ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering | e–ISSN: 2067 – 3809
Tome XVII [2024] | Fascicule 1 [January – March]

[1.]Ştefan ȚĂLU

# CRYPTOGRAPHY TECHNIQUES FOR SATELLITE–BASED COMMUNICATIONS: CHALLENGES, POTENTIAL SOLUTIONS, AND FUTURE TRENDS

[1.] Technical University of Cluj–Napoca, The Directorate of Research, Development and Innovation Management (DMCDI), Cluj–Napoca, ROMANIA

**Abstract:** Satellite–based communication (SATCOM) systems are experiencing renewed momentum in both industry and academia evolving to meet the demands of a rapidly changing world. They are essential for achieving global connectivity goals, advancing research and innovation, and providing critical services in public, commercial, economic, military, and scientific domains. Significant improvements in SATCOM systems were obtained through the combination of new manufacturing processes and radio technologies that have the potential to reduce costs, enhance performance, expand coverage, and enable a wide range of applications, making satellite–based communication an important component of global connectivity solutions. Updating and enhancing cybersecurity measures for SATCOM systems is essential to protect against evolving cyber threats and ensure the reliability and security of critical communication infrastructure through a proactive, multi–layered approach that combines technology, processes, and collaboration across the industry and government sectors. To address these challenges, SATCOM operators should strike a balance between business objectives and security requirements. This study presents a comprehensive analysis on cryptography techniques that are operating in SATCOM systems. Additionally, by outlining challenges, potential solutions, and future research issues, this approach encourages ongoing investigation and development in the field of SATCOM security to address these challenges through innovative solutions and collaborative efforts to secure SATCOM systems effectively.
**Keywords:** cryptography techniques, satellite–based communication, satellites cybersecurity

## INTRODUCTION

Over the past five decades, SATCOM technology has undergone a remarkable evolution, serving as a cornerstone in global telecommunication systems. This evolution has been characterized by advancements that encompass higher bandwidth, improved reliability, and expanded capabilities. Consequently, SATCOM systems are poised to maintain their pivotal role in facilitating global connectivity and supporting a diverse array of applications across various fields and sectors in the foreseeable future [1–6]. In sectors such as telecommunications, aviation, maritime, military, and defence, SATCOM technology remains indispensable, providing critical communication infrastructure and enabling mission–critical operations. Moreover, SATCOM plays a vital role in enhancing efficiency and safety in industries like agriculture, emergency services, oil and gas, mining, environmental monitoring, logistics and transportation, healthcare, and space exploration. In addition to these essential sectors, SATCOM technology finds application in a wide range of other domains.

For instance, in meteorology, broadcasting, entertainment, and the internet of things (IoT), SATCOM facilitates real–time data transmission and connectivity. Furthermore, it supports scientific research endeavours across disciplines and plays a crucial role in educational initiatives, ensuring access to remote learning resources and educational content worldwide. As technology continues to advance, SATCOM systems will likely further diversify their applications and capabilities, contributing to the advancement and innovation across various sectors and enabling connectivity and communication in even the most remote and challenging environments.

The tech companies in satellite–based systems like SpaceX (project Low Earth Orbit (LEO) Satellite Constellation), Facebook (now Meta Platforms, Inc.) (project Athena), Amazon (project Kuiper), UK–based OneWeb, Telesat, and GW (a Chinese state–owned company) rekindled interest in the possibilities and potential of satellite technology in various industries and applications [7]. As these tech companies continue to invest in satellite technology and infrastructure, they are poised to drive innovation, expand market opportunities, and shape the future of global telecommunications. With their combined expertise and resources, they are not only rekindling interest in satellite technology but also paving the way for a new era of connectivity and exploration, where the boundaries of possibility are continually pushed and the benefits of satellite technology are realized on a global scale.

As SATCOMs continue to evolve, they are poised to become essential facilitators for the next

generation of telecommunications networks, including 6G. These systems will play a pivotal role in shaping the future of connectivity on a global scale, offering unprecedented levels of bandwidth, coverage, and reliability [8]. The projected growth of the SATCOM market, with an anticipated value of USD 41,860 million by 2025 and a Compound Annual Growth Rate (CAGR) of 8.40%, underscores the robust expansion potential and escalating importance of satellite communication technology [9].

This exponential growth trajectory reflects increasing demand for satellite–based services across diverse sectors and industries, driven by the need for ubiquitous connectivity, resilient communication infrastructure, and advanced data transmission capabilities.

SATCOMs are uniquely positioned to address these requirements, offering scalable and flexible solutions that can extend connectivity to remote and underserved regions, support critical applications in areas such as emergency response and disaster recovery, and enable seamless integration with emerging technologies such as Internet of Things (IoT) and autonomous systems.

Moreover, as the global telecommunications landscape continues to evolve, SATCOMs will play a crucial role in bridging connectivity gaps, enabling digital inclusion, and fostering innovation across various domains. Their ability to deliver high–speed, low–latency communication services, coupled with advancements in satellite technology and network optimization techniques, positions SATCOMs as indispensable components of future telecommunications ecosystems.

