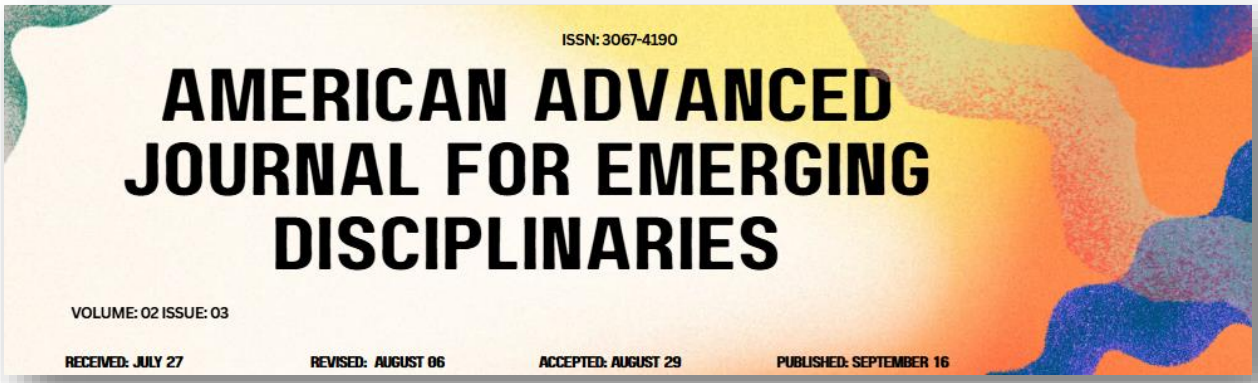


Quantum Cryptanalysis and Cyber Deterrence Mechanisms in Digital Warfare

Dhanaraj Sathiri
Independent Researcher
dhanrajsathiri@gmail.com

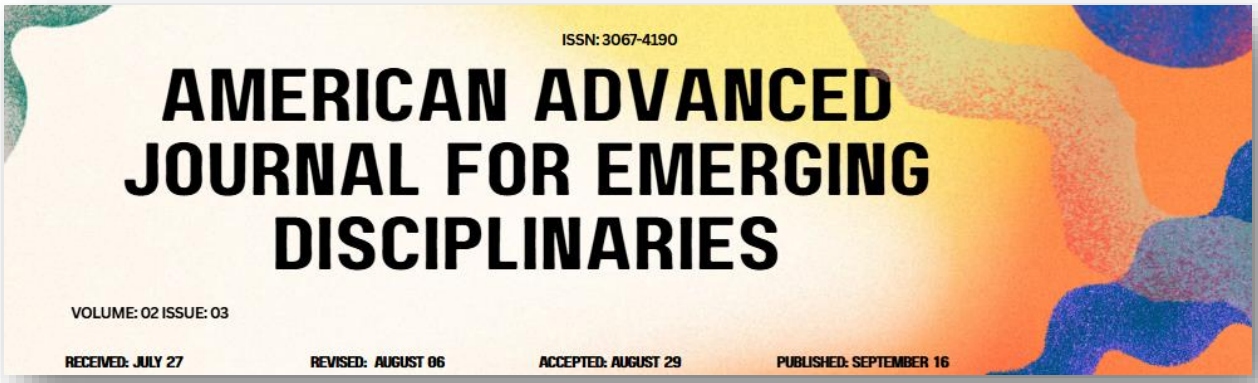
Abstract

Quantum threats to classical and quantum-resilient cryptography and deterrence mechanisms for cyber warfare underpinnings are investigated. The fundamental principles of quantum eavesdropping techniques, quantum computing, and cryptanalytic algorithms, including Shor's and Grover's algorithms, are outlined. The most widely examined post-quantum cryptography primitives—lattice-based, multivariate-quadratic-equations-based, code-based, and hash-based solutions—are compared in terms of their respective capabilities and inherent vulnerabilities. Quantum cyber deterrence concepts—strategic stability, defensive postures, resilience, risk management, capability hardening, and offensive thresholds—are examined. The potential for deterrent or coercive application of quantum computing in digital warfare is analyzed, with an emphasis on ethical, legal, and strategic considerations.

The development of internationally accepted certification procedures and compliance frameworks is essential to effectively manage the post-quantum digital transition, providing a foundation for effective risk management and enable the emergence of governance, regulatory, and normative frameworks for responsible and stable cyber operations. The establishment of strategic, cooperative, and operational confidence-building measures, as well as the generation of deterrent cyber-resilience capabilities, is crucial to enabling stable deterrence in digital space—one that supports not only the prevention of cyberwar but its controlled, limited, and responsible conduct when required.

Keywords: Quantum Cryptographic Threats, Quantum-Resilient Cryptography, Quantum Eavesdropping Techniques, Quantum Computing Capabilities, Shor’s Algorithm, Grover’s Algorithm, Post-Quantum Cryptography, Lattice-Based Cryptography, Multivariate Quadratic Cryptography, Code-Based Cryptography, Hash-Based Cryptography, Cryptographic Vulnerabilities, Quantum Cyber Deterrence, Strategic Stability, Cyber Resilience, Risk Management Frameworks, Capability Hardening, Offensive Cyber Thresholds, Cyber Governance And Regulation, Ethical And Legal Considerations.

1. Introduction



Quantum hacking poses an increasing threat to cryptography and cyber defenses. Research questions include: What cyber strategies mitigate the threat of quantum cryptanalysis? What aspects of deterrence theory apply in the quantum domain? Deterrence mechanisms against quantum threats require risk management, resilience, and capability hardening. Signals of offensive capabilities may support deterrence, but thresholds and compliance with legal and ethical principles remain challenging. Aided by disorderly quantum processes, the co-opetition model of cyberspace offers experimental opportunities for decoupled rapprochement.

Cybersecurity standards address classical, artificial intelligence, and quantum risks, but maintaining conditions for secure deterrence remains paramount. Such conditions can be assessed in detail; attacks on the security of deterrent objectives, such as nuclear weapons and critical infrastructure, should be explicitly prohibited, and caution advised in linking quantum capabilities to demands for general cyber deterrence. Additional aspects of quantum deterrence theory – affiliation theory, the role of intra-asymmetry, reputational thresholds, deterrence by denial, the relationship with strategic stability, and the role of Japan and the United States – require further study.

1.1. Overview of Key Concepts and Scope

The introduction presents an overview of cybersecurity and cyber deterrence considerations in the presence of developmental and possible operational quantum computing capabilities. The intersection is especially concerning, because of the substantial risk that quantum attackers present to the encryption protocols upon which computer, network, data, and transaction protection depends. Developmental quantum capabilities also afford the possibility for more classic offensive cyber operations that target the sensitive information processed, stored, and transferred in secrecy protected by classical asymmetric encryption methods. Cybercrime and state-sponsored espionage such as that reported against trade and technological research secrets are highly sensitive to the capability of actors—defensive and offensive—to maintain or degrade

ISSN: 3067-4190

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 02 ISSUE: 03

RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

the assurance of those secrets.

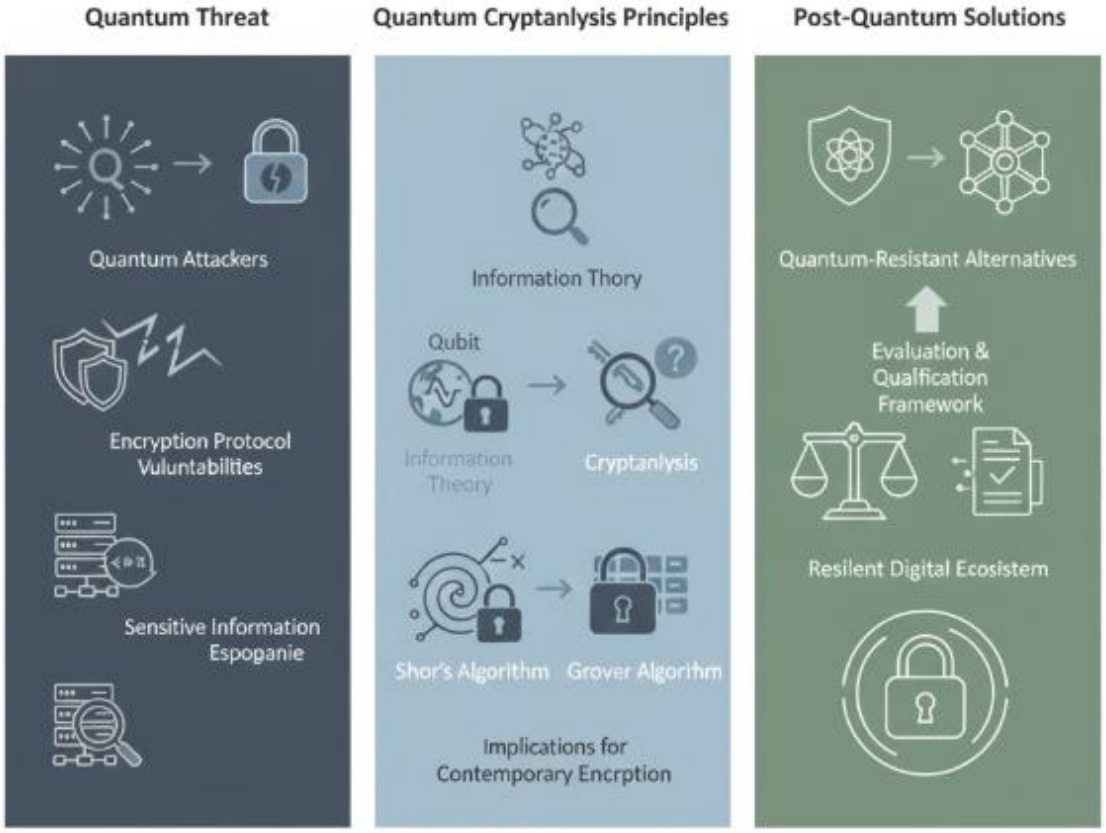
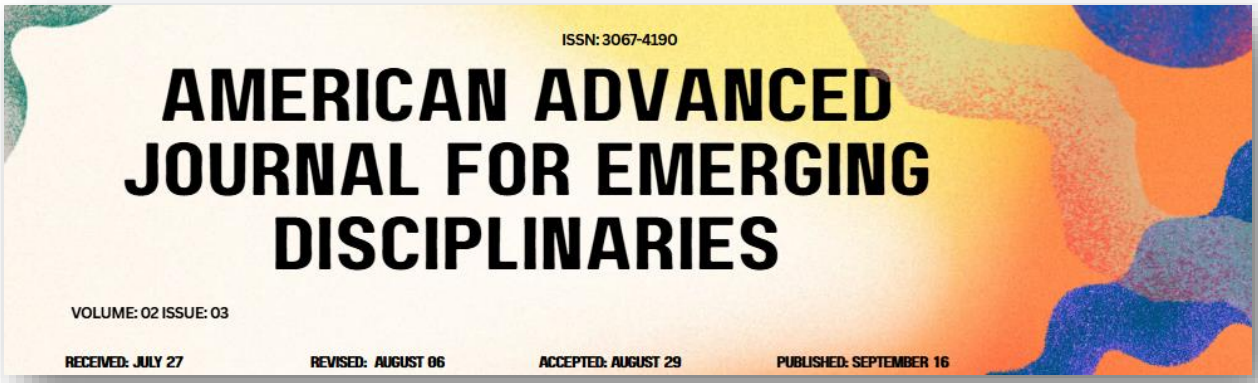


