International Journal of Mathematics and
Computer Science, **18**(2023), no. 4, 599–606

Integer matrix size 2×2 sub-decomposition method for elliptic curve cryptography

Ruma Kareem K. Ajeena

Department of Mathematics
Education College for Pure Sciences
University of Babylon
Babil, Iraq

email: pure.ruma.k@uobabylon.edu.iq

(Received March 1, 2023, Accepted April 5, 2023,
Published May 31, 2023)

Abstract

This work proposes a new version of integer sub-decomposition of a scalar k in an elliptic curve scalar multiplication kP which is a core operation for elliptic curve cryptography (ECC). A scalar k is represented as a random matrix size 2×2, its elements are integers k_{11}, k_{22}, k_{12} and k_{21} which are less than k and lying in the range $[1, n-1]$, where n is a prime order of a generator point P on an elliptic curve E defined over a prime field F_p. The integers k_{11}, k_{22}, k_{12} and k_{21} are sub scalars of k which also represented by random matrices size 2×2 with elements are less than them. With integer matrices size 2×2 sub-decomposition ($IM_{2\times2}SD$) method, more speeding up for computing the kP is done in compare to use the previous proposed GLV decomposition and ISD sub-decomposition methods. The security of $IM_{2\times2}SD$ method is determined based on the random representations of a scalar k and its sub-scalars that give many possible cases for generating these matrices which are used to compute kP. New experimental results of the $IM_{2\times2}SD$ method have been presented.

Elliptic scalar multiplication techniques are used essentially as a key point in cryptography, especially in ECC [1],[2]. ECC is presented by Victor Miller

Key words and phrases: ECC, Scalar multiplication, ISD method, $IM_{2\times2}SD$ method, Security.
AMS (MOS) Subject Classifications: 94A60, 14H52, 15Bxx.
ISSN 1814-0432, 2023, http://ijmcs.future-in-tech.net

and Neal Koblitz in 1985 [3],[4]. Many researchers have attracted to work using ECC, since the ECDLP can not be solved with good selected properly of E by any sub-exponential algorithm [5]. Comparable security levels between ECC and Rivest, Shamir and Adleman (RSA), makes ECC is used as an alternative RSA. The scalar multiplication kP is major operation in ECC as well as multiple point multiplication $lP + mQ$ operation, with k, l and m are integer numbers. The computations of kP and $lP + mQ$ are done using several different methods. The GLV method [6] speeds up a kP through decomposing k and pre-computing the efficiently computable endomorphism ψ of E defined over F_p. The gaps on GLV generators is proved by Kim and Lim through proposed necessary condition in 2003 [7]. Recently, in 2010, Zhou et al. [8] presented a three dimensional 3-GLVmethod using two distinct endomorphisms of E. In 2011, Galbraith et al. [9] used the twists of E over a field F_{p^2} for decomposing k in 4-dimensions. Another idea in 2013 is proposed by Ruma Ajeena [10] which is based on the GLV method that is known by ISD method to sub-decompose a scalar k and to work outside the range $\pm\sqrt{n}$ in compare to GLV idea that it doesnt work, also see [11],[12]. The hybrid GLV-ISD method [13] of scalar multiplication is proposed in 2014 for increasing the percentage of computing kP. Also see [14], [15].
This work introduces new version for sub-decomposing a scalar k in kP which uses the random choosing for integer matrices [16], [17] size 2×2. The summery of this work is: Section 2 includes new definition for representing an integer by integer matrices size 2×2. Section 3 explains the $IM_{2\times2}SD$ method for computing kP. Section 4 presents new computational results for calculating kP. The efficiency and security analysis is discussed in Section 5. Finally, Section 6 draws the conclusions.

1 Integer Matrices Size 2×2

This section presents new definition to represent any integer as a square matrix size 2×2. This definition is given by

Definition 1.1. *(Integer Matrix Size 2×2). Let g be any element in Z^+. The integer matrix size 2×2 is defined by*

$$g_{M_{2\times2}} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

such that

$$Tr_1(g_{M_{2\times2}}) + Tr_2(g_{M_{2\times2}}) = a + d + b + c = g.$$

Remark 1.2. *1. With p is a prime number, it is easy to define the prime matrix size* 2×2 *by*

$$p_{M_{2\times 2}} = \begin{bmatrix} e & f \\ h & i \end{bmatrix}$$

such that

$$Tr_1(p_{M_{2\times 2}}) + Tr_2(p_{M_{2\times 2}}) = e + i + f + h = p.$$

2. With g is a negative number, it is easy to define the matrix size 22 by

$$-g_{M_{2\times 2}} = -\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

such that

$$-[Tr_1(g_{M_{2\times 2}}) + Tr_2(g_{M_{2\times 2}})] = -(a + d + b + c) = -g.$$

