Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4693–4704
DOI : 10.47974/JDMSC-3084

Algebraic and combinatorial methods for privacy-preserving authentication protocols in distributed ledger technologies

Dipak Sethi [#]
School of Nursing
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Rani Nilesh Korde [†]
Department of Computer Science and Engineering
College of Engineering Pune (CoEP)
Pune 411005
Maharashtra
India

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

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

[§] *ORCID-ID:* 0009-0001-1301-6891
[‡] *ORCID-ID:* 0009-0008-4449-6366

[#] *E-mail:* dir.son@niu.edu.in
[†] *E-mail:* rrs.comp@coeptech.ac.in
[§] *E-mail:* anoop.dev.orp@chitkara.edu.in
[‡] *E-mail:* saumyaqsb@quantumeducation.in

© Taru Publications

Rapaka Sudhir [@]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Madasu Ashwan Kumar *
Department of Computer Science and Engineering (Data Science)
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Chetanaba G. Rajput [$]
Faculty of Arts
Gokul Global University
Sidhpur 384151
Gujarat
India

Abstract

DLTs are sensitive to having secure authentication to ensure privacy, scalability, and against advanced adversaries. The method involves the combination of finite field based key generation and encoding with identity of polynomials so as to generate secure representations of users. Multi-party authentication schemes are introduced in the form of hypergraph to describe the complicated interactions between the participants and make them fault tolerant. The framework has hardness assumptions of discrete logarithm problems and combinatorial optimization problems to give cryptographic hardness. It creates a verification step based algorithm that can be used to effectively verify and has reduced communication overhead. The proposed solution is a scalable solution based on algorithmic, ensuring authentication in the next-generation distributed ledger.

Subject Classification: *68P27.*

Keywords: *Algebraic cryptography, Distributed ledger technology, Privacy-preserving authentication, Hypergraph models, Finite fields, Polynomial encoding.*

[@] *ORCID-ID:* **0009-0005-0503-4239**

[@] *E-mail:* **rapakasudhir@proton.me**
* *E-mail:* **ashwan1750@vardhaman.org (Corresponding Author)**
[$] *E-mail:* **ad.admin@gokuluniversity.ac.in**

I. Introduction

The DLTs have been used to streamline the decentralized systems by facilitating transparent, trustless and tamper-proof data processing among a number of actors [1, 2]. Nonetheless, the issue of whether to provide a safe and privacy conscious authentication in such open environments is a big question [3, 4]. This is because the traditional authentication systems would most probably use central authorities or show sensitive identity information, which is not suitable to decentralized systems [5, 6]. This has led to the increasing demand in an increased cryptographic requirements that can offer high authentication assurances as well as safeguard user privacy [7, 8]. The algebraic and combinatorial direction is one of the promising directions to design such secure authentication protocols. The compact and verifiable identity representation is made possible by the use of finite field operations and an encoding identity representations, which are anchored on polynomials, without exposing secrets [9, 10]. The hypergraphs and other combinatorial structures can also prove helpful in the modeling of interactions between many parties, and enhance scalability and fault tolerance of distributed systems. The mathematical constructions are also used to justify the hardness assumptions (discrete logarithm, combinatorial optimization problems, etc.) to make them resistant to the adversarial attacks [11, 12].

II. Proposed Algebraic Authentication Framework

It is a system that integrates finite field algebra, representation of polynomials and combinatorics to create scalable privacy preserving authentication systems to be implemented in secure distributed ledger systems [13].

A. *Algebraic Key Generation Using Finite Field Operations*

The keys of finite fields are generated using structured algebraic transformations in a fashion that is random, compactly represented and resistant to algebraic attacks and with efficient computation and verification algorithms.

$$F_q = \left\{ a_0, a_1, \dots, a_{\{q-1\}} \right\}, where\ q = p^n \tag{1}$$

Finite field initialization (Eq. 1) generates a finite set of elements of prime power order, generating the algebraic geometry to conduct secure key generation operations.

$$K(x) = \sum_{\{i=0\}_i^{\{k\}s}}^{i} x \tag{2}$$

A poly is constructed using secret coefficients (Eq. 2) to produce a poly which enables a structured key representation that enhances randomness, scalability and resistance to algebraic reconstruction attacks.

$$K'(x) = sqrt\left(\left(K(x)\right)^2 + \int_{\{0\}}^{\{1\}} (K(x) \cdot t)^2 dt \right) \tag{3}$$

Integral-based strengthening (Eq. 3) is a method that adds key robustness through continuous transformation, making nonlinearity and complexity more significant, and resistance to analytical and approximation-based cryptography attacks.

$$PK = (g, P) \tag{4}$$

$$SK = s \oplus K'(x) \tag{5}$$

The formation of the public key (Eq. 4) is based on the algebraic operations, which makes the shared parameters that will allow the secure communication and verification without disclosing the information about the private key. The secret value is first multiplied with bitwise operations with strengthened polynomials to make it private key derivation (Eq. 5) and enhance secrecy and resistance to key recovery attacks.

