Implementation of an Efficient Blind Signature Scheme

Aye Aye Thu and Khin Than Mya

Abstract—**Nowadays, security of the user's data is the major problem over internet. Privacy is one of the basic rights for individuals and institutions that need to preserve their confidentiality. Blind signature scheme are widely used for various applications of E-commerce like digital payments systems and electronic voting system where to maintain the privacy of customer is necessary. Blind signature is needed in applications that guarantee the anonymity of the participants. We propose blind signature scheme based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) and it satisfies the requirements of blindness, correctness, unforgeability and untraceability. The propose scheme intended to develop the blind signature scheme with improve performance as compared to the other existing schemes. Most of blind signature scheme are very high at computational overhead and memory usage problem. This scheme desired to reduce time consuming problem by using Elliptic Curve Cryptography (ECC). The proposed scheme can apply in electronic voting system or cash system.**

Index Terms—**Blind signature, DLP, ECC, ECDLP, e-commerce, electronic voting system, ECDSA.**

I. Introduction

Nowadays people can accomplish their daily tasks, such as banking tractions, without leaving their homes by using Internet. People always do shopping through internet, which has increased the growing rate of the e-commerce. Now, the challenge is appeared and it is need to improve the security and anonymity of the people in dangerous environment. So, we use the concept of blind Digital Signature (BDS) presented in.

Blind Signature is a form of digital signature in which the message is blinded before it is signed, in order to allow the requester to get a signature without giving the signer any information about the actual message or the resulting signature.Several blind signature schemes are proposed in the literature.

Elliptic Curve Cryptosystem is accepted to be a secure and efficient public-key cryptosystem. In this paper, we would like to focus on the security of ECC relying upon the difficulty of solving the discrete logarithm problem.

The objective of this paper isto propose blind signature scheme based on Elliptic Curve Discrete Logarithm Problem by applying the strength of the ECC. It can fulfill the requirements of blind signature scheme like correctness, blindness, unforgeability and intraceability. The system will provide comparison of proposed blind signature scheme to the schemes presented in previous research. It is also show the computation cost of proposed scheme. It is intend to improve the performance of voting system or other applications by applying proposed blind signature scheme.

The structure of the paper is as follows: Section IIdiscusses theconcept of elliptic curve cryptosystem and Blind Signature Scheme. Section III explains an overview of previous approaches on blind signature scheme.In Section VI, propose blind signature is presented. Section V providessecurity analysis of the system. The performance of this scheme is examined in Section VI. Finally, conclusions and future work are presented in Section VII.

II. Elliptic Curve Cryptosystem

There are three types of public key cryptosystem are considered secure and efficient.They are

1) Integer Factorization System
2) Discrete Logarithm System
3) Elliptic curve Cryptosystem

Elliptic curves are used to construct the public key cryptography system.The private key *d* is randomly selected from [1, *n*-1], where n is integer. Then the public key *Q* is computed by dP, where *P*, *Q* are points on the elliptic curve. Like the conventional cryptosystems, once the key pair (*d*, *Q*) is generated, a variety of cryptosystems such as signature, encryption/decryption, and key management system can be set up.Computing *dP* is denoted as scalar multiplication. It is not only used for the computation of the public key but also for the signature, encryption, and key agreement in the ECC system. ECC is provided with strong processing power, less storage space, less power consumption [1].

Elliptic Curve on a prime field $E\ (F_p)$ is

$$y^2 mod\ p = x^3 + ax + b\ mod\ p$$

where $4a^3 + 27b^2 \neq 0$

$G = (x_G, y_G)$ is a base point on $E(F_p)$.Main operation in ECC is Point Multiplication [2]. Point Multiplication is achieved by two basic curve operations:

1) Point Addition, $L = J + K$,

$$\lambda = (y_k - y_j / x_k - x_j)\ mod\ p,$$

$$x_R = \lambda^2 - x_j - x_k\ mod\ p \text{ and}$$

$$y_R = \lambda(x_j - x_R) - y_j\ mod\ p$$

2) Point Doubling, L = 2J,

$$\lambda = (3x^2 + a/2y_p)\ mod\ p,$$

$$x_R = (\lambda^2 - 2x_p) mod\ p \text{ and}$$

$$y_R = (\lambda(x_p - x_R) - y_p\ mod\ p$$

Manuscript received September10, 2014; revised December 2, 2014.

