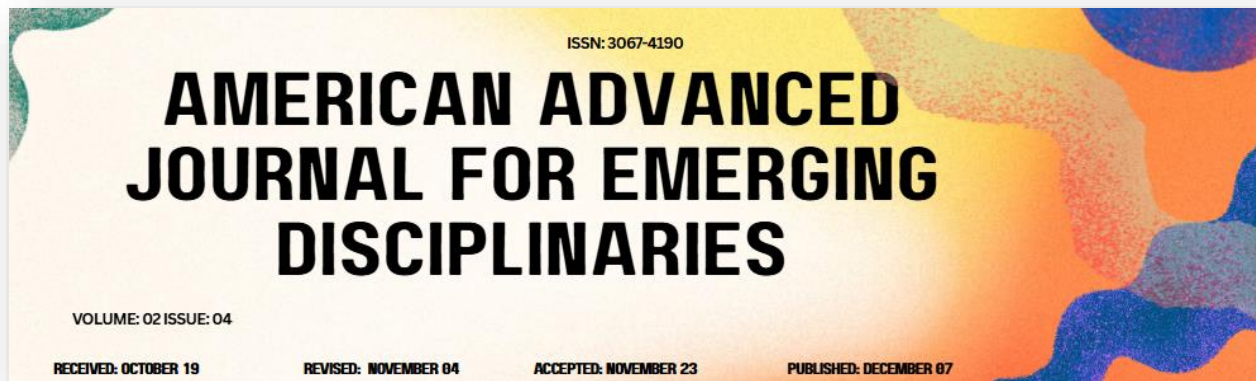




Safeguarding Digital Sovereignty in the Quantum Era

Dileep Valiki

Independent Researcher

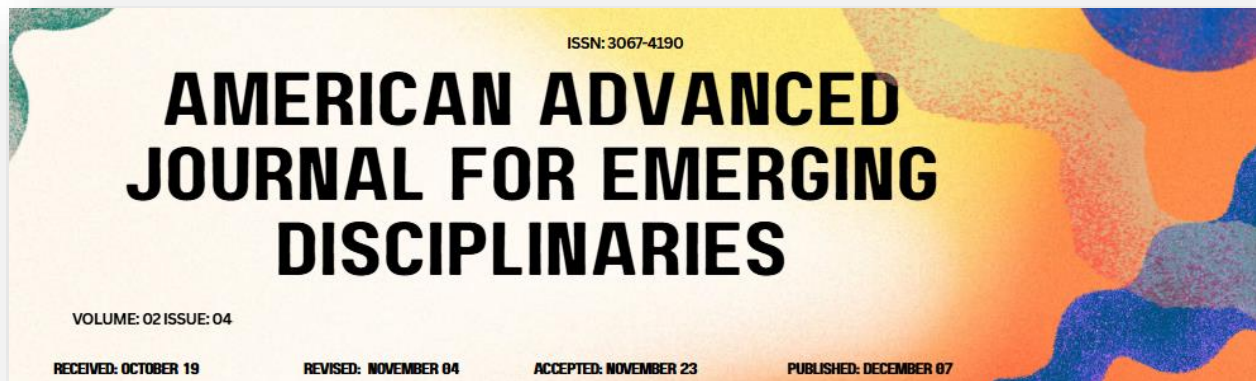
valiki.dileep.researcher@gmail.com

Abstract

Digital sovereignty encompasses a nation or region's control over information and services crucial to the nation state. This involves making essential decisions about security, economic, ethical, and political factors contributing to the provisioning of those services. National digital sovereignty risk being compromised when critical services such as authentication, signing, encryption, or confidentiality are provided by foreign providers. Sovereignty in general can also be considered more broadly at the regional level and include other service attributes, such as resilience, diversity of supply, and quality.

The increasing arrival of quantum computers will undermine classical public-key cryptography. Although the development of practical quantum computers is not imminent, governments, regulators, and other owners of critical infrastructure must urgently begin adopting post-quantum key-management solutions as part of a wider digital-sovereignty strategy. Failure to do so will not only compromise the confidentiality and integrity of data exchanged over many years, but also introduce a risk of undetected abuse of those communications during the transition. The increasing arrival of quantum computers will undermine classical public-key cryptography. Although the development of practical quantum computers is not imminent, governments, regulators, and other owners of critical infrastructure must urgently begin adopting post-quantum key-management solutions as part of a wider digital-sovereignty strategy. Failure to do so will not only compromise the confidentiality and integrity of data exchanged over many years, but also introduce a risk of undetected abuse of those communications during the transition.

Keywords: Digital Sovereignty, National Information Control, Critical Digital Services, Cryptographic Independence, Foreign Provider Risk, Authentication Infrastructure, Encryption And Confidentiality, Resilient Digital Systems, Supply Chain Diversity, Service Quality Assurance, Quantum Computing Impact, Classical Cryptography Vulnerability, Public-Key Cryptography Breakdown, Post-Quantum Cryptography Adoption, Post-Quantum Key Management, Critical Infrastructure Protection, Data Confidentiality And Integrity, Transition-Phase Security Risks, Long-Term Communication Security, Sovereignty-Oriented Cyber Strategy.



1. Introduction

Digital sovereignty denotes a jurisdiction's capacity to control the digital space of its territory according to its values and interests and engage in trustworthy cross-border communication. In the post-quantum era, technological shifts will impose new, urgent demands for national control of the digital space, secure and resilient operation of national critical infrastructures, and long-term confidentiality and integrity of sensitive data. A full-cycle post-quantum cryptographic framework provides direction for mitigating the associated risks, from threat assessment through deployment considerations to potential policy and social implications.

Governments, especially in technologically advanced countries, are taking steps to formalize a strategy for a controlled transition to post-quantum cryptography (PQC). Risk-mitigation objectives involve not only the reinforcement of sovereign digital-space control but also the preservation of customer trust and avoidance of potential financial losses. The required measures cut across regulatory, economic, and technical domains and should be shaped in coherence with broader considerations for digital sovereignty and national security—notably, protection against hostile technological dominance and the economic and political consequences that may follow.

1.1. Overview of Digital Sovereignty and the Need for Post-Quantum Cryptography

Digital sovereignty encompasses the demand for greater national jurisdiction and control over data, computing, and communication resources, economies, rights, and survival. These freedoms are primarily the state's responsibility, but national security, economy, critical infrastructure, and

society depend on the secrecy and integrity of almost all tap-water-size digital information.

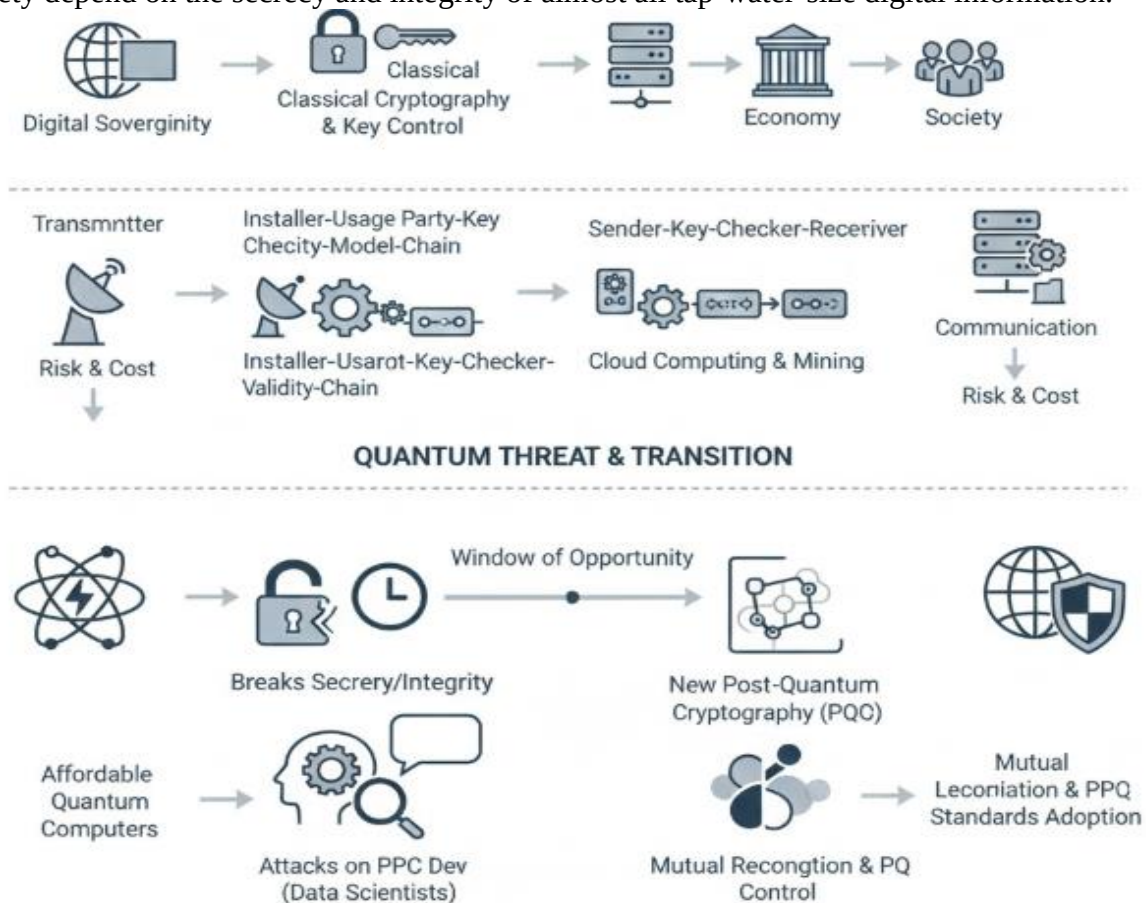
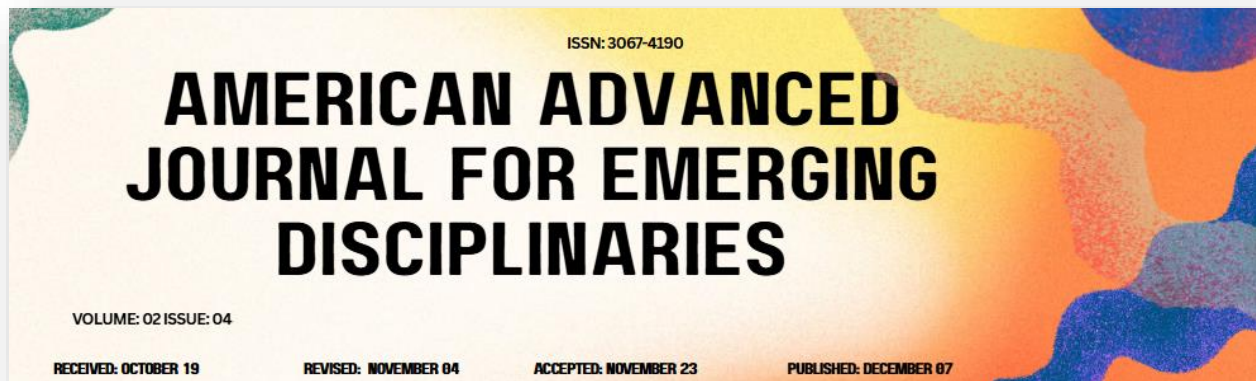


