Proceedings of the 3rd International Conference on Applied Physics and Mathematical Modeling
DOI: 10.54254/2753-8818/2025.DL28334

Encryption Algorithms: Architecture, Sector - Specific Deployment, and Implementation Challenges

Zixuan Qu

School of Computer Science, Beijing University of Technology, Beijing, China
zixuan.qu@ucdconnect.ie

Abstract. Digital trust has a cornerstone, which is encryption. Encryption supports secure communications, financial stability, healthcare privacy, and national defense. This paper does a structured analysis. It analyzes symmetric, asymmetric, and elliptic-curve cryptography. Also, it looks at emerging paradigms like homomorphic and post - quantum encryption. The paper shows how these algorithms get implemented. They are implemented across different sectors. In finance, it's for mobile payments and central bank digital currencies. In healthcare, it's for electronic health records and telemedicine. In internet communications, it is for QUIC-based secure transport. In defense, it's for AES-256-protected tactical systems. By connecting cryptographic principles with case studies specific to each sector, the study highlights two things. It shows the achievements of real-world deployment. It also points out the shortcomings. There are some challenges that get special consideration. For example, there's lifecycle key management. IoT and embedded devices have performance limitations. Human error can cause vulnerabilities. There are legal and regulatory conflicts, like GDPR against the CLOUD Act. There is an urgent need for post-quantum readiness. The findings confirm something. Encryption is not just a technical safeguard. It is also a socio-technical infrastructure. The study comes to a conclusion. The development of encryption technologies is very crucial. Lightweight and quantum-resistant solutions, especially, will help shape the next -generation secure digital infrastructures.

Keywords: encryption, key management, Transport Layer Security 1.3, 5g security, post - quantum cryptography.

1. Introduction

Societies have seen changes in how they communicate, transact, and manage information. This is because digital infrastructures have expanded. In the early 20th century, encryption was mainly a military resource. Nations invested a lot in cipher machines such as the Enigma. They believed that communication confidentiality could decide the outcomes of wars. During World War II, the Allies decrypted the Enigma. It's now widely thought this cut the length of the conflict by a few years. This shows that cryptography has always been a factor in strategic strength [1].

Encryption is used in the military field. But another thing worth mentioning is that its use among civilians is even more crucial.

During the 1970s, there was a significant expansion in the civilian use of encryption. Two important developments played a key role. First, the U.S. National Institute of Standards and Technology (NIST) adopted the Data Encryption Standard (DES). Second, Diffie and Hellman invented public - key cryptography. DES is a standardized symmetric cipher. It was introduced into commerce and banking. This helped safeguard ATM networks and early electronic transactions [2]. Public-key cryptography, on the other hand, represented a theoretical revolution. It allowed two parties who had no prior interaction to establish a shared secret through an insecure channel. The RSA algorithm was introduced in 1977. It showed that mathematics could provide security without pre-shared keys. This enabled digital signatures and laid the groundwork for secure e - commerce [3].

Over the next decade, these technologies found significant applications. They gradually evolved into crucial infrastructure for major undertakings around the world. From the mid - 1990s to the early 2000s, the internet expanded. This led to a strong need for securing communication channels. Secure Sockets Layer (SSL) protocols, especially its successor, Transport Layer Security (TLS), used symmetric and asymmetric operations in an intertwined way. Session keys were set up through asymmetric operations or algorithms. Then, they were carried out via symmetric encryption algorithms like AES. At the same time, telecommunications also changed in a similar way. Cellular telephony first used some simple algorithms. These algorithms later developed into much more powerful forms. (A well-known example still in use is the GSM mobile algorithm: A5/1). Advanced mobile telecom versions, such as 4G Long Term Evolution (LTE) or the fifth - generation systems, usually called 5G by vendors, also have highly advanced cryptography protection mechanisms at the network level and for each communication [4].

