International Journal of Scientific & Engineering Research Volume 10, Issue 10, October-2019
712
ISSN 2229-5518

M.S.H. Biswas crypto-intensive techniques

Md Shamim Hossain Biswas

Abstract—M.S.H. Biswas crypto-intensive techniques in combination of Encryption algorithm, Signature generation algorithm, Signature verification algorithm and Decription algorithm. Michael O. Rabin Signature scheme uses random padding to validate signature. Analogously the proposed techniques uses same padding system including additional quotient and residuum. The only difference is that Rabin signature is pair or triple in some special cases but proposed model uses forefold signature system. Michael O. Rabin Cryptosystem can generate same ciphertext form different plaintext as well as multiple plaintext from single cyphertext. To solve those issues, i designed a new cryptosystem "A mathematical model for ascertaining same ciphertext generated from distinct plaintext in Michael O. Rabin Cryptosystem". But it did not have authentication system to verify sender and valid message because there was no signature generation facility.In this article, i have designed a new signature algorithm in combination with previous techniques and Michael O. Rabin public key Signature scheme. Receiver can decipher secret message from sender's signature. The proposed crypto intensive technique uses two times security key by slightly altering Diffie-Hellman key exchange protocol. The advantage of proposed crypto intensive technique is that the sender generate signature using encrypted text and intended receiver can retrieve plaintext from signature through signature verification system.The proposed crypto teachniques secure against man-in-the-middle attack. It is unforgeable while Rabin's signature is forgeable in forgery attack.

Index Terms— Michael O. Signature scheme, Rabin's Cryptosystem, Diffie-Hellman key exchange protocol, modular arithmetic, Bezout's Coefficient, Extended Euclidean Algorithm, Chinese Remainder Theorem, Congruence, ASCII- Code, Quadratic reciprocity.

1 INTRODUCTION

In cryptography, the Rabin signature algorithm is a method of digital signature originallyly proposed by Michael O. Rabin. It was one of the first digital signature schemes that relates the hardness of forgery directly to the problem of integer factorization. It was existensitally unforgeablev in the random oracle model assuming the integer factorization problem was intractable and closely related to the Rabin crptosystem [1]. Since its publication on January 1979. A huge number of research was carried out by several researchers.[2]

A digital signature is a mathematical techniques for verifying the authenticity of digital messages or documents. Authentication means that a valid digital signature gives a recipient very strong reason to believe that the message was created by a known sender and the integrity ensure that the message was not altered in transit. It is a standard element of most cryptographic protocol and commonly used for software distribution, financial transactions, contract management system and to detect forgery or tampering specially intentional modification of product.

The term tempering referes to as many form of sabotage. The term authentication can be refered to computer communication protocol. Or cryptographic protocol specilly designed for transfer of authentication data between two entities.

The term data integrity can be refered to maintenance and the assurance of the accuracy and consistency of data over its entire life-cycle.

The encryption mechanism used quadratic residue to produce cipher text .The encryption of a message $m \in \mathbb{Z}^*_N$ is presented by $c = m^2 \bmod N$, where $N = p * q$ is a product of two prime numbers, and decryption is performed by solving the equation $x^2 = c \bmod N$ which has four roots; thus for complete decryption, further information is needed to identify m among these roots. It has vulnerability to chosen-plaintext attack [3-6]. Williams [7] proposed a root identification scheme based on the computation of a Jacobi symbol, using an additional parameter in the public key and two additional bits in the encrypted message.

The decryption was accomplished by Computing two square root, Bezout's Coefficient using extended Euclidean algorithm and combining them with Chinese Remainder theorem. Similarly to the RSA and ElGamal cryptosystems, Michael O. Rabin cryptosystem is described in a ring under addition and multiplication modulo composite integer.One of the main disadvantage is to generate four results during decryption and extra effort needed to sort out the right one out of four possibilities. Michael O. Rabin Signature vulnerable in forgery attack.