The classification of satellites' orbits hinges on several fundamental characteristics, including their shape (whether circular or elliptical), altitude (whether they orbit in Low–Earth, Medium–Earth, or Geostationary orbits), travel direction (whether clockwise or counter clockwise), and inclination to the plane of the Earth's equator [4].

These parameters collectively define the specific trajectory and spatial orientation of a satellite as it orbits the Earth, each contributing to its unique operational characteristics and capabilities. Understanding these orbit classifications is crucial for designing and deploying satellites tailored to specific applications and operational requirements, ranging from global telecommunications and navigation to earth observation and scientific research.

There are three primary categories of satellite networks based on their orbits: Geosynchronous equatorial orbit (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO). Each type of satellite network has its advantages and trade–offs, and the choice of orbit depends on the specific requirements of the applications they serve. Satellites in GEO orbit at an altitude of approximately 35,786 km above the Earth's equator have the same rotational speed as the Earth (making them appear stationary relative to the Earth's surface) by offering continuous coverage but have a higher latency. Satellites in MEO operate at altitudes ranging from approximately 2,000 km to 35,786 km above the Earth's surface, being positioned at intermediate altitudes between LEO and GEO satellites, and provide a balance between coverage and signal latency. Satellites in LEO orbit at altitudes ranging from approximately 180 km to 2,000 km above the Earth's surface, have much shorter orbital periods (typically 90 to 120 minutes), and offer low–latency communication but require a larger number of satellites to achieve global coverage [10].

By segregating frequency bands for uplink and downlink channels and enforcing these allocations through regulatory bodies such as the Federal Communications Commission (FCC) and the International Telecommunications Union (ITU), satellite communication systems can operate efficiently while minimizing harmful interference to other systems sharing the same frequency spectrum. This regulatory framework ensures the reliability and integrity of SATCOM services across diverse applications, ranging from broadcasting and internet access to military communications [4].

The allocation of distinct frequency bands for uplink and downlink channels enables SATCOM systems to manage data transmission in a structured and organized manner. By assigning specific frequency ranges to each direction of communication, satellites can effectively differentiate between incoming and outgoing signals, facilitating seamless data exchange without signal degradation or cross–channel interference.

Moreover, regulatory oversight from bodies like the FCC and ITU ensures compliance with international standards and guidelines, fostering interoperability and harmonization among satellite communication systems worldwide. This regulatory framework plays a critical role in safeguarding the integrity of SATCOM services,

particularly in scenarios where multiple satellite operators and users coexist within the same frequency spectrum. By establishing clear rules and procedures for frequency allocation, coordination, and interference mitigation, regulatory bodies mitigate the risk of signal congestion, spectrum pollution, and service degradation, thereby preserving the quality and reliability of satellite communication services for end–users.

The traditional SATCOM communication architecture is a complex system that involves the space segment (satellites and inter–satellite links), the ground segment (ground stations, gateways, and network infrastructure), and the user segment (end–user terminals). Each segment serves a specific purpose in facilitating communication between different points in the satellite network, enabling various services and applications [4].

While satellite communication systems offer numerous advantages and promising applications, they also introduce new cyber security challenges and potential vulnerabilities, that hackers and cybercriminals can exploit [11–14]. All segments of a SATCOM system are potential targets for attacks, and vulnerabilities can exist at various points in the communication architecture.

Attacks on satellite communication networks can be classified into several categories based on their nature, objectives, and impact. A detailed classification of these attacks is as follows:

— Electronic attacks (jamming: interference with satellite signals by broadcasting powerful signals on the same frequency, disrupting communication; spoofing: transmitting fake signals to deceive satellite receivers, potentially leading to incorrect navigation, timing, or data; interception (eavesdropping): passive attacks involving the capture and monitoring of satellite signals to access sensitive information).
— Cyber–attacks (malware and malicious software: introducing malware into satellite systems to compromise their functionality or steal data; phishing and social engineering: targeting personnel with deceptive emails or tactics to gain unauthorized access to critical systems or information; unauthorized access: illegally gaining access to satellite control systems, ground stations, or user terminals; data tampering: altering or manipulating data transmitted by satellites to provide false information or cause specific actions; denial of service (Cyber DoS): overwhelming satellite network infrastructure with excessive traffic or cyberattacks, rendering it unavailable for legitimate users; insider threats: compromising security from within by individuals with authorized access to satellite systems and data; supply chain attacks: targeting the supply chain of satellite components or software to introduce vulnerabilities during production or distribution).
— Physical attacks (anti–satellite weapons: launching physical attacks against satellites in orbit, potentially causing damage or destruction; ground station attacks: physically targeting ground stations or gateway facilities, disrupting communication or satellite operations; space debris and collisions: collisions with space debris or other objects in orbit can damage or disable satellites).
— Frequency interference (frequency jamming: disrupting communication by jamming satellite signals with electromagnetic interference; frequency interception: intercepting and decoding sensitive information transmitted over satellite frequencies).
— Orbital attacks (orbital manoeuvres: unauthorized changes in a satellite's orbital path, potentially disrupting its operation; satellite hijacking: gaining control of a satellite and manipulating its movements or functions).
— Regulatory and policy–related attacks (spectrum management issues: regulatory or policy–related challenges affecting satellite communication quality and security; coordination challenges: difficulties in coordinating satellite communication security across international boundaries and jurisdictions) [4, 10].

