Journal of Software Engineering, Information and Communication Technology (SEICT)

Journal homepage: https://ejournal.upi.edu/index.php/SEICT

A Survey on Linear Algebra Techniques for Modern Cryptography and Secure Information Systems

Sisilia Sylviani, Betty Subartini, Kankan Parmikanti

Departement of Mathematics, Faculty of Mathematics and Natural Science, Universitas Padjadjaran, Indonesia
Correspondence: E-mail: sisilia.sylviani@unpad.ac.id

ABSTRACT

This survey traces the far-reaching and critical role of linear algebra in the areas of modern cryptography and secure information systems. It explores how concepts of essential linear algebra can be applied to more advanced cryptographic algorithms including classical ciphers and the Hill Cipher through to leading edge post-quantum methods, including lattice-based cryptography, secure multi-party computation, and homomorphic encryption. Moreover, the paper discusses the wider applicability of linear algebra in reinforcing information system security such as error correction codes, anomaly detection, steganography, and digital watermarking. This survey is relevant to show how the methodology of linear algebra plays an essential role in ensuring the protection of digital information and suggests some promising studies in a gradually changing threat environment, especially as quantum computing emerges.

ARTICLE INFO

Article History:
Submitted/Received 05 July 2025
First Revised 07 September 2025
Accepted 30 September 2025
First Available online
01 December 2025
Publication Date
01 December 2025

Keyword:
Linear Algebra;
Cryptography;
Secure Information Systems;
Network Security

1. INTRODUCTION

The art and science of secure communication has evolved significantly, from ancient coding systems to the complex cryptographic schemes we use today. As digital threats have become more sophisticated, the field of secure information systems has expanded to encompass a variety of methods designed to protect the integrity, confidentiality, and availability of information. At the heart of many modern cryptographic techniques is linear algebra — a branch of mathematics that provides powerful tools for manipulating and transforming data.

Concepts such as vectors, matrices, and linear transformations are no longer merely theoretical constructs; they are essential components for designing, analyzing, and implementing cryptographic primitives and security protocols.

Linear algebra has always been pivotal, implicitly or explicitly, since the time of classical ciphers, when linear transformations performed the primary role to scramble messages, all through current applications such as post-quantum cryptography and privacy-preserving computation (David et al., 2016; Kjamili et al., 2023) Its capability to model complex relationships and manage large set of data makes it become a must in the contemporary processes, such as encryption and decryption, error correction and anomaly detection. With the further development of digital threats and the acuter need to have a secure information system, it is also of greater importance to know how linear algebra and secure information systems intersect (Feng et al., 2022).

This survey will give a very good description of how various methods of linear algebra are used in contemporary cryptography and secure information systems. It describes how fundamental ideas of linear algebra underlie a vast number of cryptographic algorithms, including both historical and present-day lattice-based and post-quantum designs. Furthermore, this review addresses its more general contributions to the enhancement of information security such as the secure error correction and error correction codes, the secure many party computation, and anomaly detection. This article aims to create a review of existing knowledge, outline the most significant developments, and point up areas of future investigations at the crossroads of linear algebra and cryptography and information security.

2. METHODS

This survey was carried out by carrying out a thorough literature review in order to detect and consolidate top research and developments on the subject of using linear algebra in cryptography and secure information systems. The implemented methodology entailed the systematic search within several academic databases and included the analysis of the IEEE Xplore, Science Direct, and an open discovery search engine (Lens.org). The formulation of the search queries was based on such keywords as linear algebra cryptography, hill cipher, lattice-based cryptography, secure multi-party computation linear algebra, digital signatures linear algebra, homomorphic encryption linear algebra, post-quantum cryptography linear algebra, error correction codes linear algebra, anomaly detection linear algebra, and network security linear algebra. It was reported that peer-reviewed journal articles, conference papers, academically renowned books, and technical reports of scientifically accredited research centers have been used to select the relevant papers.

Priority was given to recent publications (within the last 5–10 years) to capture the latest advancements, while seminal works such as those describing the Hill Cipher were also included for historical context. Additionally, survey and review articles were consulted to ensure a broad and balanced perspective on the subject.

The gathered information was then analyzed to identify recurring themes, key breakthroughs, and emerging trends. Special attention was paid to how fundamental linear algebra concepts (e.g., matrices, vectors, eigenvalues, eigenvectors, linear transformations, vector spaces, finite fields) are explicitly applied in modern cryptographic algorithms and security protocols. The review is organized to present these applications progressively, from classical techniques to contemporary secure information systems, demonstrating the critical role of linear algebra in each context.

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

3. RESULTS AND DISCUSSION

3.1. Linear Algebra in Classical Cryptography

Classical cryptography laid the groundwork for modern secure communication, with linear algebra playing a vital role even in early cipher systems. One well-known example is the Hill Cipher, invented by (L. S. Hill., 1929), which encrypts plaintext by converting letters into numerical values and then multiplying them with an invertible matrix over a finite field modulo 26. This approach applies matrix multiplication and modular arithmetic to transform plaintext blocks into ciphertext, making the system resistant to simple frequency analysis.

However, despite its elegant mathematical basis, the Hill Cipher has inherent weaknesses that make it vulnerable to modern cryptanalysis. Its linearity and small key space mean attackers can exploit known-plaintext or chosen-plaintext attacks by solving systems of linear equations or analyzing simple patterns. These limitations have driven research to develop stronger cipher models using advanced algebraic techniques. Based on data obtained from lens.org, the research results with the topic of Hill Cipher have reached 1,546, with the following growth illustrated in the accompanying graph.