- *Md. Shamim Hossain Biswas is currently pursuing MSc in Software Engineering at Daffodil International University in Bangladesh, ORCID: 0000-0002-4595-1470 PH-+8801531262445. E-mail: shamim44-165@diu.edu.bd*

The Rabin cryptosystem may also be used to create a signature by exploiting the inverse mapping. In order to sign m, the equation $x^2 = m \bmod N$ is solved and any of the four roots(S) can be used to form the signed message (m, S). However, if $x^2 = m \bmod N$ has no solution, the signature cannot be generated directly. To overcome this issue, a random pad U is used until $x^2 = m * U \bmod N$ is solvable, and the signature is the triple (m, U, s). A verifier compares s^2 with $m*u \bmod N$ and accepts the signature as valid when these two numbers are equal.

Digital signatures employ asymmetric cryptography. In many instances, they provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals, but properly implemented digital signatures are more difficult to forge than the handwritten type. It can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret. Further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bitstring: For examples include electronic mail, contracts, or a message sent via some othercrptographic protocol. It is typically consists of 3 algorithms:

1. *Key generation algorithm* that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
2. *Signing algorithm* that produces a signature.
3. *Signature verifying algorithm* that claim to message's authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the generator of the message to attach a code that acts as a signature.

In this paper, i design a new crypto-intensive techniques based on Michael O. Rabin Cryptosystem, concept of square modular arithmetic from Michael O. Rabin Signature Scheme. M.S.H. Biswas Cryptosystem [8]. Floor function and absolute value function. Two entities's current interaction key generated from Diffie-Hellman key exchange protocol. [9]

In proposed signature scheme, an entity A sends a 4-tuple signatur (Q, R, U, r_e) to B. The entity B verify the signature by $X(X+G) = Q*R*U \bmod N$. where X is the hash value of H(X), G is generator, $Q = \lfloor m^2 / K_c \rfloor$, $R = m^2 \bmod K_c$. If equality is found the signature is accepted by verifier and reveal the message by $\lfloor \sqrt{Q * k_c + R} \rfloor$ and gets only one desired plain text unlike Rabin's Cryptosystem in which she gets four different decryption results.

The rest of the paper is organized as a follows. Section 1.1 Preliminaries, Ssection 1.2 gives an overview of Rabin's Signature Scheme, Section 1.3 provides an overview of Diffie-Hellman Key Exchange protocol, and Section 2 gives Literature Review, Section 3 presents author contribution, Section 3.1 for illustration of M.S.H. Biswas crypto intensive techniques, Section 3.2 gives comparison, Finally, Section 4, 5 give conclusion and acknowledgement.

1.1 Preliminaries

Assuming that $N = p*q$ be a product of two odd primes p and q. Using the generalized Euclidean algorithm to compute the greatest common divisor between p and q ∈ N.

1. Initialize $r_0 = q$ and $r_1 = p$.
2. Compute the following sequence of equations:
   $r_0 = q_1 r_1 + r_2$, where q_1 is quotient.
   $r_1 = q_2 r_2 + r_3$,
   $r_{n-3} = q_{n-2} r_{n-2} + r_{n-1}$,
   $r_{n-2} = q_{n-1} r_{n-1} + r_n$, until there is a step for which $r_n = 0$ while $r_{n-1} \neq 0$.
3. The greatest common divisor is equal to r_{n-1}.

From which two integer numbers can be achieved after extending the theorem and that is Bezouts' coefficient, $\lambda_1, \lambda_2 \in \mathbb{Z}$, such that $\lambda_1 p + \lambda_2 q = 1$, are efficiently computed. Thus, setting $\psi_1 = \lambda_2 q$ and $\psi_2 = \lambda_1 p$, so that $\psi_1 + \psi_2 = 1$, it is easily verified that ψ_1 and ψ_2 satisfy the relations

$$\begin{cases} \Psi_1 \Psi_2 = 0 \bmod N \\ \Psi_1^{\,2} = \Psi_1 \bmod N \\ \Psi_2^{\,2} = \Psi_2 \bmod N \end{cases}$$