How significant is that? The importance of encryption can be seen from the magnitude of contemporary threats. High-profile data breaches happened on social media platforms. As a result, data of hundreds of millions was leaked. Malware, like ransomware, targets healthcare providers. It encrypts all patient files. Then it demands payment for decryption. One such incident even caused loss of life [5]. Governments, just like financial agencies, suffer annual losses reaching billions or more. Hackers use techniques such as trying to steal online banking login credentials. Some hackers try to move funds across different banks. Sometimes they also use physical theft devices. Encryption is very important in each of these situations. In some cases, maybe even more so. That is because the promised decryption might not be possible anymore. That value and utility matters, at least to those without scruples. If the technical need matches the law, other elements can be added as part of another response. Because of this, the industry first chose a standard for its cryptography. For example, in the Payment Card Industry Data Security Standard (PCI DSS), banks or retail stores have to encrypt stored cardholder numbers. This is to prevent theft from intrusions. Here, the PCI requirement is specifically about “payment card data at rest”. Robust ciphers that only work over the exact channel must be used [6].

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) has a requirement. Healthcare providers must safeguard electronic protected health information (e - PHI). They should do this through administrative, physical, and technical means. Among these, encryption is of central importance [7]. When it comes to Europe, there is the General Data Protection Regulation (GDPR). It does not make encryption obligatory in every situation. But it does designate encryption as a recognized safeguard. This safeguard helps ensure legal data processing. It also mitigates liability in case of breaches [8]. Telecommunications standards entities, like the 3rd Generation Partnership Project (3GPP), set mandatory cipher suites for mobile networks [9]. All these references together show the extensive agreement in the industry and academia. However, the practical implications within the relevant context should be considered.

Encryption has a geopolitical aspect. Governments are in debate about mandating backdoors for law-enforcement access to encrypted communications. Privacy advocates, however, argue that these mechanisms will surely weaken security for everyone. Historically, export controls on strong cryptography were meant to stop global spread. But they did not succeed much. Now, cryptography is a technical field. It enables commerce. And at the same time, it is a policy battleground.

This paper aims to provide a structured examination of encryption algorithms. It also looks at the role these algorithms play in various fields. More specifically, the paper has several objectives. First, it will explain the architecture and principles of the main algorithm classes. Second, it will examine applications in finance, healthcare, communications, and the government sector. Third, it will talk about challenges including key management, device limitations, compliance duties, and the quantum threat. Finally, the conclusion will offer guidance to practitioners on best practices and future directions.

The paper pursues these objectives. It contributes to a comprehensive synthesis of encryption. Encryption serves as both a technical safeguard and a socio-technical infrastructure. This infrastructure is essential for sustaining digital trust.

2. Encryption algorithms

Encryption algorithms are not a single, unified thing. They represent a classification of various methods. Each method has its own unique mathematical bases, operational properties, and deployment contexts. To make things clear, this section considers three main categories. These are symmetric algorithms, asymmetric algorithms, and elliptic-curve cryptography. After that, there is a discussion about emerging paradigms.

Symmetric encryption uses the same secret key for encryption. It also uses this key for decryption. Its security is based on an assumption. That is, the key can be shared safely. And it should be kept secret from adversaries.

In 1977, DES was standardized. This marked the start of the first modern symmetric cipher that got widely deployed. DES works on 64-bit blocks and uses a 56-bit key. It has 16 rounds of substitution and permutation. DES had a lot of influence. But as computing power grew, it became vulnerable. In 1998, the Electronic Frontier Foundation's "Deep Crack" machine could find keys successfully [10]. That showed DES could be broken by brute-force attacks.

The Advanced Encryption Standard (AES) is based on the Rijndael algorithm. There was an open international competition. NIST selected AES in 2001. It replaced DES. AES uses substitution–permutation networks. These networks operate on 128-bit blocks. The key sizes can be 128, 192, or 256 bits. Its mathematical structure depends on operations in the finite field GF(2^8). Governments have made AES mandatory. Virtually all software and hardware platforms support it. AES has become the de-facto global standard for symmetric encryption [11].

Symmetric encryption is efficient. It brings about high throughput. This throughput is suitable for bulk data encryption. When combined with certain operation modes, its effectiveness is especially remarkable. These modes offer authenticated encryption along with associated data (AEAD). Galois/Counter Mode (GCM) is widely preferred at present. It provides confidentiality, integrity, and authenticity in a single primitive. Also, it can support parallelizable implementations [12].

The problem of key distribution is solved by public - key or asymmetric encryption. This type of encryption uses two keys. These two keys are interconnected mathematically. One is the public key.

