Faster Scalar Multiplication Algorithm to Implement a Secured Elliptic Curve Cryptography System

Fatema Akhter, *Student Member, IEEE*

***Abstract*—Elliptic Curve Cryptography provides similar strength of protection comparing other public key cryptosystems but requires significantly smaller key size. This paper proposes a new faster scalar multiplication algorithm aiming at a more secured Elliptic Curve Cryptography scheme. This paper also proposes a novel Elliptic Curve Cryptography scheme where maximum length random sequence generation method is utilized as data mapping technique on elliptic curve over a finite field. The proposed scheme is tested on various bits length of prime field and key sizes. The numerical experiments demonstrate that the proposed scheme reduces the computation time compared to conventional scheme and shows very high strength against cryptanalytic attack particularly random walk attack.**

Keywords*—Cryptography; Elliptic curve cryptography; Scalar multiplication; Random walk; Elliptic curve discrete logarithm problem

I. Introduction

Recently, *Elliptic Curve Cryptography (ECC)* [1], [2] has gained popularity in the field of public key cryptosystem for its smaller key size, faster processing time and robust security against popular cryptanalytic attacks comparing to other *Public Key Cryptography(PKC)* systems. These features engrossed the attentions of manufacturers of small processing devices like smart cards, Raspberry computers, wireless devices, pagers, smart phones and tablets [3]. ECC is mainly used for key exchange, digital signature and authentication [4] . However, it can be applicable to any security applications where computational power and integrated circuit space is limited.

The unique idea of ECC was proposed independently by Koblitz [5] and Miller [6] in 1985. Since then on, a lot of attention has been paid to ECC, it has been studied thoroughly and still there are lots of scopes of research. Several researches are conducted to reduce the computational cost or to increase the level of security of the ECC scheme. For example, Abdalhossein Rezai [7] et al. proposed an efficient scalar multiplication algorithm for ECC using a New Signed-Digit Representation. D. Sravana Kumar [8] et al. proposed a new encryption algorithm using Elliptic Curve over finite fields. F. Amounas [9] et al. proposed an algorithm to generate a data sequence and applied it on ECC encrypted message over the finite field $GF(p)$. During this time, cryptanalysis of ECC went on with the same pace.

This paper studies the basics of ECC and some existing algorithms on it to move forward to the proposed approach. This paper proposes a faster scalar multiplication algorithm and a new scheme for ECC. In addition to these, a data mapping technique on elliptic curve over a finite field is proposed using maximum length random sequence generation algorithm. Within our knowledge, the same approach has not yet been reported neither for ECC scheme nor for scalar multiplication algorithm. The message to *points on elliptic curve* mapping is done using random sequence generation algorithm that increase the security of the proposed scheme to higher level.

The rest of the paper is organized as follows: Section II describes the preliminary studies for proposed approach. Section III describes the proposed ECC scheme and scalar multiplication algorithm along with the necessary algorithms needed to implement the proposed ECC scheme. Section IV presents the experimental results and discussions for the proposed approach. Section V provides the conclusion and future work.

II. Preliminary Study

In this section, preliminary theories and studies for ECC scheme are briefly described. An elliptic curve E over $\mathbb{F}_p$, for a prime $p > 3$ is defined with the short Weierstrass equation [10]

$$E : y^2 = x^3 + ax + b \text{ with } x,y,a,b \in \mathbb{F}_p \quad (1)$$

where a,b are integer modulo p, satisfying: $4a^3 + 27b^2 \neq 0 \mod p$, and include a point $\mathcal{O}$ called *point at infinity*. The basic condition for any cryptosystem is that the system is closed, i.e., any operation on an element of the system results in another element of the system. In order to satisfy this condition for elliptic curves, it is necessary to construct nonstandard *addition* and *multiplication* operations.

