A Novel Scheme for Digital Signatures

Maheshika W.D.M.G. Dissanayake

(Corresponding author: Maheshika W.D.M.G. Dissanayake)

Department of Computer Engineering, Faculty of Engineering, University of Peradeniya , Sri Lanka
135/1, Inner Harbour Road, Trincomalee, Sri Lanka
(Email: maheshi14d@gmail.com)

(Received June 18, 2019; Revised and Accepted Aug. 23, 2019; First Online Aug. 24, 2019)

Abstract

Digital signatures are used to confirm the identity of the sender of a digital message or a document. There are many digital signature algorithms in the world. But the need for a better signature scheme is not fulfilled yet. In this paper, a novel digital signature algorithm is presented with proving the efficiency against some kind of cyber attacks. The proposed signature scheme is based on the prime factorization and on a simple, interesting property in Mathematics. The mathematical property is the sum of 2 ancillary odd numbers is a multiple of 4. The significance of the scheme is the signature is not generated from the message, directly. The new signature scheme is very simple and fast. But, the scheme is strong as the RSA signatures in security and the scheme is faster than the RSA in some cases. We can also use hash functions with the proposed signature scheme to strong the security.

Keywords: Chosen-Message Attacks; Digital Signature Scheme; DSS; ECDSS; RSA Signatures

1 Introduction

After introducing the idea "digital signature" by Diffie and Hellman [7], the research field of digital signatures has fulfilled many important goals in the digital world. A digital signature plays a very important role in proving the identity of the correct entity in E-Transactions such as E-Commerce and E-Voting. In traditional document, the signature is a part of the document. But, when someone sends a digital document, the message and the signature send separately. In conventional signature, there is a one- to-many relationship between a signature and documents. In digital signature, there is a one-to-one relationship between a signature and a document. That is each digital document needs a new signature. As the definition of digital signature, it is a cryptographic primitive which is fundamental in authentication, authorization and non-repudiation [2].

The rest of the paper is organized as follows: Section 2 describes some definitions which are important to understand the introduced digital signature scheme. After the preliminaries, in Section 3, Related Works with RSA Digital Signature Scheme, DSS and ECDSS are discussed briefly. The new signature scheme with two examples is presented in Section 4. The Section 5 discusses the security analysis of the introduced signature scheme. The computational complexity is presented in Section 6.

2 Preliminaries

In this section, we give some definitions, theorem, and attacks.

Definition 1. *The set of integers* $\{0, 1, 2, 3, \cdots, n-1\}$ *is defined as the integers* mod n *and denoted by* Z_n.

Definition 2. *The multiplicative group of* Z_n *is* $Z_n^* = \{a \in Z_n | \gcd(a, n) = 1\}$.

Definition 3. *A structure* $(R, +, \cdot)$ *is a ring if* R *is a non-empty set and* $+$ *and* $\cdot$ *are binary operations:*

$+ : R \times R \to R,\ (a, b) \mapsto a + b;$

$\cdot : R \times R \to R,\ (a, b) \mapsto a.b.$

Such that

Addition: $(R, +)$ *is an Abelian group, that is*

Associativity: *For all* $a, b \in R$ *we have* $a + (b + c) = (a + b) + c$;

Zero Element: *There exists* $0 \in R$ *such that for all* $a \in R$ *we have* $a + 0 = 0 + a = a$;

Inverses: *For any* $a \in R$ *there exists* $-a \in R$ *such that* $a + (-a) = (-a) + a = 0$;

Commutativity: *For all* $a, b \in R$ *we have* $a + b = b + a$.