It's suitable for open sharing. The other is the private key. It needs to be kept strictly secret. Messages encrypted with the public key can only be decrypted with the corresponding private key.

The RSA algorithm is the archetypal public-key system. It was published in 1977. The RSA algorithm relies on the intractability of factoring the product of two large prime numbers. In a typical RSA setup, a modulus of 2048 bits or greater is used. This provides adequate security against contemporary adversaries. RSA also makes digital signatures possible. First use a private key to sign a message. Then it can be verified with the corresponding public key. This guarantees authenticity and non-repudiation [13].

RSA has its drawbacks. First, its operations are slow. Also, it needs key sizes that can resist attacks using newly developed factorization techniques. For many current uses, elliptic curve is better than RSA. Elliptic curves cryptography (ECC) is based on the algebra of structures on elliptic curves defined over finite fields. The idea depends on the difficulty of a computational problem. This problem is called the elliptic curve discrete logarithm problem. Compared with RSA, ECC can get the same strength with smaller-sized keys. For example, 256-bit-sized keys in ECC offer the same security as 3072-bit keys in RSA [13]. With the same security strength, ECC uses less processing time, needs a faster runtime, and requires fewer key - sized numbers than traditional symmetric cryptosystems. So overall, it costs less. ECC provides fast and secure exchange protocols like Eliptics Curves Diffie - Hellman (EC DH). It also offers digital signature schemes such as Edwards - Curves Digital Signature Algorithm (EdDSA). RFC7748 designates two curves. X25519 (Curve25519) is for Secure Key Exchanges, and Ed25519 is for signature - making. Both have been widely used. They are especially useful in recent protocols for secure communications, user identification, and identification and authentication in apps like Signal, WhatsApp, and TLS etc. This advantage cuts down on computational power usage [14]. The efficient key sizes make it convenient even for devices with limited capabilities, like smartphones and sensors. Smart devices are modern technologies with low data - encryption capabilities. ECC allows these modern devices to securely process, transmit, and exchange sensitive data over insecure mediums effectively. Its importance is more obvious especially when system processes may face resource shortages. As a result, ECC has become the standard in almost all existing implementations. These include TLS 1.3, mobile signaling technology standards like 5G wireless communication system standards, and also WPA-3 with the Wi-Fi encryption standard WPA3 256 - bit password-protected [15].

In actual operation, systems rarely use asymmetric algorithms to encrypt large amounts of data. Instead, they adopt hybrid protocols. Take TLS 1.3 as an example. First, it uses ECC for ephemeral key exchange. This is to establish a session key. After that, it relies on AES-GCM or ChaCha20-Poly1305 to efficiently encrypt data streams symmetrically [16]. This hybrid approach takes advantage of the strengths of both algorithm families.

Classical algorithms have their constraints. These constraints have instigated the exploration of novel cryptographic paradigms. Homomorphic encryption is a technique. It allows computations on ciphertexts without decryption. This technique facilitates privacy - preserving analytics in healthcare and finance [17]. Lattice-based constructions come with computational demands. Initially, it seemed the demands made practical implementations unfeasible. But advancements in these constructions have made limited practical implementations viable.

The quantum threat is more urgent. Quantum computers, if they can be scaled up, might run Shor’s algorithm. This algorithm is for factoring RSA moduli and solving the ECDLP. As a result, most public - key systems could be broken. In response, NIST has started the Post - Quantum Cryptography (PQC) standardization process. It picked algorithms such as Kyber (key encapsulation) and Dilithium (digital signatures) for future use [18]. Organisations are advised to prepare for hybrid deployments. These deployments combine classical and PQC algorithms. This ensures long-term confidentiality.

3. Applications

In the finance field, encryption is used. It helps maintain the security of online banking systems, payment apps, and digital currencies. Alipay and Apple Pay use tokenization and AES encryption. They do this to protect user credentials and transaction processes. China's Digital Yuan pilots include dual offline encryption mechanisms. This ensures that transfers can be executed securely even without network connectivity. After significant security breaches, SWIFT has a different approach. Through its Customer Security Programme, it enforces strict cryptographic controls.

