Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Performance and Security Trade-offs in Keyless Data Encryption and Decryption

Haider Abbas (Corresponding Author)
Preston University (Islamabad Campus) of Pakistan
Email: haider7717@yahoo.com

Dr. Malik Sikandar Hayat Khiyal
Preston University (Islamabad campus) of Pakistan
Email; drsikandarhayat@preston.edu.pk

Dr. Muhammad Daud Awan
Preston University (Islamabad Campus) of Pakistan
Email: drdaudawan@preston.edu.pk

ABSTRACT

Traditional cryptographic systems heavily depend on secure key management, distribution, and storage, creating vulnerabilities that become critical in the face of quantum computing threats and complex network environments. This paper explores keyless data encryption and decryption paradigms that derive security from intrinsic properties of communication channels, data context, physical environments, or biological traits, eliminating the need for pre-shared or stored keys. Drawing on information-theoretic foundations such as Shannon's perfect secrecy and Wyner's wiretap channel model, the review examines key architectural modalities, including Physical Layer Security (PLS) techniques (e.g., artificial noise injection and unshared secret key generation in 5G/6G networks), the Keyless User Defined Optimal Security (KUDOS) algorithm for memory context protection, All-or-Nothing Transforms (AONT) combined with information dispersal for distributed storage, biometric-based fuzzy vault schemes, chaos-based image encryption, and emerging quantum-resilient AI-integrated frameworks like QSAFE-MM1.A detailed analysis of performance-security trade-offs reveals inherent tensions, such as the Secrecy-Reliability Performance Trade-off (SRPT) in NOMA systems, energy efficiency constraints in IoT environments, computational overhead in fully homomorphic encryption, and acceptance-rate declines in biometric systems with increasing polynomial complexity. While keyless approaches offer advantages in reduced attack surface, lower latency, and quantum resistance, they demand careful balancing against reliability, throughput, energy consumption, and scalability limitations.The findings underscore the shift toward adaptive, hybrid security architectures that integrate physical randomness, AI-driven monitoring, and context-aware mechanisms to achieve robust, future-proof protection in heterogeneous digital ecosystems.

Keywords: Keyless encryption, Physical Layer Security (PLS), Keyless User Defined Optimal Security (KUDOS), All-or-Nothing Transform (AONT), Wiretap channel,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Secrecy capacity, Biometric cryptography, Chaos-based image encryption, Quantum-resilient security, Secrecy-Reliability Performance Trade-off (SRPT), Internet of Things (IoT) security, 6G networks

Introduction

The contemporary digital landscape is defined by an unprecedented volume of data transmission across heterogeneous networks, necessitating security architectures that can withstand both classical and quantum-era threats (Shah et al., 2025). Traditional cryptographic paradigms, while robust, have long been tethered to the complexities and vulnerabilities of key management, distribution, and storage (Mitev et al., 2024). The fundamental reliance on a shared secret whether a symmetric key or an asymmetric public-private pair introduces a single point of failure: if the key is compromised, the entire security of the communication is rendered void (Banoth et al., 2023). In response to these structural limitations, keyless data encryption and decryption have emerged as a critical field of research, shifting the security burden from a pre-distributed secret to the intrinsic properties of the communication environment, biological traits, or the structural context of the data itself (Uludag et al., 2005).

To understand the trajectory of keyless security, it is necessary to examine the evolution of cryptographic theory from computational security to information-theoretic security. Conventional systems, such as the Advanced Encryption Standard (AES) or RSA, derive their strength from the computational difficulty of mathematical problems, such as prime factorization or discrete logarithms (Campbell, 2025). However, the advent of quantum computing, specifically through Shor's algorithm, poses a terminal threat to these architectures by potentially reducing the time required to solve such problems from millennia to minutes (Nauman et al., 2025). Keyless systems, particularly those rooted in physical layer security (PLS) and information theory, offer a path toward "unconditional security," where a system is theoretically unbreakable regardless of the adversary's computational power (Shim, 2025).