Multiplication:

Associativity: *For all* $a, b \in R$ *we have* $a.(b.c) = (a.b).c$;

Addition and Multiplication together:

for all $a, b \in R$ *we have* $a.(b + c) = a.b + a.c$ *and* $(a + b).c = a.c + b.c$;

Definition 4. *A secure digital signature scheme is a triple,* $S = (KeyGeneration, Sign, Verify)$ *of algorithms which are defined as follows:*

KeyGeneration *takes as an input the unary representation of the security parameter* (1^n) *and outputs a private signing key sk and a public verification key pk.*

Sign *takes as input a signing key sk, message m and outputs a signature s.*

Verify *is a deterministic algorithm, which is input of a public key and a message-signature pair (m,s) outputs 1(accept) or 0 (reject).*

S is correct if for all public key and private key pairs generated by KeyGeneration, then, $Pr[Verify(pk, m, Sign(sk, m)) = 1] = 1$.

Theorem 1. *(Euler's 1st Theorem) If a and n are coprime then ,*$a^{\phi(n)} \mod n \equiv 1$

Theorem 2. *(Euler's 2nd Theorem) If* $n = p \times q$, $a < n$, k *is an integer,then* $a^{k \times \phi(n)+1} \mod n \equiv a$; *Here it is removed that a and n are coprime.*

Attack 1. *(Key-Only Attack) The adversary knows only the signer's public key. In this attack model, the adversary needs to create signer's signature to convince verifier that the message is coming from the signer (correct entity).*

Attack 2. *(Message Attacks) The adversary is able to examine signatures corresponding either to known or chosen messages.*

3 Related Works

There are many digital signature schemes have been introduced by researchers in recent decades. According to Diffie and Hellman scheme [7], signer's signature for a message m depends on m and on signer's secret key. Anyone can only verify the validity of the signature using the signer's public key. But, they can't create signer's signature. El-Gamal introduced a practical signature scheme in 1985 [8]. The signature scheme based on the discrete logarithm problem and there are two signatures in the signing process. Hence, in the verifying process, two functions are compared for the verification. Miller and Kobitz [9], [10], introduced elliptic curve scheme with greater security than schemes based on factorization problem and discrete logarithm problem.

S. Goldwasser, S. Micali and R. L. Rivest introduced a secure signature scheme against to adaptive chosen message attacks [1] in 1988. The scheme is stronger in security and is based on the factorization problem and "claw-free" permutation pairs. A digital signature scheme which is not trap-door type was introduced by Goldwasser, Micali and Yao [3] in 1983. Recently, Naor, Shenhav and Wool introduced a signature scheme using Fractal Merkle tree tranversal [13]. Their signature scheme is an implementation of Merkle's one-time signature scheme [14]. A signature scheme with message recovery using knapsack based elliptic curve cryptography was introduced by Ramasamy and Prabakar [22]. The scheme is secure from private key derivation, forged signature generation and digital message recovery.

Here we discuss three signature schemes, RSA Digital Signature Scheme, DSS and ECDSS further more.

3.1 RSA Digital Signature Scheme [6]

RSA Digital Signature Scheme is the most used practical signature scheme. The core of the RSA digital signature scheme is the RSA cryptosystem idea (RSA public key cryptosystem was introduced by R.L. Rivest, A. Shamir and L. Adleman in 1978). Here, public and private keys are generated by the sender. The main disadvantage of RSA signature scheme is, the scheme is not sufficiently fast for many applications. The scheme is as follows:

1) Two large prime numbers are generated. Let p and q.

2) Modulus n is generated by multiplying p and q.

3) The totient of n is $\phi(n) = (p-1).(q-1)$ is calculated.

4) Private Key: A prime number d is selected. Where $3 \leq d \leq \phi(n)$ and $gcd[d, \phi(n)] = 1$; gcd means greatest common divisor.

   Public Key: The inverse of d with respect to $\mod \phi(n)$ is calculated. The sender uses his private key d to create a signature for message m.

   The signature: $s \equiv m^d \mod n$.

5) The message m and the signature s are sent.

6) The receiver uses to verify the signature by comparing m and $s^e \mod n$.

In security, there is a serious attack on the RSA signatures "Chosen – Message Attack". This attack uses the multiplicative property to break the scheme.

3.2 Digital Signature Standard (DSS)

Digital Signature Standard is based on the discrete logarithm problem and was adopted by the National Institute of Standards and Technology (NIST). It is an efficient variant of the El-Gamal Signature Scheme with some ideas from the Schnorr signature scheme.