A. Geometric Rules of Addition

Let $P(x_1,y_1)$ and $Q(x_2,y_2)$ be two points on the elliptic curve E. The sum $R(x_3,y_3)$ is defined as: first draw a line through P and Q, this line intersects the *elliptic curve* at a third point. Then the reflection of this *point of intersection* about *X-axis* is R which is the sum of the points P and Q. The same *geometric interpretation* also applies to two points P and P, with the same *X-coordinate*. The points are joined by a *vertical line*, which can be viewed as also intersecting the curve at the *infinity point*. We, therefore, have $P + (-P) = \mathcal{O}$, the identity element which is the *point at infinity*.

B. Point Doubling

First, draw the *tangent line* to the *elliptic curve* at P which intersects the curve at a point. Then the reflection of this point about *X-axis* is R. As an example the addition of two points

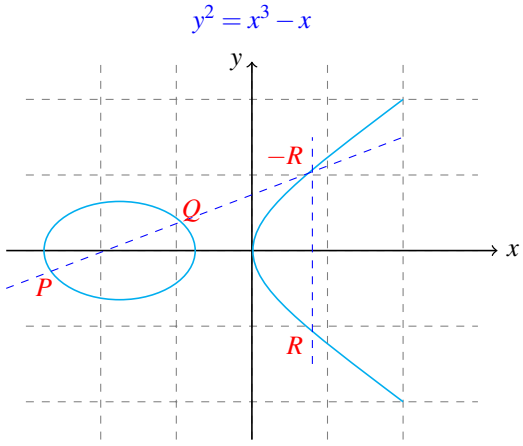

Fig. 1: Point addition on elliptic curve

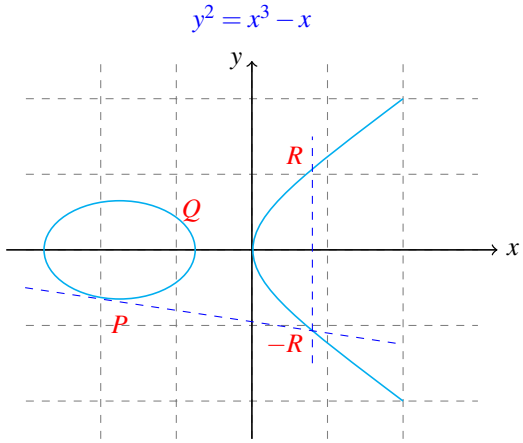

Fig. 2: Point doubling on elliptic curve

and doubling of a point are shown in Fig.1 and Fig.2 for the elliptic curve $y^2 = x^3 - x$. Point $R(x_3, y_3)$ can be derived as

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_2 - x_3) y_2 \end{aligned} \tag{2}$$

where

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & if P \neq Q \\ \frac{3 \times x_1^2 + a}{2 \times y_1} & if P = Q \end{cases}$$

C. Conventional ECC Scheme

The conventional ECC scheme is shown in Fig. 3.Suppose Alice wants to send a message to Bob and E is an *elliptic curve* over $\mathbb{F}_p$. G is an agreed upon (and publicly known) point on the curve. Bob chooses integer b and calculates $P_b = b \times G$ and makes it public. Alice maps the plaintext m to point M on curve and secretly chooses a random integer k.

Alice encrypts M as
$C_1 = k \times G$ and $C_2 = M + k \times P_b$.

Bob decrypts by calculating

$$\begin{aligned} M &= C_2 - b \times C_1 \\ &= C_2 - b \times kG \\ &= M + k \times P_b - k \times P_b \\ &= M \end{aligned}$$

D. Random Number Generation

Random number can easily be generated using *Linear-Feedback Shift Registers (LFSR)* [11] from maximum length polynomial. For polynomial $f(x) = x^4 + x + 1$, it has a shift register of length $m = 4$. So, it can produce a sequence of length $2^m - 1$, i.e.,15. In the numbers, sequence of bits appears random and has a very long cycle. For the given polynomial, random number sequence can be generated by calculating

$$x^i \ mod \ f(x) \ \ for \ i = 0, 1, 2, ..., 14. \tag{3}$$

The generated random number sequence will be like Fig. 4. Stream of values produced by registers in LFSR is completely determined by its current or previous states and the *Exclusive-OR* operation.

