Т4. №6(38)’2026

UDC 004.415.1:621.391.85:004.8

METHODS FOR ENSURING QUANTUM-ADAPTIVE SECURITY OF HYBRID CRYPTOGRAPHIC PROTOCOLS IN NEXT-GENERATION NETWORKS

T.M. Fesenko[1], A.S. Yanko[1], V.V. Magaletska[2], M.O. Plakhtii[2]
[1] Department of Computer and Information Technologies and Systems, National University “Yuri Kondratyuk Poltava Polytechnic”, Poltava, Ukraine
[2] Department of Computer Sciences, Limited Liability Company Private Higher Education Institution “University of Modern Technologies”, Kyiv, Ukraine
ORCID https://orcid.org/0009-0006-1698-3795
ORCID https://orcid.org/0000-0003-2876-9316
ORCID https://orcid.org/0009-0000-5562-699X
ORCID https://orcid.org/0000-0003-3805-0591
E-mail: al9_yanko@ukr.net

ABSTRACT

This article investigates methods for ensuring the quantum-adaptive security of hybrid cryptographic protocols in next-generation networks. 5G/6G and IoT networks necessitate the integration of classical and post-quantum algorithms. However, standard protocols combining ECDH with CRYSTALS-Kyber or CRYSTALS-Dilithium require formal security assessments. Current approaches primarily consider non-adaptive quantum adversaries, which limits their practical applicability in multi-session and dynamic environments.

The paper proposes a model of a quantum-adaptive adversary. This model integrates the adversary's classical and quantum resources, an adaptive attack strategy, and a quantum-accessible oracle. It allows for the formalization of superposition queries and multi-step interactions with the protocol. A mathematical model of a hybrid handshake protocol is introduced, where the session key is formed by combining classical and post-quantum components via a Key Derivation Function. An upper bound for the adversary's advantage is derived, accounting for both the classical and post-quantum components of the protocol.

To enhance resilience, three primary methods are proposed. The first is downgrade-resistant fixation of protocol parameters with cryptographic confirmation. The second is dynamic management of key parameters and cryptographic primitives based on an integrated risk function, which accounts for the adversary's quantum resources, network load, and attack activity. The third is compositional protocol verification considering multi-session and multi-level handshake phases, enabling the formalization of composability and the assessment of multi-level resilience. An integral metric of quantum-adaptive resilience is proposed, accounting for security, complexity, and adaptability. The results provide a scientific foundation for “harvest-now, decrypt-later” risk analysis.

Keywords: *quantum-adaptive security, hybrid cryptographic protocols, post-quantum cryptography, multi-session security, QAA-model, QROM.*

Introduction

Modern telecommunication systems, particularly 5G networks, emerging 6G architectures, and IoT infrastructures, are characterized by high dynamism, ultra-dense node deployment, and multi-session communication. These factors impose stringent requirements on cryptographic security, specifically regarding the resilience of key exchange and authentication protocols against potential quantum threats. Currently, hybrid cryptographic protocols are being implemented, combining classical mechanisms, such as ECDH or RSA, with post-quantum algorithms, notably CRYSTALS-Kyber and CRYSTALS-Dilithium, which are being standardized by NIST.

However, the current security state of these hybrid protocols remains insufficiently explored in the context of a quantum-adaptive adversary. Traditional security-proof approaches assume static attack scenarios and fail to account for the possibility of adaptive attack strategies evolving based on prior interactions with the protocol. This limitation creates gaps in practical resilience, particularly in multi-session environments and under dynamic network conditions.

Contemporary threats involve a combination of classical cryptanalytic methods and quantum computing, which can accelerate secret key retrieval or enable the modification of adversary behavior in real-time.

ISSN 2786-9024

The “harvest-now, decrypt-later” threat is particularly critical, as adversaries collect encrypted traffic today to decrypt it in the future using quantum resources. Furthermore, multi-session and scalable protocols create vulnerabilities in compositional security that classical analysis methods may not always adequately address.

