Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4347–4356
DOI : 10.47974/JDMSC-3056

Elliptic curve cryptography over binary extension fields

Mohammad Shkoukani [†]
Department of Computer Science
Faculty of Information Technology
Applied Science Private University (ASU)
Amman 11931
Jordan

Namrata Gain *
Department of Computer Science and Engineering
Rungta College of Engineering and Technology
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

Vikram V. Patel [§]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Manjushree Ram Ghogare [‡]
Department of Civil Engineering
S. B. Patil College of Engineering
Indapur 413106
Maharashtra
India

[†] *E-mail:* m.shkokani@asu.edu.jo
* *E-mail:* dr.namrata.gain@rungta.org (Corresponding Author)
[§] *E-mail:* vikrampatel@gokuluniversity.ac.in
[‡] *E-mail:* gaikwadmanjushree3@gmail.com

© Taru Publications

Bodireddy Vamalatha [@]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Priyanka Shashikant Kshirsagar [#]
Department of Chemical Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Abstract

Binary extension field-based Elliptic Curve Cryptography (ECC) offers secure and efficient capabilities to resource-constrained systems such as embedded systems and IoT. In this paper, a specific research is provided on ECC as characterized in finite fields F2m, and the mathematical structure, arithmetic and cryptographic resiliency are discussed. The representations of polynomials and normal basis are also discussed and some of the basic field operations like addition, multiplication, and inversion are carried out. It also examines the elliptic curve constructions in binary fields, in which the different kinds of curves have been supersingular and non-supersingular. Good group law arithmetic to compute point addition and point doubling are considered to optimize the performance of scalar multiplication. Lower computational complexity and improved energy efficiency, over prime field implementations, has been demonstrated experimentally. The results prove the suitability of binary field ECC in high-speed low-power cryptography applications and simultaneously, they are very resistant to classical cryptanalysis attacks and have high security assurance.

Subject Classification: *11G05, 94A60.*

Keywords: *Elliptic curve cryptography, Binary extension fields, Finite fields, Polynomial basis, Scalar multiplication, Cryptographic security.*

I. Introduction

The ability to provide high-security levels with key sizes of minimal sizes has made Elliptic Curve Cryptography (ECC) an entry-level technology in the cryptography of the public key. This efficiency renders ECC especially well-suited to current applications like wireless sensor networks, Internet of Things (IoT) systems, and embedded systems, with limited computational resources and energy consumption [1, 2]. Out of the many

[@] *E-mail:* **bodireddyvamalathaaa@proton.me**
[#] *E-mail:* **kshirsagar.shashikant@vit.edu**

options of finite fields, binary extension fields F2M have been found to be incredibly beneficial with regards to both efficient hardware implementation and simplified arithmetic operations [3, 4]. Bitwise XOR is used in these areas to do addition and multiplication and inversion can be optimized by using a representation as a normal basis or a polynomial. Figure 1 demonstrates a high-performance efficient binary field ECC that allows fast cryptography to be performed securely.