Fig 1: Securing the Sovereign Digital Frontier: Strategic Post-Quantum Transitioning and the Geopolitics of Jurisdictional Data Control

Classical cryptography and sovereign control over keys guarantee these aspects in the short-to-medium term. Transmitter-receiver pairs follow the sender-key-checker-receiver model, but the installer-usage party-key-checker-validity-model-chain paradigm applies to wider areas, such as content-sharing in cloud computing or mining. The enormous deployment of cryptography, especially key management devices, gives a hint on the risk and cost of any aspect



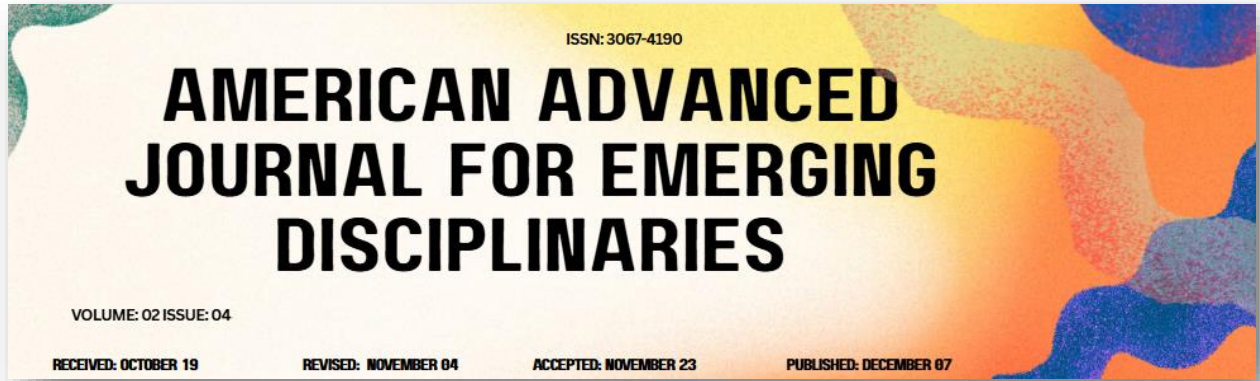
of their are operation. It should not be surprising, then, that the advent of affordable quantum computers endangers the very cryptographic principles that underpin secrecy and integrity.

The period before massive quantum computers appear and cost-efficiently break cryptography, especially invisible-key-based schemes, such as transport-layer-security, is a window of opportunity for allowing the transition to new cryptography based on new hard problems. Attacks on post-quantum cryptography development by trained data scientists trying to cheat their way to victory through blending rightful work with vault differ compared to pure market-economy approaches, and some differences need dedicated consideration. The promotion of data localization through various kinds of jurisdictional control, when suitably accepted, may also facilitate the adoption of post-quantum cryptography through eventual mutual recognition of civil-infra-political alliance structures based on the regional technical adoption of post-quantum mechanisms and standards.

2. The Imperative for Post-Quantum Cryptography in Digital Sovereignty

Post-quantum cryptography is a prerequisite for sovereign control not only over data but also over the critical infrastructure that retains the capability to respond to crises and offers long-term confidentiality and integrity. No single entity can fully ensure the viability and integrity of the data. While exposing but supposedly encrypted data under minimal authorization is undesirable, the preventive use of more secure post-quantum replacements offers a potential mitigation. An important soft component, especially for developing and transition economies, is that the least-privileged scarcities can be allowed to trade with debt while transcending identity and credit verifiability issues. The requirement is the ability to effectively and swiftly access or respond to such infra-marginal needs without jeopardizing either sovereignty or long-term confidentiality and integrity of the data traversing across a region or even globally.

Four strategic imperatives can be distilled from the earlier discussion: (i) Foster PQC deployment and adoption to mitigate risks associated with near-term quantum computing capabilities; (ii) Facilitate the PCI of critical infrastructure and ecosystem systems in line with national economic and security priorities to ensure sovereignty and resilience; (iii) Address long-term data confidentiality and integrity requirements in the presence of a fully-fledged quantum adversary; and (iv) Initiate research and practical efforts for the lossless archival of data on current or older classical systems and infrastructures to identify workable solutions that will be



technologically, operationally, and investment-wise appropriate for the least-privileged regions and nations, especially in the aftermath of crises or wars.

Equation A) Multivariate polynomial scheme (MPS) function and hardness statement

The states a multivariate mapping (public key) and a security goal:

- A multivariate polynomial function F from n variables over a finite field $\mathbb{F}_q$ to $\mathbb{F}_q$, and
- Security based on solving a system of n equations in n unknowns, or finding a common root of n polynomials of degree $d > 2$.

Step-by-step formalization (what the text describes):

1. Finite field and vector space

- Let $\mathbb{F}_q$ be a finite field with q elements.
- The space of n -tuples is $\mathbb{F}_q^n$.

2. Public map as a system of polynomials

- Define $F: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ by

$$F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$$

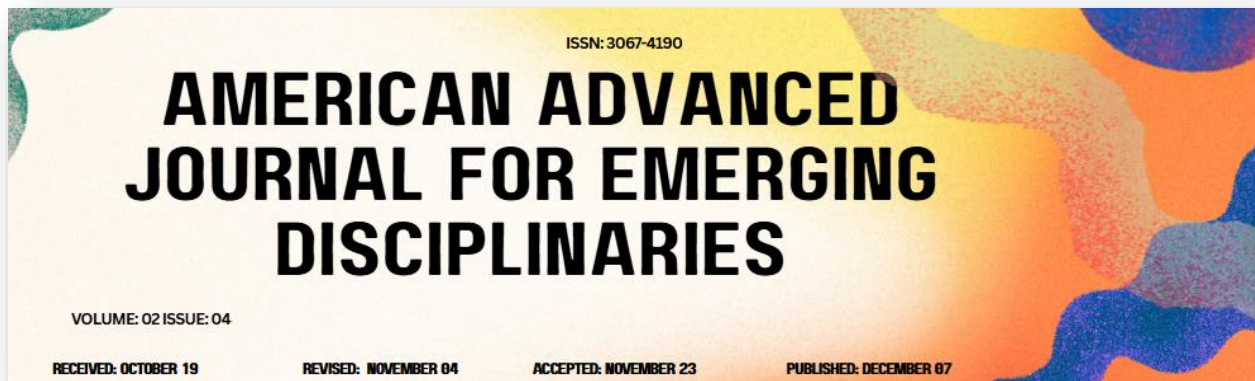
where each f_i is a multivariate polynomial over $\mathbb{F}_q$.

- (The paper shows the type signature in text: $F: \mathbb{F}_q^n \rightarrow \mathbb{F}_q$, but the *security goal* “ n polynomials in n variables” is naturally the vector form above; either way the hardness is “solve polynomial equations.”)

3. Inversion / preimage problem

- Given an output y , an attacker tries to find a preimage x such that

$$F(x) = y$$



- Expanded as equations:

$$\begin{cases} f_1(x_1, \dots, x_n) = y_1 \\ \vdots \\ f_n(x_1, \dots, x_n) = y_n \end{cases}$$

- This is exactly “solve a system of equations.”

4. “Common root” statement (signatures)

- “Finding a common root of n polynomials of degree d in n variables, $d > 2$ ” means: find $x \in \mathbb{F}_q^n$ such that

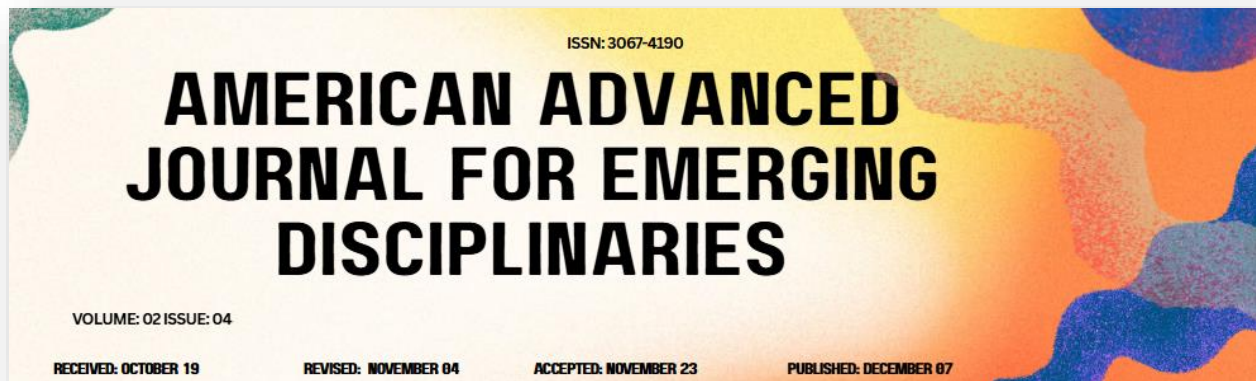
$$f_1(x) = 0, f_2(x) = 0, \dots, f_n(x) = 0$$

with each f_i having total degree $d > 2$.