Encryption is used in healthcare systems to safeguard patient data. Epic's EHR platform encrypts static records with AES - 256. For transmission, TLS 1.3 is used. During the COVID-19 pandemic, telemedicine platforms adopted end - to - end encryption. They did this to meet HIPAA requirements and keep patient information confidential.

In the field of communications, encryption is used to ensure the security of internet and mobile services. Google developed the QUIC protocol. It powers YouTube and Google Meet. This protocol includes TLS 1.3. During this process, it encrypts payloads and metadata. When it comes to mobile 5G networks, SUCI is used to hide subscriber identities. Elliptic-curve encryption is used in this step.

Encryption implementation happens in governments, defense, and national security agencies too. China has started an electronic government encryption gateway plan. This plan targets all sectors. It aims to make sure data communication is secure across government-wide and international digital government portals. In the U.S. military forces' military organizations, AES with 128 and 256 bit encryption levels is required. Specifically, in recent times, 256 - bit encryption has been used to protect tactical radios and GPS satellites in war zones. Defense contractors also need to meet certain testing standards before deploying equipment. One requirement is to use secure encryption for any communications between systems. In Europe, more users have been using cross - border cloud - based web services in recent years. Under the General Data Protection Regulation (GDPR), strict enforcement of cryptographic security has been adopted. Encrypted communications offer a secure platform for developing secure algorithms. These algorithms are based on trust relationships within a particular context.

In the world of finance, encryption is of great importance. It has multiple roles. Firstly, it safeguards monetary value. Secondly, it ensures regulatory compliance. Thirdly, it maintains trust in global payment systems. Financial institutions use encryption for account numbers, customer authentication information, and transaction records when these are being stored or transmitted. The Payment Card Industry Data Security Standard (PCI DSS) requires merchants and processors to adopt strong cryptographic methods. They also need to practice secure key management [19]. Online banking platforms usually use TLS 1.3 along with certificate-based authentication. This is to lower risks related to phishing attacks and man-in-the-middle threats.

Interbank transactions further show this dependence on encryption. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) connects over 11,000 institutions around the world. It enforces multi-layered cryptographic protections in its messaging platform.

After major breaches happened. SWIFT came up with the Customer Security Programme. This programme required strong encryption, secure key management, and strict audit practices [20].

Digital assets have emerged, bringing in new cryptographic elements. Bitcoin uses elliptic - curve signatures (ECDSA over secp256k1) to protect ownership. Ethereum, on the other hand, extends cryptographic mechanisms to the execution of smart contracts [21]. Besides these decentralized systems, central banks are exploring Central Bank Digital Currencies (CBDCs). The People’s Bank of China (Digital Yuan) and the European Central Bank (Digital Euro) have launched pilot projects. These initiatives use encryption to ensure privacy and accountability. Their goal is to prevent double spending and allow regulatory supervision [22]. These systems need to strike complex balances. They have to balance individual confidentiality, state monetary governance, and resistance to cyberattacks.

Healthcare organizations process vast amounts of sensitive data. This data ranges from patient records to genomic sequences. Breaches can harm individuals. The harm is not just financial, but can also be irreparable. In the United States, HIPAA requires providers to set up safeguards. One of these safeguards is the encryption of e - PHI during both storage and transmission [23]. European regulators enforce GDPR. It clearly lists encryption as a way to ensure legal processing. Also, it helps reduce liability if breaches occur [8].

For local storage, Electronic health record (EHR) systems use AES. When it comes to secure transmission across hospital networks, they utilize TLS 1.3. Telemedicine saw a dramatic growth during the COVID - 19 pandemic. It depends on encrypted video conferencing and authenticated device communication. Robust end-to-end protection is crucial. Otherwise, patient confidentiality would be unachievable [24].

The aim of emerging technologies is to pursue reconciling data utility and privacy. Homomorphic encryption gives researchers the ability to do statistical analysis on encrypted medical datasets. At the same time, it stops the underlying patient information from being disclosed [17]. Multi - party computation allows different hospitals to jointly compute over distributed data. It does not expose the raw records. These techniques might enable collaborative research and AI - driven diagnostics. Also, they can reduce the risks of re - identification [25].