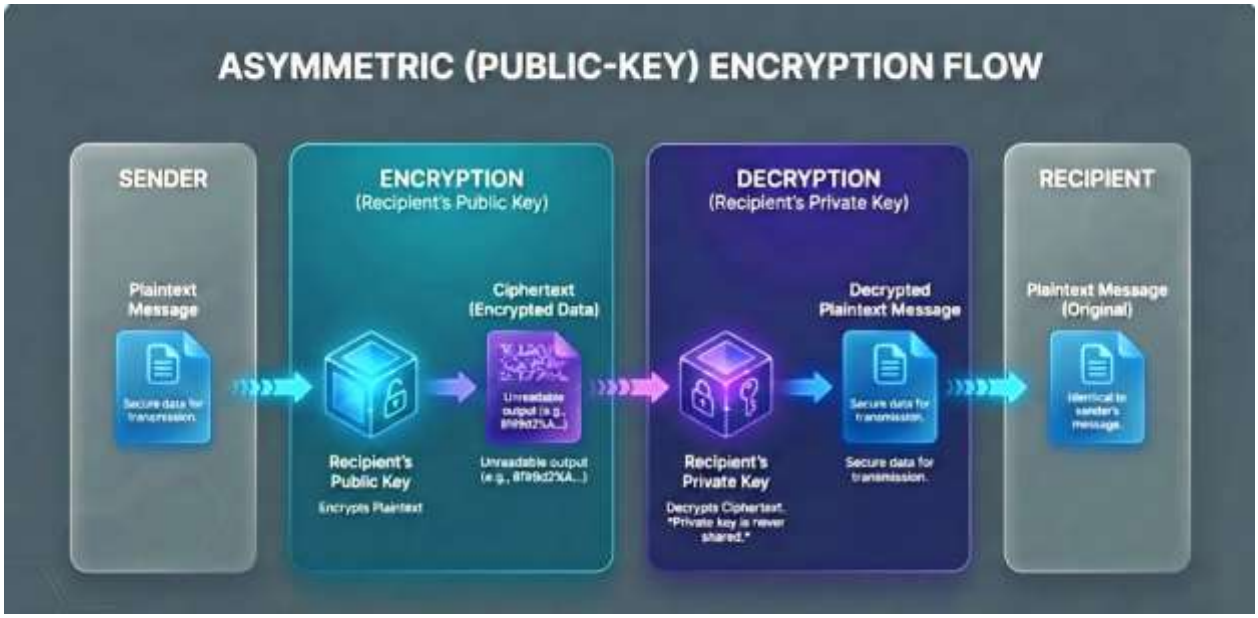
The conceptual bedrock of keyless security was established by Claude Shannon in 1949 and later expanded by Aaron Wyner through the wiretap channel model (Wyner, 1975). Shannon's definition of perfect secrecy mandates that the ciphertext must reveal absolutely no information about the plaintext to an observer who lacks the decryption mechanism. Mathematically, this is expressed as the mutual information between the message W and the adversary's observation Zn being zero: I (W; Zn) = 0 (Kuang et al., 2023).

Figure 1: Traditional Asymmetric Public-Key Encryption Architecture

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about



In practical implementations, achieving perfect secrecy requires an entropy source at least as large as the message itself, making it cumbersome for high-volume data. Consequently, researchers utilize a spectrum of secrecy metrics to quantify and manage information leakage (Torre et al., 2025).

Table 1: Secrecy Metrics and Mathematical Requirements

Secrecy Metric	Mathematical Requirement	Description and Security Implication
Perfect Secrecy	I(W; Zn) = 0	The adversary's best attack is a random guess; message and observation are statistically independent.
Weak Secrecy	(1/n) I(W; Zn) <= epsilon	Limits the rate of information leakage per bit; may still allow a high total bit leakage over large files.
Strong Secrecy	I(W; Zn) <= epsilon	Ensures the total amount of leaked information remains negligible, regardless of message length.
Semantic Secrecy	max_pW I(W; Zn) <= epsilon	The most robust metric; leakage remains negligible for any possible message distribution.

Wyner's wiretap channel model introduced the idea that secrecy can be imparted by the communication channel itself without pre-shared keys. In this model, the transmitter (Alice) communicates with a legitimate receiver (Bob) over a "main channel," while an eavesdropper (Eve) intercepts the transmission via a "wiretap channel" (Sharifian, 2020). If the main channel is superior to the wiretap channelmeaning it has a higher capacity or lower noiseAlice can employ stochastic coding to ensure Bob receives the message while Eve receives only noise (Algrøy, 2022) (Illi et al., 2023).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Architectural Modalities of Keyless Encryption

Keyless security is not a monolithic technology but a collection of diverse architectural modalities that exploit different sources of entropy and asymmetry. These range from the physical characteristics of wireless signals to the unique biological features of humans (Kshetri et al., 2024).

Physical Layer Security (PLS) in Wireless Communication

Physical Layer Security (PLS) exploits the fundamental physics of radio propagation to provide confidentiality and authentication (Sindhushree et al., 2025). Unlike traditional encryption, which operates at the higher, logical layers of the network stack, PLS focuses on the physical transmission medium (Sanenga et al., 2023).