and that $\psi_1 = 1 \bmod p$, $\psi_1 = 0 \bmod q$, and $\psi_2 = 0 \bmod p$, $\psi_2 = 1 \bmod q$. According to the Chinese Remainder Theorem (CRT), using ψ_1 and ψ_2, every element a in $\mathbb{Z}_N$ can be represented as $a = a_1\psi_1 + a_2\psi_2 \bmod N$, where $a_1 \in \mathbb{Z}_p$ and $a_2 \in \mathbb{Z}_q$ are calculated as $a_1 = a \bmod p$ and $a_2 = a \bmod q$. The four roots $x_1, x_2, x_3, x_4 \in \mathbb{Z}_N$ of $x^2 = C \bmod N$ represented as positive numbers, are obtained using the CRT from the roots $u_1, u_2 \in \mathbb{Z}_p$ and $v_1, v_2 \in \mathbb{Z}_q$ of the two equations $u_2 = C \bmod p$ and $v_2 = C \bmod q$, respectively. The roots u_1 and $u_2 = p - u_1$ have different parities; likewise, v_1 and $v_2 = q - v_1$. If p is congruent 3 modulo 4, the root u_1 can be computed in deterministic polynomialtime as $\pm C^{p+1/4} \bmod p$, $\pm C^{q+1/4} \bmod q$. However, u_1 can be computed in probabilistic

polynomial-time using Tonelli's algorithm [10] once a quadratic non-residue modulo p is known (this computation is the probabilistic part of the algorithm), or using the (probabilistic) Cantor-Zassenhaus algorithm.[11, 12, 13] to factor the polynomial $u^2 - c$ modulo p. Using the previous notations, the four roots can be written as

$$\begin{cases} x_1 = u_1\Psi_1 + v_1\Psi_2 \ mod\ N \\ x_2 = u_1\Psi_1 + v_2\Psi_2 \ mod\ N \\ x_3 = u_2\Psi_1 + v_1\Psi_2 \ mod\ N \\ x_4 = u_2\Psi_1 + v_2\Psi_2 \ mod\ N \end{cases}$$

Lemma 1 Let N = p*q be a product of two prime numbers and C be a quadratic residue modulo N. The four roots x_1, x_2, x_3, x_4 of the polynomial x^2 - C are partitioned into two sets $X_1 = \{x_1,x_4\}$ and $X_2 = \{x_2,x_3\}$ such that roots in the same set have different parities, i.e. $x_1 = 1 + x_4 \bmod 2$ and $x_2 = 1 + x_3 \bmod 2$.

Proof. Since u_1 and v_1 have the same parity by assumption, then also x_1 and x_4 have the same parity. The connection between x_1 and x_4 is shown by the following chain of equalities:

$x_4 = u_2\psi_1 + v_2\psi_2 = (p - u_1)\ \psi_1 + (q - v_1)\psi_2 = - x_1 \ mod\ N = N - x_1$, because $p\psi_1 = 0 \ mod\ N$ and $q\psi_2 = 0 \ mod\ N$, and x_1 is less than N by assumption, thus $-x_1 \bmod N = N - x_1$ is positive and less than N.

A similar chain connects x_2 and $x_3 = N - x_2$, because N is odd and thus x_1 and x_4 as well as x_2 and x_3 have different parities.