1) Choose a prime p between 512 and 1024 bits in length. The number of bits in p must be a multiple of 64.
2) Again choose a prime number q with 160 bits of length as q divides $(p-1)$.
3) Uses two multiplication groups $< Z_p^*, \times >$ and $< Z_q^*, \times >$. The second multiplication group is a subgroup of the first multiplication group.
4) Create e_1 to be the qth root of 1 mod p. Choose a primitive element $e_0 \in Z_p$ and calculate $e_1 = e_0^{(p-1)/q} \mod p$.
5) Choose a private key d and calculate $e_2 = e_1^d$. The public key is (e_1, e_2, p, q).
6) Select a random integer $r \in [1, q-1]$. (Need a new value for r in each time to sign a new message).
7) Calculate the first signature $s_1 = (e_1^r \mod p) \mod q$. This signature does not depend on the message.
8) Create a digest of message $h(M)$.
9) Calculate the second signature $s_2 = (h(M) + ds_1)r^{-1} \mod q$.
10) Send (M, s_1, s_2).
11) To verify the signatures, first check to see if $0 < s_1 < q$ and $0 < s_2 < q$.
12) Calculate a digest of M using the same hash algorithm used by sender.
13) Calculate $V = [(e_1^{h(M)s_2^{-1}} e_2^{s_1 s_2^{-1}}) \mod p] \mod q$.
14) If s_1 is congruent to V, the signature is valid.

If anyone uses same p for DSS and RSA, DSS is faster than RSA Signatures in computation.

3.3 Elliptic Curve Digital Signature Scheme (ECDSS)

ECDSS is the Digital Signature Algorithm (DSA) based on elliptic curves. The scheme is as follows:

1) Choose an elliptic curve $E_p(a, b)$ with a prime number p.
2) Choose another prime number q.
3) Choose any integer d as the private key.
4) Choose a point on the curve, $e_1(\ldots, \ldots)$.
5) Calculate another point on the curve, $e_2(\ldots, \ldots) = d \times e_1(\ldots, \ldots)$.
6) Now the public key is (a, b, p, q, e_1, e_2).

7) A random integer $r \in [1, q-1]$.

8) Select a third point on the curve $P(u,v) = r \times e_1(\ldots,\ldots)$.

9) Calculate the first signature s_1 by using the first coordinates of (u,v).$s_1 = u \mod q$.

10) Create a digest of message $h(M)$.

11) Calculate the second signature $s_2 = (h(M) + ds_1)r^{-1} \mod q$.

12) Send (M, s_1, s_2).

13) In verification, create two intermediate results A and B.

$$\begin{aligned} A &= h(M)s_2^{-1} \bmod q \\ B &= s_2^{-1}.s_1 \mod q. \end{aligned}$$

14) Now reconstruct the third point $T(x,y) = A \times e_1(\ldots,\ldots) + B \times e_2(\ldots,\ldots)$.

15) If $x = s_1 \mod q$, the signature is valid.

The signing and verifying processes of the scheme are fast.

4 Proposed Digital Signature Scheme

In this section, a new digital signature scheme is presented. Consider we have to sign a message m. Here, I get the message in numerical form. But, we can get any standard representation for a large message. In this signature scheme, the public key is (e,n). e is any large prime number less than n and r is a variable which is chosen by the signer. r does not depend on the message and can choose different r for same message. But, we should select r as the sum of r and m is a multiple of 4. Then find two ancillary odd numbers which are the sum is equal to the sum of r and m. The significance of the proposed signature scheme is the using of a very simple behavior of odd numbers. That is, the sum of any two ancillary odd numbers is a multiple of 4. The private key d is the inverse of e modulo $\phi(n)$. Then the small one of two ancillary odd numbers by raising it to the dth power modulo n is the signature for the message m. Now we send the message m,r and the signature for the verification.
In the verification, the verifier has the message m, r and the signature. Firstly, the signature by raising it to the eth power modulo n is calculated. Now the verifier has the small odd number of the two ancillary odd numbers. Then the verifier can get the other odd number. If the sum of these ancillary odd numbers is equal to the sum of the message and r, the signature is correct and can accept the message m. Otherwise the message m is rejected.

