Deployment Consideration on Secure Computation for Radix-16 Scalar Multiplication

Gautam Kumar[1(✉)], Hemraj Saini[2], and U. M. Fernandes Dimlo[1]

[1] Department of Computer Science and Engineering, Narsimha Reddy Engineering College, Maisammaguda, Secundarabad 500100, TS, India
gautam2lujrb@gmail.com, mariaprakashu2000@yahoo.com
[2] Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan 173234, HP, India
hemrajl977@yahoo.co.in

Abstract. An Elliptic Curve Cryptography (ECC) algorithm is one of the most powerful with respect to better security and performance than RSA algorithm. Most of applications prefer to implement this approach due to the use of shorter key sizes, low computation costs and most probably the discrete logarithmic problem is hard to achieve. In addition to it, with the support of hardware most of computation costs have been reduced in the general observation and widely available the reduction of pre-computed operations using strategies is playing one of the concerns in research gap creation. In the manuscript, we analyzed the proposed Radix-16 scalar multiplications without pre-computation for ECC and considered to be one of advanced approach technique, which is counted in the form of reduced complexity costs, reliable and secure computing. It also consists in relation to the more appropriateness for low memory devices and reduced instruction set computing, therefore a possible deployment is considered.

Keywords: ECC · PKC · Scalar multiplication · Radix-16 · Complexity

1 Introduction

Cryptography is one of most important technique used to hide the original information when it hangs in between the medium. It is considered to be a science with respect to the secret information to be safe, where algorithms are playing crucial role responsiveness. In a modern day applications, cryptography is a mixed resultant of the three disciplines such as mathematical approach, make it programmable through the use of computer science and finally make it applicable to end users support on electronically implementable. In all these respects, the major attention to protect information from discloser, secure transmission in unsecured environment, authenticity, and integrity purposes [1].

Diffie and Hellman [2] were the first two authors who enlighten public key cryptography (PKC). After that variety of PKC algorithms are in propositions, but Elliptic Curve Cryptography (ECC) in all of them is attracting the most attention from the research community. A number of proposed algorithms have been showing the

M. Singh et al. (Eds.): ICACDS 2018, CCIS 906, pp. 205–216, 2018.
https://doi.org/10.1007/978-981-13-1813-9_21

appropriate security need, but the major problem is the use of higher key lengths. Due its increased overhead for computation doesn't a suite for low memory containing devices in the fast growing world, where ECC is able to give the almost equal level of security strengths on comparatively shorter key sizes, as recommended by the National Institute of Standard Technology (NIST). According to the NIST-2012 guideline, the differences in key size ratio (in bits) between RSA & ECC algorithm and a comparative protection strength from attack on relative is presented in Table 1:

Table 1. Differences in security strength of RSA vs. ECC

RSA	ECC	Key size ratio	Protection from attack
1024	160–223	1:6	Until 2010
2048	224–255	1:9	Until 2031
3072	256–383	1:12	Beyond 2031
7680	384–511	1:20	…
15360	512+	1:30	…

The difference is an abstract idea to implement in manufacturing devices and acting as a key role makes. If RSA algorithm is in used on 1024 bits, for the same level of security and strength ECC works on minimum of 160 bits. The report available on NIST considered to be secured on the given subsequent periods. The major attraction appears in speedup enhancement on ratio of key sizes. The use of ECC is releasing so many benefits in terms of faster computation costs, bandwidth consumptions, most efficient key generations, almost be safe on little higher lengths of the key, etc. In general, the computation cost is reduced with the development of the new and/or modifications in the proposed approaches. What so ever is evolved for ECC, but from the research point of view it is still an excess been considered and improvements in the same is possible issue with respect to the current computations [3].