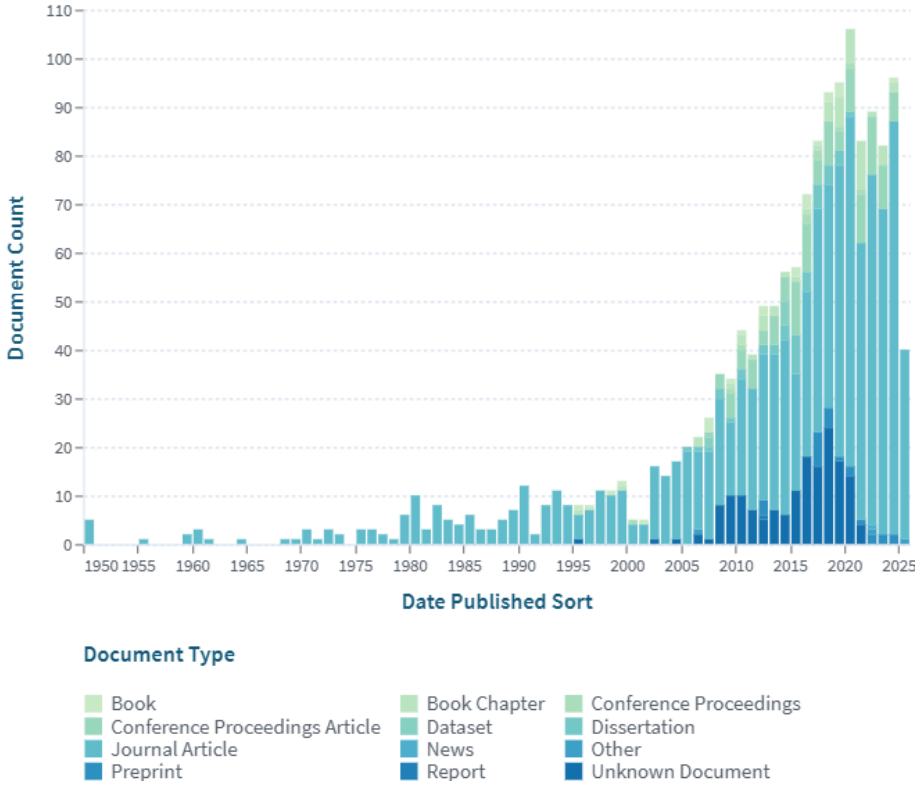

Figure 1. Publication trends on the Hill Cipher topic from 1950 to 2025 (Lens.org)

The continuous growth in studies related to the Hill Cipher demonstrates the sustained academic interest in enhancing this classical method. Various researchers have proposed modifications to address its limitations, often by expanding the key matrix, combining it with other techniques, or redesigning its block structure. Table 1 summarizes recent studies that illustrate how researchers adapt the original Hill Cipher to strengthen its security and performance.

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

Table1. Summary of selected recent research developments modifying the original Hill Cipher

Paper & Year	Methods	Results	Difference from Original Hill Cipher
Rekha & Srinivas, 2023	Block Hill Cipher: encrypts blocks of characters, expanded key space	Greater resistance to statistical attacks, improved security for longer sequences	Encrypts blocks instead of single characters, larger key space, less vulnerable to statistical analysis
Hasoun et al., 2021	Combines Hill Cipher with RSA (public key), dynamic key matrix	Increased security, more resistant to known plaintext attacks	Integrates asymmetric encryption and dynamic keys, unlike the static, symmetric original Hill Cipher
Muralidharan et al., 2023	Look-up-table for key variation, O(n) efficiency	Reduced complexity, improved speed and power efficiency	Uses dynamic key variation and lookup tables, original uses static keys and is slower
Kalpana et al., 2024	Novel alphanumeric encoding, random key generation, modulus 37	Enhanced efficiency, security, and versatility	Supports extended character set and faster key generation, original is limited to alphabet and slower
Nageshwar & Shankar, 2020	Intermediate operation modification, cryptanalysis	Simple modifications still easily broken, needs nonlinear operations	Shows that linear modifications are insufficient, original and simple variants are weak to known plaintext attacks

Finally, the Hill Cipher is purely linear. Modern cryptographic algorithms introduce non-linearity to resist attacks that exploit linear relationships. The absence of non-linearity makes the Hill Cipher predictable and easily breakable with computational power available even decades ago, let alone today. This fundamental flaw underscores why classical ciphers, despite their historical significance and mathematical elegance, are unsuitable for secure communication in contemporary information systems.

3.2. Lattice-Based Cryptography: Foundations and Hard Problems (SVP, CVP, LWE)

Lattice-based cryptography is a rapidly advancing branch of modern cryptography, recognized as a strong candidate for post-quantum security due to its resistance to attacks by quantum computers. At its core, lattice-based methods rely on the computational difficulty of solving problems in high-dimensional lattices, which are defined and analyzed using linear algebra concepts. A lattice is generated by a set of linearly independent basis vectors, forming a structure that underpins the security of various cryptosystems.

Key problems that ensure the hardness of lattice-based encryption include the Shortest Vector Problem (SVP), Closest Vector Problem (CVP), and Learning With Errors (LWE). The LWE approach, for example, builds security on the difficulty of recovering secret vectors when

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

small errors are introduced. These algebraic foundations make lattice-based schemes practical for constructing efficient and quantum-resilient encryption, digital signatures, and secure key exchange. Based on lens.org data, the topic of lattice-based cryptography has reached 5,762 results, indicating significant and growing research interest.