1.2 An illustration of Michael O. Rabin Signature

Unique signature Algorithm: The signature S is given by the following equation.

$$S= ((p^{q-2}{}_{H(m)}{}^{\frac{q+1}{4}} \bmod q)\ p + (q^{p-2}{}_{H(m)}{}^{\frac{p+1}{4}} \bmod p)\ q) \bmod N$$

Verification by $H(m) = s^2 \bmod N$, where N is composit number of p*q. The signature can be verified by everyone as N is public key. A hash function H is collision resistant if it is hard to finds that hash to the same output. If H is a collision resistant hash function which does not mean that no collision exists, simply they are hard to find. Such as, $_{H(m)}{}^{\frac{p-1}{2}} \bmod p$ $_{=1 \text{ and } H(m)}{}^{\frac{q-1}{2}} \bmod q = 1$ .The cryptographic hash function is any mathematical equation. Message m is being hashed (encrypted). The hash value 1 generates by using private key p and q. The same hash value from different hashed input is so called collision resistant and the algorithm works as follows:

The workout example, assuming that p=7 and q=11 using 4k+3 prime formation. The public key N=p*q= 77. The Hashed message $H(m)=20^2 \bmod 77=15$. Let us see collision resistant hash value $15^{\frac{7-1}{2}} \bmod 7 \ _{=1 \text{ and } 15}{}^{\frac{11-1}{2}} \bmod 11 = 1$

that is vulnerable in collision attack because a collision attack on cryptographic hash tries to find two inputs producing same Hash value.

$S = ((7^{11-2}{}_{15}{}^{\frac{11+1}{4}} \bmod 11)7 + (11^{7-2}{}_{15}{}^{\frac{7+1}{4}} \bmod 7)\ 11) \bmod 77$
$= (8*9 \bmod 11)7 + 2*11) \bmod 77$
$= (6*7 + 2*11) \bmod 77 = 64$ so the signature is unique.

Signature verification: $H(m) = s^2 \bmod 77 = 64^2 \bmod 77 = 15$. Since H(m)=H(m), the signature is valid and accepted by verifier.

Pairing signature algorithm:

Key generation:

In most presentations in modern cryptography the algorithm is simplified by choosing b = 0, where b actually basement (least prime). The signer S chooses two primes p, q privately and computes the product N = p*q, where N is declared as a public key.

Signature generation:

Signer S picks random padding U to sign a message m and calculates H (m)*U mod N. S then solves the equation X(X+b) = H (m)*Umod N. where b is basement (least prime).If there is no solution S picks a new pad U and try again. Else the signature on m is (U, x)

Signatue Verification:

Given a message m and a signature (U, x) the verifier V calculates equality of X(X+b) mod N and H(m)*U mod N where X=H(X). If equality is found, the signature is accepted.

A workout example, **a**ssuming that an entity A want to send a secret information(X=20) to other entity B using valid signature. It first hashes the secret by $m^2 \bmod N = 20^2 \bmod 77 = 15$. Where N is a composite number of two secret private key, moduli p=7, moduli q=11, both prime are Blum prime (4k+3). Public key or modulus N=p*q=7*11=77. The Hashed value 15 will be used to generate signature.

Signing: Signer S chooses number U probabilistically and see the value of random oracle modulo N matches any quadratic residue modulo N that is X(X + b) mod N= m*U modulo N.This process continue until both sides of the equation match the hash.

X(X + b) mod N	m*U mod N
⇒15 (15+2) mod 77	⇒ (15* 17) mod 77
= 24	=24

The equation is solvable that is why the signature on m is the pair (17, 15)

1.3 Diffie-Hellman Key exchange protocol

The first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography. It is generally referred to as Diffie-

Hellman key exchange protocol. A number of commercial products employ this key exchange technique. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption and decryption of messages. The algorithm itself is limited to the exchange of secret values. The Diffie-Hellman algorithm's effectiveness depends on of computing discrete logarithms.

Global public elements:
N is a prime number which can define a domain so called curve area or elliptic curve, α is a primitive root of N such that α < N.

Key generation for user A:
Select private key X_a , such that $X_a < N$. Calculate public key
$Y_a = \alpha^{xa} \bmod N$

Key generation for user B:
Select private key X_b such that $X_b < N$. Calculate public key $Y_b = \alpha^{xb} \bmod N$

Secret key for user A: $K= (Y_b)^{xa} \bmod N$

Secret key for user B: $K= (Y_a)^{xb} \bmod N$

A workout Example, an integer number N = 353 that is domain size and its primitive root α = 3. A and B select secret keys A = 97 and B = 233, respectively.
Each of them computes public key:
A computes $X = 3^{97} \bmod 353 = 40$.
B computes $Y = 3^{233} \bmod 353 = 248$.

