Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1487–1496
DOI : 10.47974/JDMSC-2147

Telemedicine formal verification using lightweight cryptography : An efficient, robust, and secure Radix-16 scalar multiplication in application validate

Gautam Kumar [§]
Department of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Atul Srivastava [†]
Department of Computer Science and Engineering
Amity School of Engineering and Technology
Amity University
Lucknow 226028
Uttar Pradesh
India

Vijay Shankar Sharma *
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Anuradha Pillai [‡]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Pune 412115
Maharashtra
India

[§] *E-mail:* gautam.kumar@jaipur.manipal.edu
[†] *E-mail:* atul.nd2@gmail.com
* *E-mail:* vijayshankar.sharma@jaipur.manipal.edu (Corresponding Author)
[‡] *E-mail:* anuradha.pillai@sitpune.edu.in

© Taru Publications

Abstract

The Elliptic curve cryptography (ECC) in cryptography is an interesting to go into the depth of the best performance optimization and fascinating area to work, where scalar multiplication is playing an important role and giving the insight in gaining the computation efficiency. A good efficient technical way is possible through the reduced number of precomputed operations use on scalar multiplication. The research gap shows here a systematic approach for one of the more efficient techniques is possible too by comparing to the most recent in variations of scalar multiplication schemes. We have proposed and applied Radix-16 Scalar Multiplication scheme which works without precomputation. The hardware and the software performances are representing a marginal enhancement in all the related proposed techniques on theoretical speedup on each key size=6.25% and on software perspective speedup on each key size=8.33%. The logic behind to take problem is to work on a smaller key to the best suits for the low memory devices, to initiate the operation on shorter clock cycles, and high speed to achieve with integrating to the marginal high level of security strengths. A Telemedicine application-oriented work is presented in this manuscript using the ECC, as a part of the lightweight cryptography approach, and a robust application scenario on reduced computational complexity. The approach is efficient, robust, and secure enough mathematically to justify the claimed work. Further, the formal verification tool AVISPA/SPAN is used to validate the considered work.

Subject Classification: *Primary 94A60, Secondary 94A62.*

Keywords: *ECC, Precomputation, Telemedicine, Radix-16 scalar multiplication, Non-fifteen Encoding.*

1. Introduction

In real life problems security and performance are the two important scenarios to concerns, implement and validate to apply for any of the applications use. The optimal performances are achievable using the optimized algorithms in reference to available scenarios. In likely for all general observations, the designed algorithms are having the basis on reduced cost of communication and computations. In addition to this, many necessities are still to be interesting concerns and demand in related to more better security services system and enhanced performance systems [1]. A Telemedicine application is attracting the work scenario in day-by-day. Its overall aim is to follow structured provisions for assessing the quality care, effectiveness, and reduced cost contributions in almost all research works. An assessment review is based on scientific methodologies to apply the same in real-life practice [2].

From the technical point of view available, the public key cryptography (PKC) was firstly created by Diffie and Hellman, in the year 1976 [3]. Then after many PKC algorithms have been projected, where Elliptic Curve Cryptography (ECC) has attracted in the highest attentions among all. ECC work on the shorter key sizes and secure enough to strengthen security compared to some of the well-known RSA algorithm, whereas other algorithms

also need a very larger key size length for realizing the equal strength of security concerns. The shorter keys compute much faster on computer system, it is suiting the best in the practice to low memory devices. Further to say, scalar multiplication is a mathematical operation in ECC and algorithm does the same scalar multiplication using repeated call of addition and doubling. Therefore, in concerns to security points of view it suits best in practice. One of comparison dictates the best RSA algorithm needs 1024 key-bits, and in comparison, to ECC uses 160 key-bits only in size, for the same level of security strength [4]. Therefore, ECC is in standardized discovery, which is directly reducing the processing overhead. We have analyzed and worked on the algorithms for ECC as a core cryptographic work [5].