Encryption is the basis of nearly all forms of modern communication. The Hypertext Transfer Protocol Secure (HTTPS) is now enforced by default across major web browsers. It uses TLS 1.3. What's its purpose? It aims to prevent eavesdropping and tampering. Messaging platforms like Signal and WhatsApp implement end-to-end encryption. They use the Double Ratchet protocol. This comes with forward secrecy and post-compromise security. It ensures confidentiality even if long-term keys are compromised.

Cryptography integration is a characteristic of transport protocols. QUIC, which was standardized by the IETF and developed by Google, combines the cryptographic and transport layers. This combination enables faster and more secure connections. QUIC encrypts not only payloads but also a large part of transport metadata. By doing this, it can resist traffic analysis.

Mobile networks still represent critical infrastructure. In 5G, 3GPP has made a rule. For both control - plane and user - plane traffic, encryption is a must. It comes with enhanced algorithms and key separation mechanisms. SUCI is used to hide subscription identifiers. This protects subscriber privacy from passive interception. Satellite communications and IoT deployments expand the cryptographic perimeter. Lightweight algorithms, ECC, and pre-shared keys are designed for devices with strict resource constraints.

Encryption is a critical element. Government agencies rely on it for diplomacy, classified communications, and national defense. Among standards, the U.S. Commercial National Security Algorithm Suite has mandates. For example, AES-256, SHA-384, and elliptic-curve algorithms should remain in use until post-quantum replacements are available. Defense networks are used in satellite uplinks, secure radios, and tactical cloud systems. They utilize layered cryptography.

Policy debates also see the intersection of encryption. Some governments support “lawful access” mechanisms. Under court order, these mechanisms would allow law enforcement to bypass encryption. Security experts always warn that such backdoors weaken security for all users. They lead to systemic vulnerabilities. Another area of contention is the persistence of cryptography export controls. Regarding this, states try to balance national security interests and commercial competitiveness. In cross - border situations, encryption is more and more seen as both a human right. It safeguards privacy and free expression. Also, it's an aspect of sovereignty.

4. Implementation challenges

Key management has its weaknesses. When institutions mismanage keys, even strong algorithms may not work well. Auditable hardware security modules and automated rotation systems are essential. They help prevent compromise. Performance issues affect IoT and embedded devices. ECC can reduce the computational load. But for large-scale secure device deployments, lightweight algorithms and hardware acceleration are still needed. Human errors can undermine encryption. Weak passwords, misconfigured certificates, and leaked private keys can all lead to breaches. The OpenSSL Heartbleed vulnerability exploited a weak component. Adversaries could eavesdrop on encrypted web traffic globally by intercepting the TLS hand - shake protocol. Legal conflicts make encryption complicated. Europe's GDPR requires strict personal data protection. The CLOUD Act, though, allows Americans abroad or remotely working in the EU to access personal digital data stored by US corporations, no matter where it is. Businesses and governments need to reconcile laws without splitting internal processes into different sub-systems. In the next few decades, quantum computing will threaten everything built on cryptanalysis. Transitioning to post - quantum methods will need new algorithms. Maybe there is a need to maintain hybrid networks. These networks support classical cryptographic schemes and proposed post - quantum ciphers at the same time. Careful planning ensures that even if future adversaries could decrypt information now, they would not be able to later. The security lifecycle, especially managing cryptographic keys, is another reason for system vulnerability. Best practices can guide the development of more secure key management. They suggest using cryptographically random number generation to create keys. Then, proper storage, distribution, use, rotation, and destruction should be tracked during the encryption process. Key storage methods suggest putting secret information in more secure places like HSMs and Trusted Platforms. During communication, the transport mechanism requires parties to authenticate each other. Then they can exchange content via secure TLS sessions. This prevents eavesdropping without prior permission. PKI improves communication authenticity when multiple parties rely on shared identities in the same framework. It gets rid of individual identification. Secure key storage environments let parties keep records. These records track different types of encryptions and monitor key lifetimes. Destruction should use cryptographic techniques. These techniques either make retrieval methods hard to find or destroy the media completely. This avoids manual identification. Properly storing keys for future erasure means not leaving any leftovers on possible access paths. Maintaining records for each step in encryption cycles gives organizations more flexibility to follow unknown regulations. IoT sensors, mobile and embedded endpoints do not have enough capability to use standard public - key algorithms.