The signing process is as follows:

1) Choose two distinct primes p and q.

2) Compute $n = p.q$.

3) Compute $\phi(n) = (p-1)(q-1)$.

4) Select any prime number d such that $gcd(d, \phi(n) = 1$ as the private key of the sender.

5) Calculate the public key e, such that $e.d \bmod \phi(n) \equiv 1$.

6) Select any integer r such that $(m + r) \bmod 4 \equiv 0$.

7) Now find two ancillary odd numbers such that their sum is equal to $m + r$

$$a + (a + 2) = m + r;$$

a is odd.

8) Now the signature is $s \equiv a^d \bmod n$.

9) Now send $(r,\ s)$ for the message m.

The verification process is as follows:

1) Calculate $s^e \bmod n = a$.

2) Check whether $a + (a + 2) = m + r$ or not.

3) If $a + (a + 2) = m + r$, the signature is valid. Otherwise the signature is not valid.

4.1 Key Generation Algorithm

The key generation of the introduced signature scheme is same as the RSA signature's key generation (See Algorithm 1).

Algorithm 1 New Signature Scheme Key Generation

1: {
2: **select:** two large primes p and q such that $p \neq q$
3: $n \leftarrow p \times q$
4: $\phi(n) \leftarrow (p-1) \times (q-1)$
5: **select** e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$.
6: $d \leftarrow e^{-1} \mod n$
7: PublicKey $\leftarrow (e, n)$
8: PrivateKey $\leftarrow (d)$
9: **return** PublicKey and PrivateKey
10: }

4.2 Signing and Verifying

Signing: The signer creates a signature using her private key, $s = a^d \mod n$ and sends the message m, the signature s and r to the verifier.

Verifying: The verifier receives m, s and r. Then, the verifier applies signer's public key to the signature as follows:

$$s^e \mod n \equiv (a^d)^e \mod n \equiv a \mod n.$$

If $a + (a + 2) = m + r$, the signature is correct and can accept the message (See the Figure-1).

Example 1.

The signing process:

1) Let $p = 11$ and $q = 13$;

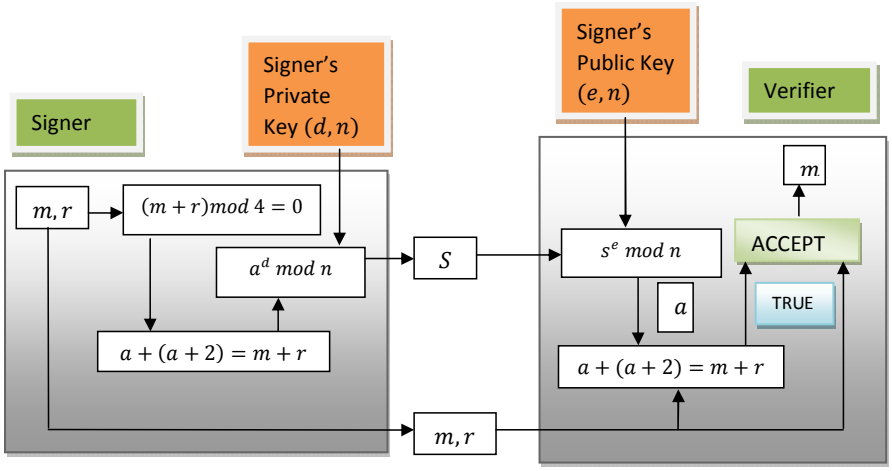

Figure 1: The signing and the verification process

2) $n = p.q = 143$*;*

3) $\phi(n) = 120$*;*

4) Select $d = 7$ *as the private key;*

5) Determine the public key, $e = 103$ *by calculating* $7.e \mod 120 \equiv 1$*;*

6) Let the message $m = 23$*. Select* $r = 5$*. Here,* $(23 + 5) \mod 4 \equiv 0$*;*

7) Now the two ancillary odd numbers are 13 and 15;

8) The signature is $s \equiv 13^7 \mod 143 \equiv 117$*;*

9) Now send (5, 117).