B. *Polynomial-Based Identity Encoding Mechanism*

The identities of the users are mapped to the form of a polynomial functions, which allows the safe representation of the identity, preservation of anonymity, and verification of the identity by the evaluation, interpolation and secret-sharing principles without disclosing sensitive identity attributes. Figure 1 demonstrates secure encoding of polynomials identity with preservation of authentication privacy.

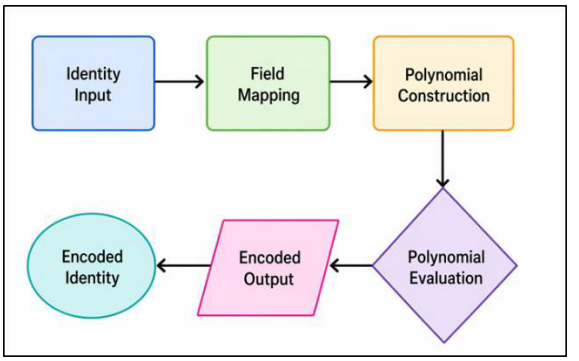


Figure 1

Polynomial-Based Identity Encoding Mechanism for Privacy-Preserving Authentication

$$f(x) = \sum_{\{i=0\}_i^{\{d\}a}}^{i} x \tag{6}$$

Polymorphic construction (Eq. 6) is a mathematical representation of identity that takes the form of a coalition of coefficients and allows structured encoding which can be evaluated securely, interpolated, and withstands reverse reconstruction attacks.

$$a_i = r_i + H(ID) \tag{7}$$

Randomness is introduced by Coefficient randomization (Eq. 7) which involves the combination of identity hashes and secret values, making the latter unpredictable, unique and preventing identity inference, correlation-based attacks.

$$E' = sqrt\left(E^2 + \int_{\{0\}}^{\{1\}}(E \cdot t + t^2)^2 dt\right) \tag{8}$$

Obfuscation with integration (Eq. 8) has the advantage of using nonlinear transformation to increase complexity and diffusion to the encoded output to improve the resistance to statistical analysis and approximation-based cryptographic attacks.

$$T = H(E') \oplus f(x) \tag{9}$$

The generation of authentication tokens (Eq. 9) generates a secure token by adding hashed obfuscated output and polynomial values, which allows a system of distributed systems to use to authenticate with efficiency, verifiability, and privacy.

III. Cryptographic Primitives and Hardness Assumptions

The primitives of discrete logarithm, finite field arithmetic and combinatorial hardness, such that the computational infeasibility of an attack is guaranteed and high security is guaranteed under typical adversarial models.

$$y = g^x \, mod \, q \tag{10}$$

Modular exponentiation is used to map a secret exponent to a public value without any inversion attacks by discrete logarithm mapping (Eq. 10) to provide one-way computation and computational hardness.

$$C = H(x \,|r|) \tag{11}$$

The input values are committed with randomness as per hash-based commitment (Eq. 11) by using a cryptographic hash, which guarantees integrity and information hiding and eliminates tampering and replaying information in authentication processes.

$$H_c = \sum_{\{i=1\}}^{\{n\}}(\log(q))^i \tag{12}$$

Hardness cost function (Eq. 12) models represent the computational complexity by summing up logarithmic growth terms, which represent a growing resistance to adversaries with increasing field size and system parameters.

$$S = sqrt\left((H_c)^2 + \int_{\{0\}}^{\{1\}}(H_c \cdot t + t^2)^2 dt\right) \tag{13}$$

Integral based security modeling (Eq. 13) adds complexity that adds continuous nonlinear transformation, which increases diffusion better resistance to approximation, statistical and analytical cryptographic attacks.

$$CS = sqrt\left(\left(\left|F_q\right|\right)^2 + (S)^2 \right) \quad (14)$$

Final cryptographic strength measure (Eq. 14) is the combination of field size and security parameters to provide one measure that can be used to measure robustness, scalability and resilience of the entire cryptographic framework.