Discrete Logarithmic Problem (DLP) is playing important role responsiveness in establishing the secure computation and is one of the major concerns in ECC, for ECC named by ECC-DLP. ECC-DLP is working on two elliptic points as an assumptions (P and Q) on the standard cubic curve equation, to determine the secret key used as k, that follow $Q = kP$, which is the heart of ECC in PKC and its building block for security issues [4]. It is based on algorithms on repeated point doubling (DBL) and point addition (ADD) operations on used scalar. DLP is one of the hearts of cryptography, where secret keys are full responsible for the same. The big significance releasing here from the research point of view is to do the computations costs with the reduced DBLs and ADDs operations and it is showing a motivations. The algorithms are playing a pivotal role for security guarantees and determining for the same in effective implementation. A low mark has been observed on the used algorithms if it is not with the appropriate satisfaction and convincing. Where, in the other ways, performances with faster algorithms are leading with high performance and high-speed in the growing field of computing and communication systems. If the assumptions proceeds in the

forward direction but behaves like negligible to revert back of used scalar k, is a major intention of the algorithms and scalar multiplication.

The three approaches are the basis for the smooth conduct of ECC operations. The first approach is its underlying operations on finite basis and either the operations based on binary field or prime fields arithmetic assumptions. The next approach is the used algorithm, the scalar representation, which decides their computational complexity costs. Here are some of the existing methods that are in the forms of Most Significant Bit (MSB) algorithm, Least Significant Bit (LSB) algorithm, Nonadjacent form (NAF), Window Method, Sliding Window Method, Width Nonadjacent Form, Frobenious Map and Radix-rNAF (r-NAF) [5–10]. Third approach uses both of the previous two approaches with the support of hardware utilizations that are effectively utilizing in reduction of pre-computation operations, and/or using in generalization of parallel operations [11–13] or/and pipelining approaches [14].

In this manuscript, the first and second approaches are combined to the third approach for dependability and likely safety measures are managed sufficiently in secure computing. The overall scenario is considered for an efficient scalar multiplication for the proposed ECC. The below following points are reflecting throughout in this presentation:

- An extended work from radix-8 to radix-16 scalar multiplication is available, that illustrates on how dependency varies from one existing platform to new platform and how measures of deployment varies.
- To analyze the security strength at various levels for its deployment i.e., power analysis, safe-error fault attacks, side channel attacks, computations costs, and in some generic considerations.

We have set the deployment of our proposed strategy is secure, stronger and efficient in comparisons to known approaches in reference to the ECC scalar multiplication algorithms. The difficult is on cryptanalysis for the cryptographers to find the used secret. In relation to the same our contribution is a deployment specification with respect to performance enhancement and security validity.

Our manuscript is organized as follows. Section 2 presents dependency on interrelated existing algorithms. In Sect. 3, the deployment perspective has been considered with the security related analysis that highlights the advantages of proposed strategy against the side channel attacks (SSCAs) and in general considered objective. Finally, we summarized our manuscript the same.

2 Dependency of Scalar Multiplication on Existing Algorithms

ECC is based on consistent operations, organized in hierarchy, and well designed on its interrelated four levels as like to be shown in Fig. 1. The top level keeps the used algorithms of ECC, which depends on scalar multiplication kP, where it depends on group operations, such as point doubling and point addition, and further these are considered in group operations based on arithmetic operations such as multiplication, subtraction, addition, inversion and squaring. Each level of operations consists in the

form of costs, where reduction in costs using the proposed methodology is one of the research gaps. A reference from [15] is tested on Star core 41000 series processor reporting a cost for one doubling is 14,000 clock cycles and for one addition is 13,617 clock cycles.