Fig 1: Securing the Quantum Frontier: Evaluating Post-Quantum Cryptographic Frameworks Against Algorithmic and State-Sponsored Threats

The second section offers an overview of the core principles of quantum computation, information theory, and cryptanalysis, followed by a summary of the main quantum algorithms and their implications for contemporary encryption protocols. Special attention is directed to Shor's and Grover's algorithms. The third section summarizes the main current efforts to develop quantum-resistant alternatives that will address those—and other inherent quantum vulnerabilities. Such alternatives are crucial because of their potential application at every level



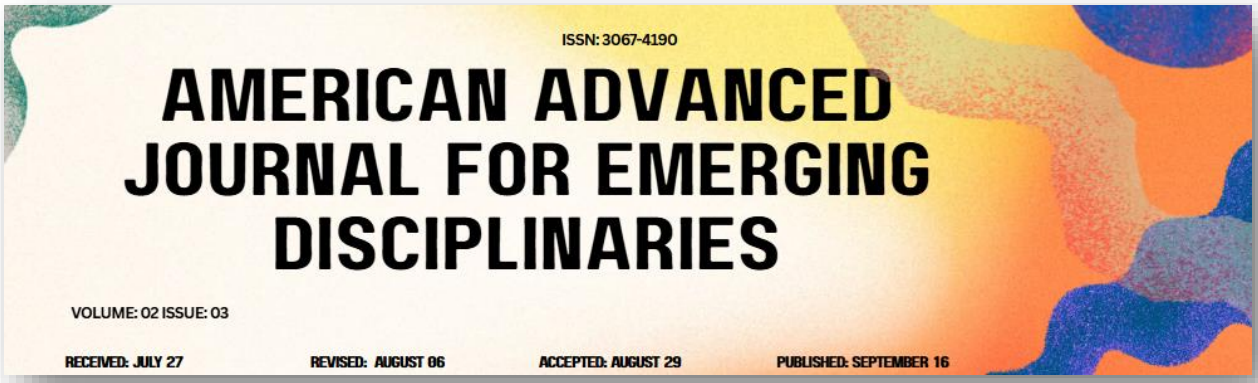
of the digital ecosystem, and efforts are underway to establish a framework that will evaluate and qualify such post-quantum solutions.

2. Fundamentals of Quantum Cryptanalysis

Provision of qubits affords a new realm of hardware, whereby computational tasks might achieve FFT, DFT, or search performance consistent with classical systems. Shor's Algorithm is the quintessential threat to the realization of a quantum computer and a measure of its success. Such machinery is currently limited to addressing small-scale issues and producing noisily coherent error-corrected output. Despite such limitations, developments in proofs that constrain computation time and space remain of utmost value. Quantification of quantum systems will afford a faster than classical performance advantage using Grover's search algorithm. A candidate measure for noise mechanisms which degrade performance offers an opportunity for superposition entangled channels. The derivation of channels that offer various Einstein-Podolsky-Rosen-type correlations is of significant consequence; the loss of these correlations increases the physical distance over which secrets can be communicated effectively. Superadditivity remains an open problem with respect to probabilistic distribution of general source-based state conversion problems.

The most important currently unbroken asymmetric protocol is RSA which is based on the integer factorisation problem. The most known attack on this problem is the number field sieve, which represents a substantial cost to use against RSA1024, though it is used regularly against smaller moduli. Nevertheless, other protocols based on non-commutative groups have not received attention. Other asymmetric protocols include quantum key distribution that offer unconditional security, threshold schemes where a consortium distributes a secret, homomorphic encryption that allows computations to be performed on encrypted text, identity-based encryption and digital signatures. Additionally, any defence against the classical attacks that are based on mathematics reducible to Gr¨obner bases or the discrete logarithm problem in partial groups is likely to defend against quantum attacks.

Primitive / Task	Best-known classical scaling (informal)	Quantum scaling (headline)	Practical implication
RSA factoring	Sub-exponential (e.g., Number Field Sieve)	Polynomial in log N (Shor)	Breaks RSA once large fault-tolerant QC exists



Primitive / Task	Best-known classical scaling (informal)	Quantum scaling (headline)	Practical implication
ECC discrete log	Sub-exponential (index calculus variants for some groups; ECC generally hard)	Polynomial in log p (Shor)	Breaks ECDH/ECDSA under same assumption
Symmetric key search	O(2^k)	O(2^(k/2)) (Grover)	To keep k-bit strength, increase to ~2k bits

Equation 1) Quantum state and "2^n configurations" claim (superposition)

The states that a qubit can be in 0 and 1 "at the same time" and gives the example that **6 qubits span all 2^6 bitstrings and 100 qubits span 2^{100} configurations**.

1.1 Single-qubit state (equation + normalization)

A qubit lives in a 2-D complex vector space with computational basis $\{|0\rangle, |1\rangle\}$.
General state:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Measurement probabilities must sum to 1:

$$P(0) = |\alpha|^2, \quad P(1) = |\beta|^2, \quad |\alpha|^2 + |\beta|^2 = 1$$

1.2 Two qubits → tensor product → 4 basis states

Two qubits' basis is the tensor product:

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

General 2-qubit state:

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

$$\left|\psi\rangle = \sum_{x\in\{0,1\}^2} \alpha_x \right| x\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Normalization:

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$$

1.3 n qubits → 2^n basis states

Inductively, adding one more qubit doubles the basis size:

- 1 qubit → 2 basis states
- 2 qubits → $2 \times 2 = 4$
- …
- n qubits → 2^n

So the general n-qubit state is:

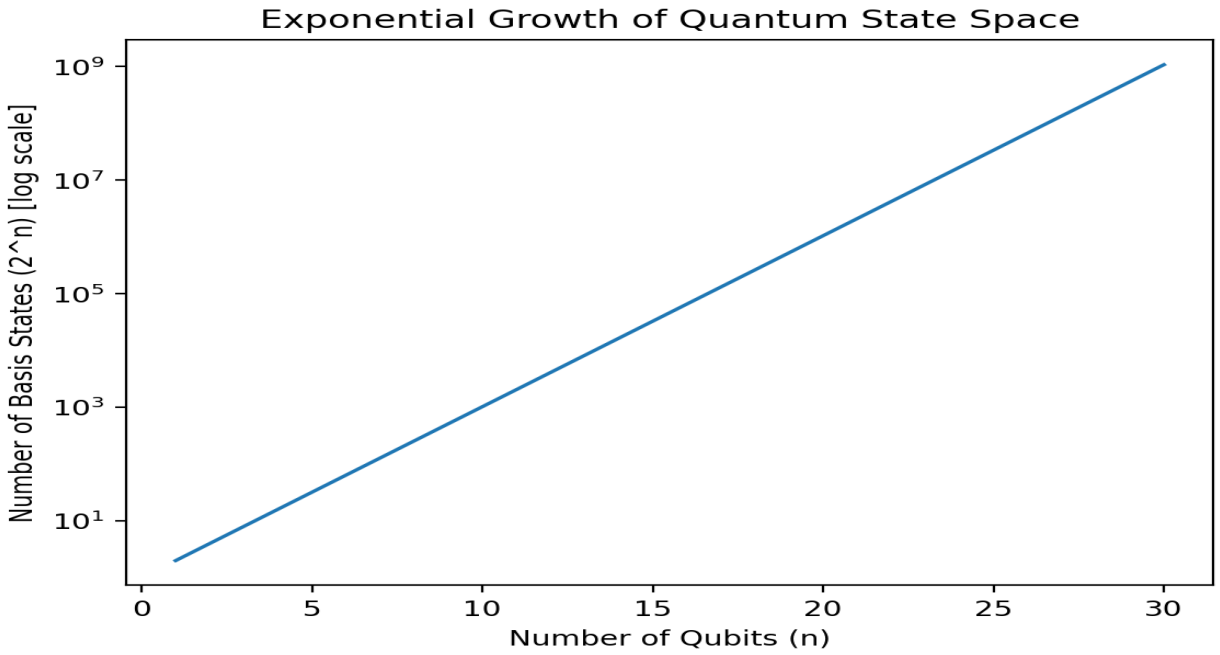
$$\left|\psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x \right| x\rangle, \qquad \sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1$$

2.1. Quantum Algorithms and Threats

The principles of quantum mechanics and the theory of quantum information enable the creation and management of quantum bits. Quantum mechanics underpin a quantum computer's extraordinary capacity to parallel process vast quantities of data and to analyze that data. A quantum computer calculates using qubits—systems that maintain the unique traits of quantum bits. The qubit is the building block of quantum computing systems, similar to a regular bit, which stores information through binary states. Nevertheless, unlike standard bits, which can exist in either 0 or 1 state at any point, a qubit can exist in both states 0 and 1 at the same time.

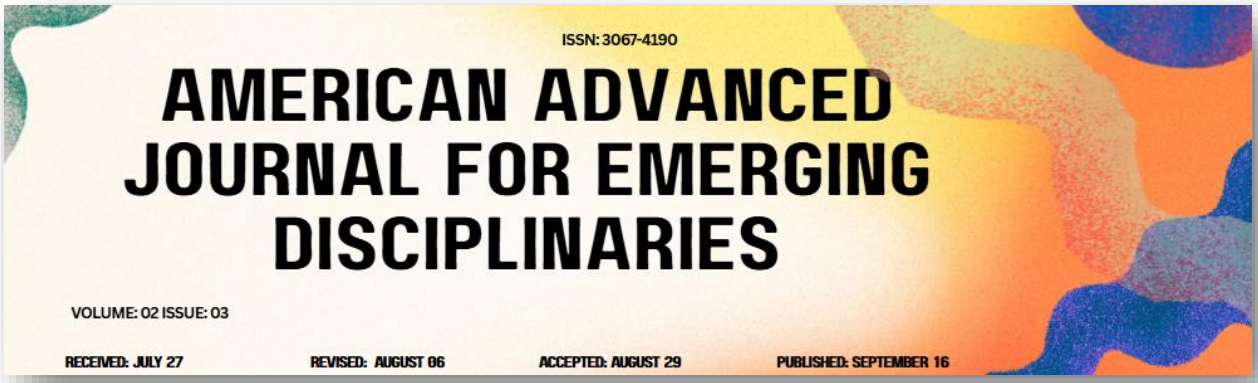
ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

It may sound impossible, but it works because the probability amplitude of a qubit's quantum state enables it to exist in multiple states simultaneously. This unique capacity of a single qubit allows many qubits to store exponentially larger amounts of data than one would expect based on their physical size. For example, six classical bits can only be in a single configuration such as "000000," while six qubits can be in the configuration "000000 + 000001 + 000010 + ... + 111111" simultaneously. Consequently, 100 qubits are capable of being in a superposition of the 2100 classical configurations. During a quantum computation, the quantum states are not entangled at all but are synchronized through a set of carefully controlled quantum gates incorporating auxiliary qubits and classical information for coherence.