They compute secret key in the following ways by exchanging public key between each other.

A computes $K = (Y)^{A} \bmod 353 = 24897 \bmod 353 = 160$.
B computes $K = (X)^{B} \bmod 353 = 40233 \bmod 353 = 160$.

2 Literature Review

if $x^2 = m \bmod N$ has no solution, the signature cannot be generated directly. To overcome this issue, a random pad U is used until $x^2 = m * U \bmod N$ is solvable, and the signature is the triple (m, U, s). J. Pieprzyk et.al. , [14] calculated random pad deterministically as follows.

$f_1 = \frac{m_1}{2}\left[1 - \left(\frac{m_1}{p}\right)\right] + \frac{1}{2}\left[1 + \left(\frac{m_1}{p}\right)\right]$

$f_2 = \frac{m_2}{2}\left[1 - \left(\frac{m_2}{q}\right)\right] + \frac{1}{2}\left[1 + \left(\frac{m_2}{q}\right)\right]$

$m = m_1\psi_1 + m_2\psi_2 \bmod N$

$m = m_1\psi_1 + m_2\psi_2 \bmod N$

$x^2 = (m_1\psi_1 + m_2\psi_2)(f_1\psi_1 + f_2\psi_2) = (f_1m_1\psi_1 + f_2m_2\psi_2) \bmod N$, where f_1m_1 and f_2m_2 is a quadratic residue modulo p and modulo q respectively,

Since $\left(\frac{m_1}{p}\right)=\left(\frac{f_1}{p}\right)$, $\left(\frac{m_2}{q}\right) = \left(\frac{f_2}{q}\right)$ so that

$\left(\frac{m_1 f_1}{p}\right) = \left(\frac{m_1}{p}\right)\left(\frac{f_1}{p}\right)=1$

$\left(\frac{m_2 f_2}{q}\right) = \left(\frac{m_2}{q}\right)\left(\frac{f_2}{q}\right)=1$

$u= R^2 [f_1\psi_1 + f_2\psi_2]$

Signed message: (m, U, s)

Verification: The Signer S verify the equation $x^2 = m*U \bmod N$, since L.H.S = R.H.S, the signature is valid for message m. This is deterministically true as x^2 pre-calculated but probabilistically there is no such x value for which the $x^2 = m*U \bmod N$ is true.

D.J. Bernstein [15] presented am application to electronic signature and its comparative analysis of Rabin-Willium signature algorithm.

[16]The Rabin-Williams Signature scheme relying on finding difficulties of square root. But it does not offer multiple signature facilities in single document.it avoids the forgery vulnerability. But it requires the use of two primes congruent to 3 and 7 modulo 8 respectively.

Michele Elia et.al.,[17] descrived a variant aims at countering the Rabin's signature vulnerability as follows.

Signed Message: $(m, U*R^2 \bmod N, S*R^3 \bmod N, R^4 \bmod N)$, so the signature is fourfold where U is padding factor and R is a random number selection, Here S is the x's value for which equation $x^2 = m*U \bmod N$ is true. It is clearly seen that x and U both unknown number which has to be chosen by entity A in order to generate signature.

Verification: Compute $(S*K^3)^2 \bmod N$ and $m*U*R^2*R^4 \bmod N$; the signature is valid if and only if aforesaid two numbers are equal.

A workout example, aassuming preprocessed m/=15, $U*R^2 = 25*3^2 \bmod 77=71$, $S*R^2=12*3^2 = 108 \bmod 77= 48$ and $3^4 \bmod 77 = 4$. So the signature (15, 71, 48, and 4) is a fourfold.