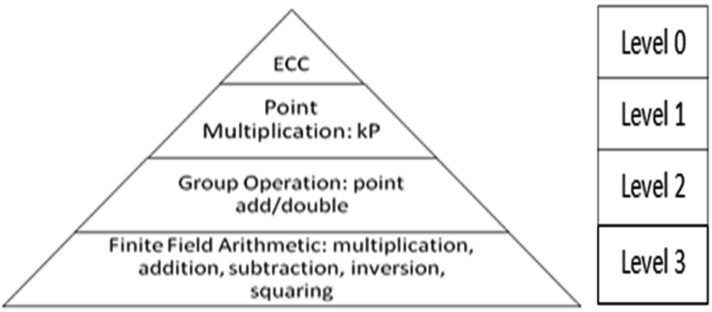

Fig. 1. Hierarchy of ECC

The most motivational concern in ECC is reduction in the computational costs. The architectural behavior of ECC is tested on the various algorithms for its better performance and is treated in the forms of advanced algorithms for end users applications. Further, these are treated in systems performance. Each algorithm consists a section of computations are in the form of pre-computation and or use of critical section. Pre-computation is an act of operations before-or-in critical section midair. Here is highlighted of enormous thought of its existing algorithms with its relative costs. On secret key k, or in general it is scalar, is considered in m-bits. The Most-Significant-Bit (MSB) algorithm needs m doublings and on average $m/2$ bits of addition operations. Means any scalar of m = 128 bits based requires 128 * 14000 clock cycle of doubling and 64 * 13617 clock cycle of addition operations. In a similar fashion Least-Significant-Bit (LSB) algorithm needs on average $m/2$ bits of doublings and same bits of additions. But both algorithms are suffer from side channel attack is possible that try to abstract the original key used for the algorithm, which has been considered to an extra source of information gain from physical implementations such as electromagnetic leakages, power consumption and sound released from the systems. Electromagnetic leakage is alarming in a sense the signal passes through medium are decoding by the adversary through the use of auxiliary equipments, instead the signals are low signals but for the interested users vulnerabilities have been reported. In a similar sense on behalf of power consumption and sound leads as a extra source of vulnerabilities. One solution for eliminating the side channel attack is use of Montgomery algorithm; in this the complexity is higher in m doubling and m addition. Further, using non-adjacent form (NAF) is one of variation of algorithm use to avoid the side channel attack on reduced complexity on average $m/2$ additions and $m/2$ doublings, representation of algorithm is in $\{-1, 0, 1\}$ [16, 17]. Again a window (w-NAF) method has been proposed on reduced complexity $m/(w+1)$ in additions only [18, 19]. One more variation in window method is available on escaping the series of zero on w-NAF, named by

sliding w-NAF, also known by Frobenious operations, that has counted as an enhancement in scalar multiplication [20, 21]. For the complexity determination, hamming-weight is in general be used for scalar representation.

ECC is likely to be secure on shorter lengths keys, due this reason it is attracting a relatively more favorable attention in more appropriateness to end user applications, as well as most suit for short memory devices, higher performance achievers etc. The real life applications are widely available in the forms of smart-cards, internet banking, mobile banking, etc. for its efficient and secure implementation approach. The applications are considered in exceptionally good functionalities in addition that may not lead to any leakages [22]. Abdulrahman and Masoleh [23] proposed a methodology on Radix-8 scalar multiplication without pre-computations with resistance to side channel attack. The main advantage of this proposed approach is without using doubling and addition, they are directly switched to arithmetic operations. This has given a slightly a new path for scalar multiplication on the computation cost $\log_8(m+1)$.

Therefore, in relation to above already proposed methodologies are representing a research gap to find a more efficient method to accelerate the scalar multiplication for ECC. Here we are going to extend the work of Radix-8 scalar multiplication without pre-computation to Radix-16 scalar multiplication. Also, we are going to elaborate the execution dependency from the hardware in Fig. 2, (here only its designed/comparison is available, interested author(s) refer the base paper) where the hardware implementation in its computation cost (basis (1/3 to 1/4) in %) = 8.33% accelerated, in Fig. 3. Further, the software execution and performance in presented in Fig. 4, where the major objective is in the relation to find the more efficient technique for accelerating the scalar multiplication in Elliptic Curve Cryptography (through the series of identified research gap), and established the same in more appropriateness with resistance to side channel attacks and safe-error fault attacks. Therefore, the novel contribution is based on the proposed algorithm of Radix-16 scalar multiplication, which is established on computation cost at $\log_{16}(k + 1)$. Compare to recently proposed Radix-8 scalar multiplication algorithm from the implementation point of view, the software performance gets an acceleration on proposed methodology with the basic difference's in its base or its computation cost on (1/8 to 1/16) in % = 6.25%, in Fig. 5.