2.2. Implications for Classical Cryptography

Many components of the Shor algorithm significantly improve the expectations around existing non-quantum-based cryptographic protocols. These include the implication of the quantum-discrete logarithm problem concerning the security of protocols based on the discrete logarithm problem and the index computation problem. The quantum information theory of

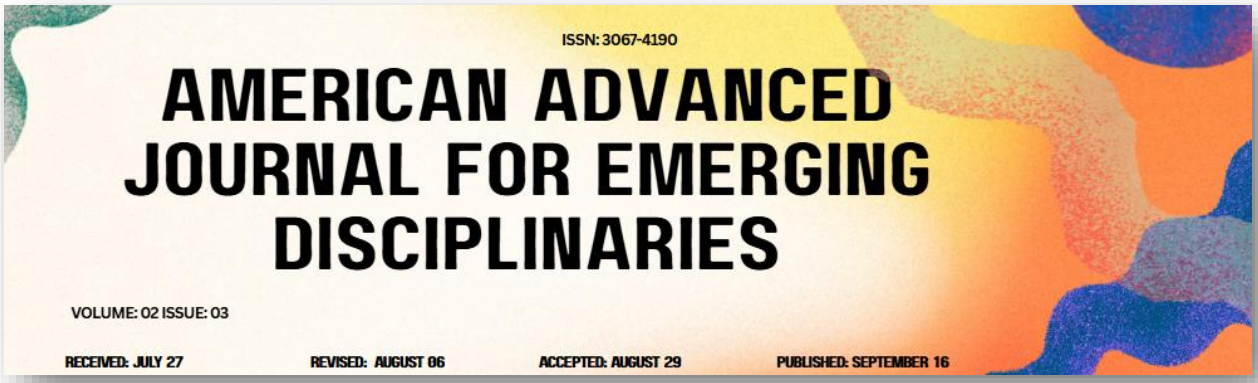


Grover implies that if a hash function is being used only as a generic (n, d)-hard function and can be tested against the definition of a (n, d)-hard function, then the size of the input to the hash function should be at least doubled to resist brute-force attacks sufficiently. Another important aspect of quantum computing is the quantum decision-tree complexity, which implies that the worst-case query complexity of a quantum decision tree is at most $O(\sqrt{n})$ times smaller than the worst-case query complexity of a deterministic decision tree. It is clear that the development of quantum computers is the area forbidding all cryptographic protocols that rely on the intractability of factorization or constituted problems.

Dismissed by classical means, an attack using quantum computers reduces the security of any protocol based on (n, d)-hard functions when the privacy/uniqueness strength is lower than or equal to d. Solutions based on weakly unforgeable signatures, public-key encryption, and key establishment must increase their privacy, uniqueness, or separation strength to at least d + 1 to remain secure against any adversary in the quantum-bounded model. The implication for classical cryptography is that protocols designed against quantum adversaries facilitate security in the classical framework. Designing protocols with respect to a quantum adversary is not only important because of the relevance of quantum computation, but also because of its influence on the classical world of computation.

3. Quantum-Resistant Cryptographic Paradigms

Quantum-safe cryptanalysis literature primarily addresses quantum-resistant alternatives to traditional encryption, key establishment, digital signature, and hash functions. While the cryptanalytical analysis of classical algorithms is exceedingly time consuming and often infeasible, quantum computing gives cryptanalysts a comparatively potent tool. Implementation of ECDSA or RSA signatures with short keys can be temporally tolerated, but the compromise of long-term key exchange algorithms (e.g., VPN, IKE, TLS key agreement) gives adversaries an opportunity to capture or passively intercept large quantities of encrypted network communications. Implementation using shortened SHA-1 hash sizes for near-term signatures or generational key multiplexing can mitigate the risk of these short keys in relatively controlled environments. Limiting digital security to “good enough” for cat-and-mouse security simply delays the inevitable and increases the likelihood of being adversely affected by discovery of a working quantum computer.



Three leading algorithms of contrastive directions in the digital veracity are the NTRU lattice encryption algorithm (lattice-based), HFE-keyed digital signature of Halinski & Wang, and the Queensland and Rutgers-Latvian University fast, reliable code-based signature based on error correction syndrome-tagged elliptical curves of Texas A&M University, the University of California-Irvine, and the National University of Radio physics and Electronics in Novosibirsk. Cryptography Exchange offers a collection of competitors suited to both near-quantum and long-term cryptanalysis in the contemporary Quantum Confusion Era (QCE). While security requires the proper deployment of the Scheme in a secure environment, its expected facilities of key multiplexing and commercial timeliness should prospectively facilitate its deployment and enable Interactive Digital Cryptographic Control for World Peace in the Magic Internet Years.

3.1. Post-Quantum Cryptography Standards

The National Institute of Standards and Technology (NIST) initiated its post-quantum cryptography (PQC) standardization effort in 2016, focusing on public-key encryption and key-establishment protocols. A total of 82 proposals were submitted, with 26 shortlisted for Round 2. Following a multi-round evaluation process, NIST selected four schemes for standardization: three key-establishment protocols (CRYSTALS-Kyber, NTRU, and SIKE) and one public-key encryption/signature scheme (CRYSTALS-DILITHIUM). Two additional signatures (FALCON and SPHINCS+) were classified as alternate candidates. Remarkably, no PQC scheme with

ISSN: 3067-4190

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 02 ISSUE: 03

RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

proven resistance against quantum computers was known.

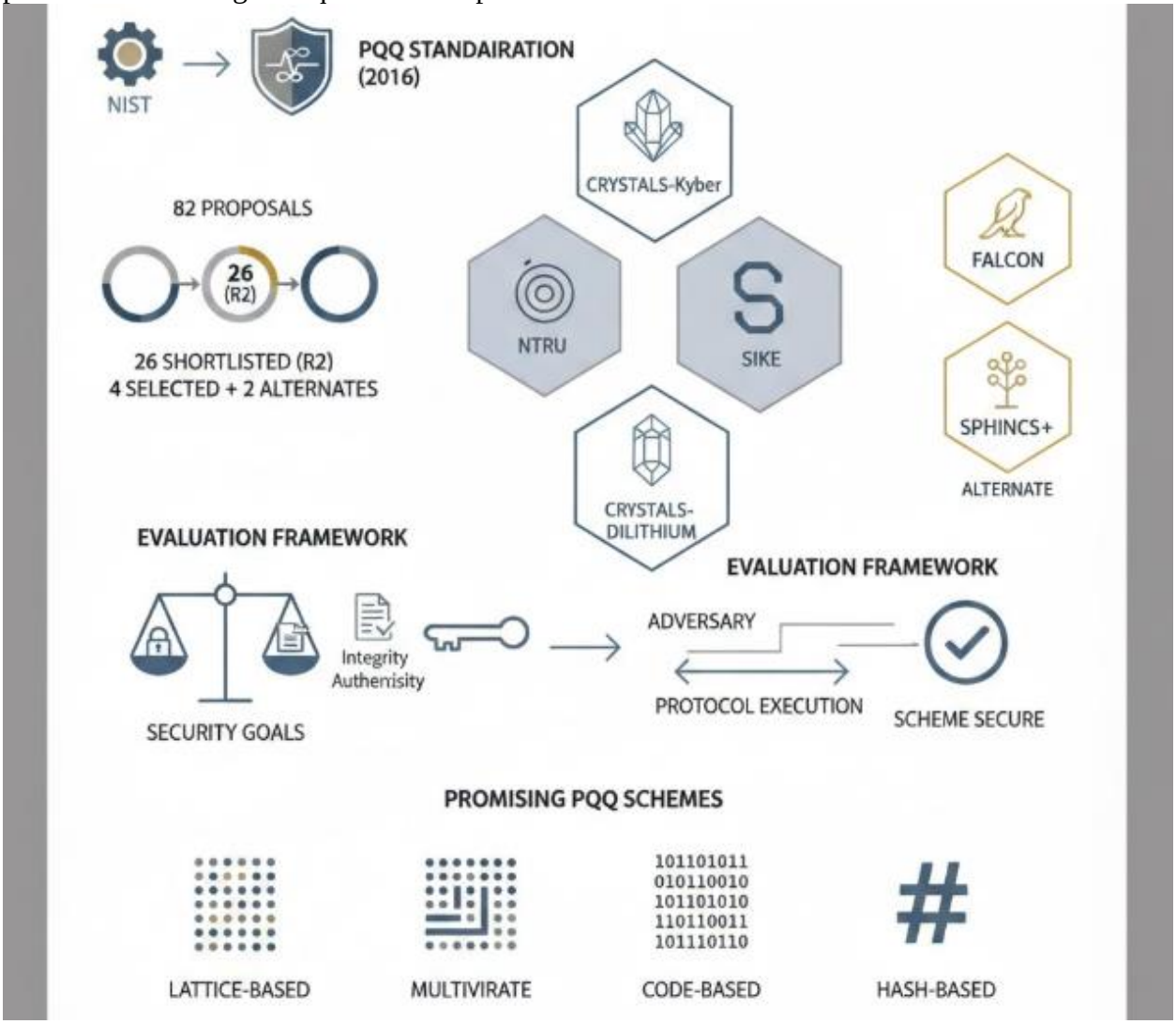
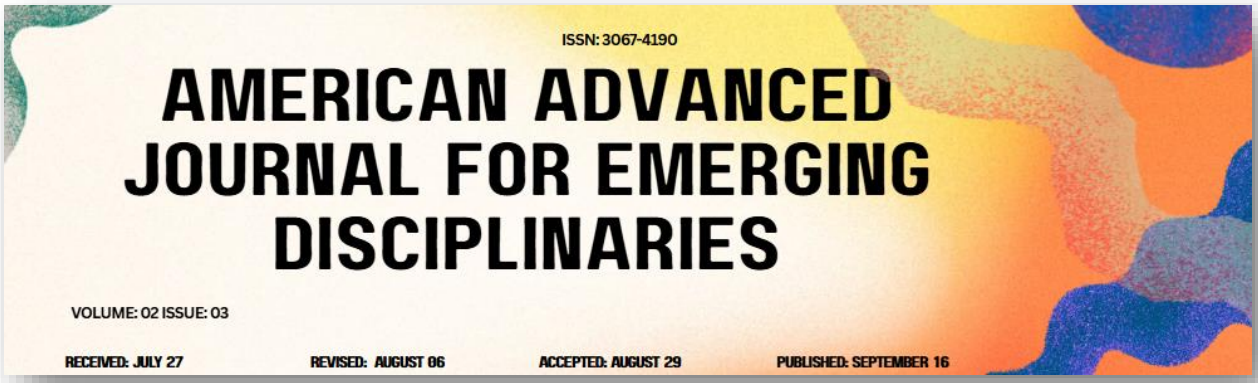


Fig 2: From Competition to Consensus: A Combinatorial Evaluation Framework for NIST's Post-Quantum Cryptographic Standards



"Post-Quantum Cryptography: A New Standard for an Old Problem" discusses the PQC standardization effort and highlights the key selection criteria. An evaluation framework describes the consideration of multiple aspects combinatorially, contrasting them with alternative approaches for symmetric key length selection. The chapter concludes by identifying lattice-based, multivariate, code-based, and hash-based PQC schemes as the most promising for future adoption.

