

Secured Space Communication using Pell Curve Digital Signature Algorithm with Cyclotomic Polynomial

R. ELUMALAI¹ AND G.S.G.N. ANJANEYULU²

ABSTRACT. The objective of this research work is to authenticate accurate satellite signals and to withstand against the security threats of modern space communication by establishing a safe connection between satellites and Earth stations. i.e. At present, 7560 operational satellites consistently provide unclassified data and making it more complex and difficult to verify the correct signals. However, obtaining and verifying the signals are challenging without allowing attackers to alter them. This is our main problem and objective of the research. To solve the issue efficiently, a DSA on the pell curve with a cyclotomic polynomial is proposed to authenticate satellite signals accurately. As a consequence, two internal objectives have been originated. The primary objective is to study cyclotomic polynomial and design a digital signature using Pell curve. The second objective is to integrate the proposed digital signature algorithm efficiently in satellite communication to transmit and authenticate accurate signals. Apart from this, the signals are free from security threats like brute force, key-only attacks, chosen message attacks, known message attacks, total break, and selective unforgeability, which have been depicted under security analysis to strengthen our DSA technique as more efficient in satellite communication.

1. INTRODUCTION

This section provides a minimal overview of satellite communication, which uses satellite signals for various applications like military operations, remote sensing, weather monitoring, radio broadcasting, television services, internet connectivity, and global positioning system technology for smooth understanding and to provide clear picture on the concept. Every signal delivered from the satellites infers a message that is to be authenticated. Digital signature is a mathematical algorithm that confirms satellite signal validity, ensuring sender cannot deny signing, but its authenticity and non-repudiation vulnerability make it susceptible to threats. The study explores the security of satellite signals in digital communication, highlighting the need to understand historical evolution, satellite orbits, space agency formation, satellite frequency, no. of satellites in Earth orbits, and cryptographic protocols to effectively verify these signals.

The security of Global Navigation Satellite Systems (GNSS) has become increasingly critical due to their widespread adoption in civil, commercial, and safety-critical applications. Early research demonstrated that civilian GNSS signals are inherently vulnerable to spoofing and replay attacks due to their open and unauthenticated structure. Tippenhauer et al. [1] systematically analyzed the practical requirements for successful GPS spoofing attacks. Their study showed that signal manipulation is feasible under realistic conditions, thereby emphasizing the urgent need for robust authentication mechanisms.

Received: 18.01.2026. In revised form: 31.01.2026. Accepted: 14.04.2026

2020 Mathematics Subject Classification. 68P30, 94A60, 94A40.

Key words and phrases. *Cryptography, Polynomials, Network design, Coding & information theory, Channel models.*

Corresponding author: G. S. G. N. Anjaneyulu; anjaneyulu.gsgn@vit.ac.in

Following this threat identification, cryptographic approaches for civil GNSS authentication were explored. Wesson et al. [2] proposed practical cryptographic authentication for civilian GPS signals using digital signatures embedded in the navigation message. Their approach demonstrated that asymmetric cryptography can provide strong authentication guarantees but introduces computational overhead and bandwidth expansion. This work laid the foundation for modern Navigation Message Authentication (NMA) schemes.

Comprehensive surveys have further examined the evolution of GNSS authentication technologies. Yuan et al. [3] presented a systematic survey of GNSS civilian signal authentication techniques, categorizing approaches into delayed authentication schemes (e.g., TESLA-based protocols), digital signature-based mechanisms, and signal watermarking methods. Their analysis highlighted the trade-offs among latency, computational complexity, and deployment feasibility. Similarly, Chen et al. [4] reviewed the technological evolution and current status of satellite navigation signal authentication in the BeiDou Navigation Satellite System (BDS), discussing practical implementation challenges and future perspectives. Their work reflects the transition from theoretical proposals to operational authentication services.

Beyond traditional navigation message authentication, hybrid communication-navigation paradigms have also been explored. Li et al. [5] proposed a navigation enhancement signal design leveraging communication satellite signals, suggesting that authentication and integrity monitoring could benefit from cross-domain architectures. This approach aims to increase resilience against spoofing attacks through diversified signal sources.

Parallel to GNSS authentication research, alternative public-key cryptographic constructions have been investigated to improve computational efficiency while maintaining strong security guarantees. Chen [6] introduced fast RSA-type schemes derived from Pell equations over Z_N , demonstrating efficient modular arithmetic operations compared to classical RSA. Building on this framework, Padhye [7] proposed a public key cryptosystem based on Pell equations, emphasizing computational efficiency and structural security properties. These schemes present potential advantages for constrained environments such as GNSS receivers, where computational resources and bandwidth are limited.

Overall, the literature reveals three major research directions: (i) threat modeling and spoofing feasibility analysis, (ii) cryptographic navigation message authentication schemes, and (iii) lightweight or alternative cryptographic constructions for efficiency enhancement. While digital signature-based authentication provides strong security guarantees, its computational and bandwidth costs motivate further exploration of lightweight cryptographic alternatives.

Despite significant advancements in GNSS authentication, most existing civilian authentication schemes rely on conventional public-key infrastructures such as RSA or elliptic curve cryptography (ECC). These schemes, although secure, may impose non-negligible computational and bandwidth overhead on resource-constrained GNSS receivers, particularly in real-time verification scenarios. Furthermore, while Pell equation-based cryptosystems have demonstrated promising computational efficiency in general cryptographic contexts, their potential integration into GNSS signal authentication frameworks remains largely unexplored.

There is therefore a clear research gap in designing a lightweight yet secure digital signature mechanism tailored for GNSS navigation message authentication using algebraic structures derived from Pell equations. To address this gap, this work proposes a novel Pell-curve-based digital signature model that aims to reduce computational complexity while maintaining strong security guarantees suitable for real-time GNSS receiver implementation.

1.1. Symmetric Key / Public Key Algorithm, Authentication and Digital Signature.

Satellite communication systems play a vital role in enabling global internet connectivity, broadcasting, navigation, remote sensing, and secure communication services. Given the critical and sensitive nature of the transmitted data, robust cryptographic mechanisms are required to ensure confidentiality, integrity, and authenticity. To protect confidential navigation and telemetry data, service providers widely employ the Advanced Encryption Standard (AES), a symmetric-key encryption algorithm known for its computational efficiency and strong resistance against cryptanalytic attacks. AES ensures that only authorized entities can access and interpret transmitted satellite information.

The Consultative Committee for Space Data Systems (CCSDS) recommends AES as a standardized encryption mechanism for maintaining secrecy and safeguarding data in space communication infrastructures. Its adoption enhances resilience against eavesdropping, signal interception, and unauthorized data manipulation.

Beyond confidentiality, satellite navigation authentication ensures the legitimacy of broadcast location and timing signals, preventing spoofing and message manipulation that could disrupt positioning services. Consequently, public key cryptography has become fundamental to satellite authentication and secure telemetry transmission, with RSA and ECC widely adopted for their strong mathematical security foundations. RSA remains the dominant public-key algorithm, accounting for over 80% of traditional secure communication deployments. However, ECC-based schemes are increasingly preferred due to their ability to provide comparable security with smaller key sizes and lower computational complexity. In particular, ECDSA is well suited for satellite systems where bandwidth and power efficiency are critical. A symmetric key strength of 112 bits is generally recommended, with curves such as K-233 considered appropriate for constrained environments.

1.2. Space Communication. Space communication refers to the transmission of information between Earth-based stations and spaceborne platforms such as satellites, spacecraft, space probes, and space stations. It forms the backbone of modern global infrastructure by enabling navigation, remote sensing, weather forecasting, scientific exploration, military operations, and deep-space missions. Space communication systems operate primarily through radio frequency (RF) and, more recently, optical (laser) links, overcoming significant challenges such as long propagation delays, signal attenuation, Doppler shifts, noise, and limited power availability. Advanced modulation, coding, multiple-access techniques, and secure cryptographic mechanisms are employed to ensure reliable and secure data transmission across vast interplanetary distances. With the rapid expansion of satellite constellations, deep-space exploration missions, and space-based internet services, space communication has become a critical domain integrating aerospace engineering, signal processing, networking, and cybersecurity to support both civil and defense applications.

Table 1 presents a structured comparison of the major GNSS authentication models based on cryptographic approach, authentication latency, receiver complexity, bandwidth overhead, deployment maturity, and overall security level. The table highlights the fundamental trade-offs between symmetric, asymmetric, hybrid, and physical-layer authentication mechanisms in satellite navigation systems.

The TESLA-based Navigation Message Authentication (NMA) scheme, implemented in Galileo OSNMA [8], relies on delayed disclosure of symmetric key chains. Although authentication is not immediate, it achieves a strong balance between security, low bandwidth overhead, and minimal receiver complexity, making it highly suitable for large-scale civil deployment. In contrast, digital signature-based NMA approaches [2] provide immediate authentication and very high cryptographic assurance through asymmetric algorithms such as ECDSA or RSA. However, these schemes incur significantly higher computational and bandwidth costs, which limits their practicality for resource-constrained GNSS receivers.

Signal watermarking techniques such as Chimera [9] introduce hybrid authentication by embedding cryptographic information directly into the signal structure, enabling near real-time authentication with moderate complexity and bandwidth overhead. Encrypted spreading codes, exemplified by GPS M-Code [10], provide immediate and very high security through secret symmetric keys at the signal level, but their use is restricted to military applications and is not available for civil users.

Information-theoretic authentication approaches [10] shift from conventional cryptography to physical-layer properties of the signal, offering immediate verification without relying solely on key-based methods. While theoretically strong, these techniques remain experimental and require high receiver sophistication. Finally, hybrid multi-layer authentication frameworks [8] combine symmetric and asymmetric mechanisms across multiple constellations to enhance robustness and resilience. Although promising for future GNSS architectures, such systems are still in the research stage due to their complexity.

Overall, the table clearly shows that no single authentication model is universally optimal. Symmetric delayed schemes such as TESLA offer the best trade-off for civil GNSS, asymmetric digital signatures provide the highest standalone security at higher cost, signal-level encryption ensures maximum protection for restricted services, and hybrid or physical-layer methods represent forward-looking research directions aimed at improving resilience against sophisticated spoofing attacks.

