Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105071, November 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

On Reduced Computation Cost for Edwards and Extended Twisted Edwards Curves

Gautam Kumar and Hemraj Saini*

Department of Computer Science and Engineering, Jaypee University of Information Technology, Solan -173234, Himachal Pradesh, India; gautam.kumar@mail.juit.ac.in, hemraj1977@yahoo.com
*Author for correspondence

Abstract

Background: Scalar multiplication is having the scope for gaining the computational efficiency for Elliptic Curve Cryptography (ECC). The security strength and effectiveness have been better reported on shorter key lengths. **Methods:** The Edwards curves are one of the form used in cryptography is showing one of advanced study for generating the more randomness and unpredictability behaviors. The numbers of researchers have shown the significant improvement to solve the same problem on two, four and eight processors and that are contributing the immense contribution in the field of security. **Findings:** The manuscript solves the Edwards Curves and twisted Edwards Curves problems on four and eight processors based on reduced computation cost from $2M + 1S + 1D + 3A$ to $2M + 1S + 1D + 2A$ on four processors and $2M + 3A$ to $2M + 2A$ on 8-processors, respectively. Our generalized computation cost $4\frac{(s)}{3}M + \frac{(s)}{3}A$ on 8-processors for s -bit scalar multiplication is reporting better than the cost $6\frac{(s-1)}{3}M + 3\frac{(s-1)}{3}A$ for Montgomery Ladder method and $5\frac{(s)}{3}M + \frac{(s)}{3}A$ for extended twisted Edwards curves on radix-8. **Applications:** The operation is performing on input scalar which multiplies with point-coordinates on curve, which has accumulated on reduced clock cycles with resistance to the simple side channel attack.

Keywords: ADDDBL, DLP, ECC, Edwards Curves, Twisted Edwards Curve

1. Introduction

Cryptography is a discipline of computer science and it has been generalized for security aspects from definition and concepts of computing systems. It is fulfilling the security requirements on systematic foundational issues. It has been treated as a branch of mathematics. Modern cryptography is mostly focusing on security problems, perfect definition and light-weight evolution methodology that suits to short-memory devices on low computation and communication cost. The security mechanisms work as a backbone for information systems. These are preventing adversaries from business secrets. Recent research trends have observed that the security on data are influencing issues on various types on used processor with the principle on sharing of resources and throughputs. These have been considered into the central role of information telecommunications systems. The core tool for data security is public-key cryptography, which uses enhanced versions of algorithms on the imposition of typical functionalities and/or modernization kinds that are ultimately reducing the requirements of hardware and software storage dependent on the base point.

In public key cryptography, ECC[1,2] has attracted the most attention from the research community in the previous three decades. ECC has gained the much popularity

*Author for correspondence

and it is much dominating RSA/DSA systems today due to its higher computational on a shorter key sizes. Scalar multiplication is a central operation of ECC that eventually depends on point addition and point doubling operations and these two operations depends on the finite field's arithmetic[3].

Discrete Logarithmic Problem (DLP) is the heart of cryptography which plays a crucial role in information security on applied algorithms. The faster running algorithms are leading with high-speed in the growing field of computation and communication[4]. DLP-ECC is working on a given two elliptic points P and Q on the curve, to find the value of k (generally secret key), such that $Q = kP$, which acts like a core building blocks in PKC[5]. It computes the cryptographic function in the forward direction using repeated point additions (ADDs) and point doublings (DBLs) operations. It is known as scalar multiplication. But, the adversaries try to find the secret key on the generated scalar multiplication values, which has been considered negligible to revert back for ECC. ECC is attracting the most attention in appropriateness to the short-memory devices. Such devices may be smart cards, net banking, mobile banking and the various real-time applications for secure and efficient implementations.

The rapid growth on memory and low cost arithmetic in cryptographic applications are attracting the most attention in the recent scenario. Edwards curves uses in the field of Elliptic Curve Cryptography (ECC), where Harold Edwards in 2007[6] first studied about a family of curves for (ECC). Thus, Edwards curves are considering as a family of elliptic curves that are often using for cryptographic functions. These are existing over finite fields arithmetic and practically applicable for security measures. The foundation of these curves is based on the mathematical formulation. Twisted Edwards curves are a generalization of the Edwards curves. The generalized curves are using in important security schemes as well and thus are worth studying.