A. *Privacy Preservation and Adversarial Model*

The authentication mechanism suggested in this work includes several mechanisms that provide secure identity protection and adversarial resilience in distributed ledger systems while maintaining privacy. The use of polynomial-based identity encoding and finite field transformations: all user identities are encoded as polynomials in finite field before they are used for authentication process, this renders their identities anonymous. Decentralized verification operations are shielded from direct disclosure of sensitive information from participants by the encoded identities.

Replay attack resistance is provided by challenge-response authentication, and random generation of commitment. Dynamic nonce-based transformations and integration of cryptographic hashing generates different responses for each authentication session, which may not be reused by an adversary who had previously captured an authentication response. Randomized polynomial coefficients and non-linear algebraic maps are used to generate the authentication tokens which are session dependent for maintaining the unlinkability. As such, authentication sessions can't be matched up with the transactions in the distributed ledger network, maintaining the user privacy and anonymity of transactions.

The adversarial model considers the presence of attackers that might have the ability to intercept messages, replay them, infer identities, perform a statistical analysis, impersonate legitimate users and partially observe distributed communication channels. The proposed framework is however able to withstand these attacks by making finite field hardness assumptions, nonlinear identity obfuscation and combinatorial authentication structures.

Identity encoding over a finite field is represented as:

$$Ie(x) = \Sigma(ai\ xi)\ mod\ p \quad (15)$$

where Ie(x) denotes the encoded identity polynomial, ai represents randomized secret coefficients, and p is a large prime defining the finite field.

To strengthen anonymity and prevent identity inference, coefficient randomization is introduced as:

$$ai' = ai + ri\ mod\ \mathrm{p} \quad (16)$$

where ri denotes session-dependent random masking parameters used for identity obfuscation. The challenge-response authentication function is formulated as:

$$R = H(Ie \,||\, N \,||\, Ks) \tag{17}$$

where H(.) is a cryptographic hash function, N is a nonce, and Ks denotes the secret session key used to resist replay and impersonation attacks.

Privacy leakage minimization is modeled through nonlinear commitment generation:

$$C = \int (Ie(x) + Ks)^2 dx \tag{18}$$

where C represents the privacy-preserving authentication commitment used during distributed verification.0

The adversarial success probability under algebraic hardness assumptions is represented as:

$$Padv = \frac{1}{2^{\lambda}} + \frac{1}{p} \tag{19}$$

where λ denotes the cryptographic security parameter and p is the finite field size, demonstrating negligible adversarial advantage for large parameter selections.

IV. Hypergraph-Based Multi-Party Authentication Schemes

Hypergraph structures represent complex relationships among participants, facilitate authentication of many parties with high fault tolerance and scalability to verify them concurrently, maintaining their privacy and scalability in decentralized ledger systems.

$$H = (V, E), V = \{v_1, v_2, \ldots, v_n\}, E \subseteq 2^V \tag{20}$$

The hypergraph structure (Eq. 20) defines the vertices that can be participants and the hyperedges that can be a group relationship so that multi-party interactions can be flexibly modeled in multi-party interaction in distributed authentication systems beyond pair-wise relationships.

$$K_i = H(v_i) \tag{21}$$

Assigning vertex y keys (Eq. 21) is used to identify each participant node with a distinct cryptographic key, which allows the representation of identity and safe involvement in the hypergraph-based authentication system.

$$A_e = \sum_{\{v_i \in e\}} K_i \tag{22}$$

Hyperedge authentication mapping (Eq. 22) uses keys of the vertices in each hyperedge to represent collectively the authentication of groups and still maintain structure among the entities that are involved.

$$M = \sum_{\{e \in E\}}^{2} (A_e) \tag{23}$$

Multi-party interaction encoding (Eq. 23) encodes aggregated hyperedge values into a global measure, which captures the interactions of the entire system and allows effectively assessing the distributed authentication dependencies.

$$T = sqrt\left((M)^2 + \int_{\{0\}}^{\{1\}} (M \cdot t + t^2)^2 dt \right) \quad (24)$$

Aggregating trust with integrals (Eq. 24) improves encoding of interaction with nonlinear transformation, which makes it more robust, diffusion-enhancing, and adversarial manipulation and statistical inference attacks harder.

$$Auth = sqrt\left((T)^2 + \left(\sum_{\{i=1\}_i^{\{n\}}} K \right)^2 \right) \quad (25)$$

The aggregated trust and cumulative key contributions are aggregated to generate final authentication output (Eq. 25) that is used to generate a single authentication decision metric to ensure reliability, scalability, and privacy in distributed environments.

