SN Computer Science (2020) 1:112
https://doi.org/10.1007/s42979-020-00122-1

ORIGINAL RESEARCH

An Identity-Based Elliptic Curve Cryptography for Mobile Payment Security

O. R. Vincent[1] · T. M. Okediran[1] · A. A. Abayomi-Alli[1] · O. J. Adeniran[2]

Received: 6 November 2019 / Accepted: 13 March 2020 / Published online: 2 April 2020

Abstract

Security breaches have been observed in different dimensions in mobile payment system. The violation of user's privacy is a common phenomenon in mobile payment transactions. This study presents an improved security scheme for a mobile payment system using elliptic curve cryptography over a binary field with International Mobile Equipment Identity to ensure higher security. The scheme uses a payment gateway for registration and maps all input text to elliptic curve points using ASCII values. Payment details are stored on the gateway, which is encrypted but decrypted only with merchant's decryption key. The proposed scheme was evaluated in terms of key size, security strength, computational power, memory capacity, encryption and decryption time and mobile phone battery. The result shows that the scheme provides integrity, confidentiality and privacy. The result also shows that the proposed scheme is time-efficient and computationally inexpensive for resource-constrained environment like mobile payment system.

Keywords Mobile payment · Security · Payment gateway · Cryptography · ECC · IMEI

Introduction

The mobile payment system is a fast-growing and acceptable form of payment system. Mobile devices such as smartphones and tablets are quickly becoming the dominant devices for accessing Internet resources and has gained popularity with higher memory capacity, processor speed and battery life due to advancement in technology, making it suitable for mobile transactions [56, 57]. Mobile phones are common in our society today due to its multi-purpose usage, the convenience and mobility advantages, ease of purchase and it is used for payment on the move; payment anywhere and anytime [5, 37, 40, 44].

In recent times, mobile devices are often shared by multiple applications and for multiple purposes, which result in the breach of confidential information in financial transactions. Such confidential information breach includes illegal access to confidential data, identity fraud, man-in-the-middle attack, malware, phishing, spamming [3, 8, 20]. The Public dispersion of mobile phone increases the possibility of eavesdropping and abuse [23], risk and theft [41] and the security of user's valid credentials in the Internet of Things (IoT) [12]. Payment information is therefore exposed to compromise. Hence, fraud and identity theft become inevitable in mobile payment system [12, 23, 34]. Protecting user's data, which include user's valid credentials, smart card details and payment information, are essential.

Several research efforts have been devoted to addressing some of the challenges associated with mobile payment security. The dominant models used to fight against these challenges include biometric authentication [2]; cloud-based payment gateway [61]; Anonymous Gateway Payment protocol [17]; Secure wireless Payment protocol [21]; Rivest Sharma Addleman (RSA) concept for mobile users [34];

✉ O. R. Vincent
vincent.rebecca@gmail.com

T. M. Okediran
timothyokediran@gmail.com

A. A. Abayomi-Alli
abayomialliaa@funaab.edu.ng

O. J. Adeniran
adeniranoj@funaab.edu.ng

[1] Department of Computer Science, College of Physical Sciences, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria

[2] Department of Mathematics, College of Physical Sciences, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria

Lightweight Payment protocol [19], Pollard Rho [55] and Secure Mobile Payment system using QR code [37].

Though, confidentiality has been addressed to some extent, some of the models still have germane weaknesses. For instance, the significant advantages of the cloud-based payment gateway are the ease of access, cost, delivery and maintenance, computing power and purchase of computer equipment, but cloud server is not considered wholly secured because it cannot resist impersonation attack, lack of standards and continuous evolution [26, 33, 34, 49]. On the other hand, the payment gateway model provided confidentiality, integrity and anonymity, but does not provide fairness and non-repudiation [61]. Besides, the RSA, which has better security performance, is still susceptible to hacking [43, 53]. Biometric security also requires extra hardware that is not common to all mobile phones. In another perspective, the anonymous gateway protocol is not suitable for impersonation attack, though it protects the user's identity [61].

This paper presents an improved security scheme using identity-based elliptic curve cryptography (ECC) for a mobile payment system. The elliptic curve is defined over a finite binary field and is used as a public-key cryptosystem for encryption and decryption to provide confidentiality. The International Mobile Equipment Identity (IMEI) of the mobile phones serves as an identity element because of it uniqueness to all mobile phones.

There are two significant contributions of this paper. Firstly, the use of a modified ECC over a finite binary field, $F(2^m)$ on a payment gateway as an encryption protocol provides confidentiality and security against known attacks. Secondly, the incorporation of mobile phone IMEI protects against identity theft and non-repudiation. Other contributions include usability, low computational power and the possibility of shorter key size. This scheme is appropriate for the merchant's website, especially in a business-to-business transaction where both entities are registered parties on the payment gateway. The user, merchant, issuer and acquirer can communicate with the payment gateway.

The rest of the paper is organized as follows. Section two provides the literature review and background to ECC over Binary Field. Section three discusses the proposed identity-based ECC for mobile payment security and its architecture. Section four presents the implementation, result and evaluation, while section five gives the discussion of various parameters, and section six is the conclusion of this work.

Literature Review

Related Work

ECC has been deployed more recently in the electronic payment system because of its small key size. Chaudhry et al. [8] modified the ECC variation used by Yang et al. [60]. It used the properties of the elliptic curve such as its being symmetry about the x-axis, and the straight line through the curve would only intersect the curve in no more than three points. It was an efficient authenticated encryption scheme with a vast amount of possibilities which is proper for ad hoc wireless and mobile networks environment.

Mandal et al. [31] proposed an electronic payment system based on the authenticated key exchange protocol. An active owner tracing mechanism was introduced to identify malicious customers where participants can mutually authenticate each other. The security of the scheme was based on the hardness assumption of computational Diffie–Hellman and discrete logarithm problems. The security scheme was simulated in the automated validation of Internet security protocols and applications tool and proved that the scheme was secured against replay and man-in-the-middle attacks.

