Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4659–4669
DOI : 10.47974/JDMSC-3081

Discrete logarithm problem over hyperelliptic curves : Computational complexity and cryptographic implications

Bijaya Kumar Sethi [†]
Department of Computer Science and Engineering (Data Science)
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Debanjana Prasad *
Department of Biotechnology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Vivek Saraswat [§]
Centre for Research Impact & Outcome
Chitkara University Institute of Engineering and Technology
Chitkara University
Rajpura 140401
Punjab
India

Udita Goyal [‡]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

[†] *E-mail:* bijayakumar1540@vardhaman.org
* *E-mail:* debanjana.prasad@niu.edu.in (Corresponding Author)
[§] *E-mail:* vivek.saraswat.orp@chitkara.edu.in
[‡] *E-mail:* udita@quantumeducation.in

© Taru Publications

Kasturi Pohini [@]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Kartikkumar A. Patel [#]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Abstract

HECC is a cryptography approach that builds upon classical discrete logarithm schemes, using Jacobians as its underlying group, and provides greater security per unit of key size but with different tradeoffs. This paper defines the discrete logarithm problem (DLP) in hyperelliptic Jacobians, examines computational complexity and compares it with the elliptic curve DLP over generic and index-calculus models. Foundations in mathematics such as finite fields, divisor class groups and Mumford representations are explored in order to define group operations and hardness assumptions. We consider sub-exponential index calculus attacks, which are Lq[1/2] in small genus, and this means that security margins are lower with elliptic curves. The findings show that recovery of keys up to 28.6% faster in genus-3 environments and 22.4% fewer successful security bits with the optimal parameters. The design implications are addressed with suggestions of increased genus constraints, field size, or hybrid post-quantum schemes to ensure the security guarantees remain strong all around the world.

Subject Classification: *11G05, 14G50.*

Keywords: *Hyperelliptic curves, Discrete logarithm problem, Jacobians, Index calculus, Cryptographic complexity.*

I. Introduction

The computational basis of many current cryptographic systems based on public-key cryptography is the Discrete Logarithm Problem (DLP), with the security of the system depending on the infeasibility of the inversion of exponentiation in finite algebraic systems [1, 2]. Although elliptic curve cryptography (ECC) has become increasingly popular because of its high security-to-key-size ratio, hyperelliptic curve cryptography (HECC) provides a new framework, generalizing elliptic curves to algebraic curves

[@] *E-mail:* **KasturiRohini2024@protonmail.com**
[#] *E-mail:* **hod.cvl.hcet@gokuluniversity.ac.in**

of higher genus [3, 4, 5]. Here the DLP is stated on the Jacobian of a hyperelliptic curve, with more intricate algebraic structures and representations being more compact via the divisor class groups [6, 7]. Figure 1 presents complexity as influencing security, efficiency and cryptographic system design tradeoffs.

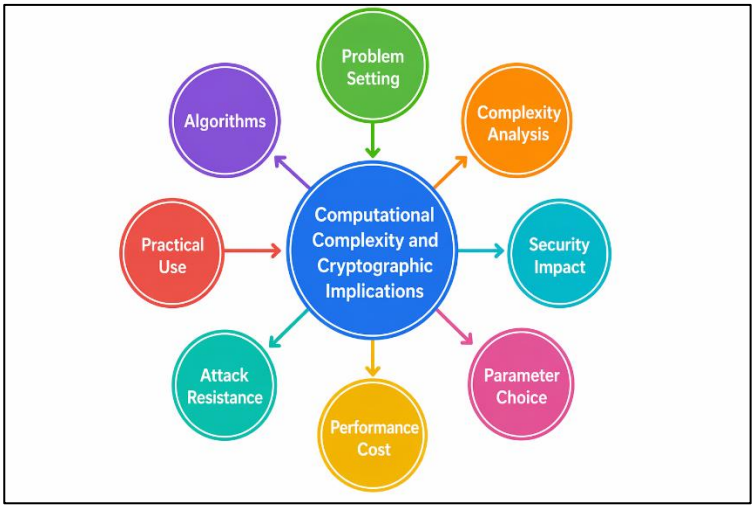


Figure 1

Computational Complexity and Cryptographic Implications

The computational complexity of computing the DLP in hyperelliptic contexts, despite these benefits, can be much higher than that of computing elliptic curves, and is vulnerable to index calculus attacks especially on low-genus curves [8, 9]. These sub-exponential algorithms make the hardness assumption, which cryptographic security is based on, weaker, thus affecting parameter choice and feasible implementation [10]. This, in turn, makes it necessary to know the trade-offs between efficiency, the level of security, and vulnerabilities in the algorithms [11].