Bernstein and Lange developed various applications for Edwards curves in cryptography[7]. They pierce the same on numerous advantages of Edwards form in contrast in relation to the well-recognized Weierstrass form. Here we have summarized the related works to Edwards and twisted Edwards curves:-

- Edwards follows addition law on the results produced from the Gauss/Euler example and generalized the form of elliptic curve to do the arithmetic on this curve in[6]. The general equation of Edwards curves is:

$x^2 + y^2 = 1 + dx^2y^2$, for some scalar, where $d \in \{0,1\}$. (1)

One another form for Edwards curves is also available with c and d parameters such as:

$x^2 + y^2 = c^2\left(1 + dx^2y^2\right)$, where c, d with $cd(1 - c^4.d) \neq 0$. (2)

The reviews on addition, doubling and a dual addition-doubling law for Edwards and Twisted Edwards curves fulfill the criteria into the complete curves. The following terms such as unified refers to addition formula remain valid when two input points are identical and it can also be used for point doubling, and the term complete refers the addition formula for all inputs.

The Edwards addition law: The Edwards curves (2) say two elliptic points, such coordinates (x_1, y_1) and (x_2, y_2), addition point (x_3, y_3) is based on affine coordinates as:

$$(x_3, y_3) \rightarrow \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}, \frac{y_1y_2 - cx_1x_2}{1 - dx_1y_1x_2y_2}\right) \quad (3)$$

To make a little variation into the suitable denominators one should to insert the Edwards addition law into the projective synchronization coordinates, inverted synchronization coordinates, extended synchronization coordinates, and completed synchronization coordinates.

A unified addition law for Edwards curve is strong enough to justify its problem on the generic doubling consideration and it can also be formulated. The addition law on point $(0,1)$ is the neutral point, whereas the negative of any point on curve (x_1, y_1) is $(-x_1, y_1)$.

Affine Doubling Formulae (independent of d):

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{y_1^2 + ax_1^2}, \frac{y_1^2 - ax_1^2}{2 - y_1^2 + ax_1^2}\right) = (x_3, y_3) \quad (4)$$

The dual addition law: Hisil et al. in [29] introduced the addition law

$$[(x]_3, y_3) \rightarrow \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + cx_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2\, y_1}\right) \quad (5)$$

The addition law on dual production produces the same output as described for the Edwards addition law on the defined coordinates, and instead of the same on the

applications for exceptional cases they are diversifying its properties.

- A general version defined by Bernstein and Lange $x^2 + y^2 = a^2(1 + dx^2y^2)$ or simply $x^2 + y^2 = 1 + dx^2 y^2)$ together for computing the group operations on projective coordinates in[7]. The outcome of addition cost $10M + 1S + 1D$ with a=1. The rest of this paper includes multiplication by constant curve factor D.
- Bernstein and Lange in 2007 introduced the invented Edwards coordinates in[8], which reduced the group operations on the standard point addition costs $9M + 1S + 1D$ on Edwards curves.
- Bernstein et al. introduced the new form of twisted Edwards curves on $ax^2 + y^2 = 1 + dx^2y^2$ and considered to be a generalization of the same[9]. Due to this reason the arithmetic speed was enhanced on a suitable point representation. This new representation is known as extended twisted Edwards curves which add an auxiliary coordinate to twisted Edwards coordinates. Despite of the same they developed the faster ways for doing the point addition and composed coordinates on the lower degree of arithmetic computation.
- Jacobian Projective coordinates have generalized on 4-processors by Patrick Longa and Ali Miri the Fast and Flexible Prime Fields[10]. They accelerated the techniques on cheaper operations on the substitution of multiplication with square on the fact that a square cost is less than multiplication. The conventional approach also works for the same and its significance is protecting Simple Side-Channel Attacks (SSCA).
- Huseyin Hisil et al.[11] introduces a new and fastest technique to perform the group operations on twisted Edwards curves that are pushing the speed limits for Elliptic Curve Cryptography (ECC) into numerous applications on wide spread. The things to be notable were the constant factor for selected curve uses into the new the new addition technique. In order to make a comparison for the fastest point addition technique on twisted Edwards curves states 9M+1S consolidated operations in the literature. They have further shown the new addition formula can also be in favorable indications for four processors to drops its effective cost upto 2M. This is an indication the effective increase in speed by a marginal factor on the sequential case. Their results consent to be a faster realization on elliptic curve scalar multiplication. In addition to the above, the point addition (new) technique can be used to make a natural protection against from the side channel attacks on the Simple Power Analysis technique (SPA).
- Bernstein et al. in[12] suggested to use Elliptic curve method for Edwards curves that pointed out the improvement above the arithmetic level as follows: (1) on behalf of Montgomery curves they used Edwards curves; (2) used Edwards (extended) coordinates; (3) the substitutions chain on addition-subtraction for sliding-window; (4) window size to increase the batch primes; (5) small parameters on the chosen curves with respect to the base points; (6) a large torsion on the chosen curves.
- Abdulrahman and Masoleh in 2015[13] solve the problem of Edwards and Twisted Edwards curves on 4-processors and 8-processors respectively on the cost of 2M+1S+1D+2A and 2M+3A.
- Our paper has organized as follows. Section 2 denotes the basic symbols used in the whole sections. Section 3 contains the Edwards curve problem on two coordinates solves on 4-processors architecture. The advantages we represent in the form of computation cost. Similarly we solve the problem of extended twisted Edwards curves which is based on 8-processors with its computational cost in Section 4. Finally, we summarize our manuscript.