3 Deployment Perspective of Radix-16 Scalar Multiplication

The Radix-16 scalar multiplication methodology is presented by Gautam and Hemraj [24] to records the Discrete Logarithmic Problem (DLP) for its assumed significance on finite basis. The DLP is computationally probable infeasible to get the used secret (scalar) key. In relation to these preferences the software and hardware performances are significantly improved. Interested author(s) can refer the dependency graph for the solution presented in 'Secure and Efficient ECC: Radix-16 Scalar Multiplication without Pre-Computation'. The proposed scalar multiplication technique is enriching its benefits on low computation costs. The new era's are mostly looking with stronger security in connection to advanced security approaches, where our objective is meeting with the same. The major attention is to deploy the same for application purposes. The applications are in online and offline services, such as in data processing, transactions

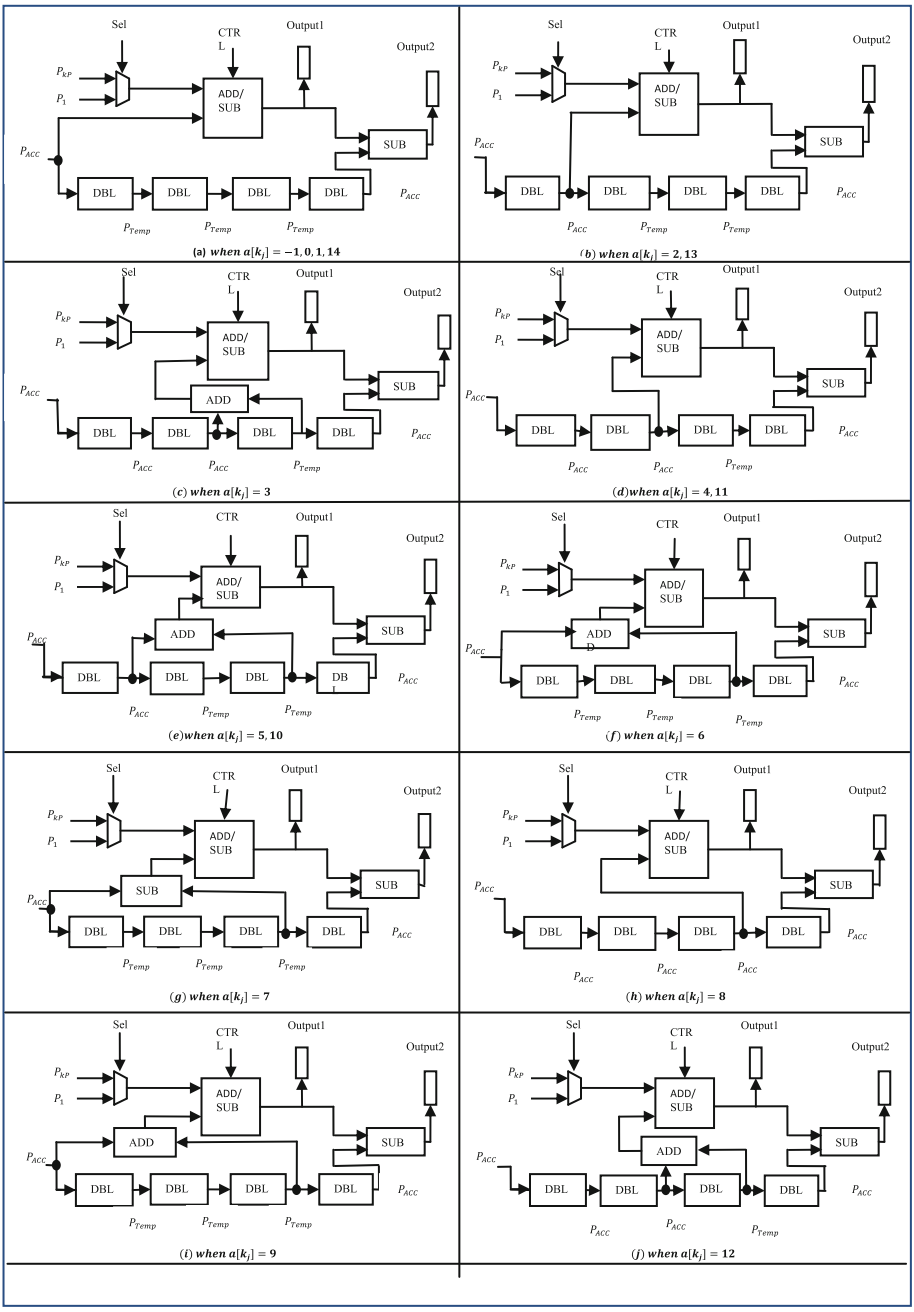

Fig. 2. Hardware dependency graph

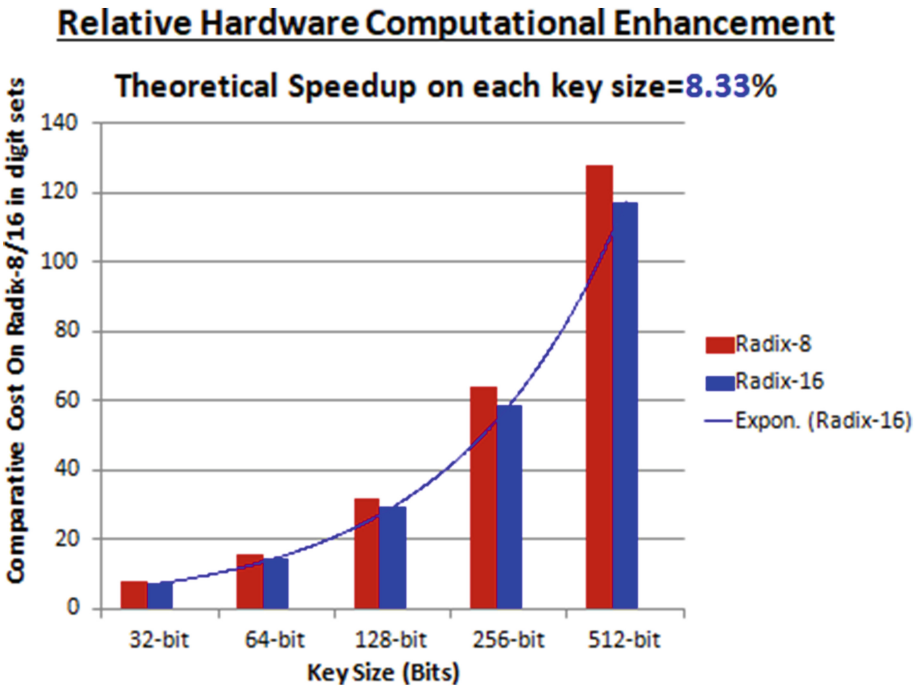

Fig. 3. Performance enhancement from hardware perspective

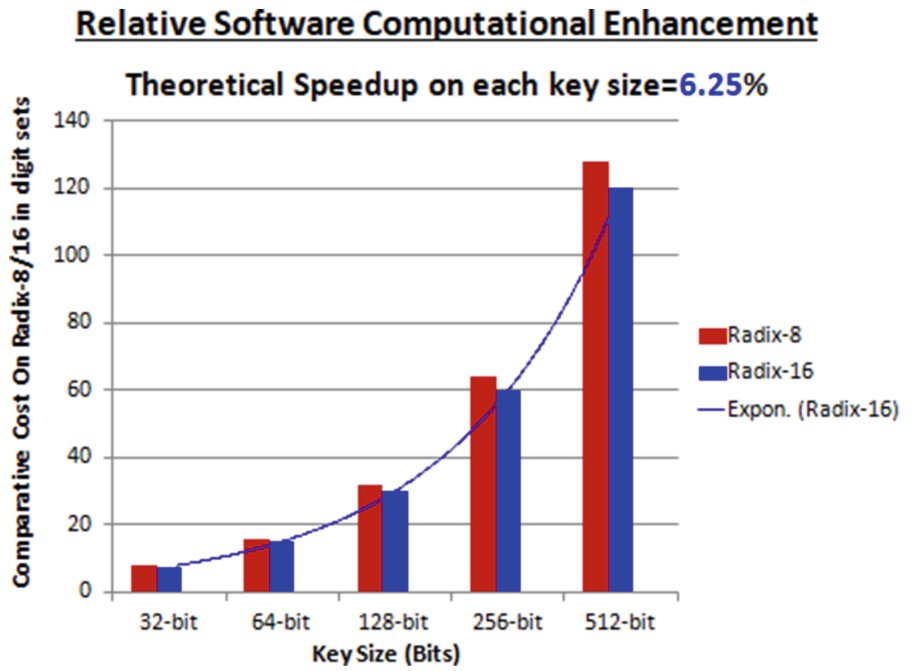

Fig. 4. Performance enhancement from hardware perspective

are most favorable cases. Implementing the same in firmware as a component of security points are also be a considerable situations.

3.1 Side Channel Attacks