0 0 0 1 (=01)
0 0 1 0 (=02)
0 1 0 0 (=04)
1 0 0 0 (=08)
0 0 1 1 (=03)
0 1 1 0 (=06)
1 1 0 0 (=12)
1 0 1 1 (=11)
0 1 0 1 (=05)
1 0 1 0 (=10)
0 1 1 1 (=07)
1 1 1 0 (=14)
1 1 1 1 (=15)
1 1 0 1 (=13)
1 0 0 1 (=09)

Fig. 4: Random number sequence.

III. Proposed Approach

In this section, the proposed ECC scheme, proposed scalar multiplication algorithm and the necessary algorithms to implement the ECC scheme are described.

A. Proposed ECC Scheme

Suppose, Alice and Bob want to communicate using ECC scheme. They have to agree on some issues related to elliptic curve parameters and base point. The proposed ECC scheme for covert communication is described in Algorithm 1 and shown in Fig. 5.

B. Proposed Scalar Multiplication Algorithm

The efficiency of an ECC implementation mainly depends on the way it implements the Scalar or Point Multiplication [12]. Most of the existing algorithms focus on the minimization of Hamming weight [13] of the given value by converting it to binary or sign binary numbers [14]. The proposed algorithm also works with a view to making the hamming weight minimal choosing whatever is suitable between sign binary or binary multiplication without conversion overhead. The proposed Scalar Multiplication algorithm is described in Algorithm 2.

C. Rational Point Generation

To generate rational point $P(x, y)$ from the elliptic curve equation $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ for a large prime p, it is necessary to satisfy the condition, $4A^3 + 27B^2 \neq 0 \mod p$. Any point (x_i, y_i) for $i = 0, 1, .., p-1$ is a rational point on the curve if $y_i^2 == x_i^3 + Ax_i + B \mod p$ holds. The rational point generation is described in Algorithm 3.