The verification process:

Calculate $s^e \mod n \equiv 117^{103} \mod 143 \equiv 13$*:*

$$13 + 15 = 28 = 23 + 5 = m + r.$$

The signature is correct.

Example 2.

The signing process:

1) Let $p = 83$ *and* $q = 91$*;*

2) $n = p.q = 7553$*;*

3) $\phi(n) = 7380$*;*

4) Select $d = 71$ *as the private key;*

5) Determine the public key, $e = 1871$ *by calculating* $71.e \bmod 7380 \equiv 1$*;*

6) Let the message is $m = 42$*. Select* $r = 50$*. Here,* $(42 + 50) \bmod 4 \equiv 0$*;*

7) Now the two ancillary odd numbers are 45 and 47;

8) The signature is $s \equiv 45^{71} \bmod 7553 \equiv 2273$*;*

9) Now send (50, 2273).

The verification process:

Calculate $s^e \bmod n \equiv 2273^{1871} \bmod 7553 \equiv 45$

$$45 + 47 = 92 = 42 + 50 = m + r.$$

The signature is correct.

5 Security

5.1 Key-Only Attack

The proposed signature scheme is invulnerable for Key-Only Attack as difficult to solve the discrete logarithm problem.

5.2 Chosen-Message Attack

Assume an adversary sends to sign a message (m_1) to the signer. The signer creates a signature (s_1) for the message (m_1).

$$\begin{aligned} s_1 &\equiv (a_1)^d \bmod n \\ 2a_1 + 2 &= m_1 + r_1. \end{aligned}$$

Then the signer sends (s_1, r_1) to the adversary. Now, the adversary is able to find a_1. But, he can't create $(a_1)^d \bmod n$. Because of the adversary does not know the secret key d.

Then the adversary sends to sign another message m_2 to the signer and gets (s_2, r_2). Here,

$$\begin{aligned} s_2 &\equiv (a_2)^d \bmod n \\ 2a_2 + 2 &= m_2 + r_2. \end{aligned}$$

Now, the adversary can find a_2. But he can't create $(a_2)^d \bmod n$.

In this case, the adversary can ask to sign number of messages from the signer. But, the selection of variables a_1, a_2, r_1 and r_2 are changed message by message. Therefore, it is difficult to apply Chosen-Message-Attack to the introduced signature scheme.

5.3 The Introduced Signature Scheme on the Message Digest

A strong cryptographic hash function can build up a high security for the introduced signature scheme. For an instance, if the hash function is pre-image resistant, the signature scheme is strong in security. In fact, hash functions are also speed up the encryption and decryption processes.

In the message digest Case 1 (See the Figure 2), the hashing function is used for only the message m. In the message digest Case 2 (See the Figure 3), the hashing function is used for both the message m and the small one of the two ancillary odd numbers a.