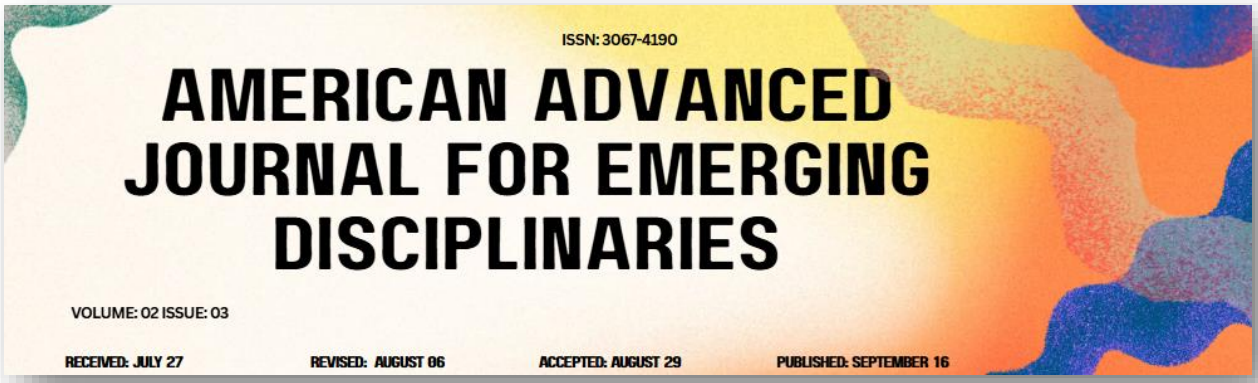
Cryptographic protocols aim to provide information security goals—such as confidentiality, integrity, and authenticity—against potential leaks and forgeries. These goals can be expressed formally as game-based security definitions between an adversary and an experimental execution of the protocol. If the goals hold, the scheme is secure. The definitions are then used to develop a construction for the protocol that is secure against the specific type of adversary.

3.2. Lattice-Based and Multivariate Schemes

Lattice-based and multivariate systems dominate post-quantum public-key encryption and digital signature proposals and are widely perceived as strong candidates for standardized solutions. Research continues to widen their applications and reduce computational costs by seeking new underlying hard problems, novel security proofs with smaller key sizes, and simpler encryption and signing procedures.

Examples of lattice-based public-key cryptosystems include the NTRUEncrypt encryption scheme; the NTRUSign and BLISS signature schemes; and the Encryption for Lattice and PoV-based Group Signatures (E-LAGT) digital signature scheme. The latter can accommodate very small key sizes, but does not offer efficient signing or verification; substantial improvements have recently been proposed. An example of a lattice-based key encapsulation mechanism is NewHope, a recent key-exchange mechanism that has been adopted in beta by Google’s native Android applications. Multivariate cryptography remains popular for digital signatures, with GGH14 as the benchmark, but has made only limited forays into encryption.

Lattice-based systems and multivariate schemes are attractive because their underlying hard problems resist both classical and quantum attacks, and because they are the only remaining submissions that offer cryptographic signatures with clear efficiency advantages against all existing asymmetric signatures. Both families are considered suitable for at least limited use in



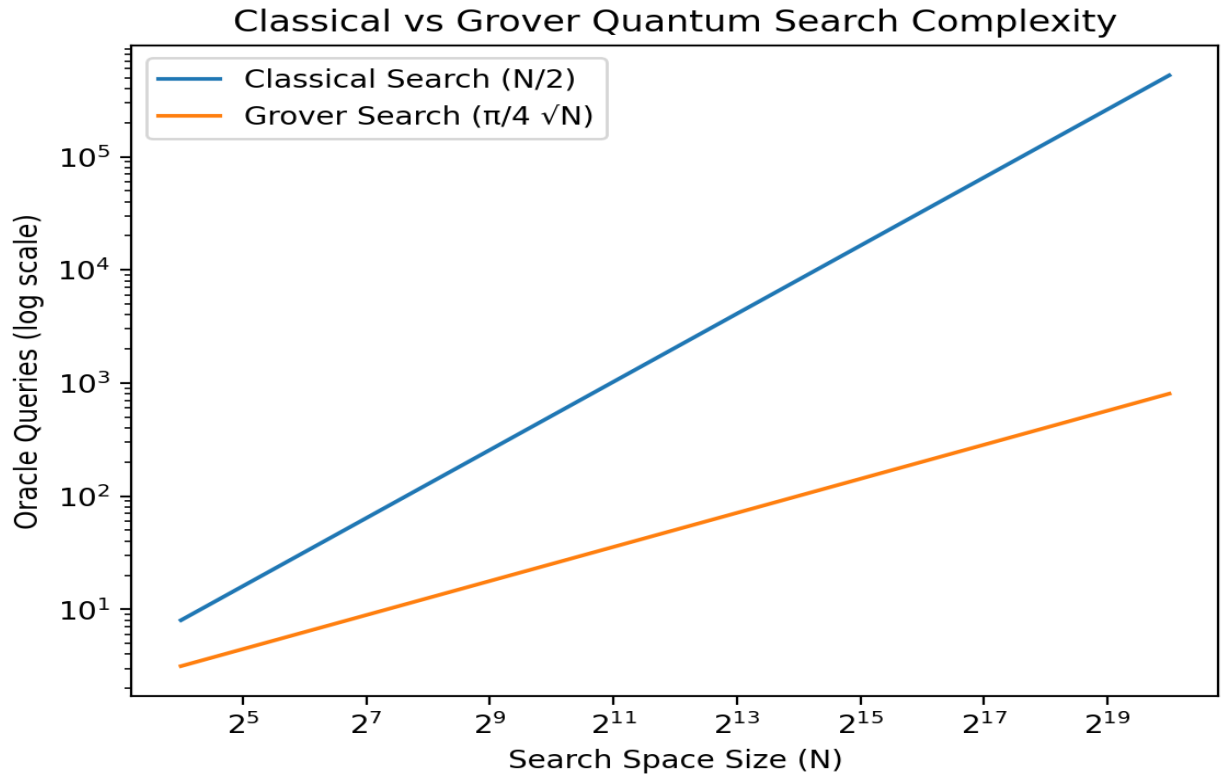
the most resource-constrained environments, although the signers and verifiers of the signature schemes must still leverage significant resources.

4. Digital Warfare and Deterrence Theory

Digital warfare deploys a set of cyber operations and techniques to elude and disrupt communication systems, attack critical infrastructure, corrupt key data or models, and embarrass governments and leaders. Such actions intensify geopolitical tensions and contribute to a new form of cold war, fuelling a pressing demand for effective deterrence measures. Cyber deterrence has been discussed extensively, addressing the implementation of classical deterrence theory concepts of denial, punishment, resilience, and stability; adapting co-operation, coercion, threshold, and capability-hardening considerations; and examining the development of deterrent frameworks for strategic stability, coercive diplomacy, and conditions for success. Yet, despite the growing use of cyber capabilities, no established government has made the first offensive move in a significant cyber conflict, giving rise to a cyber cold war.

Looking to the future, the emergence of quantum computers capable of breaking existing public-key protocols raises questions not just about the denial and punishment postures of a cyber cold war, but also about the deterrent options available to both quantum-capable offensive actors and their targets. For a sufficiently powerful Quantum Computer, the building blocks of contemporary cyber deterrence fall away; the capability to introduce risk through punishment no longer protects a state from the repercussions of its actions, nor does a resilient cyber posture shield from the threat of coercion and a lack of stability in sensitive geopolitical affairs. However, the emergence of Quantum Computing opens more than just a risk: offensive ability can outpace the growing capabilities of Quantum Computers. If just a part of the message of Quantum Information Theory can be put into action, then the potential to deter through the demonstrated ability to puncture current public key systems, thus removing a certain operational element of classical asymmetric warfare, becomes possible.

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16



Equation 2) Grover's algorithm (step-by-step) and why it is $O(\sqrt{N})$

The references Grover and "faster than classical search" and also implies doubling hash input sizes against brute force.

2.1 Problem setup

We have an unstructured search over N items. There is (for simplicity) one "marked" solution w. Define oracle $f(x) = 1$ iff $x = w$, else 0.

Oracle phase flip:

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

$$\mathcal{O}_f|x\rangle = (-1)^{f(x)}|x\rangle$$

(standard formulation)

2.2 Start in uniform superposition

Use Hadamards to create:

$$\left|s\right\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\left|x\right\rangle$$

Initial success probability if you measure immediately:

$$P_0 = |\langle w|s\rangle|^2 = \left|\frac{1}{\sqrt{N}}\right|^2 = \frac{1}{N}$$

2.3 Decompose into a 2-D rotation plane

Let

$$|w\rangle = \text{(marked state)}, \qquad |w_\perp\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq w}|\,x\rangle$$

Then $|s\rangle$ can be written:

$$|s\rangle = \sin\theta\,|w\rangle + \cos\theta\,|w_\perp\rangle$$

Compute $\sin\theta$:

$$\sin\theta = \langle w|s\rangle = \frac{1}{\sqrt{N}} \quad \Rightarrow \quad \theta = \arcsin\left(\frac{1}{\sqrt{N}}\right)$$

2.4 One Grover iteration = two reflections = rotation by 2θ

Define diffusion operator (reflection about $|s\rangle$):

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

$$D = 2|s\rangle\langle s| - I$$

Grover iterate:

$$G = D\,\mathcal{O}_f$$

Geometrically, $\mathcal{O}_f$ reflects about $|w_\perp\rangle$ and D reflects about $|s\rangle$; two reflections compose into a rotation by 2θ in the span $\{|w\rangle, |w_\perp\rangle\}$.