The manuscript work is organized in the following fashions. Section 2 presents background details about applications with the technology augmentation. Section 3 presents the telemedicine application scenario that works for the research point of view. The Radix-8 and Radix-16 techniques without precomputation for the scalar multiplication, presented in section 4. Both techniques are comparatively showing the computation, reduced cost reductions, and enhanced performance its related works. Section 5 applies with formal verification using AVISPA/SPAN tools working and its validation. At the end, we summarized our manuscript.

2. Background

Telemedicine studies and reports [6] have explored the advantages, cost-savings and gain in efficiency by feasibly implemented with technological works and inline the systems in digitized process. But this application is contributing its benefits through online training and education awareness on geographical exposure and are claiming its cost efficient (computation and communication cost) and its effectiveness (time saving, economic benefits, resource) in the real world.

In general, now a days most of the healthcare services deals with Telemedicine using the Information Communications Technologies (ICT) [7], where a two-way communication can be best utilized as service from any user as a professional in health sector and sick persons or in close association with professionals in healthcare's. The services may to sicker observation, treatments, tracking diseases, education among the workforce in healthcare and new knowledge sharing or conducts. But some of the studies are the motivational concerns, where it doesn't come into the accepted standards building a robust for innovations needs further development. Further to say transferability assessment scale up results to the large extent and the participants may have many assessments, such as model should be defined, clear, potential effective, relevant, outcome measurable and should be included issues.

3. Applications Scenarios for Telemedicine

The application scenario we have considered between medical practitioner and a patient, which finds its effectiveness on presented data's. In general

consideration in sharing information computers, hardware devices such as network cables, cameras, and designed radix-8 algorithms. In general resources considers as computer(s), computing devices, networks, speaker(s)s, camera(s), image(s), cable(s)s, and more. The algorithm radix-8 is corelated with work, as depicted in figure 1, where more about Radix-8 is described in the upcoming section. It shows a two-way communication, discussing a simple medical diagnosis, where both are not at the same place too, follow-ups, diagnosis report reception, and prescription design. The major thing is of accessing the mainstream of medicine having specialist, large scale facilities accessible and, broadening the services and more, but with the advanced technique was missing with scientific evidence and may extended to a large-scale too.

Figure 1
Telemedicine Scenario

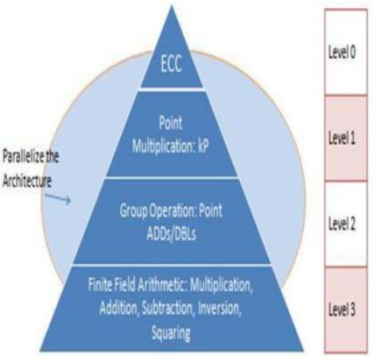

Figure 2
Hierarchy of ECC Operations

For the advanced aspects in Cryptography Discrete Logarithmic is considered to the backbone in this field, which acts as a central role on applied algorithms in security. It refers to required precomputed operations before to initiate any task. Rigorous research is in continuation to reduce the precomputation. An algorithm is said to be faster and efficient on the precomputed operations, if algorithms run on high-speed with reduced precomputed operations.

DLP works for ECC on two points P and Q on which is defined the elliptic curve, as a secret key k, $Q = kP$, which builds a core building blocks in public key cryptography [8]. The ECC function in cryptography computes, with repeatedly calls of point(s) additions (ADD) and doublings (DBL). One of the major advantages with ECC is that it works on very shorter key sizes relative to the RSA algorithm and best suites to short-memory devices that ensure its standardization globally on a bigger extent. Such devices are mobile banking, net banking, smart cards, and many real-time efficient applications to fit into the same.