In response to modern threats, quantum-adaptive security methods for hybrid cryptographic protocols are being actively implemented. Downgrade protection ensures the integrity of the selected algorithm suite throughout the session and neutralizes attempts at malicious interference with protocol parameters. Dynamic parameter management provides adaptive adjustment of key lengths and cryptographic primitive characteristics based on risk levels, the adversary's quantum resources, and current network activity. The formalization of composability and multi-session security enhances protocol resilience in multi-user and multi-layer networks, ensuring reliability during the simultaneous interaction of a large number of participants. Integral metrics of quantum-adaptive resilience allow for a quantitative assessment of protocol security by combining the analysis of classical and post-quantum components with the determination of the adversary's adaptability impact and the complexity of compositional interdependencies. Such a comprehensive approach forms a scientifically grounded basis for developing reliable protocols in 5G, 6G, and IoT networks, ensuring a high level of adaptive protection and readiness for potential quantum attacks.

Thus, the problem statement consists of ensuring the robust resilience of hybrid cryptographic protocols in next-generation networks against quantum-adaptive attacks. Under these conditions, a comprehensive approach to formalizing adversary models, dynamic parameter management methods, and protection mechanisms is crucial for providing a quantitative assessment of overall protocol resilience. The application of these methods will ensure a high level of security for 5G/6G and IoT systems, guaranteeing real-time adaptive security and increasing resilience to future quantum threats.

Literature review and problem statement

The field of quantum-adaptive security and post-quantum cryptography (PQC) is actively evolving within the global scientific community. In international review papers on cryptography and information security, post-quantum approaches are systematized as a key component for protecting future networks, specifically 5G, 6G, and IoT. These works emphasize the shortcomings of classical security proofs when considering adaptive quantum attacks and highlight the need for more generalized security models [1]. A significant role in the international context is played by the standardization process of new cryptographic mechanisms initiated by the NIST Post-Quantum Cryptography Project [2], which has identified the first standardized encryption and digital signature algorithms designed to withstand quantum threats.

Recent review studies, such as in-depth surveys on post-quantum cryptography and security, cover various PQC algorithm classes, their mathematical foundations, performance, and hardware acceleration requirements. They also address integration issues with existing protocols, including TLS and IoT environments [3]. Despite the high level of generalization, these works note that real-world adaptive attack scenarios and adversary behavior in complex protocols remain insufficiently studied.

Certain international publications propose applied framework solutions that combine classical cryptography, PQC, and Quantum Key Distribution (QKD) to build adaptive security in real-world networks. For instance, research into the advantages of a hybrid security framework integrated into a containerized testbed infrastructure demonstrates a dynamic transition between pure QKD, hybrid, and PQC modes to ensure end-to-end quantum-secure communication [4]. Other work in the field of combining classical, post-quantum, and QKD methods proposes a hybrid encryption scheme that optimizes both data protection and network performance [5].

Currently, a significant portion of publications is dedicated to hybrid authentication and key exchange protocols that maintain backward compatibility with existing standards while incorporating quantum-resistant components. For example, authentication protocols for 5G networks have demonstrated that hybrid solutions can support forward secrecy and enhance quantum resilience with minimal impact on performance [6]. European publications also highlight the architectural and implementation aspects of post-quantum cryptography. Such research analyzes approaches to building secure cryptographic protocol stacks, modeling composability, and the challenges of interoperability between new algorithms and existing data protection protocols [7].

The Ukrainian research landscape demonstrates positive trends in fundamental studies of post-quantum cryptography. Works by Ukrainian authors offer broad overviews of quantum-resistant algorithms and their mathematical foundations, describe classes of cryptographic schemes, and evaluate the general challenges of implementing such algorithms in critical information systems [8]. At the level of academic development, projects are being implemented focusing on post-quantum encryption and key updates in modern VPN systems based on Kyber algorithms, indicating a

drive to adapt post-quantum solutions to real-world network scenarios. Furthermore, the implementation of quantum-resistant digital signatures based on mathematical constructions with no known effective quantum attacks is being explored, strengthening the national contribution to the development of post-quantum protection mechanisms [9].

At the same time, there is a noticeable lack of large-scale empirical evaluations of complex hybrid protocol behavior under adaptive quantum threats within the national scientific community. A significant number of review and theoretical works are characteristic, yet there is a shortage of systematized adversary models, formal security proofs, and experimentally verified results in complex network contexts. This aligns with global publication trends, where the issues of adversary adaptability and composability require further development and deeper formal conceptualization.