Mitigating cyber security challenges within SATCOM systems necessitates a multifaceted strategy that encompasses a range of approaches, including electronic warfare countermeasures, cyber security protocols, physical security measures, and adherence to regulatory and policy standards [11–14]. Encryption, founded on modern cryptographic techniques, stands as a fundamental pillar of SATCOM security, playing a pivotal role in fortifying the confidentiality, integrity, and availability of data traversing satellite links [15–18]. However, encrypting data within satellite environments presents unique hurdles and

complexities, underscoring the need for ongoing research and development efforts [19–22].

These endeavours strive to address the intricacies of securing data transmitted to and from satellites amid the challenges posed by the space environment, ensuring robust protection and integrity throughout the communication process. By combining encryption with a comprehensive cyber security framework, SATCOM systems can effectively bolster their defences against evolving threats and uphold the integrity of critical communications in space–based operations.

## REVIEW METHODLOGY

The review methodology is structured around three fundamental steps:

- Collating relevant articles of the research;
- Examining literature review articles to evaluate, recognize, and grasp the findings;
- Performing a systematic review by systematically examining and synthesizing research findings methodically.

Throughout these steps, database searches are conducted using prominent online resources such as academic databases, digital libraries, and specialized research repositories. These searches are guided by specific keywords, terms, and criteria relevant to the research topic, ensuring the identification of relevant studies while minimizing the risk of bias or omission.

## KEY CRYPTOGRAPHY TECHNIQUES COMMONLY EMPLOYED IN SATCOM

Cryptography plays a crucial role in securing communication over satellite links, and there are various contributions and approaches in this area. Many contributions in this field primarily concentrate on ensuring the authenticity (verification of the sender's identity) and confidentiality (protecting the content of the communication) in SATCOM systems.

Some of the research work in SATCOM security involves adapting security primitives and techniques that were originally developed for other domains, such as computer networks or the internet. Part of the research in this area focuses on modifying the implementation and network architecture of well–known cryptographic solutions to suit the unique characteristics and requirements of SATCOM scenarios.

Another aspect of research involves exploring novel paradigms, such as quantum computing, while another part of research deals with security service.

### A. Authentication

Many authentication protocols have been proposed and discussed in the literature in function of the specific security requirements, the technology stack in use, and the threat model of the system or application. There are various classification methods relative to the scientific contributions in the field of SATCOM authentication across multiple criteria, including communication architecture, cryptographic technique, security properties, security analysis, and assessment methodology, facilitating a comprehensive assessment of their strengths and suitability for different scenarios [4].

Many research address the protection of the Global Positioning System/Global Navigation Satellite System communication link. However, it's worth noting that other links within SATCOM systems are rarely studied in these works [23–25].

Various methods and protocols can be employed for key sharing in SATCOM systems. The choice of key sharing technique in a SATCOM system will depend on factors such as the security requirements, the number of entities involved, the available resources, and the specific characteristics of the communication network. Additionally, a combination of these techniques may be used to achieve a higher level of security and flexibility in key management for SATCOM systems.

Elliptic Curve Cryptography (ECC) is a public key encryption method (asymmetric encryption) for SATCOM systems, introduced independently in 1985, by Victor S. Miller [26] and Neal Koblitz [27]. ECC is based on the algebraic structures of the elliptic curves over finite fields and on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) [16, 22, 28], that is known for its ability to provide strong security with smaller key sizes compared to other encryption techniques, such as RSA (Rivest–Shamir–Adleman, first publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, researchers at the Massachusetts Institute of Technology, USA) or DSA (Digital Signature Algorithm), thereby consuming less resource and ameliorating performance on the systems.

ECC certificates offer several advantages in terms of resource efficiency, which can have a significant impact on network performance, particularly for high–volume or high–traffic websites. ECC algorithms can use different underlying elliptic curves in a simplified form (the reduced/short Weierstrass normal form), and the choice of the curve significantly impacts the

cryptographic strength, performance, key length, and even the underlying algorithms used [29]. An elliptic curve group can provide the same level of security as RSA–based systems with a much larger modulus and correspondingly larger key. For example, a 256–bit ECC key is equivalent to a 3072–bit RSA key and a 384–bit ECC key is equivalent to a 7680–bit RSA key [30].

Certain cryptographic proposals, particularly those based on symmetric key cryptography, operate under the assumption of a pre–shared key (PSK), which is established and familiar to the communicating entities beforehand. In these schemes, the identical key serves the dual purpose of encryption and decryption [31, 32].

This approach offers notable advantages in terms of speed and efficiency in secure communication, as the symmetric encryption and decryption processes are computationally less demanding compared to their asymmetric counterparts. However, the security of such systems heavily relies on meticulous key management practices [33].

