UDC 004.056.55

Maksym Manko, student,
Viacheslav Tuz, professor,
Cherkasy State Technological University

COMPARATIVE ANALYSIS OF CLASSICAL, POST-QUANTUM, AND QUANTUM CRYPTOGRAPHIC METHODS FOR SECURE MILITARY COMMUNICATIONS

Abstract. This paper provides a structured comparison of classical cryptosystems (symmetric and public-key), post-quantum cryptography (PQC), and quantum key distribution (QKD) with respect to their suitability for secure military communications. We analyze threat models (classical supercomputer vs. quantum-capable adversary), secrecy properties, channel requirements (fiber-optic and free-space optics), and the impact on latency, throughput, and key-lifecycle management. We show that AES-256 in authenticated modes remains the foundation for bulk traffic, while public-key schemes based on factorization/discrete logarithms require migration to PQC standards. QKD delivers physics-grounded key establishment for critical routes but requires specialized infrastructure and careful integration with key management systems (KMS). We propose a phased hybrid architecture (QKD+PQC+AES) and outline a deployment roadmap for Ukraine's security and defense sector.

Introduction and Motivation. Resilience of secure communications amid long-term warfare and increasingly sophisticated cyber operations is a national priority. Classical symmetric ciphers (AES) provide high-throughput confidentiality, while public-key schemes (RSA/ECC) support key establishment and digital signatures. Large-scale quantum computing undermines trust in many public-key algorithms (Shor's algorithm) and moderately affects symmetric ciphers (Grover's algorithm), which can be countered by parameter increases. Two complementary lines of response are emerging: post-quantum cryptography (PQC) – standardized, quantum-resistant algorithms deployable without changing the physical medium; and quantum key distribution (QKD) – a physical-layer method for establishing keys with security guaranteed by quantum mechanics [4–6].

Objective. To justify the cryptographic choices for military communications by comparing classical, post-quantum, and quantum approaches and proposing a viable model for their combined use [8–10].

***Methodology and Comparison Criteria*.** We evaluate along: (i) security model (classical/quantum adversary, forward/backward secrecy, resistance to "record-now-decrypt-later"), (ii) key establishment mechanisms and refresh rates, (iii) latency/throughput and hardware acceleration, (iv)

channel requirements and delivery reliability (BER, atmospheric effects for FSO), (v) compatibility with existing MACsec/IPsec and KMS, (vi) CAPEX/OPEX and lifecycle assurance, (vii) alignment with standards and security policies.

Technical Overview.

1. Symmetric cryptography. AES-256-GCM/CTR as the baseline for bulk data encryption; low latency, broad hardware support, and manageable "quantum overhead" via parameter scaling.

2. Public-key / post-quantum cryptography. Traditional RSA/ECC are vulnerable to Shor's algorithm; migration to standardized PQC KEMs/signatures (e.g., ML-KEM, ML-DSA, SLH-DSA) is recommended. Their advantages include software compatibility and scalability across existing networks [4–6].

3. Quantum key distribution (QKD) Protocols BB84/E91/MDI-QKD; channels include optical fiber and free-space/satellite; required components are single-photon sources/detectors, QRNG, synchronization, and error-correction/privacy-amplification stacks [6–10]. QKD feeds fresh key material into the KMS for use by symmetric protocols (IPsec/MACsec/one-time pad on critical routes) [6–10].

Comparative Analysis

Table 1 – Comparative analysis of cryptographic approaches for military communications.

Criterion	**AES-256 (symmetric)**	**RSA/ECC (classical PK)**	**PQC (ML-KEM / ML-DSA / SLH-DSA)**	**QKD**
Security basis	Computational hardness; Grover mitigated via larger parameters [1,3].	Computational hardness; vulnerable to Shor's algorithm [2].	New hardness assumptions (lattices / hashes) designed to resist quantum attacks [4–6].	Laws of quantum physics (no-cloning, measurement disturbance) [7–10].
Role in system	Bulk encryption + authentication [1].	Key exchange/signatures (legacy paradigm) [2].	Key exchange/signatures (soft-rollout migration) [4–6].	Supplies keys to KMS/OTP [8-10].
Performance	Very high; low latency [1].	Moderate/high with acceleration [2].	Better than RSA at comparable security; larger keys/sigs [4–6].	Channel-limited; key rates are distance-/loss-limited [8-10].
Infrastructure	Existing [1].	Existing [2].	Existing (SW/FPGA/NIC updates) [4–6].	Quantum modules, fiber/FSO, trusted nodes required [9-10].