After k Grover iterations:

$$G^k|s\rangle = \sin\big((2k+1)\theta\big)\,|w\rangle + \cos\big((2k+1)\theta\big)\,|w_\perp\rangle$$

So the success probability is:

$$P_k = \sin^2\big((2k+1)\theta\big)$$

2.5 Choose k to maximize success

We want $(2k+1)\theta \approx \frac{\pi}{2}$.

$$(2k+1)\theta \approx \frac{\pi}{2} \quad \Rightarrow \quad k \approx \frac{\pi}{4\theta} - \frac{1}{2}$$

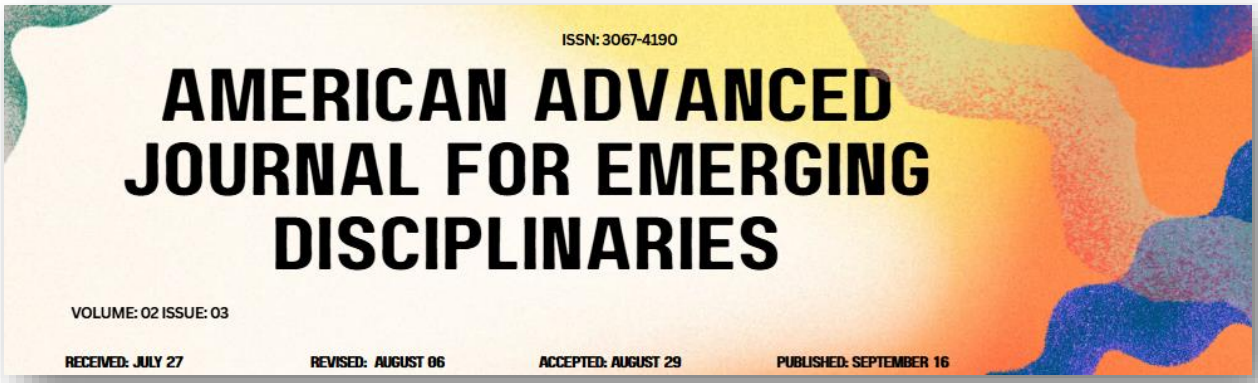
For large N, $\theta \approx \frac{1}{\sqrt{N}}$, hence:

$$k \approx \frac{\pi}{4}\sqrt{N}$$

Therefore Grover uses $O\big(\sqrt{N}\big)$ oracle calls (headline result).

4.1. Concepts of Cyber Deterrence

In digital warfare, cyber deterrence theory broadly constitutes an unseen strategy, which implicitly strives to prevent a future conflict. Concepts of strategic stability and coercive diplomacy, derived from classical nuclear deterrence theory, comprise the core of this theory. Strategic stability prevails if states, through capability hardening and other risk management



strategies, do not reduce the likelihood of war despite heightened tensions. Such stability requires mutual cognizance and sufficient monitoring of the full capability spectrum. Cyber deterrence operates under two assumptions. First, the attacking nation possesses a credible threat arsenal. Second, the target nation continues an offensive-defensive posture, aiming to succeed as the aggressor and thereby attain its strategic goals. Coercive diplomacy examines whether threats of punishment deter an operator from an affirmative cyber act. Coercive diplomacy operations, including cybercalibrated responses, assume that an operator's threshold lies below the deterrence-offer level.

When applied to classical and conventional deterrence theory, the transitive response between adversarial abilities is a necessary but insufficient condition for operational deterrence. Such transitive posturing arises from geographical realities, relative political structures, and informative systems. The existence of cyberdeterrent theory does not occur across all digital actors. Subsequent discussion of these concepts relies on similar definitions, arguing that states cannot always impose strategic or transitive stability on others. Mutual transitive stability is possible in digital space only if states conditionally accept the existing of-function state—namely, that constrained systems are stable systems.

5. Deterrence Mechanisms in Quantum Contexts

Digital-defence strategies encompass a range of instruments designed to protect electronic assets against future potential exploits. These include risk management, organisational resilience, capability hardening and the establishment of advance warning systems. Although cyber deterrence is primarily associated with offensive capabilities, deterrent effects can also be achieved by investing in demonstrably impenetrable defences. Within a quantum context, these effects may be obtained by demonstrating that the cost of overcoming available defensive measures outweighs the perceived strategic payoff.

Recent advances in quantum machine learning highlight the challenges of risk management and defence in depth. These problems arise not only from the ability of quantum adversaries to steer processes within uncontrollable quantum systems but also from the enhanced capabilities for classified quantum ciphertext surveillance and for modelling and predicting the behaviour of classical systems such as power grids, financial institutions and supply chains. Nevertheless, the central principle remains valid: effective risk management and robust defence-in-depth techniques reduce the probability of successful attack and serve as a hedge against

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

highly uncertain quantum threats. Opportunities to achieve deterrent effects should therefore be evaluated.

5.1. Defensive Postures and Risk Management

In the context of cyber deterrence, defensive postures against quantum threats comprise multiple interrelated dimensions. Defense-in-depth strategies seek to reduce exposure to quantum-enabled attacks and mitigate any breaches, while risk management processes account for transfer and acceptance of quantum risk. Resilience concepts encompass adaptation and recovery from operations that do encounter quantum risk, and capable hardening examines quantitative offset of sub-threshold operational risk by increased capability.

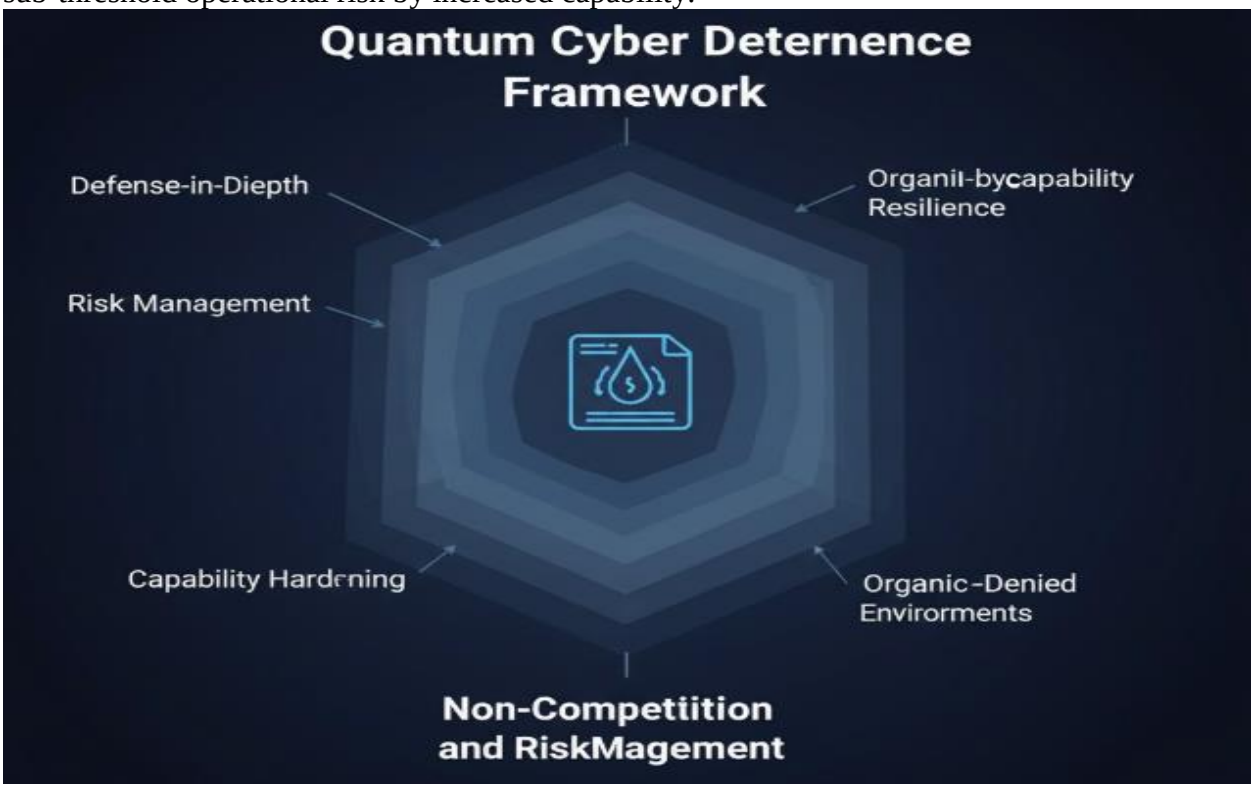
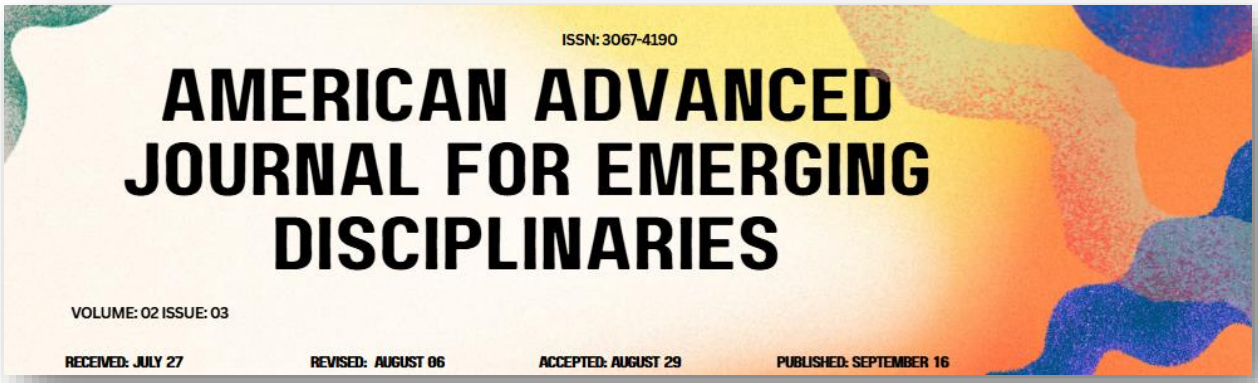


Fig 3: Quantum-Enabled Cyber Deterrence: A Multi-Dimensional Framework for Denial-by-Capability and Operational Resilience