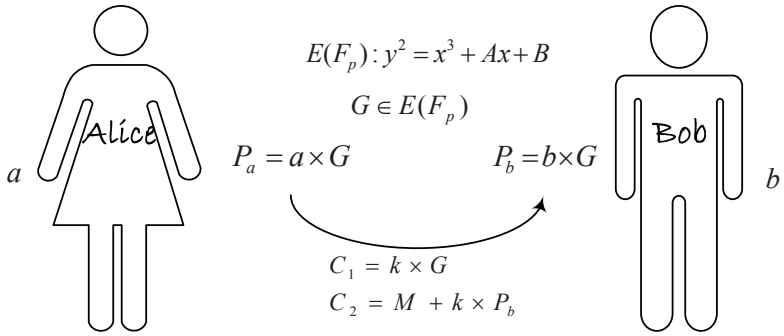

Fig. 3: Conventional ECC scheme

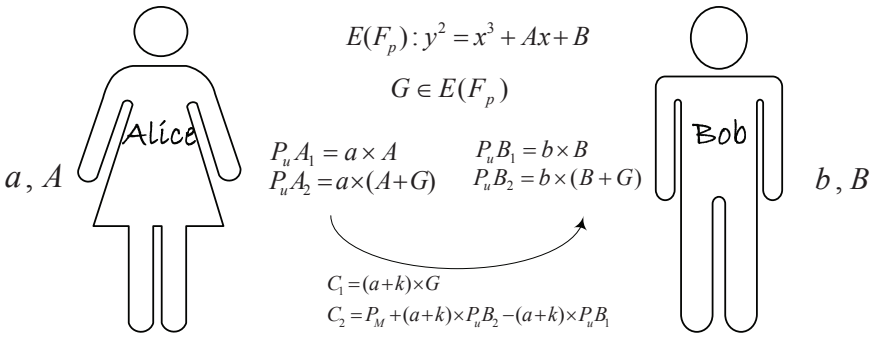

Fig. 5: Proposed ECC scheme

Algorithm 1 Proposed ECC Scheme

1: Both agree on curve $E : y^2 = x^3 + Ax + B$ on large prime field $\mathbb{F}_p$ for prime p and a common point G.
2: Alice chooses a *random number a* and a *random point A* on the curve, keeps them as her *private key* $PrA\{a, A\}$. She calculates $PuA_1 = aA$ and $PuA_2 = a(A+G)$ and made them public.
3: Bob chooses *random number b* and a *random point B* on the curve, keeps them as his *private key* $PrB\{b, B\}$. He calculates $PuB_1 = bB$ and $PuB_2 = b(B+G)$ and made them public.
4: If Alice wants to send message M to Bob, then Alice encrypts the message in following way
   a) maps message M to point P_M using *random sequence generation method*, $M \rightarrow P_M$.
   b) generate a *random number k*.
   c) Calculate $C_1 = (a+k)G$ and $C_2 = P_M + (a+k)PuB_2 - (a+k)PuB_1$.
   d) Alice sends $\{C1, C2\}$ to Bob.
5: Bob decrypts the message in the following way
   a) Calculate $P_M = C_2 - bC_1$.
   b) Then message is derived, $P_M \rightarrow M$.

Algorithm 2 Scalar Multiplication, kP

```
procedure SCALAR MULTIPLICATION(k, P)
    R ← 0
    S ← 1
    while k > 0 do
        x ← ⌊log2 k⌋
        if (k − 2^x) > (2^(x+1) − k) then
            R ← R + (s)2^(x+1).P
            k ← 2^(x+1) − k
            s ← −s
        else
            R ← R + (s)2^x.P
            k ← k − 2^x
        end if
    end while
    Return R
end procedure
```

D. Rational Point Addition

Algorithm provision for Rational Point Addition has already been described in section II-A. The algorithm is presented in Algorithm 4.

E. Message to Point Mapping

This section describes how a message M is mapped to point P_M. First random sequences from *maximum length polynomial*

Algorithm 3 Rational Point Generation

```
procedure RATIONALPOINTGENERATION(p, A, B)
    for i = 0 to p do
        for j = 0 to p do
            if (i^3 + a × i + b) mod p == j^2 mod p then
                P_i.x ← i
                P_i.y ← j
                P_{i+1}.x ← i
                if j ≠ 0 then
                    P_{i+1}.y ← p − j
                else
                    P_{i+1}.y ← j
                end if
            end if
            break
        end for
    end for
    return P
end procedure
```

Algorithm 4 Rational Point Addition

```
procedure RATIONALPOINTADDITION (P(x,y), Q(x,y))
    if P == 0 then
        R ← Q
    end if
    if Q == 0 then
        R ← P
    end if
    if P.y == −Q.y then
        R ← 0                                   ▷ when, P = −Q
    end if
    if P == Q then                              ▷ Point Doubling
        λ ← (3 × P.x^2 + a) / (2 × P.y)
        R.x ← λ^2 − 2 × P.x
    else                                        ▷ Point Addition
        λ ← (P.y − Q.y) / (P.x − Q.x)
        R.x ← λ^2 − (P.x + Q.x)
    end if
    if λ ≠ 0 then
        R.y ← −P.y + λ × (P.x − R.x)
    else
        R ← 0
    end if
    return R
end procedure
```

are generated. For random sequence, this paper used LFSR technique on the polynomial x^7+x^6+1 to generate random sequences. This polynomial has maximum period of 127 values ranging from 1 to 127. So it can represent 127 characters without any repetition. This paper uses only alphanumeric letters where every letter is assigned a value in the order it is generated in the sequence. For letters starts with numbers $[0-9]$, small letters $[a-z]$ and capital letters [A-Z] .

