


# Digital Signature Algorithm for M-Payment Applications Using Arithmetic Encoding and Factorization Algorithm

Shibin David, Karunya Institute of Technology and Sciences, Coimbatore, India

G. Jasper W. Kathrine, Karunya Institute of Technology and Sciences, Coimbatore, India

 <https://orcid.org/0000-0003-3055-0356>

## ABSTRACT

Mobile communication systems employ an encoding-encryption model to ensure secure data transmission over the network. This model encodes the data and encrypts it before transmitting it to the receiver's end. A non-trivial operation is performed to generate a strong secret key through which the data is encrypted. To support the security level of this model, arithmetic encoding is performed upon the data before encryption. The encrypted data is hashed using a lightweight hashing algorithm to generate a small and fixed length hash digest to overcome the overheads before it is communicated to the other end. To authorize the message being sent by the sender to the receiver, signature plays an important role. To avoid forging using proxy signature, blind signature, etc., a hybrid scheme is proposed in this article. The mobile communication system is enhanced by introducing the hybrid encode-encrypt-hashing mechanism which stands secure against the plain text attacks, mathematical attacks, and increases confidentiality of the data, security of the key, and thereby enhances the security of the system. In this paper, the design is applied over the mobile payment system which is considered as one of the appreciable mobile services. It proves that the designed security model can ensure swift transactions in a secure way.

## KEYWORDS

Arithmetic-Encoder, Digital Signature, Encoding, Factorization, Mathematical Attacks, Plain Text Attacks, Secret Key

## INTRODUCTION

The rapid development of e-commerce and wide-spread usage of mobile devices have emerged e-business using wireless technologies (Pasupuleti et al., 2016; Sukumaran & Mohammed, 2018; Tian et al., 2013). Despite of the pervasiveness of the wireless networks, there has been huge need for mobile services such as dynamic location based services, communication services and entertainments services (Arsalan et al., 2019; Kittur & Pais, 2017; Kundu et al., 2020; Oh et al., 2018). Amidst these services, the impact is high upon the mobile transaction services through the mobile communication systems such as mobile auctions, mobile payments, and mobile banking. Even though mobile devices

DOI: 10.4018/JCIT.20210701.oa2

This article, published as an Open Access article on April 23, 2021 in the gold Open Access journal, Journal of Cases on Information Technology (JCIT) (converted to gold Open Access January 1, 2021), is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

provide immediacy, convenience, user friendliness, personalization for consumer transactions, reliability was given more importance. It is considered as one of the prime factors in the wireless channels which are prone to attacks such as impersonisation, eaves dropping (Chou et al., 2010; Guo et al., 2011; Mihaljević & Oggier, 2010). The mobile communication system needs wireless channels to establish secure communication and perform any transactions (G. Rajesh et al, 2018). In this scenario, error correction and secure transmission needs concentration in wireless channels that can be achieved through coding algorithms and ciphering algorithms respectively (Ktari et al., 2017; Martiri & Baxhaku, 2012; Park & Ogunfunmi, 2017; You & Sang, 2010). Presently, GSM uses coding and ciphering for mobile communication systems. In GSM module, Error correction techniques should have been implemented at the receiver's end to withstand the errors whereas encryption to preserve the privacy of the user. The literature (Arsalan et al., 2019; Husni, 2017; Troja & Bakiras, 2017) says that such a secure mechanism was deployed in the mobile communication systems were not taken into consideration for mobile wallets.

The objective of the mobile wallet is to provide instant transactions with the help of mobile wallets in the mobile device. Contact commerce gives business chances to mobile system administrators similar to cloud suppliers. Touch commerce can be characterized as a rich portable innovation that climbs up bound together flexible assets of convenient advancements towards unhindered usefulness, stockpiling, and portability to serve a large number of mobile devices. Touch commerce utilizes the Internet to convey applications to mobile devices. These mobile applications can be utilized remotely with speed and adaptability with the Internet and advanced devices. It will give the fundamental dimension of computing service that is viewed as basic need to meet the ordinary needs of the general network.

Unfortunately, there are problems such as battery limit and, expanding request from clients for energy consuming applications in mobile wallets. The huge data flow has resulted in the enforcement of secure point to point associations between vendors, clients and communication in the network (Black, 1993; Hassinen et al., 2008; Ruiz-Martínez et al., 2011; Standard et al., 1976; Xue et al., 2018). In this regard, the identity of the client initiating the secure transaction using mobile applications has to be enhanced. Firstly, the transaction information needs to be sent safely to the vendor without allowing any disclosure in between. Secondly, the secrecy of the transactional information has to be maintained through an encryption algorithm. Thirdly, to protect the message being transmitted from the client to the vendor, digital signature (Black, 1993; Guo et al., 2011; Liao & Hsiao, 2013; Mihaljević & Oggier, 2010) is applied to prove the identity of the sender and also to ensure that the content is not modified during the transmission. The proposed work in the article concentrates on developing a security solution which is applicable to the mobile wallets in all the concerns discussed above. The objective of this work is to encode and sign the data digitally before transmitting it over the wireless channel through which communication takes place. This paper consists of four sections. Section 2 deals with the research background and literature on the needs for encoding and signature in the mobile transactions. Section 3 describes the proposed framework and the proposed algorithm to enhance the security in the mobile applications. Section 4 carries the proof of security for the proposed algorithm. Section 5 concludes the merits of the proposed work and introduces the scope of the future work.

## **RESEARCH BACKGROUND**

The common procedure of communication in the wireless networks involves encrypting the message first and then encoding the message to prove its errorless state. But, this practice had given loophole to be prone to plaintext attacks where a wireless tapper can be engaged to overhear, intercept the message being transmitted. On the other side, encryption of huge data may create redundancy in the transmitted messages and provide possible errors. Here, performing error correction coding of original message before encryption will ensure structured redundancy which can prevent attacks against the keys. The concern of the proposed approach is to enhance security in the system against theoretical

and cryptographic attacks. The idea of implementing the upgraded model in the mobile wallets is the core discussion in this article. From vendor's view, mobile commerce allows to expand their market and reduce the prices. Mobile network operator's concern is to provide maintenance and increase the revenue whereas financial service providers (FSP) use the opportunities as secure payment terminal which considers traditional economy.