Overall, the analysis of scientific research confirms that the issue of quantum-adaptive security for hybrid protocols remains one of the most promising yet underdeveloped research areas, despite significant progress in the standardization of post-quantum algorithms and the development of practical hybrid schemes for data protection in future networks.

The aim and objectives of the study

The objective of this article is to develop comprehensive methods for ensuring the quantum-adaptive security of hybrid cryptographic protocols in 5G, 6G, and IoT networks, enabling them to withstand both current and prospective quantum threats.

The work is grounded in the formalization of adaptive adversary behavior and the assessment of protocol resilience under dynamic quantum influence conditions, providing a scientifically substantiated framework for the practical implementation of defense mechanisms.

A review of existing hybrid protocols identifies critical vulnerabilities and gaps in composability and multi-session security that limit the effectiveness of contemporary solutions. This underscores the necessity of developing a formalized quantum-adaptive adversary model that accounts for the real-time dynamic evolution of attacker actions and enables accurate modeling of their impact on protocols.

This research presents an integrated approach to evaluating protocol resilience, factoring in the combination of classical and post-quantum components, the effect of adversary adaptability, and compositional complexity. The proposed methodology ensures comprehensive risk control and establishes the scientific and technical foundation for constructing robust hybrid protocols. Such solutions are capable of effectively countering quantum-adaptive threats, integrating into modern IoT infrastructures, and maintaining high security levels in multi-layered networks.

Materials and methods

A system analysis of hybrid cryptographic protocols reveals that combining classical algorithms with post-quantum schemes ensures both high performance and resilience to quantum attacks. In modern 5G, 6G, and IoT networks, hybrid solutions are integrated into TLS, VPN, and IPsec protocols, providing backward compatibility and reducing the need for large-scale infrastructure modernization. This approach maintains session stability and prevents security degradation during the transition to new algorithmic standards.

Particular attention is paid to modeling the behavior of a quantum-equipped adversary capable of executing superposition queries, combining classical and quantum methods, and adaptively modifying attack strategies based on obtained results. The Quantum-Accessible Random Oracle Model (QROM) allows for the formalization of such scenarios by integrating the adversary's capabilities into the protocol's security proofs and providing a mathematical justification for resilience [10]. This approach paves the way for building robust hybrid protocols capable of countering complex quantum-adaptive threats in real-time.

The analysis of established solutions indicates their sufficiently high resilience to standard quantum attacks, including Shor's and Grover's algorithms. At the same time, critical gaps persist in multi-session security and composability, which limits the effectiveness of protocols in multi-user and multi-layer networks. Dynamic parameter management becomes a decisive factor, where adaptive adjustment of key lengths, selection of cryptographic primitives, and algorithmic configurations based on risk assessment ensure protocol resilience even in complex environments with high network activity and a powerful quantum adversary.

An integrated approach to security assessment allows for the combination of classical and post-quantum components while accounting for the effect of attack adaptability and the complexity of protocol composition [11]. Such a comprehensive methodology forms the basis for creating next-generation hybrid protocols capable of effectively protecting information flows, integrating into modern telecommunications and IoT infrastructures, maintaining high performance, and withstanding quantum-adaptive threats.

It should be noted that while existing hybrid protocols provide basic resilience, they require further development in the areas of adversary adaptability, composability, multi-session security, and integral metrics for resilience assessment. These aspects define key scientific gaps and outline promising directions for further research in the field of quantum-adaptive security.

Under these conditions, the study of modern hybrid protocols reveals significant deficiencies in ensuring composability. Specifically, most solutions are tested only in isolated scenarios, which ignores the interactions between different protocol components. This leads to the emergence of potential indirect attack vectors, where the compromise of a single session affects the security of others. Such threats are particularly relevant in multi-user 5G and 6G environments, where hundreds of thousands of active sessions operate simultaneously. Consequently, the lack of formalized composable models complicates the construction of security proofs and creates “dark zones” that can be exploited by a quantum-adaptive adversary to optimize attacks.