TABLE 1. Comprehensive System-Level Comparison of Representative GNSS Authentication Frameworks

Model (with Ref.)	Type	Example System	Crypto Type	Auth. Delay	Receiver Complexity	Bandwidth Overhead	Deployment Status	Security Level	Overall Assessment
TESLA-Based NMA [8]		Galileo OS-NMA	Symmetric (Key Chain)	Delayed	Low	Low	Operational (Civil)	High	Efficient and scalable for civil GNSS
Digital Signature-Based NMA [2]		GPS / SBAS Proposals	Asymmetric (ECDSA/RSA)	Immediate	High	High	Research Stage	Very High	Strong security but computationally intensive
Signal Watermarking (Chimera) [9]		GPS L1C	Hybrid (TESLA + Watermark)	Immediate	Medium	Medium	Deployment Phase	High	Real-time authentication capability
Encrypted Spreading Codes [10]		GPS M-Code	Symmetric (Secret Keys)	Immediate	Medium	None	Military Only	Very High	Highly secure but restricted access
Information-Theoretic Authentication [10]		Research Prototypes	Physical-Layer Based	Immediate	High	Medium	Experimental	Theoretical High	Promising but immature
Hybrid Multi-Layer Authentication [8]		Multi-Constellation Research	Mixed (Symmetric + Asymmetric)	Mixed	High	Medium	Research	Very High	Future-oriented robust framework

Table 2 presents a concise comparison of representative GNSS authentication models based on authentication type, security level, computational cost, latency, bandwidth requirement, and their most suitable application domain. The table shows that TESLA-based schemes such as Galileo OSNMA, CHIMERA (GPS), and general Navigation Message Authentication (NMA) follow a delayed symmetric authentication approach. These models provide high security while maintaining low computational cost and low bandwidth overhead, making them highly suitable for mass-market and open-service civil receivers. Although authentication is not instantaneous due to delayed key disclosure, the latency remains acceptable for most navigation applications. In contrast, Signal Distortion Monitoring (SDM) adopts a signal-based authentication strategy that operates at the physical layer. It offers immediate detection capability with very low computational complexity and no additional bandwidth requirement; however, its security level is comparatively moderate since it primarily detects spoofing rather than providing cryptographic authentication. Overall, the table highlights the trade-off between cryptographic assurance and real-time detection, showing that delayed symmetric schemes are optimal for scalable civil deployment, while signal-based methods are effective complementary mechanisms for spoof detection.

TABLE 2. Performance-Oriented Comparison of GNSS Authentication Techniques

Model	Auth. Type	Security	Comp. Cost	Latency	Bandwidth	Best Application
TESLA (Galileo OSNMA)	Delayed Symmetric	High	Low	Medium	Low	Mass-market receivers
CHIMERA (GPS)	Delayed Symmetric	High	Low	Medium	Low	Civil GPS users
Navigation Message Authentication (NMA)	Delayed Symmetric	High	Low	Medium	Low	Open service
Signal Distortion Monitoring (SDM)	Signal-based	Medium	Very Low	Immediate	None	Spoof detection

Table 3 provides a comparative evaluation of prominent digital signature schemes considered for GNSS authentication, based on their underlying security assumptions, key and signature sizes, computational overhead, authentication latency, practical feasibility in GNSS broadcast environments, and overall suitability. The table highlights the trade-offs between classical public-key cryptography, modern elliptic-curve schemes, aggregation techniques, and post-quantum approaches.

RSA [11], which relies on the Integer Factorization Problem, requires large key sizes (2048–4096 bits) and produces comparatively large signatures, resulting in high computational overhead and significant bandwidth consumption. Although authentication is immediate, its heavy resource requirements make it impractical for bandwidth-constrained GNSS broadcast systems. ECDSA [12], based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), significantly reduces key and signature sizes while maintaining strong security, offering a more suitable balance for GNSS environments. EdDSA (Ed25519) [13] further improves efficiency by using twisted Edwards curves, providing small fixed-size signatures (64 bytes), lower computational cost, and high implementation robustness, making it particularly attractive for embedded GNSS receivers.

Aggregate signature schemes [14], built on bilinear pairings, enable multiple satellite signatures to be combined into a single compact authentication value, thereby improving bandwidth efficiency in multi-satellite constellations. Finally, CRYSTALS-Dilithium [15], a lattice-based post-quantum signature scheme, offers resistance against quantum attacks but introduces large key and signature sizes along with high computational overhead. While future-proof, its current resource demands limit immediate practicality in GNSS broadcast authentication. Overall, the table demonstrates that elliptic-curve-based signatures, particularly EdDSA, currently provide the most favorable balance between security, efficiency, and GNSS deployment feasibility, whereas post-quantum schemes represent an important direction for long-term resilience.

TABLE 3. Comprehensive Cryptographic-Level Evaluation of Digital Signature Schemes for GNSS Authentication

Signature Scheme (Ref.)	Security Basis	Typical Key Size	Signature Size	Computation Overhead	Authentication Latency	GNSS Practicality	Overall Assessment
RSA [11]	Integer Factorization Problem	2048–4096 bits	Large (>256 bytes)	High (Exp. Operations)	Immediate	Poor (Bandwidth Heavy)	Not suitable for broadcast GNSS
ECDSA [12]	Elliptic Curve Discrete Logarithm	256–521 bits	Moderate (64–132 bytes)	Medium	Immediate	Good	Widely adopted in secure systems
EdDSA (Ed25519) [13]	Twisted Edwards Curve (ECDLP)	256 bits	Small (64 bytes)	Low–Medium	Immediate	Very Good	Best balance for embedded GNSS receivers
Aggregate Signatures [14]	Bilinear Pairings (ECC)	256 bits (per signer)	Compressed (Combined)	Medium	Immediate	Promising (Multi-satellite)	Efficient for constellation-wide auth.
CRYSTALS-Dilithium [15]	Lattice-Based (Module-LWE)	2–4 KB public key	2–3 KB signature	High	Immediate	Experimental	Future-proof but heavy for current GNSS

Table 4 presents a comparative overview of representative GNSS digital signature models based on signature type, security strength, computational cost, authentication latency, bandwidth requirement, and their most suitable application scenarios. The table emphasizes the trade-offs between classical public-key schemes, modern elliptic-curve approaches, and post-quantum cryptographic proposals within the constraints of GNSS broadcast environments.

The ECDSA-based NMA model offers very high security derived from elliptic curve cryptography, providing immediate authentication. However, it introduces relatively high computational cost and bandwidth overhead due to signature transmission and verification requirements, making it more appropriate for high-security receivers with sufficient processing capability. RSA-based authentication also provides very high security but incurs very high computational and bandwidth costs because of large key and signature sizes, limiting its practicality mainly to legacy or specialized systems rather than modern mass-market GNSS receivers.

The EdDSA-based proposal (Ed25519) achieves very high security with improved efficiency compared to ECDSA and RSA. It maintains immediate authentication while reducing computational burden and bandwidth usage to a moderate level, making it well suited for modern embedded GNSS receivers. Finally, post-quantum cryptographic (PQC) signature proposals such as Dilithium or Falcon provide extremely high security with resistance to quantum attacks. Nevertheless, their higher computational and bandwidth demands currently restrict their deployment to future-proof or research-oriented systems. Overall, the table demonstrates that while all digital signature models provide immediate authentication and strong security, their suitability for GNSS depends heavily on the balance between cryptographic strength and system resource constraints.

TABLE 4. Implementation-Oriented Performance Comparison of GNSS Digital Signature Models

Model	Signature Type	Security	Comp. Cost	Latency	Bandwidth	Best Application
ECDSA-based NMA	ECDSA	Very High	High	Immediate	High	High-security receivers
RSA-based Authentication	RSA	Very High	Very High	Immediate	Very High	Legacy systems
EdDSA-based Proposal	Ed25519	Very High	Medium	Immediate	Medium	Modern receivers
PQC Signature Proposal	Dilithium / Falcon	Extremely High	High	Immediate	High	Future-proof systems

Various methodologies have been proposed to verify satellite radio navigation signals over the past two decades. Early work explored the application of quantum cryptography to satellite communication in 2000 [16]. In 2002, Rarity and Tapster *et al.* introduced a robust key exchange technique designed to enhance secure transmission [17].

In 2005, Wullems and Pozzobon *et al.* developed signal authentication and integrity verification procedures for navigation systems [18]. A significant milestone followed in 2012, when Wesson and Rothlisberger presented the work titled “Practical Cryptographic Civil GPS Signal Authentication,” focusing on implementable civil GPS authentication mechanisms [19].

Further discussions on Global Navigation Satellite System (GNSS) security were provided by Madry and Scott in 2015 [20]. In the same year, Per K. Enge proposed a novel approach incorporating random bits to strengthen authentication robustness [21].

In 2016, Fernández-Hernández introduced an authentication framework for the Galileo Open Service, laying the foundation for operational GNSS authentication [22]. Progress in satellite-based quantum key distribution was advanced by Bedington in 2017 [23]. Subsequently, Jackson and Straub (2018) investigated cryptographic solutions for securing small satellite message transmissions [24].

In 2019, Yang, Yuanxi, et al. introduced the BeiDou 3 Navigation Satellite System [25], while Rose et al. proposed a navigation message authentication proposal for the Galileo open service [26]. In 2020, Wu, Zhijun, and Paul et al. presented TESLA-based authentication for BeiDou civil navigation messages [27]. In 2020, Paul et al. proposed an optical front-end for a quantum key distribution cubesat [28]. NASA's "9.0 Communications" in 2021 examined the effectiveness of the optical communication terminal SOLISS in two-way laser communication with an optical ground station [29]. In 2021, Komatsu, Hiromitsu, et al. demonstrated the pointing performance of the SOLISS optical communication terminal in bidirectional laser communication [30].

In 2022, Tedeschi and Sciancalepore et al. presented a scholarly article on satellite-based communications security [31], while Mishra et al. presented authentication and key updates in satellite communication [32]. In 2023, Li, Ping, et al. presented a design of navigation enhancement signals based on communication satellite signals [3, 4, 5].

The security of Global Navigation Satellite Systems (GNSS) has gained increasing attention due to the susceptibility of civilian signals to spoofing and replay attacks. One of the earliest systematic studies was conducted by Tippenhauer et al. [1], who analyzed GNSS spoofing threats and introduced a comprehensive attacker model and attack taxonomy. Although no cryptographic authentication mechanism was proposed, this work laid the foundation for subsequent GNSS navigation message authentication (NMA) research.

To address the identified vulnerabilities, Wesson et al. [33] proposed a digital-signature-based GNSS authentication scheme using public-key cryptography. Their approach enabled immediate verification of navigation messages and provided strong integrity and authenticity guarantees. However, the high computational complexity and significant bandwidth overhead associated with digital signatures limited its practical deployment in GNSS systems.