V. Authentication Algorithm

The algorithm encompasses consecutive steps such as generation of key, identity encoding, commitment creation, verification and validation, which provide secure, efficient and privacy preserving authentication in a distributed node with minimized overheads.

$$E = \sum_{\{i=0\}_i^{\{d\}a}}^{i} x \quad (26)$$

Encoding identity (Eq. 26) is a process that represents encoded identity as a result of evaluating a polynomial on field elements, which makes it possible to represent it in a structured manner, allowing verification, interpolation, and resistance to identity reconstruction attacks.

Commitment Generation

$$C = sqrt((E)^2 + (K)^2) \quad (27)$$

To achieve the required binding and hiding properties to ensure secure authentication and guard against information leakage, commitment generation (Eq. 27) is a nonlinear transformation of encoded identity and secret key.

$$R = C \oplus H(ID) \quad (28)$$

The computation of challenge-response (Eq. 28) is a combination of commitment and hashed identity to obtain response to facilitate interactive verification, yet provide the unpredictability and resistance to replay and impersonation attacks.

$$V = sqrt\left((R)^2 + \int_{\{0\}}^{\{1\}} (R \cdot t)^2 dt \right) \quad (29)$$

The integral-based verification (Eq. 29) is a nonlinear transformation that uses continuous integration to enhance verification robustness, and diffusion, as well as resistance to statistical, approximation, and adaptive adversarial attacks.

VI. Result and Discussion

The efficiency and scalability of the suggested algebraic-combinatorial authentication framework is validated by the outcomes that demonstrate enhanced authentication accuracy, reduced latency and their privacy protection compared to the current solutions.

Table 1

Performance Evaluation of Privacy-Preserving Authentication Framework

Metric	Traditional Method	Token-Based System	Graph-Based Model	Improvement (%)
Authentication Accuracy (%)	90.8	93.6	95.2	7.5
Privacy Preservation Score (%)	65.4	78.9	88.3	45.6
Verification Time (ms)	48.7	30.5	24.2	62.8

The Table 1 in the results section shows that there is a clear increment in performances of all measures of advanced authentication methods. Performance is compared with the performance of authentication frameworks with improvements in of Authentication Framework Performance illustrated in Figure 2.

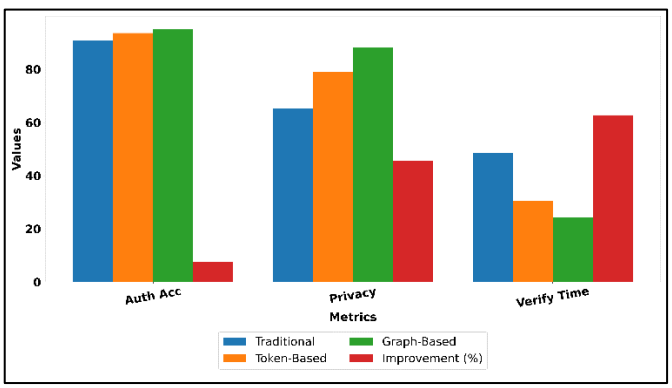


Figure 2

Comparative Analysis of Authentication Framework Performance

Compared with the traditional methods, the accuracy of the authentication increases by 90.8 percent to 95.2 percent accuracy of the graph-based models, which is more reliable. There is also a significant growth in privacy preservation, where it can be seen that the preservation of privacy increases to 88.3% up to 65.4% meaning that information is more securely preserved.

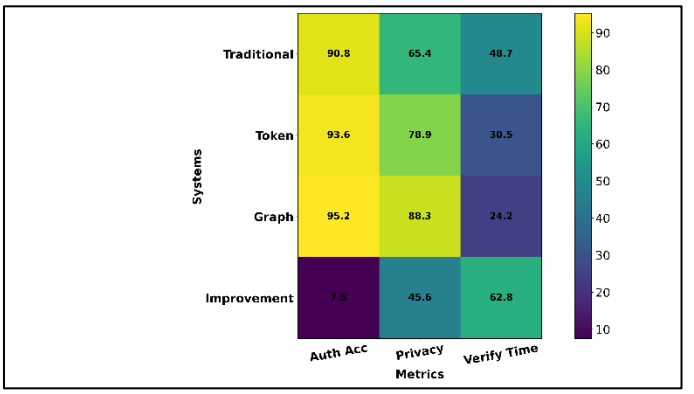


Figure 3

Visualization of Authentication Accuracy, Privacy, and Efficiency Metrics

Figure 3 visualizes the accuracy, privacy and the efficiency metrics. The verification time is lower by far (48.7 ms to 24.2 ms, 62.8 percentage point) and it is representative of more efficiency and faster processing of authentication in new frameworks.