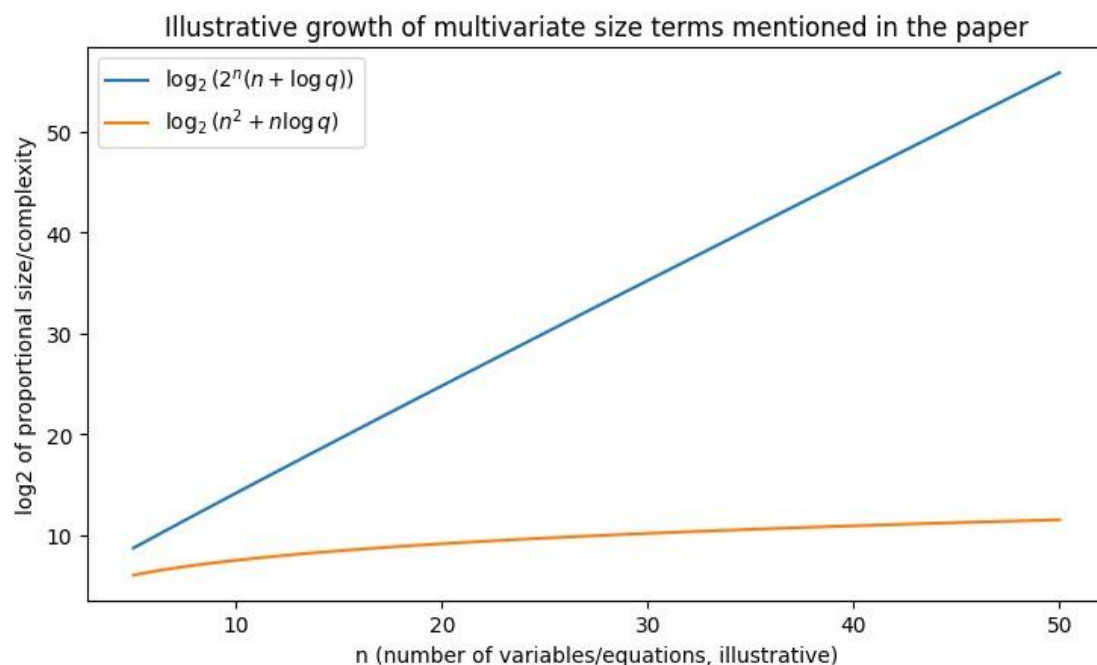
2.1. Strategic Imperatives for Implementing Post-Quantum Cryptography

National and global policy frameworks must support sovereign digital sovereignty by implementing post-quantum cryptography as part of a broader digital infrastructure. Priority areas are: achieving sovereign control over internet communication security—particularly the ability to defend against, respond to, and exploit quantum adversaries, as well as the capacity to ensure long-term evolution of deployed systems; securing digital sovereignty by guaranteeing that critical national and regional infrastructure can withstand post-quantum events; enabling the future-proofing, long-term confidentiality, and long-term integrity of sensitive data superseding classical assets; and protecting national security and economic interests by reducing reliance on external parties and jurisdictions.

To meet these strategic interests and requirements, an urgent roadmap must identify the combinations of threats and scenarios that would necessitate action before the proven ability of quantum computers to compromise classical cryptography, temporal limits, effective mitigation measures, and possible early steps. The current threat model assumes that it remains infeasible for adversaries to harvest large quantities of classic SSL/TLS and other signature-based public key exchanges for later decryption; however, it also acknowledges active attempts by hostile powers to build quantum capabilities to decrypt classical crypto. Any such capability is poised to attract minimal international use of classical key exchange; classical-signature-based trust will



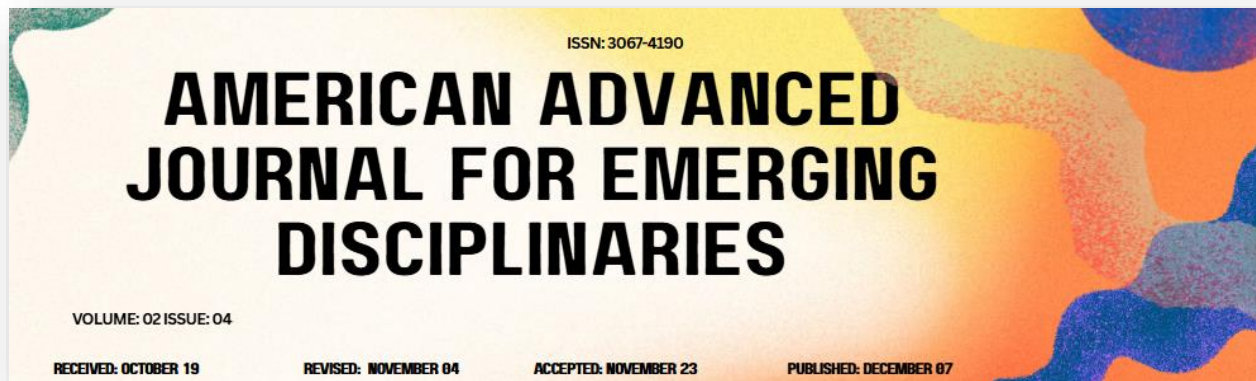
then be replaceable at low cost by the use of non-quantum asymmetric crypto agreed under digital schemes with confidentiality during operation. If critical capabilities beyond those of any threat are assured, attention naturally shifts to other real-world elements of risk and capability, such as quantum-assisted attacks on lattice-based key-agreeing schemes or long-term harvesting against signature schemes.



3. Foundations of Post-Quantum Cryptography

Post-Quantum Cryptographic Frameworks for Securing Digital Sovereignty

The foundations of post-quantum cryptography are based on problems from diverse areas of mathematics, offering different security assumptions against quantum attackers. Lattice-based primitives supported by the NIST process have generated the highest interest, but sufficiently generic, cage-based constructions do not follow the convert-and-guess paradigm. In addition to these categories, the multivariate polynomial scheme (MPS) family established the analogy with zero-knowledge identification schemes, hinted hardness in the hidden multilayer function

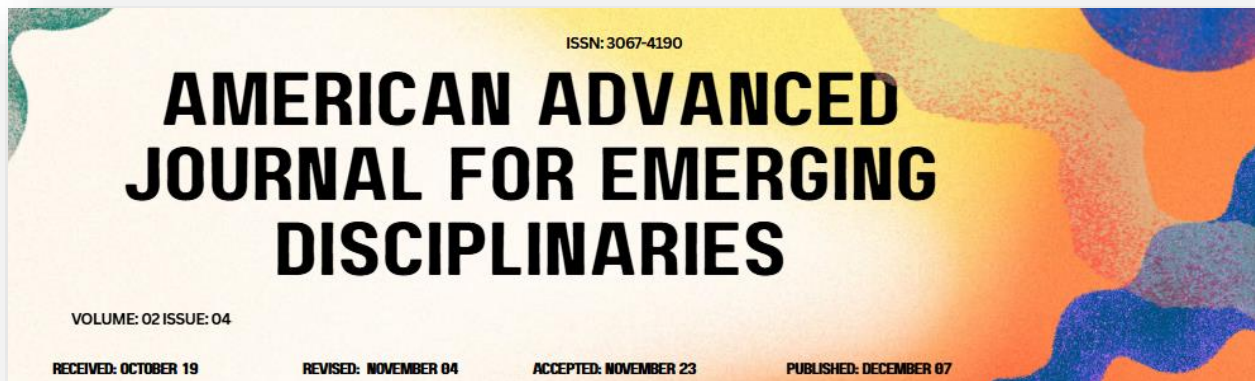


problem, and showed its suitability for public-key encryption, digital signatures, and key encapsulation mechanisms. Nevertheless, no MPS has yet reached the fully fledged state. Even so, many candidates exist for alternative configurations, enabling the investigation of new ideas, with a current key/signature size of 56/96 bytes.

Lattice-based primitives such as NTRU or its KEM, FAL, and the hardness of SIS or LWE problems constitute the core of PKC's post-quantum cryptography jungle. Standardization activities help suit the families for an ever-growing variety of tasks. Key sizes range from a few hundred bits of NTRU for high-security aims to 2/3K-LWE for 128 bits. Performance considerations combine decryption and signature speeds 0(30K) times lower than those of classic RSA at comparable key sizes. Practical implementations cover 512-bit NTRU and key encapsulation mechanism vectors giving the same security level. NIST supports the search for KEM/FAL candidates in the trapdoor proposal.

3.1. Lattice-Based Primitives

Lattices are among the most studied objects in post-quantum cryptography. NTRU is one of the oldest lattice-based problems, invented in 1996 for encryption, and NTRUEncrypt served as the basis for the level 2 ASN sign scheme. In 2003, the KEM variant was the first KEM accepted by NESSIE. More recently, an extremely compact KEM, NTRU-HRSS, was selected as the KEM of SPHINCS and proposed for NIST standardization. Other lattice-based primitives include constructions based on the Short Integer Solution and Learning With Errors problems. While these primitives are less informative, the hardness of SIS and LWE is shown to relate to that of decisional Learning With Errors. Both are multivariate problems, for which their NESSIE and



NIST candidates are Easy and NTRUPrime.

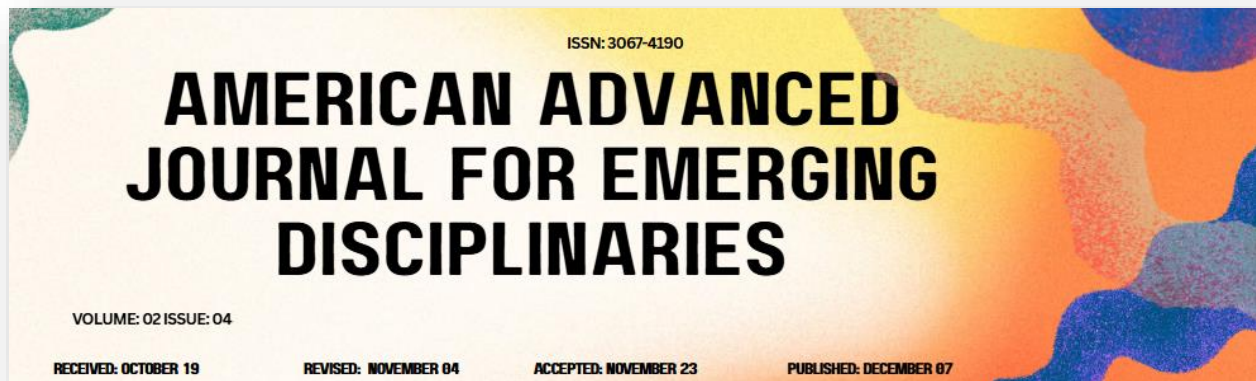


Fig 2: Lattice-Based Cryptographic Resilience: From NTRU Foundations to Post-Quantum Sovereign Security Architectures

Post-Quantum Cryptography is essential to preserve sovereign control over key exchanges and signatures, to make critical infrastructures resilient to the quantum computer threat, and to ensure long-term confidentiality and integrity of sensitive information. Furthermore, while the immediate focus must be on KEMs and signing schemes with post-quantum security levels, Medium-term goals include key encapsulation in performance-sensitive areas, authentication mechanisms for high-security contexts, and support for data in-flight and data-at-rest scenarios.