IV. Experimental Results and Discussions

In this section, numerical experiment results of proposed ECC scheme and the scalar multiplication algorithm are described. This paper proposes a new ECC scheme with a view to achieving robust securities. The results of the proposed approach are compared with the existing approach to find the effectiveness of the proposed approach in terms of number of operations and computational costs. Running time of the algorithm depends on the prime number and the message to be encrypted. This can also vary machine to machine and compiler to compiler. So this study implements some existing algorithms for comparisons. The approach presented in this paper is coded using C on an Intel laptop with speed of 2.13 GHz and 2GB of RAM under *Ubuntu 14.04 LTS* using *gcc - 4.9* compiler. For the operations of large bits this paper uses GMP library [15] , version-6.0.0a. The large primes are taken from *The Prime Pages library* [16] . It is tested on a message of 2.7 kb file containing only numbers and alphabets.

Algorithm 5 Random Sequence Generation

```
procedure RANDOMSEQUENCEGENERATOR(x^7 + x^6 + 1)
    flag ← 0x01
    data ← flag
    index ← 1
    do
        newbit ← ((data ≫ 6) ∧ (data ≫ 5)) AND 1)
        data ← ((data ≪ 1) ∨ newbit) AND 0x7f
        R_index ← data
        index ← index + 1
    while data ≠ flag
    return R
end procedure
```

A. Experimental Results of Proposed ECC Scheme

Proposed ECC scheme is compared to the conventional ECC scheme on computational cost and the level of security they offer against popular cryptanalytic attacks. Conventional ECC uses only one secret number as a private key and one point on the curve as a public key. On the other hand, the proposed ECC scheme uses one number with a point on the curve as private key and two points on the curve as public key. The additional points increase the computational cost but strengthen the security higher than the conventional ECC. Table I shows the elliptic curve operations needed for conventional ECC [17] and proposed ECC Scheme. The comparison of computational costs of Key generation, ECC encryption and ECC decryption methods of proposed scheme with the conventional ECC scheme are presented in Fig. 6, Fig. 7 and Fig. 8.

TABLE I: Comparison of required operations between [17] and proposed ECC

Algorithm	Operations	Addition	Subtraction	Multiplication
[17]	Key Generation	0	0	1
	Encryption	1	0	2
	Decryption	0	1	1
Proposed ECC	Key Generation	1	0	2
	Encryption	1	1	3
	Decryption	0	1	1