Side channel attack defines an information gain from physical implementation such as electromagnetic leakages, power consumption, or sound that can give an extra source of information but it doesn't care about the theoretical computation or brute force attacks. It has considered independently outside the computation phase. This has been added to provide the various services against the following scenarios such as Power Analysis Attacks, Timing Attacks, Differential Faults Attacks, Data remanence etc.

Fig. 5. Comparison in radix-8 and radix-16

3.2 Power Analysis Attacks

The power analysis provides the detailed information about the power consumption by the CPU or cryptographic circuits. The attacks are differentiated in simple power analysis (SPA) and differential power analysis (DPA). The SPA interprets power traces, or graphs generations on electrical activity shown over time. Whereas the DPA allows the attacker to compute intermediate cryptographic computations on statistical

analysis collected from multiple operations. Using the newly introduced algorithm of radix-16 scalar multiplication in operation with the hardware support, power analysis attack can mostly be too sophisticated. In case of power analysis, the adversary(s) try to get secret key information either from internet, passing information through channel or from physical implementation. In a similar fashion its analysis is categorized on SPA and DPA. SPA observes the proposed scheme is fixed. The scheme is intrinsic confined against simple side channel attacks on each iterations in the main loop involment. It is observed from the adopted design principles, any dummy operations except in its domain brings an incorrect result on scalar. It is in favor to safe-error fault attacks if any inclusion.

3.3 Timing Attacks

The transmissions of signals release are the part of computer operations. But, due to interested adversary that try to abstract the pattern using the cryptographic algorithms and same pattern generations for its security appearances may lead to vulnerable issues. This is treated as a stunning that is alarming in the two senses: (i) a random interference comes first, which can be only be burglars, and (ii) these signals can be amplify through some auxiliary equipments for some useful purposes. A report is available that are suggesting on electromagnetic radiation interference with radio navigation devices, as (i) it is a general procedure and it is not a point to be considerable issue, but if (ii) applies who are interested in generating of such pattern of abstraction, then decoding and restoration can lead to vulnerable information safety, feedbacks and/or secret information leakage, where an adversary try to determine the private key by keeping track on how long a computer takes to decipher the secrets messages. In practice, proposed assumptions do lead to extreme timing variations. So in regards to the same enough variations to make the algorithms be a practical choice for applications.