Proper safeguards must be implemented to protect the pre–shared keys from unauthorized access or compromise, as any breach in key security could potentially compromise the confidentiality and integrity of the communication. Thus, while symmetric key cryptography offers expedited and resource–efficient solutions for secure communication, diligent attention to key management remains paramount to uphold the overall security of the system.

It's interesting to note that some approaches have adopted the Timed Efficient Stream Loss–tolerant Authentication (TESLA) protocol for SATCOM systems, proposed by Perrig et al. [34]. TESLA is designed to provide broadcast authentication for data packets in a network, and it accomplishes this by employing a specific mechanism involving Message Authentication Codes (MACs) and key disclosure.

The core concept of the TESLA protocol is that the sender attaches a MAC to each data packet before transmission. This MAC is generated using a secret key ($k$) known only to the sender. It serves as a digital signature or authentication code for the packet. Upon receiving a packet, the recipient buffers it without initially authenticating the packet. The recipient cannot perform authentication immediately because it does not possess the key ($k$) required for the verification process. After a certain period of time, the sender discloses the key (k) to the receiver. This key disclosure event is pivotal for the receiver to be able to authenticate the packets it has received. With the disclosed key ($k$) in hand, the receiver can then authenticate the previously received packets.

By verifying the MACs of the packets using the revealed key, the recipient ensures the data's integrity and source authenticity. Furthermore, TESLA requires synchronization between the sender's and receiver's clocks, this clock synchronization ensures that the recipient knows when to expect the key disclosure event, enabling accurate packet authentication. TESLA's application in SATCOM systems is likely driven by its ability to provide delayed source authentication for broadcast communications in environments that often present resource limitations and various challenges [24, 35], and can strike a balance between maintaining security and minimizing computational overhead.

These cryptographic schemes and protocols are based, generally, on mutual authentication that ensures that both communicating entities or parties authenticate each other's identities before establishing a secure and trusted communication channel. On the other hand, message authentication is essential for ensuring the trustworthiness of data and confirming that it was sent by the expected entity. It complements mutual authentication by providing a level of assurance about the integrity of the data itself. Some studies are focused on enhancing communication security and privacy by providing additional properties, particularly anonymity and user privacy references [22, 28, 33, 36–40].

Researchers and security professionals widely used some tools, such as ProVerif (this tool is used for the formal verification of security protocols) [41], CryptoVerif (this tool is used for the formal verification of cryptographic protocols) [42], VISPA (Automated Validation of Internet Security Protocols and Applications) (this tool is specifically designed for the automated validation of internet security protocols and applications) [43], and Tamarin (this is a protocol verification tool primarily used for the analysis of security protocols) [44].

All of them are used to verify the security and correctness of cryptographic protocols and systems, as they can help identify vulnerabilities and weaknesses in cryptographic protocols, ensuring that systems are secure and resilient to attacks. In general, the evaluated schemes

predominantly rely on simulation–based assessment [24, 35, 37], with only occasional utilization of real–world data and deployed proof–of–concepts [25, 28].

**B. Key agreement**

Key agreement protocols serve as foundational elements in contemporary cryptography and secure communication, enabling entities to establish secure channels for data exchange, even in the absence of pre–existing shared secrets. These protocols are vital for guaranteeing the confidentiality, integrity, and authenticity of data transmitted within SATCOM systems.

In SATCOM systems, particularly for SG (Space–to–Ground) and SS (Space–to–Space) links, secure key establishment involves securely generating and sharing cryptographic keys (that are used to encrypt, decrypt, and authenticate data during communication) [16, 45–47]. Many of the proposed solutions require software updates, that are essential for improving the security of satellite systems, and may involve patches or changes to the software running on the satellites, ground stations, or other components of the system. These updates can be delivered through various means, including radio links (particularly useful for remote or inaccessible satellites), or in some cases, offline intervention on the satellite may be required to apply updates. The choice of update method depends on the satellite system's architecture and requirements.

It's worth to note that the security and efficiency aspects discussed for key sharing techniques (section A. Authentication) are also relevant to key agreement protocols in SATCOM links. Application of the Identity–Based Cryptography (IBC) and Chaotic Maps (CM) has several advantages and disadvantages [48, 49], such as:

- advantages (simplified key management; easy scalability; strong authentication mechanisms; more resistant to quantum attacks compared to traditional public–key cryptography; robustness against chaotic environments.
- disadvantages (key escrow problem; single point of failure; IBC and CM can be more complex to implement and maintain compared to traditional encryption methods; chaotic maps can introduce additional bandwidth overhead; The computational overhead of IBC and CM can impact the performance; lack of standardization).

Many of the security schemes and protocols analyzed in the previous paragraph are designed to achieve balanced protection (based on Confidentiality, Integrity, and Availability of data, along with identity verification) to tailor security measures to the system's specific requirements.