Best use	Any links and storage [1].	Legacy/transitio n [2].	Broad interagency use [4–6].	Highest-value corridors (HQ↔DC, government backbone) [7-10].

Note: "PQC standards used: FIPS 203/204/205; QKD profiles/interfaces: ITU-T Y.3800 series, ETSI GS QKD. [4–6] Threat model includes harvest-now-decrypt-later; QKD keys consumed by MACsec/IPsec via KMS [6–10]."

Regulatory and Standards Context (Ukraine/International).

• National cybersecurity policy and requirements for cryptographic protection in the public sector; current orders and message-format requirements for cryptographic tools.

• National encryption standards (including the Ukrainian block cipher "Kalyna"), algorithm identifiers, integration with trust services. [6, 10].

• International standards: profiles and interfaces for QKD networks (ETSI/ITU-T); PQC standards (FIPS) for KEM and signatures. [4–6] *Note.* QKD deployment must be aligned with existing KMS (REST key delivery, key-lifecycle policies, audit) [6–10].

Architecture and Roadmap for Ukraine's Security and Defense Sector.

1. Architectural principles. Trust-domain segmentation; attack-surface minimization; separation of quantum and classical channels. QKD-KMS integration with MACsec/IPsec (fresh key delivery, accounting, rotation). PQC for all interagency transits and signatures, with protocol compatibility.

2. Roadmap (phases). 1) PQC migration –transition to ML-KEM/ML-DSA/SLH-DSA and upgrade of cryptomodules and certification chains; 2) QKD pilot –link between two strategic facilities (dark fiber with FSO backup) integrated with departmental KMS; 3) Trusted-node network –backbone scaling and key-lifecycle policy alignment; 4) Expansion –evaluate satellite segments and ensure multi-vendor interoperability via open profiles.

Practical Significance and Novelty. We propose a unified model for cryptographic transformation of defense networks that combines the strengths of QKD and PQC while remaining deployable on existing infrastructure. The novelty lies in an applied focus on key lifecycle, integration interfaces, and phased implementation aligned with Ukraine's regulatory environment.

Conclusions. In the course of this work, classical (AES/RSA/ECC), post-quantum (ML-KEM/ML-DSA/SLH-DSA), and quantum (QKD) approaches for defense-grade communications were assessed. We conclude

that AES-256 (authenticated modes) is optimal for bulk traffic, public-key functions should migrate to standardized PQC, and QKD should be applied selectively on the most sensitive fixed routes to supply physics-grounded keys. The roadmap is: PQC migration across PKI/gateways → a dark-fiber QKD pilot with KMS integration and FSO backup → expansion to a trusted-node backbone with strict key-lifecycle governance. This hybrid posture strengthens forward secrecy, lowers record-now-decrypt-later risk, and scales on existing MACsec/IPsec networks.

References:

1. National Institute of Standards and Technology. (2001). FIPS 197: Advanced Encryption Standard (AES). https://doi.org/10.6028/NIST.FIPS.197

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. https://doi.org/10.1137/S0097539795293172

3. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th ACM Symposium on Theory of Computing (STOC ’96), 212–219. https://doi.org/10.1145/237814.237866

4. National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-based Key-Encapsulation Mechanism (ML-KEM). https://doi.org/10.6028/NIST.FIPS.203

5. National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-based Digital Signature Algorithm (ML-DSA). https://doi.org/10.6028/NIST.FIPS.204

6. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179. https://doi.org/10.48550/arXiv.2003.06557

7. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301

8. ETSI Industry Specification Group (ISG) QKD. (2019). ETSI GS QKD 014 V1.1.1: Quantum Key Distribution (QKD); Protocol and data format of REST- based key delivery API.

https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

9. IEEE. (2018). IEEE Std 802.1AE-2018: IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security (MACsec). https://standards.ieee.org/standard/802_1AE-2018.html

10. DSTU 7624:2014. (2015). Information technologies – Cryptographic protection of information – Symmetric block transformation algorithm. Kyiv: State Enterprise “UkrNDNC”. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=109736