n-1}, a_{n-1}, a_{n-1}, \ldots, a_2, a_1, a_0)$.

4.2. **Montgomery & NAF.** The (Non-Adjacent Form, NAF) ECC scalar algorithm has been improved and combined with the Montgomery scalar algorithm, called Montgomery&NAF. The representation of ECC based on the binary NAF method is shown below:

$$k = \sum_{i=0}^{n-1} k_i 2^i, \quad k_i \in \{0, 1, -1\} \tag{13}$$

The NAF(k) is scanned from left to right, and addition or subtraction operations are performed based on the plus or minus sign judgement of each digit.

For elliptic curves on $GF(2^m)$, Montgomery's algorithm is a new number multiplication algorithm that is well suited for execution on hardware and software. The Montgomery algorithm has the same amount of computation during each iteration and can be effective against timing attacks.

Based on the binary NAF scalar algorithm, this work improves it in order to further improve its security and reduce computational resources. The structure of the NAF form consisting of integer K shows that when a non-zero digit is arbitrarily found from the NAF(K) digit string, three consecutive digits are read from that digit, and the three digits have and only have the following six combinations of the following forms: -10-1, -100, -101, 10-1, 100, and 101. The dot-add computations corresponding to these six forms are denoted as: $Q - 5G$, $Q - 4G$, $Q - 3G$, $Q + 3G$, $Q + 4G$, and $Q + 5G$. Since only an odd number of digits within the window is required during the dot product operation, we can optimise the operation by saving only the values whose window contents are $Q \pm 3G$ and $Q \pm 5G$, and combining them with the dot-add algorithm in the binary NAF scalar algorithm to improve the speed of the dot product operation.

We take the window $m = 5$ and the binary length of the integer K to be 256. The number of dot-add and double-dot operations required by the integer K for multiple NAF algorithms is shown in Table 2. A comparison can visualise the computational requirements for the same number of doubling points, but the computation amount is reduced by 50 %.

Table 2. Comparison of four algorithms in terms of computational power

	Binary system (math)	**NAF**	**Improved NAF**
Light bulb	192	128	64
Double point	384	384	384

We take the combination of Shamir and improved NAF to propose a Montgomery&NAF double scalar multiplication algorithm, which combines the advantages of the two, and reduces the number of point multiplications while also reduces the amount of point storage, and because the increase of the window width m inevitably leads to a reduction in the amount of storage of the points, which also reduces the number of loops of the main computation to a certain extent. The following is an example of Montgomery & NAF double scalar multiplication algorithm for 256-bit integer K as shown in Algorithm 1.

Algorithm 1 Montgomery & NAF double scalar multiplication algorithm

Input: $G \in E(GF(q))$, 256-bit positive integer K;
Output: $Q = KP$;
Calculate $k = \sum_{n=0}^{256} C_n 2^n$, $C_n \in \{-1, 0, 1\}$;
Calculate np while $n \in \{\pm 3, \pm 5\}$;
$Q = 0$;
for (int $n = 256; n \geq 0; n--$) **do**
    $Q = 2Q$;
    if ($C_n = -1$) **then**
        if ($C_{n-2} = -1$) **then** $Q = Q - 5G$;
        else if ($C_{n-2} = 0$) **then** $Q = Q - 5G; Q = 2Q$;
        else if ($C_{n-2} = 1$) **then** $Q = Q - 3G$;
        end if
        $n = n - 2$;
    else if ($C_n = 1$) **then**
        if ($C_{n-2} = -1$) **then** $Q = Q + 3G$;
        else if ($C_{n-2} = 0$) **then** $Q = Q + G; Q = 2Q$;
        else if ($C_{n-2} = 1$) **then** $Q = Q + 5G$;
        end if
        $n = n - 2$;
    end if
end for
return Q

Pre-calculated arithmetic is shown as follows:

$$[(3 \cdot 2^{2(n-1)} - 2^{n-1} - 1)A + (2^{2(m-1)} - 2^{m-1})D] \tag{14}$$

where A is a dot-add operation and D is a double dot-multiplication operation.