2 Integer Matrix Size 2×2 Sub- Decomposition Method

This section proposes new version of the integer sub-decomposition (ISD) method for computing the elliptic scalar multiplication. It uses the integer matrices size 2×2 to represent the scalar k and sub scalars k_{11}, k_{12}, k_{21} and k_{22} in ISD method to compute the kP. First step is to represent a scalar k as an integer matrix size 2×2 by

$$k_{M_{2\times 2}} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$$

such that

$$\begin{aligned} Tr_1(k_{M_{2\times 2}}) + Tr_2(k_{M_{2\times 2}}) &\equiv k_{11} + k_{22} + k_{12} + k_{21} (mod\ n) \\ &\equiv [k_{11}]_{2\times 2} + [k_{22}]_{2\times 2} \cdot \lambda_1 + [k_{12}]_{2\times 2} + [k_{21}]_{2\times 2} \cdot \lambda_2 (mod\ n) \\ &\equiv k (mod\ n), \end{aligned}$$

where $[k_{11}]_{2\times 2}, [k_{22}]_{2\times 2}, [k_{12}]_{2\times 2}$ and $[k_{21}]_{2\times 2}$ are integer matrices size 2×2 are given by

$$[k_{11}]_{2\times 2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, [k_{22}]_{2\times 2} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}, [k_{12}]_{2\times 2} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

and

$$[k_{21}]_{2\times 2} = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix}$$

with $\lambda_1, \lambda_2 \in [1, n-1]$. The integer matrix size 2×2 sub-decomposition ($IM_{2\times 2}SD$) for computing the elliptic scalar multiplication kP can be expressed by

$$\begin{aligned} kP &\equiv [k_{11}]_{2\times 2}P + ([k_{22}]_{2\times 2} \cdot \lambda_1)P + [k_{12}]_{2\times 2}P + ([k_{21}]_{2\times 2} \cdot \lambda_2)P \\ &\equiv \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} P + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \cdot \lambda_1 P + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} P + \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} \cdot \lambda_2 P \end{aligned}$$

3 Computational Results of the $IM_{2\times 2}SD$ Method

Let $p = 61$ be a prime number. Suppose E is defined by $y^2 \equiv x^3 + 4x + 1$ over F_61. Let $P = (44, 12)$. The scalar multiplication kP with $k = 54$ which lies in the range $[1, 66]$ is computed using a new version $IM_{22}SD$ method by

$$\begin{aligned} 54_{M_{2\times 2}} &\equiv \begin{bmatrix} 5 & 8 \\ 16 & 25 \end{bmatrix} \\ &\equiv Tr_1(54_{M_{2\times 2}}) + Tr_2(54_{M_{2\times 2}}) \ (mod\ 67) \\ &\equiv 5 + 25 + 8 + 16 \ (mod\ 67) \\ &\equiv 5_{M_{2\times 2}} + 5_{M_{2\times 2}} \cdot 5 + 8_{M_{2\times 2}} + 4_{M_{2\times 2}} \cdot 4 \ (mod\ 67) \\ &\equiv \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot 5 + \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \cdot 4 \ (mod\ 67) \end{aligned}$$

where the elements in matrices $5_{M_{2\times 2}}, 8_{M_{2\times 2}}, 4_{M_{2\times 2}} < 5, 8, 4$. The integer matrix size 2×2 sub-decomposition ($IM_{2\times 2}SD$) of computing the elliptic scalar multiplication kP is done by

$$\begin{aligned} 54_{M_{2\times 2}}P &\equiv \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} P + \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot 5P + \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} P + \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \cdot 4P \ (mod\ 61) \\ &\equiv (P + 2P + P + P) + (P + 2P + P + P) \cdot 5 + (2P + 2P + 2P + 2P) \\ &\quad + (P + P + P + P) \cdot 4 \ (mod\ 61) \\ &\equiv [(44, 12) + (56, 10) + (44, 12) + (44, 12)] + [(44, 12) + (56, 10) + (44, 12) \\ &\quad + (44, 12)] \cdot 5 + [(56, 10) + (56, 10) + (56, 10) + (56, 10)] + [(44, 12) \\ &\quad + (44, 12) + (44, 12) + (44, 12)] \cdot 4 \ (mod\ 61) \\ &\equiv (18, 7) + 5 \cdot (18, 7) + (16, 14) + 4 \cdot (59, 30) \\ &\equiv (18, 7) + (55, 26) + (16, 14) + (41, 20) \\ &= (24, 47). \end{aligned}$$

Other experimental results over a prime field F_{61} with different values $k \in [1, 66]$ are given in Table (1).