In order to reduce authentication overhead while maintaining security, Fernández-Hernández et al. [22] introduced a TESLA-based NMA scheme for the Galileo Open Service. This approach employed delayed key disclosure and symmetric message authentication codes (MACs), allowing authentication data to fit within existing I/NAV reserved bits. While lightweight and deployable, the scheme inherently suffered from delayed authentication and dependence on secure root key distribution.

A comparative analysis of GNSS authentication mechanisms was later provided by Caparra et al. [34], who evaluated public-key signatures, TESLA-based approaches, and hybrid models. Their study highlighted the trade-offs between immediacy, message overhead, and security, concluding that no single solution fully satisfies all operational requirements across different GNSS use cases.

Despite these advances, existing GNSS authentication schemes predominantly rely on delayed verification, which can be problematic in high-dynamics and safety-critical applications. To overcome this limitation, the proposed method introduces a continuous GNSS authentication framework based on Pell-curve cryptography combined with SHA3-512 message authentication. The proposed approach enables near-real-time verification across multiple satellite orbits, mitigates TESLA-induced delays, and enhances resistance against spoofing and replay attacks, while maintaining efficient bandwidth usage at the cost of increased cryptographic and implementation complexity.

Table 5 presents a chronological (year-wise) comparison of representative GNSS authentication models, evaluated in terms of security, performance, and robustness. The evolution of these models reflects a transition from theoretical analysis to practical deployment-oriented solutions.

Tippenhauer et al. (2011) focus on threat modeling and attack classification, establishing a foundational understanding of GNSS vulnerabilities without implementing cryptographic enforcement. Wesson et al. (2012) demonstrate immediate signal authentication using digital signatures, achieving strong security guarantees but incurring notable computational and bandwidth overhead.

Fernández-Hernández et al. (2016) introduce a TESLA-based navigation message authentication scheme that offers a lightweight and GNSS-compatible solution, balancing security and efficiency through delayed verification. Caparra et al. (2016) comparatively analyze multiple authentication strategies, emphasizing trade-offs among security, latency, and system performance.

TABLE 5. Comparative Analysis of GNSS Authentication Models (Security, Performance, and Robustness Perspective)

Aspect	Tippenhauer et al., 2011	Wesson et al., 2012	Fernández-Hernández et al., 2016	Caparra et al., 2016
Primary Objective	Threat modeling and classification of GNSS spoofing attacks.	Immediate GNSS signal authentication using digital signatures.	Lightweight navigation message authentication for Galileo.	Systematic comparison of GNSS authentication strategies.
Authentication Mechanism	Not applicable (analysis-focused).	Public-key digital signatures (ECDSA).	TESLA-based delayed authentication with MACs.	Signature, TESLA, and hybrid schemes.
Security Coverage	Spoofing, replay, attacker capability modeling.	Strong integrity and authenticity guarantees.	Spoofing and replay resistance.	Comparative security trade-off analysis.
Security Level (Qualitative)	Analytical (no cryptographic enforcement).	High security, cryptographically strong.	High security with delayed verification.	Varies depending on scheme.
Performance Impact	Not applicable.	High computational and bandwidth overhead.	Low computational overhead; GNSS-friendly.	Evaluates performance trade-offs.
Authentication Latency	Not applicable.	Immediate authentication.	Delayed authentication due to TESLA.	Immediate vs. delayed comparison.
Robustness Characteristics	Identifies vulnerabilities and attack surfaces.	Sensitive to bandwidth and processing constraints.	Resilient to spoofing but sensitive to packet loss.	Analyzes robustness under different conditions.
Practical Deployability	Conceptual foundation only.	Limited due to overhead constraints.	Highly suitable for operational GNSS systems.	No single universally optimal solution.
Key Contribution	Establishes GNSS threat models.	Demonstrates feasibility of signature-based GNSS authentication.	Foundation of Galileo OSNMA design.	Guidance for selecting authentication schemes.

Table 6 presents a qualitative radar-based comparison of representative GNSS authentication models across six key evaluation axes: security strength, authentication latency, computational efficiency, bandwidth efficiency, robustness, and deployability. The assigned numerical values follow a normalized qualitative scale ranging from 0.2 to 1.2, where higher values correspond to stronger performance in the respective dimension.

Early analytical frameworks, such as Tippenhauer et al. (2011), show uniformly low scores across most axes, indicating that while they provide important theoretical insights, their suitability for practical and large-scale operational deployment is limited. Signature-based approaches, represented by Wesson et al. (2012), achieve strong security guarantees and relatively low authentication latency; however, these advantages come at the expense of increased computational load and reduced bandwidth efficiency, thereby affecting overall deployability.

In contrast, TESLA-based OSNMA and more recent operational models exhibit comparatively balanced performance profiles. These schemes achieve moderate to high scores across efficiency, robustness, and deployability, reflecting a more practical trade-off between security assurance and resource constraints. Such balanced characteristics make them more suitable for real-world GNSS authentication environments, where scalability, reliability, and system overhead are critical considerations.

TABLE 6. Radar Values (Qualitative Scores) for Existing GNSS Authentication Models

Axis	Tippenhauer (2011)	Wesson (2012)	Fernández-Hernández (2016)	Caparra (2016)
Security Strength	0.2	1.2	1.2	0.8
Authentication Latency	0.2	1.2	0.4	0.8
Computational Efficiency	0.2	0.4	0.8	0.8
Bandwidth Efficiency	0.2	0.4	1.2	0.8
Robustness	0.2	0.4	0.8	0.8
Deployability	0.2	0.4	0.8	0.8

Figure 1 presents a radar-based comparative analysis of representative GNSS authentication models across five key evaluation dimensions: security, performance, authentication latency, robustness, and deployability. Each axis corresponds to one metric, and the radial distance from the center represents the qualitative strength of a given model using a normalized scale of 0.2 (analytical or not applicable), 0.4 (low), 0.8 (medium), and 1.2 (high). The polygonal contours, shown without fill to emphasize relative shape and balance, illustrate the trade-offs inherent in different authentication approaches. Models with broader and more uniform coverage across all axes indicate a more balanced design, while elongated or compressed shapes reveal prioritization of specific metrics at the expense of others. Overall, the visualization highlights that OSNMA-based schemes achieve a more favorable balance among security, efficiency, robustness, and deployability com-

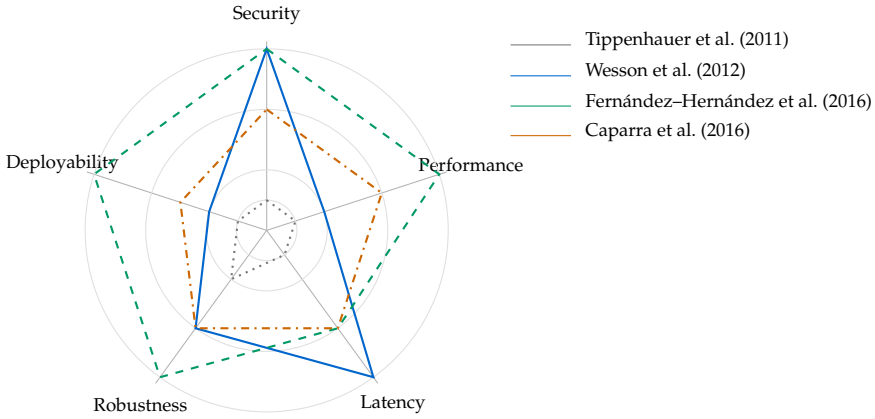


FIG. 1. Radar comparison of GNSS authentication models.

Figure 2 illustrates a security–performance quadrant analysis of representative GNSS authentication models. The horizontal axis denotes performance, interpreted in terms of computational and bandwidth efficiency, while the vertical axis represents the achieved security level, reflecting resistance to spoofing and replay attacks. Each plotted point corresponds to a specific authentication scheme, positioned according to its qualitative performance and security scores using a normalized scale of 0.4 (Low), 0.8 (Medium), and 1.2 (High). The quadrant visualization highlights the inherent trade-offs among different approaches, clearly identifying an ideal region characterized by simultaneously high security and high performance, and showing that TESLA-based OSNMA schemes occupy a more favorable balance compared to methods that prioritize only one dimension at the expense of the other.

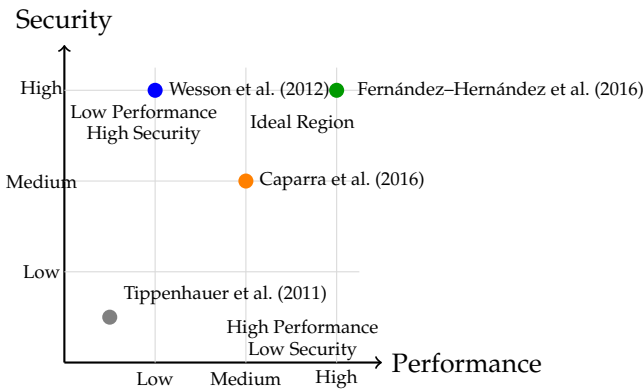


FIG. 2. Security Vs performance quadrant for GNSS authentication models.

Figure 3 presents a heatmap-based comparison of representative GNSS authentication models, including those proposed by Tippenhauer et al., Wesson et al., Fernández–Hernández et al., and Caparra et al., evaluated across the criteria of security, performance, latency, robustness, and deployability. Each cell in the heatmap encodes a qualitative assessment of the corresponding model and metric, where increasing color intensity denotes stronger capability. The numerical values displayed within the cells follow a normalized qualitative scale, with 0.2 representing not applicable or analytically supported features only, 0.4 indicating low capability, 0.8 corresponding to medium capability, and 1.2 denoting high capability.

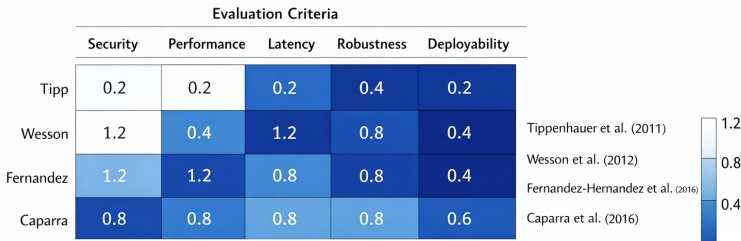


FIG. 3. Heatmap of GNSS authentication models.