3.2. Multivariate Polynomial Schemes

In multivariate cryptography, the public key is a multivariate polynomial function, whose image under a random choice of the private key is a random value in the base field. The attacker



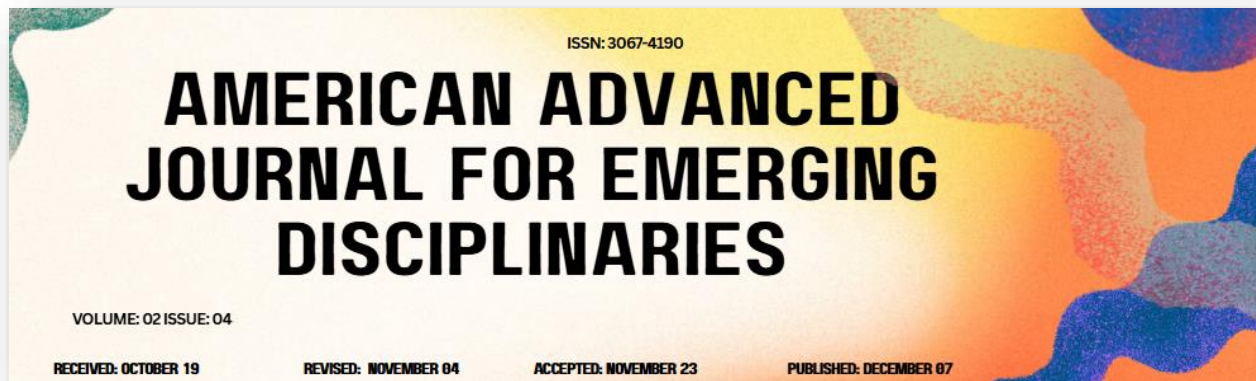
computes a preimage of this value. One of the security goals is that this problem is as hard as solving a randomly chosen system of equations with a number of equations equal to n . For signature schemes, security can also be based on the difficulty of finding a common root of n polynomials of degree d in n variables $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q$, with $d > 2$. It can be established that such signature schemes are existentially unforgeable under the standard model. A classical digital signature associated with the signature scheme and relying on the above-mentioned security goal achieves message recovery and therefore has short signatures in terms of the size of the secret key.

The sizes of the secret keys, signatures and public keys are at least $O(2n(n + \log q))$ and for signature schemes also $O(n^2 + n \log q)$. Their size is not significantly larger than the size of the secret keys of an equivalent signature scheme based on the security of finding a common root. The schemes have the same complexity as all other known multivariate signature schemes. Although the public key is large, it is much smaller than the signing key, and the size of the public key is comparable to the size of the public key of the other multivariate signature schemes mentioned above. Multivariate signature schemes can be considered a high-speed solution of the post-quantum digital signature problem, although the size of their secret keys is a major drawback compared with all other candidate schemes. Multivariate schemes are not the only ones for which the size of the secret key is much larger than the sizes of the signing keys. Other public-key schemes based on the hidden multivariate problem are as fast as multivariate signature schemes and have compact public keys, but the size of their secret keys is also huge in comparison with the size of the signing key.

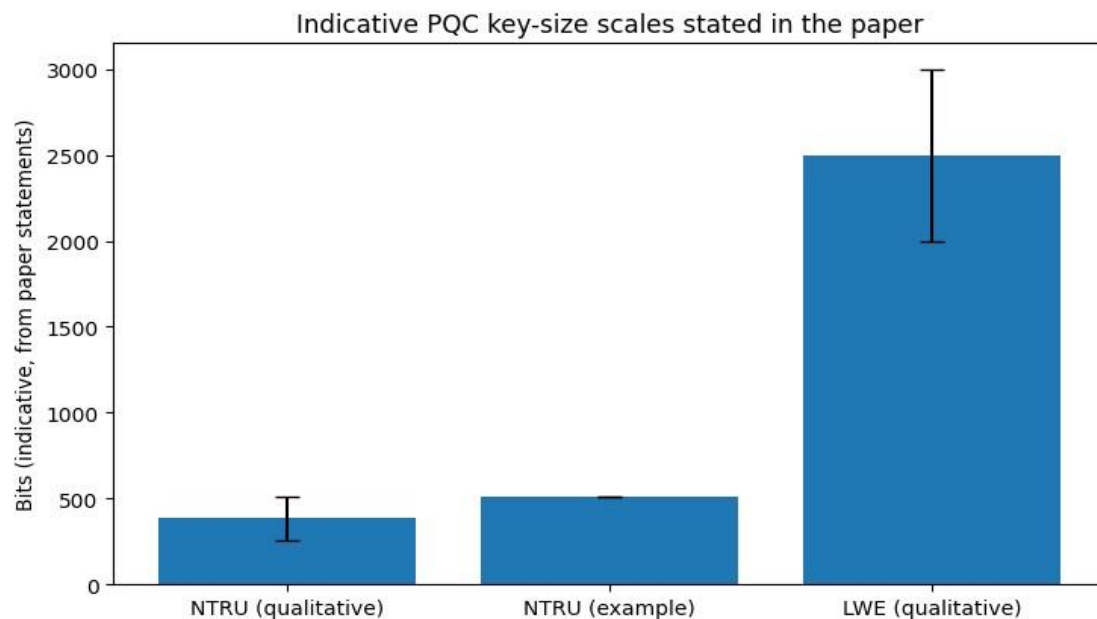
4. Threat Landscape and Security Assurances

Classical cryptographic primitives and protocols with quantum-enabling features in their architectures will need to be replaced or carefully adapted to reduce the impact of long-term attacks and the subsequent transition to post-quantum security levels. Ideally, any adaptation should not increase the attack surface. Protocols are threatening when used in conjunction with identities that could be compromised in the future.

To support security but prevent crisis, the quantum investment arms race is best seen as a temporary cost to the overall security of the system rather than the future. The growing quantum capability will therefore require an assurance that the real-world TCP/IP architecture will not expose data that future entities will exploit. As an integral component of national security and



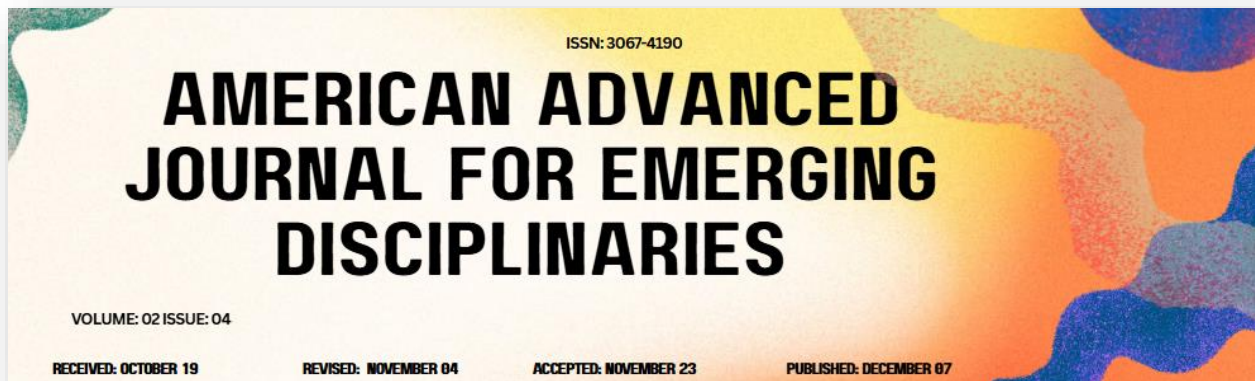
future-oriented economy, post-quantum cryptography can and must also serve the long-term interest and economy beyond the growth cycle of the quantum arms race Q: Assumptions for Post-Quantum Cryptography Looking into the classical formal cryptography literatures, there are growing academic activities supporting the necessity of looking at cryptography from the defensive side rather than the traditional position of supporting attacker mode. The attacker who can still approximately work in the standard polynomial time is the one needing a new type of asymmetric quantum-Kem Declared that finds reverse resilience.



Equation B) Size / complexity lower bounds: $O(2^n(n + \log q))$ and $O(n^2 + n \log q)$

The explicitly states:

- “sizes ... at least $O(2^n(n + \log q))$ ”
- and “for signature schemes also $O(n^2 + n \log q)$.”



1) Deriving why a term like $2^n(n + \log q)$ appears

This is a **counting/encoding** argument consistent with multivariate constructions:

5. Encoding one field element

- One element of $\mathbb{F}_q$ takes $\log_2(q)$ bits to represent.
- In big-O notation, people write $\log q$ (base doesn't matter in big-O).

6. Exponential dependence on n

- Many multivariate objects scale with the number of possible assignments of variables, which is q^n , or with structures that grow like 2^n when q is treated as constant-ish in the expression.
- The form $2^n(n + \log q)$ indicates: “**number of components $\sim 2^n$** ” $\times$ “**bits per component $\sim (n + \log q)$** ”.

7. Combine

$$\text{size} \in O(2^n \cdot (n + \log q))$$

meaning if you scale n up even modestly, that exponential term dominates.