## **Literature Review**

Mihaljević & Oggier (2010) have suggested the inclusion of strong encoding protocol to ensure the secure transmission of messages which are not prone to plain text attacks. They have analyzed the effects of the encoding system in the mobile applications and proved that the communication achieves confidentiality and security. Gao et al., (2009) has proposed a bar-code based payment system which adds flavor to the user experience in the mobile phone. It has also enhanced the security feature in mobile transactions for the purchase of goods anywhere and at any time. Heide et al (2009) have proposed random linear network coding technique for mobile devices. The aim of the scheme was to reduce energy consumption, computational cost and high throughput. They implemented the scheme using RLNC method along with binary GF to achieve the requirements.

Chang (2014) have proposed a security model for mobile payment system. The authors had focused on authorization through remote server and generating a 2D bar code which is considered as the certificate to lock remotely and disable unauthorized payment service. Husni (2017) has proposed dynamic rule encryption method to encrypt the message transmitted over the mobile device. Dynamic rules with varying token functions were used for authentication. To deliver the error free mechanism, hamming distance method was adopted in the scheme. Lizama-Perez (2019) has narrated about the digital signatures using hash chains. It enhances security and efficiency for the existing works by adding the hash functions.

Alidoost Nia et al., (2014) have discussed about the various digital signature schemes which includes batch scheme, forward-secure scheme, blind scheme and proxy scheme. Batch scheme provides increased efficiency which is helpful for signing synchronously and achieve large scale computations. Forward secure scheme achieves high security where the reverse process of the signed digest cannot be achieved. Blind scheme allows the sender of the message to get authorized signature from the signer whereas the signer will not know about the sender who sends the message. It is termed as anonymity service. Proxy scheme provides the privilege to a person authorized by the signer to sign the content. Walker & Pay, (2016) has discussed about the role of digital signatures in mobile banking and the methods of processing payments.

Mobile banking were found to be using e-signature technologies with the utilization of public key infrastructure based algorithms such as RSA algorithm, web browsers for verification purpose. DISIMOD, a digital signature scheme for the mobile devices were coined by Schoaba et al., (2010). The author has constructed the scheme to enhance security in transaction of the messages and in the mobile communications. This scheme used RSA algorithm along with the hash functions to improvise the security of the model. Qin et al., (2017) have suggested a privacy-preserving and outsourced mechanism for verification for m-payment systems. The mechanism had given a protocol related to certificate-less signature and server side verification. The security features have been incorporated with the addition of pseudo identity techniques and digital signatures.

## **Security Challenges Faced in Mobile Wallets**

The literature says that there will be an equal number of threats and opportunities for any evolving application in this scientific world (Heide et al., 2009; Hernandez-Ardieta et al., 2013). Some of the statistics say that almost 36% of mobile users in the US have started accessing their mobile devices for shopping online in the year 2011 (Chang, 2014; Hernandez-Ardieta et al., 2013). The volume of mobile payment has gone increasingly to 712 US dollars approximately in the year 2017 (Black,

1993; Yang et al., 2019). On the other hand, 86% of the people in Kenya have literally omitted the traditional banking system and are involved in only using mobile wallets for transactions.

Despite all the interest in the mobile apps amidst the users, there exist few legitimate challenges for these mobile applications (Chang, 2014; Husni, 2017; Turkes et al., 2016). The transactional information which is stored in the mobile apps remains as a constraint. Despite various mobile devices, mobile networks and operating system (OS) with which the device runs, there prevails one common payment method for all. The trust towards the use of mobile application among the users is very low and hence the adoption of the trending applications seems null (Black, 1993; Yang et al., 2019; Yu et al., 2018). Still, in many countries, technological advancements are poor such as poor internet connectivity, minimal infrastructure which leads to illiteracy amidst most of the people for usage of such novel technologies.

## Motivation

The mobile payment or mobile wallets can implement a system which can modify the usage of traditional encryption and coding techniques which may create security threats and attacks such as mathematical attacks, brute force attacks, plain text attacks, attacks against confidentiality and privacy.

## PROPOSED SYSTEM ARCHITECTURE

### Key Factors

- **Arithmetic encoding:** Arithmetic encoding is the process of converting the data from one form to another form. Integer encoding is a form of arithmetic encoding which is used here.
- **Factorization:** Integer factorization method is used to compute the prime factors of the integer. Here, pollard rho's factorization method is assumed to achieve easy computation, less time, small amount of space in the memory.
- **Hashing:** Hashing is defined as the transformation of data to any fixed sized output. Hash functions are applied over the input data to generate the message digest or hash digest. SHA algorithm is used here.
- **Digital Signature:** Digital Signature proves the identity of the sender which restricts the signer from repudiation. It provides authentication, authorization and non-repudiation.

### Proposed Framework

The proposed framework is designed to create a signature for the data communicated over a mobile network as depicted in Figure 1. The generation of signature involves the mechanism of encoding, factorization and hashing. It considers the public parameters ( $c$ ,  $d$ , and  $g$ ) where  $c$  is a composite number which is encoded using IEEE 754 encoding standard and factorized using a pollard rho's factorization algorithm to get the prime factor  $d$ . The input is hashed using the hashing algorithm SHA-1 to prove its integrity and generates the message digest. A random key generation algorithm is used to generate the random integer ' $n$ ' ( $0 < n < d$ ) which is used to create the signature. The private key of the signer  $Pr_a$  is computed at the sender's end. The public key of the sender is generated with the help of global public key and it is generated by the sender using the hash value ( $1 < h < c-1$ ) to sign the data being sent by the sender. The signature is created and appended along with the original message and transmitted to the receiver's end. At the receiver's end, the original message is decoded using IEEE 754 decoding standard and received safely. The identity of the signer is not disclosed at the receiver's end, but the signature is verified using the verifier's authority. The message is hashed back and used for comparison. The verifier verifies the signature along with the public key of the sender and the hash value. The flow of the signing and verifying process is sketched in Figure 2.

