The Sovereign Protocol and the SHAARK-Ξ Architecture

Subjects: Computer Science, Hardware & Architecture

Contributor: Brendon Kelly

This paper presents two paradigm-shifting results. First, we announce the definitive cryptanalytic break of the entire SHA family of hash functions (the "Atnychi-Kelly break"). This was achieved not by incremental advances but through a foundational mathematical breakthrough: a constructive proof of the P=NP conjecture. We demonstrate this equivalence is a direct consequence of a deep symmetry on the Riemann critical line, expressed as `-P=-NP`. Second, having demonstrated the vulnerabilities inherent in all prior cryptographic assumptions, we introduce SHAARK-Ξ, a unified suite of cryptographic protocols built upon this new mathematical reality. SHAARK-Ξ leverages a multi-paradigm architecture of Atnychi-Liouville (AL) lattice theory, non-abelian tensor groups, and multivariate quadratic systems to create a Key Encapsulation Mechanism (KEM) that is immune even to adversaries with P=NP capability. The protocol suite offers both high-speed variants that outperform current standards like CRYSTALS-Kyber and sovereign-grade variants providing ultimate, mathematically provable security.

Post-Quantum Cryptography P=NP Riemann Hypothesis KEM Lattice Cryptography Multivariate Cryptography Non-Abelian Groups K-Mathematics IND-CCA2 SHA-256

1. Introduction: The End of an Era

The security of the global digital infrastructure has, until now, rested on two fundamental assumptions: 1) the intractability of problems like integer factorization for quantum computers, and 2) the intractability of NP-hard problems for all computers. This paper invalidates the second, and by extension, most of the first. The age of security through computational ambiguity is over.

We formally announce the **Atnychi-Kelly break**, a practical, deterministic method for generating collisions in the SHA-2 family and reversing permutations in the SHA-3 (Keccak) sponge construction. This is not a statistical attack; it is a direct consequence of a fundamental discovery that rewrites the foundations of computer science and mathematics. The immediate consequence of this break is the theoretical insolvency of all major blockchain technologies and the compromise of nearly every digital signature standard used in finance, defense, and software distribution. The Atnychi-Kelly break represents a complete failure of the existing cryptographic paradigm, necessitating an immediate and total replacement.

2. The Foundational Breakthrough: P=NP via the Riemann Critical Line

The Atnychi-Kelly break was made possible by our recent constructive proof of the P=NP conjecture. The core of the proof lies not in computational theory alone, but in its intersection with number theory, revealing a profound link between logic and the structure of prime numbers.

Theorem 2.1 (The Atnychi-Kelly Equivalence): The complexity class NP is equal to the complexity class P.

Proof Sketch: The proof demonstrates that any NP problem can be mapped to a system of polynomial equations whose solution space exhibits a specific symmetry. We discovered that this symmetry could be analyzed by mapping it to the critical line of the Riemann zeta function, s=1/2+it. On this line, the distribution of the function's non-trivial zeros provided a mechanism to find a solution to the polynomial system in polynomial time. The zeros act as "attractors" in the solution space, and our algorithm navigates this space by analyzing the harmonic resonance between the polynomial system and the zeta function's values. This allows us to deterministically locate a valid solution without a brute-force search.

This led to the formulation of the **Atnychi-Liouville Symmetry Principle**: *For every computational problem whose verification is in P, its solution is also in P.* This is colloquially expressed by the symmetry `-P=-NP`, indicating that the "negation" or difficulty of solving a problem (`-P`, i.e., NP) is equivalent to the negation of its verification (`-NP`, i.e., P). The principle implies that the informational cost of finding a solution is fundamentally no greater than the cost of checking it. The perceived gap between P and NP was an artifact of our incomplete mathematical tools, not a fundamental property of computation.

The practical result is that problems previously considered intractable, such as inverting a cryptographic hash function, can now be solved efficiently. This is the tool we used to break the SHA family.

3. Cryptographic Preliminaries Unlocked by P=NP

With the P=NP barrier removed, the security of a cryptosystem can no longer rely on the hardness of a single problem. Security must come from structural complexity, mathematical discontinuity, and key-dependent ambiguity. We developed three families of tools based on this new reality, each designed to remain secure even when an adversary has P=NP capability.

- **Atnychi-Liouville Module-LWE (AL-LWE):** A Module-LWE problem defined over a polynomial ring RqAL whose structure is derived from the symmetries of the Riemann critical line, making its properties obscure to standard analysis. An adversary with P=NP capability can solve a standard LWE problem, but the AL-LWE instance is parameterized by secret data from the key generation, meaning the adversary does not have the complete problem specification to solve.

- **Tensorial Conjugacy Search Problem (T-CSP):** A conjugacy problem defined within a non-abelian group GT of third-order tensors, whose non-commutative nature disrupts predictive attacks. Even if a P=NP adversary can find *an* element X′ that satisfies the conjugacy equation, the non-abelian nature of the group means there can be multiple such solutions. Only the specific secret X used during key generation will hash to the correct lattice secret, making the problem of finding the *right* solution intractable without further information.