The verification computations are

1. $(12*3^3)^2 \bmod 77= (12^2*3^6) \bmod 77= 25$ and
2. $15*25*3^2*3^4 \bmod 77=25$

Counter forgery 4-tuple signature (15, 71, 48, and 41) verifi-

cation is successful, so the signature is valid and accepted.

Jaweria Usmani, et.al, [18] proposed a secure gateway discovery protocol using Rabin Signature Scheme in MANET that ensures confidentiality goal in heterogeneous environments. Registration process was included to remove the malicious nodes. This protocol removes the threat of anti-confidentiality, anti-authentication and anti-duplication. The efficiency of this protocol is shown through AVISPA tool.

Chaoyang Li et.al. , [19] proposed an efficient ID-based signature scheme based on Rabin's cryptosystem by using the forking lemma theorem. This scheme has less exponential operations, it is secure against existential forgery under adaptively chosen identity and message attacks in the random oracle model.

Daniel Bleichenbacher [20] presents a method to compress Rabin signature. Rabin signatures and compressed signatures are equally difficult to forge. Compression requires a continued fraction expansion and takes time $O(\log(n)_2)$. Decompression requires two multiplications and an inverse over $\mathbb{Z}\mathbb{Z}/_n\mathbb{Z}\mathbb{Z}$ and a square root in $\mathbb{Z}\mathbb{Z}$ and require time $O(\log(n)_2)$.

3 Author contributions

Prseumablly let an entity A wants communicate information to other entity B. Entities A and B both should have some confidentiality. The both entities A and B create a shared secret key using aforesaid key exchange protocol and then both of them add additional pre-negotiated key with newly generated key. A encrypts secret information with a secret key so that unauthorized entity cannot presume and disclose real information. A encrypts information and chooses an equivalent residuum to generate signature by solving equation $R(R+G) = Q*R*U$ modulo K_c, where R is quadratic residue modulo K_c, G is generator, Q is quadratic quotient modulus K_c and U is selected urbitarily to justify truthness of equation. A sends only 4-tuple signature (Q, R, U, r_e) to receiver B.The entity B verify the signature by checking truthness of equation $r_e=Q*R*U$ modulo K_c . B opens message by $\left|\sqrt{Q * k_c + R}\right|$ iff above equation is true, otherwise reject.

Key Generation Algorithm:

$K = (Y_b)^{xa} \bmod N$
$= (\alpha^{xb} \bmod N)^{Xa} \bmod N$
$= (\alpha^{xb})^{Xa} \bmod N$
$= \alpha^{xb\ Xa} \bmod N$
$= (\alpha^{Xa})^{xb} \bmod N$
$= (\alpha^{xa} \bmod N)^{Xb} \bmod N$
$= (Y_a)^{xb} \bmod N$

Current key (K_c) = Pre-negotiated symmetric key + Exchange key (K)

Encryption Algorithm:

To encrypt a message m, following logic are considered

$Q = \llcorner m^2 / K_c \lrcorner$
$R = m^2 \bmod K_c$
C= (Q, R), where Q= Quotient, R=Residuum, and C= Cipher.

Signing Algorithm:

To sign a message signer S try to find the solution of the equation $R(R+G) = C*U \bmod Kc$

$\Rightarrow R(R+G) = Q*R*U \bmod Kc.$

$\therefore$ Signature is 4-tuple (Q, R, U, r_e), where $r_e = R(R+G) \bmod Kc$, r_e = Equivalent residuum.

Decryption Algorithm:
The verifier V verify the signature by calculating the equation $r_e = (Q*R*U) \bmod K_c$. and opens message by $\left|\sqrt{Q * k_c + R}\right|$

3.1 Summary of proposed Crypto techniques

Assuming that Alice want to send a secret information (A=65) to Bob using valid signature. She first hashes the secret message by m^2 mod shared secret key (K_c) and floor value of m^2/Kc. She sends together signature and hashed message with to Bob. Bob reveals message after verifying the signature of sender. The entire process are as follows.