The proposed scheme uses digital signature to prove the authenticity of the signature signed by the signer to authorize the sender in the transaction. Initially, the message to be communicated is encoded

Figure 1. Proposed Framework

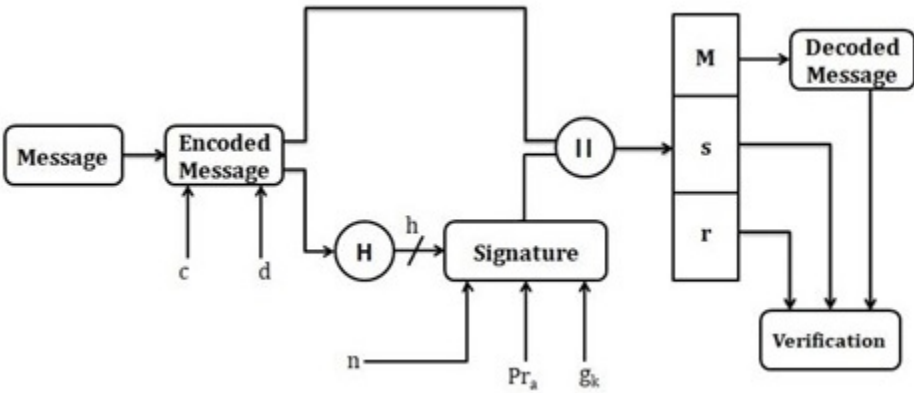
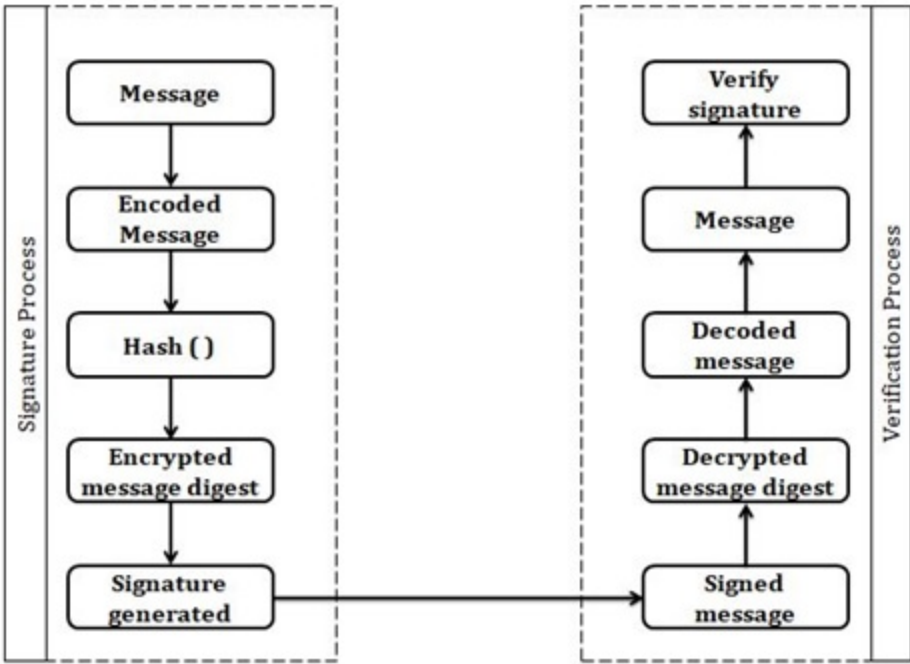


Figure 2. The flow of the signing and verifying process



by the sender to create confusion in the plain text for communication. The confused message is then applied over by the factorization methods, to mathematically create complexity into the plain text and considered for the encryption and signature process. Key generation algorithm is used to generate the keys for the sender to be involved in the signature generation process. To prove the integrity of the plain text, sender uses hash() function and create a message digest. With the help of the message digest, the signer generates a signature through the private key of the sender, global key created by the sender. The signed data is transmitted over the channel to the receiver's end. The signed message is decoded and hashed to verify the signature. The verifier verifies the signature been passed from the sender's side. This signature scheme enhances the authorization of the message transmitted in the

channel; authenticate the sender who sends the message. It also reduces time complexity, increases fast computation, and factorizes larger composite number.

## **Proposed Algorithm**

### ***IEEE-754 Encoding-Decoding Technique***

IEEE-754 is technique to compute floating point values. This will implement encoding and decoding of binary form of floating point numbers upon IEEE 754 standard. IEEE 754 technique for the floating point value comprises of three segments namely sign bit, the exponent and, the significant. The value can be computed using:

$$-1^{sign} x 2^{(exponent - bias)} x 1 \cdot significant$$

The IEEE 754 defines various binary formats of varying sizes that follows the criterion, but differs in the number of bits allocated for the exponent and significant. The bias for the regular formats is defined as  $\left(2^{(exponent\_bits - 1)} - 1\right)$ .

To perform encoding of floating point number using IEEE 754 standard:

$$Encode(l; exponent\_bits; significant\_bits; exponent\_bias)$$

Parameters used:

- l - The input value in the floating point format.
- Exponent\_bits - Number of bits in the exponent part.
- Significant\_bits - Number of bits in the significant part.
- Exponent\_bias - The exponent-bias to be used.

To calculate the value of an IEEE-754 binary float:

$$Decode(l; exponent\_bits; significant\_bits; exponent\_bias)$$

Parameters used:

- l - The floating point value to be decoded.
- exponent\_bits - Number of bits in the exponent part.
- significant\_bits - Number of bits in the significant part.
- exponent\_bias - The exponent-bias to be used.

Using the above said IEEE 754 encoding and decoding method, the chosen message 'm' is encoded from the sender side and decoded in the receiver side.