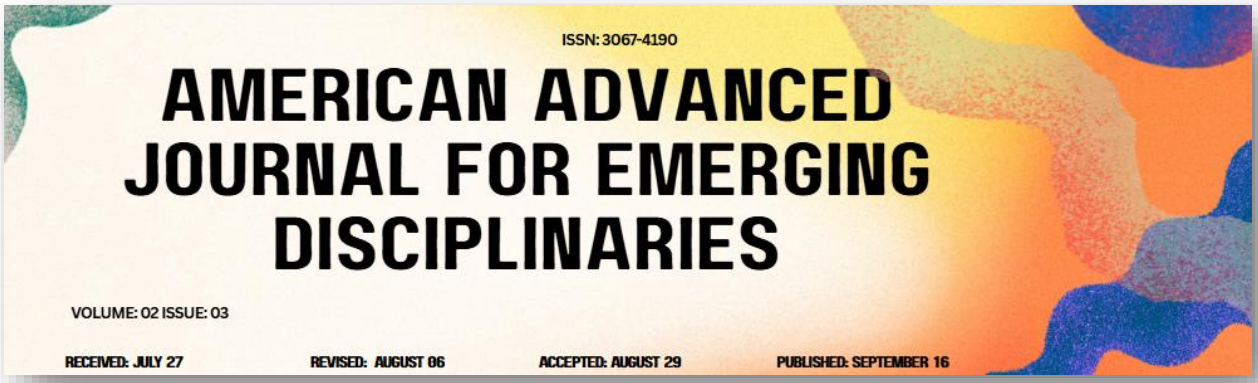
A place for deterrence as a quantum concept in cyberspace manifests in expected-organic-denied environments: threats of retaliation by adversaries perceived as unwilling or politically unable to execute denial are seen to create exploitable layers of opportunity. Further work shows that the depth of denial-by-capability posturing, in combination with the availability of some counter-capability, may work to create mechanisms for non-competition in cyber operations. In these arenas, quantum or quantum-enabled capabilities can act to open windows of opportunity for denial attacks in-depth through asymmetric improvement. Elements within quantum development and defence third-party cooperation also work towards reinforcing some cake-sharing panes.

5.2. Offensive Capabilities and Thresholds

Strong quantum capabilities exhibited extant or anticipated by state and non-state actors—apparent through direct actions, capability disclosure or defence investment—could enable coercive cyber-offensives or active cyber-warfare against quantum-resistant deployed alternatives, which may nevertheless remain expeditionary, adversary-specific and time-limited. Such capabilities would accordingly be made delicate again through investments in post-quantum cryptography standards by adversaries. Although deterrent thresholds and conflict deterrence may still therefore correspond with shocks to cyber-stability following losses of quantum futures, political thresholds for considering and accepting shocks or responsiveness appear more open than would act in traditional conflict.

Credited deterrent actions—such as capable hostile operations against values or Command Control Intelligence Support Systems (CCIS)—at-power should therefore also consider other-than-their-normative-audiences, including relevance in decision-processes by state leadership outside the quantum challenge because of such opening. Recognising the comparative breaking of boundaries between deterrents from and vulnerability to quantum futures, Deterrence Theory analyses into quantum contexts require scrutiny of expected forms and bodies at stake, and the requisite norms for military operations when operating across classes with different forms. But the analysis of ethical, legal, strategic or just-political regimes would ideally occur only later, to permit the genesis by testing of possible operations that now reward daring in all Capitals.

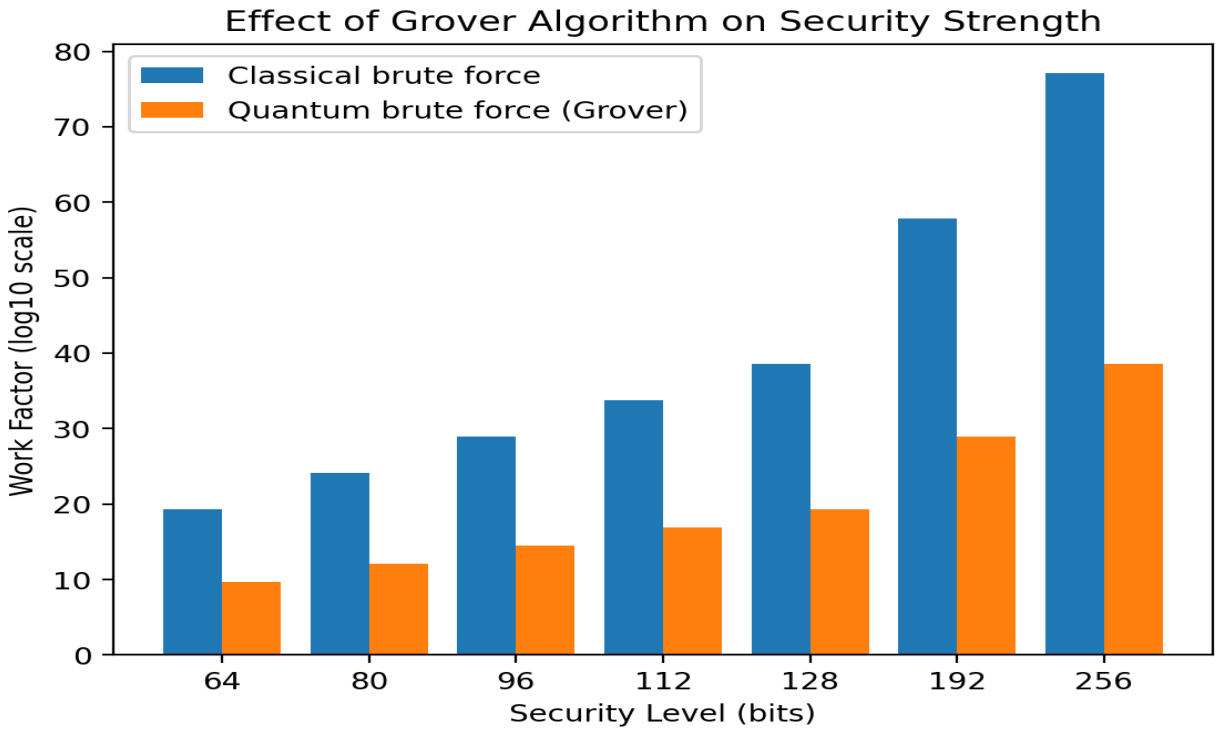
6. Policy and Governance Implications



The threat of quantum computing is more immediate in cyber warfare than anywhere else. The development of threat-neutralizing codes has been acknowledged as a significant project in many nations, and efforts have been launched to create new configurations. Adaptation to a new defense environment is desired. It is logical for countries with these deterrence capabilities to use this factor to enhance their cyber-deterrence approaches. At present, whether these deterrence approaches are feasible is a speculative issue. The debate centers on four areas: risk management, resilience improvement, strengthening of deterrence capabilities, and the establishment of offensive deterrent capabilities.

Six possibilities exist for risk management. First, threat detection is a process that involves achieving awareness over threats. No system is completely safe, as illustrated by the disclosures from Snowden and Pegasus. Second, a system hardening targeting hidden vulnerabilities will never be sufficient. An additional approach is to strengthen software quality at the large-volume-open-source code level. Third, if a detection technology to discover hidden threats is developed, it is possible to test open-source codes to detect hidden flaws, just as constructors investigate the integrity of codes. Fourth, it is important to develop risk answers for those threats that cannot be completely prevented. Fifth, a deterrence capacity adjustment strategy should accompany the deterrence capability adjustment strategy to respond to the evolution of a nation's offensive capabilities. Lastly, the relatively higher establishment and operating costs of quantum computers should be exploited to delay the production of quantum computers in adversarial nations.

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16



Equation 3) Shor's algorithm (step-by-step) as "factoring → order finding"

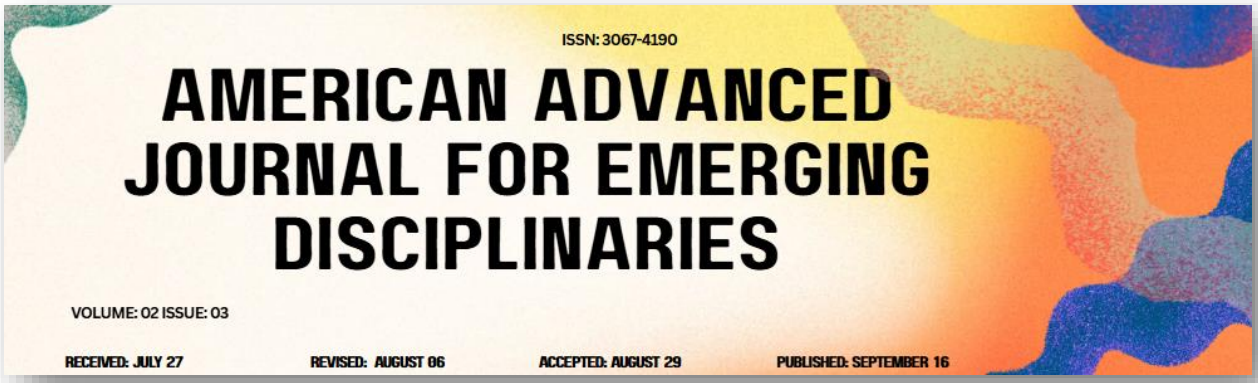
The identifies Shor as the "quintessential threat" and notes RSA relies on factoring.

3.1 RSA security assumption (factoring)

RSA modulus:

$$N = pq \quad (p, q \text{ large primes})$$

Breaking RSA essentially requires finding p, q (factoring N).



3.2 Shor reduces factoring to order finding

Pick random integer a with $1 < a < N$. Compute:

$$\gcd(a, N)$$

- If $\gcd(a, N) \neq 1$, you already found a nontrivial factor.
- Otherwise, a is invertible mod N.

Define the **order** r of a modulo N:

$$r = \min\{r > 0 : a^r \equiv 1 \pmod{N}\}$$

3.3 Why order gives factors

If r is even, consider:

$$a^r \equiv 1 \pmod{N} \quad \Rightarrow \quad a^r - 1 \equiv 0 \pmod{N} \quad \Rightarrow \quad \left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) \equiv 0 \pmod{N}$$

So N divides the product. Often (not always) this implies N shares a nontrivial gcd with one of the factors:

$$p_1 = \gcd\left(a^{r/2} - 1, N\right), \qquad p_2 = \gcd\left(a^{r/2} + 1, N\right)$$

If additionally $a^{r/2} \not\equiv -1 \pmod{N}$, then at least one of these gcds is a nontrivial factor.