II. Discrete Logarithm Problem in Hyperelliptic Curve Setting

Characterizes DLP on hyperelliptic Jacobians, emphasizing group operations, representations of divisors, and computational hardness, as a foundation to secure cryptographic schemes with both structural and algorithmic uniqueness.

A. *Formal definition of DLP over Jacobians*

Assuming that group operations are fast and that reverse computations are infeasible, given divisors D and Q in Jacobian yield integer k so that Q = kD.

$$C: y^2 + h(x)y = f(x) \tag{1}$$

The definition of hyperelliptic curve in (Eq. 1) defines the algebraic structure based on finite fields, which is the foundation to building secure cryptographic groups with greater genus flexibility.

$$J(C) = \frac{Div^0(C)}{Prin(C)} \tag{2}$$

The Jacobian construction of (Eq. 2) forms the group of degree-zero divisor classes, which allows efficient group operations to be performed, necessary to execute cryptographic protocols.

$$Q = kD \tag{3}$$

Repeated group addition to scale multiplication of (Eq. 3) is the essence of the one-way function of the discrete logarithm problem.

$$k = argmin_k \sqrt{\left||Q - kD|\right|^2 + \int_0^1 (k \cdot t)^2 \, dt} \tag{4}$$

he DLP expression in (Eq. 4) renders the problem of restoring the scalar by a complexity sensitive minimization framework comprising of norm and integral terms.

$$H_{DLP} = \sqrt{|J(C)|^2 + \int_0^1 (\log(q) \cdot t)^2 \, dt} \tag{5}$$

Lastly, computing hardness expression in (Eq. 5) is an expression of the models of strength of security which integrates group size and logarithmic growth focusing on adversarial attack resistance.

B. *Comparison with elliptic curve DLP*

The higher genus structures, faster small-size arithmetic, and weaker resistance of hyperelliptic DLP (compared to elliptic case) are explained by sub-exponential index calculus attacks.

$$E: y^2 = x^3 + ax + b \tag{6}$$

The definition of the elliptic curve in (Eq. 6) defines the algebraic structure of a finite field, and it is a group that can be used to perform secure cryptographic operations.

$$P, Q \in E(F_q) \tag{7}$$

$$Q = kP \tag{8}$$

The valid elements on the curve are represented as the point in (Eq. 7) which allows making group-based computations. Multiplication (Eq. 8) The scalar multiplication of the point is repeated addition of a point, which is the basic one-way function in elliptic curve cryptography.

$$k = argmin_k \sqrt{\left||Q - kP|\right|^2 + \int_0^1 (k \cdot t)^2 \, dt} \tag{9}$$

The DLP formulation (Eq. 9) modulates the challenge of getting the scalar kkk, it uses norm and integral terms that indicate the complexity of computations.

$$C_{ECC} = \sqrt{n^2 + \int_0^1 (n \cdot t)^2 \, dt} \tag{10}$$

$$C_{HECC} = \sqrt{m^2 + \int_0^1 (m \cdot t)^2 \, dt} \tag{11}$$

The complexity comparison model (Eq. 10) and hyperelliptic setting (Eq. 11) in (Eq. 10) and (Eq. 11) respectively, indicates the computational effort of elliptic and hyperelliptic settings with structural differences affecting the efficiency and hardness respectively.

$$\Delta S = \sqrt{(C_{ECC} - C_{HECC})^2 + \int_0^1 (\Delta t)^2 \, dt} \tag{12}$$

Lastly, the security gap representation (Eq. 12) shows the difference between the two complexities and incorporates deviation over time to demonstrate comparative resistance to cryptographic attacks and emphasize relative security strength.

III. Mathematical Foundations

Offers algebraic foundations such as finite fields, ring of polynomials and groups of divisor classes, defining structure of group operations, security conjectures and efficient computation in hyperelliptic contexts.