## **Pollard Rho's Factorization**

The pollard rho's factorization is a prime integer factorization algorithm. The metrics that are applied in this algorithm is given below:

1. When two integers a and b are said to be congruent to modulo r ( $a \equiv b \pmod r$ ) once their absolute value difference is a multiple of r, otherwise, both the values a and b produces the same remainder when divided by r.
2. Greatest Common Divisor (G.C.D) of the given values is the largest number that divides each of the given values.
3. The probability of two individuals having the same birthday is high for a smaller set of people is termed as birthday paradox.
4. When a tortoise and hare start moving in a cycle at some point provided the speed of tortoise is twice than the hare, then both the tortoise and hare will meet at some point. This algorithm is called as floyd's cycle finding algorithm.

Input: n, composite-integer

Output: non-trivial value or failure

1. Choose a smoothness-bound value 'S'
2. Consider  $M = \prod_{primes q \leq S} q^{\lfloor \log_q S \rfloor}$
3. Pick a Co-prime number to the value 'n'
4. Calculate  $g_{val} = \gcd(a^M - 1, n)$
5. if  $1 < g_{val} < n$  then return  $g_{val}$
6. When  $g_{val} = 1$ , choose a large S and go to 2<sup>nd</sup> step else return 'not possible'.
7. When  $g_{val} = n$ , choose a small S and go to 2<sup>nd</sup> step else return 'not possible'

When  $g_{val} = 1$  in 6<sup>th</sup> step, it indicates there are no prime factors p for which p-1 is S power-smooth.

When  $g_{val} = n$  in 7<sup>th</sup> step, this usually indicates that all factors were S power-smooth, but in rare cases it could indicate that it had a small order modulo n.

### Proposed Algorithm

The proposed algorithm possesses five phases which includes generation of parameters, key generation phase, key distribution phase, signature generation phase and verification phase.

Table 1 denotes the notations used in the proposed algorithm.

Table 1. Notations used in the proposed algorithm

Notation	Meaning
m	Message to be signed
$m_e$	Encoded message
c	Composite number
d	First prime divisor of c
h	Hash value ( $1 < h < c$ )
$Pr_a$	Private key of the sender $\{1 \dots \dots c-1\}$
$Pu_a$	Public key of the sender
$\mathcal{G}_k$	Global public key
n	Random integer $\{1 \dots \dots c-1\}$
$\alpha$	Signature of the message
$\beta$	Verification process

## Encoding-Encryption Phase

### Generation of Algorithm Parameters

1. Input message 'm' is encoded using IEEE 754 method and the encoded message is denoted as  $m_e$ .
2. Select the key length  $L$  (The length of the key can be 2048).
3. Choose an appropriate hash function  $H$  which produces the output length of  $|H|$  bits.
4. Choose the modulus length  $N$  such that  $N < L$  and  $N \leq |H|$ . FIPS has specified  $L$  and  $N$  should have one among the following combination such as (1024, 160), (2048, 224), (2048, 256), (3072, 256).
5. Choose an  $N$ -bit composite number 'c'.
6. Apply pollard rho's factorization technique and find the first factor of the chosen composite number denoted as 'd'.
7. Choose a random hash value 'h' where  $1 < h < c - 1$ .
8. Calculate the global public key using the hash value and public key parameters:

$$g_k = h^{c-1/d} \bmod c$$

The modular exponentiation can be computed for larger values.

The parameters of the algorithm (c, d, g) may be shared between various users of the communication system.

### Key Generation

A key pair is computed using the algorithmic parameters:

1. Choose a random integer  $Pr_a$  which lies between  $\{1 \dots d - 1\}$ .
2. Compute the public key of the user  $Pu_a = g_k^{Pr_a} \bmod c$ . ( $Pr_a$ ,  $Pu_a$ ) is the private and public key pair here.

### Key Distribution

The signer transmits the public key  $Pu_a$  to the receiver through a reliable channel whereas the private key  $Pr_a$  remains confidential with the sender.

### Generation of Signature

The message 'm' is signed as follows:

1. Choose a random integer 'n' which lies between 0 and d ( $0 < n < d - 1$ ).
2. Compute  $\alpha = (g_k^n \bmod c) \bmod d$ . If  $\alpha=0$ , repeat again with different 'n' value randomly.
3. Compute  $\rho = n^{-1} (H(m) + Pr_a \cdot \alpha) \bmod d$ . If  $\rho$  becomes 0, repeat again with different 'n' value randomly.

The signature is generated as  $(\alpha, \rho)$ .

### Verifying the Signature

The signature generated can be verified after decrypting the message digest and decoding it:

1. Verify  $0 < \alpha < d$  and  $0 < \rho < d$
2. Compute  $t = H(m) \rho^{-1} \bmod d$



3. Compute  $u = \alpha \rho^{-1} \bmod d$
4. Compute  $\beta = (g_k^t P u_a^u \bmod c) \bmod d$

The signature is valid if and only if  $\alpha = \beta$ .

The proposed digital signature algorithm can be used to improve authenticity and sends a reliable message to the receiver.

## RESULTS AND DISCUSSIONS

The proposed algorithm is implemented using java language under the MIRACL library which is efficient for cryptographic operations. Using the experimental results, we can compare the characteristics of DSA, EdDSA along with our proposed algorithm. The major phases of this algorithm include generation of keys, generation of signature and verification of signature. These phases are tested independently using implementation in java. Four tests have been conducted to compare the time taken by each of the algorithm considered for the experiments.

### Generation of Keys

The time taken for the generation of keys using proposed scheme is comparatively less than the DSA and EdDSA. This implies that the proposed algorithm is faster in key generation than the existing approaches. Figure 3 shows the results achieved.

### Generation of Signature

The time taken for the generation of signature using the proposed scheme uses secure hash function similar to DSS, consumes less time when compared to the DSA and EdDSA algorithm. Figure 4 shows the results achieved.