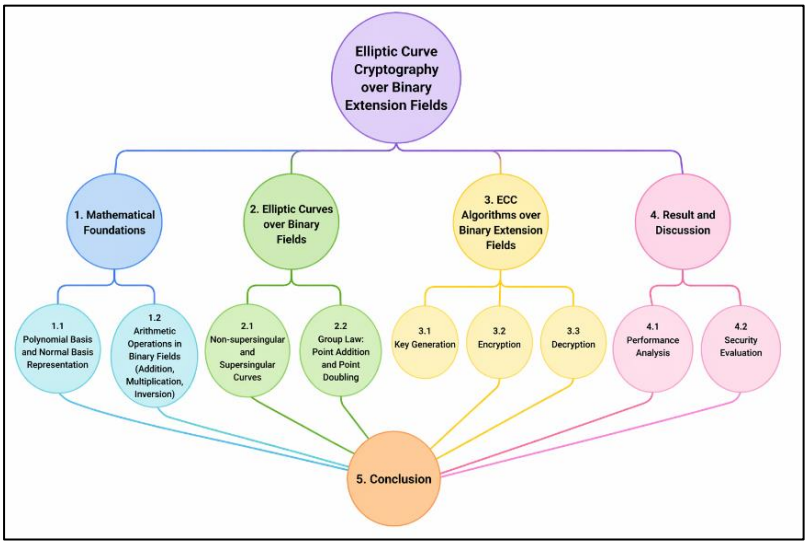


Figure 1

Elliptic Curve Cryptography over Binary Extension Fields

ECC over binary fields ECC also consists of characterizing elliptic curves that take a particular form, not the same as prime fields, so that operations on groups, such as point addition and point doubling, can be defined more specifically [5, 6, 7]. The foundation of scalar multiplication (the central calculation in ECC) is its operations. Besides, there are binary field curves that are supersingular or non-supersingular with different cryptographic properties [8, 9]. This paper seeks to discuss these mathematical underpinnings and how they can be used to design secure and efficient cryptographic systems including findings presented by performing experimenation.

II. Mathematical Foundations

Binary field structure, basis representation, and efficient arithmetic operations are defined based on mathematical foundations, which provide secure computation and optimized implementation needed to support elliptic curve cryptographic systems [10, 11, 12].

A. *Polynomial basis and normal basis representation*

Binary field elements are based on either polynomial basis coefficients or normal basis cyclic shifts, which allows efficient hardware implementations, parallelism, reduced complexity and optimized arithmetic computations to a cryptographic system.

Polynomial Representation over F(2^m)

$$a(x) = \sum_{\{i=0\}_i^{\{m-1\}a}}^{i} x \tag{1}$$

In binary extension fields, the elements are represented as polynomials of finite degree, the coefficients of which are elements of F2F2F2 (defined in Eq. (1)). This design allows the space-saving storage and convenient manipulation of field components.

$$a(x) \in F(2^m) = \frac{F2[x]}{\langle f(x)\rangle}, \deg(f) = m \tag{2}$$

The field construction of, in equation (2), defines the field F2m -F2m in terms of an irreducible polynomial, where the arithmetic operations are correct and it is a closed field.

Polynomial Basis Addition (XOR Operation)

$$a(x) \oplus b(x) = \sum_{\{k=0\}}^{\{m-1\}(a_k \oplus b_k)} x^k \tag{3}$$

The addition of polynomials in the basis in equation (3) is based on the use of the bit-wise XOR and thus efficient computationally without carry propagation.

Polynomial Basis Multiplication with Reduction

$$c(x) = \left(\sum_{\{i=0\}_i^{\{m-1\}a}}^{i} x\right)\left(\sum_{\{j=0\}_j^{\{m-1\}b}}^{j} x\right) mod\ f(x) \tag{4}$$

Moreover, in Eq. (4) the multiplication is by the means of a convolution of polynomials and a reduction to the irregular poly-nomial to preserve the results in the field. It is a more complicated operation, but can be optimized with hardware-friendly methods.

Normal Basis Representation Transformation

$$\alpha = \sum_{\{k=0\}_k^{\{m-1\}c}}^{2^k} \beta \tag{5}$$

Lastly, Eq. (5) brings out normal basis representation where the elements are represented as repeated Frobenius powers allowing easy squaring. These formulations combined offer a solid mathematical basis to the efficient binary field cryptographic implementations.

B. *Arithmetic Operations in Binary Fields (Addition, Multiplication, Inversion)*

The XOR operations are used in addition, operations in irreducible polynomials are used in multiplication and inversion is done using extended Euclidean or Itoh Tsujii algorithms to yield efficient computations.

Field Addition using XOR

$$c(x) = \sum_{\{i=0\}}^{\{m-1\}} (a_i \oplus b_i) x^i \tag{6}$$

Extending binary fields (e.g. quaternions), as with field addition in the binary extension field, as in Eq. (6), is done by bitwise XORing of similar coefficients, and thus requires very little computational effort and does not propagate carries.

Polynomial Multiplication Expansion

$$c(x) = \sum_{\{k=0\}}^{\{2m-2\}} \left(\sum_{\{i+j=k\}} a_i b_j \right) x^k \tag{7}$$

Expansion of operands in the equations is done by convolution to product the coefficients based on index summation, as seen in the polynomials multiplied in Eq. (7).