This visualization enables an intuitive, side-by-side assessment of trade-offs among different authentication approaches and highlights the balanced performance profile achieved by operational OSNMA-based solutions.

Remark 1.1. *Since the evaluated GNSS authentication models are reported using heterogeneous experimental setups and performance metrics, a qualitative normalization approach is adopted [1, 2, 8, 34]. For each evaluation criterion, models are categorized as N/A (analytical only), Low, Medium, or High based on reported results and discussions in the literature. To enable visual comparison across models, these qualitative categories are mapped to numerical values {0.2, 0.4, 0.8, 1.2}. This mapping is author-defined and follows common practice in qualitative multi-criteria comparison and visualization, preserving ordinal relationships rather than implying precise quantitative equivalence [35, 36].*

Table 7 presents a unified qualitative and numerical comparison of representative GNSS authentication models across key evaluation metrics, using a normalized scoring scale from 1 (very low) to 5 (very high), where higher values indicate stronger performance. The evaluation dimensions include *Security Strength*, *Authentication Latency Efficiency*, *Computational/Bandwidth Efficiency*, *Robustness*, and *Overall Practical Suitability*. Conceptually, the results can be interpreted as a multi-axis radar chart. The comparison highlights fundamental trade-offs among different design philosophies: early analytical models [1] primarily support security assessment and theoretical insight with limited operational applicability; signature-based schemes [2] and TESLA-based OSNMA approaches [8] achieve the highest security scores. Signature-based methods excel in authentication latency but incur significant computational and bandwidth overhead, resulting in lower efficiency. In contrast, TESLA-based OSNMA demonstrates a more balanced performance profile by combining high security, excellent computational efficiency, and strong robustness validated under real satellite operational conditions, albeit with

TABLE 7. Unified Qualitative and Numerical Comparison of GNSS Authentication Models.

Metric	Tippenhauer et al., 2011 [1]	Wesson et al., 2012 [2]	Fernández-Hernández et al., 2016 [8]	Caparra et al., 2016 [10]
Security Strength	Low (1)	Very High (5)	High (4)	Medium (3)
Authentication	Not Applicable	Very High (5)	Low (2)	Medium (3)
Latency Efficiency				
Computational / Bandwidth Efficiency	Very High (5)	Very Low (1)	Very High (5)	Medium (3)
Robustness in Operational Conditions	Medium (2)	Medium (3)	High (4)	Medium (3)
Overall Practical Suitability	Low (2)	Low (2)	Very High (5)	Medium (3)
Best-Suited Scenario	Security analysis	Immediate authentication	Resource-constrained GNSS receivers	Design-time comparison

Key Takeaway: TESLA-based OSNMA achieves an effective balance across security, efficiency, and operational robustness, whereas signature-based schemes prioritize immediate authentication at the expense of computational cost and overall system efficiency, limiting their suitability for resource-constrained GNSS receivers.

TABLE 8. Interpretation of Numerical Scores Used in Table 7

Score	Interpretation
1	Very Low: Minimal or no support; unsuitable for practical deployment.
2	Low: Limited capability with significant trade-offs.
3	Medium: Adequate performance; acceptable under specific conditions.
4	High: Strong performance with minor limitations; suitable for most operational scenarios.
5	Very High: Optimal or near-optimal performance; well-suited for operational deployment.

Note: For Authentication Latency Efficiency and Computational/Bandwidth Efficiency, higher scores indicate better performance (i.e., lower latency and lower overhead).

Table 8 provides a qualitative interpretation of the numerical scores used in Table 7 for evaluating and comparing authentication schemes. A score of 1 represents very low capability, indicating minimal or no functional support and unsuitability for practical deployment, while a score of 2 denotes low capability with significant limitations and trade-offs. A score of 3 corresponds to medium performance, reflecting adequate functionality that is acceptable under specific or constrained conditions. Scores of 4 and 5 indicate high and very high performance, respectively, where a score of 4 signifies strong capability with only minor limitations and suitability for most operational scenarios, and a score of 5 represents optimal or near-optimal performance that is well-suited for real-world deployment. For authentication latency efficiency and computational or bandwidth efficiency metrics, higher scores indicate better performance, corresponding to lower latency and

2. NECESSITY, MOTIVATION AND OVERVIEW OF THE PAPER

2.1. Necessity of Proposed Digital Signature Algorithm. As of January 2024, a union of concerned scientists estimated that the Earth is monitored by 7560 operational satellites, including 5184 from the US, 181 from Russia, 628 from China, and 1572 from other countries. The data shows the number of satellites in four different orbits: there are 6768 satellites in LEO, 143 in MEO, 59 in HEO, and 590 in GEO. The USA has allocated a large amount of funding to the development of satellites, even though it began its space project eight years after Russia. These satellites are providing unclassified data to ground stations. However, obtaining and verifying these signals is challenging without allowing attackers to alter them. It is crucial to verify the correct signal from the correct satellites. This issue will be addressed in the subsequent section. This section explores GNSS, including military, navigation, and weather satellites from various countries, including NORAD catalogue numbers, launch details, and total number of satellites in four orbits.

The North American Aerospace Defence (NORAD) Catalogue Number is assigned by the US Space Command to all artificial objects in Earth's orbit and those that have departed Earth's orbit. The Sputnik 1 launch vehicle, identified by its number 1, was the first recorded item, while the second recorded item pertains to the Sputnik 1 satellite.

As an inference from the above discussion a vast quantity of signals is consistently obtained from civil, commercial, government, and military satellites, and so on. Overall, there are 7560 active satellites. It is thus a really challenging issue which leads to our motivation and objective. i.e. to get the accurate signals from their own country's satellites. Therefore, we are proposing a DSA on the Pell curve using cyclotomic polynomials to authenticate accurately all these satellite signals.

2.2. Motivation and Overview. The papers [6, 7] discussed a rapid RSA-like scheme, cryptosystem and digital signature based on the Pell equation, and a signature scheme using the Lagrangian continued fraction method. In 2018, Ignacio Fernandez-Hernandez presented a study on digitally-signed satellite radio-navigation signals [37]. *None of the above has given any perfect solution to the issue addressed above. So our research work aims to address this issue by designing a digital signature algorithm on the Pell curve using cyclotomic polynomials in relation to accurate satellite signal authentication for messages and pictures, which also involves the location and time of the signal.*

The paper is structured in the following manner: The section 3 introduces a digital signature method that utilizes the Pell curve and cyclotomic polynomial. This scheme is utilized in the realm of space communications. Section 4 delves into the topic of security attacks. The final section concludes with a summary of the contributions.

3. MATERIALS AND METHODS

3.1. Mathematical Background - Pell Curve & Cyclotomic Polynomial. Let us consider a Pell curve

$$(3.1) \quad P_{N,k^2}(F_p) = \{(x, y) : x^2 - Ny^2 = k^2 \pmod{p}\}$$

for $N = m^2 - k^2, k \in \mathbb{N}$ over any finite field F_p . The binary operation for the set of all rational points on the Pell curve over F_p is point addition, i.e.

$$(3.2) \quad (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 + Ny_1y_2}{k}, \frac{x_1y_2 + y_1x_2}{k} \right).$$

The algebraic structure $(P_{N,k^2}(F_p), +)$ satisfies all the group axioms and is named as Pell curve group (PCG) and more related details can be seen in [38].

Cyclotomic polynomials $\phi_n(x)$ are a subject of interest in algebraic number theory. These polynomials are defined as irreducible polynomials with coefficients in the rational numbers, which have roots that are primitive.

An essential connection between cyclotomic polynomials and the n th root of unity is

$$(3.3) \quad x^n - 1 = \prod_{d|n} \phi_d(x).$$

For instance, if $n = 27$, then $\phi_{27}(x) = x^{18} + x^9 + 1$. If a prime number $q \nmid n$, then $\phi_n(x)\phi_{qn}(x)$ and $\phi_n(x^q)$ have the same number of roots in $\mathbb{N}[x]$ [39]. Hence we have

$$(3.4) \quad \phi_n(x)\phi_{qn}(x) = \phi_n(x^q).$$

Cyclotomic polynomial property illustrated in the Eqn. (3.4) and the platform of Pell curve have been used to develop our security protocols like digital signature and authentication in the forthcoming subsections 3.2. The logical reason to apply this one as a platform is that we obtain the exact number of elements over finite field F_p like in ECC.

The proposed digital signature algorithm on the Pell curve using a cyclotomic polynomial addresses the challenge of verifying the authenticity of satellite signals is as follows:

3.2. Proposed Digital Signature Algorithm on Pell Curve (PCDSA). This section introduces a digital signature algorithm that has been developed and implemented in the realm of space communication. It assesses the authenticity of open satellite radio navigation signals at the user's receiver level. The algorithm involves receiving a radio navigation signal from a satellite that may not be connected to a ground mission section, and a second signal from a satellite connected to a ground mission segment. The second signal contains a digital signature, created by applying a cryptographic hash function to a specific portion of the message. The digital signature is then decrypted using a cryptographic hash function on the first message's random bits section. If the hash value and decoded digital signature are congruent, the recipient should configure their system to regard the first and subsequent radio-navigation signals as genuine.

3.2.1. Global Domain Parameters. Let $P_{N,k^2}(F_p) : x^2 - Ny^2 = k^2 \pmod p$, be a pell curve group of order m' and Υ represent the base point of the group [38]. Alice and Bob refer to satellite and Earth station, respectively, in this system. Satellite proceeds by selecting a positive number, denoted as n , in a random manner. It then proceeds to determine the appropriate cyclotomic polynomial, denoted as $\phi_n(x)$, which is widely recognised and acknowledged. In the present scenario, the public parameters are k, N, p, Υ, m' and $\phi_n(x)$.

Algorithm 1 Global Domain Parameters**Satellite****Require:** (m, k, p) **Ensure:** The public parameters

- 1: chooses a large random prime number p .
- 2: chooses a random number $m > k \in \mathbb{N}$.
- 3: $N \leftarrow (m^2 - k^2)$.
- 4: finds a base point Υ in $P_{N,k^2}(F_p)$
- 5: computes order m' of the group $P_{N,k^2}(F_p)$
- 6: chooses a random positive integer n
- 7: computes cyclotomic polynomial $\phi_n(x)$
- 8: **return** $(k, N, p, \Upsilon, m', \phi_n(x))$

3.2.2. *Key Generation.* Satellite selects a positive integer d at random from the interval $[1, m' - 1]$ and a prime number ρ at random, ensuring that $\rho \nmid n$. Subsequently, Satellite does calculations

$$(3.5) \quad \Omega = \phi_n(d)\Upsilon \bmod m',$$

which is a point in the $P_{N,k^2}(F_p)$. The public key (k_{pub}) in this case is Ω , and the private key (k_{pr}) is $\phi_n(d)$. Cyclic polynomials are used to generate a high-level private key $\phi_n(d)$, which is then connected DLP over the Pell curve for enhanced security.