Key generation process:

Pre-negotiated key(P_{sk}) =17 <128(ASCII)			
Alice		Bob	
known	unknown	Known	unknown

Curve area N=113		✓	
Generator =5		✓	
key P=7	q=11	key q=11	P=7
A=5^{7} (113) =42		B=5^{11}(113)=34	
A=34^{7}(113)=40=k_a		B=42^{11} (113) =40=k_b	
(K_c)= Ka + P_{sk} =40+17=57		K_c = K_b + P_{sk} =40+17=57	

Current key K_c=exchange key+pre-negotiated key. Alice and Bob have acquire new key by mixturing the exchange key with their predefined key. Predefined key protect from man in middle attack as they both exchange their key publicly. Exchange key may be achieved by eavesdropper but they donot have access to the pre-negotiated key. She will lock written message by using new key. Then, she will signg on encrypted message and send to Bob.

Message encryption process:

Message A=65(ASCII)
Quotient$(Q) = \left|(065)^{2}/_{57}\right| = 74$
Residuum (R) = $(065)^2$ mod 57 = 7
Cypher text(C) = Q , R

Signature generation process:
R(R+G) = H(m)* U mod K_c ⇨R(R+G) = C*U mod K_c
⇨ R(R+G) = Q*R* U mod K_c
⇨ 7(7+5) = 74*7* 45 mod 57
⇨ 54 = 54 (modulo 57)

Let equivalent residue r_e= 54, Hence Signature is 4-tuple (74, 7, 45, and 54). Bob verify signature by computing equality of equation as follows.

Signature verification process:

⇨ r_e= Q*R*U mod K_c.
⇨r_e = 74*7*45 mod 57

∴ r_e = 54 (mod 57) verified.

Message opening process:

Now, Bob reveal the message by applying square root over the result of Q*K_c+R after that he accepts the absolute value as a desired plaintext.

Decryption=D=$\left|\sqrt{Q * k_c + R}\right|$
$= \left|\sqrt{74 * 57 + 7}\right|$
$= \left|\sqrt{4225}\right|$=65=A (reveal).

3.2 Comparison

Advantage of Michael O. Rabin Signature:

This signature actually contains several interesting feature are are as follows. The signature is possible using every pair of primes. Different signatures of the same document are different. The verification needs only two multiplications and therefore it is fast enough to be used in authentication protocol.

Disadvantage of Michael O. Rabin Signature:

It is vulnerable to forgery attacks. It is relatively easy to compute S^2 mod N, choose any message m/ and compute multiplicative inverse of m/ (hash value of m), compute U/ = S^2 * $m^{/-1}$ mod N and forge the signature as ($m^{/-1}$, U/, s) without knowing the factorization of N.

Advantage of M.S.H. Biswas signature:

The signature is generated using one part of hashed messsage, a generator and random padd computing equation of R(R+G) = C*U modulo two step security key. Where R is a quadratic rsudue modulo K_c and C is pair of ciphertext in context of M.S.H. Biswas cryptosystem. It is strong aginst man-in-middle attack, forgery attack. It does not rquire to compute four roots. It require less timecomplexity compare to Michael O. Rabin public key signature scheme.

4 conclusion

The proposed M.S.H.Biswas crypto-intensive techniques are efficient for solving four to one mapping signature.Its first objective to identify each ciphertext separately because modular arithmetic can generate same cyphertext from different plaintext. The proposed model can efficiently identify each ciphertext separately generated form modular reduction arithmetic. Its 2nd objective to verify sender and validate

message through signauture verification system where both authentication and integrity elements have been succefully deployed to implement signature scheme. Proposed key generation technique is derived from Diffie-Hellman key-exchange protocol but there was a security vulnerability in symmetric key geration stage (man in the middle attack), because it could not authenticate the participants. The proposed crypto techniques ensure security by combing exchange key with pre-negotiated key that is unknown to adversary. I left encryption scheme for future reader to make concrete (single) ciphertext which can uniquely identify similar quadratic resisdeue separately generated from different input.