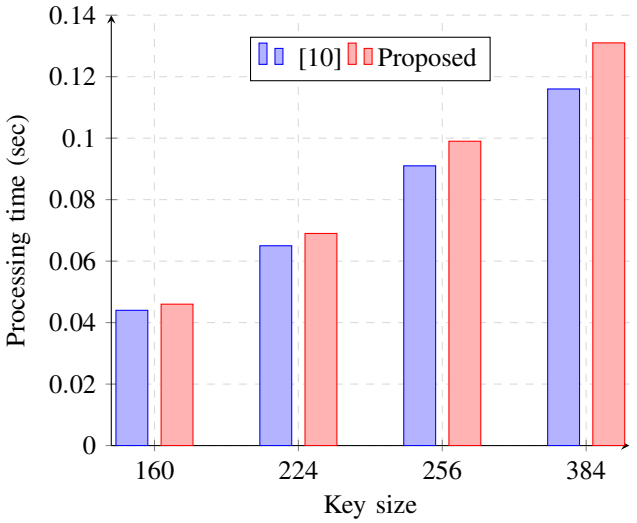

Fig. 6: Comparison of key generation cost between [10] and proposed ECC

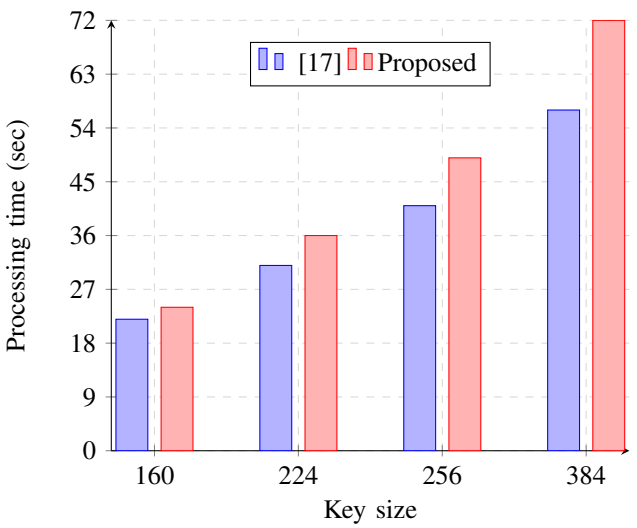

Fig. 7: Comparison of encryption cost between [17] and proposed ECC

B. Experimental Results of Proposed Scalar Multiplication

The efficiency of an ECC scheme depends largely on the scalar multiplication. Most of the existing algorithms have the overhead of converting the scalar number to binary or sign binary presentation to minimize the Hamming Weight. Proposed algorithm doesn't have such overhead except it needs pre-computed doublings and minimizes the Hamming Weight. The computational cost of the proposed Scalar Multiplication is shown in Fig. 9. The experimental results show that the computational cost of the proposed scalar multiplication algorithm is less than that of [18] and [7] which proves the efficiency of the proposed scalar multiplication algorithm.

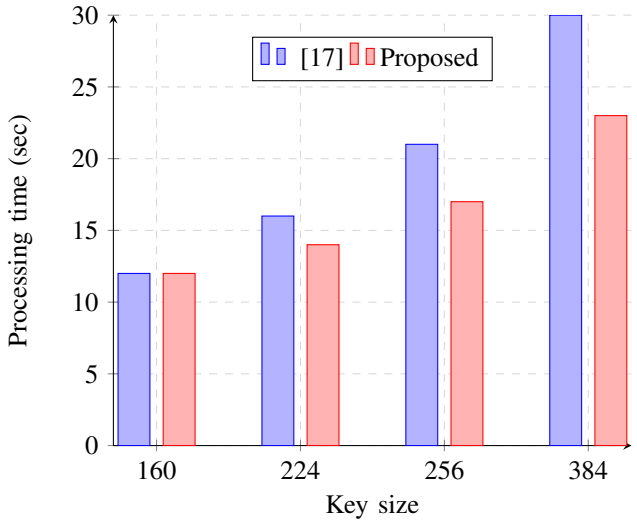

Fig. 8: Comparison of decryption cost between [17] and proposed ECC

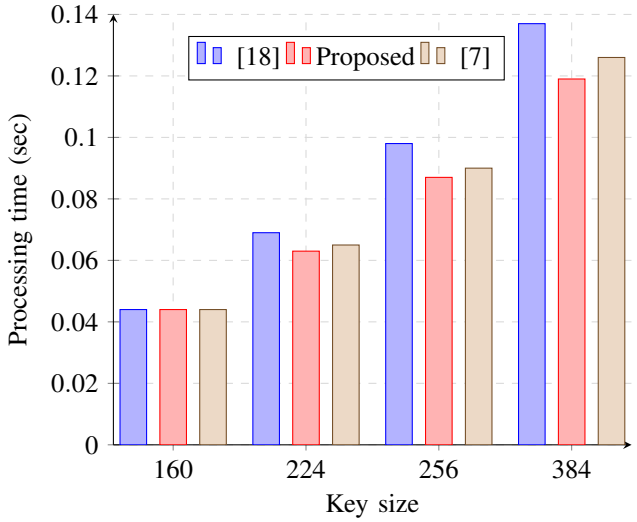

Fig. 9: Comparison of computational cost of scalar multiplication among [18], proposed ECC and [7]

C. Resistance against Attack on Proposed ECC Scheme

Proposed ECC has higher level of security than conventional ECC and experimental results for different attacks confirm it. The standard attack on ECC is *Random Walk* [19] which uses *Pollard-Rho* method for solving Elliptic Curve Discrete Logarithm Problem(ECDLP) [20] . The strategy behind the algorithm is to produce a sequence of randomly generated terms (R,a,b) where R is a point on the curve E and a,b lie in $\mathbb{F}_p$. As $E(\mathbb{F}_p)$ is periodic, eventually it will back again to some point. Using this technique, the secret is calculated. Pollard-Rho [21] proved that the expected running time of the method is $\sqrt{\frac{\pi \times n}{2}}$ steps, where a step here is an elliptic curve addition. As the proposed algorithm has two different secret keys the expected running time will be twice of the stated cost.