In the realm of secure key agreement protocols, the Canetti–Krawczyk (CK) security model and its extended counterpart, the extended Canetti–Krawczyk (eCK) security model, stand as foundational frameworks. These models are widely adopted for scrutinizing and validating diverse security aspects inherent in the key exchange process, encompassing critical facets like peer entity authentication and the preservation of message authenticity [50]. Through rigorous analysis of these models, protocol designers can ascertain the resilience of their systems against various cryptographic attacks and ensure robust security guarantees for communication channels.

Researchers employ a spectrum of assessment methodologies to comprehensively evaluate the performance of key agreement protocols within SATCOM systems. These methodologies encompass formal analysis, simulation tools, and real system performance evaluation [16, 51, 52]. Through formal analysis, they scrutinize the protocols against theoretical cryptographic models to validate their security properties rigorously. Simulation tools enable researchers to simulate various scenarios and assess protocol behavior under different conditions, providing insights into scalability, efficiency, and resilience. Additionally, real system performance evaluation involves deploying protocols in real–world environments to measure their effectiveness, latency, throughput, and other relevant metrics, thus offering practical validation of their performance.

By integrating these diverse methodologies, scientists can gain a holistic understanding of key agreement protocol performance and make informed decisions regarding their deployment in SATCOM systems.

**C. Quantum key distribution**

Stephen Wiesner's concept of quantum conjugate coding, introduced in the early 1970s, was an innovative and pioneering idea in the field of quantum information theory. His work laid the foundation for exploring the unique properties of quantum mechanics for information encoding and transmission.

The collaboration between Charles H. Bennett and Gilles Brassard, which began at the 20th IEEE Symposium on the Foundations of Computer Science in 1979, was a pivotal moment in the

development of quantum cryptography and information theory. This meeting led to the incorporation and expansion of Stephen Wiesner's earlier findings on quantum conjugate coding [53].

Quantum Key Distribution (QKD) represents a groundbreaking paradigm in secure communication, harnessing the fundamental principles of quantum mechanics. Unlike conventional encryption methods, which rely on the computational complexity of mathematical algorithms, QKD's security foundation lies in the intrinsic properties of quantum mechanics.

By exploiting phenomena such as quantum entanglement and the uncertainty principle, QKD enables the exchange of cryptographic keys with unprecedented security assurances. This approach ensures that any attempt to intercept or eavesdrop on the communication will unavoidably disturb the delicate quantum states, thereby alerting legitimate users to potential intrusions.

Consequently, QKD offers a level of security that is theoretically unbreakable, making it a highly promising solution for safeguarding sensitive information in the face of emerging threats from quantum computing and other advanced adversaries.

QKD protocols rely on the principles of quantum mechanics, such as the Heisenberg Uncertainty Principle and the "no–cloning" theorem. Also, it allows the parties engaged in key exchange to detect the presence of an eavesdropper. The security of QKD is information–theoretic and offers perfect forward secrecy, while QKD protocols allow two remote parties to establish a shared secret key, which can be used for encryption purposes. QKD offers strong security guarantees, however, its practical deployment and use are still evolving [54, 55].

While there is a gap between theory and practice in QKD, ongoing research and development are narrowing that gap and bringing practical QKD solutions closer to real–world deployment, through:

— hardware improvements;
— protocols and algorithms;
— integration;
— standardization; and
— long–term security planning.

Leveraging quantum technology for secure communication links in Satellite Ground (SG) and Space Satellite (SS) communication is an exciting prospect, but it does come with several challenges, such as:

— interference and environmental factors;
— quantum channel loss;
— quantum key distribution range;
— authentication and security protocols;
— quantum device reliability;
— integration with existing infrastructure;
— quantum technology development, and
— cost and resource constraints.

While there are still ongoing research efforts to address challenges in QKD, such as improving range and efficiency, the practical adoption of QKD in optical communication channels can be highlighted by some key points, such as:

— operational use;
— optical communication security,
— point–to–point communications;
— diverse applications;
— global quantum networks; and
— commercial solutions.

This is a crucial step forward in enhancing the security of communications and protecting against potential threats, including those posed by future quantum computing technologies [56].

In literature, different works studied:

— BB84 quantum key distribution scheme [57, 58];
— schemes based on quantum entanglement [59, 60];
— generic QKD [61];
— custom QKD [62];
— Decoy–state QKD [63];
— BB84 + Decoy [64, 65]; and
— B92 [66, 67].

Many studies within the realm of secure communication have explored the application of QKD for disseminating cryptographic keys across different scenarios. These include investigations into free space QKD, as well as detailed examinations of its feasibility and efficiency, as evidenced by references [57–59, 64, 66].

Researchers in various studies obtained a comprehensive understanding of the feasibility and performance of satellite–based QKD, by combining theoretical analysis, experimental assessment, and simulation.

**FUTURE CHALLENGES**

The development of 6G networks presents complex security and privacy challenges, particularly when accommodating various technologies and meeting stringent requirements.

A multi–faceted approach, including physical–layer security, cryptography, standardization efforts, and emerging architectural solutions like Zero Trust, will be essential to address these

challenges effectively and create a secure and resilient communication infrastructure for the future, especially to accommodate satellites, unmanned aerial vehicles, and undersea communications.