3.4 How the quantum part finds r (phase estimation idea)

Shor uses quantum period finding / phase estimation to extract information about the periodic function:

$$f(x) = a^x \bmod N$$

This function has period r in the exponent (modular sense).

The quantum subroutine produces a measurement outcome k such that:

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 02 ISSUE: 03
RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

$$\frac{k}{Q} \approx \frac{s}{r}$$

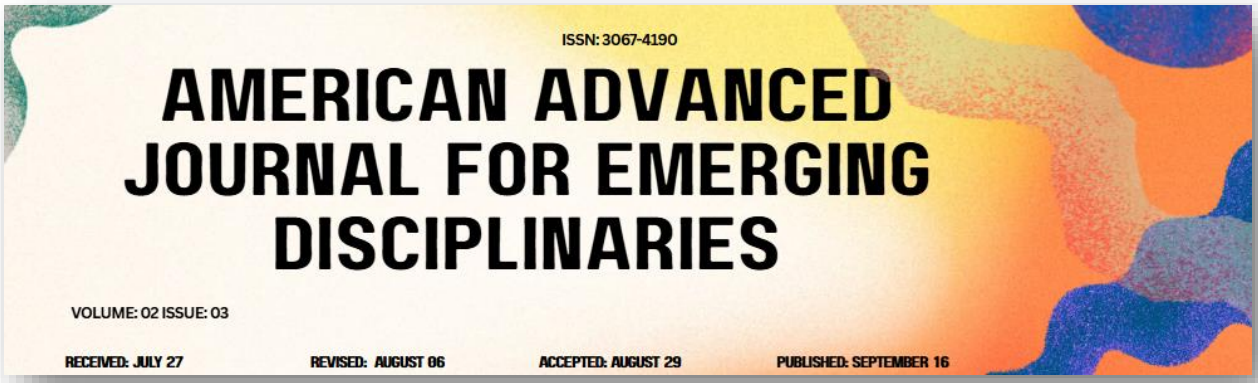
for some integer s, where Q is a power of 2 chosen large enough. Then you recover r by **continued fractions** on k/Q to find the best rational approximation with small denominator

6.1. International Cooperation and Norms

Opportunities for cooperation abound in the quantum domain, particularly regarding the development of international standards for quantum keys, quantum key distribution protocols, and quantum-safe cryptography. Specific national or regional quantifiable advantages may be foregone at this initial stage of development. Managed growth may mitigate the risk of a new science arms race, and the avoidance of low-cost quantum-safe international keys may allay concerns that quantum-safe systems hurriedly developed by single states may become known to other parties.

Governments are already investing heavily in national quantum-enabled cryptographic capabilities and are concerned that within a decade-once quantum computers of sufficient scale may become publicly available-robust quantum-safe keys may no longer be available for delivery to end-users by trusted sources. The identity management and public-key infrastructure necessary to enable trustworthy quantum key distribution and delivery must be operationally solved before the first spurious or computationally reversible costs of quantum cryptanalysis destabilize current public-key protocols. Without reliable means for the non-repudiation and identity credence of quantum keys, recipients will be obliged to build trenchant skepsysms against external quantum costs by avoiding quantum key use and digital confidential and secrets or alternative services.

Vulnerabilities in defence-mined fixed-dimensional key-establishing systems with direct quantum bypass-security proofs have already been identified, raising the spectre of serious pan-economical and critical infra-structural and service interruptions devoid of readily available quantum-safe alternatives. The ethical guidance of the Geneva Dialogues on Ethics of Emerging Military Technologies (GDEMET), directed at systems with positional-empirical high-tech advantages, applies equally to systems-provide-cost quanta and SPDC, SHG- and DAC-based techniques–algorithms cannot be a justifying precept for developing offensive largetry.



6.2. Standards, Certification, and Compliance

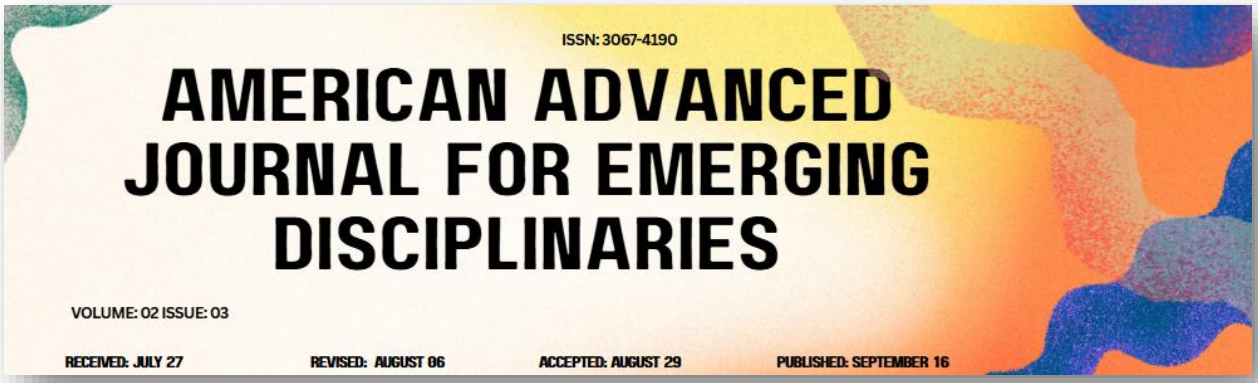
Diabetes is a disease that affects the body's ability to produce and/or respond to insulin and subsequently leads to abnormal metabolism of carbohydrates and elevated levels of glucose in the blood and urine. Diabetes can be classified into two major categories, type 1 and type 2. Each type differs in its pathophysiology, treatment, and potential complications.

Diabetes occurs from a deficiency of the hormone insulin secreted by the beta cells of the endocrine pancreas. Diabetes has an insidious course and presents with the classic symptoms of polyuria, polydipsia, polyphagia, and weight loss. The diagnosis is based on a fasting plasma glucose concentration of 126 mg/dL or higher, a casual plasma glucose concentration of 200 mg/dL or higher associated with classic symptoms, or an abnormal oral glucose tolerance test. A fasting plasma glucose concentration greater than 126 mg/dL needs to be confirmed by a second fasting plasma glucose measurement, unless the patient has the classic symptoms of hyperglycemia or hyperglycemia crisis.

Type 1 diabetes is an autoimmune process whereby T-lymphocyte-mediated destruction of the pancreatic beta cells leads to insulin deficiency. It typically presents in childhood or adolescence. Type 2 diabetes results from a combination of resistance to insulin action and an inadequate secretory response by the pancreatic beta cells. It is most prevalent in older, obese individuals. Diabetic patients are predisposed to atherosclerosis and its complications, especially coronary heart disease. Diabetes mellitus can also be associated with cystic fibrosis, may be secondary to pancreatic disease, and can result from a variety of endocrine disorders.

7. Conclusion

The analysis demonstrates that quantum computing represents a profound, fundamental risk not just for the brute-force breaking of encryption with widespread consequences, but also for the strategic deterrence game such capability unleashes: the destabilization of deterrent balances, the introduction of new offensive threats, and new forms of existential risk. Empirical evidence strongly suggests that the state of these domains, conceptually and operationally, may currently be viewed as the reverse of stabilizing—these elements suggest it is improbable that countries will be able to credibly deter one another from pursuing full-scale quantum offensive capabilities. Those findings provide a framework for identifying not what should be done to attain deterrent stability but rather, what should be avoided to prevent rapid strategic destabilization.



Preparation and consideration of defensive postures able to lessen the danger of rapid destabilization should focus on quantum-resilience in terms of robust risk management; indeterminate resilience to risk that cannot be cost-effectively eliminated, for instance by quantum-secure cyber; and general capability hardening. Similarly, much is to be hoped from investment in capabilities able to enable an ex ante accounting for constraints. At the same time, a far-reaching, concentrated effort is needed to ensure a properly integrated understanding of deterrent dynamics in quantum environments, combining the perspective of deterrent stability—the ability to deter the use of full-scale quantum capabilities— with those aspects highlighted in the analysis: the opportunity to accelerate their development and use.