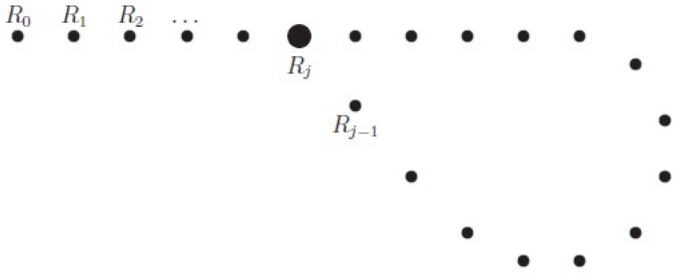

Fig. 10: Finding repetition of points using random walk technique

TABLE II: Comparison of computation cost required to break ECC

Key Size	ECC [22]		Proposed ECC	
	Cost	MIPS years	Cost	MIPS years
160	2^{80}	9.6×10^{11}	2×2^{80}	1.92×10^{12}
186	2^{93}	7.9×10^{15}	2×2^{93}	1.58×10^{16}
234	2^{117}	1.6×10^{23}	2×2^{117}	3.2×10^{23}
354	2^{177}	1.5×10^{41}	2×2^{177}	3.0×10^{41}
426	2^{213}	1.0×10^{52}	2×2^{213}	2.0×10^{52}

So the expected cost of breaking the proposed ECC scheme will roughly be $2 \times \sqrt{\frac{\pi \times n}{2}}$ steps. A *MIPS (Million Instructions Per Second)* year is presented as the computational power of a computer that is rated at 1 MIPS and utilized for one year. The comparison of computation cost required to break the proposed ECC with the conventional ECC [22] are presented in Table II.

V. Conclusion and Future Work

This paper proposes a new ECC scheme and a scalar multiplication algorithm for it. When developing ECC scheme, this paper aims the higher level of security to be the foremost criteria to improve than the conventional ones. For scalar multiplication, reduction of computation cost is chosen to be the primary criteria and this is achieved including the advantages of both binary and signed binary presentation in the proposed algorithm. Future study aims to integrate the advantages of double scalar multiplications in the proposed ECC scheme to further minimize the computation cost. Then, the proposed scheme will be evaluated on different key sizes against different cryptanalytic attacks for further improvement of the proposed scheme.

References

[1] R. de Clercq, L. Uhsadel, A. Van Herrewege and I. Verbauwhede, *Ultra low-power implementation of ECC on the ARM Cortex-M0+*, Proceedings of the 51st Annual Design Automation Conference ACM, pp. 1-6, June 2014.

[2] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig and E. Wustrow, *Elliptic curve cryptography in practice*, Financial Cryptography and Data Security, LNCS vol. 8437, pp. 157-175, Springer Berlin Heidelberg, March 2014.

[3] Z. Liu, J. Groschdl and D. S. Wong, *Low-weight primes for lightweight elliptic curve cryptography on 8-bit AVR processors*, Information Security and Cryptology, LNCS vol. 8567, pp. 217-235, Springer International Publishing, January 2014.

[4] H. L. Yeh, T. H. Chen and W. K. Shih, *Robust smart card secured authentication scheme on SIP using elliptic curve cryptography*, Computer Standards and Interfaces, vol. 36, no. 2, pp. 397-402, February 2014.

[5] N. Koblitz, *Elliptic Curve Cryptosystems*, Mathematics of Computation, vol. 48, no. 177, pp. 203 -209, 1987.