Aye Aye Thu is with the Hardware Department, Computer University, Hinthada, Myanmar (e-mail: suchiq13@gmail.com).

KhinThan Mya is with University of Computer Studies (Yangon), Myanmar (e-mail: khinthanmya@gmail.com).

DOI: 10.7763/IJIMT.2014.V5.556

Example: If d = 23; then,

$$dP = 23J= 2(2(2(2J) + J) + J) + J$$

In this system, we don't use the whole process of elliptic curve cryptosystem's encryption and decryption techniques. The system just used ECDLP multiplication techniques. It is difficult to solve at calculation.

1) ECDLP (Elliptic curve discrete logarithm problem).

Given an elliptic curve E defined over a finite field F_q, a point $P \in E(F_q)$ of order n, and a point $Q \in E$, find the integer $d \in [0, n\text{-}1]$ such that $Q=dP$. The integer d is called the discrete logarithm of Q to the base p denoted as $d= \log_p Q$. If d is sufficient large, then it is infeasible to compute it.

The ECDLP is considered to be more difficult to solve than the IFP (Integer Factorization Problem) and the DLP (Discrete Logarithm Problem) [3].

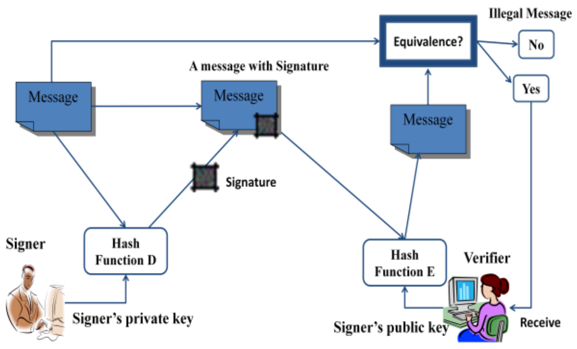

Fig. 1. Digital signature.

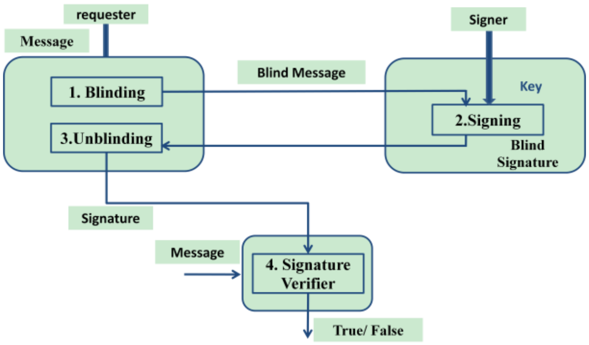

Fig. 2. Flow of blind signature.

2) Digital Signature. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. In the digital signature scheme, there are two participants namely the signer and the verifier. The signer first uses a private key to sign a message and then sends this signature to the verifier. After the verifier receives the signature, he/she can use a public key to verify the Legitimacy of the signature.

3) Blind Signature Scheme, Blind signature is a kind of digital signatures. Unlike a normal digital signature scheme, in a blind signature scheme; a signer signs a message without knowing what the message contains. The blind signature can protect people's privacy with in a network, especially in an electronic cash payment system, e-commerce and electronic voting system. In the blind signature scheme, there are three participants, namely, the requester, the signer and the verifier [4].

The differences of blind signature and digital signatures are shown in Fig. 1 and Fig. 2.

- Short Illustration of Blind Signature

Blind signature schemes consist of four phases. They are blinding, signing, unblinding and verification phases [5].

1) Blinding Phase

The sender chooses a random number called a blind factor to blind his message such that the signer will not be able to view the contents of the message.

2) Signing Phase

When the signer gets the blinded message, he encrypts the blinded message using his private key and then sends back the blind signature to the sender.

3) Unblinding Phase

The sender uses the blind factor to recover the signer's digital signature from the blinded message.

4) Verification Phase

Anyone can use the signer's public keys to verify whether the signature is authentic or not.