Wang et al. [56] presented another mobile payment security scheme, evaluating the threats and challenges. The study categorized mobile payment into five including payment at POS, mobile payment as the POS, mobile payment platform, independent mobile payment system and direct carrier billing. The work proposed a mobile payment processing model and summarized the security services desired on mobile payment systems. Security issues identified were SSL/TLS vulnerabilities and data breaches with four security challenges like malware detection, multi-factor authentication, data breach prevention and fraud detection prevention in mobile payment systems. The study suggested that mobile users and service providers both need to take measures to avoid data breaches and payment risk.

In 2017, Mohit et al. designed a secure and efficient electronic payment system for mobile users using RSA concept. Though the study had better security performance, however, it was only linked to the merchant website, which was also subject to malicious file execution and cross-site scripting. The risk to an organization and the flaws of RSA remains. Besides, there was no direct communication between the user and merchant as well as acquiring and the issuing banks ([22, 25, 43, 53]). Yang, in 2017, proposed an electronic transaction mechanism using mobile devices for cloud computing. The mechanism used the exclusive-OR (XOR) operation and one-way hash function to reduce the computation cost. The study does not require a pre-shared key between the client and the vendor for authentication. Thus, the mechanism has less communication cost compared with the previous research works, and the mechanism was more efficient and suitable for electronic transactions using mobile devices in cloud computing.

A lightweight elliptic curve cryptosystem was also proposed for smart grid communication. The smart grid enables appropriate adjustments in the amount of electricity generation by providing the capability to monitor the consumption

behavior of customers. Different devices communicate with each other to exchange information; the devices must be authenticated to ensure secure communication with legitimate entities. The scheme was designed to authenticate such communicating devices using a lightweight authentication protocol that makes use of elliptic curve cryptography. In the protocol, each participant has to register itself with the Trusted Third Party. Then, each registered participant can initiate an authentication process with another participant to initiate a secure session of communication after successful authentication [29].

Why ECC over Binary Field?

Elliptic curve cryptography (ECC) is a public-key cryptographic method introduced by Koblittz in 1987 [27]. ECC is used to provide a key exchange, encryption and digital signature, based on the difficulty of an underlying mathematical problem such as the discrete logarithm problem (DLP) in a group defined by points on an elliptic curve over a finite field [11]. ECC remains the strongest public-key cryptosystem known with an addition rule enabling encryption and decryption [1, 51]. It uses a small key size, and it is a replacement to Rivest, Shamir, Adleman (RSA) protocols [3]

The elliptic curve cryptography is performed over two finite fields: (1) Prime field (F_p) and (2) Binary field $F(2^m)$. The field is chosen with a finitely large number of points suited for cryptographic operations [50]. Both fields are considered to provide a similar level of security [27], but the arithmetic of the binary field $F(2^m)$ is quite simple [38, 45]. The primary distinguishing factors between ECC prime and binary fields are the bit-fiddling operation and simplicity in the arithmetic of the binary field, while the prime field requires more logic gates [4, 13, 14]. For instance, the elliptic curve equation over prime field (F_p) is

$$y^2 = x^3 + ax^2 + b, \tag{1}$$

where $4x^3 + 27b^2 \neq 0$ and the element of the finite prime field are integers between 0 and $p-1$. All the operations such as addition, subtraction, division and multiplication involve integer between 0 and $p-1$. The prime number p is chosen such that there are a finitely large number of points on the elliptic curve to secure the cryptosystem [47].

On the other hand, the elements of the finite binary field are integers of length with at most m bits. The numbers are considered as a binary polynomial of degree $(m-1)$. In binary polynomial, the coefficients can only be 0 or 1. Over the years, ECC over prime field has been exhaustively used and the computer itself works on the binary number operation. Thus, the need to explore the functionality of the binary field.

Background to ECC Over Binary Field $F(2^m)$

An elliptic curve E over binary field $F(2^m)$ is a set of points $p = (x, y) \in E$. $F(2^m)$ satisfying

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

where $b \neq 0$, x and y are variables, a and b are constants. Equation (2) is a non-supersingular curve, and the elements of the finite field are integers of length with at most m bits [52]. These numbers can be considered as a binary polynomial of degree $(m-1)$. In binary polynomial, the coefficients can only be 0 or 1. All the operation such as addition, subtraction, division, multiplication involves polynomials of degree $m-1$ or lesser. The m is a positive integer chosen such that there is a finitely large number of points on the elliptic curve to making the cryptosystem secure.

In this study, a binary method for point multiplication is used to compute $Q = kP$, where integer k is represented as

$$k = k_{n-1}2^{n-1} + k_{n-2}2^{n-2} + \cdots + k_1 + k_0. \tag{3}$$

In Eq. (3), $k_i \epsilon\, 0, 1$ and $n = 0, 1, 2, \ldots, n-1$. Thus,

$$k = \sum k_i 2^j \tag{4}$$

is a binary method, which scans the bits of k either from left-to-right or right-to-left. The cost of multiplication depends on the length of the binary representation of k and the number of 1s in the representation. If the representation $(k_{n-1}, \ldots, k_1, k_0)_2$ has k_{n-1} number of 0s, then the number of doubling operations is $(n-1)$ and the number of addition operation is one less than the number of nonzero digits in $(k_{n-1}, \ldots, k_1, k_0)_2$. The number of nonzero digits is called the Hamming weight of scalar representation. In the average, binary method requires $n-1$ doubling and $\frac{n-1}{2}$ additions. For instance, when the bit is 1, two elliptic curve arithmetic operations such as elliptic curve doubling (ECDBL) and elliptic curve addition (ECADD) are made, and if it is 0, only one operation, ECDBL is required. So, the number of 1s is reduced in this study in the scalar representation to speed up the computation.

The domain parameters for the proposed elliptic curve over $F(2^m)$ are predefined constants $(m, f(x), a, b, G, n, h)$ [48]. The parameters are explained as follows:

1. m is a positive integer defined for the finite field $F(2^m)$ and the element of $F(2^m)$ are integers of length m bits;
2. $f(x)$ is an irreducible polynomial of degree m used for elliptic curve operation;
3. a and b are constant parameters defining the curve $y^2 + xy = x^3 + ax^2 + b$ while x and y are variable points;

4. G is the point generator. It is given as g_x, g_y or $G(x_G, y_G)$, a point on the elliptic curve chosen for cryptographic operations;
5. n is the order of the elliptic curve also called range of finite field. The scalar for point multiplication is chosen as a number between 0 and $n - 1$;
6. h is the cofactor, where

$$h = \frac{\#EF(2^m)}{n} \tag{5}$$

7. $\#EF(2^m)$ represents the number of points on an elliptic curve.