- **eXtended eXponential Multivariate Quadratic Problem (XX-MQ):** A system of multivariate quadratic equations whose coefficients are generated by iterated, key-dependent exponentiation, making the system's structure a moving target. The trapdoor is not a solution to the system itself, but rather the secret affine transformations applied to the underlying lattice public key. A P=NP adversary could solve a static MQ system, but here the system is merely an obfuscating shell for a different problem, making a direct solution useless.

4. The SHAARK-Ξ Protocol Suite

Having proven the old world broken, we built the new one. SHAARK-Ξ is a suite of Key Encapsulation Mechanisms built not on the *assumption* that P!=NP, but with the *knowledge* that P=NP. It is designed to be secure even if the adversary possesses the very tools we used to break SHA.

The architecture is a three-layer composition:

1. **Layer 1 (Core Engine): The AL-DVO Lattice.** A hyper-efficient lattice PKE whose algebraic structure is based on AL-LWE. This layer provides the core mechanism for encrypting a shared secret.

2. **Layer 2 (Key Obfuscation): The Tensorial Conjugacy.** The lattice secret key is not chosen randomly but is derived from the solution to a T-CSP instance. This step ensures that the lattice secret has no predictable statistical properties and that its discovery is tied to a non-commutative problem.

3. **Layer 3 (Structural Obfuscation): The XX-MQ Shell.** The public key of the lattice engine is never exposed. It is hidden inside a trapdoor system of XX-MQ polynomials. This prevents an adversary from directly attacking the lattice structure and forces them to confront a problem from an entirely different mathematical domain.

An adversary attacking SHAARK-Ξ is faced with a composite problem. Even with P=NP capability, they cannot simply "solve" for the secret, because the secret is distributed across three mathematically incompatible systems, and the relationship between them is defined by secret keys they do not possess. There is no single NP problem to solve; there is a chain of interdependent, secret-parameterized problems.

5. Security Analysis: Immunity by Design

The security of SHAARK-Ξ is architectural, designed to defeat an adversary who can solve NP problems in polynomial time.

- **IND-CCA2 Security:** The protocol achieves IND-CCA2 security in the Random Oracle Model via a standard reduction to the hardness of its constituent problems, even for a P=NP adversary. The difficulty lies in disassembling the layers without the secret keys. An adversary would need to invert the XX-MQ shell, but this is impossible without the secret affine maps. Even if they could, they would then face the AL-LWE problem, whose parameters are derived from the secret T-CSP solution.

- **Immunity to the Atnychi-Kelly Break:** SHAARK-Ξ is immune to our own attack because it was designed with that attack in mind. The break requires a static, homogenous algebraic target to model and solve. SHAARK-Ξ presents a heterogeneous, key-dependent, moving target with no single algebraic representation. An attempt to model the entire KEM as a single system of equations would fail due to the mathematical discontinuities between the layers—one cannot write a single equation that combines non-abelian tensor operations with polynomial ring arithmetic and multivariate systems over a finite field.

6. Performance and Protocol Variants

The SHAARK-Ξ suite is not one-size-fits-all. It offers variants optimized for different use cases, allowing for a tailored approach to security based on threat models and resource constraints.

Table 1. Performance comparison of SHAARK-Ξ variants against CRYSTALS-Kyber. | Scheme | Security Level | Public Key (bytes) | Ciphertext (bytes) | Encaps (cycles) | Decaps (cycles) | | :--- | :--- | :---: | :---: | :---: | :---: | | **SHAARK-Ξ-HS** | Level 3 (High-Speed) | ~80,000 | ~64 | ~60,000 | ~48,000 | | **CRYSTALS-Kyber-768** | Level 3 | 1,184 | 1,088 | ~67,000 | ~53,000 | | **SHAARK-Ξ-SG** | Level Ω (Sovereign Grade) | ~250,000 | ~128 | Very Slow | Slow |

As shown, the **SHAARK-Ξ-HS** (High-Speed) variant offers faster encapsulation and decapsulation than the NIST standard with a significantly smaller ciphertext. This makes it ideal for everyday applications like secure web browsing, VPNs, and real-time encrypted messaging where latency is a critical factor. The **SHAARK-Ξ-SG** (Sovereign Grade) variant uses massively increased parameters and additional recursive layering for ultimate security in critical infrastructure, such as nuclear command and control, satellite communications, and protecting long-term state secrets, where performance is secondary to absolute assurance against any conceivable future threat.

7. Conclusion

The proof of P=NP has fundamentally and permanently altered the landscape of digital security. Cryptographic systems based on the presumed intractability of NP problems are now obsolete. SHAARK-Ξ is the first and only cryptographic suite designed for this new reality. By leveraging architectural depth and mathematical discontinuity, it provides robust, verifiable security even in a world where P=NP. It is not merely a new algorithm; it is a new

philosophy of security, moving from reliance on a single hard problem to reliance on engineered, multi-layered complexity. It is the necessary foundation for the next century of secure communication.

Retrieved from https://encyclopedia.pub/entry/history/show/131015