2) Deriving the polynomial term $O(n^2 + n \log q)$

1. Split the term:

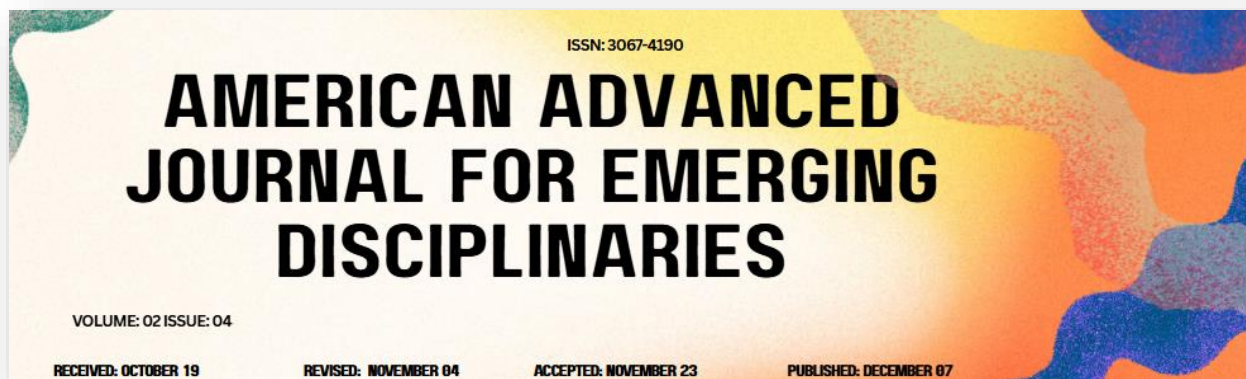
$$n^2 + n \log q = n(n + \log q)$$

2. Interpretation: you often store on the order of n^2 coefficients/relations plus some n values each costing $\log q$ bits to represent.

3. Big-O form:

$$\text{size} \in O(n^2 + n \log q)$$

4.1. Quantum Attacks on Classical Protocols



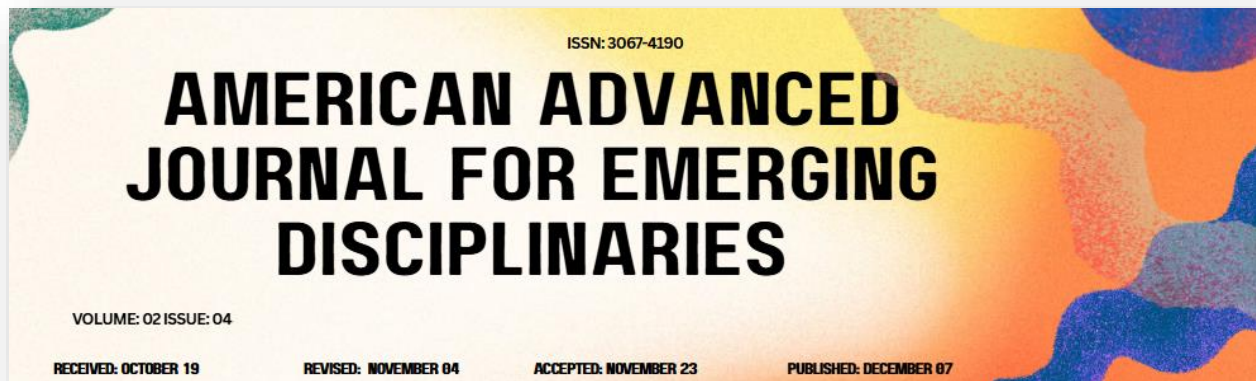
Post-quantum cryptography (PQC) readiness requires mitigating Shor's and Grover's capabilities with implementations resilient to both classical and quantum adversaries in a thermodynamic asymptotic sense. The overall security landscape is dominated by the aging of public-key algorithms and the associated risk of covert key retrieval in the near term. Note that confidentiality and trust in sensitive electronic communications or data are ultimately required for the entire credential duration, hence the need for PQC to secure key harvest now for future protect later.

The key strategists of major geopolitical actors are well aware when designing long-term infrastructure investment programs, apportioning finite resources between planning for now, the near term, the medium term, and the long-term horizons. Long-term targets, such as space ventures, nuclear programs, or time-sensitive innovations like COVID vaccines, demand resources anyway, regardless of quantum cryptography being deployed or not. Organisational intelligence is of course vulnerable to clandestine action, even with non-quantum digital signatures, thus key harvest now and decrypt at leisure with shor at least trades speed at the time of operation against future security of harvested traffic. Any cryptanalysis of classical protocols that can be speeded up by grover now falls into the near-term horizon bucket.

5. Architectural Frameworks for National and Regional Systems

The foundational principles of resilient national and regional digital sovereignty systems are valid for any digital activity. The architecture of such a system needs to meet four initial, interrelated imperatives. It must satisfy a country's own national sovereignty requirements, enable the substantiation of its trust relations with other jurisdictions in a contemporary way, permit the establishment of a system that is capable of surviving future quantum attacks, and do so in a manner that reduces the risk and impact of cyberattacks on the nation's infrastructure. Once these imperatives are met, consideration can be given to subsequent integration with broader regional or global systems.

The architectural principles for the sovereign national system can also be applied to it. An important enabler for the successful rapid and long-term development of post-quantum infrastructure in all jurisdictions is the ability to establish all PKI and credential life cycle management processes at least initially by using only symmetric cryptography foundations and not yet introducing post-quantum cryptography primitives. Such an approach reduces risk in the early adoption phase and enhances crypto-agility within the systems. The evolving PKI and



credential life cycles need to support complete crypto-agility of services, where the use of an individual sub-key can be cryptographically switched to any other required advanced primitive or length. Nevertheless, it remains essential to provide mutual recognition of post-quantum standards where needed to support externally facing services across jurisdictions.

5.1. Key Management in a Post-Quantum Era

A credential life cycle management system should control the generation, registration, archiving, updating, revocation, and destruction of credentials across the entire post-quantum cryptographic ecosystem, with adaptability to alternative or stronger algorithms across generations. Requirements for such a system include a PKI, Generalized PKI, Generic Information Sharing Environment (GISE), and Archives/Trust services.

Post-quantum key management requirements revolve around the risk of asymmetric encryption and signature keys being compromised by future decryption, the size growth of asymmetric keys (requiring extensions of existing frameworks), the need to support long-term confidentiality of symmetrically protected data, post-quantum Algo Agility, and the need for backups and recovery of long-term ECC keys. Such keys must be archived as a collection of public and private key shares distributed among TTPs coded with Shamir's secret sharing. Suboptimal secret-sharing configurations should preferably be carefully avoided; for example, a collection of N shares for a DH secret-sharing system should be coded into N shares using the (N,T) -Shamir scheme.

The threats generated by these factors call for extensive adaptation of digital signatures and public-key infrastructures (PKIs) by crypto-agility techniques (enabling key replacements within the main PKI structure) as well as the entire lifecycle of trust services (defined in a wide sense) for both short- and long-term signatures. Some special back-up and recovery considerations are needed for commitments and zero-knowledge proofs. No outright alternative is available for current TLS proxies in terms of economy, simplicity, and ZZ assumption. Only complex modifications of VPNs and end-to-end communication avoid storing full PKI keys. Similarly, VPN backbones and cross-IoT-encryption proxies become obvious applications. The simplest and most efficient retrofitting is the proposed overlay for secret-sharing-based IoT devices.

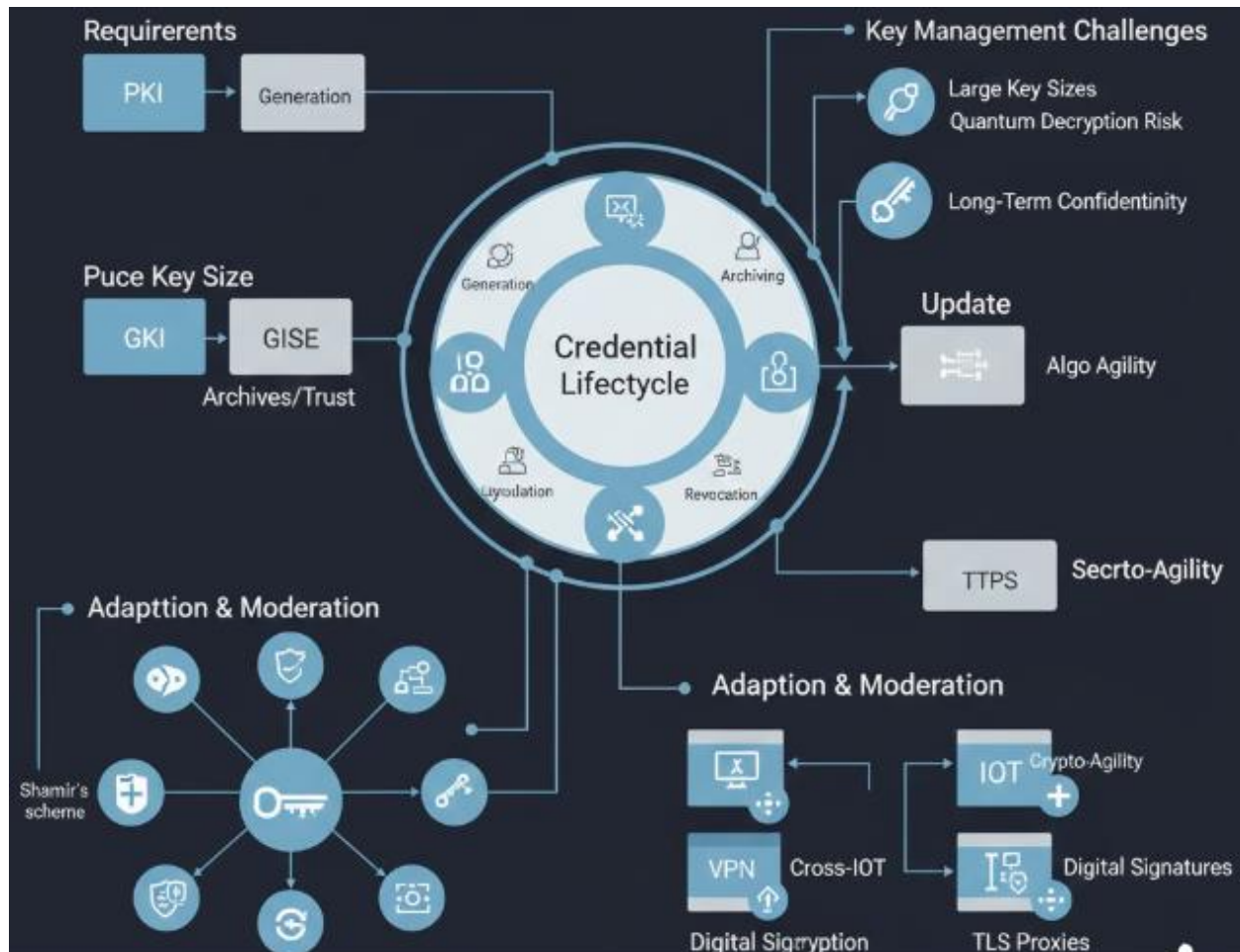
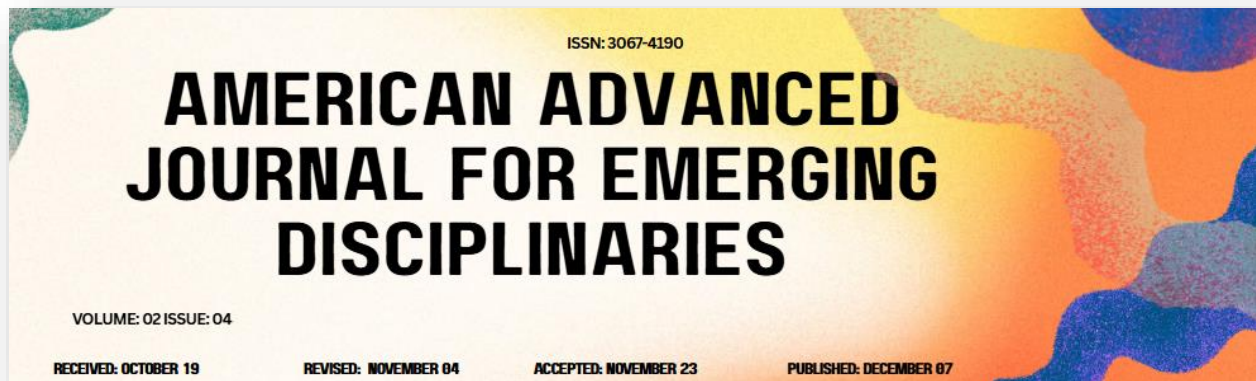