When considering the multi-session aspects of modern hybrid protocols, it is notable that security is often limited to certificates and the handshake phases of an individual session. Such an approach fails to account for an adaptive adversary capable of aggregating data from multiple sessions to perform effective cryptanalysis. Scenarios of this type fall outside the scope of traditional security proofs and create additional attack vectors. Adversary adaptability allows for optimized key searching, a reduction in the entropy of session parameters, and the potential undermining of protocol resilience in multi-session environments.

Researching the integration of post-quantum algorithms with classical primitives leads to the conclusion that it also entails significant technical limitations [12]. Classical protocols, such as TLS 1.3, have established stages for key exchange and authentication. Incorporating PQC components for instance, CRYSTALS-Kyber for key exchange or CRYSTALS-Dilithium for digital signatures, sometimes results in alterations to the message-flow. Such changes violate the underlying assumptions of security proofs that rely on a specific handshake structure. Consequently, an adaptive adversary can exploit these modifications for downgrade attacks or to optimize attacks within QROM scenarios.

To provide a clear comparison of hybrid protocol effectiveness in the context of composability, multi-session security, and the integration of PQC with classical algorithms, Table 1 is presented. It demonstrates the strengths and weaknesses of various implementations across different network environments and highlights key gaps that require further research.

Comparative data highlight that even in the most common hybrid implementations, gaps remain in multi-session security and composability. Under these conditions, the integration of post-quantum schemes into classical protocols requires a formalized approach that accounts for adversary adaptability and the complexity of multi-session scenarios.

The results of such an approach form the basis for improving the analysis and design methods of next-generation hybrid protocols; however, achieving practical reliability necessitates a comprehensive evaluation of existing gaps. Simultaneously, a systematic and clear identification of weaknesses in implementation and security mechanisms is an indispensable prerequisite for the effective development of hybrid protocols. A multi-level analysis allows for the timely detection of deficiencies in composability properties, multi-session protection mechanisms, and the integration processes of post-quantum and classical components. Consequently, these aspects become critically important in the distributed and highly dynamic environments of 5G/6G and IoT, where scalability, session parallelism, and device heterogeneity significantly increase the requirements for the consistency and integrity of the cryptographic architecture.

Under these circumstances, the technical integration of post-quantum mechanisms reveals several significant architectural features. In particular, the implementation of CRYSTALS-Kyber in TLS 1.3 is carried out by extending the key agreement procedure and adding corresponding key-exchange messages [13]. Such a modification alters the protocol's message flow, affecting not only the temporal structure of the handshake but also the formal construction of the security proof, as new dependencies between exchange stages and additional assumptions regarding the adversary model emerge.

Similar features are observed in other network protocols. In the IPsec architecture, the Security Association

Table 1. Evaluating hybrid cryptographic protocols: Composability, multi-session security, and PQC-classical integration

Protocol	Composability	Multi-session Security	PQC Integration
TLS 1.3 + Kyber	Limited; does not account for multi-session interactions	Weak; lacks adaptive mechanisms	Partial; handshake changes may violate security proof
IPsec + PQC	Stable within a single SA, but not for multi-SA	SA support; lacks assessment of adaptive adversary behavior	PQC integrated locally; composability not proven
SSH + PQC	Individual sessions; composability is absent	Medium; local session security	Key exchange integrated; lacks adaptive assessment
IKEv2 + Kyber	Unstable in multi-level networks	Does not cover QROM scenarios	PQC added; composability not formally proven

(SA) mechanism ensures the preservation of the cryptographic state between sessions, which increases the efficiency of reconnections. However, this model does not provide a formalized assessment of adversary adaptability, where an attacker could simultaneously operate multiple SAs and exploit cross-session correlations. In the absence of clear compositional guarantees, this creates potential cross-session attack vectors [14].

Similar limitations are observed in SSH with integrated PQC key exchanges, as well as in IKEv2, where the compromise of a single Security Association (SA) or an individual session could theoretically have an indirect impact on other active connections. Collectively, such scenarios demonstrate practical attack vectors in multi-session environments and underscore the necessity of formally accounting for the adversary's adaptive multi-channel activity within an integrated security model.

Within the post-quantum paradigm, the analysis of adversary models focuses on their capability to perform superposition queries to cryptographic oracles in the Quantum Random Oracle Model (QROM). This characteristic fundamentally expands the set of admissible attacks compared to the classical computational model [15], as the adversary gains the ability to exploit quantum parallelism while interacting with cryptographic primitives.