2. Notation Symbols

The manuscript considers notations that represent its meaning in manuscript, such as, elliptic curve group element operations as EC-Operations, point addition ADDs, doubling DBLs, subtraction SUB, composite addition-doubling ADDDBL, simple side channel attack SSCA, multiplication M, subtraction Sub, addition A, squaring

S, inversion I, scalar multiplication SM, and elliptic curve scalar multiplication ECSM.

3. Parallel Architecture on Edwards

In this section, we parallel the architecture of Edwards curves on 4-processors that are showing a significant addition operation the proposed work. This follows on two points coordinates of Edwards curve such as $P_1(X_m, Z_m)$ and $P_2(X_n, Z_n)$ present a protected scalar multiplication scheme for the prime field on all the parallel and simple side channel attacks that have reported with the various proposed approaches on the fast Montgomery curve for Montgomery Ladder method[11] and radix-8 scalar multiplication[13].

To represent the point coordinates for addition operation on the given formula is on:

$$\begin{cases} X_{m+n} = (X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)) \\ Z_{m+n} = X_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n) \end{cases} \quad (6)$$

whereas, the coordinates of point doublings are as follows:

$$\begin{cases} 4X_m Z_m = (X_m + Z_m)^2 - (X_m - Z_m)^2 \\ X_{2m} = (X_m + Z_m)^2 . (X_m - Z_m)^2 \\ Z_{2m} = 4X_m Z_m \left((X_m + Z_m)^2 + \left(\left(\frac{A+2}{4} \right) (4X_m Z_m) \right) \right) \end{cases} \quad (7)$$

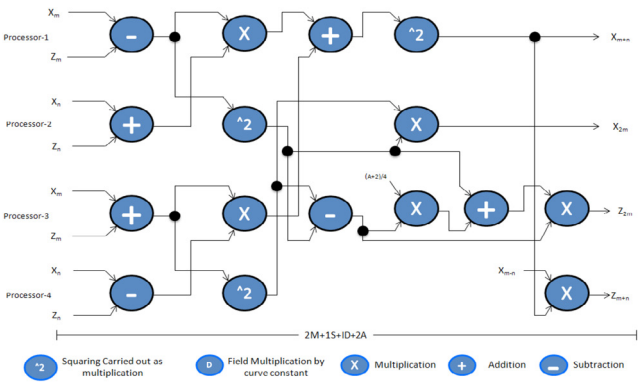

Figure 1. Parallel architecture for ADDDBL on 4-processors

The proposed method is solving this problem for ADDDBL operations on the reduced computational complexity from 2M+1S+1D+3A [13] to 2M+1S+1D+2A based on the 4-processors, as shown in Figure 1. The comparative study in relation to the proposed scheme is showing it is a significant improvement in addition.