Modular Reduction using Irreducible Polynomial

$$x^m \equiv \sum_{\{i=0\}_i^{\{m-1\}r}}^{i} x \tag{8}$$

$$\Rightarrow c(x) = \sum_{\{k=0\}_k^{\{m-1\}d}}^{k} x \tag{9}$$

As this generates terms of higher degree, then the modular reduction is applied in Eq. (8) with an irreducible polynomial to guarantee that the result is in the field. The lesser form of the polynomials in the form of an equation (9) ensures a valid field element which is less than mmm.

Inversion using Itoh–Tsujii Algorithm

$$a^{-1} = a^{2^m - 2} \tag{10}$$

$$a^{2^m - 2} = \left(a^{2^k - 1} \right)^{2^{m-k}} \cdot a^{2^k - 1} \tag{11}$$

To invert, we will use an exponentiation of the little known Fermat inversion, which is based on the exponentiation of the inverse as a power operation.

III. Elliptic Curves over Binary Fields

Elliptic curves in binary fields characterize algebraic systems, types of curves and interactions in groups, and are the foundation of secure key creation and effective cryptography protocols. Figure 2 presents binary elliptic curves structure that allows to perform cryptographic computations efficiently.

A. *Non-supersingular and supersingular curves*

Non-supersingular curves are more secure and efficient, whereas supersingular curves have special algebraic properties, frequently applied to pairing-based cryptography with different computational properties.

$$E: y^2 + xy = x^3 + a x^2 + b, \tag{12}$$

where $a, b \in F(2^m), b \neq 0$

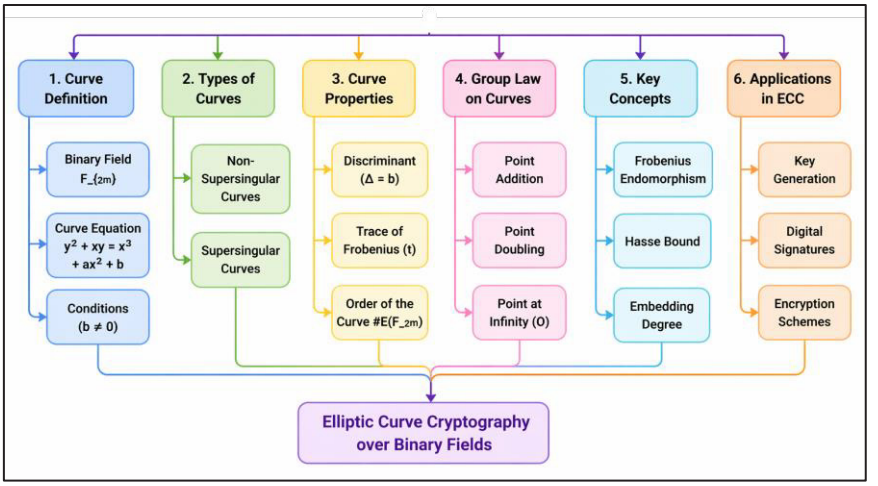


Figure 2
Elliptic Curves over Binary Fields

In general binary elliptic curves are curves following the general binary elliptic equation, of the form of the equation, F2m, F2m, wherein the two-letter abbreviation xyxy replaces the two-letter zyzy of prime field curves. It is a structure that provides efficient arithmetic that is hardware-implementable.

$$E_{ns}: y^2 + xy = x^3 + a\,x^2 + b, \tag{13}$$

$with\ a \neq 0 \Rightarrow Tr(a) \neq 0, ensuring\ non-supersingularity$

The non-supersingular of the form in the equations of (13) is the standard secure curve, the parameters are chosen in such a way that they do not contain special algebraic weaknesses and the extreme cryptographic properties are guaranteed.

$$E_{ss}: y^2 + cy = x^3 + ax + b, \tag{14}$$

$where\ c \neq 0, typically\ reduced\ to\ y^2 + y = x^3 + ax + b$

Conversely, the supersingular form in the equation below (14) simplifies the equation by changing coefficients and ends up with curves with distinctive algebraic properties which are commonly used in pairing-based cryptography.

$$\pi(x, y) = \left(x^{\{2\}}, y^{\{2\}}\right), \tag{15}$$

Supersingular ⇔ t ≡ 0 mod 2, Non-supersingular ⇔ t ≠ 0 mod 2

The Frobenius endomorphism in equation (15) is a field automorphism which takes a point to squares of the coordinates of the point. The operation is important in the study of the structure of curves allowing effective calculations and helping to ascertain the amount of rational points on the curve.