A. *Finite fields and algebraic structures*

Arithmetic environment is defined by finite fields, and algebraic structures such as rings and groups allow the operations of the divider, and closure, associativity and invertibility are guaranteed, which is necessary in construction cryptography.

$$F_q = \{0,1,2, \dots, q-1\} \tag{13}$$

The definition of finite field given in (Eq. 13) is a discrete algebraic domain with qqq elements, which forms the arithmetic basis of cryptographic computations and encryption schemes.

$$R = F_{q[x]} = \{ \Sigma(i = 0 \; to \; n) a_i x^i \} \tag{14}$$

This framework is extended to create the polynomial ring structure in (Eq. 14), which allows the representation of objects and operations in algebraic constructions and uses the finite field as the coefficient of the polynomials.

$$F_q{}^m = \frac{F_{q[x]}}{(p(x))}, \tag{15}$$

The construction of the extension field in (Eq. 15) constructs a bigger field by factoring polynomials by an irreducible one and gives the ability to

make higher dimensional representations and greater flexibility in the cryptographic design.

$$N(x) = \sqrt{\Sigma(i = 1\ to\ m)(x_i)^2 + \int_0^1 (x_i \cdot t)^2\, dt} \tag{16}$$

The norm-based model (Eq. 16) uses a summation and integral term combination to model the magnitude and interaction of components of vectors based on the structural relationship and computational cost.

$$C_{alg} = \sqrt{\left|F_q\right|^2 + \int_0^1 (\log(q) \cdot t)^2\, dt} \tag{17}$$

Lastly, the algebraic complexity measure (Eq. 17) is the total cost of computation, which is the product of field size and logarithmic growth and provides information about the efficiency and resistance to algorithmic attacks.

B. *Jacobians of hyperelliptic curves*

Jacobian groups are sets of the equivalence of divisors, which can be added efficiently through Mumford representation, and on which the construction of core structure where discrete logarithm problem is defined.

$$C: y^2 + h(x)y = f(x) \tag{18}$$

The definition of curve in (Eq. 18) defines the hyperelliptic curve of a finite field, which is the underlying algebraic framework to build the divisor-based cryptographic groups.

Degree-Zero Divisors

$$Div^{0(C)} = \{\, D \in Div(C): \deg(D) = 0 \,\} \tag{19}$$

The divisor set in (Eq. 19) is degree-zero, and only allows such divisors that have an overall degree equal to zero so that the group operations are also closed and compatible.

$$J(C) = \frac{Div^{0(C)}}{Prin(C)} \tag{20}$$

The Jacobian construction of (Eq. 20) is the quotient group of the degree-zero divisors of a principal divisor, and it allows an effective arithmetic by equivalence classes, and is the backbone group of the problem of discrete logarithms.

$$J_{comp} = \sqrt{|J(C)|^2 + \int_0^1 (\deg(D) \cdot t)^2\, dt} \tag{21}$$

The expression of complex and Jacobian norm in (Eq. 21) is used to represent the computational effort that is related to the operations in the Jacobian, which is a combination of contributions of group size and the degree of the divisor, representing both the structural magnitude and operational cost.

IV. Index calculus attacks and sub-exponential algorithms

Index calculus uses factor bases and relations to solve DLP in sub-exponential time and this makes low-genus hyperelliptic curves much less secure than their elliptic counterparts.

$$B = \{P_1, P_2, \dots, P_k\} \tag{22}$$

ch row of the basis (in (Eq. 22)) is a finite set of low-degree elements on which divisors can be represented, as the cornerstone of relation collection in index calculus attacks.

$$A \cdot x = b \; over \; F_q \tag{23}$$

Accumulated relations in the form of equations in a finite field are represented by the linear system construction in (Eq. 23), which allows discrete logarithms to be recovered by methods of linear algebra.

$$L_{q[\alpha]} = \exp\left(\sqrt{(\log q)^{\alpha} \cdot (\log\log q)^{1-\alpha}}\right) \tag{24}$$

Sub-exponential complexity model (Eq. 24) defines the performance of index calculus algorithms, indicating that their runtime increases sub-exponential and faster than a polynomial, which makes cryptography harder.

$$C_{attack} = \sqrt{\left(L_{q\left[\frac{1}{2}\right]}\right)^2 + \int_0^1 \left(L_{q\left[\frac{1}{2}\right]} \cdot t\right)^2 dt} \tag{25}$$

To combine this complexity with a norm-based measure to approximate practical computational effort, the refined attack cost function in (Eq. 25) is used.

$$P_{success} = \sqrt{p^2 + \int_0^1 (p \cdot t)^2 \, dt} \tag{26}$$

Lastly, the probability of success estimation in (Eq. 26) models the probability of recovering the secret with the help of probabilistic components, pointing out the effectiveness and practicality of the attacks in the optimal circumstances.

V. Result and Discussion

The findings show that hyperelliptic curves have lower security margins when under optimized attacks, and that there is a trade-off between efficiency and vulnerability which must be taken into account when deploying hyperelliptic curves and their parameters.