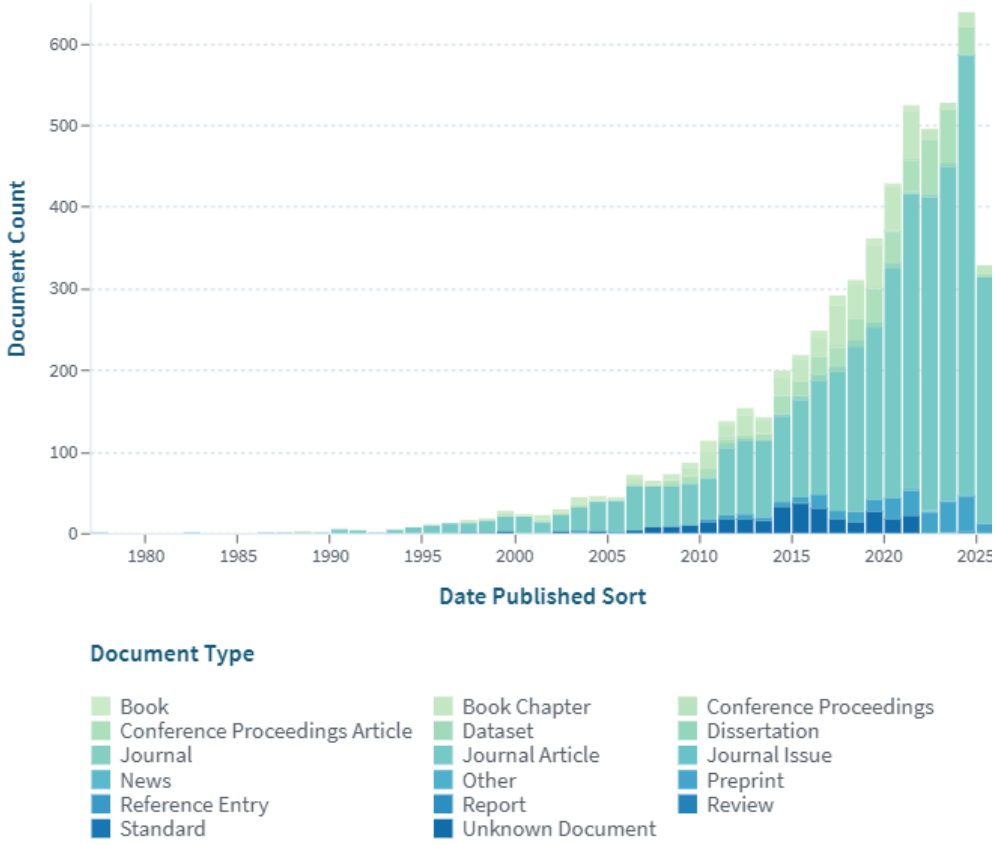

Figure 2. Publication trends on lattice-based cryptography from 1980 to 2025 (Lens.org).

The steady rise in publications reflects the growing attention given to lattice-based cryptography as a promising post-quantum solution. Researchers have actively explored its practical deployment, security strengths, and technical challenges. Table 2 highlights selected recent studies discussing trends, implementation strategies, and key gaps that remain in developing lattice-based cryptosystems.

Table 2. Summary of selected studies on lattice-based cryptography

Paper & Year	Methods	Results	Gaps/Challenges
Asif, 2021	Survey of lattice-based cryptography for IoT, lightweight cryptography	Lattice-based methods are promising for IoT due to efficiency and quantum resistance	Real-time implementation, hardware constraints, and lightweight adaptation remain challenging
Xu et al., 2022	Side-channel analysis on Kyber (NIST finalist), adaptive EM attacks	Demonstrated efficient key extraction with few traces, exposed vulnerabilities	Need for robust countermeasures against side-channel attacks in practical deployments

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

Bandara et al., 2022	Review of public-key encryption, LWE and ring-based variants	Discussed current status and implementations, highlighted trapdoor functions	Optimization of parameters and efficient deployment in real-world systems needed
Wei, 2025	Comprehensive survey, security analysis, performance evaluation	Lattice cryptography is efficient, secure, and multifunctional; NIST recognition	Ongoing challenges in performance, security analysis, and standardization

3.3 Secure Multi-Party Computation (MPC): Role of Linear Algebra in Privacy-Preserving Protocols

Secure Multi-Party Computation (MPC) allows multiple parties to jointly compute a function over their private inputs without revealing them to one another. This approach is essential for privacy-preserving data analysis, auctions, and collaborative machine learning. Linear algebra is central to many MPC protocols, especially those built on secret sharing schemes and homomorphic encryption, which frequently use matrix operations and vector spaces over finite fields.

In practice, schemes like Shamir's Secret Sharing or Linear Secret Sharing Schemes (LSSS) represent secrets as linear combinations of random vectors. Advanced MPC protocols often rely on matrix multiplication or solving linear equations, using techniques such as oblivious transfer or homomorphic operations. Linear algebra supports the efficiency, correctness, and provable security of these systems. Based on data from lens.org, research output on MPC topics involving linear algebra has reached 13,160 results, with the trend summarized in the figure below.

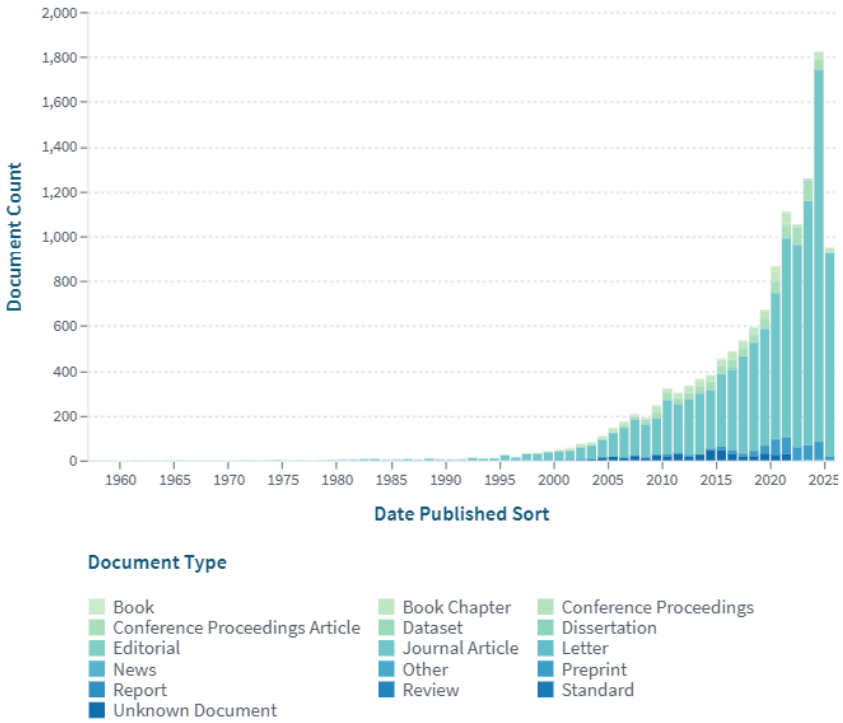

Figure 3. Publication trends on MPC using linear algebra, (Lens.org).