Lightweight cryptography, like PRESENT, KLEIN, or SPECK, offers secure choices. It only requires minimal hardware. Elliptic curve cryptography (ECC) is much smaller than RSA for similar security levels. This helps to minimize computational efforts. Symmetric Authenticated Encryption with Associated Data (AEAD), such as AES - GCM or ChaCha20 - Poly1305, provides symmetric confidentiality. It also guards against tampering. The low - latency overhead adds more cryptographic capabilities. There are other approaches. They include session resumption, pre-shared crypto keys, and cryptographic offloading from device endpoints by nearby gateways. 5G can help. It might allow ephemeral key usage. It also separates control and user-plane functions. This reduces attack exposure. System design has to consider two things. One is the need for a secure, computationally intensive configuration. The other is the manageability of larger data-storage elements. Strong encryption can cause problems for some applications. These applications need more access to encrypted material for analysis. Homomorphic encryption (HE) is a special form of algorithms. They are designed for computation without decryption. HE maintains data confidentiality, especially in sectors like healthcare, finance, or government. Combining HE with differential privacy (DP) ensures something. No matter how the algorithm works on the aggregated output, identification won't lead to a breach. But HE brings performance penalties. These penalties increase as the complexity in terms of noise and parameters goes up. Hybrid techniques can be used. They selectively use HE when computation involves crucial calculations. This balances the cost of HE. At the same time, it keeps the utility of conventionally encrypted pipelines. System designers must think carefully about the attack model. They need to evaluate how different cryptanalytic threats affect the confidentiality of the data-management-process. DP tries to get strong confidentiality. It does this by quantitatively limiting knowledge. HE does the same by encrypting computation while protecting identity. These two have complementary strengths. To evaluate them, both models aim to provide strong confidentiality without being attacked. Nowadays people are facing a serious threat. More powerful quantum- processor-equipped computer systems are coming. They enable Shor's Algorithm to factor large primes used by RSA in real - time. They can also solve the Elliptic Curve Discrete Logarithm Problem (ECDLP). This exposes any asymmetrical key length. Conventional Asymmetrical Public-Key Cryptographic methods can not rely on safe exposure time anymore. As a first step, NIST started the selection of Post - Quantum Cryptography (PQC) algorithms. Examples are Kyber (key encapsulation) and Dilithium (digital signature). Applications are recommended to use a mix of classical and post - quantum PQC during the transition period. Especially because existing applications can't handle PQC computation without big changes. Organizations have to think about two things. One is avoiding “harvest - now, decrypt - later” risks. The other is replacing some system infrastructure. This is to meet PQC computational demands without hurting system and data - pipeline performance.

5. Conclusion

Various sectors, including finance, medical, communications, and governmental organizations, design and utilize encryption algorithms. This has always been the popular topic people review and do examination. The practical context of applying academic research in cryptography has become intertwined. Challenges related to using encryption algorithms are discussed. These include issues about key usage, performance in constrained applications like IoCs, human errors, legal conflicts, and the emerging threat of quantum computation. This work found that cryptography plays a crucial role in maintaining trust within the communication grid. Encryption makes secure transactions possible among different parties across industries. It safeguards the handling of medical records. It also ensures national cybersecurity, and provides assurance for electronic communications and identities. Symmetric cryptosystems, such as AES, can encrypt large volumes of data efficiently. Public key-based cryptosystems or elliptic curves allow for private key sharing and secure message signing. Combined cryptography solutions, like those in protocols such as TLS v1.3, ensure robustness and good performance in real-world implementations. But the usage itself, especially proper implementation, brings challenges. There's a need for information on secret management.

Also, there are performance limitations due to resource - constrained computing in IoCs or human reliance. And legal oversight adds complexities to providing secure encrypted communications across different applications in an industry-specific way. Newer technologies question conventional ways of designing encryption algorithms. They may lack confidentiality assurance. Through this study, when evaluating viable and efficient cryptographic frameworks and techniques successfully used in several digital systems across sectors, researchers can address priority without too much burden through the cryptographic methods shown here. In doing so, practical examples of cryptography applied closely to engineering utilization have been given. This minimizes unnecessary burdens on users when they transmit and receive encrypted traffic reliably over scalable information grids. It also maintains anonymity, correctness, and reliability for users according to legal and ethical principles followed globally. This essay mainly focused on documented cases in major companies and government departments worldwide using encryption at commercial or government levels. Potentially higher-classified or proprietary implementations in other environments is not considered. Those could involve more trade-offs than this work shows. In some cases, theoretical studies might gain from hands-on experiments using libraries for cryptosystems implemented on existing research platform architectures. For the future evaluation of encrypted packet transmissions, conducting large-scale analysis of various IoT infrastructures is a good choice. Using packet capture for encrypted network traffic can be helpful too.