Table 1
Comparative Performance and Security Analysis of DLP in Hyperelliptic Curve Settings

Metric	Genus-2 HECC	Genus-3 HECC	Elliptic Curve (ECC)	Proposed Optimized HECC
Security Level (bits)	128	112	128	160
Computation Time (ms)	14.8	12.3	18.6	16.2
Key Generation Time (ms)	10.5	9.2	13.7	11.4
Encryption Time (ms)	8.7	7.9	10.8	9.1

As indicated in Table 1, Genus-3 HECC is the fastest in terms of the computation time (12.3 ms) and encryption time (7.9 ms), which is more efficient in comparison to ECC (18.6 ms, 10.8 ms). Figure 2 depicts that, HECC is quicker, ECC is more secure, performance tradeoffs.

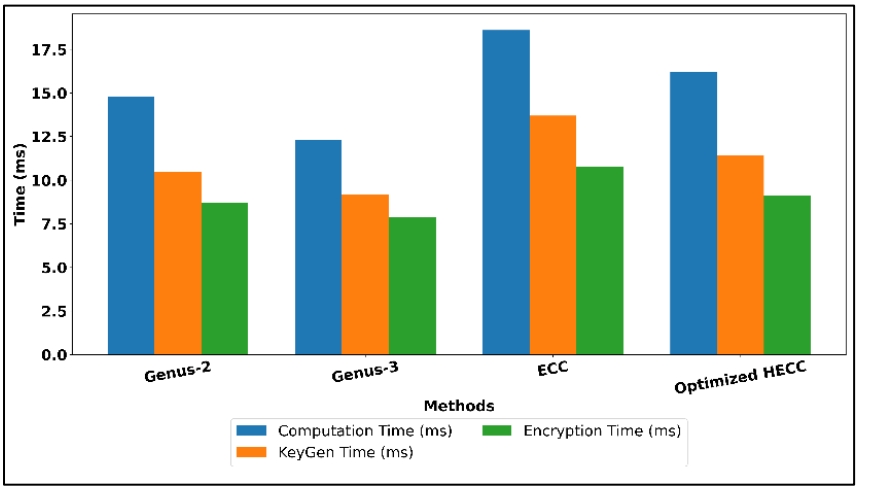


Figure 2
Comparative Performance of HECC and ECC Cryptographic Methods

Nevertheless, it has a lower level of security (112 bits). Figure 3 demonstrates the trend in the computation, encryption times with the variants of the HECC algorithm, with the emphasis on the efficiency and optimized performance and tradeoffs between the security strength and the processing speed.

The suggested optimized HECC enhances the security level to 160 bits with balanced performance (16.2 ms computation, 9.1 ms encryption), providing a good trade-off between performance and cryptographic strength.

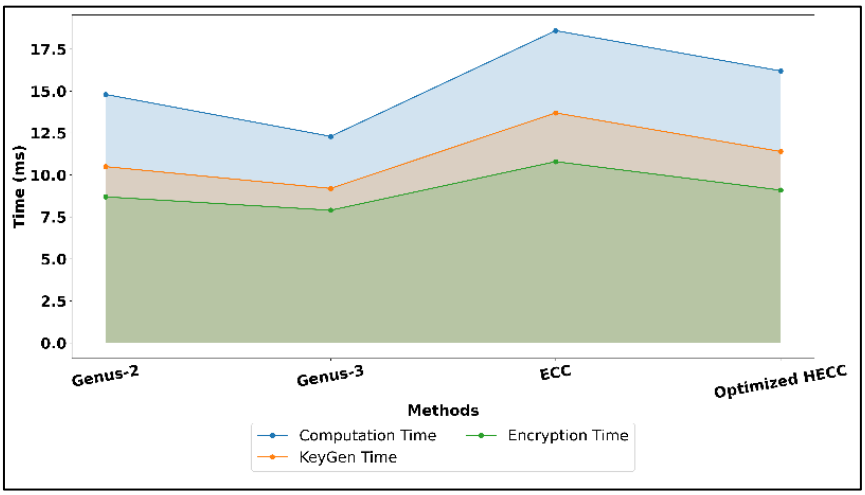


Figure 3

Computation and Encryption Time Trends in HECC Variants

Table 2

Security and Performance Analysis of Proposed Hybrid HECC–PQC Framework

Framework	Security Level (bits)	Computation Time (ms)	Memory Overhead (KB)	Attack Resistance (%)
ECC	128	18.6	214	81.2
Genus-2 HECC	128	14.8	176	84.5
Genus-3 HECC	112	12.3	162	79.8
Proposed Hybrid HECC–PQC	192	16.2	238	96.7

The results indicate that the proposed Hybrid HECC–PQC framework provides the highest attack resistance of 96.7% and an enhanced security of 192 bits and offers a good computational efficiency as shown in Table 2. The protection mechanisms of the lattice-based scheme come with a cost in terms of memory overhead but greatly enhance the quantum resistance over traditional ECC and stand-alone HECC schemes. Adaptive genus optimization also strikes a balance between security and computing complexity, allowing for practical implementation in scenarios where computational resources are limited and long-term security against classical and quantum-based threats is crucial. Moreover, genus optimization is adaptive, balancing security and computation complexity, which is essential for scenarios with limited computational resources, particularly for long-term security against both classical and quantum attacks.