4. Parallel Architecture on Extended Twisted Edwards Curves

A finite fields operation on arithmetic cost for ADDDBL operation on the prime extended twisted Edwards curve on 8-processor implementation is generalized on the Edwards curve [7] with its equation:

$$\varepsilon_T : ax^2 + y^2 = 1 + dx^2 y^2 \quad (8)$$

where, $a, d \in GF(p)$, with $ad(a-d) \neq 0$. To make an evolution for the much faster method to perform ADD and DBL operations in[11], in this case one additional coordinate (auxiliary) was added into the extended twisted Edward curve coordinates. It is obvious from[11] and with a reasonable reason to make for the extended twisted Edwards curves is represented in the form of quadruple coordinate.

According to the definition of twisted Edwards curves say that this is based on four coordinates with two point's scalar multiplication. Let $P_1(X_1, Y_1, T_1, Z_1)$, and $P_2(X_2, Y_2, T_2, Z_2)$, be two distinct points on ε^e, where ε^e denotes the extended twisted Edwards coordinates, with $Z_1 \neq 0$ and $Z_2 \neq 0$, then the coordinates of the point addition $P_3(X_3, Y_3, T_3, Z_3)$, has given as follows[11]:

$$(X]_1 Y_2 - Y_1 \quad (9)$$

and the doubling proceeds on the coordinates of, i.e., $P_4(X_4, Y_4, T_4, Z_4) = 2P$, is given in [11] by:

$$\begin{cases} X_4 = (2X_1 Y_1)(2Z_1^2 - Y_1^2 + X_1^2) \\ Y_4 = (Y_1^2 - X_1^2)(Y_1^2 + X_1^2) \\ T_4 = (2X_1 Y_1)(Y_1^2 + X_1^2) \\ Z_4 = (Y_1^2 - X_1^2)\left(2Z_1^2 - Y_1^2 + X_1^2\right) \end{cases} \quad (10)$$

To make a anonymous results the constant case $a = -1$, is a special case for the same. DBL needs $4M + 4S + 6A$ and ADD needs $8M + 10A$ operations, considers to arithmetic subtraction and addition are equal. The proposed composite (ADD+DBL=ADDDBL) operation for this curve has solved for both ADD and DBL operations in 5 steps on splitting the computational task on 8-processors in [13]. This has reported to the fastest way

to do the scalar multiplication. According to the same, the effective and rationally have reduced to $2M + 3A$ $2M + 3A$ operations on 8 processors.

The objective of our proposed scheme is achieving the faster scalar multiplication result, in Figure 2. It is important to note that on simplicity purpose that some of the used (registers) in the ECSM schemes are not analyzed or discussed. Also in the paralleling process, we imposed the architecture restriction on SIMD (Single Instruction Multiple Data) operations that are as similar to[14] and[10]. According to our proposed work, we solved the same problem for the scalar multiplication at 4-states, which takes a shorter clock cycle to initiate the process in one's multiplication reduction (in relation to the previously proposed work) and it is considering in immense contribution to the overall performance improvement. The data dependency graph for both (9) and (10) shows combining these two equations require a computational cost of one's multiplicative operation saved. The ADDDBL operation scheme consists of eight independent processing elements, i.e., process 1 to process 8. Where finite field arithmetic operations are represented by a circle and it is labeled according to the type of operations. In the scheme, it is explicit that the squaring (S) operation performed in step-1 is carried out as multiplication (M) operations. The effective cost time of DBL operation of the prime extended twisted Edwards curves has obtained by one round saved computation for scalar and have been accomplished on effective time of $2M + 2A$.

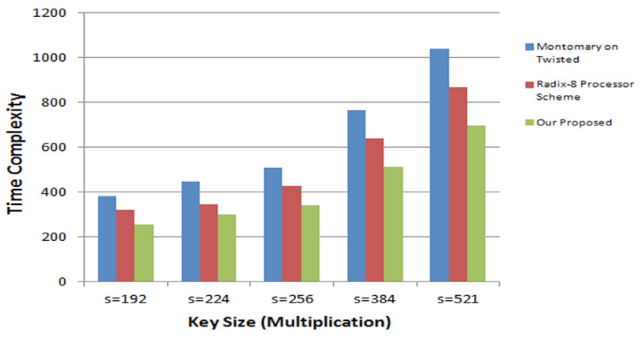

Figure 2. Paralleling ADDDBL operation on prime extended twisted Edwards curve.