The Proposed Identity-Based ECC for Mobile Payment Security

This study presents a mobile payment technology that uses mobile devices for payment transaction communications between customers and merchants. The technology establishes a connection between the mobile phone and a terminal. Payment data are sent, using close-proximity radio frequency identification, from the phone to the card reader and, once the customer has validated his identity, transaction is allowed.

The Secure Mobile Payment Architecture

The mobile phone has an identity number called International Mobile Equipment Identity (IMEI).

The IMEI number of the mobile is unique and is used only for identification of the device over the wireless network, and subscriber has only semi-permanent relation to the IMEI number [28]. The proposed scheme uses the following elements to establish security:

1. Username and password: this is used for every user registration on the payment gateway through the mobile phone to create a user account;
2. Subscriber Identity Module (SIM) card: the SIM card number for every individual is unique;
3. The phone IMEI is registered on the payment gateway during user's registration to generate mobile PIN;
4. The generated or paired key is computed by the ECC algorithm over the binary field;
5. The mobile PIN is also generated for login through the payment gateway.

The ECC domain parameters are mapped to some points on the elliptic curve. The elliptic curve over the binary field is used for its computation as implemented on the payment gateway. Figure 1 describes the relationship between all entities involved in the mobile payment transaction from the user to the merchant. The arrows show the communication pathway as numbered. The entities interact with each other through the payment gateway over a wireless network. The issuing bank and acquiring bank also communicate with the payment gateway and interact with each other over the virtual private network of the banks.

Figure 1 presents the mobile payment model. The proposed scheme consists of five entities: User (U), Merchant (M), Payment Gateway (PG), Issuer (I) and Acquirer (A). The user makes use of the Subscriber Identity/Identification Module (SIM) and the mobile phone, which initiates requests through USSD code on the phone or open an application on a mobile phone to make payment to the merchant. The first step is to register on the payment gateway to obtain

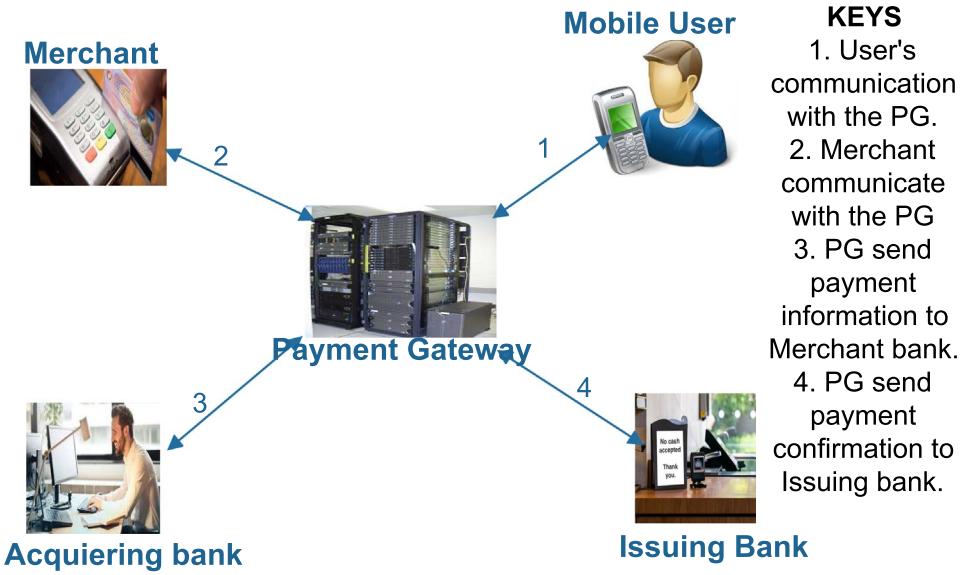

Fig. 1 The proposed architecture for mobile payment security

valid credentials needed for the transaction. The user is identified through the subscriber's identity module (SIM), plus the phone International Mobile Equipment Identity (IMEI) number on a mobile operator network. The user provides a username and mobile PIN to log in. The password strength is at least eight (8) digits, the first four letters must be numeric which is the first four digits of the mobile phone number from a network operator excluding the network code with dollar sign ($) and last three digits of the IMEI number to provide non-repudiation and improve password strength. A mobile Personal Identification Number (PIN) is generated during user registration using IMEI on the payment gateway and is available at every login. The merchant receives a request to make the payment from the user through the payment gateway. The merchant is also a registered party on the payment gateway. Algorithms 1 and 2 provide the ECC F_2^m for mobile payment encryption and decryption, respectively.

ALGORITHM 1: The ECC F_2^m Encryption for Mobile Payment

INPUT : *Plaintext* m
OUTPUT:*Ciphertext* C_1, C_2

1 $for\ char \in m\ do$ and char $\longleftarrow$ binary ASCII char (char)
2 $char \longleftarrow$ padding (char); $append\ (M, char)$
3 $end\ for$
4 $blocklength \longleftarrow \frac{N}{7}$
5 $M \longleftarrow$Block $(M, blocklength)$
6 $k \longleftarrow Random$ ([1, n-1])
7 $C_1(x_1, y_1) \longleftarrow$kP
8 $C_1(x_1, y_1) \longleftarrow$M + kQ
9 $for\ char \in M\ do$
10 $cipher \longleftarrow char\ x^2$
11 $append\ (B_2, cipher)$
12 $end\ for$
11 $retund\ (C_1(x_1, y_1), B_2)$

ALGORITHM 2: The ECC F_2^m Decryption for Mobile Payment

INPUT : $(C_1(x_1, y_1), B_2)$
OUTPUT:*Plaintext* m

1 $C_2(x_2, y_2) \longleftarrow mC_1$
2 $for\ cipher \in B_2\ do$
3 $char \longleftarrow \frac{cipher}{x^2}$
4 $char \longleftarrow padding(char)$
5 $append(m, char)$
6 $end\ for$
7 $m \longleftarrow split(m)$
8 $for\ char \in m\ do$
9 $char \longleftarrow DeASCII(char)$
10 $append\ (m, char)$
11 $end\ for$
12 $retund\ m$

The payment gateway is used in the payment transaction as an intermediary between the banks and merchants. At the payment gateway, authentication and clearing are done. The encryption and decryption keys are generated. The payment gateway requests for the generated key are used for encryption on mobile phone user and decryption from merchant's end.