The steady increase in publications highlights the growing interest in developing secure MPC schemes that leverage linear algebra to enable privacy-preserving computations. Recent

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

studies demonstrate various improvements in trust models, verification, and secret sharing protocols. Table 3 presents an overview of selected works that illustrate how linear algebra concepts are applied to support distributed computation and enhance MPC security.

Table 3. Selected studies on MPC implementations using linear algebra

Authors (Citation)	Title	Methods	Results	Linear Algebra Concepts Used
Chuan Zhao, Shengnan Zhao, M. Zhao, Zhenxiang Chen, Chong-zhi Gao, Hongwei Li, Yu-an Tan	Secure Multi-Party Computation: Theory, practice and applications	Survey of SMPC protocols: secret sharing, homomorphic encryption, garbled circuits	Comprehensive review, highlights advances in efficiency and real-world applications	Matrix operations, polynomial computations, general linear algebra
Changbin Lu, Fuyou Miao, Junpeng Hou, Zhaofeng Su, Yan Xiong	Secure multi-party computation with a quantum manner	Quantum SMPC, mutually unbiased bases, quantum Fourier transform	Secure against passive adversaries, demonstrated on IBM Q, scalable to high-dimensional problems	Polynomial functions, quantum Fourier transform, orthonormal bases
Xiaotong Li, Hao Wang, Zhi Li, Lei Wu, Xiaochao Wei, Ye Su, Rongxing Lu	Publicly Verifiable Secure Multi-Party Computation Framework Based on Bulletin Board	Homomorphic MACs, pairing-based commitments, secret sharing	Enables public verifiability, efficient computation, and detection of malicious servers	General computation, supports high-level ops (e.g., comparison, bit decomposition)
Jiapeng Zhou, Yuxiang Feng, Zhenyu Wang, Danyi Guo	Using Secure Multi-Party Computation to Protect Privacy on a Permissioned Blockchain	Homomorphic encryption, secret sharing, zero-knowledge proofs	Publicly verifiable protocol, strong privacy for blockchain transactions, efficient performance	Homomorphic operations, secret sharing (matrix and vector computations)

3.4. Digital Signatures: Linear Algebra in Authentication Schemes

Digital signatures are cryptographic mechanisms used to verify the authenticity and integrity of digital messages or documents. While many widely used digital signature schemes like RSA and ECDSA rely mainly on number theory and elliptic curves, linear algebra still plays an important role in some aspects, such as hash functions and code-based schemes. Hash functions in digital signatures often use linear mixing operations or vector space transformations to compress data into fixed-size digests efficiently.

More advanced digital signatures include code-based cryptography and lattice-based schemes. Code-based signatures rely on the hardness of decoding linear codes, which involves matrix operations and permutation matrices. Similarly, lattice-based digital signatures, which are significant for post-quantum security, use vector and matrix operations

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

to secure the relationship between private keys and signatures. Based on data from lens.org, research outputs on digital signatures involving linear algebra have reached 3,790, with the growth trend shown in the following figure.

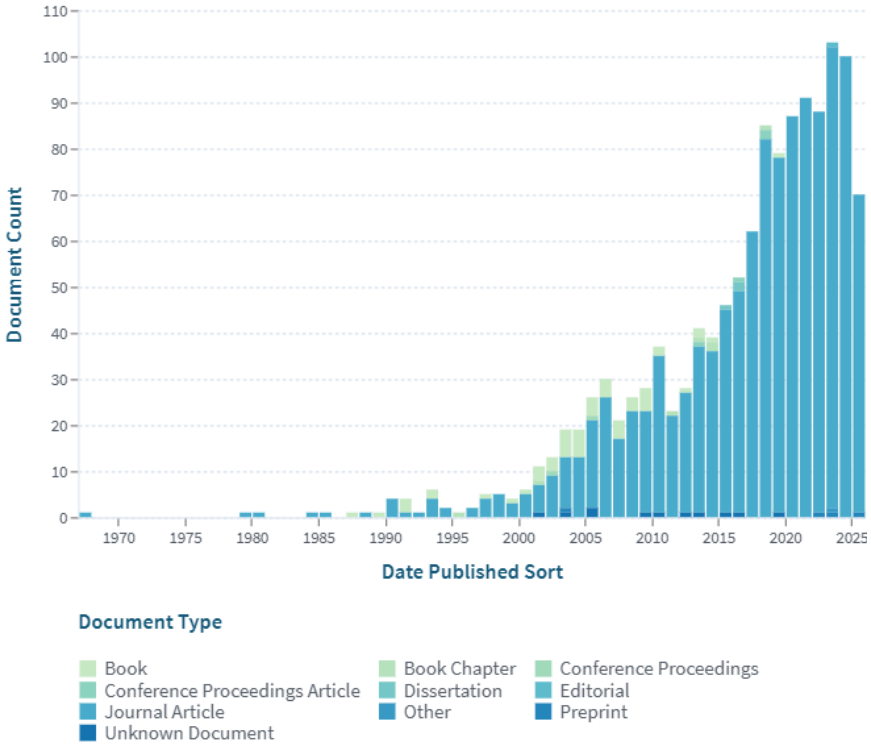

Figure 4. Publication trends on digital signature schemes involving linear algebra from 1970 to 2025 (Lens.org)

The steady increase in publications highlights the significant role of linear algebra in strengthening digital signature schemes, especially those built on code-based and lattice-based problems. Recent research explores how linear codes, vector spaces, and matrix operations contribute to enhancing key management, revocability, and fine-grained access control. Table 4 summarizes selected studies demonstrating the use of linear algebra in modern authentication schemes.