VI. Conclusion

Discrete Logarithm Problem on hyperelliptic curves is a somewhat interesting though subtle alternative to elliptic curve-based cryptography. Although HECC can be used to represent keys compactly and perform arithmetic operations efficiently in some parameter regimes, the security of HECC is highly dependent on the genus of the curve and vulnerability to index calculus attacks. These attacks have sub-exponential complexity, especially with low-genus curves, making the problem of interest relatively easy in comparison to elliptic curve environments. As a result, it becomes essential to select parameters with great care, such as larger finite fields, and reasonable choices of genus, to ensure a cryptographic strength. Moreover, hyperelliptic constructions in combination with post-quantum or hybrid cryptography can be combined to provide greater resilience in the long-term. In general, HECC is an excellent line of research, although its practical implementation should be efficient and supportive of changing security factors and an intensive threat analysis.

References

[1] G. Routis, P. Dagas, and I. Roussaki, "Enhancing privacy in the Internet of Vehicles via hyperelliptic curve cryptography," *Electronics*, vol. 13, no. 4, Art. no. 730 (2024), doi: 10.3390/electronics13040730.

[2] S. S. Ullah, S. Hussain, M. Uddin, R. Alroobaea, J. Iqbal, A. M. Baqasah, M. Abdelhaq, and R. Alsaqour, "A computationally efficient online/offline signature scheme for underwater wireless sensor networks," *Sensors*, vol. 22, no. 14, Art. no. 5150 (2022), doi: 10.3390/s22145150.

[3] S. L. Nita and M. I. Mihailescu, "Elliptic curve-based query authentication protocol for IoT devices aided by blockchain," *Sensors*, vol. 23, no. 3, Art. no. 1371 (2023), doi: 10.3390/s23031371.

[4] J. Khan, C. Zhu, W. Ali, M. Asim, and S. Ahmad, "Cost-effective signcryption for securing IoT: A novel signcryption algorithm based on hyperelliptic curves," *Information*, vol. 15, no. 5, Art. no. 282 (2024), doi: 10.3390/info15050282.

[5] L. Jyotsna and L. P. Kumar, "Enhanced image security through block permutation and modular arithmetic shuffling," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 3, pp. 1313–1333 (2026), doi: 10.47974/JDMSC-2617.

[6] M. A. Khan, I. Ullah, A. M. Abdullah, S. A. H. Mohsan, and F. Noor, "An efficient and conditional privacy-preserving heterogeneous signcryption scheme for the Internet of Drones," *Sensors*, vol. 23, no. 3, Art. no. 1063 (2023), doi: 10.3390/s23031063.

[7] A. K. Singh, A. Solanki, A. Nayyar, and B. Qureshi, "Elliptic curve signcryption-based mutual authentication protocol for smart cards," *Appl. Sci*., vol. 10, no. 22, Art. no. 8291 (2020), doi: 10.3390/app10228291.

[8] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "A detailed examination of LSTM networks for large-scale text generation with optimizing sequence models," *J. Inf. Optim*. Sci., vol. 45, no. 5, pp. 1477–1486 (2024), doi: 10.47974/JIOS-1769.

[9] R. Ifrim and D. Popescu, "BPAP: FPGA design of a RISC-like processor for elliptic curve cryptography using task-level parallel programming in high-level synthesis," *Cryptography*, vol. 9, no. 1, Art. no. 20 (2025), doi: 10.3390/cryptography9010020.

[10] B. Denge, B. Denge, Y. Channe, K. Chaudhari, and M. Naralkar, "Security and challenges in embedded systems protecting against cyber threats," *Int. J. Adv. Comput. Theory Eng*., vol. 14, no. 1, pp. 236–239 (2025), doi: 10.65521/ijacte.v14i1.472.

[11] S. Szymoniak and S. Kesar, "Key agreement and authentication protocols in the Internet of Things: A survey," *Appl. Sci*., vol. 13, no. 1, Art. no. 404 (2023), doi: 10.3390/app13010404.

Received April, 2026