III. Related Works

Today, blind signatures are widely used for constructing the infrastructures of many communication services such as electronic voting or electronic cash systems.The first scheme proposed by Chaum, it based on RSA signature [6]. In 2005, Camenisch *et al.* [7] proposed a novel blind signature scheme based on the discrete Logarithm problem. But it fails the untraceability. AbhijitSaml and AnimeshChhotaray [8] proposed novel blind signature based upon ECDLP that it does not satisfy computational overhead problem.

Morteza and Ali [9] proposed an efficient untraceable blind signature scheme. They declared that their blind signature scheme has a performance compared to Camenisch *et al.*

Jena *et al.* [10] proposed two novel blind signature schemes; nevertheless there was no reasonable proof for correctness of their schemes.

The advantages of myproposd system solved the problem of memory space and computing power by reducing random factor and calculation of multiplication with smaller key sizes.

IV. The Proposed Blind Signature Scheme

The proposed BDS scheme was derived from a variation of the ECDSA (Elliptic Curve Digital Signature Algorithm).Moreover, the scheme is based on solving the difficulty of elliptic curve discrete logarithm problem.The proposed BDS system contains five phases. They are

- Initialization
- Blinding
- Signing
- Unblinding and
- Verifying

In my proposed scheme, used the elliptic curves over the F_p prime field, which has been suggested by National

Institute of science and Technology (NIST) [11]. Elliptic curve domain parameters over F_p are defined as follow:

$$T= (p, F_p, a, b, G, n, h) \quad (1)$$

P is an integer specifying the F_p finite field; $a, b \in F_p$ are integers specifying the elliptic curve $E(F_p)$ defined by

$$E(F_p) : y^2=x^3 + ax + b \ (mod\ p) \quad (2)$$

where $G= (x_G, y_G)$ is a base point on $E(F_p)$, n is primenumber defining the order of *G*, and h is an integer defining the cofactor: $h=\#E(F_p)/n$.The system consists of three participants: They are requester, signer and verifier.The signer declares the necessary information in the initialization step. The requester submits a blinded version of the message to the signer to get the signature of a message at the blinding phase. The signer signs the blinded message and sends the result back to the requester at the signing phase. The requester extracts the signature in the unblinding phase. Finally, the validity of the signature is verified. The details of these phases are describedbelow.

A. Initialization Phase

The signer defines the elliptic curve domain parameters *T*, defined as in (1). Then, for each request, an integer *k* is randomly selected by the elliptic curve point *R*' is calculated.

$$R' = kG = (x_1, y_1) \quad (3)$$

$$r' = x_1\ (mod\ n) \quad (4)$$

The Signer checks ($r' \neq 0$),

Otherwise signer selects another *k* randomly and repeats till his find *r*′. If the result is true; the signer sends the elliptic curve point R′ to the requester.

B. Blinding Phase

To blind the message m, the requester needs the elliptic curve domain parameters *T* of the signer. And then calculates *r*′ from the elliptic curve point *R*′. The requester randomly chooses integer *v* and

$$\text{Compute } R=v^{-1}R'=(x_0, y_0) \quad (5)$$
$$r=x_0\ mod\ n$$

Then calculate *r* from the elliptic curve point *R*.

Requester generates the blinded message m and sends it back to the signer for signing operation:

$$m'= H(m)\ r^{-1}r'v \ \ (mod\ n) \quad (6)$$

where *H* is the Hash function and we use SHA-1 [6] algorithm as the hash function.

C. Signing Phase

The signer receives the blinded message *m*′ from the requester; he generates the blind signature *s* by following steps.

1) Signer randomly chooses integer *d* in the range (1, *n*-1)
2) Then calculates elliptic curve point

$$Q = dG=(x_Q, y_Q) \quad (7)$$

3) Signer check (k, m) already exists in database?
4) If exist, go to the initialization step and re-select *k*.
5) Otherwise, compute

$$s= dm' + kr'(mod\ n) \quad (8)$$

Next, he sends the message-signature pair (m ′, s) pair back to the requester.

D. Unblinding Phase

When the requester receives the blind signature *s* from the signer, the unblinding operation is needed to obtain the digital signature *s*′ on message m.

$$s'=sv^{-1}r'^{-1}r\ (mod\ n) \quad (9)$$

The requester needed to verify the blind signature and message are intended to him.