Table 4. Selected recent studies on digital signature schemes utilizing linear algebra

Paper & Year	Authors	Methods	Results	Linear Algebra Concept Used
Attribute-Based Identity Authentication Scheme Based on Linear Codes (2020)	Zhiqiang Zhang, Suzhen Cao, Longbo Han, Xueyan Liu	Constructed a traceable and revocable attribute-based authentication scheme using linear codes	Achieved fine-grained access control, efficient key revocation, and reduced computational overhead	Linear codes, vector spaces
Learning-Aided Physical Layer Authentication as an Intelligent Process (2018)	He Fang, Xianbin Wang, L. Hanzo	Used kernel machines and modeled authentication as a linear system;	Improved authentication reliability and robustness in time-varying environments	Linear systems, kernel methods

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

		applied convex optimization		
Homomorphic Linear Authentication Schemes from (ε)-Authentication Codes (2016)9	Shuai Han, Shengli Liu, Fangguo Zhang, Kefei Chen	Modular construction of homomorphic linear authentication schemes from ε-authentication codes	Provided secure, communication-efficient proofs of data possession/retrievability for cloud storage	Homomorphic linear authentication, vector spaces, algebraic curves

3.5. Homomorphic Encryption: Linear Algebra for Computations on Encrypted Data

Homomorphic Encryption (HE) is a cryptographic technique that enables computations to be performed directly on encrypted data without prior decryption, which is crucial for privacy-preserving cloud computing, secure outsourcing, and collaborative data analysis. Many HE schemes rely heavily on linear algebra, especially those based on the Learning With Errors (LWE) problem and polynomial rings. Schemes like the Brakerski-Gentry-Vaikuntanathan (BGV) and Cheon-Kim-Kim-Song (CKKS) frameworks use vector and matrix representations to perform linear transformations and modular arithmetic, enabling both additive and multiplicative operations while preserving encryption.

In these systems, encryption often encodes plaintexts as polynomials or vectors with added random noise. Operations on ciphertexts, such as addition and multiplication, are implemented as vector operations or matrix multiplications, while noise management relies on linear algebra techniques to maintain security and correctness. This synergy supports practical bootstrapping and deeper computations. Based on data from lens.org, research output on homomorphic encryption involving linear algebra has reached 13,831, with related trends shown in the following figure.

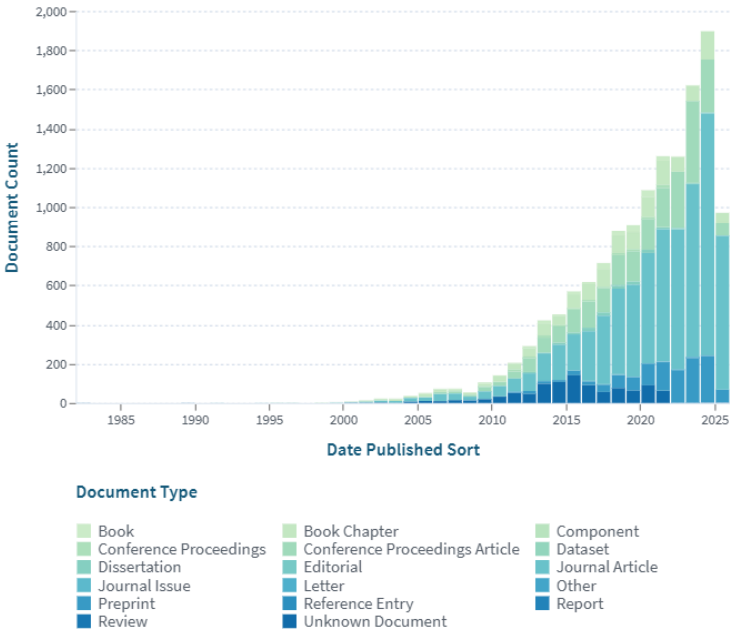

Figure 5. Overall publication trends on the application of linear algebra in cryptography and secure information systems (Lens.org).

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

The figure above illustrates the overall publication growth related to the intersection of linear algebra and cryptography or secure information systems. This trend, mapped using Lens.org, highlights the rising interest across diverse subtopics, from classical cipher methods to modern post-quantum and privacy-preserving technologies. Table 5 summarizes selected representative works, outlining their methods, results, and key linear algebra principles applied.

Table 5. Representative studies on linear algebra applications in cryptography and security

Paper & Year	Method	Results	Linear Algebra Concept
Marcolla et al., 2022	Survey of FHE schemes (LWE, RLWE-based)	Comprehensive review of FHE theory, applications in privacy-preserving ML, and performance of libraries	Lattice-based cryptography, Learning With Errors (LWE), Ring-LWE
Liu et al., 2025	Survey on Approximate HE (AHE)	Analyzes bootstrapping, precision improvements, and AHE variants for ML applications	Lattice-based schemes, approximate arithmetic over rings
Yang et al., 2021	Comparative analysis of HE libraries (Helib, SEAL, TFHE)	Summarizes theoretical and practical advances, compares performance of major libraries	Polynomial rings, lattice-based encryption
Mert et al., 2020	Hardware acceleration for BFV scheme	FPGA-based accelerator achieves up to 12× speedup for encryption/decryption	Polynomial multiplication, modular arithmetic in rings
Brakerski et al., 2020	Split FHE for indistinguishability obfuscation	Proposes split FHE using LWE-based FHE and linearly homomorphic encryption	Linear decrypt-and-multiply, LWE-based schemes

3.6. Post-Quantum Cryptography (PQC): Linear Algebra's Role in Quantum-Resistant Algorithms

The rise of quantum computing has driven the development of Post-Quantum Cryptography (PQC) to protect data against quantum attacks that could break classical schemes like RSA and ECC. Linear algebra plays a fundamental role in many leading PQC approaches, particularly those relying on lattice-based, code-based, and multivariate polynomial frameworks. The National Institute of Standards and Technology (NIST) has been coordinating standardization efforts for these algorithms.

Lattice-based PQC schemes build security on the hardness of problems like SVP and LWE, deeply rooted in linear algebra through vector and matrix operations. Code-based cryptography leverages the difficulty of decoding linear error-correcting codes using generator and parity-check matrices. Multivariate polynomial schemes, while nonlinear, often use linear algebra in solving systems and analyzing algebraic structures. Based on data from lens.org, research output on PQC involving linear algebra has reached 15,472, with growth shown in the following figure.