Mechanisms of Interference and Noise

One of the most potent techniques in PLS is Artificial Noise (AN) injection. In a multi-antenna (MIMO) system, the transmitter can generate noise and align it with the null space of the legitimate receiver's channel (Guo et al., 2024). Because the noise is in Bob's null space, it is effectively invisible to him, allowing him to decode the message without interference. However, because Eve is at a different physical location, her channel is spatially distinct, and the noise will significantly degrade her received signal (Qiu al., 2023).

The Unshared Secret Key (USK) cryptosystem represents an advancement of this concept, where the AN is designed to act as a one-time pad secret key that is generated on-the-fly based on the channel's instantaneous state (Let al., 2020). This provides a mechanism for Shannon's ideal secrecy without requiring any explicit key exchange between the communicating parties, thereby bypassing the risks of interception during key distribution (Cerruti et al., 2021).

Secrecy in 5G and 6G Networks

The transition to 5G and upcoming 6G networks introduces ultra-reliable low latency communication (URLLC), which poses significant challenges for traditional cryptography (Salh et al., 2021). Standard key-based handshakes are often too slow to meet the sub-millisecond latency requirements of mission-critical applications like autonomous driving or robotic surgery (Mohammed et al., 2024). PLS offers a low-complexity alternative that generates less signaling overhead and consumes less computational power, making it more robust against jamming and eavesdropping in highly dynamic network topologies (Siddiqui et al., 2023).

Keyless User Defined Optimal Security (KUDOS) and Memory Context

In computing environments where memory management is critical, the Keyless User Defined Optimal Security (KUDOS) algorithm provides a mechanism for encrypting and decrypting memory context without external keys (IJFMR, 2024). KUDOS derives its encryption parameters directly from the data context, such as memory addresses or data strings, eliminating the need for key storage and reducing the attack surface for key-extraction attempts (Yusop et al., 2025).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

KUDOS Process and Performance Metrics

KUDOS utilizes a hybrid architecture that combines stream and block cipher techniques, ensuring high diffusion and security at multiple levels (Takei et al., 2024). The algorithm performs character transposition, string shuffling (where characters from two strings are sequentially alternated), and bit-level shift operations (Marufuzzaman., et al., 2019).

Table 2: KUDOS Algorithm Performance vs Traditional Lightweight Benchmark

Security Metric	KUDOS Algorithm Performance	Traditional Lightweight Benchmark
Confidentiality Measure	9.13	~8.45
Integrity Metric	9.35	~8.80
Encryption Speed	High (Context-derived)	Variable (Key-dependent)
Resilience to DPA	Excellent (No static key)	Moderate (Vulnerable)

The high confidentiality (9.13) and integrity (9.35) scores demonstrate that KUDOS can outperform traditional techniques while maintaining the efficiency required for resource-constrained IoT devices (Abinaya, 2025). By removing the energy expenditure associated with key production and the memory requirements for key storage, KUDOS extends the operational life of remote sensors and edge processors (Aldwairi et al., 2023).

All-or-Nothing Transform (AONT) and Information Dispersal

The All-or-Nothing Transform (AONT) is a keyless, unkeyed transformation designed as a pre-processing step to strengthen encryption. The core principle of AONT is that a message can only be recovered if the entire output of the transform is available to the receiver (Watanabe et al., 2015).

Figure 2: Threat Landscapes and Privacy Requirements in Distributed Cloud Storage



The Package Transform

The original AONT, known as the package transform, was described by Ronald Rivest in 1997. It involves XORing plaintext blocks with pseudorandom blocks

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

generated using a random internal key K'. The key K' is then XORed with the hashes of all the transformed blocks and appended to the message (Peterson et al., 2020). An adversary who intercepts 99% of the blocks still cannot recover a single bit of the original plaintext because they cannot recompute the hash required to reveal K' (Esfahani et al., 2021).

This property is particularly valuable in cloud storage. A client can apply an AONT to a file and then use an Information Dispersal Algorithm (IDA) to spread the shares across multiple Cloud Service Providers (CSPs) (Peterson, 2021). Because each CSP only holds a fragment of the AONT output, no individual providernor a collusion of providers below a specific thresholdcan gain any information about the data (Resch & Plank, 2011).

Performance Scaling in Distributed Storage

Table 3: Comparison of Information Dispersal and Data Replication Methods

Distribution Method	Storage Overhead	Security Property
Replication	N x Input Size	Low (Each copy is vulnerable)
Shamir's Secret Sharing	N x Input Size	High (Information-Theoretic)
Rabin's IDA	(N/K) x Input Size	Computational (Requires AONT)
AONT-RS	(N/K) x Input Size	Computational + High Speed

The integration of AONT with Systematic Reed-Solomon encoding (AONT-RS) allows for high-speed encoding and simpler rebuilding compared to traditional secret sharing, while maintaining a level of security comparable to "Secret Sharing Made Short" (Tian et al., 2020).