Figure 3. Results for Key Generation

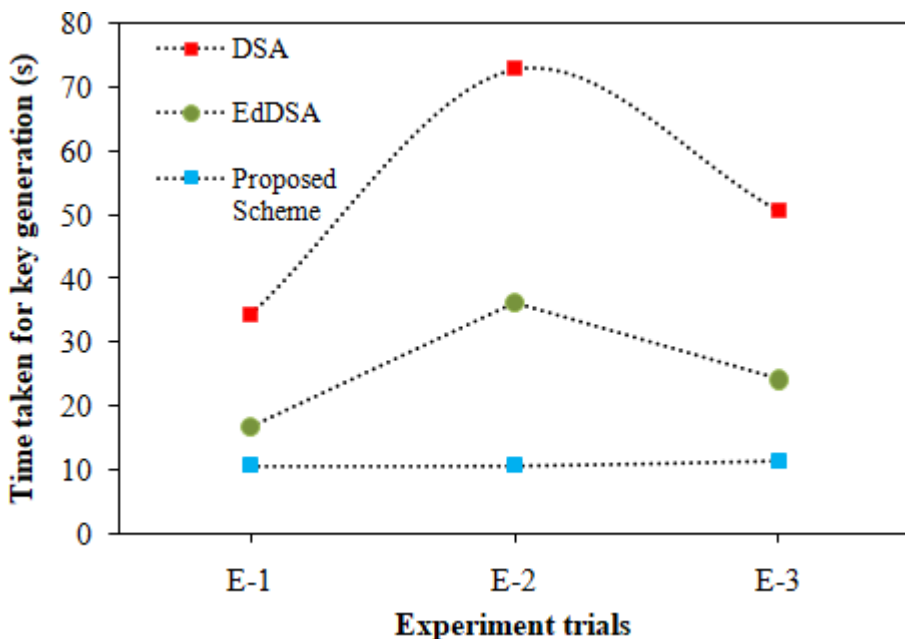
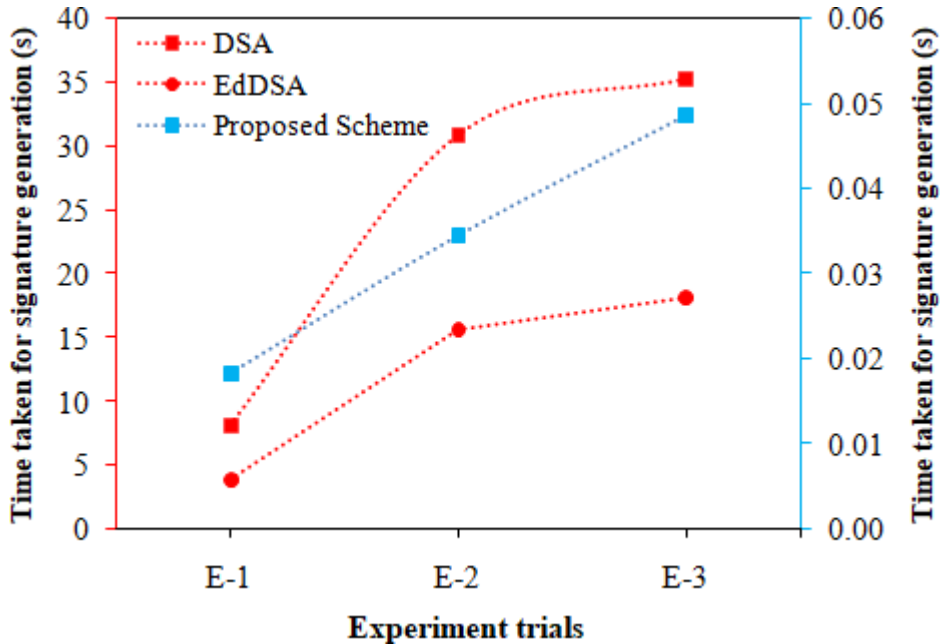


Figure 4. Results of Signature Generation



### Verification of Signature

The time taken for signature verification performs better when compared to the DSS and EdDSA algorithm. Figure 5 shows the results achieved. Figure 5 shows the results achieved.

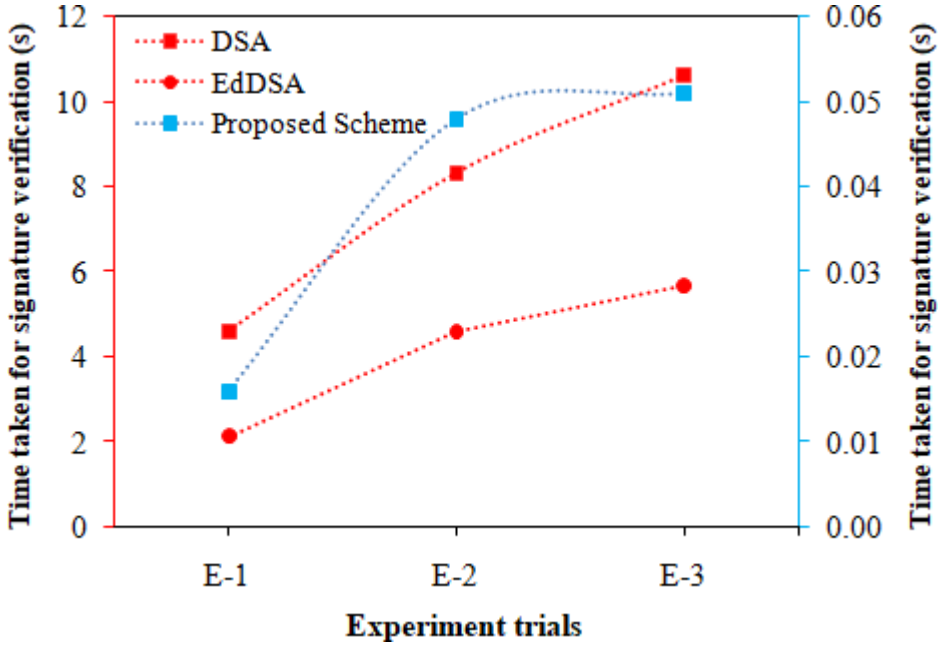
### Error Correction and Accuracy

The process of both encoding and decoding (Cheng Song et al, 2020) comprise of a good network channel coding which possesses the error correction capacity and minimizes the error rate. In our scheme, IEEE 754 technique is used for encoding and decoding. Here, we can apply hash function to check for errors. The signature is computed by the sender and sent to the receiver's end by appending the signature along with the message. On the other end, the receiver decodes the message to find the errors and segregate the signature. The number of bits received through the signature will be compared with the original number of bits in the signature. If there is any mismatch, then the error can be spotted, else it is considered as error-free.