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

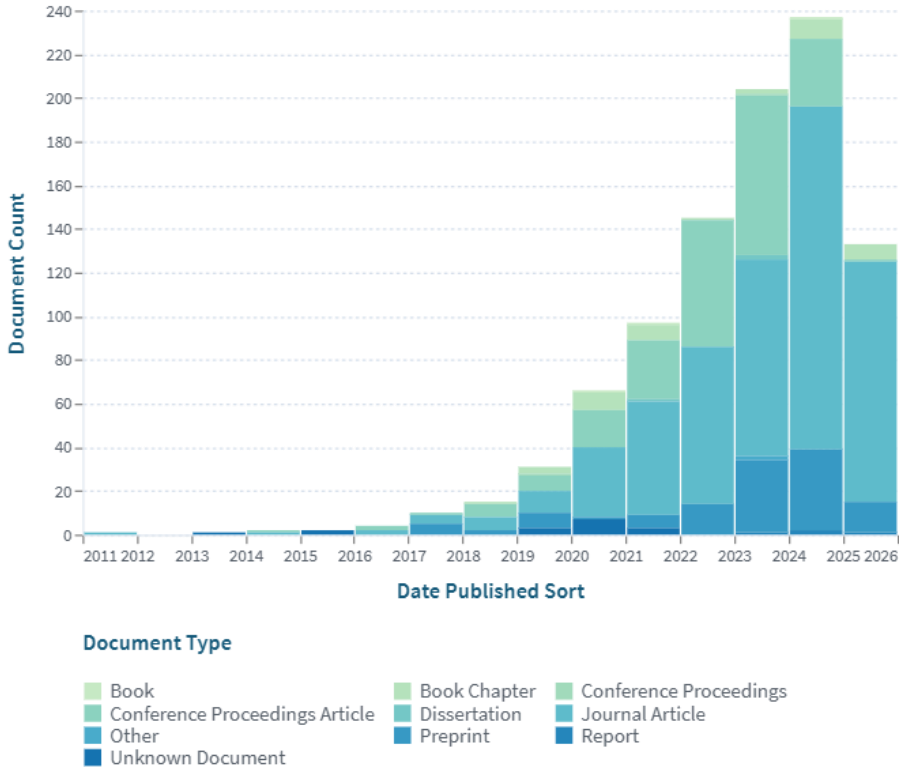

Figure 6. Publication trends on PQC involving linear algebra, (Lens.org)

The increasing trend in publications on Post-Quantum Cryptography (PQC) shows the growing research interest in designing quantum-resistant schemes that leverage linear algebraic principles. Recent studies provide comprehensive overviews, practical frameworks, and comparative analyses of lattice-based, code-based, and multivariate polynomial approaches. Table 7 summarizes representative PQC works, outlining the methods, key results, and specific linear algebra concepts that underpin their security.

Table 6. Publication trends on Post-Quantum Cryptography (PQC) involving linear algebra

Paper & Year	PQC Methods Discussed	Main Results	Linear Algebra Concepts Used
Cherkaoui Dekkaki et al., 2024	Lattice-based (CRYSTALS-Kyber, Dilithium, Falcon), code-based, hash-based, isogeny-based, multivariate	Comprehensive review of PQC algorithms, NIST standardization, transition strategies, hybrid cryptography	Lattice theory, matrix operations, polynomial rings
Chib et al., 2025	CRYSTALS-Kyber, CRYSTALS-Dilithium, NIST standards	Highlights NIST standardization, need for global PQC adoption, impact of quantum computing advances	Lattice-based cryptography (vector spaces, matrix multiplication)
Zhang et al., 2025	Overview of main PQC technical routes	Analyzes threats, introduces PQC routes, proposes	Lattice structures, error-correcting codes

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

		testing/evaluation system	
Jency Rubia et al., 2024	Families of PQC, NIST process	Reviews PQC families, standardization, challenges	Lattice-based (linear algebra), code-based (matrix codes)

3.7. Linear Algebra in Secure Information Systems

Beyond direct cryptographic applications, linear algebra is fundamental to the broader field of secure information systems, contributing significantly to data integrity, reliability, and threat detection. Its ability to model relationships and transformations in data makes it an invaluable tool for ensuring the trustworthiness and resilience of digital information.

Error Correction Codes (ECCs) are crucial for ensuring reliable data transmission and storage in the presence of noise or errors. Many ECCs, especially linear block codes, are based on linear algebra principles over finite fields. A linear code is defined as a subspace of a vector space, where valid codewords are generated by multiplying a message vector with a generator matrix. Decoding relies on parity-check matrices and the computation of syndromes to detect and correct errors efficiently.

Popular ECCs such as Hamming codes, Reed-Solomon codes, and LDPC codes illustrate how matrix operations and vector space properties safeguard data integrity. By representing bits and codewords as vectors, linear algebra provides a robust mathematical foundation for encoding and error detection. Based on data from lens.org, research outputs related to ECCs using linear algebra have reached 160.781 results, as summarized in the figure and table below.