The main calculation has an arithmetic capacity:

$$[(((2^{2m} - 1)e/2^{2m}) - 1)A + (e - 1)mD] \tag{15}$$

When $m = 2$, the expected count is shown as follows:

$$9A + 2D = 9(I + S + 2M) + 2(I + 2S + 2M) = 120.4 \tag{16}$$

When $m = 2$, the main computation is shown as follows:

$$119A + 254D = 119(I + S + 2M) + 254(I + 2S + 2M) = 4231.6 \tag{17}$$

The comparison of Montgomery's algorithm and Montgomery & NAF algorithm in terms of point storage and computation when the window width m is 2, 3, and 4 is shown in Table 3 and Table 4.

From the above comparison, it can be seen that when m is large and the number of bits of *(K, C)* is small, the precomputation and point storage using Montgomery's algorithm are large and the utilisation of stored points is low. If the Montgomery & NAF algorithm

Table 3. Point Storage Comparison

	Montgomery	Montgomery & NAF	Percentage reduction
m=2(K, C= 256)	17	7	59 %
m=3 (K, C= 576)	62	18	71 %
m=4(K, C= 1024)	236	42	82 %

Table 4. Comparison of calculations

	Montgomery	Montgomery & NAF	Percentage reduction
m=2(K, C= 256)	4148 M	5248 M	21 %
m=3 (K, C= 576)	8762 M	10056 M	13 %
m=4(K, C= 1024)	15482 M	16886 M	8 %

is used instead, not only the storage of points can be reduced significantly, but also the arithmetic of point multiplication is not increased significantly.

5. Experimental results and analyses.

5.1. **Security performance analysis.** Currently, ECC commonly uses a security key word length of 1024 bits or more, but increasing the key length will directly cause the ECC encryption and decryption speeds to decrease dramatically, making hardware implementation more difficult as well. MIPS is commonly used to measure the security of a cipher, which represents the time required for a computer executing 1 million instructions per second to run for one year. Generally, a cipher whose deciphering time reaches 1012 MIPS years is regarded as a secure cipher. a comparison of the deciphering times of Montgomery and Montgomery & NAF is shown in Figure 2.