Comparative evaluations can identify alternatives. These alternatives have similar functionality but lower overhead in respective applications. Or they have stronger computational integrity assurance against emerging threats, like zero-day exploits. Proposals for newer schemes are new exploration areas. These schemes have more functional homomorphic properties, and the goal is similar. This coordinated effort has implications for crypto policies. The implications are on a larger international scale. It aims for better interoperability. This can balance privacy concerns across global border jurisdiction interests. At the same time, it preserves national and organizational interests related to enforcement and law-related activities. Initially, it is thought that this can be achieved alone. But in fact, collaborations are needed. Collaborations among professional industry stakeholders, academics in the cryptographic field, and experts, officials, and politicians from different scientific domains are required. The goal is to achieve an overarching, comprehensive, interdisciplinary work. This work ensures the ability to tackle ongoing and expected threats. These threats emerge in previously unexplored areas.

References

[1] Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. 21(2), 120–126.

[2] Diffie, W., & Hellman, M. (1976). New directions in cryptography. 22(6), 644–654.

[3] Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. 28(2), 270–299.

[4] Boneh, D., & Shoup, V. (2020). Draft manuscript.

[5] Katz, J., & Lindell, Y. (2020). (3rd ed.). CRC Press.

[6] Chen, H., Laine, K., & Rindal, P. (2020). Homomorphic encryption for machine learning. 10(4), 255–272.

[7] Albrecht, M. R., Player, R., & Scott, S. (2021). On the concrete hardness of Learning with Errors. 34(2), 421–456.

[8] Liu, Y., & Xu, Q. (2021). Secure federated learning: Threats, privacy and incentives. 16, 719–734.

[9] Zhang, T., et al. (2022). Practical post-quantum hybrid TLS deployment: experiences and challenges. 1243–1260.

[10] Chen, L., et al. (2022). Lightweight cryptography for IoT: a survey and performance evaluation. 54(6), Article 121.

[11] Wang, S., et al. (2023). Blockchain privacy and anti-frontier techniques: a review. 25(1), 1–34.

[12] Kapoor, R., & Singh, A. (2021). Secure EHR systems: cryptographic primitives and deployment practices. 45(11), 98–112.

[13] Miller, A., & Roberts, J. (2020). Analysis of TLS 1.3 adoption and security in modern browsers. 89–102.

[14] Soto, P., et al. (2024). Post-quantum signature usage in practical systems: benchmarking and interoperability. 22(2), 45–58.

[15] Patel, N., & Gomez, R. (2022). Privacy-preserving analytics in healthcare with homomorphic encryption and secure multiparty computation. 129, 104075.

[16] Brakerski, Z., & Vaikuntanathan, V. (2020). Efficient fully homomorphic encryption from (standard) LWE. 49(5), 1166–1198.

[17] Bindel, N., Brendel, J., Fischlin, M., et al. (2021). Hybrid key encapsulation mechanisms: Post-quantum security and practical performance. 1005–1020.

[18] NIST. (2001). FIPS PUB 197: Advanced Encryption Standard (AES).

[19] Rescorla, E. (2018). RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3.

[20] Iyengar, J., & Thomson, M. (2021). RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport.

[21] PCI Security Standards Council. (2022). Payment Card Industry Data Security Standard (PCI DSS) v4.0.

[22] U.S. Department of Health and Human Services. (2013). HIPAA Security Rule Guidance.

[23] European Union. (2016). General Data Protection Regulation (GDPR).

[24] 3GPP. (2022). TS 33.501: Security Architecture and Procedures for 5G System.

[25] NIST. (2022). Post-Quantum Cryptography Standardization (Kyber, Dilithium, SPHINCS+).