E. Verifying Phase

Digital signature of (*s*′, *R)* on the message m can verify by examining the correctness of the equation

$$s'G^? = QH(m) + Rr \quad (10)$$

Table I defines the notifications used in this paper and Table II illustrates the flow of the proposed blind signature.

TABLE I: NOTATIONS AND SYSTEM PARAMETERS

T	Elliptic curve domain parameter
a,b	Coefficient defining the elliptic curve
m	Message
G	Base point
n	Order of *G*, a prime number
h	Hash value
m′	Blinded message
s	Blind signature
s′	Signature
r′	*x* coordinate of *R*′
r	*x* coordinate of *R*
R, R′	Points on Elliptic Curve
d	Private key of the Signer

V. SECURITY ANALYSIS

This section examines the properties of blind signature to fulfill security requirements. The security of the proposed method is based on the difficulty of the ECDLP.

A. Proof of Blindness

We used r^{-1}, v^{-1} and *v* in the blind phase. The signer can never find r^{-1}, v^{-1} and *v* so blind property is correctly achieved. Blindness is the first important property in a blind signature. The requester calculates (5) and generates *m*′ defined in (6).

Hence, the signer cannot know the message m.

B. Proof of Unforgeability

No one can forge (m_1', R_1, s_1') because the elliptic curve discrete logarithm is difficult to solve. We assume three situations as follows.

$$\text{Ats}_1'G^? = QH(m) + R_1r_1$$

Situation 1: If attacker tried to fake m_1', R_1 he/she cannot obtain s_1' becausethey don't know s_1'. *Situation 2*: If attacker gets s_1' and m_1' he/she cannot obtain R_1. *Situation 3*: If attacker tries to fake s_1', R_1 he/she cannot obtain m_1'. It is also an elliptic curve discrete logarithm problem and difficult to solve.

TABLE II: THE FLOW OF THE PROPOSED BLIND SIGNATURE

Requester	***Signer***
Blinding Phase	***Initialization Phase***
Calculates r' from the elliptic curve point R' Integers v (randomly selected in the range (1, n-1)) Compute $R=v^{-1}R'=(x_0,y_0)$ $r=x_0$ mod n (blinding factor) $m'=H(m)\,r^{-1}r'v \ (mod\ n)$ * h is the hash function with SHA-1 algorithm $\xleftarrow{R'}$ $\xrightarrow{m'}$	Publish $E_p\,(a, b)$ Base Point $G = (x, y)$ Integer k (randomly selected in the range (1, n-1)) $R' = kG = (x_1, y_1)$ and Compute $r' = x_1$ (mod n) if $(r' \neq 0)$, Else if choose another k and find r'
Unblinding	***Signing Phase***
$s'=sv^{-1}r'^{-1}r \ (mod\ n)$ $\xleftarrow{(s,m')}$ The unblinding operation is needed to obtain the digital signature (s', R) on message m.	*Private key* = *d* (d randomly selected in the range (1, n-1)) *Public key* = $Q = dG = (x_Q, y_Q)$ Check (k, m') in database? If yes, re-select k. Otherwise, compute $s= dm' + kr'(mod\ n)$
Verifying Phase Any party who has the elliptic domain parameter T of the Signer and the public key of the signer can verify the signature is genuine. $s'\,G \overset{?}{=} QH(m) + Rr$	

TABLE III: CORRECTNESS PROOF OF THE PROPOSED SCHEME

$$s'\,G = QH(m) + Rr$$

$$s'G - Rr = QH(m)$$

$$sv^{-1}r'^{-1}rG - Rr = QH(m)$$

$$[dm' + kr']\,v^{-1}r'^{-1}rG - Rr = QH(m)$$

$$[dm'v^{-1}r'^{-1}rG + kr'v^{-1}r'^{-1}rG] - Rr = QH(m)$$

$$[d[H(m)r^{-1}r'v]v^{-1}r'^{-1}rG] + [kr'v^{-1}r'^{-1}rG] - Rr = QH(m)$$

$$[dH(m)G] + [kv^{-1}rG] - Rr = QH(m)$$

(Substitute $kG=R'$ and $Q=dG$)

$$QH(m) + R'v^{-1}r - Rr = QH(m)$$

(*Substitute* $R= R'v^{-1}$)

$$QH(m) + Rr - Rr = QH(m)$$

$$QH(m) = QH(m)$$

C. *Proof of Correctness*

The correctness of our scheme can be easily verified as follows Table III. The verifier has only digital signature (r, R, s') of message m for verification defined in (10).