3.4 Differential Fault Analysis

The differential fault analysis principle induces on faults due to unexpected conditions on environmental factors using the cryptographic algorithms design and implementations that steals to their internal working. Where, our proposed approach is meeting with the cryptographic function generations on fixed computations costs on multifold security properties. The real beauty of the algorithm lies on working nature in support of hardware perspective. Due this nature, the most level of confusion is applied to frustrate the adversaries.

3.5 Data Remanence

The data remanence is one of the important factor that represents the residual information that release or hide the information in likely intractable forms. The resultant residual may left intact information, or keeps nominal information even after deletion, or reformatting does not erase the data for verification purpose at later stage, or physical properties may be recoverable on previous used activity. It may make inadvertent in

uncontrolled environment to sensitive information. Depending on the used algorithms, a vast amount of algorithms are available for data remanence. But, some specific methods are possible through which encryption, destruction, overwriting and disgusting is possible, where radix-16 releasing benefits low computations costs.

3.6 Brute-Force Attacks

Possibly finding all the secret key and making a defense attacks the proposed approach is suit here, and using the hardware support it adds the additional strengths. This type of approach considered to be the special case in Elliptic Curve Cryptography. Therefore the presented scenario is sufficiently works on the smaller keyed length. In relation to the same, the execution time takes a shorter time for execution and reflects a big impact on efficiency consideration. A sufficient number of reports are available in regard to the computational performance in comparison to ECC and RSA algorithms, where our approach in regards the speed, efficiency, and cryptanalysis are better in many ways.

3.7 Chosen-Ciphertext Attacks

This attack is a form of active attack, where adversaries try to find plaintext corresponding to its ciphertexts by its choice. The first choice may experience on decryption module on a random chosen ciphertexts, before the actual ciphertext sent for an interested use. The second choice involves the same module on input of one's choice at any time, where these all are recorded and try to gain the actual plaintexts. As the presented algorithm experience a blind feedbacks, where the Noncommutative cryptography is not a vulnerable one to chosen ciphertext attacks (CCA) especially for ring or semi-ring, group and Heisenberg elements; because in CCA an adversary chooses a number of ciphertext and try to decrypt with targeted private keys, where the chosen cipher text is hashed with the corresponding polynomial exponentials.

3.8 General Consideration

Radix-16 scalar multiplication is lowering feasibility parallel consideration on arithmetic operations. The abstract reason clears the fundamental principle on computation of hexadecimal on binary information conversion. To add a random delay in the proposed algorithm is one of the good way to more frustrate the adversaries, instead of the same blinding creation in modulus and/or exponential of the computational procedure. It offers relatively faster computation, less memory requirements, and smaller execution of memory area.

4 Conclusion

In this manuscript, a radix-16 scalar multiplication deployment scenario is presented. Using this approach, as assessment of digit set elements are identify uniquely by a single digit set of used Radix-16 algorithm, so this may be considered as one of the advanced way to do the computation and applicable for desired applications in the

rapidly growing world. The scheme presentation is considered in software implementation point of view as well as hardware, where securities and performance are the most in demand and scarce resources use is the issue. In relation to same, reduced instruction set computing is one of the most suitable methods for widely applicable and use of short-memory devices are most attractive with resistant to simple-side channel attack and safe-error fault attack on deployment considerations.