An ECC working is defined in levels with the hierarchal and consistent operations, having the four interrelated levels in correlation. As presented in Figure 2, level 0 is highest level that keeps ECC defined algorithms to apply. The designed algorithms consist of scalar multiplication kP, defined on level 1, further scalar multiplication consists of combinations of operations as point additions ADDs and/or operations of doubling DBLs, and these ADDs and DBLs are further be dependent to microlevel of operations such as multiplication, addition, subtraction, inversion, and squaring as a micro-level operation. The defined precomputed operations in [9] by Catherine H. Gebotys is presented $13{,}617$ clock cycles for one addition (ADDs) operation and $14{,}000$ clock cycles are for one point doubling (DBLs) operations that decides the complexity of the working system. Here, important scalar multiplication techniques are presented with it computation costs, the existing algorithms are (i) MSB- the Most Significant Bit first, (ii) LSB- the Least Significant Bit first, (iii) NAF- Nonadjacent form, (iv) Window Method, (v) Sliding Window Method, (vi) Width Nonadjacent Form, (vii) Frobenious Map and (viii) Radix-rNAF (r-NAF) and (ix) Radix-rNAF (r-NAF) [10],[11]. For a clear understanding to know we shall explore the same using the mathematical model.

Let's assume k is a secret key or scalar value, in m bits binary values. MSB techniques needs m doubling (DBLs) (in no. of bits of scalar representation) and $\mathrm{m}/2$ addition (ADDs) (on an average half of scalar bits) operations. In a similar fashion, if we see the LSB first algorithm, it contains in average case $\mathrm{m}/2$ ADDs and same label of bits for DBLs. If we consider on likely high length key, it's a huge complexity. Further to say, a non-adjacent form (NAF) available in the forms of $\{1, 0, -1\}$, algorithm on $\mathrm{m}/2$ ADDS in average case and $\mathrm{m}/2$ DBLs are needed for this algorithm, but we receive an additional advantage as benefits of side-channel attacks [12]. One of the variations of NAF, w-NAF the complexity is $\mathrm{m}/(\mathrm{w}+1)$ ADDs, means no DBLs needed as huge advantageous. One more variation of w-NAF is possible too, named as sliding w-NAF (or Frobenious), that does scalar multiplication by escaping the series of zeros.

4. Proposes Radix-8 Recording Technique

In 2015, [13] presented techniques on Radix-8 computation short of precomputation and model for the avoidance of simple side channel attacks (SSCAs) is a convincing. It is proposed on without precomputed operations on Radix-8 scalar multiplications. This computes on $log_{8^{(k+1)}}$ without (ADDs & DBLs) operations are one of the bigger technology augmentations. The field and point arithmetic parallelism enhance its speedup due to the properties of this algorithm. The secret scalar k computes the range of $[-1, 6]$ for DLP, which counts its run time complexity and it is close in fashioned to the above designed algorithms and approaches [14].

4.1 *Radix Scalar Representation Brief*

Let the secret key scalar k of having the length of m-bits and the base is r in power of 2, as $r = 2^w$, and w is $2 \leq w \leq m-1$. Then, the scalar multiplication defined as rP by repeated calls DBLs, for an elliptic point . The scalar is signed representation and divided into l bits, $l = \lceil \frac{m}{w} \rceil$, and digit each of k as k_i' for $0 \leq i \leq l-1$. In general, the scalar k contains n more expansions $(k_{l-1}', \ldots, k_1', k_0')_r$, where $k_i' \in \{0,1, \ldots \ldots, r-1\}$ for $i \leq l-1$, available in equation (1):

$$k = \sum_{i=0}^{l-1} k_i' r^i, k_i' \in \{0,1, \ldots \ldots, r-1\} \quad (1)$$

The scalar multiplication kP as in (2):

$$kP = \sum_{i=0}^{l-1} k_i' r^i \mathrm{P}. \quad (2)$$

For an identity, one of the abelian considerations with an elliptic point $E(F_q)$ Ò, let $P \in E(F_q)$ is an initial point. The scalar multiplication in the further phases, computes $kP \in E(F_q)$ is also an abelian group. Assume kP and P_1 are points for elliptic curve. Then, the scalar multiplication is defined as:

$$P_{kP}^j = \sum_{i=0}^{j} k_i' r^i P, \text{ for any } 0 < j < l. \quad (3)$$

Comparing (2) and (3), one can see that $kP = P_{kP}^{l-1}$ is possible. To expose the upper j^{th} from (3), one can get