5 Acknowledgement

I am very grateful to my family members who supported financially to conduct study because without their financial support, love and affection, this work could not be carried out. I am very grateful to well-wisher friends. I thank Md. Maruf Hassan for his inpiratiional advice and Dr. Md. Mostafijur Rahman (Assistant professor, Department of software Engineering, Daffodil International University) for insightful discussion during the preparation of this paper. This work is a part of thesis and research activities of Daffodil International Univeristy for academic curriculum fulfillment of MSc in software engineering.

References

[1] Michael. Rabin, probabilistic algorithm, algorithm and complexity, recent results and new directions, J. F. Traub, editor, ACADEMIC PRESS, INC. New York San Francisco, December 1976, pp. 21-40

[2] Michael. Rabin, Digitized signatures and public key functions as in tractable as factorization, Technical report MIT-LCS-TR-212, MIT la boratory for computer science, 1979

[3] J.A. Buchmann, Introduction to Cryptography, Springer, New York, 1999.

[4] J. Hoffstein, J. Pipher, J.H. Silverman, An introduction to mathematic cal cryptography, Springer, New York, 2008

[5] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Ap plied Cryptography, CRC Press, Boca Raton, 1997.

[6] B. Schneier, Applied cryptography, Wiley, 1996

[7] H.C. Williams, A modification of the RSA public-key encryption proce dure, IEEE Trans. on Inform. Th., IT-26(6), November 1980, pp.726-729.

[8] Md Shamim Hossain Biswas, "A mathematical model for ascertain ing same ciphertext generated from distinct plaintext in Michael O. Rabin Cryptosystem", In: International Journal of Scientific & Engi neering Research Volume 10, Issue 6 (2019). ISSN 2229-5518, DOI: 10.14299/ijser.2019.06.08.

[9] Diffie–Hellman key exchange protocol was introduced by Malcolm John Williamson (British mathematician and cryptographer) in1974.

[10] E. Bach, J. Shallit, Algorithmic Number Theory, MIT, Cambridge Mass., 1996.

[11] D.G. Cantor, H. Zassenhaus, A new Algorithm for Factoring Polyno mials over Finite Fields, Math. Comp., Vol. 36, N. 154, April 1981, pp.587- 592

[12] M. Elia, D. Schipani, Improvements on the Cantor-Zassenhaus Factori zation Algorithm, to appear in Math. Bohem.

[13] J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cam bridge Univ. Press, 1999.

[14] J. Pieprzyk, T. Hardjono, J. Seberry, Fundamentals of Computer Secu rity, Springer, New York, 2003.

[15] D.J. Bernstein, Proving tight security for Rabin-Williams signatures, EUROCRYPT2008 (N. P. Smart, ed.), LNCS, vol. 4965, Springer, 2008, pp. 70–87.

[16] S. Galbraith, the Mathematics of Public Key Cryptography, Cam bridge Univ. Press, 2012

[17] Michele Elia∗, Matteo Piva†, Davide Schipani‡ The Rabin cryptosys tem revisited, arXiv: 1108.5935v3 [math.NT] 3 Nov 2013

[18] Jaweria Usmani, Jay Prakash , A Secure Gateway Discovery Proto col Using Rabin Signature Scheme in MANET. October 2017, In: International Journal on Communications Antenna and Propaga tion 7(5):439 DOI: 10.15866/irecap.v7i5.12581

[19] Chaoyang Li1, Xiangjun Xin2 and Xiaolin Hua, Efficient ID-based Rabin Signature without Pairings, In: International Journal of Multi media and Ubiquitous Engineering Vol.12, No.3 (2017), pp.75-80 DOI: 10.14257/ijmue.2017.12.3.08

[20] Daniel Bleichenbacher, Compressing Rabin Signatures, In: T. Oka mo to (Ed.): CT-RSA 2004, LNCS 2964, pp. 126–128, 2004. c Springer-Verlag Berlin Heidelberg 2004, Bell Labs – Lucent Tech nologies