Fig 3: Adaptive Lifecycle Governance for Post-Quantum PKI: Crypto-Agility, Shamir Secret-Sharing, and Strategic Retrofitting

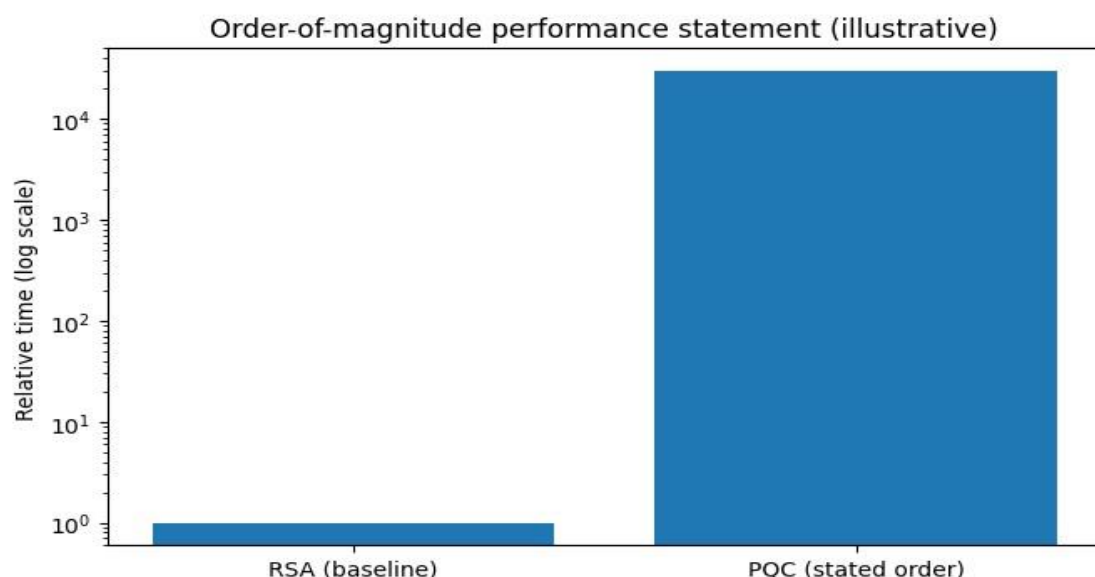
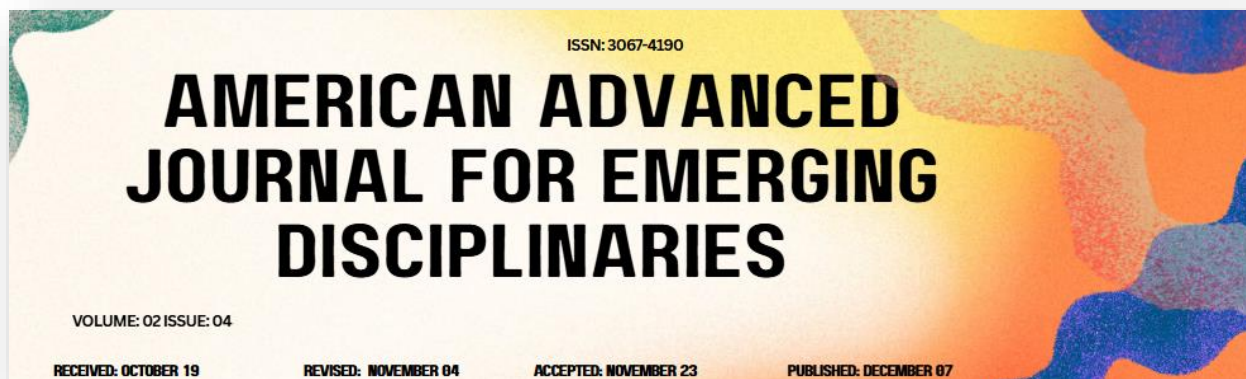
5.2. Protocol Adaptation for Internet Infrastructure

Fundamental shifts in cryptographic paradigms raise serious concerns for supporting internet infrastructure: authentication, confidentiality, and integrity at regional and global scales must remain viable and cost-effective in a post-quantum world. Major application-layer



protocols such as TLS will inherently require adaptation, as will VPNs, messaging services, and wireless authentication. In each case, the relevance of quantum computing to a specific application must be carefully considered, with particular attention to the threat of opportunistic, quantum-enabled capture. As the potential capabilities of long-term adversaries become more predictable, a well-coordinated transition either to post-quantum solutions or to those whose security does not depend solely on classical assumptions will increasingly be paramount.

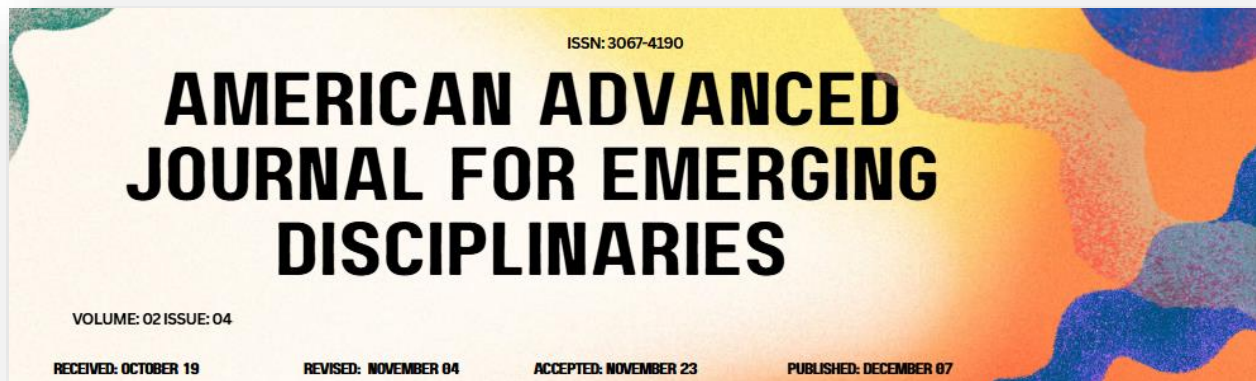
Internet and cloud services offered by organizations without an established or apparent national security imperative are another area of great concern. Capture of encrypted communication with those services represents an exceptional, but generally short-term, risk in light of Grover's algorithm; therefore, service owners should institute quantum-resistant key management, end-to-end encryption, and/or support for post-quantum credentials within TLS. A lack of attention here carries the real danger of open or cloud services unintentionally becoming the preferred conduits or storage for the sensitive data of long-lived jurisdictions. Considerations for IoT systems, where "perpetual" operation is often assumed but update capability may be severely limited, may also need to extend beyond the usual hardware constraints. Actual practice remains to be assessed, but the long projection timelines of most popular public key systems suggest that an orderly transition should be possible and that misuse of these devices for persistent data storage is unlikely to be a common concern.



6. Governance, Policy, and Sovereignty Considerations

Laying the governance groundwork enables effective risk mitigation, facilitates trust, and assures the ethical integrity of PQC deployment. Adoption must comply with established rule-of-law principles. Transparency enables accountability; governance frameworks define qualified authorities and processes; and faith in regulatory assurances rests on capable audit trails. Hence, administrative and conduct rules must address these dimensions. Emerging governance frameworks focus on addressing PQC deployment process risks. The Blue Dot Network, for example, promotes other nations' critical-priority infrastructure investment decisions. Supporting national supply chains and reducing reliance on strategically compromised partners is equally important. Yet transnational trade requires trust assurance. Cross-border agreements streamline concordance, allowing fewer rule overlaps for lower transaction costs and greater transnational efficiency.

Greater digital sovereignty strengthens a nation's bargaining power in these talks. Established jurisdictional concepts apply to data in transit, while jurisdiction-affiliated local standards can control data at rest or use. PQC adoption adds another layer of cross-border recognition: mutual agreement of the risk-linked standard's post-quantum assurances. Outside



these controls, the risk lies with the data using-party. Yet supporting deeper PQC deployment also creates a basis for digital protectionism, as a complete sovereign ecosystem gives a partner greater regulatory reach and the ability to require local data storage.

Consider policy-making in digital space. The absence of territorial line definition in cyberspace makes involvement personal rather than territorial. Jurisdictional authority and cyber-responsibility are thus actual, not physical. Violating this principle brings diplomatic repercussions, like expulsion from alliances, but lacks international legal support. Data privacy protectionism and localization efforts rest on a nation's ability to prevent malicious personal data use. Adopting data localization laws makes it costly to host locally, while recognizing that hosting country prevents abuse creates its reverse. Data processing use must thus fall under the jurisdiction of both parties for greater transnational trust.