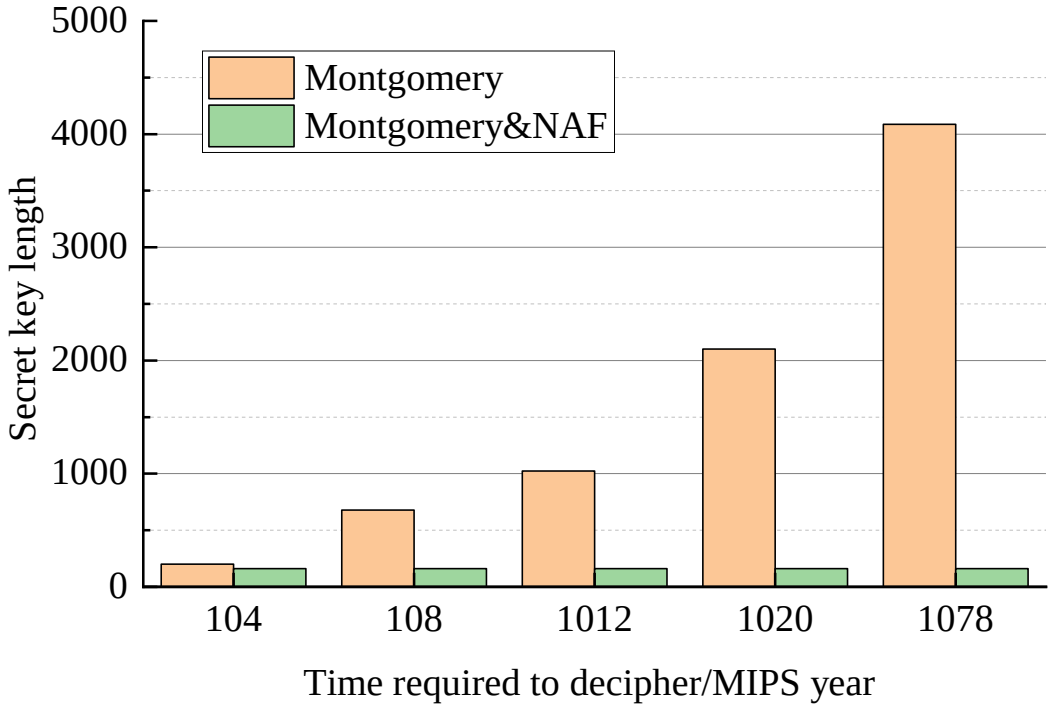

Figure 2. Comparison of deciphering times

It can be seen that Montgomery&NAF is more secure than Montgomery, which requires only 160 bits of key length for security, compared to 1024 bits for Montgomery. As the

key length increases, the security of Montgomery & NAF increases much faster than that of Montgomery.

In order to better compare ECC with RSA in depth, we take out different key lengths of Montgomery and Montgomery & NAF for encryption and decryption operations respectively. The key length ratios of the three groups are 128/1024,160/2048 and 192/4096 respectively. Table 5 defines the key length and message length.

Table 5. Key Size and Message Length

Montgomery & NAF	**Montgomery**	**Message length**
128	1024	1500/3000/5000
160	2048	1500/3000/5000
192	4096	1500/3000/5000

Firstly, the encryption part is analysed. A comparison of the encryption time consumption of the two algorithms for a message length of 5000 bit is shown in Figure 3. In this experiment, the 5000 bits is divided into 625 blocks for the operation, and an independent number of encryptions is used for each message block.