D. *Proof of Unlinkability*

The signer will keep a set of records (k, R', m', s) for each blind signature requested. When the message m and its signature (s', R) are revealed to the public.

The revealed message-signature pair (m, s', R)

$$s'G= QH(m) + Rr$$

The signer tries to check the correctness of equation to trace the blind signature. The signer needs to have the blind factor (r, v, v^{-1}, r^{-1}) in addition to the values of points R, R'. However, he only has the following information for calculation (k, R', m', s, m, s', R). And there are only three equations including the blind factor defined in (5), (6) and (9).

There is no way for the signer to trace the blind signature by checking the correctness of equation from (10).

The privacy of the user is correctly protected and the signer is not able to derive the link between a signature and the corresponding instance of signing protocol which produced that signature.

TABLE IV: UNIT CONVERSION OF VARIOUS OPPERATIONS IN TERMS OF TMUL

Time complexity of an operation Unit	Time complexity in terms of Multiplication
T_{EXP}	240 T_{MUL}
$T_{EC\text{-}MUL}$	$29T_{MUL}$
$T_{EC\text{-}ADD}$	$0.12T_{MUL}$
T_{ADD}	negligible
T_{INV}	0.073 T_{MUL}

VI. PERFORMANCE EVALUTION

The following notations are used to estimate the time complexity. Any digital signature is compared on the basics of number of operations rather on the basics of time complexity from (4).

T_{MUL}: the time required for the modular multiplication.

T_{EXP}: the time required for the modular exponentiation.

T_{INV}: the time required for the modular inversion.

T_{ECMUL}: the time required for the multiplication of as scalar and an elliptic curve point.

T_{ECADD}: the time required for the addition of two points over an elliptic curve.

The time complexity of the various operations units in terms of time complexity of a modular multiplication is shown in Table IV.

The following Table V compares our scheme with two other standard schemes. The required computational cost for all schemes has been estimated by accumulating execution times of all the required operations.

TABLE V: REQUIRED TIME COMPLEXITY IN UNIT OF TMUL

Schemes	Time Complexity	Rough Estimation
Morteza & Ali [9]	$7T_{EC\text{-}MUL}$+$6T_{MUL}$+3 $T_{EC\text{-}ADD}$+ T_{INV} +3 T_{ADD}	203.57 T_{MUL}
Abhijit Sal & Animesh Chhotaray [8]	$14T_{ECMUL}$+$2T_{MUL}$+$8T_{ECADD}$+2 T_{INV}	407.106 T_{MUL}
Proposed Scheme	$6T_{ECMUL}$+$8T_{MUL}$+T_{ECADD}+3 T_{INV}	182.339 T_{MUL}

Note that the time for computing modular addition is ignored because it is smaller than time for modular multiplication and modular inverse. So, my proposed scheme will be reducedefficiently at calculation time.

TABLE VI: COMPARISION BETWEEN SCHEMES

Schemes	Blind Factors	Security Assumption	Most Costly Primitive
Morteza & Ali [9]	3	ECDLP	Blindness
AbhijitSal & Animesh Chhotaray [8]	2	ECDLP	Blindness
Proposed Scheme	1	ECDLP	Blindness

Table VI shows the number of blind factor, security assumption and describes the computational cost of blind signature for each of the three schemes. Moreover, they can give same degree of security. In real, it is needed to do a blind signature scheme efficiently, using only one blind factor. By comparison, my proposed scheme is more suitable for reduce computational overhead and memory usage problem.

The minimum requirement of time complexity for ECDLP based blind signature is given by $1T_{EC\text{-}MUL}$ + $1T_{EC\text{-}ADD}$+ $1T_{MUL}$ + $1T_{INV}$ or equal to $30.19T_{MUL}$ for overall process. To estimate our scheme, we use the following formulas:

speedup=

$$\mathbf{100}\% - \left(\frac{\boldsymbol{Timecomplexityofourscheme(inT_{MUL}) - 30.19T_{MUL}}}{\boldsymbol{Timecomplexityofourscheme(inT_{MUL})}}\right) \times \mathbf{100}\%$$

Any scheme can cmpare this formaula with 100% efficiency. The speedup of schemes can be calculated as below.