$$P_{kP}^j = k_i' r^i P + P_{kP}^{j-1}. \quad (4)$$

The auxiliary P_{ACC} and P_1 point needs, where P_{ACC} represents for j^{th} bit as in (5):

$$P_{ACC}^{(j)} = r^j P, \quad (5)$$

It initially initializes to P, i,e., $P_{ACC}^{(0)} = r^j$. Substitutes in equation (4), it gets P_{kP}^j as

$$P_{kP}^j = k_j' P_{kP}^j + P_{kP}^j. \quad (6)$$

Now, P_1 is a recursive point, which call on the curve as:

$$P_1^j = r^{j+1} P - P_{kP}^j \quad (7)$$

For the consistency purpose the computation for each input k_i', and the two recursive points P_{kP}^j and P_1^j.

4.2 *Scalar k into Radix-8 mathematical explanation*

The basic idea to record the scalar is available in [14]. Initially, the input secret scalar k decimal, converts first octal digits, and then changes into the non-seven encoding representation, stores at k_j positions, where $k_j \in \{0,1,2,3,4,5,6,7\}$ and add one extra works as signed number. An initial counter sets the total number present in the non-seven encoding digits. Now scan

non-seven from righthand side-to-lefthand side, at beginning by $j = 0$ as LSB first. If any non-seven at $\boldsymbol{k_j = 7}$ it gets as replacements by -1, and further to add 1 as a carry to next $\boldsymbol{k_j}$ to its left, in other case $\boldsymbol{k_j}$ only records if SC doesn't reach to zero. Further, to record array $a[k_j]$ for scalar multiplication k in from $\{-1, 0, \dots, 6\}$, as depicted in Figure 3.

We have presented an example of mathematical example to justify the scalar multiplication as scalar secret key $k = 14715$. Its $(034673)_8$ is octal representation, further, to say its non-seven encoding is represented as $(0346\bar{1}3)$, in Figure 4. Table 1 is representing the computation process on scalar multiplication. There are three registers are available as per algorithms, the execution works in supposed to t times, then $t = \lceil log_8 14715 \rceil + 1 = 6$ in depicted problem. Further, on the scale of k length the computation cost t for scalar multiplication $t = \lceil log_8 k \rceil + 1$. It was showing one of the most reduced complexity towards the most available elliptic scalar multiplication. Furthermore, radix-16 for scalar multiplication is shown is table 2.

5. Formal Verification

For formal verification of the work, one of the impressive tool is available as SPAN tool for protocol specification. An AVISPA [15] is a automatic validation and verification tool on the designed protocols. The designed protocol offers formal language specification with measures safety into four(04) back-ends under one of the structure named AVISPA.