The general operations for 8-processors on s -bit scalar multiplication requires $6\frac{(s-1)}{3}M + 3\frac{(s-1)}{3}A$ for Montgomery Ladder method in[15] and the extended twisted Edwards curves on radix-8 ECSM method requires $5\frac{(s)}{3}M + \frac{(s)}{3}A$ in[13]. Our proposed ECSM required operations of $4\frac{(s)}{3}M + \frac{(s)}{3}A$.

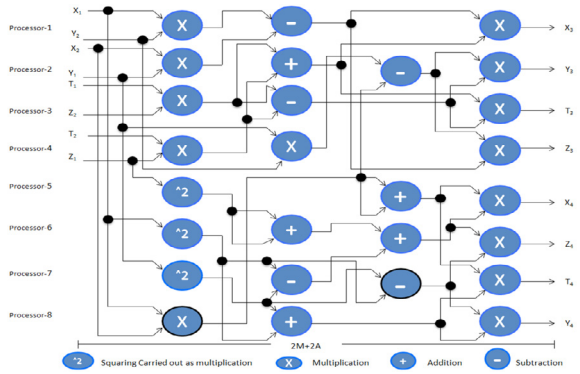

Figure 3. Comparative cost reduction of our proposed approach.

In Figure 3, we make a comparative study that our proposed solution for extended twisted Edwards curve is better than the existing methodologies, which has generalized from the formerly reported literature. The comparative time complexity to complete the point ADDs and point DBLs takes the shorter clock cycle to initiate the same. Finally, in Table 1, we linked the related parallel schemes and its required complexities on key sizes s={192,224,256,384,521}. The relative computational time complexities presented in the respective literature presented for Jacobian projective coordinates as mentioned in[16], the extended twisted Edwards curves for the 4-processor scheme as in[11], the Montgomery curve on 4-processor for Montgomery Ladder method in[15], the Montgomery curve on the 4-processor Montgomery Ladder method as shown in[15], the 8-processor scheme for the extended twisted Edwards curves in[13]. But our 8-processor extended twisted Edwards curves in terms of computational time complexity on prime field is better than all.

In this section, we proposed a protected scalar multiplication for the prime extended twisted Edwards curve that can perform all the parallel be faster in respective approaches and protected schemes for SSCA, on behalf of literature including the faster Montgomery curve on the Montgomery Ladder method as compared and presented in[15] and at Radix-8 [13].

Table 1. Comparison of Related Parallel Scheme on Edwards Curves

Prime Field Size	Schemes on Processor	Computational Time Complexity
s=192	4 Processors for Jacobian Projective Coordinates[16]	191M+637S
	4 Processors for Extended Twisted Edwards[11]	319M+191S
	Montgomery Ladder method on the Montgomery curve[15]	382M+382S
	Montgomery Ladder at Montgomery curve[11]	382M+191S
	New Regular Radix-8 Processor Scheme13	320M+64S
	Our Proposed 8 Processors Scheme	256M+64S
s=224	4 Processors for Jacobian Projective Coordinates[16]	223M+744S
	4 Processors for Extended Twisted Edwards[11]	372M+223S
	Montgomery Ladder method on the Montgomery curve[15]	446M+446S
	Montgomery Ladder at Montgomery curve[11]	446M+223S
	New Regular Radix-8 Processor Scheme[13]	446M+75S
	Our Proposed 8 Processors Scheme	299M+75S
s=256	4 Processors for Jacobian Projective Coordinates[16]	225M+850S
	4 Processors for Extended Twisted Edwards[11]	425M+245S
	Montgomery Ladder method on the Montgomery curve[15]	510M+510S
	Montgomery Ladder at Montgomery curve[11]	510M+255S
	New Regular Radix-8 Processor Scheme[13]	427M+86S
	Our Proposed 8 Processors Scheme	342M+86S
s=384	4 Processors for Jacobian Projective Coordinates[16]	383M+1177S
	4 Processors for Extended Twisted Edwards[11]	639M+383S
	Montgomery Ladder method on the Montgomery curve[15]	766M+766S
	Montgomery Ladder at Montgomery curve[11]	766M+383S
	New Regular Radix-8 Processor Scheme[13]	640M+128S
	Our Proposed 8 Processors Scheme	512M+128S
s=521	4 Processors for Jacobian Projective Coordinates[16]	520M+1734S
	4 Processors for Extended Twisted Edwards[11]	867M+520S
	Montgomery Ladder method on the Montgomery curve[15]	1040M+1040S
	Montgomery Ladder at Montgomery curve[11]	1040M+520S
	New Regular Radix-8 Processor Scheme[13]	869M+174S
	Our Proposed 8 Processors Scheme	695M+174S