Algorithm 2 Key Generation**Satellite****Require:** $(d, \rho, n, \Upsilon, m')$ **Ensure:** Public and Private key

- 1: selects random $d \in [1, m' - 1]$
- 2: computes cyclotomic polynomial $\phi_n(d)$
- 3: $\Omega \leftarrow \phi_n(d)\Upsilon \bmod m'$
- 4: **return** $(k_{pr}, k_{pub}) = (\phi_n(d), \Omega)$

3.2.3. *Signature Generation.* In Satellite using PRNG, prime numbers ρ, q, r are generated, ensuring that they are not divisors of n . It then proceeds to compute the cyclotomic polynomial $\phi_n(d^\rho)$. Subsequently, Satellite ascertains the coordinates of the two-dimensional point using the k_{pub} .

$$(3.6) \quad C = (x, y) = \phi_n(d^\rho)\Upsilon \bmod m'$$

and Satellite determines signature u and k as follows:

$$(3.7) \quad u = (x +_p y) \bmod m'$$

$$(3.8) \quad k = \phi_n(d^\rho)\phi_{\rho n}^{-1}(d)r$$

and Satellite chooses the message M , then finds $\phi_n(M^q)$, $\phi_{qn}^{-1}(M)$, hashes these using SHA3 512, and obtains the signature s is as follows:

$$(3.9) \quad s = H(\phi_n(M^q)\phi_{qn}^{-1}(M))\phi_{\rho n}^{-1}(d)\phi_n(d)r$$

Now Satellite sends the 3-tuple (u, k, s) to Earth station along with the message M .

Algorithm 3 Signature Generation**Satellite**

Require: $(p, d, M, n, \rho, q, \Upsilon, m')$
Ensure: The signature (u, k, s)

- 1: finds a random prime $\rho, q, r \nmid n$
- 2: $C(x, y) \leftarrow \phi_n(d^\rho)\Upsilon \bmod m'$
- 3: $u \leftarrow (x +_p y) \bmod m'$
- 4: $k \leftarrow \phi_n(d^\rho)\phi_{\rho n}^{-1}(d)r$
- 5: chooses the message M
- 6: $H(\phi_n(M^q)\phi_{qn}^{-1}(M))$, using SHA3-512
- 7: $s \leftarrow H(\phi_n(M^q)\phi_{qn}^{-1}(M))\phi_{\rho n}^{-1}(d)\phi_n(d)r$
- 8: **return** (u, k, s, M)

3.2.4. *Signature Verification.* The Earth station performs a verification process to confirm the validity of the signal. At first, the Earth station stores the signature (u, k, s, M) after receiving it from the satellite, then finds $\phi_n(M)$ and hashes it using SHA3 512. Second, it finds the inverse of the signature S and multiplies it with k , then finds a two-dimensional point using the previously sent k_{pub} is as follows:

$$(3.10) \quad C' = (x', y') = H(\phi_n(M))(s^{-1}k)\Omega \bmod m'$$

and then, Earth station calculates

$$(3.11) \quad v = (x' +_p y') \bmod m'.$$

If $v = u$, Earth station accepts the signature.

Algorithm 4 Signature Verification**Earth station**

Require: $(n, \Omega, u, k, s, M, \rho, m')$
Ensure: signature authentic or not authentic

- 1: signature (u, k, s, M) is received and stored in memory
- 2: computes the cyclotomic polynomial $\phi_n(M)$
- 3: computes $H(\phi_n(M))$ using SHA3-512
- 4: $C'(x', y') \leftarrow H(\phi_n(M))(s^{-1}k)\Omega \bmod m'$
- 5: $v \leftarrow (x' +_p y') \bmod m'$
- 6: **if** $v = u$ **then**
- 7: valid signature
- 8: **else**
- 9: invalid signature
- 10: **end if**

3.2.5. *The Validity of the Proposed algorithm.* The signature will be consistently accepted by the receiver, provided that the signer adheres to the aforementioned conditions. The validity of the suggested algorithm is proven in the following manner: Eqns. (3.10), (3.9), (3.8) and (3.5) provide the following results:

$$\begin{aligned}
(3.12) \quad C' &= (x', y') = H(\phi_n(M))(s^{-1}k)\Omega \bmod m' \\
&= H(\phi_n(M))((H(\phi_n(M^q)\phi_{qn}^{-1}(M))\phi_{pn}^{-1}(d)\phi_n(d)r)^{-1} \\
&\quad (\phi_n(d^p)\phi_{pn}^{-1}(d)r)\phi_n(d)\Upsilon \bmod m' \\
&= H(\phi_n(M))((H(\phi_n(M^q)\phi_{qn}^{-1}(M)))^{-1}(\phi_n(d^p))\Upsilon \bmod m' \\
&= \phi_n(d^p)\Upsilon \bmod m'
\end{aligned}$$

By referring to Eqns. (3.6) and (3.12), it may be seen that:

$$(3.13) \quad C'(x', y') = C(x, y).$$

So,

$$(3.14) \quad (x' +_p y') \bmod m' = (x +_p y) \bmod m'.$$

The proof $v = u$ is obtained from Eqns. (3.14), (3.11), and (3.7) .

3.3. Integration - Pell Curve Digital Signature Algorithm in Space Communication.

3.3.1. *Drawbacks: Existing Digital Signature algorithm over Space Communication.* Let Satellites 1, 2, and 3 broadcast their standard navigation messages, denoted as M_1 , M_2 , and M_3 . In addition to typical navigation content such as ephemeris data, clock corrections, and ionospheric parameters, each message also includes randomly or pseudorandomly generated bits originating from the satellite. These additional fragments do not carry semantic meaning but provide unpredictability against potential adversaries.

A standard cryptographic hash function is applied to M_1 , M_2 , and M_3 , producing the corresponding hash values H_1^1 , H_2^2 , and H_3^3 . The superscript denotes the association of each hash with the data received from Satellites 1, 2, and 3, respectively. The receiver stores these hash values in its local memory for subsequent verification.

At a later time instant, the receiver progressively obtains the digitally signed messages $DS(M_1)$, $DS(M_2)$, and $DS(M_3)$ transmitted by Satellite 4. The receiver verifies the authenticity of these signatures using the standard digital signature verification procedure. By using the previously distributed public key, the receiver decrypts the signed messages and extracts the hash values H_1^4 , H_2^4 , and H_3^4 . These extracted hashes correspond to the signed versions of M_1 , M_2 , and M_3 .

Finally, the receiver compares H_1^1 with H_1^4 , H_2^2 with H_2^4 , and H_3^3 with H_3^4 . If all corresponding hash pairs match simultaneously, the signals received from Satellites 1, 2, and 3 are authenticated as genuine.

To authenticate Satellite messages M_1 , M_2 , and M_3 , digital signatures (of Satellites 1, 2, and 3) are required from Satellite 4. However, this may not always be possible due to different satellite velocities $\{V_{sat1}, V_{sat2}, V_{sat3}\} \neq V_{sat4}$, and weather-related issues that may prevent the validation of the signature's authenticity, which is a major drawback of the existing algorithm in space communication shown in Fig. 4. For example, Sat1: NOAA 21 has perigees of 833 km and apogees of 835 km, with periods of 101 minutes. Sat2: SPIRALE A has perigees of 469 km and apogees of 17360 km, with periods of 313 minutes. Sat3: NAVSTAR 81 has perigees of 20152 km and apogees of 20226 km, with periods of 718 minutes. Sat4: GOES 17 has perigees of 35786 km and apogees of 35801 km, with periods of 1436 minutes. Satellites Sat1, Sat2, and Sat3 are unable to transmit signals to Sat4 due to varying velocities. The research methodology leads the main issue

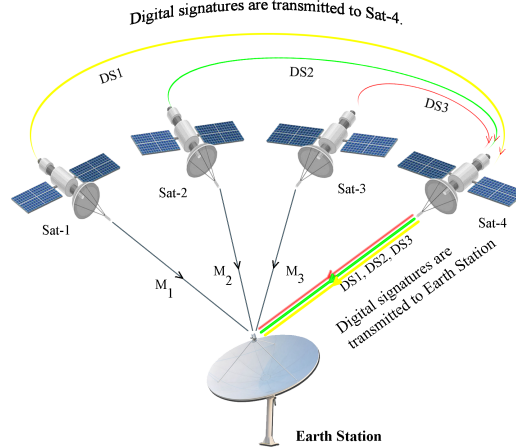


FIG. 4. To verify satellite signals, including messages, object position, timing information, and signal time of arrival, four satellites are needed.

Credits: Ignacio Fernandez-Hernandez

addressed in the abstract, which will be overcome using the proposed digital signature algorithm.

3.3.2. *Significance of PCDSA in Space Communication.* The aim is to manipulate a primary radio-navigation Satellite's behavior by introducing random bits. A monitor receiver receives a navigation message with unexpected bits and uses it to construct a digital signature using cryptographic hash function, cyclotomic polynomial, Pell curve and encryption. The digital signature is transmitted to a secondary Satellite connected to the ground mission segment, which inserts it into a subsequent navigation message. The digital signature must have a minimum symmetric-key strength of 112 bits to resist exhaustive key search attacks. The navigation message section, including unpredictable components, must have a minimum length of 1024 bits using the SHA3 512 cryptographic hash algorithm and PCDSA K-512 encryption.

The user or receiver can view the sequence of events as follows:

Large-lens, high-resolution CCD cameras are used by Satellites to take pictures of their surroundings. Their closeness in LEO allows them to collect higher-resolution photos. In fewer rotations, Satellites may capture low-resolution photographs, or they can capture high-resolution images over longer times. To capture high-resolution photographs of wide regions, many photos must be acquired and stitched together to form a single bigger image. The clarity of an image is determined by its spatial resolution, not the number of pixels. It refers to the precision of a measurement with respect to space, namely the number of independent pixel values per unit length. EOSDA LandViewer offers Satellite data with low ($> 100 \text{ m/pxl}$), medium ($10 - 50 \text{ m/pxl}$), and high spatial resolutions ($1 - 4 \text{ m/pxl}$) for various use cases, ensuring accurate and precise image resolution.