## CONCLUSIONS

The main aim of the article is to offer a comprehensive perspective on cryptography techniques for satellite–based communications, covering the challenges, potential solutions, and future trends in this domain.

The multidimensional approach that incorporates advanced security practices, adaptability, and collaboration is indeed crucial for building resilient and secure SATCOM systems, particularly in the face of continually evolving security and privacy challenges.

In summary, it's important to emphasize that there is no one–size–fits–all solution, and the choice depends on a variety of factors and criteria. Systematic analysis and comprehensive evaluation are the best approaches to making an informed decision based on the specific SATCOM system's objectives, requirements, and constraints will enable us to make an informed and well–considered choice regarding the most suitable encryption standard.

### References

[1] Jeremy E. Allnutt, and Timothy Pratt,"Satellite communications", 3rd edition, John Wiley & Sons Ltd., Hoboken, USA, 2019.

[2] Gerard Maral, Michel Bousquet, and Zhili Sun,"Satellite communications systems: systems, techniques and technology", 6th edition, John Wiley & Sons Ltd, CPI Group Ltd, Croydon, UK, 2020

[3] Daljeet Singh, Krishna Dev Kumar, and Raghvendra Kumar Chaudhary (Eds.),"Computer aided constellation management and communication satellites", Springer Nature Singapore, 2023

[4] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro,"Satellite–based communications security: a survey of threats, solutions, and research challenges", Computer Networks, 216: 109246, pp. 1–18, 2022

[5] R. Dallaev, T. Pisarenko, Ş. Ţălu, D. Sobola, J. Majzner, and N. Papež,"Current applications and challenges of the Internet of Things". New Trends In Computer Sciences, vol. 1, issue 1, pp. 51–61, 2023

[6] A. Nazarov, D. Nazarov, and Ş. Ţălu,"Information security of the Internet of Things". In: Proceedings of the International Scientific and Practical Conference on Computer and Information Security – INFSEC, SCITEPRESS – Science and Technology Publications, Lda, vol. 1, pp. 136–139, 2021.

[7] A.C. Boley, and M. Byers,"Satellite mega–constellations create risks in Low Earth Orbit, the atmosphere and on Earth". Sci Rep., 11, 10642, 2021

[8] M.Z. Asghar, S.A. Memon, and J. Hämäläinen,"Evolution of wireless communication to 6G: potential applications and research directions". Sustainability. 14(10): 6356, 2022

[9] *** "Global satellite communication (SATCOM) market overview", https://www.marketresearchfuture.com/reports/satellite–communication–market–8466 (accessed February 10, 2024).

[10] R. Fratty, Y. Saar, R. Kumar, and S. Arnon,"Random routing algorithm for enhancing the cybersecurity of LEO satellite networks". Electronics. 12(3): 518, 2023

[11] A.J. Akande, E. Foo, Z. Hou, and Q. Li,"Cybersecurity for satellite smart critical infrastructure". In: Pal, S., Jadidi, Z., Foo, E., Mukhopadhyay, S.C. (eds.) Emerging smart technologies for critical infrastructure. Smart sensors, measurement and instrumentation, vol 44. Springer, Cham, 2023

[12] R. Singh, I. Ahmad, and J. Huusko,"The role of physical layer security in satellite–based networks", In: 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 2023, pp. 36–41

[13] M. Torky, T. Gaber, E. Goda, V. Snasel, and A.E. Hassanien,"A blockchain protocol for authenticating space communications between satellites constellations". Aerospace. 9(9): 495, 2022

[14] Y. Zhang, Y. Wang, Y. Hu, Z. Lin, Y. Zhai, L. Wang, Q. Zhao, K. Wen, and L. Kang. "Security performance analysis of LEO satellite constellation networks under DDoS attack". Sensors. 22(19): 7286, 2022

[15] S. Jackson, J. Straub, and S. Kerlin,"Exploring a novel cryptographic solution for securing small satellite communications". Int. J. Netw. Secur., 20(5): 988–997, 2018

[16] [16] A. Ostad–Sharif, D. Abbasinezhad–Mood, and M. Nikooghadam,"Efficient utilization of elliptic curve cryptography in design of a three–factor authentication protocol for satellite communications". Comput. Commun. 147: 85–97, 2019.

[17] [17] A. Murtaza, S.J.H. Pirzada, M.N. Hasan, T. Xu, and L. Jianwei,"An efficient encryption algorithm for perfect forward secrecy in satellite communication". In Advances in Cyber Security; M. Anbar, N. Abdullah, S. Manickam (Eds.). Springer: Singapore, pp. 289–302, 2020.

[18] [18] S.J.H. Pirzada, A. Murtaza, T. Xu, and L. Jianwei,"Architectural optimization of parallel authenticated encryption algorithm for satellite application". IEEE Access, 8: 48543–48556, 2020.

