


# Chapter 94

## Secure and Robust Telemedicine using ECC on Radix-8 with Formal Verification

**Gautam Kumar**

*Jaypee University of Information Technology, Solan, India*

**Hemraj Saini**

 <https://orcid.org/0000-0003-2957-1491>

*Jaypee University of Information Technology, Solan, India*

### ABSTRACT

*The scalar multiplication techniques used in Elliptic curve cryptography (ECC) are having the scope for gaining the computation efficiency. This is possible through the reduction of precomputed operations. Finding the more efficient technique compares to the most recent or efficient one is a research gap for all schemes. The manuscript presents an application oriented work for Telemedicine using ECC. It is based on robust application on reduced computational complexity. The methodology we apply for the same is Scalar Multiplication without precomputation on Radix-8. Introduced software and the hardware performance are reporting a big advantage over all the related proposed techniques. The reason to cover this problem is to provide a path on a fascinating area of ECC on a smaller key size be applicable for all applications on a same level of security strengths. The smaller length key gives the higher speed and shorter clock cycle to initiate the operation.*

### INTRODUCTION

The scenario for all applications concerns to performance and considerable security services in the real life. The security services are using with the concept of cryptography and it has been considered to be a discipline of computer science. The performances are achieving through the use of optimized algorithms.

DOI: 10.4018/978-1-7998-5351-0.ch094

The used algorithms are running with the data security techniques. In general, all the developed algorithms have based on reduced costs of computation and communication cost. The associated researchers and/or cryptographers have shown their matured behaviors in the field of security. But, in preference to this, still the various requirements are motivational issues related to more enhanced performance and system security services. The applications of security are to protect information from secure message transmission, disclosure, and guaranteed authenticity of data (Jirasek, 2012).

The public key cryptography (PKC) was proposed in 1976 by (Diffie & Hellman, 1976). Afterword's various PKC algorithms have been proposed, but in all of them Elliptic Curve Cryptography (ECC) has attracted the most attention. ECC algorithm has been considered to be secure on shorter key sizes. This level of security is also achieving by algorithms but they need a very higher length of the key sizes. The shorter length keys computes much faster and that also the best suits to low memory devices. For example, for the same level of security RSA uses 1024-bit key whereas ECC only uses 160 bit key sizes (Bos et al., 2009). We have considered and analyzed the algorithms for ECC on the core work of cryptography, which shows still the opportunities of improvements in the algorithms are possible in relations to the proposed algorithms.

The heart of cryptography is Discrete Logarithmic Problem (DLP), which plays a central role in information security on applied algorithms. The used algorithms are running with their own complexity that depends on the precomputed operations. Lower precomputed operations are putting a high mark on system performance. The faster running algorithms are leading with high-speed in the growing field of computation and communication (Jarvinen & Skytta, 2008).

DLP for 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 (Koblitz, 1987). It computes for 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 behalf of generated scalar multiplication, 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.

An ECC is a hierarchy of consistent operations structured into different but interrelated levels. As depicted in Figure 1, the highest level i.e., level 0, ECC presents algorithms for scalar multiplication  $kP$  with ensuring to group operations such as ADDs and DBLs, and finally these operations depend on finite field arithmetic operations such as addition, subtraction, multiplication, inversion, and squaring. The respective precomputed operations realized by (Gebotys, 2010, pp. 75-109) for one point ADDs are 13,617 and for one point DBLs are 14,000 clock cycles.

To accelerate the performance of ECC, the hierarchy has been parallelized on reduced pre-computed operations. To reduce the precomputations are also our motivational issue for the same. The scalar multiplication techniques contain the existing algorithms such as using Most Significant Bit (MSB) first, Least Significant Bit (LSB) first, Nonadjacent form (NAF), Window Method, Sliding Window Method, Width Nonadjacent Form, Frobenious Map and Radix-rNAF (r-NAF) and Radix-rNAF (r-NAF) (Miller, 1986; Izu & Takagi, 2002; Knuden, 1999; Blake et al., 2005; Hankerson et al., 2004). Here, we are giving a simple thought about the known algorithms and its computational complexities. Suppose  $k$  is a scalar, represented in the form of  $m$  bit binary. It requires  $m$  bits doubling (DBLs) and on average  $m/2$  bits of addition (ADDs) operations using MSB techniques. Similarly, for Least Significant Bit (LSB) first, it requires on average  $m/2$  bits of ADDs and same bits of DBLs. A non-adjacent form (NAF) is a

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/secure-and-robust-telemedicine-using-ecc-on-radix-8-with-formal-verification/268685](http://www.igi-global.com/chapter/secure-and-robust-telemedicine-using-ecc-on-radix-8-with-formal-verification/268685)

## Related Content

---

### Contextual Inquiry of Food Ordering Apps: An Indian Perspective

Ganesh D. Bhutkar, Mishail Shailendra Singhand Yohannes Kurniawan (2022). *Designing User Interfaces With a Data Science Approach* (pp. 68-85).

[www.irma-international.org/chapter/contextual-inquiry-of-food-ordering-apps/299747](http://www.irma-international.org/chapter/contextual-inquiry-of-food-ordering-apps/299747)

### Animal Activity Recognition From Sensor Data Using Ensemble Learning

Derya Birantand Kadircan Yalniz (2022). *Emerging Trends in IoT and Integration with Data Science, Cloud Computing, and Big Data Analytics* (pp. 165-180).

[www.irma-international.org/chapter/animal-activity-recognition-from-sensor-data-using-ensemble-learning/290080](http://www.irma-international.org/chapter/animal-activity-recognition-from-sensor-data-using-ensemble-learning/290080)

### Resource Allocation Scheduling Algorithm Based on Incomplete Information Dynamic Game for Edge Computing

Bo Wangand Mingchu Li (2022). *Research Anthology on Edge Computing Protocols, Applications, and Integration* (pp. 414-439).

[www.irma-international.org/chapter/resource-allocation-scheduling-algorithm-based-on-incomplete-information-dynamic-game-for-edge-computing/304316](http://www.irma-international.org/chapter/resource-allocation-scheduling-algorithm-based-on-incomplete-information-dynamic-game-for-edge-computing/304316)

### Exploring Data Science Initiatives Through an International Lens

Nandita S. Mani, Emily P. Jones, Rebecca Carlson, Fidan Limani, Atif Latif, Klaus Tochtermann, Faten Hamad, Christine J. Urquhart, Victoria Lemieux, Sarah Ames, Jenna Bainand Justin M. Clark (2022). *Handbook of Research on Academic Libraries as Partners in Data Science Ecosystems* (pp. 1-24).

[www.irma-international.org/chapter/exploring-data-science-initiatives-through-an-international-lens/302744](http://www.irma-international.org/chapter/exploring-data-science-initiatives-through-an-international-lens/302744)

### A Novel Feature Correlation Approach for Brand Spam Detection

Bharat Tidkeand Swati Tidke (2021). *Data Preprocessing, Active Learning, and Cost Perceptive Approaches for Resolving Data Imbalance* (pp. 149-161).

[www.irma-international.org/chapter/a-novel-feature-correlation-approach-for-brand-spam-detection/280915](http://www.irma-international.org/chapter/a-novel-feature-correlation-approach-for-brand-spam-detection/280915)