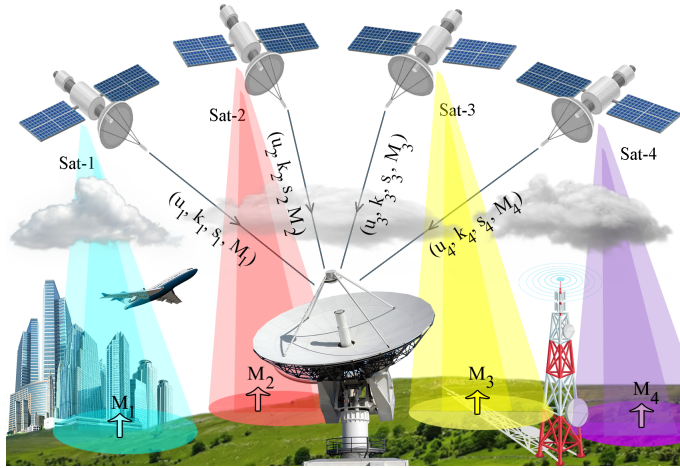
Satellites captured photo stores as $M_1, M_2, M_3, \dots, M_n$. The PCDSA is applied to these stores, generating signatures $(u_1, k_1, s_1), (u_2, k_2, s_2), (u_3, k_3, s_3), \dots, (u_n, k_n, s_n)$. These signatures include standard navigation signatures, messages, and random or pseudorandom bits. These fragments lack semantic significance but exhibit unpredictability for deceptive entities. The Earth station receives these signatures $(u_1, k_1, s_1), (u_2, k_2, s_2), (u_3, k_3, s_3), \dots, (u_n, k_n, s_n)$ and messages one by one from satellites and stores this information in memory. After applying the cyclotomic polynomial $\phi_n(x)$ to the messages $M_1, M_2, M_3, \dots, M_n$, the Earth station hashes the result using SHA3 512, multiplies it by the signature s_i^{-1}, k_i , and uses the previously provided public key $k_{pub} = \Omega_i$ to obtain v_i . The comparison is made between u_1 and v_1, u_2 and v_2, u_3 and v_3, u_4 and v_4, \dots, u_n and v_n . When all n occurrences occur simultaneously and equal, it may be assumed that the signals coming from the satellites are authentic. The detailed explanation is provided in Fig. 5.

In order to check the time of arrival of satellites, the Earth station may use several techniques, such as jamming detectors, receiver clock jump detectors, and measurement consistency. To enhance security, it is essential for the receiver to include anti-tampering measures that effectively detect unauthorised individuals from gaining access to and changing memory regions that are critical for authentication purposes. By using measurements and data obtained from a minimum of four validated satellites, the receiver has the capability to ascertain an authenticated three-dimensional position and corresponding time. It is recommended to use SHA3-512 in conjunction with a 1024-bit digital signature with PCDSA K-512. According to the requirement, it is necessary for the message to have a length that is at least twice the size of the output of the hash function. In the case of SHA3-512, it is recommended to use a signature length of 1024 bits. The E1B signal of Galileo has the capability to transmit these bits within a time frame of 4 seconds. This time frame is equivalent to two standard pages. According to the Galileo Open Service Signal-in-Space (OS SIS) and Observed Carrier-to-Noise Density (OCD) specifications, it is stated that a single I/NAV message frame requires a duration of 720 seconds. The total number of subframes is 24, with each subframe having a duration of 30 seconds. Each subframe consists of a total of 15 nominal pages. Each nominal page is comprised of two pages: an even page and an odd page, each with a duration of one second. The odd page contains textual information, such as ephemeris and almanacks, along with supplementary fields. The term "data" is presented on the even-numbered pages.

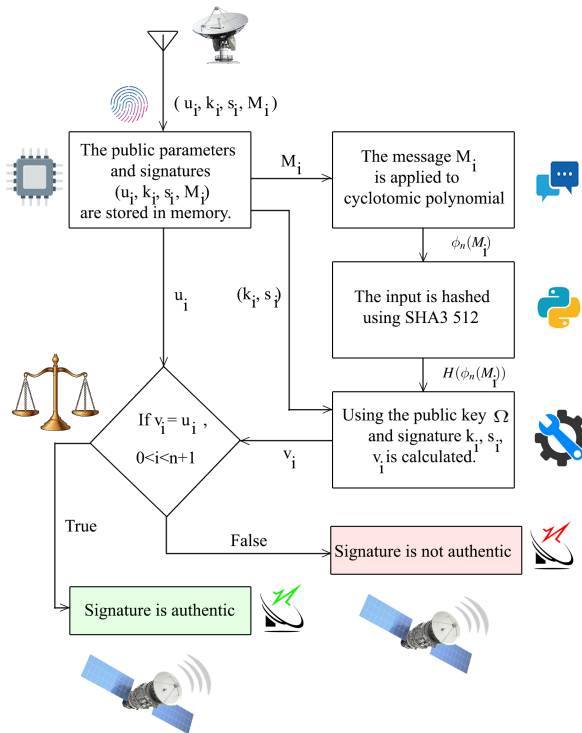
OSNMA: Nav Msg \rightarrow Wait \rightarrow Key Disclosure \rightarrow Verify

Proposed Method: Nav Msg \rightarrow Hash + Pell Authentication \rightarrow Immediate Verify

The OSNMA authentication process requires the reception of the navigation message followed by a waiting period for delayed key disclosure before verification can be performed, resulting in unavoidable authentication latency. In contrast, the proposed method enables immediate verification of the navigation message by combining cryptographic hash functions with Pell-based authentication, thereby removing key disclosure dependency and significantly reducing both time delay and computational overhead.



Weather satellites use multi-channel imagers and a 19-channel sounder to scan the Earth and atmosphere at resolutions ranging from 1 km to 10 km. The captured images (M_1, M_2, \dots) are digitally signed as (u_i, k_i, s_i) . Global domain parameters are transmitted first, followed by the digital signatures, which are relayed to the Earth station.



After receiving the signatures from the satellites, the Earth station verifies the validity of the signatures using the previously received global domain parameters and public key.

FIG. 5. The process of authenticating satellite signals.

TABLE 9. Security, Performance, and Robustness Comparison between Fernández-Hernández OSNMA and the Proposed Method

Parameter	Fernández-Hernández OSNMA	Proposed Method
Authentication Framework	TESLA-based delayed key disclosure scheme for Galileo Open Service.	Hybrid continuous authentication using Pell curve cryptography and SHA3-512.
Cryptographic Primitives	ECDSA for root key authentication; TESLA MACs for navigation messages.	Pell-curve-based public key structure with embedded MACs for continuous verification.
Hash Function	SHA-224 (selected due to Galileo message size constraints).	SHA3-512 (longer digest length; stronger collision resistance).
Authentication Latency	Delayed authentication due to TESLA key disclosure window.	Near-real-time authentication with continuous verification.
Security Against Spoofing	Strong forward security, but vulnerable during disclosure interval.	Very high resistance; no disclosure window and higher cryptographic entropy.
Security Against Replay	Protected via TESLA timing constraints.	Inherently resistant due to continuous message binding and hashing.
Computational Overhead	Moderate to high (ECDSA verification + TESLA processing).	Low to moderate (lightweight Pell arithmetic + hash operations).
Bandwidth Overhead	Very low; optimized to fit Galileo I/NAV reserved bits.	Low; authentication data embedded efficiently per message block.
Robustness to Packet Loss	Sensitive to message loss during key disclosure.	High robustness; continuous authentication tolerates intermittent losses.
Velocity and Doppler Sensitivity	Performance degrades in high-dynamic environments (e.g., LEO).	Velocity-independent; suitable for high-dynamic satellite motion.
Orbit Compatibility	Primarily optimized for MEO Galileo constellation.	Applicable to LEO, MEO, and GEO constellations.
Scalability	Bound to Galileo OSNMA infrastructure and timing constraints.	Scalable across heterogeneous multi-orbit satellite systems.
Satellite Resource Impact	Higher memory and processing requirements.	Reduced onboard computation and memory usage.
Practical Deployability	Operationally proven in Galileo OSNMA.	Suitable for next-generation multi-orbit satellite authentication.
Overall Balance (Security - Efficiency - Practicality)	Well-balanced for MEO civilian navigation use cases.	Better overall balance for high-security, dynamic, and multi-orbit scenarios.

3.4. Comparison between Proposed method and Fernandez-Hernandez method. The Table 9 provides a detailed comparison between the Fernández-Hernández OSNMA scheme and the proposed authentication method with respect to security, performance, and robustness in satellite navigation systems.

The Fernández-Hernández OSNMA approach is based on a TESLA-style delayed key disclosure mechanism combined with ECDSA and the SHA-224 hash function, which offers proven security for the Galileo Open Service in MEO constellations but introduces inherent authentication latency and temporary vulnerability during the key disclosure window, particularly under high-dynamic conditions or packet loss. In contrast, the proposed method employs a hybrid continuous authentication framework using Pell curve cryptography and the SHA3-512 hash function, enabling near-real-time authentication without delayed disclosure. This design significantly enhances resistance to spoofing and replay attacks, improves robustness against intermittent message loss, and reduces dependency on satellite velocity and orbital dynamics. Furthermore, the proposed method demonstrates lower computational and memory overhead on satellite resources while remaining scalable across LEO, MEO, and GEO constellations, making it more suitable for next-generation multi-orbit and high-security GNSS authentication scenarios.

Table 10 summarizes the qualitative-to-quantitative mapping used for radar, scatter, and bubble plot visualizations, ensuring transparent and reproducible comparison between OSNMA and the proposed method.