Performance and Security Trade-offs: A Nuanced Analysis

The adoption of keyless security is inherently a process of balancing conflicting requirements. In every implementation, there is a tension between the strength of the security provided and the performance of the system in terms of latency, throughput, and energy consumption (Schinagl et al., 2020

The Secrecy-Reliability Performance Trade-off (SRPT)

In wireless networks, especially those employing Non-Orthogonal Multiple Access (NOMA) and millimeter-wave (mmWave) frequencies, the Secrecy-Reliability Performance Trade-off (SRPT) is a central design consideration. Reliability is typically measured by Outage Probability (OP), while secrecy is measured by Intercept Probability (IP) (Solanki et al., 2021).

Numerical analysis of SRPT reveals that improving secrecy by decreasing IP invariably leads to an increase in OP, thereby deteriorating reliability (Chen et al., 2019). This trade-off is managed through power allocation coefficients (alpha). A primary user may be allocated a higher share of power to ensure reliability, but this increased power also makes the signal easier for an eavesdropper to intercept (Xiang et al., 2020).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

NOMA vs. OMA Secrecy Performance

A critical insight in SRPT research is that NOMA does not always provide better secrecy than Orthogonal Multiple Access (OMA). There exists a specific threshold for the power allocation coefficient, alpha_s*, under which NOMA guarantees superior secrecy (Lei et al., 2019). Interestingly, this optimal value depends solely on the target and secrecy rates and is independent of general system parameters like SNR or fading coefficients (Ahmed et al., 2024). If the required power allocation falls below this threshold, the system must switch to OMA to maintain security, highlighting the need for "mode switching" in intelligent 6G networks (Wang et al., 2019).

Energy Efficiency in IoT Environments

For Internet of Things (IoT) devices, the trade-off is often between security strength and battery lifetime. While traditional ciphers like AES are robust, their software implementation on 8-bit or 16-bit microcontrollers can be prohibitively slow and energy-intensive (Seferagić et al., 2020).

Lightweight Algorithm Comparisons

Evaluations on Nordic Thingy:53 platforms show that lightweight stream ciphers often offer the best energy profile for high-throughput tasks, while integrated Authenticated Encryption with Associated Data (AEAD) ciphers like ASCON are superior for sparse communication Al-Turjman et al., 2017).

Table 4: Energy Efficiency and Throughput of Lightweight Cryptographic Algorithms

Algorithm	Energy (uJ/byte)	Throughput	Complexity
ASCON32	~0.72	High	Integrated AEAD
XChaCha20	~0.74	Very High	Stream + Separate MAC
Salsa20	~0.74	High	Stream + Separate MAC
HC-256	>1.50	Low	Cache-Optimized
AES-CBC (SW)	High	Low	Iterative Block

The exclusion of hardware-accelerated AES in these tests is vital for understanding the baseline performance of software-defined security. Software-based AES-CBC is significantly slower and more power-hungry than ChaCha20 or Salsa20, yet many IoT platforms lack the AES-NI instructions found in modern PC processors (Alharby et al., 2018). This "hardware gap" makes lightweight, keyless, or reduced-round ciphers a necessity rather than an option for low-cost sensors (Qaim et al., 2020).

Biometric-Based Keyless Cryptography (Bio-Cryptography)

Biometric cryptosystems merge the convenience of biological identification with the security of cryptographic proof. In a keyless biometric system, a cryptographic key is not stored; instead, it is generated or released only upon the successful presentation of a biological trait, such as a fingerprint, iris scan, or voice embedding (Uludag et al., 2005).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

The Fuzzy Vault and Noise Sensitivity

The primary challenge in bio-cryptography is the "noisiness" of the input data. Unlike a digital key, a biometric trait is never captured perfectly identically twice. The Fuzzy Vault scheme addresses this by hiding a secret polynomial within a set of "chaff points"random data points that do not lie on the polynomial (Omotosho et al., 2017). A user can only recover the secret if their biometric sample provides enough correct points to filter out the chaff and perform Lagrange interpolation (Tantubay et al., 2021).

Table 5: Impact of Polynomial Degree on Biometric Security and Acceptance

Polynomial Degree	GAR (%)	FAR (%)	Security Level
Degree 3	92.0	High	Moderate
Degree 4	90.0	Moderate	High
Degree 5	85.0	Low	Very High

The trade-off here is evident: as the degree of the polynomial increases, the system becomes more secure against brute-force attacks (lower FAR), but the Genuine Acceptance Rate (GAR) drops, leading to more "false rejects" for legitimate users whose finger placement was slightly off (Voudouris et al., 2005).