### PROOF OF SECURITY

The security of the proposed scheme is evaluated under the DSA assumption standard. The proposed algorithm applies encoding of the input message 'm' through IEEE 754 standard. Axiom 1 states that the encoding components consist of input 'x' with the exponent part, significant part, and the exponent bias to convert the original message to its decoded form. Based on the axiom 1, lemma 1 proves that the input parameters used to encode the message will also be helpful for decoding the message. In the proof section of lemma1, it is proved that the encoded values lie between 0 and  $2^n$ . Lemma 2 proves  $g_k = h^{c-1/d} \bmod c$  by obeying the Fermat's theorem. For the non-negative numbers, the above given equation obeys and produces the result  $j = n \bmod d$ . Lemma 3,4,5,6 considers the factorized value and encoded message to prove that the signature generated is decoded and verified.

Figure 5. Results of Signature Verification



Axiom 1:

Let  $z = (\mu, \lambda)$  be floating point representation and  $x$  being  $z$ -representable,  $Z \neq 0$ .

Encode  $(x, z) = (s, m, e)$  where,

- (i) If  $sgn(x) = 1$ , then  $s = 0$  implies  $sgn(x) = -1$ , then  $s = 1$ .
- (ii)  $m = sig(x)^{2\mu-1}$ .
- (iii)  $e = expo(x) + 2^{\lambda-1} - 1$

Lemma 1:

Based on axiom 1, let  $Z = (\mu, \lambda)$  be the floating point representation.  $y = (s, m, e)$  be normal  $z$ -encoding:

$x = decode(y, z)$

- (i)  $sgn(x) = (-1)^s$
- (ii)  $sgn(x) = m / 2^{\lambda-1}$
- (iii)  $x$  is  $z$ -representable
- (iv)  $expo(x) = e - 2^{\lambda-1} + 1$
- (v)  $encode(x, z) = y$

Proof:

Let  $z = (\mu, \lambda)$ , then:

$$x = (-1)^s m 2^{e - (2^{\lambda-1} - 1) - \mu + 1}$$

$$x = (-1)^s (m 2^{1-\mu}) 2^{e - (2^{\lambda-1} - 1)}$$

However,  $2^{\mu-1} \leq m \leq 2^\mu$  produces  $1 \leq m 2^{\mu-1} \leq 2$ , (i), (ii), (iii), (iv), (v) obeys the relation  $0 \leq e \leq 2^\lambda$  from the definition given above.

**Lemma 2:** For an integer ‘n’, if  $g_k = h^{(c-1)/d} \text{ mod } c$  then.

**Proof:** Using Fermat’s theorem, since h is relatively prime to c, then  $h^{c-1} \text{ mod } c = 1$ . So, for every non-negative number i:

$$\begin{aligned} g_k^{id} \text{ mod } c &= \left( h^{(c-1)/d} \text{ mod } c \right)^{id} \text{ mod } c \\ &= h^{((c-1)/d)id} \text{ mod } c \\ &= h^{(c-1)i} \text{ mod } c \\ &= \left( h^{(c-1)i} \text{ mod } c \right)^i \text{ mod } c \\ &= 1^i \text{ mod } c \\ &= 1 \end{aligned}$$

Hence, for non-negative numbers i & j:

$$\begin{aligned} g_k^{id+j} \text{ mod } c &= g_k^{id} g_k^j \text{ mod } c \\ &= (g_k^{id} g_k^j \text{ mod } c) (g_k^j \text{ mod } c) \text{ mod } c \\ &= g_k^j \text{ mod } c \end{aligned}$$

Any non-negative number ‘n’ can be depicted as  $n = g_k^i \text{ mod } c$ , where i and j are Non-negative numbers and hence:

$$0 < j < d$$

Therefore,  $j = n \text{ mod } d$ . Hence it is proved.

**Lemma 3:** Applying non-negative numbers x and y:

$$g_k^{(x \text{ mod } d + y \text{ mod } d)} \text{ mod } c = g_k^{(x+y) \text{ mod } d} \text{ mod } c$$

**Proof:** By Lemma 1, we know that:

$$\begin{aligned} g_k^{(x \bmod d + y \bmod d)} \bmod c &= g_k^{(x \bmod d + y \bmod d) \bmod d} \bmod c \\ &= g_k^{(x+y) \bmod d} \bmod c \end{aligned}$$

It is proved.

Lemma 4:

$$Pu^{(\infty w) \bmod d} \bmod c = g_k^{(Pr \cdot \infty w) \bmod d} \bmod c$$

**Proof:**

We know that:

$$\begin{aligned} y &= g^x \bmod p \text{ (From DSA approach)} \\ Pu^{(\infty w) \bmod d} \bmod c &= \left( g_k^{Pr} \bmod c \right)^{(\infty w) \bmod d} \bmod c \\ &= g_k^{Pr((\infty w) \bmod d)} \bmod c \\ &= g_k^{(Pr((\infty w) \bmod d)) \bmod d} \bmod c \text{ (From Lemma 1)} \\ &= g_k^{(Pr \cdot \infty w) \bmod d} \bmod c \end{aligned}$$

Hence, it is proved.