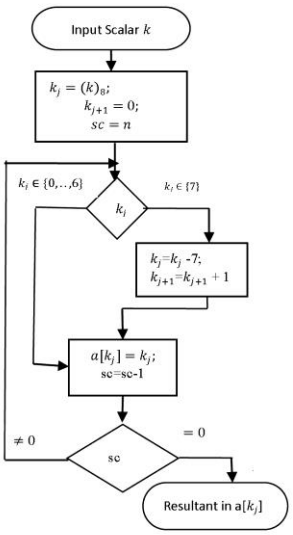

Figure 3
Encoding in Non-Seven

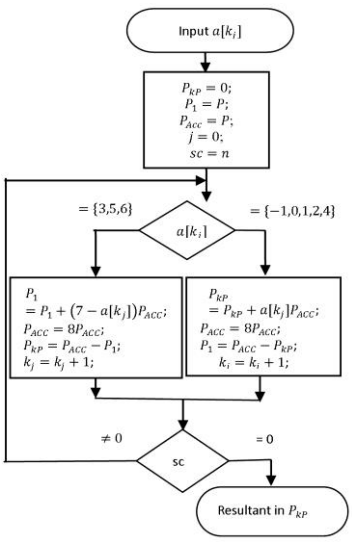

Figure 4
Scalar Multiplication using Radix-8

Table 1
Radix-8 scalar multiplication

Register Array	Initiali-zation	(Iteration from Right-to-Left)					
		SC=6, $a[k_j] = 3$	SC=5, $a[k_j] = -1$	SC=4, $a[k_j] = 6$	SC=3, $a[k_j] = 4$	SC=2, $a[k_j] = 3$	SC=1, $a[k_j] = 0$
$\mathbf{a[k_j]} \in \{-1, 0,1,2,4\}$	$P_{kP} = 0$; $P_1 = P$; $P_{Acc} = P$		$P_{kP} = -5P$ $P_{Acc} = 64P$ $P_1 = 69P$		$P_{kP} = 2427P$ $P_{Acc} = 4096P$ $P_1 = 1669P$		$P_{kP} = 14715P$ $P_{Acc} = 262144P$ $P_1 = 247429P$
$\mathbf{a[k_j]} \in \{3,5,6\}$		$P_1 = 5P$ $P_{Acc} = 8P$ $P_{kP} = 3P$		$P_1 = 133P$ $P_{Acc} = 512P$ $P_{kP} = 379P$		$P_1 = 18053P$ $P_{Acc} = 32768P$ $P_{kP} = 14715P$	

In similar fashion, for radix-16 computation works as, suppose scalar k=89973, Hexadecimal=015F75, and its non-fifteen encoding is = 016-175, table 2.

Table 2
Radix-16 scalar multiplication

SC=6, 5	SC=5, 7	Iteration from Right-to-Left = 016-175					
		SC=6, 5	SC=5, 7	SC=4, -1	SC=3, 6	SC=2, 1	SC=1, 0
∈{-1, 0, 1, 2, 4, 7, 8, 9, 10, 12}	PkP = 0; P1 = P; PACC = P;		PkP = 117P; PACC = 256P; P1 = 139P;	PkP = -139P; PACC =4096P; P1 =4325P;		PkP = 117P; PACC = 256P; P1 = 139P;	PkP = –139P; PACC = 4096P; P1 = 4325P;
∈{3, 5, 6, 11, 13, 14}		P1 =11P; PACC = 16P; PkP = 5P;			P1 = 41099P; PACC = 65536P; PkP = 24437P;		

The language requires for AVISPA is to write a High Level Protocol Specification Language (HLPSL. It comprises four back-ends such as: On-the-fly Model Checker (OFMC) [16], Constraint Logic-based Attack Searcher (CL-AtSe) [17], SAT-based Model Checker (SATMC), and Tree-Automata Based Protocol Analyzer (TA4SP). OFMC is one of the useful debugging tools that execute all the steps of the protocol on the honest policy to its specification agents. CL-ATSE uses to catches attacks with is set of defined constraints logic. Telemedicine of our specification (between medical practitioner and patient via

unsecured mediam) represents a simple interactive Message Sequence Chart (MSC) as a building blocks. The Telemedicine proposed resultant in the safe working states, presented in figure 5, for OFMC and CL-AtSe.