1) (Morteza & Ali) speedup

$$= 100\% - \left(\frac{203.57 - 30.19}{203.57}\right) \times 100\% = 14.83\%$$

2) (AbhijitSal&AnimeshChhotaray) speedup

$$= 100\% - \left(\frac{407.106 - 30.19}{407.106}\right) \times 100\% = 7.41\%$$

3) (Proposed Scheme) speedup

$$= 100\% - \left(\frac{182.339 - 30.19}{182.339}\right) \times 100\% = 16.55\%$$

From Table V and the above estimation, it is explain that my proposed scheme improves and increases entirely the efficiency for all operations.

VII. CONCLUSION

The proposed scheme can be applied in electronic voting system, electronic cash system and electronic commerce and so on. In a electronic voting system, it canprovide basis security requirements and the voter's identity remain hidden.Moreover, it may satisfy the requirements of a blind signature scheme.ECDLP based blind signature difficult to compute for attacker and can provide efficient performance thanthe first generation public key techniques (RSA and Diffie-Hellman). My proposed scheme shows efficiency owing to lower storage requirements and reduces the time complexity, which is due to use of ECDLP.

ACKNOWLEDGMENT

Much gratitude is owed to Dr.Mie Mie ThetThwin, Rector, University of Computer Studies, Yangon (UCSY), for her kind permission to carry out this paper. I would like to express grateful thanks to my teacher Dr.KhinThan Mya (UCSY), for her helpful advice, encouragement and giving me the opportunity.

REFERENCES

[1] M. S. Anoop. (2001). Elliptic Curve Cryptography. *An Implementation 2001*. [Online]. Available: http://www.Infosecwriters .com/text_resources/Elliptic_Curve_Anno Ms.pdf

[2] N. Koblitz, A. J. Menezes, and S. A. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes and Cryptography*, vol. 19, NO. 2-3, pp. 173-193, 2000.

[3] F. Liu, "A Tutorial on elliptic curve cryptography," Brandenburg Technical University of Cottbus,Computer Networking Group, 2004.

[4] S. A. Vanstone, "Elliptic curve cryptosystem the answer to strong, fast public key cryptography for securing constrained environments," *Information Security Technical Report*, vol. 2, no. 2. pp.78-87, 1997.

[5] F. G. Jeng, T. S. Chen, and T. L. Chen, "A blind signature scheme based on elliptic curve cryptosystem," *Journal of Networks*, vol. 5, pp. 921-927, August 2010.

[6] D. Chaum, "Blind signatures for untraceable payments," in *Proc. CRYPTO 82*, New York: Plenum Press, 1983, pp. 199-203.

[7] J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," *Advances in Cryptography EUROCRYPT Lecture Notes in Computer Science*, vol. 950, pp. 428-432, 1994.

[8] A. Samal and A. Chhotaray, "A novel blind signature based upon ECDLP," Thesis, Department of Computer Science and Engineering, Orissia, Japan, 2010.

[9] M. Nikooghadam and A. Zakerolhosseini, "An efficient blind signature scheme based on the elliptic curve discrete logarithm problem," *International Journal of Information Security* , vol. 1, no. 2 , pp. 125-131, July 2009.

[10] D. Jena, S. Jena, and B. Majhi, "A novel untraceable blind signature based on elliptic discrete logarithm problem," *International Journal of Computer Science and Network Security*, pp. 269-275, 2007.

[11] (October, 2011). SEC 1: Elliptic Curve Cryptography. Standards from Efficient Cryptography Group. [Online]. Available: http://www.secg.org/.

Aye Aye Thu was born in Hinthada, Ayerawady Division, Myanmar. She received the B.C.Tech and B.C.Tech (Hons.) degrees from Computer University, Hinthada, Ayerawady Division, Myanmar in 2007, the master of computer technology (M.C.Tech) degree from Computer University, Mawlamyine, Mon State, Myanmar in 2010. She is a tutor in the Hardware Department at the Computer University, Hinthada, Myanmar. She has published 4 research papers in various national/international conferences and journals. She is currently attending her Ph.D at University of Computer Studies, Yangon, Myanmar. Her research interests mainly include network security and cryptography.