Scalability and Voice Embeddings

Research into voice-based authentication highlights the scalability limitations of biometric systems. While high stability is observed with small user bases, accuracy gradually declines as the database size increases, indicating that larger systems require higher-dimensional embeddings or more sophisticated distance metrics like cosine distance to maintain effective separation between users (Oyebode, 2025).

Image Encryption: Keyless and Chaos-Based Approaches

Digital images require specialized encryption due to high pixel correlation and massive data volume, which can make standard block ciphers like DES or AES inefficient. Keyless image encryption techniques often utilize cipher-grid chains or chaotic maps to scramble data without explicit keys (Aithal, 2018).

Cipher-Grid Superimposition

In certain keyless image encryption models, a chain of cipher-grids is created where each successive grid can partially decrypt the previous one. Only when all cipher-grids are superimposed can the original image be recovereda form of visual secret sharing. This method is computationally efficient because it relies on simple logical operations (like XOR) rather than complex mathematical transformations (HS et al., 2017).

Chaotic Map Performance Metrics

Chaos-based encryption uses non-linear dynamical systems to produce pseudorandom sequences that are highly sensitive to initial conditions. The effectiveness of these schemes is measured by the Number of Pixel Change Rate (NPCR) and the Unified

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Average Changing Intensity (UACI) (Murillo-Escobar et al., 2015).

Table 6: Measured Performance Metrics for Chaos-Based Image Encryption

Metric	Measured Value	Ideal/Theoretical Value	Implication
NPCR	99.61%	>99.60%	High resistance to differential attacks.
UACI	33.46%	~33.46%	Good sensitivity to small changes.
Speed	30.33 ms	< 50 ms	Suitable for real-time video/image streaming.

While chaotic maps provide high speed and security, they can be vulnerable to chosen-plaintext attacks if the map's parameters are not sufficiently dynamic (Shende et al., 2024). Integrating chaotic maps with biometric data or channel-derived entropy sources can further harden these systems against cryptanalysis (El-Hameed et al., 2022).

Quantum-Resilient and AI-Integrated Security

As we look toward the future, the intersection of keyless security, artificial intelligence, and quantum computing defines the next frontier of data protection. Information-theoretic keyless models are inherently quantum-resistant, as their security does not rely on the complexity of mathematical problems. However, for systems that still require some form of digital signature or key encapsulation, post-quantum cryptography (PQC) based on lattice problems is being integrated (Campbell, 2025).

QSAFE-MM1: A Case Study in On-Device AI Security

The QSAFE-MM1 architecture is designed to secure mobile AI models (like Apple's MM1) against quantum threats using a combination of Federated Learning (FL), Fully Homomorphic Encryption (FHE), and lattice-based signatures (Dilithium and Falcon) (Nauman et al., 2025).

The Experimental Trade-offs of QSAFE-MM1

The implementation of advanced security layers on handheld devices reveals a stark contrast between security and usability. FHE, which allows for encrypted inference, is particularly resource-intensive (Nanda et al., 2024).

Table 7: Experimental Performance and Resource Trade-offs for QSAFE-MM1 Configurations

Configuration	Processing Efficiency	Energy (J)	Battery Drain	Thermal Impact
Baseline	100%	-	-	-
FL Only	94%	1020	7%/hr	+ 4 Celsius
FHE Only	19%	1600	13%/hr	+ 7 Celsius
FL+FHE+DP	79%	1700	14%/hr	+ 8 Celsius

The efficiency drop to 19% when using FHE alone illustrates a "performance cliff"

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

where the computational overhead of high-security encryption renders the device nearly unusable for real-time tasks (Smetters et al., 2002). However, the integrated stack (FL+FHE+DP) manages to recover some efficiency (up to 79%) through optimized noise injection and parallel processing, demonstrating that hybrid approaches are the only viable path for quantum-secure mobile AI (Weichbroth et al., 2020).

AI-Driven Self-Monitoring and Watchdog Networks

Beyond encryption, AI is being used to build "dynamic, self-monitoring" security systems. Dedicated watchdog neural networks can monitor for tampering, weight manipulation, or replay attacks in real-time. These systems can even implement "semantic" security by detecting anomalies in the message space that traditional bit-level encryption might miss (Campbell, 2025). The synergy between AI's processing power and the unbreakable nature of keyless PLS promises a future where data remains impervious to breaches even as adversaries become more sophisticated (Xiang et al., 2020).