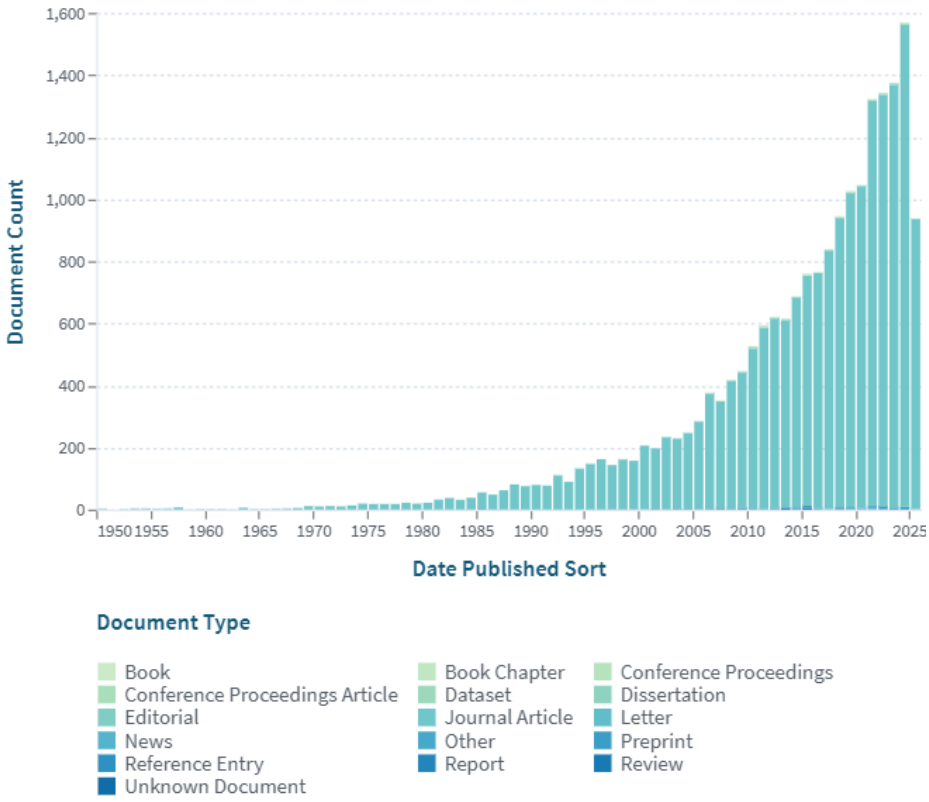

Figure 7. Publication trends on ECCs involving linear algebra (Lens.org)

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

The growing body of research shows how linear algebra continues to support innovations in error correction, ensuring robust and secure data transmission. Recent studies explore advanced ECCs that extend classical linear codes with new algebraic constructs and practical applications. Table 5 summarizes selected works highlighting key methods, results, and the linear algebra principles involved.

Table 7. Selected studies on modern error correction codes using linear algebra

Paper & Year	Methods	Results	Linear Algebra Concepts
Ly & Soljanin, 2025	Function-correcting codes (FCCs) over finite fields; derived upper/lower bounds on redundancy	Proved tight redundancy bounds for FCCs across all finite fields; constructed optimal encoding schemes	Vector spaces, code dimension, minimum distance
Nabipour & Gholizade, 2023	Analysis of arithmetic operations in GF(2^m) for BCH and Reed-Solomon codes	Detailed the necessity of efficient field arithmetic (division, multiplication, etc.) for code implementation	Galois fields, polynomial arithmetic, field operations
Cintas-Canto et al., 2023	Error detection for finite field inversions in GF(2^m) using Hamming codes and CRC on FPGA	Developed error detection schemes with low overhead for hardware reliability in field arithmetic	Hamming codes, polynomial basis, error syndromes
Hu & Liu, 2023	Construction of quantum error-correcting codes via Euclidean duals over finite fields	Produced QEC codes with improved parameters over previous literature	Dual codes, Euclidean inner product, finite field vector spaces
Yamasaki et al., 2023	Variable-length orthogonal codes using inverse DFT matrices over finite fields, combined with Reed-Solomon coding	Enabled simultaneous data multiplexing, error correction, and multi-rate transmission	Orthogonal matrices, Reed-Solomon codes, DFT over finite fields

3.8. Other Applications (e.g., Steganography, Watermarking)

Beyond cryptography, error correction, and anomaly detection, linear algebra also supports other aspects of secure information systems, especially in data hiding and intellectual property protection, such as steganography and digital watermarking.

Steganography hides a secret message within another medium so its presence is undetectable. Unlike cryptography, which encrypts data, steganography embeds information by subtly modifying transform-domain coefficients. Many methods use linear algebra concepts such as matrix decompositions, transform matrices (e.g., Discrete Cosine Transform, Discrete Wavelet Transform), and vector operations to divide the host data into blocks,

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

transform it, and embed hidden data by adjusting specific coefficients. This ensures minimal visual or auditory distortion while preserving the cover medium and secret message integrity.

Digital Watermarking protects digital content by embedding a watermark into a host signal (image, audio, or video) so that removal or tampering is difficult. Transform-domain watermarking uses the same linear algebra tools: basis transforms, orthogonal matrices, and matrix operations to encode the watermark into selected coefficients. Detection often requires vector space projections or inverse transforms to extract or verify the watermark. Together, these linear algebra techniques ensure robustness, allowing the watermark to survive common signal processing operations.

4. CONCLUSION

This survey has demonstrated the background and growing importance of linear algebra to present-day cryptography and secure information systems. Linear algebra is the mathematical foundation upon which digital data can be transformed and safeguarded, whether through classical systems such as the Hill Cipher or newer post-quantum and privacy-preserving tools and applications.Today, linear algebra is becoming increasingly important in modern cryptography, in systems based on lattices and on Secure Multi-Party Computation (MPC), in digital signatures and in Homomorphic Encryption. They require vector and matrix operations, modular arithmetic and polynomial rings to guarantee data security and integrity. Outside of cryptography, linear algebra also serves as the basis of Error Correction Codes (ECCs) and in aid of threat detection and watermarking with approaches such as PCA and SVD. To draw a conclusion, linear algebra is an important, living technique between cryptography and information security, allowing robust systems in an age of ever more sophisticated attacks. Advances in linear algebra will endure to determine the security environment as the digital data environment becomes more intricate and to provoke uses that are directed at new research directions.

6. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

7. REFERENCES

Hill, L. S. (1929). Cryptography in an Algebraic Alphabet. The American Mathematical Monthly, 36(6), 306-312. (While the original paper is not directly linked, its principles are widely discussed in various academic resources.

Number Analytics. (2025, June 14). Linear Algebra for Quantum-Resistant Cryptography.

Regev, O. (2005). On Lattices, Learning with Errors, and Cryptography. Journal of the ACM (JACM), 56(6), 1-40. (For a general understanding of LWE.

Khechekhouche, A., Benhaoua, B., Manokar, M., Sathyamurthy, R., and Driss, Z. (2020). Sand dunes effect on the productivity of a single slope solar distiller. *Heat and Mass Transfer*, *56*(4), 1117-1126.

Khechekhouche, A., Benhaoua, B., Driss, Z.., Attia, M. E. H., and Manokar, M. (2020 A). polluted groundwater treatment in southeastern algeria by solar distillation. *Algerian Journal of Environmental and Sciences*, *6*(1).1207-1211.