[19] [19] P. Zuo, J. Wei, K. Zhang, X. Liu, C. Guo, and R. Hu,"An intelligent encryption decision method for autonomous domain of multilayer satellite network". Alexandria Engineering Journal, 81: 337–346, 2023

[20] [20] I. Altaf, M. Arslan Akram, K. Mahmood, S. Kumari, H. Xiong, and M. Khurram Khan,"A novel authentication and key–agreement scheme for satellite communication network". Trans Emerg Telecommun Technol. 32(7): e3894, 2021.

[21] [21] Y. Chen, and J. Chen,"An enhanced dynamic authentication scheme for mobile satellite communication systems". Int Satell Commun Netw. 39(3): 250–262, 2021.

[22] [22] S. Xu, X. Liu, M. Ma, and J. Chen,"An improved mutual authentication protocol based on perfect forward secrecy for satellite communications". Int J Satell Commun Netw., 38(1): 62–73, 2020.

[23] [23] B. Bhatta,"Global Navigation Satellite Systems: New Technologies and Applications", CRC Press, 2nd ed., Boca Raton, USA, 2021.

[24] [24] K. Ghorbani, N. Orouji, and M. Mosavi,"Navigation message authentication based on one–way hash chain to mitigate spoofing attacks for GPS L1", Wirel. Pers. Commun. 113(4): 1743–1754, 2020.

[25] [25] J.T. Curran, M. Paonni, and J. Bishop,"Securing the open–service: A candidate navigation message authentication scheme for Galileo E1 OS", in: European Navigation Conference, (ENC–GNSS), 2014.

[26] [26] V. Miller,"Use of Elliptic Curves in Cryptography". In: Williams, H.C. (eds) Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg

[27] [27] N. Koblitz,"Elliptic curve cryptosystems, Mathematics of Computation", 48: 203–209, 1987

[28] [28] W. Meng, K. Xue, J. Xu, J. Hong, and N. Yu,"Low–latency authentication against satellite compromising for space information network". In: 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2018, pp. 237–244.

[29] [29] S.R. Singh, A.K. Khan, and T.S. Singh,"A critical review on Elliptic Curve Cryptography", 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, India, 2016, pp. 13–18

[30] V. Gopinath, and R.S. Bhuvaneswaran,"Design of ECC based secured cloud storage mechanism for transaction rich applications", Computers, Materials & Continua, 57(2): 341–352, 2018.

[31] W. Xinghua, Z. Aixin, L. Jianhua, Z. Weiwei, and L. Yuchen,"A lightweight authentication and key agreement scheme for mobile satellite communication systems". In: Information Security and Cryptology, Springer International Publishing, Cham, 2017, pp. 187–204.

[32] W. Zhao, A. Zhang, J. Li, X. Wu, and Y. Liu,"Analysis and design of an authentication protocol for space information network", in: MILCOM 2016 – 2016 IEEE Military Communications Conference, 2016, pp. 43–48.

[33] Y. Liu, A. Zhang, S. Li, J. Tang, and J. Li,"A lightweight authentication scheme based on self–updating strategy for space information network", Int. J. Satell. Commun. Netw. 35(3): 231–248, 2017.

[34] A. Perrig, R. Canetti, J.D. Tygar, and D. Song,"The TESLA broadcast authentication protocol", RSA Cryptobytes, 5(2): 2–13, 2002.

[35] 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: 2016 International Conference on Localization and GNSS (ICL–GNSS), 2016, pp. 1–6.

[36] C.L. Chen, K.W. Cheng, Y.L. Chen, C. Chang, and C.C. Lee,"An improvement on the self–verification authentication mechanism for a mobile satellite communication system", Appl. Math. Inf. Sci., 8(1L): 97–106, 2014.

[37] W. Xinghua, Z. Aixin, L. Jianhua, Z. Weiwei, and L. Yuchen,"A lightweight authentication and key agreement scheme for mobile satellite communication systems". In: Information Security and Cryptology, Springer International Publishing, Cham, 2017, pp. 187–204.

[38] S. Xu, X. Liu, M. Ma, and J. Chen,"An improved mutual authentication protocol based on perfect forward secrecy for satellite communications". Int. J. Satell. Commun. Netw. 38(1): 62–73, 2020.

[39] Y. Zhang, J. Chen, and B. Huang,"An improved authentication scheme for mobile satellite communication systems". Int. J. Satell. Commun. Netw. 33(2): 135–146, 2015.

[40] A.D. Jurcut, J. Chen, A. Kalla, M. Liyanage, and J. Murphy,"A novel authentication mechanism for mobile satellite communication systems", in: 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW), IEEE, 2019, pp. 1–7.

[41] N. Dalal, J. Shah, K. Hisaria, and D. Jinwala,"A comparative analysis of tools for verification of security protocols". Int. J. Comm. Netw Syst Sci., 3: 779–787, 2010

[42] B. Blanchet,"CryptoVerif: A computationally–sound security protocol verifier", Tech. Rep., 2017

[43] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P.H. Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron,"The AVISPA tool for the automated validation of internet security protocols and applications", in: K. Etessami, S.K. Rajamani (Eds.), Computer Aided Verification, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 281–285.