The user logs in and initiates a request to make payment to the merchant by dialing a USSD code, through the merchant's website. The merchant receives a request to make payment through the payment gateway. The payment gateway notifies the issuer and the acquirer of the transaction and performs key generation and pairing between the user and the merchant. The user's payment details, which include the bank name, account number, amount, etc. with encryption key generated by the payment gateway, are sent to the merchant through the payment gateway. In Algorithm 1, the payment gateway converts the message to binary codes, while it is encrypted and sent to the merchant.

In Algorithm 2, the merchant receives notification for payment, login and enters decryption key to decrypt the message to confirm payment. The confirmatory message is forwarded to the user. The connections between all entities (User, Issuer, Merchant, Payment gateway and Acquirer) are established through general packet radio service (GPRS) [18].

The Mobile Payment Procedure Using Identity-Based ECC Over Binary Field

A typical mobile phone has a unique identity number. The International Mobile Equipment Identity (IMEI) number is used by the wireless network operator, GSM network, to identify valid devices over the network and to stop the continued use of the phone from accessing network if IMEI number is put on the blacklist by the network operator. In this paper, seven (7) phases were identified for the proposed mobile payment security. These are:

Registration Phase It is required for users and merchants to register on the payment gateway to obtain valid credentials like a mobile PIN for login and to generate the encryption key.

Transaction Phase The user initiates a request to make a payment and any transaction with the merchant through the payment gateway, and the merchant will have to confirm payment information and the details of the user.

Table 1 Key generation and pairing between user and merchant

User (U)	Payment gateway	Merchant (M)
Private key β	$y^2 + xy = x^3 + ax^2 + b$	Private key α
$1 \leq \beta \leq n-1$	m	$1 \leq \alpha \leq n-1$
Compute	a	Compute
$U_{(ID)} = \beta\, G(x_G, y_G)$	b	$M_{(ID)} = \alpha\, G(x_G, y_G)$
Receive	G	Receive
$M_{(ID)} = (x_{M_{ID}}, y_{M_{ID}})$	n	$U_{ID} = (x_{U_{ID}}, y_{U_{ID}})$
Compute	h	Compute
$P = \beta\, \alpha$ G	$U_{ID}, M_{ID}\, \sharp E(F2^m)$	$P = \alpha\, \beta\, G$

Payment Authorization Phase This is implemented on the payment gateway through the Issuer and the Acquirer to validate payment credentials and authorize the payment through the confirmation from the merchant module.

Payment Confirmation Payment is confirmed from the merchant through the payment gateway to the user, so non-repudiation is established.

Key Generation and Pairing Phase In the key generation phase, an appropriate elliptic curve and the corresponding elliptic curve parameters are chosen to generate the elliptic curve points. The user selects private key $n_A\, \epsilon\, [1, n-1]$, where n_A represents the key for the user, which is used to calculate public key $Q_(A = n_A G)$. The merchant select a private key $n_B\, \epsilon\, [1, n-1]$ and calculates public key $Q_{B=n_B G}$. Table 1 describes what happens in the key generation and pairing between the user and Merchant, while Algorithm 3 presents the section of key generation.

ALGORITHM 3: ECC F_2M Key Generation

INPUT : $F_2M Domain\ parameters : (m, p, n)$
OUTPUT:$Public\ Key\ Q\ and\ Private\ key\ d$
1 $Select\ d \in \Re[1, n-1]$
2 $compute$ Q = dP
3 $return$ (Q,D)

In point multiplication, a point P on the elliptic curve is multiplied with a scalar k to obtain another point Q on the elliptic curve, that is, $k = P = Q$. Point multiplication is achieved by two basic operations: point addition and point doubling. Algorithm 4 is a description of the binary method for point multiplication.

ALGORITHM 4: Binary Method for Point Multiplication

INPUT : $k = (k_{(n-1)}, ..., k_1, k_0)_2$
OUTPUT: kP
$R \longleftarrow P$
$for\ i = n-2\ to\ 0\ do$
$R \longleftarrow 2R\ (doubling)$
$if\ k_i = 1, then,\ \mathrm{R} = \mathrm{R} + \mathrm{P}\ (addition)$
$i \longleftarrow i-1$
$end\ if$
$retund\ R$
$end\ for$

Now, we have the key exchange between the user and merchant as Q_A and Q_B while the shared key computation is $k_A = n_A Q_B$ and $k_B = n_B Q_A$. $k = n_A Q_B = n_A n_B p = n_B Q_A$.

Encryption and Decryption The user input a plaintext m, the plaintext to be encrypted is then converted to binary M. It then calculates the pair of points for encryption and decryption as

$$C_1 = k * G, C_2 = p + k * Q_B \tag{6}$$

In this case, $C_1 = kp$ while $C_2 = M + kp$. In the decryption process, blocks of the ciphertext are firstly decrypted while ensuring that the length of each block of the decrypted ciphertext is divisible by 7; seven bits was used in this case. This is made visible with a padding process. Each block is broken into sub-blocks of length 7, and the sub-blocks are converted into the original character of the plaintext.

Message representation of a point The ECC cryptosystem deals with the point, which lies within the defined elliptic curve to performing its operation like key generation, encryption and decryption of text. The plain text inputs are mapped to elliptic curve points during encryption. The points are randomly generated on the curve using the ASCII value of the plaintext.

Implementation of ECC $F(2^m)$ Point Multiplication on Payment Gateway

The study uses Elliptic Curve Integrated Encryption Scheme (ECIES) over the binary field as defined in SECG SEC2, ANSI X9.62. The curves chosen are presented in Table 2, as recommended by NIST and Federal Information Processing Standard (FIPS) 186-2 [30].