Figure 3: Core Security Objectives: Confidentiality, Integrity, and Compliance



Conclusion

The review of performance and security trade-offs in keyless data encryption and decryption reveals a technology at a pivotal inflection point. Keyless paradigms, rooted in the fundamental laws of physics and information theory, offer a definitive solution to the vulnerabilities of key management and the existential threat of quantum computing. From the Unshared Secret Key (USK) cryptosystems in the physical layer to the context-aware KUDOS algorithm in memory management, these methods provide a path toward unconditional security.

Online ISSN 3007-3197
Print ISSN 3007-3189

However, the transition to keyless architectures is not without cost. The Secrecy-Reliability Performance Trade-off (SRPT) in 5G/6G networks highlights that securing information in ultra-low latency environments requires a meticulous balance of power and spectrum (Solanki et al., 2021). In the realm of IoT, the energy-efficiency gap between software-defined lightweight ciphers and hardware-accelerated standards continues to dictate device longevity (Sensors, 2025). Furthermore, the high computational and thermal overhead of quantum-resilient stacks like QSAFE-MM1 underscores the need for specialized hardware acceleration and more efficient algorithmic designs (Nauman et al., 2025).

For practitioners and researchers, the path forward involves a departure from "one-size-fits-all" security. The most resilient systems of the future will be those that are adaptiveutilizing AI to dynamically shift between keyless PLS, biometric-based authentication, and post-quantum transforms based on the real-time constraints of the network and the value of the data being protected. By weaving together the randomness of the physical world with the precision of modern cryptography, we can build a digital infrastructure that is not only faster and more efficient but fundamentally secure against the threats of tomorrow (Campbell, 2025).

References

Aithal, G. (2018). A survey on key(s) and keyless image encryption techniques. ResearchGate. https://www.researchgate.net/publication/321637906_A_Survey_on_Keys_and_Keyless_Image_Encryption_Techniques

Campbell, R. (2025). The sovereign SOC: A simulation framework for quantum-enhanced federated security operations. Preprints.org. https://doi.org/10.20944/preprints202510.1816.v1

Keyless mechanism for encrypting and decrypting memory context, leveraging the innovative keyless user defined optimal security (KUDOS) algorithm. (2024). International Journal for Multidisciplinary Research, 6(6). https://www.ijfmr.com/papers/2024/6/30797.pdf

Mitev, M., Chorti, A., Poor, H. V., & Fettweis, G. P. (2024). Keyless physical-layer cryptography. ResearchGate. https://www.researchgate.net/publication/397103565_Keyless_Physical-Layer_Cryptography

Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., & López-Gutiérrez, R. M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. ResearchGate. https://www.researchgate.net/publication/282268976_A_robust_embedded_biometric_authentication_system_based_on_fingerprint_and_chaotic_encryption

Nauman, U., Deng, M., Zhang, Y., & Khan, S. (2025). Quantum resilient security framework for privacy preserving AI in Apple MM1 on device architecture. Scientific Reports, 15, Article 38297. https://doi.org/10.1038/s41598-025-22056-5

Palaparthy, H., et al. (2022). Securing IoT in resource-constrained settings: A survey on lightweight cryptographic protocols. Nanotechnology Perceptions, 18(3),

Online ISSN 3007-3197
Print ISSN 3007-3189

286–298. https://nano-ntp.com/index.php/nano/article/download/5079/4023/9913

Performance metrics for various lightweight cryptographic algorithms evaluated on the Nordic Thingy:53 IoT platform. (2025). Sensors, 25(18), 5887. https://doi.org/10.3390/s25185887

Pradhan, A., Das, S., Piran, M. J., & Han, Z. (2024). A survey on physical layer security of ultra/hyper reliable low latency communication in 5G and 6G networks: Recent advancements, challenges, and future directions. IEEE Access, 12, 112320–112356. https://doi.org/10.1109/ACCESS.2024.3429285

Resch, J., & Plank, J. S. (2011). AONT-RS: Blending blocks for data storage efficiency and security. Proceedings of the 9th USENIX Conference on File and Storage Technologies (FAST '11). https://www.usenix.org/events/fast11/tech/slides/resch.pdf

Rivest, R. L. (1997). All-or-nothing encryption and the package transform. Proceedings of the 4th International Workshop on Fast Software Encryption (FSE '97), 210–218. https://doi.org/10.1007/BFb0052347

Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Solanki, S., Gurjar, D. S., Sharma, P. K., Sharma, S. K., & Chatzinotas, S. (2021). On the secrecy-reliability performance trade-off for NOMA-enabled 5G mmWave networks. 2021 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC 2021), 720–725. https://doi.org/10.1109/PIMRC50174.2021.9569610

Uludag, U., Pankanti, S., & Jain, A. K. (2005). Fuzzy vault for fingerprints. Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '05), 310–319. https://doi.org/10.1007/11527923_32

Wyner, A. D. (1975). The wire-tap channel. Bell System Technical Journal, 54(8), 1355–1387. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

Banoth, R., & Regar, R. (2023). Asymmetric Key Cryptography. In Classical and Modern Cryptography for Beginners (pp. 109-165). Cham: Springer Nature Switzerland.