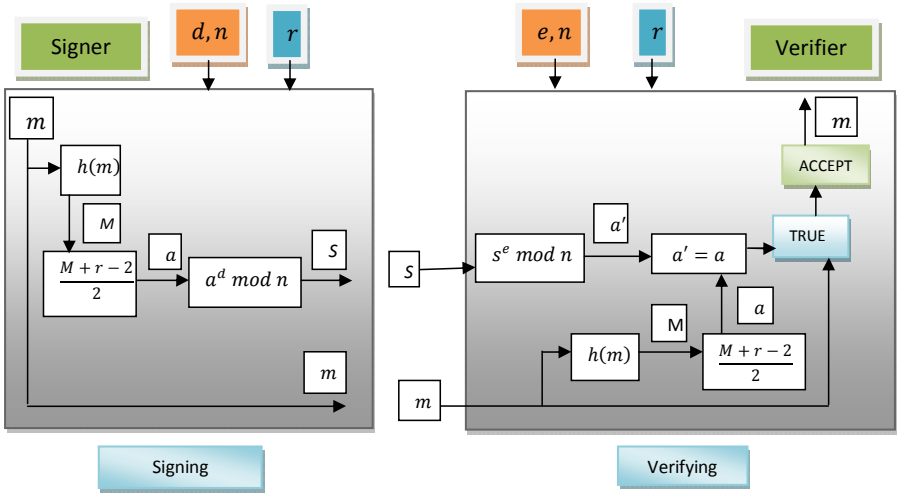

Figure 2: Message Digest- Case 01

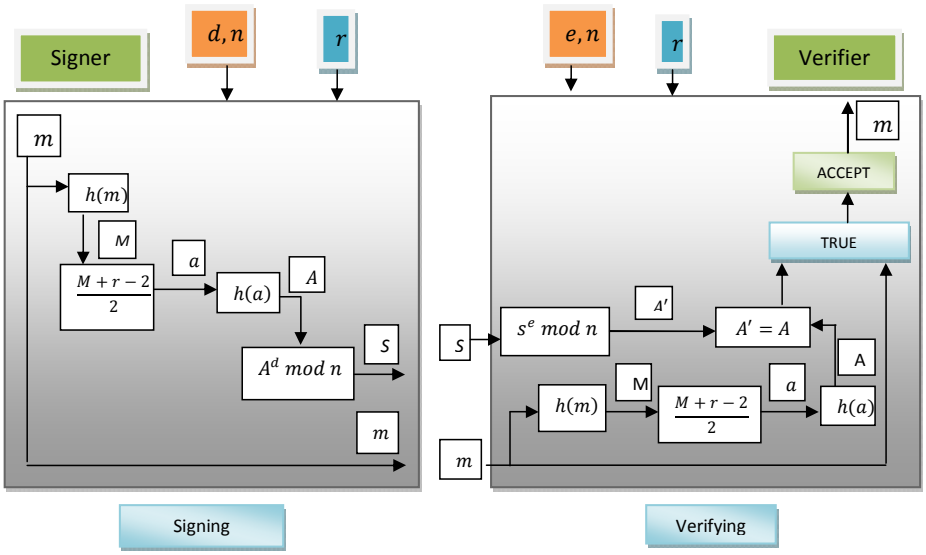

Figure 3: Message Digest- Case 02

6 Computational Complexity

The computational complexity for Key generations of the new scheme same as RSA signatures. The comparison of computational complexities for the encryption and the decryption of the introduced signature scheme and the RSA signature scheme as Table 1.

Table 1: Comparisons of computational complexities

Since, a = (m+r-2)/2 :

Cases:	**Computational complexity for encryption and decryption**
If $r \leq m$ then $a < m$	The introduced signature scheme < RSA Signature scheme
If $r > m$ then $a \geq m$	The introduced signature scheme > RSA Signature scheme

7 Conclusion

Here we have introduced a simple and practical digital signature scheme, faster than RSA signatures in some cases. The modulus of the introduced scheme is same as the RSA signatures. But, the signature does not depend directly on the message and it is not created from the message. We can also use any standard security model with the new signature scheme to increase the security.

8 Acknowledgment

I would like to thank Dr. Sandirigama M. (Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka) and Dr. Ishak M.I.M. (Department of Engineering Mathematics, Faculty of Engineering, University of Peradeniya, Sri Lanka) for providing helpful feedback and advice in this research. I also gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. I. Ali, "Comparison and evaluation of digital signature schemes employed in NDN network," *International Journal of Embedded systems and applications*, vol. 5, no. 2, pp. 15–29, 2015.

[2] M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, "Relations among notions of security for public key encryption schemes," *Lecture Notes in Computer Science*, vol. 1462, pp. 26–45, 1998.