The study considers a case where the user selects a request to make payment and enter transaction details on the payment gateway. The issuing bank is notified by the payment gateway with a request to debit or credit the user's account. The merchant receives a request for payment, and the acquiring bank is also notified of the transaction in progress. The confirmatory message is forwarded to the user to complete the transaction.

On the other hand, the merchant login to the payment gateway to decrypt the message and confirm payment. The merchant then decrypts the ciphertext to plaintext. A confirmation message is forwarded to the user through the payment gateway from the merchant before closing the session.

Now, the number of points chosen to secure the cryptosystem is large and represented as $\#E(F(2^m)$. The E is the point generator used for successive addition and point doubling during key pairing. The scalar for point multiplication is chosen as a number between 0 and $n-1$, for n is the range of finite field. The plain text input is mapped to the elliptic curve point during encryption. The point is randomly generated on the curve using the ASCII value of the plain text.

Evaluation

The performance of the proposed ECC over the binary field for mobile payment is evaluated and compared with RSA in

Table 2 Elliptic curves over F_2^m in SunEC

SECG SEC 2	NIST FIPS 186-2
sect163k1	NIST K-163
sect163r2	NIST B-163
sect233k1	NIST K-233
sect233r1	NIST B-233
sect239k1	NIST K-239
sect283k1	NIST K-283
sect283r1	NIST B-283
sect409k1	NIST K-409
sect409r1	NIST B-409
sect571k1	NIST K-571
sect571r1	NIST B-571

terms of key size, security strength, computational power, memory capacity, encryption and decryption time and mobile phone battery. The secret sharing schemes, pycryptodome and Tkinter, were used. The sharing schemes manage key agreement, encryption, decryption, key generation and authentication.

Computational Power

The study computed a comparative performance analysis with RSA for the mobile transaction using the same PINs. Response time of ECC and RSA for every transaction was recorded. It was observed that ECC-163 provides the same security as RSA-1024. Similarly, in Table 3, ECC-233 and ECC-283 provided the same security with RSA-1536 and RSA-3072, respectively. The result shows that ECC provides an efficient computational speed compared to RSA. Hence, its design in securing mobile payment system proves to be a reliable scheme due to its efficiency. Table 3 shows that the use of ECC allows the server to handle a large number of requests than RSA.

Encryption and Decryption

The encryption and decryption are observed for the different keys. The speedup of the execution time of ECC and RSA encryption and decryption was computed. Table 4 shows the result of ECC and RSA encryption and decryption. It is cleared that ECC, $F(2^m)$ encryption and decryption times are lower than RSA. Besides, RSA decryption is exponentially high in terms of computational cost. Thus, ECC, $F(2^m)$ performs better in terms of speed. In Table 5, ECC over finite

Table 3 Performance of ECC and RSA

	RSA-1024	ECC-163	RSA-1536	ECC-233	RSA-2048	ECC-283
Time (ms)	9.79	3.67	22.24	2.63	61.62	6.08
Perform. ratio	1	2.60	1	8.50	1	10.10
Key-size ratio	6.40	1	8	1	9.14	1
Speedup	1	17.5	1	30.1	1	48.7

Table 4 Computational time between ECC $F(2^m)$ and RSA

Key size	$F(2^m)$-E (ms)	$F(2^m)$-D (ms)	Total (ms)	Key size	RSA-E (ms)	RSA-D (ms)	Total (ms)
163	0.30	1.23	1.53	1024	0.46	8.60	9.06
239	0.35	1.32	1.67	1536	0.63	11.83	12.46
283	0.42	1.57	1.99	3072	0.85	15.89	16.84
409	0.52	2.09	2.61	7680	1.29	24.39	25.68
571	0.53	2.23	2.76	15,360	3.39	64.41	67.80

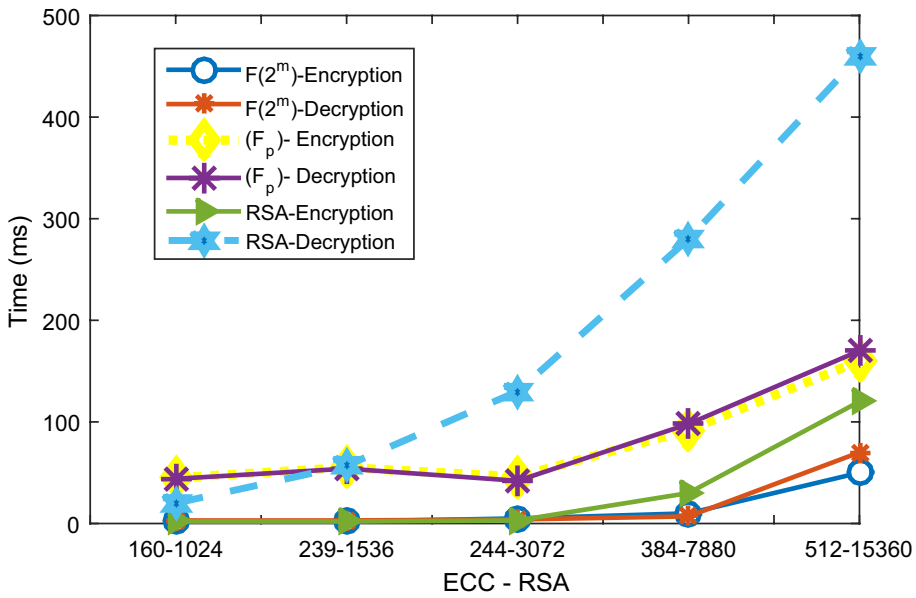

Fig. 2 Response time for ECC ($F2^m$) and RSA

Table 5 Computational time between ECC (F_p) and RSA

Key size	ECC (F_p)-E (ms)	ECC (F_p)-D (ms)	Total (ms)	Key (ms)	RSA-E (ms)	RSA-D (ms)	Total (ms)
160	2.65	1.31	3.96	1024	0.46	8.60	9.06
192	3.18	1.57	4.75	1536	0.63	11.83	12.46
224	3.71	1.83	5.54	2048	0.76	13.58	14.34
256	4.24	2.09	6.33	3072	0.85	15.89	16.84
384	6.37	3.14	9.51	7680	1.29	24.39	25.68
521	6.64	4.25	12.89	15,360	3.39	64.41	67.80

field was compared with RSA and it was observed that the finite field performs better the RSA. Figure 2 also shows the analysis of the encryption and decryption of the schemes, comparing ECC over finite field (F_p), $F(2^m)$, and RSA. $F(2^m)$ also performs better than (F_p) and RSA.