5. Conclusion

The manuscript contributes a significant improvement in performance for the scalar multiplication techniques proposed for the Edwards and extended twisted Edwards curves. The problem statements have been defined on 4-processors and 8-processors having to gain the computational efficiency for Elliptic Curve Cryptography (ECC). The ECC is justifying the security strength and effectiveness on the shorter key lengths. The comparative reduction cost on the 4-processors is $2M + 1S + 1D + 3A$ to $2M + 1S + 1D + 2A$ and on the 8-processors is $2M + 3A$ to $2M + 2A$. The generalized computation cost is reporting better than the existing approaches any length of key size scalar multiplication on 8-processors schemes.

6. Acknowledgement

This work is supported by the Jaypee University of Information Technology, Himachal Pradesh, India.

7. References

1. Diffie W, Hellman ME. New directions in cryptography. IEEE Transaction on Information Theory. 1976 Nov; 22(6):644–54.
2. Jarvinen K, Skytta J. Parallelization of high-speed processor for elliptic curve cryptography. IEEE Transaction on VLSI. 2008 Sep; 16(9):1162–75.
3. Koblitz N. Elliptic curve cryptosystems. Math Computation. 1987; 48(177):203–9.
4. Joppe WB, Marcelo EK, Kleinjung T, Arjen KL, Peter LM. On the security of 1024-bit RSA and 160-bit elliptic curve cryptography. IACR Cryptology ePrint Archive; 2009. p. 389.
5. Miller VS. Use of elliptic curves in cryptography. Advances in Cryptology. Williams HC, editor, Lecture Notes in Computer Science Publications: Springer Berlin Heidelberg. 1986; 218:417–26.
6. Harold ME. A normal form for elliptic curves. Bulletin of the American Mathematical Society. 2007 Jul; 44(3):393–42.
7. Daniel JB, Lange T. Faster addition and doubling on elliptic curves. ASIACRYPT 2007. Kurosawa K, editors, Lecture Notes in Computer Science Publications: Springer Berlin Heidelberg. 2007; 4833:29–50.
8. Daniel JB, Lange T. Inverted Edwards coordinates. AAECC-17. Boztas S, Lu HF, editors, Lecture Notes in Computer Science Publications: Springer Berlin Heidelberg. 2007; 4851:20–7.
9. Daniel JB, Birkner P, Joye M, Lange T, Peters C. Twisted Edwards curves. AFRICACRYPT-2008. Vaudenay S, editor, Lecture Notes in Computer Science Publications: Springer Berlin Heidelberg. 2008; 5023:389–405.
10. Longa P, Miri A. Fast and flexible elliptic curve point arithmetic over prime fields. IEEE Transaction on Computers. 2008 Mar; 57(3):289–302.
11. Hisil H, Koon-Ho WK, Carter G, Dawson E. Twisted Edwards curves revisited. Advances in Cryptology. ASIACRYPT 2008. Pieprzyk J, editors, Lecture Notes in Computer Science Publications: Springer Berlin Heidelberg. 2008 Dec; 5350:326–43.
12. Bernstein DJ, Lange T. Analysis and optimization of elliptic-curve single scalar multiplication. Contemporary Mathematics; 2000.
13. Ebrahim AHA, Reyhani-Masoleh A. New regular radix-8 scheme for elliptic curve scalar multiplication without precomputation. IEEE Transactions on Computers. 2015 Feb; 64(2):438–51.
14. Izu T, Takagi T. Fast elliptic curve multiplications with SIMD operations. Information and Communication Security. Lecture Notes in Computer Science Publications: Springer Berlin Heidelberg. 2002 Dec; 2513:217–30.
15. Peter LM. Speeding the Pollard and elliptic curve methods of factorization. Mathematical Computation. 1987 Jan; 48(177):243–64.
16. Baldwin B, Moloney R, Byrne A, McGuire G, Marnane William P. A hardware analysis of twisted Edwards curves for an elliptic curve cryptography. ARC 2009. 5th International Workshop on Applied Reconfigurable Computing. Lecture Notes in Computer Science Publications: Springer Berlin Heidelberg. 2009; 5453:355–61.