Khechekhouche, A., Bouchmel, F., Kaddour, Z., Salim, K., and Miloudi, A. (2020 C). Performance of a wastewater treatment plant in south-eastern Algeria. *International journal of Energetica*, *5*(2), 47-51.

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

Belbahloul, M., Abdeljalil, Z., and Abdellah, A. (2014). Comparison of the efficacy of two bioflocculants in water treatment. *International Journal of Scientific Engineering and Technology*. *3*(6), 734-737.

Behera, B., and Sethi, N. (2020). Analysis of household access to drinking water, sanitation, and waste disposal services in urban areas of Nepal. *Utilities Policy*, *62*(2020), 100996.

Heba, A., Eman, S. M. (2020). Co-sensitization of mesoporous ZnS with CdS and polyaniline for efficient photocatalytic degradation of anionic and cationic dyes. *Colloid and Interface Science Communications, 39*(2020), 100330.

Bencheikh, I, Azoulay, K., Mabrouki, J., Hajjaji, S. E., Moufti, A., and Labjar, N. (2021). The use and the performance of chemically treated artichoke leaves for textile industrial effluents treatment. *Chemical Data Collections*, *31*(2021), 100597.

Stewart, E. J. (2012). Growing unculturable bacteria. *Journal of bacteriology*, *194*(16), 41514160.

Kim, Y. K., Yoo, K., Kim, M. S., Han, I., Lee, M., Kang, B. R., and Park, J. (2019). The capacity of wastewater treatment plants drives bacterial community structure and its assembly. *Scientific Reports*, *9*(1), 1-9.

Sadasivuni, K. K., Panchal, H., Awasthi, A., Israr, M., Essa, F. A., Shanmugan, S., and Khechekhouche, A. (2020). Ground water treatment using solar radiation-vaporization and condensation-techniques by solar desalination system. *International Journal of Ambient Energy*, 1-7.

David, B., Dowsley, R., Graaf, J., Marques, D., Nascimento, A., & Pinto, A. (2016). Unconditionally Secure, Universally Composable Privacy Preserving Linear Algebra. *IEEE Transactions on Information Forensics and Security*, 11, 59-73.

Kjamilji, A., and Güney, O. (2023). Highly efficient secure linear algebra for private machine learning classifications over malicious clients in the post-quantum world. *J. King Saud Univ. Comput. Inf. Sci.*, 35, 101718

Feng, D., Zhou, F., He, D., Guo, M., and Wu, Q. (2022). Secure Distributed Outsourcing of Largescale Linear Systems. *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*, 1110-1121.

Rekha, G., and Srinivas, V. (2023). A Novel Approach in Hill Cipher Cryptography. *International Journal Of Mathematics And Computer Research*.

Hasoun, R., Khlebus, S., and Tayyeh, H. (2021). A new approach of classical Hill Cipher in public key cryptography. *International Journal of Nonlinear Analysis and Applications*, 12, 10711082.

Basavaiah, J., Anthony, A., and Patil, C. (2021). Visual Cryptography Using Hill Cipher and Advanced Hill Cipher Techniques.429-443.

D, M., R, B., R, V., and K, C. (2023). Performance And Security Enhanced Improved Hill Cipher. *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 1-5.

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699

Kalpana, P., Sumathi, P., Jose, T., Deepa, S., Mary, P., and Manimekala, B. (2024). Enhanced Hill

Cipher Algorithm with Novel Encoding and Key Generation. *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, 1-6.

Paragas, J., Sison, A., and Medina, R. (2019). An Improved Hill Cipher Algorithm using CBC and Hexadecimal S-Box. *2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*, 77-81.

Nageshwar, K., and Shankar, N. (2020). Cryptanalysis of Modification in Hill Cipher for Cryptographic Application.659-666.

Olufemi, O., and Oluwasesan, O. (2022). Trust-aware and incentive-based offloading scheme for secure multi-party computation in Internet of Things. *Internet of Things*.

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C., Li, H., and Tan, Y. (2019). Secure Multi-Party Computation: Theory, practice and applications. *Inf. Sci.*, 476, 357-372.

Lu, C., Miao, F., Hou, J., Su, Z., and Xiong, Y. (2020). Secure multi-party computation with a quantum manner. *Journal of Physics A: Mathematical and Theoretical*, 54.

Li, X., Wang, H., Li, Z., Wu, L., Wei, X., Su, Y., and Lu, R. (2024). Publicly Verifiable Secure MultiParty Computation Framework Based on Bulletin Board. *IEEE Transactions on Services Computing*, 17, 1698-1711.

Zhou, J., Feng, Y., Wang, Z., and Guo, D. (2021). Using Secure Multi-Party Computation to Protect Privacy on a Permissioned Blockchain. *Sensors (Basel, Switzerland)*, 21.

Galindo, C., Hernando, F., Matsumoto, R., and Ruano, D. (2018). Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. *Quantum Information Processing*, 18.

Ly, H., and Soljanin, E. (2025). On the Redundancy of Function-Correcting Codes over Finite Fields. *ArXiv*, abs/2504.14410.

Nabipour, S., and Gholizade, M. (2023). Arithmetic Operators over Finite Field GF(2m) for Error Correction Codes Application. *ArXiv*, abs/2310.12319.

Cintas-Canto, A., Kermani, M., and Azarderakhsh, R. (2023). Error Detection Constructions for ITA Finite Field Inversions Over on FPGA Using CRC and Hamming Codes. *IEEE Transactions on Reliability*, 72, 651-661.

Hu, P., and Liu, X. (2023). Quantum error-correcting codes from the quantum construction X. *Quantum Information Processing*, 22, 1-19.

Yamasaki, S., Matsushima, T., Ono, K., and Tanaka, H. (2024). Variable-Length Orthogonal Codes over Finite Fields Realizing Data Multiplexing and Error Correction Coding Simultaneously. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 107, 373-383.

DOI: https://doi.org/10.17509/seict.v6i2.87393
p-ISSN 2774-1656 | e-ISSN 2774-1699