Shah, A. M., & Gor, A. (2025). Comprehensive Survey of Symmetric and Public-Key Cryptographic Algorithms: Foundations, Attacks, and Applications.

Shim, K. A. (2015). A survey of public-key cryptographic primitives in wireless sensor networks. IEEE Communications Surveys & Tutorials, 18(1), 577-601.

Kuang, R., & Bettenburg, N. (2020, October). Shannon perfect secrecy in a discrete Hilbert space. In 2020 IEEE international conference on quantum computing and engineering (QCE) (pp. 249-255). IEEE.

Torre, D., Chennamaneni, A., Jo, J., Vyas, G., & Sabrsula, B. (2025). Toward enhancing privacy preservation of a federated learning cnn intrusion detection system in iot: method and empirical study. ACM Transactions on Software Engineering and Methodology, 34(2), 1-48.

Sharifian, S. (2020). Contributions to Information Theoretically Secure Communication.

Online ISSN 3007-3197
Print ISSN 3007-3189

Algrøy, J. (2022). Secure, reliable, and efficient communication over the wiretap channel (Master's thesis, The University of Bergen).

Illi, E., Qaraqe, M., Althunibat, S., Alhasanat, A., Alsafasfeh, M., De Ree, M., ... & Al-Kuwari, S. (2023). Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks. IEEE Communications Surveys & Tutorials, 26(1), 347-388.

Kshetri, N., Rahman, M. M., Rana, M. M., Osama, O. F., & Hutson, J. (2024). algoTRIC: Symmetric and asymmetric encryption algorithms for Cryptography--A comparative analysis in AI era. arXiv preprint arXiv:2412.15237.

Sanenga, A., Mapunda, G. A., Jacob, T. M. L., Marata, L., Basutli, B., & Chuma, J. M. (2020). An overview of key technologies in physical layer security. Entropy, 22(11), 1261.

Qiu, S., Wei, Z., Huang, Y., Abbaszadeh, M., Charmet, J., Li, B., & Guo, W. (2023). Review of physical layer security in molecular Internet of Nano-Things. IEEE Transactions on NanoBioscience, 23(1), 91-100.

Li, G., Zhang, Z., Zhang, J., & Hu, A. (2020). Encrypting wireless communications on the fly using one-time pad and key generation. IEEE Internet of Things Journal, 8(1), 357-369.

Cerruti, U. (2021). One time pad and the short key dream. arXiv preprint arXiv:2108.06981.

Salh, A., Audah, L., Shah, N. S. M., Alhammadi, A., Abdullah, Q., Kim, Y. H., ... & Almohammedi, A. A. (2021). A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems. IEEe Access, 9, 55098-55131.

Mohammed, S. M., Al-Barrak, A., & Mahmood, N. T. (2024). Enabling Technologies for Ultra-Low Latency and High-Reliability Communication in 6G Networks. Ingenierie des Systemes d'Information, 29(3).

Siddiqui, M. U. A., Abumarshoud, H., Bariah, L., Muhaidat, S., Imran, M. A., & Mohjazi, L. (2023). URLLC in beyond 5G and 6G networks: An interference management perspective. IEEe Access, 11, 54639-54663.

Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity. IEEE Access.

Takei, Y., & Shudo, K. (2024, May). Pragmatic analysis of key management for cryptocurrency custodians. In 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 747-765). IEEE.

Marufuzzaman, M., Al Karim, S., Rahman, M. S., Zahid, N. M., & Sidek, L. M. (2019). A review on reliability, security and memory management of numerous operating systems. Indonesian Journal of Electrical Engineering and Informatics (IJEEI), 7(3), 577-585.

Abinaya, P. (2025). Enhanced Security Using Modified Logical Keyless Encryption Algorithm (MLKA). In Sustainable Information Security in the Age of AI and Green Computing (pp. 369-384). IGI Global Scientific Publishing.

Aldwairi, M., Badra, M., & Borghol, R. (2023, October). Doccert: Nostrification, document verification and authenticity blockchain solution. In 2023 Fifth

Online ISSN 3007-3197
Print ISSN 3007-3189

International Conference on Blockchain Computing and Applications (BCCA) (pp. 652-657). IEEE.

Watanabe, D., & Yoshino, M. (2015). Key update mechanism using all-or-nothing transform for network storage of encrypted data. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 98(1), 162-170.