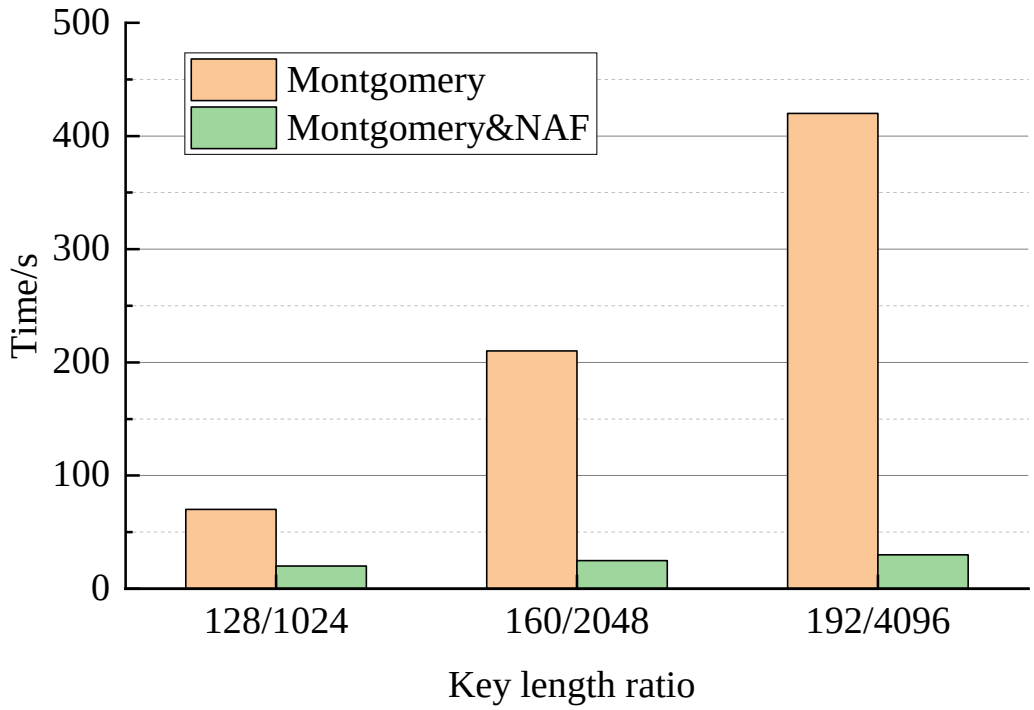

Figure 3. Comparison of encryption time consumption

The key length ratios of the two algorithms during encryption are 128/1024, 160/2048, and 192/4096. it can be seen that the encryption time consumed by Montgomery increases significantly with the increase in the key length compared to Montgomery & NAF. Comparison of decryption time consumption of the two algorithms at 5000-bit message length is shown in Figure 4. The decryption time spent by Montgomery increases significantly as the key length increases, compared to Montgomery & NAF where the decryption time spent by Montgomery & NAF is slightly increased within acceptable limits.

In summary, based on the experimental results of encryption and decryption operations, we can see that Montgomery & NAF performs faster and has superior performance. And

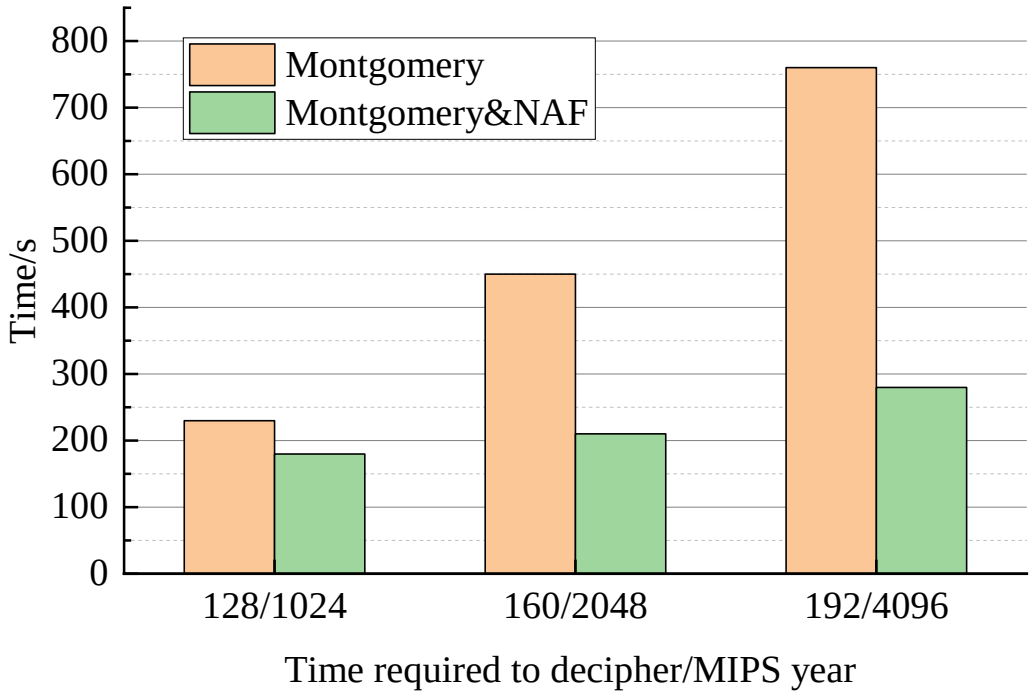

Figure 4. Comparison of decryption time consumption

as the key length increases, the time consumed for encryption and decryption grows less in Montgomery & NAF compared to Montgomery. Therefore, we can conclude that Montgomery & NAF is a better encryption and decryption method in SET protocol.

5.2. **Feasibility analysis.** The sample files are randomly selected for encryption and decryption operations. Table 6 represents the information about all the encrypted files including file serial number, storage, time, memory information and file size of all the encrypted files.