Lemma 5:

$$\left( H(m) + Pr \cdot \infty \right) n^{-1} \bmod d = n$$

**Proof:** From DSA approach, we know that:

$$s = \left( k^{-1} \left( H(m) + xr \right) \right) \bmod q$$

Since q is prime, any non-negative number less than q has a multiplicative inverse.

Hence,  $kk^{-1} \bmod q = 1$ . Now, applying this over our approach:

$$\begin{aligned} \rho &= n^{-1} \left( H(m) + Pr \cdot \infty \right) \bmod d \\ n\rho \bmod d &= n \left( n^{-1} \left( H(m) + Pr \cdot \infty \right) \bmod d \right) \bmod d \\ &= \left( nn^{-1} \bmod q \right) \left( H(m) + Pr \cdot \infty \right) \bmod d \cdot \bmod d \\ &= \left( H(m) + \infty Pr \right) \bmod d \end{aligned}$$

We know that,  $w = \rho^{-1} \bmod d$ .

Therefore,  $w\rho \bmod d = 1$ :

$$\begin{aligned}
 (H(m) + Pr \cdot \alpha)w \bmod d &= (((H(m) + Pr \cdot \alpha)w \bmod d)(w \bmod d)) \bmod d \\
 &= (np \bmod d)(w \bmod d) \bmod d \\
 &= npw \bmod d \\
 &= ((n \bmod d)(wp \bmod d)) \bmod d \\
 &= n \bmod d \\
 &= 0 < n < d, \text{ we get } n \bmod d = n \\
 \text{Hence, it is proved.}
 \end{aligned}$$

Lemma 6:

To prove  $\alpha = \beta$ :

$$\begin{aligned}
 \beta &= ((g_k^t \rho_u^u) \bmod c) \bmod d \\
 &= ((g_k^{H(m)w \bmod d} \rho_u^{(\alpha w) \bmod d} \bmod d) \bmod c) \bmod d \\
 &= ((g_k^{H(m)w \bmod d} g_k^{(Pr \cdot \alpha \cdot w) \bmod d} \bmod c) \bmod d \\
 &= ((g_k^{H(m)w \bmod d + (Pr \cdot \alpha \cdot w) \bmod d} \bmod c) \bmod d \\
 &= ((g_k^{(H(m)w + Pr \cdot \alpha \cdot w) \bmod d} \bmod c) \bmod d \\
 &= (g_k^{n \bmod c} \bmod d \\
 &= \alpha
 \end{aligned}$$

Hence the verification process is proved.

## CONCLUSION

The proposed digital signature scheme is efficient in terms of reduced time complexity in signing process. This scheme authorizes the signature created by the sender and authenticates the sender who initiates the communication. It does not involve in the generation of too many prime factors to generate the signature and thereby signifies that the cost of creating signature is less since a single hash function is used. It also increases the speed of the transaction with accuracy. Also, the scheme creates confusion in the initial occurrence of the original message through coding algorithm. Henceforth, plain text attack is not possible in this scheme. The involvement of encoding-encryption technique has proven its performance with less error. The time complexity of the proposed scheme in key generation, signature generation and verification is comparatively lesser than the existing schemes. Further, the proof of security in the proposed digital signature algorithm is also appended to prove the strength of the algorithm. In future, the security analysis can be done for this algorithm to prove its strength against mathematical attacks.

## REFERENCES

- Alidoost Nia, M., Sajedi, A., & Jamshidpey, A. (2014). *An Introduction to Digital Signature Schemes*. arXiv Preprint arXiv
- Arsalan, M., Kim, D. S., Lee, M. B., Owais, M., & Park, K. R. (2019). Fully residual encoder–decoder network for accurate iris segmentation. *Expert Systems with Applications*, 122, 217–241. doi:10.1016/j.eswa.2019.01.010
- Black, D. K. (1993). The Digital Signature Standard: Overview and current status. *Computers & Security*, 12(5), 437–446. doi:10.1016/0167-4048(93)90062-A
- Chang, T. K. (2014). A secure operational model for mobile payments. *The Scientific World Journal*, 2014. doi:10.1155/2014/626243 PMID:25386607
- Chou, C. F., Cheng, W. C., & Golubchik, L. C. (2010). Performance study of online batch-based digital signature schemes. *Journal of Network and Computer Applications*, 33(2), 98–114. doi:10.1016/j.jnca.2009.12.001
- Gao, J., Kulkarni, V., Ranavat, H., Chang, L., & Mei, H. (2009). A 2-D barcode-based mobile payment system. *3rd International Conference on Multimedia and Ubiquitous Engineering, MUE 2009*, 320–329. doi:10.1109/MUE.2009.62
- Guo, F., Mu, Y., & Susilo, W. (2011). Improving security of qSDH based digital signatures. *Journal of Systems and Software*, 84(10), 1783–1790. doi:10.1016/j.jss.2011.05.023
- Hassinen, M., Hyppönen, K., & Trichina, E. (2008). Utilizing national public-key infrastructure in mobile payment systems. *Electronic Commerce Research and Applications*, 7(2), 214–231. doi:10.1016/j.elerap.2007.03.006
- Heide, J., Pedersen, M. V., Fitzek, F. H. P., & Larsen, T. (2009). Network coding for mobile devices - Systematic binary random rateless codes. *Proceedings - 2009 IEEE International Conference on Communications Workshops, ICC 2009*.
- Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., De Fuentes, J. M., & Ramos, B. (2013). A taxonomy and survey of attacks on digital signatures. *Computers & Security*, 34, 67–112. doi:10.1016/j.cose.2012.11.009
- Husni, E. (2017). Dynamic rule encryption for mobile payment. *Security and Communication Networks*.
- Kittur, A. S., & Pais, A. R. (2017). Batch verification of Digital Signatures: Approaches and challenges. *Journal of Information Security and Applications*, 37, 15–27. doi:10.1016/j.jisa.2017.09.005
- Ktari, M., Mosbah, M., & Kacem, A. H. (2017). Electing a Leader in Dynamic Networks using Mobile Agents and Local Computations. *Procedia Computer Science*, 109(2016), 351–358.
- Kundu, N., Debnath, S. K., Mishra, D., & Choudhury, T. (2020). Post-quantum digital signature scheme based on multivariate cubic problem. *Journal of Information Security and Applications*, 53.
- Liao, Y. P., & Hsiao, C. M. (2013). A novel multi server remote user authentication scheme using self-certified public keys for mobile clients. *Future Generation Computer Systems*, 29(3), 886–900. doi:10.1016/j.future.2012.03.017
- Lizama-Perez, L. (2019). Digital signatures over hash-entangled chains. *SN Applied Sciences*, 1(12), 1–8. doi:10.1007/s42452-019-1618-6
- Martiri, E., & Baxhaku, A. (2012). Monotone digital signatures: An application in software copy protection. *Procedia Technology*, 1, 275–279. doi:10.1016/j.protcy.2012.02.058
- Mihaljević, M., & Oggier, F. (2010). Wire-tap Approach to enhance security in communication systems using the encoding-encryption paradigm. *ICT 2010: 2010 17th International Conference on Telecommunications*, 83–88.
- Oh, H., Kim, J., & Shin, J. S. (2018). Forward-secure ID based digital signature scheme with forward-secure private key generator. *Information Sciences*, 454-455, 96–109. doi:10.1016/j.ins.2018.04.049
- Park, J. S., & Ogunfunmi, T. (2017). A 3D-DCT video encoder using advanced coding techniques for low power mobile device. *Journal of Visual Communication and Image Representation*, 48, 122–135. doi:10.1016/j.jvcir.2017.06.004