TABLE 10. Side-by-Side Radar Value Assignment for Fernández-Hernández OSNMA and the Proposed GNSS Authentication Method

Axis	Fernández-Hernández OSNMA		Proposed Method	
	Justification	Value	Justification	Value
Security Strength	Strong spoofing and replay protection using TESLA-based delayed authentication and ECDSA root key verification.	1.2	Higher cryptographic entropy with continuous authentication and no key disclosure window.	1.2
Authentication Latency	Delayed authentication caused by TESLA key disclosure intervals.	0.4	Near-real-time verification enabled by continuous authentication.	1.2
Computational Efficiency	Moderate to high processing cost due to ECDSA verification and TESLA operations.	0.8	Lightweight Pell-curve arithmetic combined with hash-based verification.	1.2
Bandwidth Efficiency	Very low overhead optimized to fit within Galileo I/NAV reserved bits.	1.2	Low overhead through efficient embedding of authentication data per message block.	0.8
Robustness	Sensitive to packet loss during key disclosure and degraded performance in high-dynamic environments.	0.8	High tolerance to packet loss and independence from velocity and Doppler effects.	1.2
Deployability & Scalability	Operationally proven within Galileo OSNMA but constrained to MEO and system-specific infrastructure.	0.8	Scalable across LEO, MEO, and GEO constellations for next-generation GNSS.	1.2

The radar chart shown in Fig. 6 presents a qualitative comparison between the Fernández-Hernández OSNMA scheme and the proposed authentication method across six evaluation dimensions: security, authentication latency, computational efficiency, bandwidth efficiency, robustness, and deployability. Each axis of the radar plot corresponds to one performance metric, enabling a visual comparison of the relative strengths and limitations of the two approaches. The plotted values are assigned using a normalized qualitative scale, where 0.2 indicates a feature that is not applicable or supported only through analytical assumptions, 0.4 denotes low performance, 0.8 represents medium performance, and 1.2 corresponds to high performance. Larger radial values indicate better capability in the respective dimension, allowing the radar chart to clearly highlight trade-offs and demonstrate the improved overall balance achieved by the proposed method.

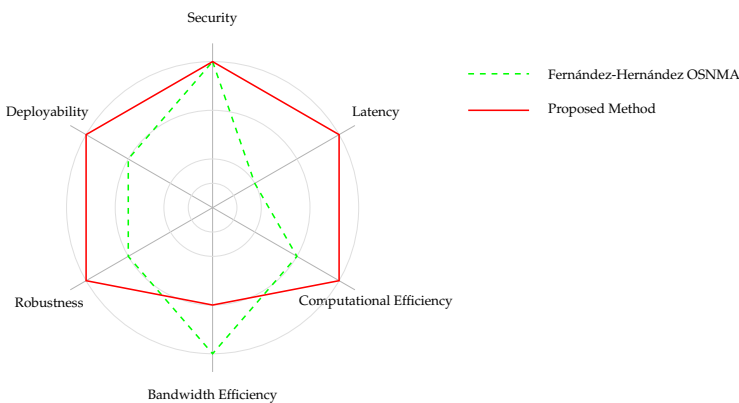


FIG. 6. Radar comparison between Fernández-Hernández OSNMA and the proposed authentication method.

The bubble plot shown in Fig. 7 illustrates a comparative analysis of the Fernández–Hernández OSNMA scheme and the proposed GNSS authentication method in terms of security, authentication latency, and robustness. The horizontal axis represents authentication latency, where higher values indicate lower effective delay and faster authentication, while the vertical axis denotes the achieved security level. Robustness is encoded by the size of each bubble, with larger bubbles corresponding to higher tolerance to packet loss, high-dynamic environments, and adverse operating conditions. All values are assigned using a normalized qualitative scale, where 0.2 denotes features that are not applicable or supported only analytically, 0.4 represents low capability, 0.8 indicates medium capability, and 1.2 corresponds to high capability. This visualization highlights the trade-offs between the two approaches and emphasizes the superior balance achieved by the proposed method across the evaluated dimensions.

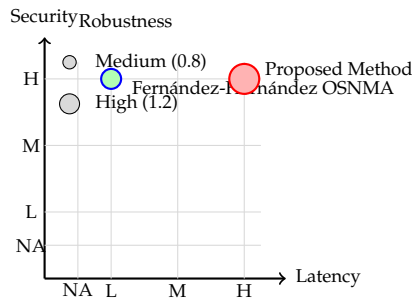


FIG. 7. Security–latency–robustness bubble plot comparing Fernández–Hernández OSNMA and the proposed GNSS authentication method.

The proposed method occupies the upper-right region of the security–latency plane while exhibiting a larger robustness bubble, indicating simultaneous improvements in security strength, authentication timeliness, and resilience to packet loss compared to OSNMA.

The Fernández-Hernández OSNMA method relies on elliptic curve cryptography combined with the SHA-224 hashing algorithm, primarily to meet the strict bandwidth constraints of Galileo navigation messages. While this design choice ensures compatibility with legacy GNSS infrastructures, the reduced hash length and delayed authentication mechanism introduce limitations in terms of cryptographic strength and real-time security assurance.

In contrast, the proposed method employs Pell curve cryptography together with the SHA3-512 hashing algorithm. Although both elliptic curves and Pell curves are defined over finite fields with a comparable number of group elements asymptotically proportional to p , the computational structure of Pell curves enables more lightweight arithmetic operations. This characteristic reduces computational complexity during key generation and verification while maintaining equivalent algebraic hardness assumptions.

From a security standpoint, the use of SHA3-512 significantly increases resistance to collision, preimage, and second-preimage attacks when compared to SHA-224. The larger digest size and sponge-based construction of SHA-3 provide stronger security margins, which are particularly important in long-term satellite deployments exposed to evolving cryptanalytic and quantum-assisted attack models.

Moreover, unlike TESLA-based authentication schemes, the proposed approach eliminates the delayed key disclosure window, thereby removing a known vulnerability period during which spoofing attacks can be mounted. Continuous authentication ensures immediate verification of navigation messages, enhancing robustness against replay and impersonation attacks under high-dynamic satellite conditions.

Consequently, while both elliptic curve-based and Pell curve-based approaches offer similar theoretical group sizes, the proposed method achieves a more favorable balance between computational efficiency and cryptographic strength. This balance results in improved security, reduced authentication latency, and greater robustness, as summarized in **Table 5** and **Table 9**. These characteristics make the proposed method more suitable for next-generation multi-orbit satellite authentication systems.

4. RESULTS AND DISCUSSION

This study presents a digital signature-based authentication framework built on Pell curve cryptography combined with cyclotomic polynomials for securing satellite communication signals. The proposed method is designed to support a large-scale satellite environment, including approximately 7,560 operational satellites, of which 114 belong to GNSS constellations. Unlike conventional GNSS authentication mechanisms that rely on delayed verification or fixed orbital assumptions, the proposed approach enables continuous authentication under diverse satellite dynamics.

Existing GNSS authentication schemes face practical challenges due to variable satellite velocities, Doppler shifts, atmospheric disturbances, and strict bandwidth constraints. These factors limit their effectiveness in high-dynamic or multi-orbit environments. The proposed method addresses these limitations by eliminating dependence on delayed key disclosure and enabling real-time authentication, thereby improving signal trustworthiness across LEO, MEO, and GEO constellations.

From a security perspective, the proposed scheme guarantees essential cryptographic properties, including authenticity, integrity, non-repudiation, and selective unforgeability. The use of Pell curve-based public key operations and SHA3-512 hashing significantly increases cryptographic entropy, strengthening resistance against spoofing, replay, and impersonation attacks. Unlike TESLA-based approaches, the proposed method does not expose a vulnerability window during key disclosure, which is particularly critical in adversarial satellite environments.

Performance evaluation indicates that the proposed method achieves strong security guarantees while maintaining computational efficiency. Pell curve arithmetic requires fewer resources than conventional elliptic-curve-based digital signature verification, making the scheme suitable for resource-constrained onboard satellite processors. Additionally, the continuous authentication mechanism reduces authentication latency, enabling near-real-time verification without imposing excessive bandwidth overhead.

Robustness analysis further demonstrates the effectiveness of the proposed approach under realistic satellite conditions. Continuous authentication improves tolerance to packet loss and signal interruption, which are common in space communication channels. Furthermore, the velocity-independent design ensures stable performance even in high-dynamic scenarios, such as LEO satellite motion, where Doppler effects and rapid topology changes challenge traditional GNSS authentication methods.

Overall, the comparative results indicate that while existing OSNMA-based solutions offer a practical balance for civilian MEO GNSS applications, the proposed method provides a superior balance between security, efficiency, and practicality for next-generation satellite systems. Its adaptability to multi-orbit architectures, reduced authentication latency, and enhanced robustness make it particularly suitable for emerging satellite-based navigation, communication, and forecasting applications.

5. SECURITY ANALYSIS

5.1. Total Break. Total break is impossible in this algorithm since the proposed algorithm is based on a discrete logarithm over the Pell curve. Consider the elliptic curve $E_{a,b}(F_p)$. Let Ω be a point obtained by multiplying base point Υ by a scalar k , where $1 \leq k \leq (|E_{a,b}(F_p)| - 1)$, i.e., $\Omega = k\Upsilon$. Determining the value k is very difficult known as ECDLP [40].

In the context of elliptic curves, let us consider a Pell curve denoted as $P(N, k^2)$ defined over a finite field F_p . Suppose we have a point Υ belonging to the set $P_{N,k^2}(F_p)$, which has an order of m' . Additionally, let Ω be a point obtained by multiplying base point Υ by a scalar k , where $1 \leq k \leq (m' - 1)$. i.e. $\Omega = k\Upsilon$. The task involves determining the value of k , known as PCDLP, which is challenging to find in Pell curves like elliptic curves.

The spy satellite is aware of the public key Ω and base point Υ , and it tries to find the secret key $\phi_n(d)$, but it is based on PCDLP. Therefore total break is not possible.

5.2. Brute Force Attack. Given that n is much less than m' , the key space may be expressed as the product of $(\pi(n) - \text{no. of prime divisors of } n)$ and d , where $\pi(n)$ represents the prime-counting function. If n is more than or equal to m' , then the key space is equal to $m' - 1$. If the field size p exceeds 112 bits, finding k_{pr} by spy satellite is beyond the current computational limit, making brute-force attacks unattainable.

5.3. Key-Only Attack. The spy satellite has knowledge of public key Ω and base point Υ , which is scalar multiplication by k_{pr} . The satellite uses the inverse operation of Υ , suggesting inverse is Ω , but this is false, preventing access to confidential key $\phi_n(d)$. As a result, the key-only attack is not feasible.

5.4. Valid Signature Attack. The spy satellite is aware of the message M_i , as well as the signatures u_i , k_i , and s_i . (i) It uses C' instead of C to calculate d from C , however it is based on DLP. (ii) The secrecy of q implies that determining d given s falls within DLP. This means that the attack using a valid signature is impossible.

5.5. Direct Chosen Message Attack. The spy satellite uses the public key Ω to acquire signatures on messages and replaces the original message with a new one, leaving the original signature intact, but this approach cannot be achievable due to the hash function. Therefore, the direct chosen message attack is impossible.