[3] M. Bellare, O. Goldreich, S. Goldwasser, "Incremental Cryptography: The Case of Hashing and Signing," in em Advances in Cryptology – Crypto'94, Desmedt, Y.G. (Ed), LNCS 839, Springer-Verlag, Heidelberg, pp. 216–233, 1994.
[4] M. Bellare, P. Rogaway, "The exact security of digital signatures-How to sign with RSA and Rabin," in *Proceedings of Eurocrypt'96*, LNCS, Springer-Verlag, pp. 399–416, 1996.
[5] R. Cramer, V. Shoup, "Signature schemes based on the strong RSA assumption," *ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 161–185, 2000.
[6] W. Diffie, M. Hellman, "New directions in Cryptography," *IEEE Translations on Information Theory*, vol. 22, pp. 644–654, 1976.
[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol.31, pp. 469–472, 1985.
[8] D. Estes, L. Adleman, K. Kompella, K. McCurley, G. Miller, "Breaking the Ong-Schnorr-Shamir signature scheme for quadratic number fields," in *Proceedings of Crypto'85*, Springer-Verlag, pp.3-13, 1986.
[9] B. A. Forouzan, D. Mukhopadhyay, "Cryptography and Network Security," *Tata McGraw Hill Education Private Limited, India* 2nd edn, Special Indian Edition, pp. 358–376, 2010.
[10] S. Goldwasser, S. Micali, R. L. Rivest, "A digital signature scheme secure against adaptive chosen message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp.281–308, 1988.
[11] S. Goldwasser, S. Micali, A. Yao, "Strong signature schemes," *15th ACM Symposium on the Theory of Computing on Proceedings*, pp. 431–439, 1983.
[12] A. Khaled, A. Abdulbast, "A new scheme for sealed digital signatures," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 4, no. 2, pp. 231–238, 2013.
[13] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–209, 1987.
[14] X. Li, X. Shen, H. Chen, "Elgamal digital signature algorithm of adding a random number," *Journal of Networks*, vol. 6, no. 5, pp. 774–782, 2011.
[15] R. C. Merkle, "A certified digital signature," in *Advances in Cryptology – Crypto'89*, Brassard, G.(Ed), Springer, pp. 218–238, 1989.
[16] V. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology, Crypto'85*, LNCS 218, pp. 417–426, 1985.
[17] S. Mohanty, B. Majhi, S. K. Baral, "A novel time-stamped signature scheme based upon DLP," in em International Conference of Recent Advances in Information Technology on Proceedings, 2012.
[18] D. Naor, A. Shenhav, A. Wool, "One-time signatures revisited:practical fast signatures using fractal Merkle tree traversal," in *IEEE 24th Convention of Electrical and Electronics Engineers in Israel*, pp.255–259, 2006.
[19] A. Negi, P. Sharma, P. Chaudhary, H. Gupta, "New method for obtaining digital signature certificate using proposed RSA algorithm," *International Journal of Computer Applications*, vol. 121, no. 23, pp. 24–29, 2015.
[20] D. Pointcheval, "New Public Key Cryptosystems based on the Dependent-RSA Problem," in *Advances in Cryptology – Proceedings of EUROCRYPT '99*, Stern, J.(Ed), LNCS 1592, Springer – Verlag, pp. 239–254, 1999.
[21] D. Pointcheval, J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, pp. 361–396, 2000.
[22] P. R. Ramasamy, M. A. Prabakar, "Digital signature scheme with message recovery using knapsack-based ECC," *International Journal of Network Security*, vol. 12, no. 1, pp. 7–12, 2011.
[23] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signature and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.
[24] C. Schnorr, "Efficient signature generation by smart cards," in *Advances in Cryptology-Crypto'89*, Lecture notes in computer science, Springer-Verlag, pp. 161–174, 1991.
[25] C. Yuan, M. Xu, X. Si, "Research on a new signature scheme on blockchain," *Security and Communication Networks. Hindawi*, 2017.

Biography

Maheshika W.D.M.G. Dissanayake received her BSc degree in Computer Science, Mathematics and Applicable Mathematics from University of Ruhuna, Sri Lanka. She has finished the MPhil in Computer Engineering (Cryptography and Network Security) at Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka. Her research interests include Cryptography and Network Security.