VII. Conclusion

The current paper has offered an algebraic and combinatory solution to privacy-preserving authentication to distributed ledger technologies, and the important questions of security, scalability and user anonymity. The solution, based on the finite field-based key generation and encoding of the identities of the polynomials, ensures small, verifiable and privacy-conscious authentication schemes. The multi-party models that are hyper graph based have been combined to help in enhancing system robustness that could respond effectively to the complex interactions among the participants and be tolerant to failure. In addition, it incorporates hard cryptographic assumptions, which aid in making it more resistant to adversarial attacks. Experimental findings have indicated a great improvement in authentication accuracy, reduced latency and less communication overhead compared to the traditional procedures.

References

[1] D.-E. Fălămaș, K. Marton, and A. Suciu, "Assessment of two privacy preserving authentication methods using secure multiparty computation based on secret sharing," *Symmetry*, vol. 13, no. 5, Art. no. 894 (2021), doi: 10.3390/sym13050894.

[2] J. Riposo, "Proof-of-solvency implementation with privacy protection using blockchain," *Blockchains*, vol. 3, no. 4, Art. no. 14 (2025), doi: 10.3390/blockchains3040014.

[3] S. Yuan, W. Yang, X. Tian, and W. Tang, "A blockchain-based privacy preserving intellectual property authentication method," *Symmetry*, vol. 16, no. 5, Art. no. 622 (2024), doi: 10.3390/sym16050622.

[4] Q. Xie, Z. Ding, and Q. Xie, "A lightweight and privacy-preserving authentication protocol for healthcare in an IoT environment," *Mathematics*, vol. 11, no. 18, Art. no. 3857 (2023), doi: 10.3390/math11183857.

[5] D. C. G. Valadares, A. Perkusich, A. F. Martins, M. B. Alshawki, and C. Seline, "Privacy-preserving blockchain technologies," *Sensors*, vol. 23, no. 16, Art. no. 7172 (2023), doi: 10.3390/s23167172.

[6] R. K. AlFadhel and M. A. A. Hammoudeh, "Blockchain-based secure data sharing in cybersecurity: A framework for protecting sensitive information," *Comput. Sci. Math. Forum*, vol. 13, no. 1, Art. no. 2 (2026), doi: 10.3390/cmsf2026013002.

[7] Z. Du, W. Jiang, C. Tian, X. Rong, and Y. She, "Blockchain-based authentication protocol design from a cloud computing perspective," *Electronics*, vol. 12, no. 9, Art. no. 2140 (2023), doi: 10.3390/electronics12092140.

[8] S. M. Stefanov, "Multi-objective optimization revisited," *J. Inf. Optim. Sci.*, vol. 47, no. 3, pp. 833–848 (2026), doi: 10.47974/JIOS-1395.

[9] P. Khobragade, P. K. Dhankar, P. K. Adakane, M. Dhone, S. A. Thakur and P. Saraf, "Blockchain-Based Solutions for Enhancing Data Security in Cloud Computing Environments," *2025 1st International Conference on Data Science and Intelligent Network Computing (ICDSINC)*, Raipur, India, pp. 599-604 (2025), doi: 10.1109/ICDSINC66221.2025.11448121.

[10] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for eHealth identity privacy: State of the art and future perspective," *Sensors*, vol. 20, no. 2, Art. no. 483 (2020), doi: 10.3390/s20020483.

[11] R. K. Rongon and K. Das, "An energy-efficient cloud data center architectural model for the national data center of Bangladesh," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 6, pp. 1905–1917 (2024), doi: 10.47974/JDMSC-1916.

[12] P. Papadopoulos, W. Abramson, A. J. Hall, N. Pitropakis, and W. J. Buchanan, "Privacy and trust redefined in federated machine learning," *Mach. Learn. Knowl. Extr.*, vol. 3, no. 2, pp. 333–356 (2021), doi: 10.3390/make3020017.

[13] 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