Table 1: Experimental results of $IM_{2\times2}SD$ method over F_p.

k	$k_{M_{2\times2}}$	k_{11}	k_{22}	k_{12}	k_{21}	λ_1	λ_2	$\begin{matrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{matrix} + \begin{matrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{matrix} \cdot \lambda_1$ $\begin{matrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{matrix} + \begin{matrix}d_{11} & d_{12}\\ d_{21} & d_{22}\end{matrix} \cdot \lambda_2$	kP
63	$\begin{bmatrix}10 & 11\\ 12 & 30\end{bmatrix}$	10	30	11	12	3	3	$\begin{matrix}3 & 3\\ 2 & 2\end{matrix} + \begin{matrix}3 & 3\\ 2 & 2\end{matrix} \cdot 3$ $\begin{matrix}3 & 3\\ 3 & 2\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 3$	(59,31)
43	$\begin{bmatrix}9 & 10\\ 16 & 8\end{bmatrix}$	9	8	10	16	2	4	$\begin{matrix}3 & 2\\ 2 & 2\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 2$ $\begin{matrix}3 & 3\\ 2 & 2\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 4$	(43,40)
59	$\begin{bmatrix}10 & 11\\ 12 & 26\end{bmatrix}$	10	26	11	12	2	3	$\begin{matrix}3 & 3\\ 2 & 2\end{matrix} + \begin{matrix}3 & 4\\ 3 & 3\end{matrix} \cdot 2$ $\begin{matrix}3 & 3\\ 3 & 2\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 3$	(16,47)
38	$\begin{bmatrix}4 & 10\\ 16 & 8\end{bmatrix}$	4	8	10	16	2	4	$\begin{matrix}1 & 1\\ 1 & 1\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 2$ $\begin{matrix}3 & 3\\ 2 & 2\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 4$	(9,41)
29	$\begin{bmatrix}6 & 6\\ 9 & 8\end{bmatrix}$	6	8	6	9	2	3	$\begin{matrix}2 & 1\\ 1 & 2\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 2$ $\begin{matrix}2 & 1\\ 1 & 2\end{matrix} + \begin{matrix}1 & 1\\ 1 & 1\end{matrix} \cdot 3$	(9,20)

4 The Efficiency and Security Analysis

The sub-decomposition of the scalars using the integer matrix size 2×2 accelerates computing the kP. Also, it reduces the computational complexity of the ISD method in compare to the previous proposed ISD idea in [18]. In the current idea of ISD, it does not need to create the ISD generators,

so the computational complexity of this creation will be shorthanded. As well as most of the scalars values k in the range $[1, n-1]$ have matrices size 2×2 sub-decomposition, namely the scalars that previously did not have the GLV decomposition and ISD sub-decomposition, also here have the $IM_{2\times2}SD$ representations. Thus, the successful percentage for computing kP has been increased. On the other hand, the $IM_{2\times2}SD$ representations of the sub scalars k_{11}, k_{22}, k_{12} and k_{21} help us to perform the computation of kP is more faster in compare to previous proposed GLV and ISD methods, since the simulations computations are done with the same values of representing k_{11}, k_{22}, k_{12} and k_{21} as matrices size 2×2 speed up computing of kP. Furthermore, the most important point with the proposed $IM_{2\times2}SD$ method is to increase the security, since the random generation of the matrices size 2×2 that are corresponded to the sub scalars k_{11}, k_{22}, k_{12} and k_{21} takes many probable cases. Each element in any matrix can take all the possible values that are lying in $[1, n-1]$ and less than k_{ij} for $i = j = 1, 2$ or $i \neq j, i, j = 1, 2$. Hence, it is more difficult of attackers to determine the matrix size 2×2 for any sub scalars k_{ij}.