Table 6. File Encryption Time, Memory and File Size

No.	Time/ms	Memory consumption/KB	File size
1	179	21304.24535	110
2	92	41612.40423	105
3	233	23402.11316	105
4	165	44308.62127	100
5	335	34144.25235	185
6	202	17412.56431	30
7	315	17314.12356	42
8	258	16809.25475	40
9	16	12154.25187	14
10	14	12583.48112	15

The memory consumption indicates the amount of main memory required to process the encryption algorithm. It can be observed that the encryption memory consumption is roughly all under 45000 KB and the time required for encryption is all under 350 ms. Data decryption accuracy is the amount of data that is accurately recovered after the encrypted file is decrypted. The quasi-accuracy of data decryption is shown in Figure 5. The decryption accuracy of the improved scheme is basically 98 %. The analysis shows

that the time and memory consumed for encryption and decryption are within acceptable limits. From the analysis of the above figure, it can be seen that the storage overhead increases with the increase in the size of the original file and overall the overhead is less. The result shows that the system recovers 98 % of the data during the decryption process. Thus the algorithm consumes less memory resources as well as time resources while maintaining security thus showing the effectiveness of the proposed technique.

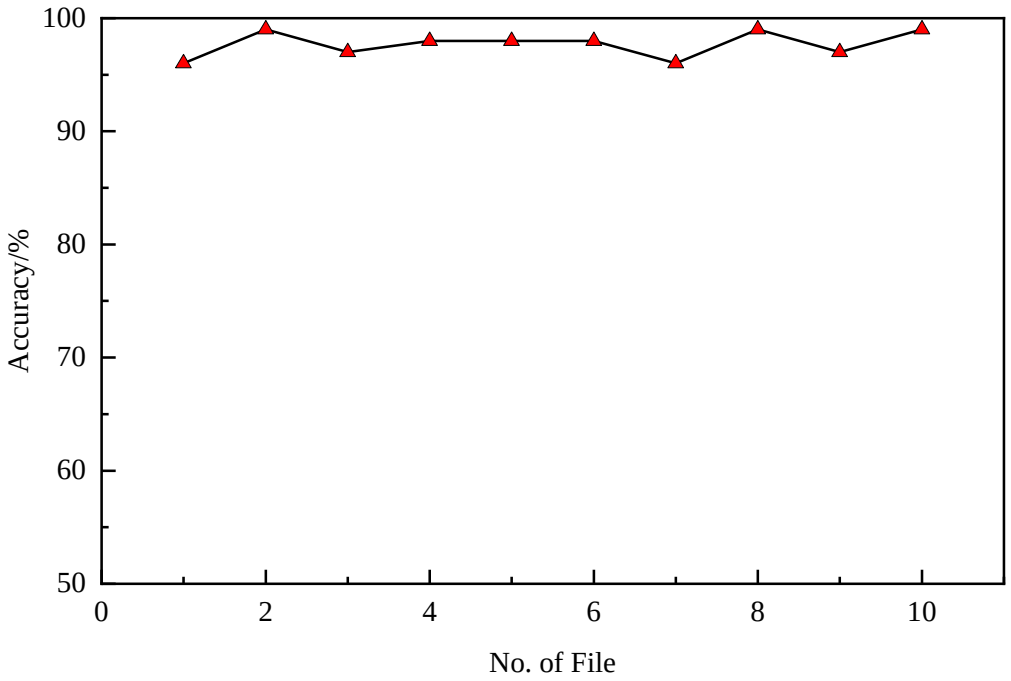

Figure 5. Decryption accuracy

6. **Conclusion.** This work gives the key modules of secure e-commerce payment system based on SET protocol. By improving the principle of digital signature, the digital signature module is adopted to connect two messages sent to different recipients to realize double digital signature, thus ensuring the payment safety of cardholders. The e-commerce recommendation method based on payment encryption is given. In addition, a Montgomery & NAF algorithm is proposed to improve the speed, performance and security of the SET protocol. Experimental results show that the E-commerce payment system based on the proposed SET protocol can recover 98 % of the data during the decryption process. Thus, the algorithm consumes less memory resources as well as time resources while ensuring security thus demonstrating the effectiveness of the proposed technique. However, choosing the parameters of the elliptic curve is a critical issue. The selection of parameters for security requires considering both security and performance and ensuring that the points on the elliptic curve provide sufficient security strength. Therefore, subsequent studies will address this issue with extended analyses.