Equation C) Equations that the relies on but does not write out: Shamir Secret Sharing

The explicitly requires archiving keys as “shares distributed among TTPs coded with Shamir’s secret sharing” and mentions an (N, T) -Shamir scheme.

Here is the **full step-by-step derivation** of (N, T) Shamir Secret Sharing:

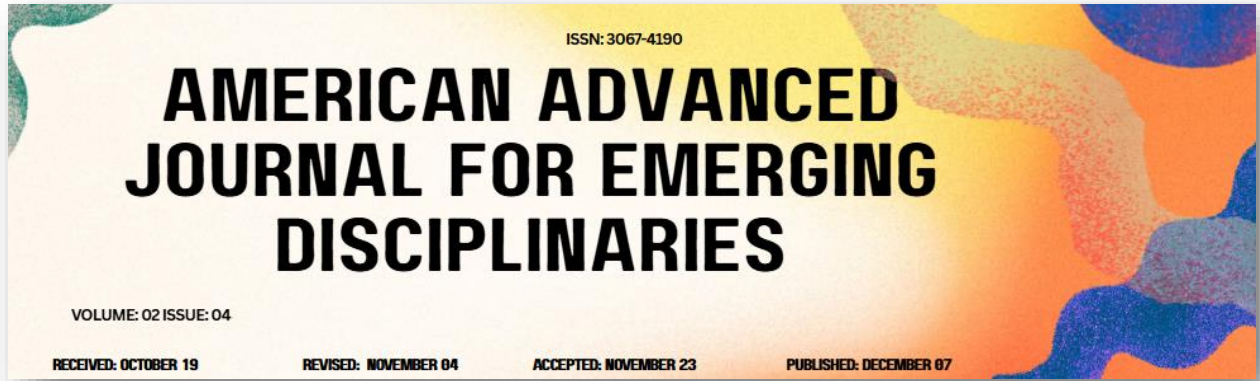
Goal

Split a secret s into N shares such that:

- Any T shares can reconstruct s ,
- Any $T - 1$ or fewer shares reveal nothing about s .

Step 1: Choose a finite field

Pick a prime p (or field $\mathbb{F}_q$) such that $s \in \mathbb{F}_p$.
All arithmetic is modulo p .



Step 2: Construct a random polynomial of degree $T - 1$

Define

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{T-1}x^{T-1}$$

Set the constant term to the secret:

$$a_0 = s$$

Choose $a_1, \dots, a_{T-1}$ uniformly at random from $\mathbb{F}_p$.

Step 3: Generate N shares by evaluating the polynomial

Pick N distinct non-zero x -values, e.g. $x = 1, 2, \dots, N$.

Compute:

$$\text{Share}_i = (x_i, f(x_i))$$

Step 4: Reconstruction from any T shares via Lagrange interpolation

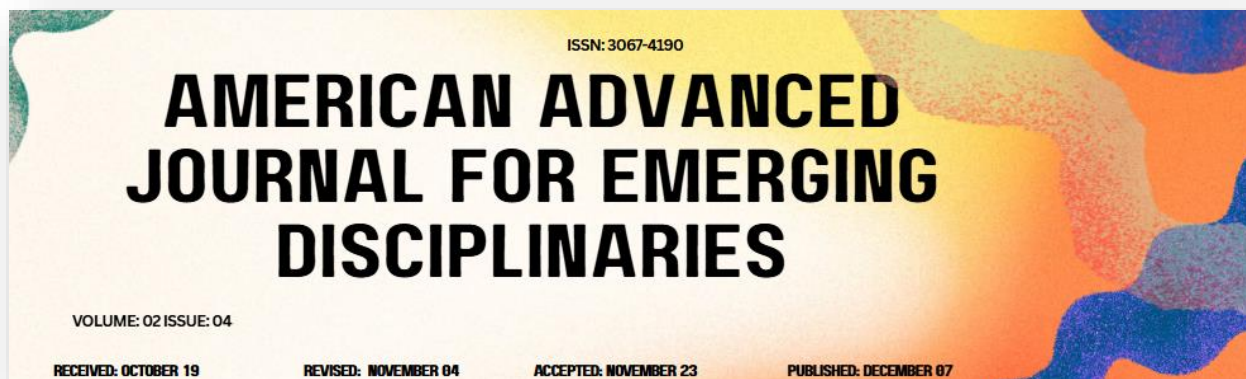
Given T points $(x_1, y_1), \dots, (x_T, y_T)$ with $y_i = f(x_i)$, the unique degree- $(T - 1)$ polynomial is:

$$f(x) = \sum_{i=1}^T y_i \cdot \ell_i(x)$$

where the Lagrange basis polynomials are

$$\ell_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^T \frac{x - x_j}{x_i - x_j}$$

6.1. Data Localization and Cross-Border Trust



National law governs the use and access to data accessible in or owned by servers under an administrative jurisdiction. Therefore, critical data may need to be stored physically within the relevant jurisdiction. Cryptocurrency has shown that data localization requirements introduce additional resource-efficiency overheads, which tends to be reduced but can never be completely avoided by the use of low-layer protocols without such a requirement. Thus, any partition that minimizes the required currency resource workload should also minimize the workload required for data localization. Countries that do not have foreign jurisdiction over their data still face trust issues in cross-border digital communications and transactions. Even with appropriate data localization, such countries cannot be exempt from the general need for a mutual recognition agreement of cross-border digital transactions.

Post-quantum cryptographic(NTRU, KEM, FAL, Lattice Hardness, SIS, LWE) schemes provide sufficient security for some time. However, national critical infrastructure, especially long-lived ones, should consider the situation when schemes appear that allow breaking all known PQC with reasonable computational effort. The high number of keys involved in Internet and cloud applications makes these infrastructures potentially exposed to such threats. Since the cost of real-world attacks is a monotonically non-decreasing function of time, the required security for long-lived sensitive long-term communications needs to be at least twice the security level provided by a post-quantum scheme for which no other mitigation approach is available.

7. Conclusion

Post-quantum cryptography is essential for protecting digital sovereignty and for the digital security of future generations. Digital sovereignty crucially depends on controlling cryptography, because digital infrastructures are relied upon for economic and national security reasons. National and regional infrastructures must be built with this imperative in mind. Progress must start without delay to develop a post-quantum PKI capability, adapt the Internet protocols, and incorporate related considerations into the design of critical applications. The PKI and associated credential life cycles must become crypto-agile, archival, and support algorithm-agnostic authentication integrity.

MGF is an Internet Key Management facility continuously evaluating key technologies and providing digital certificates to enable scalable trust-based authentication. One primary task of MGF is to work with national and regional authorities to provide operational keys for trust-based authentication. By continually evaluating emerging key technologies including

cryptographic technology, MGF will also provide suitable controls using post-quantum infrastructure such that the information in trust-based public keys will not be compromised. As PKI is adapted, mutual recognition of all credential standards under the auspices of MGF will be essential. дорожній знак шкідливий Because credential repositories and the communications that access them will contain sensitive keying material during the transition to post-quantum Public Key Infrastructure (PKI), the Internet transport protocols TLS and IPsec will need to be adapted for a new secrecy-providing KEY CONFIRMATION (KC) [45]. Additional aspects of the IoT need to be addressed, including suitable adaptation of the TLS (and/or QUIC) communication protocol stack.

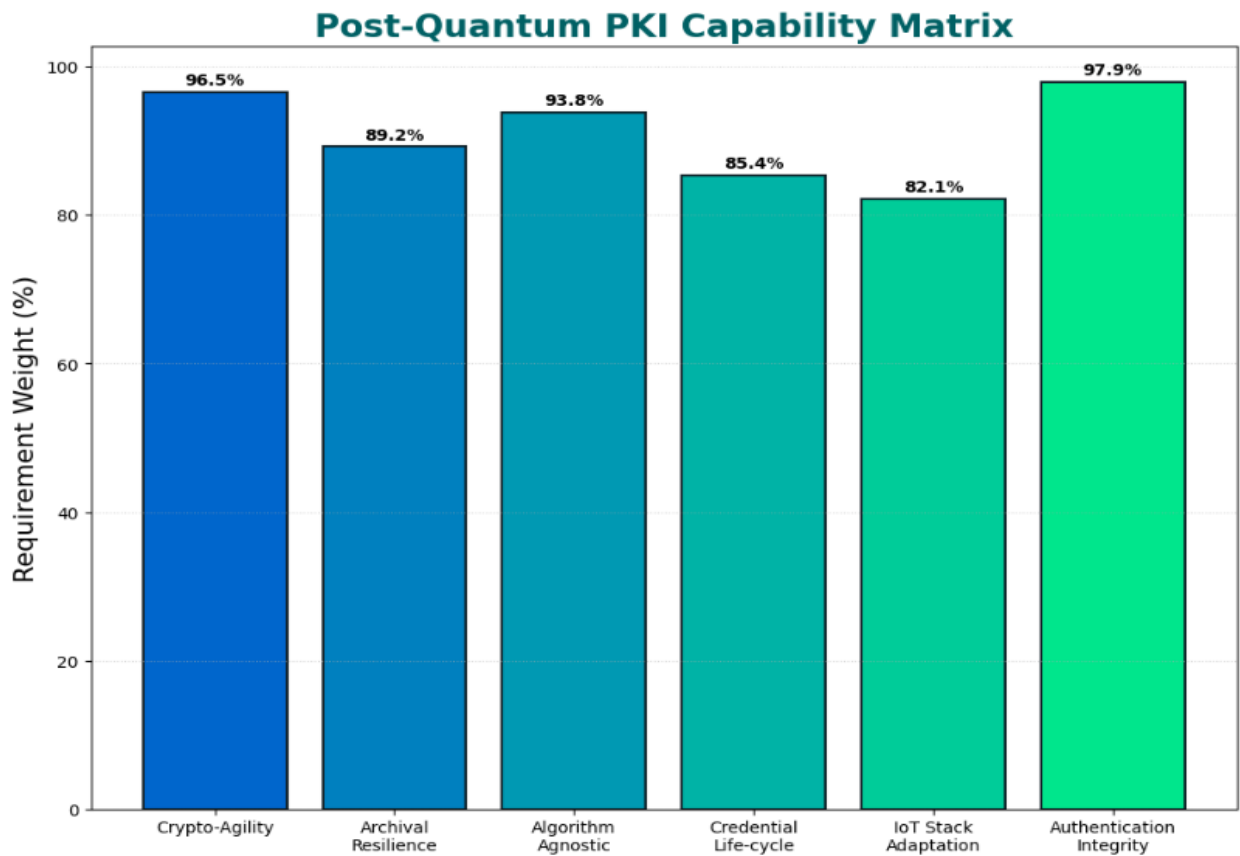
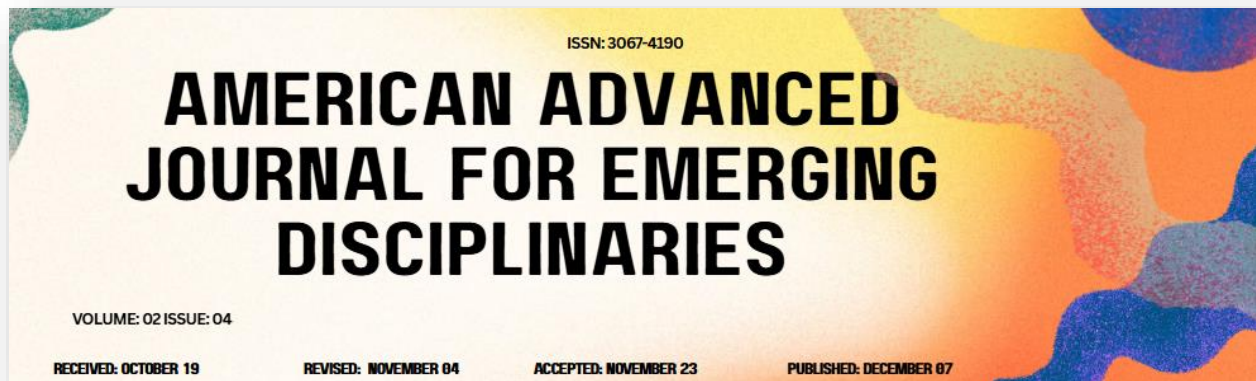