Peterson, R. A., & Peterson, M. R. A. (2020). Package 'bestNormalize'. Normalizing transformation functions. R package version, 1.

Esfahani, N. N., & Stinson, D. (2021). Rectangular, range, and restricted AONTs: Three generalizations of all-or-nothing transforms. arXiv preprint arXiv:2111.05961.

Peterson, R. A. (2021). Finding optimal normalizing transformations via bestNormalize.

Tian, Y., Hothorn, T., Li, C., Harrell Jr, F. E., & Shepherd, B. E. (2020). An empirical comparison of two novel transformation models. Statistics in medicine, 39(5), 562-576.

Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. Computers & Security, 122, 102903.

Chen, R., Li, C., Yan, S., Malaney, R., & Yuan, J. (2019). Physical layer security for ultra-reliable and low-latency communications. IEEE Wireless Communications, 26(5), 6-11.

Xiang, Z., Yang, W., Cai, Y., Ding, Z., Song, Y., & Zou, Y. (2020). NOMA-assisted secure short-packet communications in IoT. IEEE Wireless Communications, 27(4), 8-15.

Lei, H., Yang, Z., Park, K. H., Ansari, I. S., Guo, Y., Pan, G., & Alouini, M. S. (2019). Secrecy outage analysis for cooperative NOMA systems with relay selection schemes. IEEE Transactions on Communications, 67(9), 6282-6298.

Ahmed, A., Wang, X., Hawbani, A., Yuan, W., Tabassum, H., Liu, Y., ... & Ng, D. W. K. (2024). Unveiling the Potential of NOMA: A Journey to Next-Generation Multiple Access. IEEE Communications Surveys & Tutorials, 27(5), 3099-3164.

Wang, Z., & Peng, Z. (2019). Secrecy performance analysis of relay selection in cooperative NOMA systems. IEEE Access, 7, 86274-86287.

Seferagić, A., Famaey, J., De Poorter, E., & Hoebeke, J. (2020). Survey on wireless technology trade-offs for the industrial internet of things. Sensors, 20(2), 488.

Al-Turjman, F. M., Imran, M., & Bakhsh, S. T. (2017). Energy efficiency perspectives of femtocells in Internet of Things: Recent advances and challenges. IEEE Access, 5, 26808-26818.

Alharby, S., Harris, N., Weddell, A., & Reeve, J. (2018). The security trade-offs in resource constrained nodes for IoT application. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 12(1), 52-59.

Qaim, W. B., Ometov, A., Molinaro, A., Lener, I., Campolo, C., Lohan, E. S., & Nurmi, J. (2020). Towards energy efficiency in the internet of wearable things: A systematic review. IEEE Access, 8, 175412-175435.

Online ISSN 3007-3197
Print ISSN 3007-3189

Omotosho, A., Emuoyibofarhe, J., & Oke, A. (2017). Securing private keys in electronic health records using session-based hierarchical key encryption. Journal of Applied Security Research, 12(4), 463-477.

Tantubay, N., & Bharti, J. (2021). An Efficient Biocrypto-system Using Least Square Polynomial Curve Fitting with Interpolation Based New Chaff-Points Generation Method. Advances in Electrical & Computer Engineering, 21(3).

Voudouris, A., Tressos, A., Zarras, A., & Xenakis, C. (2025). Game on: a performance comparison of interpolation techniques applied to Shamir's secret sharing. The Computer Journal, 68(3), 261-272.

Oyebode, O. O. (2025). Adapting a Cell Phone with Voice Biometric Verification.

HS, R. K., SP, F. S., Aithal, G., & Shetty, S. (2017). A survey on key (s) and keyless image encryption techniques. Cybernetics and Information Technologies, 17(4).

Shende, S. W., Tembhurne, J. V., & Ansari, N. A. (2024). Deep learning based authentication schemes for smart devices in different modalities: progress, challenges, performance, datasets and future directions. Multimedia Tools and Applications, 83(28), 71451-71493.

El-Hameed, H. A. A., Ramadan, N., El-Shafai, W., Khalaf, A. A., Ahmed, H. E. H., Elkhamy, S. E., & El-Samie, F. E. A. (2022). Cancelable biometric security system based on advanced chaotic maps. The Visual Computer, 38(6), 2171-2187.

Nanda, A., Jeong, J. J., Shah, S. W. A., Nosouhi, M., & Doss, R. (2024). Examining usable security features and user perceptions of Physical Authentication Devices. Computers & Security, 139, 103664.

Smetters, D. K., & Grinter, R. E. (2002, September). Moving from the design of usable security technologies to the design of useful secure applications. In Proceedings of the 2002 workshop on New security paradigms (pp. 82-89).

Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. Mobile Information Systems, 2020(1), 8828078.