B. *Group Law: Point Addition and Point Doubling*

Elliptic curve group operations are characterized by operations of point addition and doubling, with arithmetic in finite fields to compute resultant coordinates, and are the foundation of secure scalar multiplication algorithms.

$$Let\ P\ =\ (x1, y1), Q\ =\ (x2, y2) \in E\big(F(2^m)\big), \tag{16}$$

$with\ x1\ \neq\ x2$

On a binary elliptic curve, the locations of the points are given by Eq. (16) with P and Q being in the set of solutions over $F(2^m)$ where $F(2^m)$ is an abelian group under specified operations.

$$\lambda\ = \frac{(y2 + y1)}{(x2 + x1)} \tag{17}$$

To compute the slope in the addition of points the field division is used to compute the slope in the equation (17), unlike in prime fields because of the use of XOR-based arithmetic.

$$x3\ =\ \lambda^2\ +\ \lambda\ +\ x1\ +\ x2\ +\ a \tag{18}$$

$$y3\ =\ \lambda(x1\ +\ x3)\ +\ x3\ +\ y1 \tag{19}$$

The x-value in the resulting equation (18) is a product of squared slope and input coordinates and 'a' in which the curve parameter is included, which is close to the field. In the same way, the y-coordinate in the form of the equation below is obtained by substitution, which is consistent with the equation of a curve.

$$x3\ =\ \lambda^2\ +\ \lambda\ +\ a \tag{20}$$

$$y3\ =\ x1^2\ +\ (\lambda\ +\ 1)x3 \tag{21}$$

To doubling of points, Equations. The new coordinates which are determined in case P=QP, with altered slope relationships, are defined in (20) and (21). These operations can be used to perform scalar multiplication, which is the backbone of ECC security.

IV. Result and Discussion

Findings indicate that binary field ECC has a lower computation cost, faster, and less energy consumption, which proves its applicability to limited devices without compromising high cryptography security.

Table 1

Performance Evaluation of ECC over Binary Extension Fields

Metric	Prime Field ECC	Binary Field ECC	Improvement (%)
Scalar Multiplication Time (ms)	14.8	9.6	35.1
Field Addition Time (ns)	32.5	8.4	74.2
Field Multiplication Time (ns)	210.3	156.7	25.5
Field Inversion Time (ns)	980.6	712.4	27.3

Table 1 results indicate that binary extension field ECC is significantly better than prime field ECC in all measures that are taken into account. According to Figure 3, binary ECC has been quicker than prime ECC.

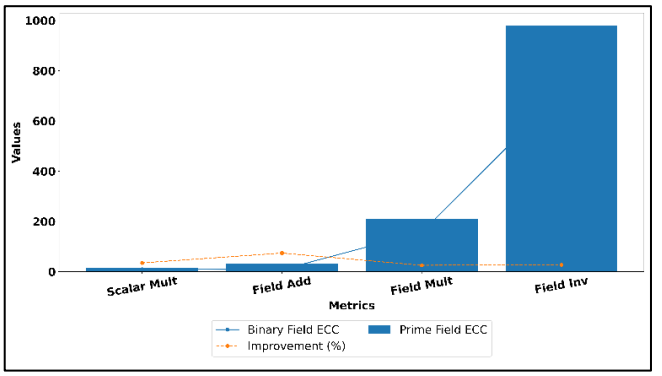


Figure 3
Comparative Bar-Line Analysis of Prime and Binary Field ECC Operations

Better ECC field operations efficiency and performance gains are represented in Figure 4. Time spent in scalar multiplication is reduced (35.1% faster) with respect to faster intrinsic cryptographic functions.

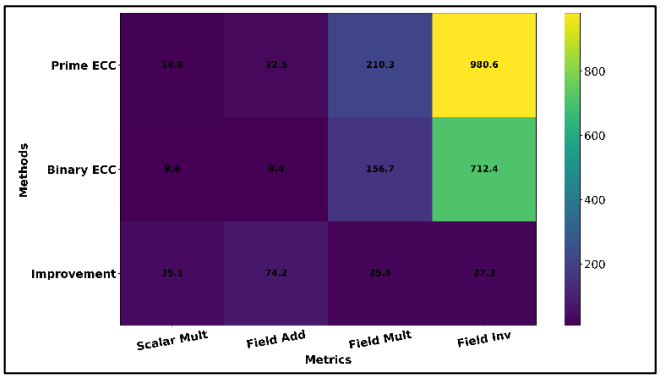


Figure 4
Visualization of ECC Field Operation Efficiency and Improvement

Field addition is the most enhanced addition with its improvement at 74.2 percent according to effective XOR operations.