REFERENCES

[1] B. S. Marció, P. Nienheysen, D. Habor, and R. C. Flesch, "Quality assessment and deviation analysis of three-dimensional geometrical characterization of a metal pipeline by pulse-echo ultrasonic and laser scanning techniques," *Measurement*, vol. 145, pp. 30-37, 2019.

[2] Y. H. Jo and S. Hong, "Three-dimensional digital documentation of cultural heritage site based on the convergence of terrestrial laser scanning and unmanned aerial vehicle photogrammetry," *ISPRS International Journal of Geo-Information*, vol. 8, no. 2, 53, 2019.

[3] J.-R. Roussel, D. Auty, N. C. Coops, P. Tompalski, T. R. Goodbody, A. S. Meador, J.-F. Bourdon, F. De Boissieu, and A. Achim, "lidR: An R package for analysis of Airborne Laser Scanning (ALS) data," *Remote Sensing of Environment*, vol. 251, 112061, 2020.
[4] S. Wittke, X. Yu, M. Karjalainen, J. Hyyppä, and E. Puttonen, "Comparison of two-dimensional multitemporal Sentinel-2 data with three-dimensional remote sensing data sources for forest inventory parameter estimation over a boreal forest," *International Journal of Applied Earth Observation and Geoinformation*, vol. 76, pp. 167-178, 2019.
[5] M. J. Allen, S. W. Grieve, H. J. Owen, and E. R. Lines, "Tree species classification from complex laser scanning data in Mediterranean forests using deep learning," *Methods in Ecology and Evolution*, vol. 14, no. 7, pp. 1657-1667, 2023.
[6] J. Chen, Z. Kira, and Y. K. Cho, "Deep learning approach to point cloud scene understanding for automated scan to 3D reconstruction," *Journal of Computing in Civil Engineering*, vol. 33, no. 4, 04019027, 2019.
[7] V. Jain, B. Malviya, and S. Arya, "An overview of electronic commerce (e-Commerce)," *Journal of Contemporary Issues in Business and Government*, vol. 27, no. 3, pp. 665-670, 2021.
[8] S. Escursell, P. Llorach-Massana, and M. B. Roncero, "Sustainability in e-commerce packaging: A review," *Journal of Cleaner Production*, vol. 280, 124314, 2021.
[9] G. Taher, "E-commerce: advantages and limitations," *International Journal of Academic Research in Accounting Finance and Management Sciences*, vol. 11, no. 1, pp. 153-165, 2021.
[10] V. Alfonso, C. Boar, J. Frost, L. Gambacorta, and J. Liu, "E-commerce in the pandemic and beyond," *BIS Bulletin*, vol. 36, no. 9, pp. 1-9, 2021.
[11] H. Jeong, Y. Yi, and D. Kim, "An innovative e-commerce platform incorporating metaverse to live commerce," *International Journal of Innovative Computing, Information and Control*, vol. 18, no. 1, pp. 221-229, 2022.
[12] T.-Y. Wu, X. Guo, Y.-C. Chen, S. Kumari, and C.-M. Chen, "SGXAP: SGX-Based Authentication Protocol in IoV-Enabled Fog Computing," *Symmetry*, vol. 14, no. 7, 1393, 2022.
[13] T.-Y. Wu, Q. Meng, L. Yang, X. Guo, and S. Kumari, "A provably secure lightweight authentication protocol in mobile edge computing environments," *The Journal of Supercomputing*, vol. 78, no. 12, pp. 13893-13914, 2022.
[14] T. Wu, X. Guo, Y. Chen, S. Kumari, and C. Chen, "Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks," *Drones*, vol. 6, no. 1, 10, 2021.
[15] E. W. Mainardes, I. M. de Souza, and R. D. Correia, "Antecedents and consequents of consumers not adopting e-commerce," *Journal of Retailing and Consumer Services*, vol. 55, 102138, 2020.
[16] X. Lin, X. Wang, and N. Hajli, "Building e-commerce satisfaction and boosting sales: The role of social commerce trust and its antecedents," *International Journal of Electronic Commerce*, vol. 23, no. 3, pp. 328-363, 2019.
[17] G. Xu, Y. Zhang, A. K. Sangaiah, X. Li, A. Castiglione, and X. Zheng, "CSP-E2: An abuse-free contract signing protocol with low-storage TTP for energy-efficient electronic transaction ecosystems," *Information Sciences*, vol. 476, pp. 505-515, 2019.
[18] J. Chen, H. Xiao, M. Hu, and C.-M. Chen, "A blockchain-based signature exchange protocol for metaverse," *Future Generation Computer Systems*, vol. 142, pp. 237-247, 2023.
[19] C.-M. Chen, Z. Li, S. Kumari, G. Srivastava, K. Lakshmanna, and T. R. Gadekallu, "A provably secure key transfer protocol for the fog-enabled Social Internet of Vehicles based on a confidential computing environment," *Vehicular Communications*, vol. 39, 100567, 2023.
[20] H. Xiong, Z. Zhou, L. Wang, Z. Zhao, X. Huang, and H. Zhang, "An Anonymous Authentication Protocol with Delegation and Revocation for Content Delivery Networks," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4118-4129, 2022.
[21] H. Xiong, C. Jin, M. Alazab, K.-H. Yeh, H. Wang, T. R. Gadekallu, W. Wang, and C. Su, "On the Design of Blockchain-Based ECDSA with Fault-Tolerant Batch Verification Protocol for Blockchain-Enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1977-1986, 2022.
[22] H. Xiong, J. Chen, Q. Mei, and Y. Zhao, "Conditional Privacy-Preserving Authentication Protocol with Dynamic Membership Updating for VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 2089-2104, 2022.
[23] V. Kavitha, "Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 821-836, 2021.