5 Conclusions

A new version of the ISD method which is called the $IM_{2\times2}SD$ method was proposed in this work which depended on the random integer matrices size 2×2 representations of scalar k and sub-scalars k_{11}, k_{22}, k_{12} and k_{21}. On the proposed $IM_{2\times2}SD$ method, faster computations resulted to determine kP which is core operation to compute the public key and the ciphertext in ECCs. The security with using $IM_{2\times2}SD$ method was determined as well based on the difficulty to recover a secret key k from its random integer matrices size 2×2 representation. Attackers need to compute many cases of these representations. So the $IM_{2\times2}SD$ method for computing kP was fast and more secure for ECCs.

References

[1] Darrel Hankerson, Alfred J. Menezes, Scott Vanstone, Guide to elliptic curve cryptography, Springer Science and Business Media, 2006.

[2] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, Frederik Vercauteren, eds., Handbook of elliptic and hyper-elliptic curve cryptography, CRC press, 2005.

[3] Victor S. Miller, Use of elliptic curves in cryptography, Springer Berlin Heidelberg, 1986, 417–426.

[4] Neal Koblitz, Elliptic curve cryptosystems, Mathematics of computation, **48,** no. 177, (1987), 203–209.

[5] Yuanling Hao, Shiwei Ma, Guanghua Chen, Xiaoli Zhang, Hui Chen, Weimin Zeng, Optimization algorithm for scalar multiplication in the elliptic curve cryptography over prime field, In Advanced Intelligent Computing Theories and Applications, 4th International Conference on Intelligent Computing, Shanghai, China, Proceedings 4, Springer Berlin Heidelberg, (2008), 904–911.

[6] Robert P. Gallant, Robert J. Lambert, Scott A. Vanstone, Faster point multiplication on elliptic curves with efficient endomorphisms, Advances in CryptologyCRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, Proceedings, Berlin, Heidelberg: Springer Berlin Heidelberg, (2001).

[7] Dongryeol Kim, Seongan Lim, Integer decomposition for fast scalar multiplication on elliptic curves, Selected Areas in Cryptography: 9th Annual International Workshop, SAC 2002 St. Johns, Newfoundland, Canada, Springer Berlin Heidelberg, (2003).

[8] Zhenghua Zhou, Zhi Hu, Maozhi Xu, Wangan Song, Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves, Information Processing Letters **110,** no. 22 (2010), 1003–1006.

[9] Steven D. Galbraith, Xibin Lin, Michael Scott, Endomorphisms for faster elliptic curve cryptography on a large class of curves, Journal of cryptology **24,** no.3, (2011), 446–469.

[10] Ruma Kareem K. Ajeena, Hailiza Kamarulhaili, Analysis on the Elliptic Scalar Multiplication Using Integer Sub-Decomposition Method, International Journal of Pure and Applied Mathematics, **87**, no. 1, (2013), 95–114.

[11] Ruma Kareem K. Ajeena, Hailiza Kamarulhaili, Point multiplication using integer sub-decomposition for elliptic curve cryptography, Applied Mathematics & Information Sciences **8,** no. 2, (2014), 5–17.

[12] Ruma Kareem K. Ajeena, Integer sub-decomposition method for elliptic curve scalar multiplication, Diss. Universiti Sains Malaysia, (2015).

[13] Ruma Kareem K. Ajeena, Hailiza Kamarulhaili, A hybrid approach for elliptic scalar multiplication, AIP Conference Proceedings, **1660,** no. 1, AIP Publishing LLC, (2015).

[14] Ruma Kareem K. Ajeena, The soft graphic integer sub-decomposition method for elliptic scalar multiplication, Journal of Discrete Mathematical Sciences and Cryptography, **24,** no. 6, (2021), 1751–1765.

[15] Jolan Lazim Theyab, Ruma Kareem K. Ajeena, The 3-dimension integer sub-decomposition method for Edwards curve cryptography, AIP Conference Proceedings, **2398,** no. 1, AIP Publishing LLC, (2022).

[16] John Henry Wilkinson, Friedrich Ludwig Bauer, C. Reinsch, Linear algebra, **2,** (2013).

[17] Karim M. Abadir, Jan R. Magnus, Matrix algebra, **1,** Cambridge University Press, (2005).

[18] Ruma Kareem K. Ajeena, Hailiza Kamarulhaili, The computational complexity of elliptic curve integer sub-decomposition method, AIP Conference Proceedings, **1605**, no. 1, American Institute of Physics, 2014.