5.6. Known Message Attack. The spy satellite is aware of the signatures u_i , k_i , and s_i as well as the messages collection M_i . Determining the value of d_i based on C_i (after designating C' as C) or s_i falls within the scope of DLP. Therefore, the known messaging attack is unfeasible.

5.7. Total Break. The spy satellite is aware of the public key Ω and base point Υ , and it tries to find the secret key $\phi_n(d)$, but it is based on PCDLP. Therefore total break is not possible.

5.8. Selective Unforgeability. The spy satellite chooses a message M' and determines the appropriate signature (u', k', s', M') using randomly picked ρ, q, d , and r , then broadcasts these to the Earth station. The Earth Station computes v using the previously sent original public key containing the secret parameter d . In this case, the Earth station discovers $v \neq u'$ and decides that malicious behaviour happened during transmission. As a result, selective forgery is not conceivable.

Let's say the spy satellite forges a public key as well. After then, the Earth station determines that the signature is genuine by computing $v = u'$. Selective forgery is thus feasible. By using the time data of satellite passes over the Earth's horizon, we can defeat this fraud.

5.9. Existential Unforgeability. If (u, s) in ECDSA is a legitimate signature for a particular message, then spy satellites will calculate $(u, s - m')$, which is also a legitimate signature for the same message as well, means existential forgery is possible. However, by using the inverse of the signature (s^{-1}) in the verification, this suggested technique ensures that if (u, k, s) represents a valid signature for a particular message, then $(u, k, s - m')$ cannot be a valid signature for the same message. It is thus impossible to commit existential forgery.

6. CONCLUSION

The summary provides an overview of Global Navigation Satellite Systems (GNSS), including military budget allocation over a five-year timeframe, satellite frequency bands and their corresponding uses, and the total number of satellites currently in Earth's orbit. A digital signature algorithm using a Pell curve and cyclotomic polynomials has been developed. This algorithm was effectively integrated into satellite navigation signal, which comprise satellite location, and signal arrival time. The proposed algorithm classifies accurate signals as authenticated and other signals will be filtered. Also the proposed algorithm was proved better after a comparison with the Fernandez-Hernandez method using many security attacks. In consequence, the signal communicated by the satellites to the Earth station are more secure in terms of data integrity, authentication, and confidentiality using PCDSA.

AUTHOR CONTRIBUTIONS

Conceptualization, E.R.; methodology, E.R. and G.S.G.N.A.; writing original draft preparation, E.R.; writing reviews and editing, E.R. and G.S.G.N.A.; supervision, G.S.G.N.A.; All authors have read and agreed to the published version of the manuscript.

DATA AVAILABILITY STATEMENT

Not applicable.

ACKNOWLEDGMENTS

We express our gratitude to the Vellore Institute of Technology, Vellore - 632014, for their support of this research.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

- [1] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, 2011, pp. 75–86.
- [2] Wesson, Kyle, Mark Rothlisberger, and Todd Humphreys. "Practical cryptographic civil GPS signal authentication." *NAVIGATION: Journal of the Institute of Navigation* 59.3 (2012): 177-193.
- [3] Yuan, Muzi, Xiaomei Tang, and Gang Ou. "Authenticating GNSS civilian signals: A survey." *Satellite Navigation* 4.1 (2023): 1-18.
- [4] Chen, Xiao, et al. "Satellite Navigation Signal Authentication in GNSS: A Survey on Technology Evolution, Status, and Perspective for BDS." *Remote Sensing* 15.5 (2023): 1462.
- [5] Li, Ping, et al. "A Design of Navigation Enhancement Signal Based on Communication Satellite Signal." *China Satellite Navigation Conference*. Singapore: Springer Nature Singapore, 2023.
- [6] Chen, Chien-Yuan. "Fast RSA-type Schemes Based on Pell. Equations over Z_N ." (1996).
- [7] Padhye, Sahadeo. "A public key cryptosystem based on Pell equation." *Cryptology ePrint Archive* (2006).
- [8] I. Fernández-Hernández, G. Seco-Granados, J. A. López-Salcedo, and G. L. Basilio, "A navigation message authentication proposal for the Galileo open service," *NAVIGATION: Journal of the Institute of Navigation*, vol. 63, no. 1, pp. 85–102, 2016.
- [9] J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O'Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," in *Proc. 30th Int. Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, Portland, OR, USA, Sep. 2017, pp. 2388–2416.
- [10] G. Caparra, S. Sturaro, N. Laurenti, and C. Wullems, "Evaluating the security of one-way key chains in TESLA-based GNSS navigation message authentication schemes," in *Proc. International Technical Meeting of The Satellite Division of The Institute of Navigation (ION GNSS+)*, 2016.
- [11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [12] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.
- [13] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B. Yang, "High-speed high-security signatures," *Journal of Cryptographic Engineering*, vol. 2, no. 2, pp. 77–89, 2012.
- [14] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology – EUROCRYPT 2003*, Lecture Notes in Computer Science, vol. 2656, Springer, 2003, pp. 416–432.
- [15] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, no. 1, pp. 238–268.
- [16] Hughes, Richard J., et al. "Quantum cryptography for secure satellite communications." 2000 IEEE Aerospace Conference. Proceedings (Cat. No. 00TH8484). Vol. 1. IEEE, 2000.
- [17] Rarity, John G., et al. "Ground to satellite secure key exchange using quantum cryptography." *New Journal of Physics* 4.1 (2002): 82.
- [18] Wullems, Christian, Oscar Pozzobon, and Kurt Kubik. "Signal authentication and integrity schemes for next generation global navigation satellite systems." *European navigation conference (ENC-GNSS 2005)*. 2005.
- [19] Wesson, Kyle, Mark Rothlisberger, and Todd Humphreys. "Practical cryptographic civil GPS signal authentication." *NAVIGATION: Journal of the Institute of Navigation* 59.3 (2012): 177-193.
- [20] Madry, Scott. *Global Navigation Satellite Systems and Their Applications*. Springer New York, 2015. DOI.org (Crossref), <https://doi.org/10.1007/978-1-4939-2608-4>.
- [21] Enge, Per K. "Authentication based on random bits in satellite navigation messages." U.S. Patent No. 8,930,556. 6 Jan. 2015.
- [22] Fernández-Hernández, Ignacio, et al. "A navigation message authentication proposal for the Galileo open service." *NAVIGATION: Journal of the Institute of Navigation* 63.1 (2016): 85-102.
- [23] Bedington, Robert, Juan Miguel Arrazola, and Alexander Ling. "Progress in satellite quantum key distribution." *npj Quantum Information* 3.1 (2017): 30.
- [24] Jackson, Samuel, Jeremy Straub, and Scott Kerlin. "Exploring a Novel Cryptographic Solution for Securing Small Satellite Communications." *Int. J. Netw. Secur.* 20.5 (2018): 988-997.
- [25] Yang, Yuanxi, et al. "Introduction to BeiDou-3 Navigation Satellite System." *Navigation*, vol. 66, no. 1, Jan. 2019, pp. 7–18. DOI.org (Crossref), <https://doi.org/10.1002/navi.291>.
- [26] Rose, T. S., et al. "Optical communications downlink from a low-earth orbiting 1.5 U CubeSat." *Optics express* 27.17 (2019): 24382-24392.

- [27] Wu, Zhijun, et al. "TESLA-based authentication for BeiDou civil navigation message." *China Communications* 17.11 (2020): 194-218.
- [28] Serra, Paul, et al. "Optical front-end for a quantum key distribution cubesat." *International Conference on Space Optics - ICSO 2020*. Vol. 11852. SPIE, 2021.
- [29] Caldwell, Sonja. "9.0 Communications." NASA, 16 Oct. 2021, <http://www.nasa.gov/smallsat-institute/sst-soa/communications>.
- [30] Komatsu, Hiromitsu, et al. "The pointing performance of the optical communication terminal, SOLISS in the experimentation of bidirectional laser communication with an optical ground station." *Free-Space Laser Communications XXXIII*. Vol. 11678. SPIE, 2021.
- [31] Tedeschi, Pietro, Savio Sciancalepore, and Roberto Di Pietro. "Satellite-based communications security: A survey of threats, solutions, and research challenges." *Computer Networks* 216 (2022): 109246.
- [32] Mishra, Mukesh Kumar, and Priyanka Ahlawat. "Authentication and Key Update in Satellite Communication." *Proceedings of 3rd International Conference on Machine Learning, Advances in Computing, Renewable Energy and Communication: MARC 2021*. Singapore: Springer Nature Singapore, 2022.
- [33] Wesson, K. D., Humphreys, T. E., and Shepard, D. P., "Open-Source GPS Receiver Implementations for Navigation Message Authentication Research," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012)*, Nashville, TN, USA, Institute of Navigation, 2012, pp. 2332–2343.
- [34] Caparra, G., Sturaro, S., and Laurenti, N., "A Survey on Navigation Message Authentication for Global Navigation Satellite Systems," in *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS 2016)*, Savannah, GA, USA, IEEE, 2016, pp. 969–977.
- [35] Belton, Valerie, and Theodor Stewart. *Multiple criteria decision analysis: an integrated approach*. Springer Science & Business Media, 2012.
- [36] Ishizaka, Alessio, and Philippe Nemery. *Multi-criteria decision analysis: methods and software*. John Wiley & Sons, 2013.
- [37] Fernandez-Hernandez, Ignacio. "Digitally-signed satellite radio-navigation signals." U.S. Patent No. 9,952,325. 24 Apr. 2018.
- [38] Elumalai R, Anjaneyulu G.S.G.N, An Efficient Practical Alternative to ECC, Pell Curve Cryptography (PCC) : A New Vision, *cryptologia*, 01 Mar. 2025.
- [39] Porter, Brett. "Cyclotomic polynomials." (2015).
- [40] Silverman, Joseph H., and Joe Suzuki. "Elliptic curve discrete logarithms and the index calculus." *International Conference on the Theory and Application of Cryptology and Information Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998.

¹ RESEARCH SCHOLAR, DEPARTMENT OF MATHEMATICS, SAS, VELLORE INSTITUTE OF TECHNOLOGY, VELLORE, INDIA

Email address: elumalai.r2019@vitstudent.ac.in

² PROFESSOR, DEPARTMENT OF MATHEMATICS, SAS, VELLORE INSTITUTE OF TECHNOLOGY, VELLORE, INDIA

Email address: anjaneyulu.gsgn@vit.ac.in