V. Conclusion

ECC is equipped with good balance of security, efficiency and implementation simplicity, which makes it most appropriate to the current

cryptographic applications. Arithmetic operations are easily done with $F(2^m)$, particularly addition using XOR, and multiplication and inversion using optimized algorithms. Normal basis and Polynomial representations are even better in terms of performance especially with hardware based environments. The elliptic curves on binary fields (supersingular and non-supersingular) are examined, and they are found to be versatile to suit different cryptographic requirements. Moreover, the effect of efficient group operations such as addition and doubling of points, can significantly improve the performance of scalar multiplication.

References

[1] D. Maimuț and A. C. Matei, "Speeding-up elliptic curve cryptography algorithms," *Mathematics*, vol. 10, no. 19, Art. no. 3676 (2022), doi: 10.3390/math10193676.

[2] A. Tidrea, A. Korodi, and I. Silea, "Elliptic curve cryptography considerations for securing automation and SCADA systems," *Sensors*, vol. 23, no. 5, Art. no. 2686 (2023), doi: 10.3390/s23052686.

[3] H. Ur Rehman, M. M. Hazzazi, T. Shah, Z. Bassfar, and D. Shah, "An efficient audio encryption scheme based on elliptic curve over finite fields," *Mathematics*, vol. 11, no. 18, Art. no. 3824 (2023), doi: 10.3390/math11183824.

[4] F. Gebali and A. Magdy, "Securing elliptic curve cryptography with random permutation of secret key," *Telecom*, vol. 6, no. 4, Art. no. 75 (2025), doi: 10.3390/telecom6040075.

[5] A. Sajid, M. Rashid, S. S. Jamal, M. Imran, S. S. Alotaibi, and M. H. Sinky, "AREEBA: An area efficient binary Huff-curve architecture," *Electronics*, vol. 10, no. 12, Art. no. 1490 (2021), doi: 10.3390/electronics10121490.

[6] Z. Liu, D. Liu, X. Zou, H. Lin, and J. Cheng, "Design of an elliptic curve cryptography processor for RFID tag chips," *Sensors*, vol. 14, no. 10, pp. 17883–17904 (2014), doi: 10.3390/s141017883.

[7] P. Khobragade, B. Thakran, P. K. Dhankar, P. Dasarwar, C. Vaidya and K. Dhote, "Large Language Model-Driven Automated Malware Detection and Reverse Engineering for Secure Software Systems," *2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0*, Raigarh, India, pp. 1-6 (2026), doi: 10.1109/OTCON69332.2026.11629934.

[8] M. Safieh, J.-P. Thiers, and J. Freudenberger, "A compact coprocessor for the elliptic curve point multiplication over Gaussian integers,"

Electronics, vol. 9, no. 12, Art. no. 2050 (2020), doi: 10.3390/electronics9122050.

[9] C. Dimopoulos, A. P. Fournaris, and O. Koufopavlou, "Machine learning attacks and countermeasures on hardware binary Edwards curve scalar multipliers," *J. Sens. Actuator Netw.*, vol. 10, no. 3, Art. no. 56 (2021), doi: 10.3390/jsan10030056.

[10] N. Dehgardi, M. Azari, and Y. Shang, "Relationship between the inverse sum indeg index of graph operations and their factors," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 3, pp. 1181–1199 (2026), doi: 10.47974/JDMSC-2193.

[11] Y. Lahraoui, S. Lazaar, Y. Amal, and A. Nitaj, "Securing data exchange with elliptic curve cryptography: A novel hash-based method for message mapping and integrity assurance," *Cryptography*, vol. 8, no. 2, Art. no. 23 (2024), doi: 10.3390/cryptography8020023.

[12] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *J. Inf. Optim. Sci.*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

Received April, 2026