[6] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in CryptologyCRYPTO85 Proceedings, LNCS vol. 218, pp. 417-426, Springer Berlin Heidelberg, 1986.

[7] A. Rezai and P. Keshavarzi, *An Efficient Scalar Multiplication Algorithm for Elliptic Curve Cryptography Using a New Signed-Digit Representation*, Advanced Science and Technology Letters, vol. 44, pp. 44-48, 2013.

[8] D. S. Kumar, C. H. Suneetha and A. Chandrasekhar, *Encryption of data using Elliptic Curve over finite fields*, International Journal of Distributed and Parallel Systems, vol. 3, no.1, January 2012.

[9] F. Amounas and E. H. El Kinani, ECC Encryption and Decryption with a Data Sequence, Applied Mathematical Sciences, vol. 6, no. 101, pp. 5039-5047, January 2012.

[10] D. Hankerson, A. J. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

[11] A. Canteaut, *Linear Feedback Shift Register*, Encyclopedia of Cryptography and Security, pp. 726-729, Springer US, 2011.

[12] C. L. Leca and C. I. Rincu, *Combining point operations for efficient elliptic curve cryptography scalar multiplication*, Communications (COMM) 2014 10th International Conference, pp. 1-4, IEEE, May 2014.

[13] R. M. Avanzi, C. Heuberger and H. Prodinger, *Minimality of the Hamming weight of the -NAF for Koblitz curves and improved combination with point halving*, Selected Areas in Cryptography, LNCS vol. 3897, pp. 332-344, Springer Berlin Heidelberg, January 2006.

[14] K. Koyama and Y. Tsuruoka, *Speeding up elliptic cryptosystems by using a signed binary window method*, Advances in cryptology-CRYPTO92, pp. 345-357, Springer Berlin Heidelberg, January 1993.

[15] J. Liu, Y. H. Lu and C. K. Koh, *Performance Analysis of Arithmetic Operations in Homomorphic Encryption*, ECE Technical Reports, Purdue University, 2010. Online available at: https://gmplib.org/

[16] C. K. Caldwell, *The prime pages (prime number research, records and resources)*, 2012.

[17] I.F. Blake, G. Seroussi and N. P. Smart, *Advances in elliptic curve cryptography*, vol. 317, Cambridge University Press, 2005.

[18] P.Balasubramaniam and E. Karthikeyan, *Elliptic curve scalar multiplication algorithm using complementary recoding*, Applied mathematics and computation, vol. 190, no.1, pp. 51-56, July, 2007.

[19] F. Zhang and P. Wang, *Speeding up elliptic curve discrete logarithm computations with point halving*, Designs, codes and cryptography, vol. 67, no. 2, pp. 197-208, Springer US, 21 December 2011.

[20] D. Baehr, S. McKinney, A. Quirk and K. Harfoush, *On the practicality of elliptic curve cryptography for medical sensor networks*, High-capacity Optical Networks and Emerging/Enabling Technologies (HONET) 2014 11th Annual, pp. 41-45, IEEE, December 2014.

[21] J. M. Pollard, *Monte Carlo Methods for Index Computation (mod p)*, Mathematics of Computation, vol. 32, no. 143, pp. 918-924, July 1978.

[22] D.B. Johnson and A.J. Menezes, *Elliptic curve DSA (ECDSA): an enhanced DSA*, Proceedings of the 7th conference on USENIX Security Symposium. vol. 7, pp. 13-23, 1998.

Fatema Akhter with department of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul University, Trishal, Mymensingh-2220, Bangladesh. e-mail: fatema.kumu02@gmail.com. Her general research interests are in the area of Cryptography and Network Security, Public Key Cryptosystem, Image Steganography, Quantum Cryptography and Anonymous Credential System. Her current research focuses on Elliptic Curve Cryptography and Noiseless Steganography. Part of this paper is presented at the International Conference on Computer & Information Engineering (ICCIE 2015),RUET, Rajshahi, Bangladesh.