Fig 4: Post-Quantum PKI Capability Matrix



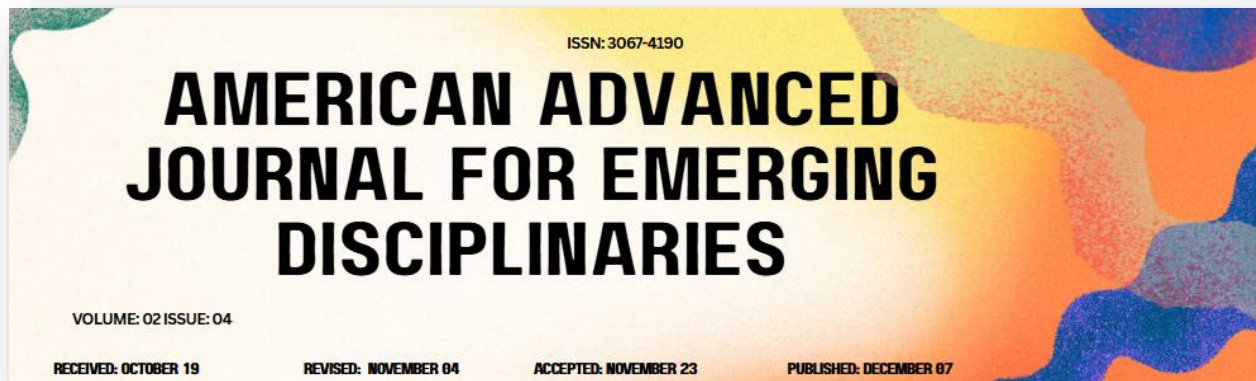
7.1. Final Reflections and Future Directions in Post-Quantum Cryptography

The need for a definitive leap in post-quantum cryptographic risk mitigation is unavoidable. It is essential to align with the common goals of sovereignty: control of security and communications, the resilience of critical infrastructure, and the confidentiality and integrity of data over the long term. However, these are only surface reflections. The more fundamental level of insight lies in how all of these can also help enhance the foundational national security and economic priorities arising from the risk of economic espionage coupled with locally exploitable Quantum Computing resources.

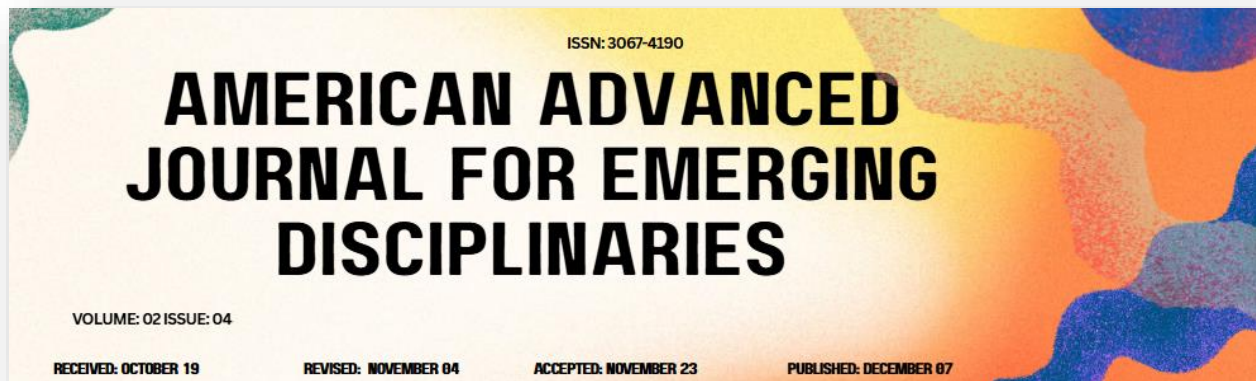
More than a decade has gone by since the first decision of waiting for the formal conclusion of the standardization process led by NIST. In that time, there has been ample indication in the public domain of the likely period for movement into the next generation of Quantum Computing capability. Nevertheless, the evidence is in sight of the second closing window of opportunity to leave classical algorithms behind in the defence of sensitive data. Time has been wasted to work on the Quilotime scenario, and even more on poorly understood Post-Quantum Security policies. The WHY to migrate into PQC is well established; Miranda is now coming close to offering the HOW. Identifying Data-LocalizationStructures is a way to consolidate Jurisdictional Control and enhance the Local Response for both clearly Quasi-Social and Defence-Related critical Infrastructure. Data-Localization Structures can also assist in better managing Data-Residency control on cross-domain Data-flows by establishing mutual trust on the post-quantum security of shared Information.

References

- [1] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2, 79.
- [2] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509.
- [3] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Annual ACM Symposium on Theory of Computing*, 212–219.
- [4] Bernstein, D. J., Buchmann, J., & Dahmen, E. (2019). *Post-quantum cryptography*. Springer.
- [5] Alagic, G., Alperin-Sheriff, J., Apon, D., et al. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. *NIST Interagency Report*, 8413.



- [6] Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. National Institute of Standards and Technology.
- [7] Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4), 283–424.
- [8] Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). NTRU: A ring-based public key cryptosystem. *Lecture Notes in Computer Science*, 1423, 267–288.
- [9] Bernstein, D. J., Lange, T., & Peters, C. (2008). Attacking and defending the McEliece cryptosystem. *Lecture Notes in Computer Science*, 5299, 31–46.
- [10] Ding, J., & Petzoldt, A. (2017). Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4), 28–36.
- [11] Hülsing, A., Rausch, L., & Buchmann, J. (2018). Optimal parameters for hash-based signatures. *Journal of Cryptographic Engineering*, 8(3), 229–243.
- [12] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing*, 175–179.
- [13] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., et al. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3), 1301–1350.
- [14] Mosca, M. (2018). Cybersecurity in an era with quantum computers. *IEEE Security & Privacy*, 16(5), 38–41.
- [15] National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum computing: Progress and prospects*. National Academies Press.
- [16] Khatri, V., & Brown, C. V. (2018). Designing data governance. *Communications of the ACM*, 53(1), 148–152.
- [17] Otto, B. (2019). Organizing data governance. *Journal of Data and Information Quality*, 11(1), 1–36.
- [18] Floridi, L. (2020). The fight for digital sovereignty. *Philosophy & Technology*, 33(3), 369–378.
- [19] Floridi, L., Cows, J., King, T. C., & Taddeo, M. (2020). How to design AI for social good. *Science and Engineering Ethics*, 26(3), 1771–1796.
- [20] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things. *Computer Law & Security Review*, 32(5), 715–728.
- [21] Shackelford, S. J. (2020). *Governing cyber peace*. Cambridge University Press.
- [22] Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.



- [23] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365–404.
- [24] Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
- [25] Buchanan, B. (2020). *The hacker and the state*. Harvard University Press.
- [26] Herr, T., Laudrain, A., & de Spiegeleire, S. (2021). Cyber deterrence revisited. *Journal of Cyber Policy*, 6(1), 1–24.
- [27] Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, 556(7701), 296–298.
- [28] Gartzke, E., & Lindsay, J. R. (2019). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, 28(2), 316–348.
- [29] Raji, I. D., Smart, A., White, R. N., et al. (2020). Closing the AI accountability gap. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 33–44.
- [30] Gunning, D., & Aha, D. (2019). DARPA’s explainable artificial intelligence program. *AI Magazine*, 40(2), 44–58.
- [31] Pearl, J., & Mackenzie, D. (2018). *The book of why: The new science of cause and effect*. Basic Books.
- [32] Puranam, P., Cooney, J., & Vaaler, P. (2023). Algorithms and organizational design. *Academy of Management Annals*, 17(1), 1–40.
- [33] Fan, W., & Liu, H. (2023). Trustworthy artificial intelligence for enterprise and national systems. *IEEE Intelligent Systems*, 38(2), 14–22.
- [34] Weber, R. H., & Schmid, M. (2023). Governance of artificial intelligence in sovereign digital infrastructures. *Computer Law & Security Review*, 49, 105735.
- [35] Alagic, G., & Majenz, C. (2024). Cryptographic agility and migration to post-quantum systems. *IEEE Security & Privacy*, 22(1), 56–64.