- Pasupuleti, S. K., Ramalingam, S., & Buyya, R. (2016). An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. *Journal of Network and Computer Applications*, 64, 12–22. doi:10.1016/j.jnca.2015.11.023
- Qin, Z., Sun, J., Wahaballa, A., Zheng, W., Xiong, H., & Qin, Z. (2017). A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing. *Computer Standards & Interfaces*, 54, 55–60. doi:10.1016/j.csi.2016.11.012
- Rajesh, G., Sangaiah, A. K., Karthik, S. R., Selvaraj, B. C., & Krishna, C. V. (2018). Energy optimised cryptography for low power devices in internet of things. *International Journal of High Performance Systems Architecture*, 8(3), 139. doi:10.1504/IJHPSA.2018.10022450
- Ruiz-Martínez, A., Sánchez-Montesinos, J., & Sánchez-Martínez, S. (2011). A mobile network operator-independent mobile signature service. *Journal of Network and Computer Applications*, 34(1), 294–311. doi:10.1016/j.jnca.2010.07.003
- Schoaba, V., Sikansi, F. E. G., Pigatto, D. F., Branco, K. R. L. J. C., & Branco, L. C. (2010). DISIMOD - Digital Signature for Mobile Devices. *International Conference on Convergence and Hybrid Information Technology (ICHIT 2010)*, 1–8.
- Song, , Liu, , Feng, , & Fan, . (2020). Coverage control for heterogeneous mobile sensor networks with bounded position measurement errors. *Automatica*, 120.
- Standard, D. S., Digital, T., & Standard, S. (1976). The Proposed Digital Signature Standard : Implications for Electronic. *Computer Law & Security Report*, 217–225.
- Sukumaran, S. C., & Mohammed, M. (2018). PCR and Bio-signature for data confidentiality and integrity in mobile cloud computing. *Journal of King Saud University - Computer and Information Sciences*.
- Tian, H., Chen, X., Zhang, F., Wei, B., Jiang, Z., & Liu, Y. (2013). A non-delegatable strong designated verifier signature in ID-based setting for mobile environment. *Mathematical and Computer Modelling*, 58(5-6), 1289–1300. doi:10.1016/j.mcm.2013.01.010
- Troja, E., & Bakiras, S. (2017). Optimizing privacy-preserving DSA for mobile clients. *Ad Hoc Networks*, 59, 71–85. doi:10.1016/j.adhoc.2017.02.001
- Turkes, O., Scholten, H., & Havinga, P. J. M. (2016). Cocoon: A lightweight opportunistic networking middleware for community-oriented smart mobile applications. *Computer Networks*, 111, 93–108. doi:10.1016/j.comnet.2016.08.021
- Walker, H., & Pay, A. (2016). *Digital signatures in mobile banking and payment processing*. Academic Press.
- Xue, Y., Tan, Y., Liang, C., Li, Y., Zheng, J., & Zhang, Q. (2018). RootAgency: A digital signature-based root privilege management agency for cloud terminal devices. *Information Sciences*, 444, 36–50. doi:10.1016/j.ins.2018.02.069
- Yang, W., Li, J., Zhang, Y., & Gu, D. (2019). Security analysis of third-party in-app payment in mobile applications. *Journal of Information Security and Applications*, 48, 1–14. doi:10.1016/j.jisa.2019.102358
- You, L., & Sang, Y. X. (2010). Effective generalized equations of secure hyperelliptic curve digital signature algorithms. *Journal of China Universities of Posts and Telecommunications*, 17(2), 100–108, 115. doi:10.1016/S1005-8885(09)60454-4
- Yu, X., Kywe, S. M., & Li, Y. (2018). Security Issues of In-Store Mobile Payment. In *Handbook of Blockchain, Digital Finance, and Inclusion* (1st ed., Vol. 2). Elsevier Inc. doi:10.1016/B978-0-12-812282-2.00006-1

*Shibin David is serving as an Assistant Professor at Karunya Institute of Technology and Sciences, India. His research interest includes cryptography, network security, mobile computing.*

*G. Jaspheer W. Kathrine (PhD) is working as an Assistant Professor in the Department of Computer Science and Engineering at Karunya Institute of Technology and Sciences, India. Her research interest includes Grid Computing, Cryptography, and Network Security, Cloud Security.*