ISSN: 3067-4190

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 02 ISSUE: 03

RECEIVED: JULY 27 REVISED: AUGUST 06 ACCEPTED: AUGUST 29 PUBLISHED: SEPTEMBER 16

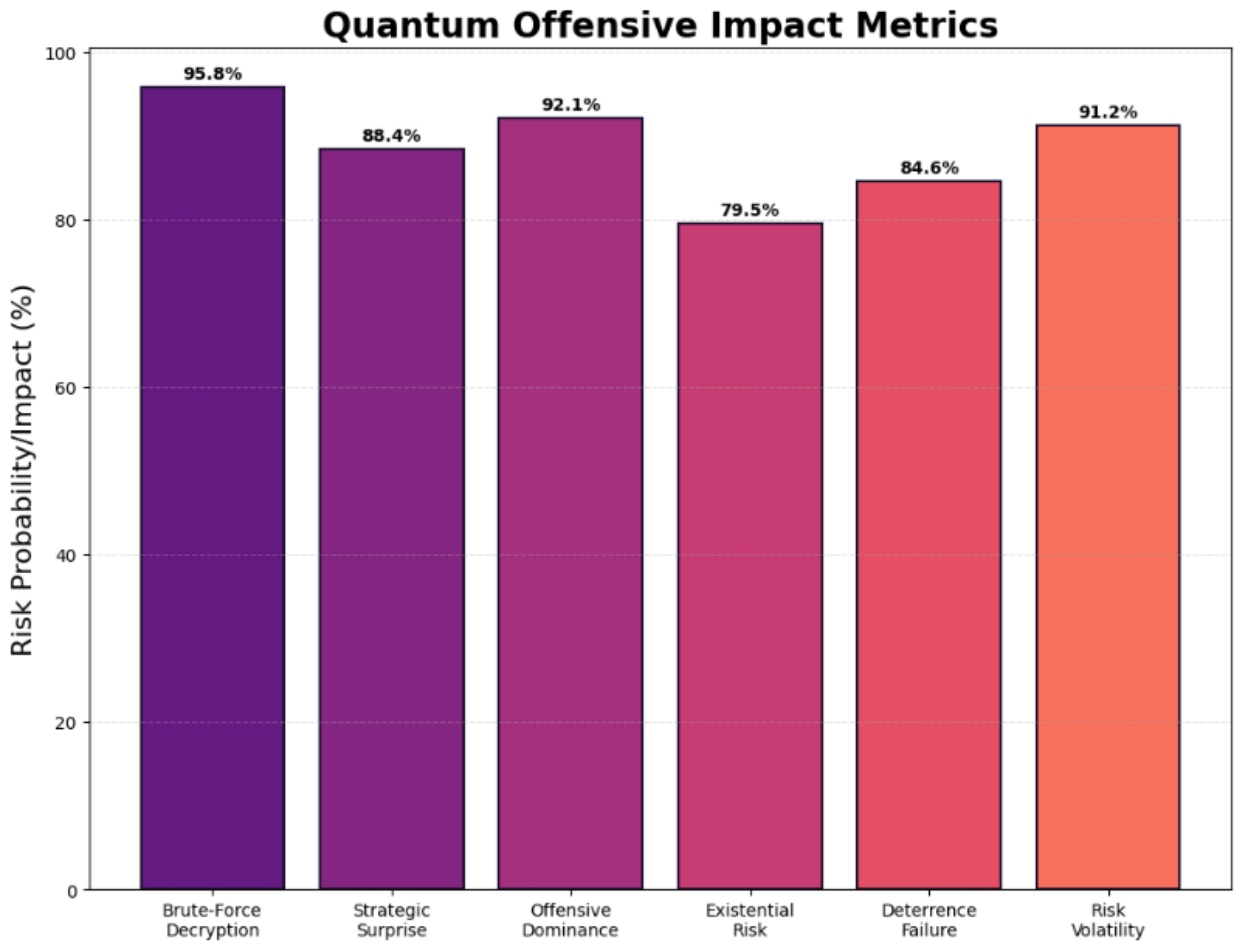
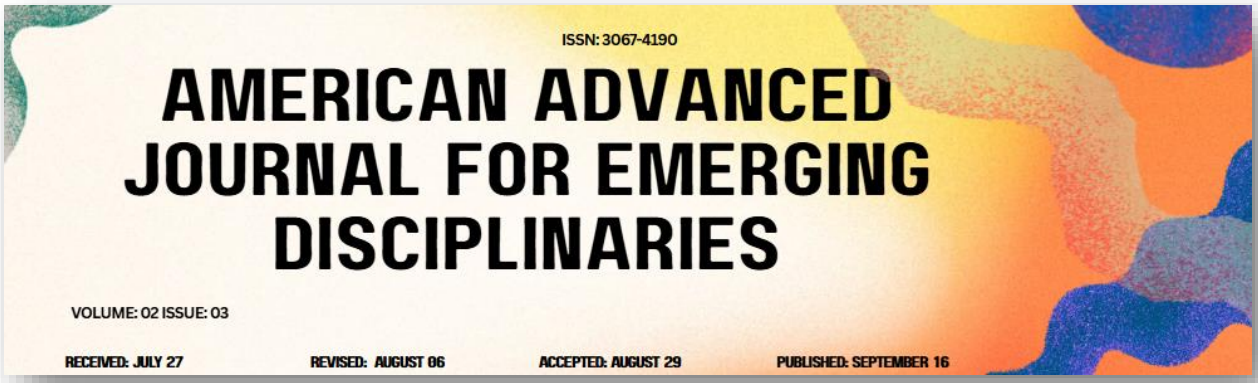


Fig 4: Quantum Offensive Impact Metrics

7.1. Final Reflections and Future Directions

Although quantum threats to cryptography have yet to reach a level of maturity that justifies a radical overhaul of current defenses, robust solutions nonetheless require a time-consuming evaluation process. Such cycles should be informed by possible future developments in capability, doctrine, and decision-making with regard to quantum technology in the context of cyber deterrence. These considerations suggest that the risk landscape for these operations and

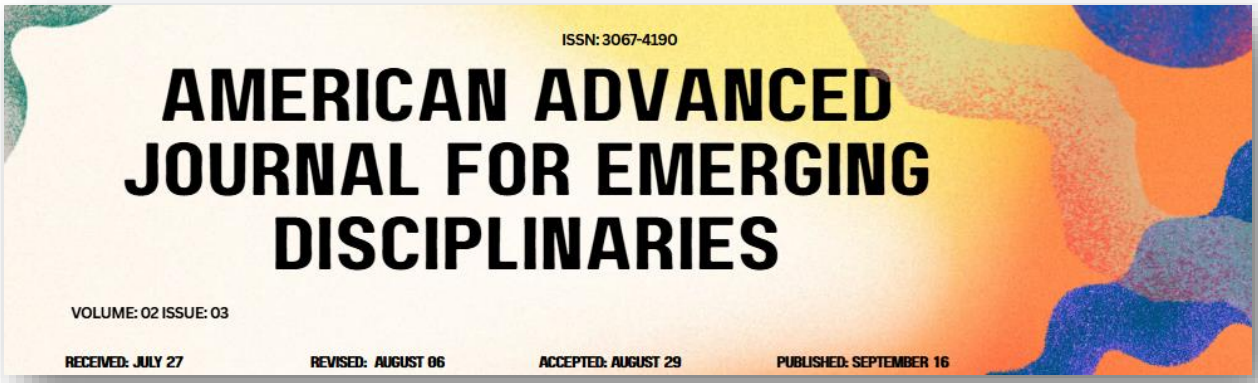


their supporting resources, services, and infrastructures may change over time, warranting a monitoring regime to ensure their security remains commensurate with between- and within-war expectations of enemy behavior. Speculating on future developments in quantum capabilities is inherently difficult, yet they remain of considerable strategic interest to all possessors, innovators, and adjacent actors, particularly given the dangers they pose to critical high-technology services that could be relied on to support a country's economy, prosperity, and military might in the face of an imminent conventional conflict.

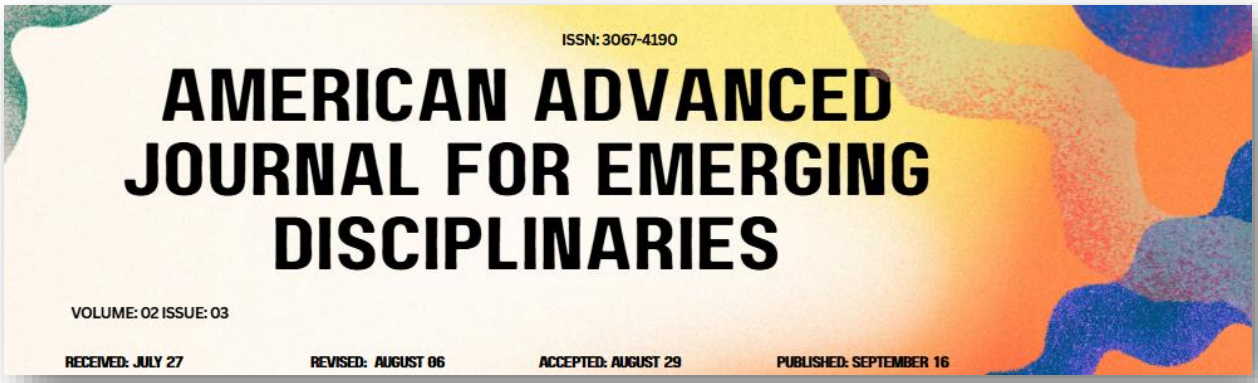
The implications of potential future quantum capabilities for quantum-coercive cyber operations are even more elusive. Warfare, particularly deterrently directed conflict, is about military capability and willingness to employ it, where the future calculus of choice governs responses to perceived advantages held by an opponent. Thus, if the possessors of a revolutionary quantum capability that might have an impact upon global strategic stability were subsequently to relax their deterrence posture towards their own expected cyber-harder targets, an irregular, asymmetrical or indirect deterrence edge may evolve for regions or actors lacking development of a similar quantum capability or deterrent force. The challenge remains for these nations or regions to monitor the service-resilient defensive posture maintenance of their potential quantum-coercive rivals without raising the continuing cyber-stability dangers posed by preeminent Russian, Chinese, Iranian or North Korean development of a quantum-CW regime.

References

[1] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.
[2] Harrow, A. W., & Montanaro, A. (2017). Quantum computational supremacy. Nature, 549(7671), 203–209.
[3] Arute, F., Arya, K., Babbush, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510.
[4] 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.
[5] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the ACM Symposium on Theory of Computing, 212–219.
[6] Bernstein, D. J., Buchmann, J., & Dahmen, E. (2019). Post-quantum cryptography. Springer.
[7] Chen, L., Jordan, S., Liu, Y. K., et al. (2016). Report on post-quantum cryptography. National Institute of Standards and Technology.



[8] 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.
[9] Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4), 283–424.
[10] Bernstein, D. J., Lange, T., & Peters, C. (2008). Attacking and defending the McEliece cryptosystem. Post-Quantum Cryptography, 31–46.
[11] Ding, J., & Petzoldt, A. (2017). Current state of multivariate cryptography. IEEE Security & Privacy, 15(4), 28–36.
[12] Hülsing, A., Rausch, L., & Buchmann, J. (2018). Optimal parameters for hash-based signatures. Journal of Cryptographic Engineering, 8(3), 229–243.
[13] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, 175–179.
[14] 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.
[15] Mosca, M. (2018). Cybersecurity in an era with quantum computers. IEEE Security & Privacy, 16(5), 38–41.
[16] Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., & Fedorov, A. K. (2020). Quantum-secured blockchain. Quantum Science and Technology, 5(3), 035004.
[17] Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78(1), 351–382.
[18] Buchmann, J., Dahmen, E., & Hülsing, A. (2014). Hash-based digital signature schemes. Post-Quantum Cryptography, 35–93.
[19] National Academies of Sciences, Engineering, and Medicine. (2019). Quantum computing: Progress and prospects. National Academies Press.
[20] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404.
[21] Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71.
[22] Libicki, M. C. (2018). Cyber deterrence and cyberwar. RAND Corporation.
[23] Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37.
[24] Healey, J. (2017). A fierce domain: Conflict in cyberspace, 1986–2012. Cyber Conflict Studies Association.



[25] Gartzke, E., & Lindsay, J. R. (2019). Weaving tangled webs: Offense, defense, and deception in cyberspace. Security Studies, 28(2), 316–348.
[26] Brantly, A. F. (2018). The cyber deterrence problem. Orbis, 62(3), 367–380.
[27] Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556(7701), 296–298.
[28] Shackelford, S. J. (2020). Governing cyber peace. Cambridge University Press.
[29] Buchanan, B. (2020). The hacker and the state. Harvard University Press.
[30] Clarke, R. A., & Knake, R. K. (2019). The fifth domain. Penguin Press.
[31] Jensen, B. M., Valeriano, B., & Maness, R. C. (2019). Cyber strategy. Oxford University Press.
[32] Herr, T., Laudrain, A., & de Spiegeleire, S. (2021). Cyber deterrence revisited. Journal of Cyber Policy, 6(1), 1–24.
[33] Kello, L. (2017). The virtual weapon and international order. Yale University Press.
[34] Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2020). How to design AI for social good. Science and Engineering Ethics, 26(3), 1771–1796.
[35] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things. Computer Law & Security Review, 32(5), 715–728.