[24] D. Noori, H. Shakeri, and M. Niazi Torshiz, "Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment," *EURASIP Journal on Information Security*, vol. 2020, pp. 1-11, 2020.

[25] M. Kalaiarasi, V. Venkatasubramani, V. Vinoth Thyagarajan, and S. Rajaram, "A parallel elliptic curve crypto-processor architecture with reduced clock cycle for FPGA platforms," *The Journal of Supercomputing*, vol. 78, no. 13, pp. 15567-15597, 2022.

[26] M. Alkhatib and W. S. Aldalbahy, "A Low-Cost and High-Performance Cryptosystem Using Tripling-Oriented Elliptic Curve," *Intelligent Automation & Soft Computing*, vol. 37, no. 2, pp. 167-187, 2023.

[27] D. Wang, Y. Lin, J. Hu, C. Zhang, and Q. Zhong, "FPGA Implementation for Elliptic Curve Cryptography Algorithm and Circuit with High Efficiency and Low Delay for IoT Applications," *Micromachines*, vol. 14, no. 5, 1037, 2023.

[28] D. B. Roy and D. Mukhopadhyay, "High-speed implementation of ECC scalar multiplication in GF (p) for generic Montgomery curves," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 27, no. 7, pp. 1587-1600, 2019.

[29] M. Bedoui, B. Bouallegue, H. Mestiri, B. Hamdi, and M. Machhout, "An improvement of both security and reliability for elliptic curve scalar multiplication Montgomery algorithm," *Multimedia Tools and Applications*, vol. 82, no. 8, pp. 11973-11992, 2023.

[30] J. C. Bajard and S. Duquesne, "Montgomery-friendly primes and applications to cryptography," *Journal of Cryptographic Engineering*, pp. 1-17, 2021.