Discussion

The most benefiting factor of ECC over RSA is that ECC uses point addition and point multiplication as basic operations. These operations are known to be computationally expensive. As a result, it is unlikely that a sub-exponential attack on ECC will be discovered soon. Though, some claims of attacks still exist over some curves; the curves are identified and not recommended for use. The existing attacks are based on similar discrete logarithm problems that use complex point addition, which turns out to be much slower.

RSA exponentiation includes a sequence of modular multiplication which has a known sub-exponential attack working generally. To have the same security level with ECC for the same computational power, the number of bits required in the RSA generated key pair will rise much faster than in the generated key pair on ECC. ECC key generation is faster than the corresponding RSA with the same key length (see Fig. 2).

Encryption and decryption for any message represent a function of the key size and data size in either ECC or RSA. Encrypted message in ECC keys is smaller and with less computational cost. Therefore, the faster computation of ECC catered for the computational stress imposed on the payment gateway or server. To effectively determine the performance of the mobile payment system, the speed of operation and the response rate to service requests were examined. The use of ECC in data security for mobile payment reveals that sensitive customer's information and personal data over the Internet are very crucial, where speed is also a concern. Replacing the traditional RSA public-key cryptosystem with ECC, the speed of mobile transactions has increased. The significant benefit of ECC over the binary field is the bit-fiddling operation and arithmetic simplicity, while the prime field requires more logic gates. The binary field, thus, allows for efficient modulation reduction.

The ECC uses a small storage capacity, which makes it appropriate for mobile phones usage with a little amount of memory [10]. The binary ECC requires lesser storage space because it uses the binary representation of the ASCII code of each character in plaintext. The domain parameters are computed for the binary field ECC; it then maps it to some points on the elliptic curve. The hamming weight is reduced by lowering the number of 1s. Only point addition and point doubling are used, no inverse operation and subtraction in order to reduce storage space.

The primary concern for today's smartphones is the rate of battery life consumption. The difference is mainly reflected by the phones' capacity, which have devices with much more power-consuming smartphone components, such as the multi-core application processor. The application processor must be active when any smart applications are being used. The battery capacity of mobile phones has been improved by manufacturers to last longer and to improve the efficiency of mobile phones. This scheme examines an average battery life of a mobile phone running mobile application when fully charged. The battery consumption is 3%, which is very lower in comparison with the security effect.

Table 6 Security comparison with other models

Security issues	Isaac and Zeadally [17]	Yang and Lin [61]	Mohit et al. [34]	Proposed
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Non-repudiation	No	Yes	Yes	Yes
Anonymity	No	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes
Insider attack	Yes	Yes	Yes	Yes
Impersonation attack	No	No	Yes	Yes
Identity fraud	No	No	No	Yes
Device recovery	No	No	No	Yes
Shoulder surfing	No	No	No	Yes

Table 7 Differences between prime field and the proposed binary field

S/N	Prime field ECC	The proposed binary field
1	Requires more cycle to perform operations [6, 39]	Requires less cycle to perform operations [6, 16]
2	Slower Multiplication [6]	Faster multiplication [6, 58]
3	Higher power consumption [36]	Lower power consumption [7, 36]
4	Cannot be implemented directly on the mobile phone [23, 54]	Can be implemented directly on the mobile phone.
5	Prime field processors are usually slower than binary field processors [15, 32]	Binary field processors are usually faster than prime field processors [32]

The proposed model was compared with others in the literature. Table 6 shows the result of the analysis, which describes the strength of scheme against others. In Table 6, A "Yes" indicates agreement that the scheme can combat against such attack while "NO" shows a weakness in fighting the attack. The security issues presented in Table 6 are discussed in relation to the proposed model as follows.

1. Confidentiality: All information are stored on the payment gateway, and no entity will have access to it. It is therefore a confidential information that is not available to neither the merchant nor customer. Everyone is entitled to information and transaction details necessary for use during transaction [42].
2. Integrity: the integrity of this model is confirmed following the registration of all entities on the payment gateway, and there is assurance that a participant is whom it is claimed to be and transaction data can be prevented from modification [59].
3. Non-repudiation: the use of IMEI had ensured that no entity can deny its transaction. The possibility that a user can deny the transaction is conquered as every transaction can be traced to the mobile device used to perform it, and the payment gateway can also send a feedback to the user that the merchant received payment.
4. Anonymity: That there is no physical contact between participating entities and that only payment gateway has a record to trace and identify an entity for this scheme provided anonymity [35].
5. Replay attack: After every transaction, the session is closed. This will ensure that there cannot be any other transaction except another connection is established.
6. Insider attack: There is no internal user at any point on this scheme. All communication with both entities take place via the payment gateway, and bank communication is done over a virtual private network under the tracking and authority of the payment gateway. This will control insider posing an attack [9].
7. Impersonation attack: All entities are registered on the payment gateway, and this is the first step for identification. There will be no two users with same phone number or same IMEI. Therefore, the issue of impersonation is under control [24].
8. Identity fraud: The identity of all entities must be taken and stored on the payment gateway. At this point, they are traceable and unique to everyone. To change a phone IMEI, the phone number and other personal details will not change for same user [46].
9. Device recovery: Stolen devices can be recovered on a mobile operator network by blacklisting and tracking a mobile device using its IMEI. When the IMEI or phone number is restored, the account can be recovered without any change to personal details.
10. Shoulder surfing: The problem of password is shoulder surfing. This study conquers that by concatenating on the mobile phone number and the IMEI.

The proposed model therefore shows that the security issues stated in Table 6 can be totally controlled.