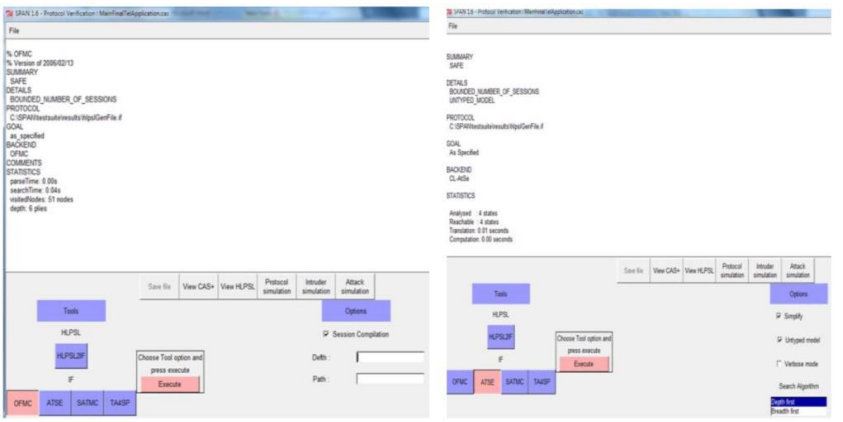

Figure 5
OFMC and CL-ATSE Results

Conclusion

A telemedicine application is simulated using formal verification and validation by the use of SPAN/AVISPA tool using the lightweight Elliptic Curve Cryptography (ECC) approach variation Radix-16 scalar multiplication, which works on the reduced precomputations. The motivation behind the chosen problem have systematically reviewed, by closely considering the research gaps between its varying ECC approached for ECC. The hardware and software performance are shown with its mathematical modeling comparisons to Radix-8 scalar multiplication. The proposed claim is justifying our work used in the scenarios of efficient, robust and secure approaches.

References

[1] V. Jirasek, "Practical Application of Information Security Models," *Information Security Technical Report*, vol. 17, no. 1–2, pp. 1-8 (Feb. 2012).

[2] F. Mair and P. Whitten, "Systematic review of studies of patient satisfaction with telemedicine," *British Medical Journal*, vol. 320, pp. 1517–1520 (2000).

[3] W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Transaction on Information Theory*, vol. 22, No. 6, pp. 644-654 (Nov. 1976).

[4] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery, "On the security of 1024-bit RSA and 160-bit elliptic

curve cryptography," IACR Cryptology ePrint Archive, vol. 2009, p. 389. [Online]. Available: https://www.iacr.org/cryptodb/archive/2009/389/edcl21.dvi

[5] K. Jarvinen and J. Skytta, "Parallelization of High-Speed processor for Elliptic Curve Cryptography," *IEEE Transactions on VLSI,* vol. 16, No. 9, pp. 1162-1175 (Sep. 2008).

[6] Matthew A. Hein, Telemedicine: An Important Force in the Transformation of Healthcare (June 2009) [http://www.trade.gov/td/health/telemedicine_2009.pdf]

[7] Benjamin Abaidoo and Benjamin Teye Larweh, "Consumer Health Informatics: The Application of ICT in Improving Patient-Provider Partnership for a Better Health Care, Online Journal of Public Information, 6 (2) (2014).

[8] N. Koblitz, "Elliptic Curve Cryptosystems," *Math Computation*, vol. 48, No. 177, pp. 203-209 (1987).

[9] Catherine H. Gebotys, "Elliptic Curve Cryptography, Security in Embedded Devices," *Springer,* pp. 75-109 (2010). DOI: 10.1007/978-1-4419-1530-6

[10] V.S. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology*, pp. 417-426 (1986). DOI: 10.1007/3-540-39799-X_31

[11] D.R. Hankerson, A Menezes and S. Vanstone, "Guide to Elliptic Curve Cryptography," *Springer* (2004). DOI: 10.1007/b97644

[12] P. Longa and A. Miri, "Fast and Flexible Elliptic Curve Point Arithmetic over Prime fields," *IEEE Transaction on Computers,* vol. 57, No. 3, pp. 289–302 (2008).

[13] E.A.H. Abdulrahman and A. R-Masoleh, "New Regular Radix-8 Scheme for Elliptic Curve Scalar Multiplication without Pre-Computation," *IEEE Transaction on Computers*, vol. 64, No. 2, pp. 438-451 (Feb. 2015). DOI: 10.1109/TC.2013.213

[14] B. Parhami, Computer Arithmetic: Algorithms and Hardware Designs, 2nd Edition, Oxford University Press (2010).

[15] AVISPA-Automated Validation of Internet Security Protocols [online] Available: http://www.avispa-project.org

[16] D. Basin, S. Modersheim, and L. Vigano, "OFMC: A Symbolic Model-Checker for Security Protocols," *International Journal of Information Security,* vol. 4, pp. 181-208 (2005). DOI: 10.1007/s10207-004-0055-7.

[17] M. Turuani, "The CL-Atse Protocol Analyzer," Lecture Notes in Computer Science, vol. 4098, *F. Pfenning, Eds. in RTE,* pp. 277-286 (2006).

Received November, 2024