[44] X. Zhang, Y. Zhu, C. Gu, and X. Miao,"A formal verification method for security protocol implementations based on model learning and Tamarin". J. Phys.: Conf. Ser. 1871, 012102, 2021

[45] L. Deng, S. Ye, and H. Qiu,"Transmission security platform for transportation information based on BeiDou navigation satellite system", in: 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2018, pp. 2110–2113.

[46] M. Qi, J. Chen, and Y. Chen,"A secure authentication with key agreement scheme using ECC for satellite communication systems". Int. J. Satell. Commun. Netw. 37 (3) (2019) 234–244.

[47] C.–C. Lee,"A simple key agreement scheme based on chaotic maps for VSAT satellite communications". Int. J. Satell. Commun. Netw. 31(4): 177–186, 2013.

[48] M. Joye, and G. Neven,"Identity–Based Cryptography", vol. 2, IOS Press, 2009.

[49] L. Kocarev,"Chaos–based cryptography: a brief overview", IEEE Circuits Syst. Mag. 1(3): 6–21, 2001.

[50] A.P. Sarr, P. Elbaz–Vincent, and J.–C. Bajard,"A new security model for authenticated key agreement", in: J.A. Garay, R. De Prisco (Eds.), Security and Cryptography for Networks, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 219–234.

[51] I. Altaf, M.A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C–M. Chen,"A lightweight key agreement and authentication scheme for satellite–communication systems". IEEE Access, 8, 46278–46287, 2020.

[52] M. Qi, J. Chen, and Y. Chen,"A secure authentication with key agreement scheme using ECC for satellite communication systems". Int. J. Satell. Commun. Netw. 37 (3): 234–244, 2019.

[53] G. Brassard,"Brief history of quantum cryptography: a personal perspective". IEEE Information Theory Workshop on Theory and Practice in Information–Theoretic Security, 2005., Awaji, Japan, 2005, pp. 19–23

[54] E. Diamanti, H.–K. Lo, B. Qi, and Z. Yuan,"Practical challenges in quantum key distribution". Npj Quantum Inf. 2 (1): 1–12, 2016.

[55] R. Bedington, J.M. Arrazola, and A. Ling,"Progress in satellite quantum key distribution". NPJ Quantum Inf 3, 30, 2017

[56] W. Cui, Z. Song, G. Huang, and R. Jiao,"Satellite–based phase–matching quantum key distribution". Quantum Inf Process, 21, 313, 2022

[57] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi,"Experimental satellite quantum communications". Phys. Rev. Lett. 115 (4): 040502, 2015.

[58] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi,"Feasibility of satellite quantum key distribution". New J. Phys. 11(4), 045017, 2009.

[59] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M.J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes,"Higher–dimensional orbitalangular–momentum–based quantum key distribution with mutually unbiased bases". Phys. Rev. A 88(3), 032305, 2013.

[60] R. Bedington, T. Zhongkan, R. Chandrasekara, C. Cheng, T.Y. Chuan, K. Durak, A.V. Zafra, E. Truong–cao, A. Ling, and D. Oi,"Small photon entangling quantum system (SPEQS) enabling space based quantum key distribution (QKD)", in: International Astronautical Congress, Jerusalem, Israel, 2015.

[61] Y.C. Tan, R. Chandrasekara, C. Cheng, and A. Ling,"Radiation tolerance of optoelectronic components proposed for space–based quantum key distribution". J. Modern Opt. 62(20): 1709–1712, 2015.

[62] T. Jennewein, C. Grant, E. Choi, C. Pugh, C. Holloway, J. Bourgoin, H. Hakima, B. Higgins, and R. Zee,"The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite" in: Emerging Technologies in Security and Defence II; and Quantum–Physics–Based Information Security III, Vol. 9254, International Society for Optics and Photonics, 2014, 925402.

[63] J.–Y. Wang, B. Yang, S.–K. Liao, L. Zhang, Q. Shen, X.–F. Hu, J.–C. Wu, S.–J. Yang, H. Jiang, and Y.–L. Tang,"Direct and full–scale experimental verifications towards ground–satellite quantum key distribution". Nat. Photonics, 7(5): 387–393, 2013.

[64] J.–P. Bourgoin, N. Gigov, B.L. Higgins, Z. Yan, E. Meyer–Scott, A.K. Khandani, N. Lütkenhaus, and T. Jennewein,"Experimental quantum key distribution with simulated ground–to–satellite photon losses and processing limitations". Phys. Rev. A 92 (5): 052339, 2015.

[65] S. Liao, W. Cai, W. Liu, L. Zhang, Y. Li, J. Ren, J. Yin, Q. Shen, Y. Cao, and Z. Li,"Satellite–to–ground quantum key distribution". Nature, 549 (7670): 43–47, 2017.

[66] H. Takenaka, A. Carrasco–Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima,"Satellite–to–ground quantum–limited communication using a 50–kg–class microsatellite". Nat. Photonics 11(8): 502–508, 2017.

[67] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, M. Takeoka, M. Fujiwara, and M. Sasaki, "Polarization–basis tracking scheme in satellite quantum key distribution". Int. J. Opt. 254154, 2011



ISSN: 2067–3809