An analysis of ECC prime and binary fields strength was done. Table 7 shows a clear comparison of security strength and weaknesses of both schemes. The analysis shows that binary curves are smaller and faster than prime field ECC. This is because binary fields have a shorter formula. The binary operations have no carry element, and squaring is less computationally expensive. The binary-based processors outperform the prime processors when performing point multiplication [58]. For instance, Tables 6 and 7 show that the proposed binary field outperforms the prime field.

Conclusion

Mobile payment has improved e-commerce, making life convenient for mobile users. However, the security of transactions and users' information is a great concern. The paper has presented an improved scheme to mobile payment system using elliptic curve cryptography over binary field. This paper focused on mobile payment transactions and the security of users' information during transactions over the Internet. The use of IMEI with ECC provides integrity,

non-repudiation and protection against identity theft for the mobile users. The ECC over binary field is used for key generation, encryption and decryption to ensure authenticity. The payment details are protected and stored on the payment gateway to achieving confidentiality and anonymity. This scheme protects users against other known attacks such as man-in-the-middle attack, impersonation attack.

The result obtained has proven that the time taken to perform transaction operations was lower with the proposed $F(2^m)$ and compared to the RSA. Thus, it was observed that the scheme is time-efficient in a resource-constrained environment such as e-payment. The computational power of the proposed scheme is efficient for low resource mobile devices in terms of battery life, memory space and processor speed.

This suggests the superiority of ECC as compared to other public-key cryptography schemes, since it does not only offer a higher level of security when the underlying parameters are chosen correctly but also offer more significant advantages due to its shorter key sizes, faster generation of encryption and decryption keys, smaller space requirements and efficient implementation techniques.

However, the limitation of this work is that the mobile phone data are not encrypted directly on the mobile phone but, on the payment gateway.

Acknowledgements We thank the reviewers for their constructive comments and suggestions that helped to improve on the quality of the paper.

References

1. Abdurahmonov T, Yeoh ET, Hussain HM. Improving smart card security using elliptic curve cryptography over prime field (f p). In: Software engineering, artificial intelligence, networking and parallel/distributed computing. Springer; 2011. p 127–40.
2. Ahsan I, Nadeem H. A mobile payment model using biometric technology. Int J Adv Sci Eng Technol. 2016;4(4):12–24.
3. Alkhateeb EM, Alia MA, Hnaif AA. The generalised secured mobile payment system based on ECIES and ECDSA. In: ICIT 2015 The 7th international conference on information technology, vol 10; 2015.
4. Anoop MS. Elliptic curve cryptography, an implementation guide. online Implementation Tutorial, Tata Elxsi, India; 2007.
5. Antovski L, Gusev M. M-payments. In: Proceedings of the 25th international conference on information technology interfaces, 2003. ITI 2003. IEEE; 2003. p. 95–100.
6. Bapat AC, Nimbhorkar SU. Multilevel secure RFID based object tracking system. Procedia Comput Sci. 2016;78:336–41.
7. Brocanelli M, Wang X. Making smartphone smart on demand for longer battery life. In: 2017 IEEE 37th international conference on distributed computing systems (ICDCS). IEEE; 2017. p. 2288–2293.
8. Chaudhry SA, Farash MS, Naqvi H, Sher M. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electron Commer Res. 2016;16(1):113–39.
9. Das SK, Kant K, Zhang N. Handbook on securing cyber-physical critical infrastructure. Amsterdam: Elsevier; 2012.
10. Dawahdeh ZE, Yaakob SN, Sagheer AM. Modified elgamal elliptic curve cryptosystem using hexadecimal representation. Indian J Sci Technol. 2015;8(15):64749.
11. Gajbhiye S, Karmakar S, Sharma M, Sharma S, Kowar MK. Application of elliptic curve method in cryptography: a literature review. Int J Comput Sci Inf Technol. 2012;3:4499–503.
12. Hamburg M. Compression and encryption approach for data security in mobile internet of things. Int J Adv Res Comput Eng Technol. 2017;6(1):39–42.
13. Hankerson D, Hernandez J, Menezes A. Software implementation of elliptic curve cryptography over binary fields. In: International workshop on cryptographic hardware and embedded systems. Springer; 2000. p. 1–24.
14. Hankerson D, Menezes AJ, Vanstone S. Guide to elliptic curve cryptography. Berlin: Springer; 2006.
15. Hutter M, Wenger E. Fast multi-precision multiplication for public-key cryptography on embedded microprocessors. J Cryptol. 2018;31(4):1164–82.
16. Imran M, Rashid M, Jafri AR, Najam-ulIslam M. Acryp-proc: flexible asymmetric crypto processor for pointmultiplication. IEEE Access. 2018;6:22778–93.
17. Isaac JT, Zeadally S. An anonymous securepayment protocol in a payment gateway centric model. Procedia Comput Sci. 2012;10:758–65.
18. Isaac JT, Zeadally S. Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model. Computing. 2014;96(7):587–611.
19. Isaac JT, Zeadally S, Cámara JS. A lightweight secure mobile payment protocol for vehicular ad-hoc networks (VANETs). Electron Commer Res. 2012;12(1):97–123.
20. Islam SKH, Amin R, Biswas GP, Obaidat MS, Khurram Khan M. Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system. Arab J Sci Eng. 2016;41(8):3163–76.
21. Javan SL, Bafghi AG. An anonymous mobile payment protocol based on swpp. Electron Commer Res. 2014;14(4):635–60.
22. Jaiswal A, Raj G, Singh D. Security testing of web applications: issues and challenges. Int. J. Comput. Appl. 2014;88(3):180–90.
23. Javidan R, Pirbonyeh MA. A new security algorithm for electronic payment via mobile phones. In: 2010 3rd international symposium on applied sciences in biomedical and communication technologies (ISABEL). IEEE; 2010. p. 1–5.
24. Jiang J, Zheng Y, Shi Z, Yao J, Wang C, Gui X. Towards privacy-preserving user targeting. J Commun Inf Netw. 2016;1(4):22–32.
25. Kaur D, Kaur P. Empirical analysis of web attacks. Procedia Comput. Sci. 2016;78:298–306.
26. Kavitha K. Study on cloud computing model and its benefits, challenges. Int J Innov Res Comput Commun Eng. 2014;2(1):2423–31.
27. Koblitz N. Elliptic curve cryptosystems. Math. Comput. 1987;48(177):203–9.
28. Kumar K, Kaur P, Amritsar GNDU. Vulnerability detection of international mobile equipment identity number of smartphone and automated reporting of changed imei number. Int J Comput Sci Mob Comput. 2015;4(5):527–33.
29. Mahmood K, Chaudhry SA, Naqvi H, Kumari S, Li X, Sangaiah AK. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Gener Comput Syst. 2018;81:557–65.
30. Martinez VG, Hernandez Encinas L. Implementing ECC with java standard edition 7. Int J Comput Sci Artif Intell. 2013;3(4):134.
31. Mandal S, Mohanty S, Majhi B. Design of electronic payment system based on authenticated key exchange. Electron. Comm. Res. 2016;18(2):359–88.