References

1. Jirasek, V.: Practical application of information security models. Inf. Secur. Tech. Rep. **17** (1–2), 1–8 (2012)
2. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
3. Jarvinen, K., Skytta, J.: Parallelization of high-speed processor for elliptic curve cryptography. IEEE Trans. VLSI **16**(9), 1162–1175 (2008)
4. Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. **48**(177), 203–209 (1987)
5. Miller, V.S.: Use of elliptic curves in cryptography. Adv. Cryptol. **218**, 417–426 (1986)
6. Izu, T., Takagi, T.: Fast elliptic curve multiplications with SIMD operations. In: Deng, R., Bao, F., Zhou, J., Qing, S. (eds.) ICICS 2002. LNCS, vol. 2513, pp. 217–230. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36159-6_19
7. Knudsen, E.W.: Elliptic scalar multiplication using point halving. In: Lam, K.-Y., Okamoto, E., Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 135–149. Springer, Heidelberg (1999). https://doi.org/10.1007/978-3-540-48000-6_12
8. Blake, I.F., Murty, V.K., Xu, G.: A note on window τ-adic NAF algorithm. Inf. Process. Lett. **95**, 496–502 (2005)
9. Hankerson, D., Vanstone, S., Menezes, A.: Guide to Elliptic Curve Cryptography. Springer Professional Computing. Springer, New York (2004). https://doi.org/10.1007/b97644
10. Arno, S., Wheeler, F.S.: Signed digit representations of minimal hamming weight. IEEE Trans. Comput. **2**(8), 1007–1010 (1993). https://doi.org/10.1109/12.238495
11. Longa, P., Miri, A.: Fast and flexible elliptic curve point arithmetic over prime fields. IEEE Trans. Comput. **57**(3), 289–302 (2008)
12. Faye, Y., Guyennet, H., Niang, I., Shou, Y.: Fast scalar multiplication on elliptic curve cryptography in selected intervals suitable for wireless sensor networks. In: Wang, G., Ray, I., Feng, D., Rajarajan, M. (eds.) CSS 2013. LNCS, vol. 8300, pp. 171–182. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-03584-0_13
13. Fischer, W., Giraud, C., Knudsen, E.W., Seifert, J.P.: Parallel scalar multiplication on general elliptic curves over F(p) hedged against non-differential side-channel attacks. In: IACR (2002/007) Cryptology ePrint Archive (2002). http://eprint.iacr.org/2002/007
14. Mishra, P.K.: Pipelined computation of scalar multiplication in elliptic curve cryptosystems (extended version). IEEE Trans. Comput. **55**(8), 1000–1010 (2006)
15. Gebotys, C.H. (ed.): Security in Embedded Devices, pp. 75–109. Springer, New York (2010)
16. Heuberger, C., Pondinger, H.: Analysis of alternatives digits sets for non-adjacent representation. SIAM J. Discrete Math. **19**(1), 165–191 (2006)
17. Okeya, K., Takagi, T.: The width-*w* NAF method provides small memory and fast elliptic scalar multiplications secure against side channel attacks. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 328–343. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36563-X_23

18. Vuillaume, C., Okeya, K., Takagi, T.: Short-memory scalar multiplication for Koblitz curve. IEEE Trans. Comput. **57**(4), 481–489 (2008). https://doi.org/10.1109/TC.2007.70824
19. Okeya, K., Kurumatani, H., Sakurai, K.: Elliptic curves with the montgomery-form and their cryptographic applications. In: Imai, H., Zheng, Y. (eds.) PKC 2000. LNCS, vol. 1751, pp. 238–257. Springer, Heidelberg (2000). https://doi.org/10.1007/978-3-540-46588-1_17
20. Ciet, M., Lange, T., Sica, F., Quisquater, J.-J.: Improved algorithms for efficient arithmetic on elliptic curves using fast endomorphisms. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 388–400. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_24
21. Parhami, B. (ed.): Computer Arithmetic: Algorithms and Hardware Designs. Oxford University Press, New York (2010)
22. Avanzi, R.M., Heuberger, C., Prodinger, H.: On redundant τ-adic expansions and non-adjacent digit sets. In: Biham, E., Youssef, A.M. (eds.) SAC 2006. LNCS, vol. 4356, pp. 285–301. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74462-7_20
23. Abdulrahman, E.A.H., Reyhani-Masoleh, A.: New regular radix-8 scheme for elliptic curve scalar multiplication without pre-computation. IEEE Trans. Comput. **64**(2), 438–451 (2015)
24. Kumar, G., Saini, H.: Secure and efficient ECC: radix-16 scalar multiplication without pre-computation. In: International Conference on Big Data and Advanced Wireless Technologies. ACM Digital Library, USA (2016). https://doi.org/10.1145/3010089.3010105