32. Marzouqi H, Al-Qutayri M, Salah K. Review of elliptic curve cryptography processor designs. Microprocess Microsyst. 2015;39(2):97–112.
33. Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intrusion detection techniques in cloud. J Netw Comput Appl. 2013;36(1):42–57.
34. Mohit P, Amin R, Biswas GP. Design of secure and efficient electronic payment system for mobile users. In: International conference on mathematics and computing. Springer; 2017. p. 34–43.
35. Nia MA, Ruiz-Martínez A. Systematic literature review on the state of the art and future research work in anonymous communications systems. Comput Electr Eng. 2018;69:497–520.
36. Nimbhorkar S, Malik DL. Prospective utilization of elliptic curve cryptography for security enhancement. Int J Appl Innov Eng Manag. 2013;2(1)
37. Nseir S, Hirzallah N, Aqel M. A secure mobile payment system using QR code. In: *2013 5th international conference on computer science and information technology (CSIT)*. IEEE; 2013. p. 111–4.
38. Okediran TM, Vincent OR, Abayomi-Alli AA, Emmanuel JA. An enhanced mobile payment security scheme (EMPS) using ECC over binary field F(2m) and IMEI. Int J Inf Secur Priv Digit Forensics. 2018;2(1):70–7.
39. Oliveira T, López J, Cervantes-Vázquez D, Rodríguez-Henríquez F. Koblitz curves over quadratic fields. J Cryptol. 2019;32(3):867–94.
40. Owoh NP, Singh MM. Security analysis of mobile crowd sensing applications. Appl Comput Inform. 2018.
41. Olanrewaju T, Zavarsky P, Ruhl R, Lindskog D. Security modeling of mobile payment system architecture. J Comput Appl. 2013;58(16):1–9.
42. Piao C, Li X. Privacy preserving-based recommendation service model of mobile commerce and anonimity algorithm. In: 2015 IEEE 12th international conference on e-business engineering. IEEE; 2015. p. 420–7.
43. Preetha M, Nithya M. A study and performance analysis of RSA algorithm. IJCSMC. 2013;2:126–39.
44. Rahmani Z, Tahvildari A, Honarmand H, Yousefi H, Daghighi MS. Mobile banking and its benefits. Oman Chapter Arab J Bus Manag Rev. 2012;34(974):1–4.
45. Rebeiro C. Architecture explorations for elliptic curve cryptography on FPGAS. Ph.D. thesis, M. Sc. thesis. Department of Computer Science and Engineering, Indian, 2009
46. Rui Z, Yan Z. A survey on biometric authentication: toward secure and privacy-preserving identification. IEEE Access. 2018;7:5994–6009.
47. Sawlikar A. Point multiplication methods for elliptic curve cryptography. Int J Eng Innov Technol. 2012;1(1):1–4.
48. Shetty MN, Puranik T, Ghosalkar S, Jaybhaye S. Analysis of elliptic curve cryptography for mobile banking. Int J Eng Res Technol. 2015;3(7):233–43.
49. Sultan N. Cloud computing for education: a new dawn? Int J Inf Manag. 2010;30(2):109–16.
50. Suma AP, Shankar S, Puttamadappa C. Secure transmission of data in smart grid with the aid of elliptic curve cryptography method. Technology. 2016;7(1):50–63.
51. Susantio DR, Muchtadi-Alamsyah I. Implementation of elliptic curve cryptography in binary field. J Phys Conf Ser. 2016;710:012–22.
52. Sutter GD, Deschamps J-P, Imaña JL. Efficient elliptic curve point multiplication using digit-serial binary field operations. IEEE Trans Ind Electron. 2013;60(1):217–25.
53. Vijay A, Trikha P, Madhur K. A new variant of RSA digital signature. Int J Adv Res Comput Sci Softw Eng. 2012;2(10)
54. Vincent OR, Folorunso O, Akinde AD. Improving e-payment security using elliptic curve cryptosystem. Electron Commer Res. 2010;10(1):27–41.
55. Vincent OR, Lawal OM. A key agreement authentication protocol using an improved parallel pollard rho for electronic payment system. J Supercomput. 2018;74(5):1973–93.
56. Wang Y, Hahn C, Sutrave K. Mobile payment security, threats, and challenges. In: 2016 second international conference on mobile and secure services (MobiSecServ). IEEE; 2016. p. 1–5.
57. Wang Y, Vangury K, Nikolai J. Mobileguardian: a security policy enforcement framework for mobile devices. In: 2014 international conference on collaboration technologies and systems (CTS). IEEE; 2014. p. 197–202.
58. Wenger E, Hutter M. Exploring the design space of prime field vs. binary field ECC-hardware implementations. In: Nordic conference on secure IT systems. Springer; 2011. p. 256–271.
59. Xu K, Yan Z. Privacy protection in mobile recommender systems: a survey. In: International conference on security, privacy and anonymity in computation, communication and storage. Springer; 2016. p. 305–18.
60. Yang JH, Chang YF, Chen YH. An efficient authenticated encryption scheme based on ECC and its application for electronic payment. Inform. Technol. Control 2013;42(4):315–24.
61. Yang J-H, Lin P-Y. A mobile payment mechanism with anonymity for cloud computing. J Syst Softw. 2016;116:69–74.