This factor leads to additional reduction losses during the mathematical justification of security and significantly complicates the construction of formally rigorous security proofs, particularly under conditions of compositional and multi-session protocol application.

An evaluation of existing protocols, specifically CRYSTALS-Kyber and CRYSTALS-Dilithium, reveals that they are primarily oriented toward static or limited-adaptive models and do not fully account for composable scenarios involving numerous parallel sessions. Consequently, a gap emerges between the local reductionist security of individual primitives and the integral security of the protocol within a systemic context.

Such limitations lead to potential deficiencies in "standoff security", where an adversary can correlate inter-session leakage to refine hypotheses regarding secret parameters. These scenarios transcend classical security notions, such as IND-CCA and UCE, necessitating the expansion of models to incorporate quantum-adaptive multi-session adversary behavior.

When assessing multi-session environments, it is observed that the compromise of a single TLS 1.3 session or an IPsec Security Association (SA) can reduce the entropy of other sessions, creating potential lateral impact vectors. In the case of SSH with PQC key exchanges, the compromise of a private key on one station could allow for the monitoring of other sessions' behavior. Similarly, in IKEv2 with PQC integration, the compromise of a single SA increases the risk of weakening the resilience of adjacent Security Associations. These risks are especially critical for 5G/6G and IoT infrastructures, characterized by a massive number of simultaneous sessions and connected devices [16].

Regarding the resilience assessment of hybrid protocols, a critical gap is the absence of integral metrics. Current approaches are limited to measuring the local security of individual components and fail to analyze the interdependencies between sessions and handshake stages. This results in a "dark zone" between the nominal guarantees of PQC and the practical implementation of hybrid cryptographic stacks.

In conclusion, the identified gaps define three key directions for further research. The first area focuses on the development of composability-oriented security models for multi-level scenarios and multi-session adversary influence. The second area involves constructing security proof frameworks that account for adaptive adversary behavior within the Quantum Random Oracle Model (QROM). The third area concerns the development of integral metrics for the quantitative assessment of the interplay between classical and post-quantum mechanisms in hybrid protocols.

Consequently, a comprehensive resolution of these aspects establishes the foundation for building next-generation hybrid protocols. These protocols will ensure guaranteed security under composability constraints, operate efficiently in multi-session environments, and withstand adaptive quantum threats factors that are of critical importance for modern 5G/6G networks and scalable IoT infrastructures.

1. Conceptual Foundations and Systemic Problem Statement. The rapid integration of post-quantum primitives into classical transport and network layer security protocols objectively necessitates a transition from static security models to dynamic multi-session formalizations. In such an environment, the adversary ceases to be an abstract algorithmic entity and acquires the characteristics of an adaptive control system capable of modifying its strategy in real-time.

In view of this, it is appropriate to consider the protocol as an open quantum-classical system operating in a common Hilbert space

$$\mathcal{H} = \mathcal{H}_P \otimes \mathcal{H}_A \otimes \mathcal{H}_E , \quad (1)$$

where $\mathcal{H}_P$ is the subspace of honest participants, $\mathcal{H}_A$ is the internal information space of the adversary, and $\mathcal{H}_E$ is the interaction environment (network, noise effects, infrastructural states).

Thus, security is interpreted not as a property of an individual algorithm, but as a property of the system's dynamics as a whole.

The state of the system is described by the density operator

$$\rho(t) \in \mathcal{D}(\mathcal{H}), \quad \rho(t) \geq 0, \quad Tr(\rho(t)) = 1. \tag{2}$$

The presented ensures a universal description for both classical and quantum components of the protocol.

2. Operator Interpretation of the Protocol and Composability. Each round of interaction is modeled as a completely positive trace-preserving (CPTP) channel

$$\Phi_i : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H}), \tag{3}$$

reflecting the system's informational transition between protocol steps.

Furthermore, multi-session execution is formalized by the composition:

$$\Phi^{(n)} = \Phi_n \circ \cdots \circ \Phi_1, \quad \rho_n = \Phi^{(n)}(\rho_0). \tag{4}$$

In such an environment, it is fundamentally important that composability is interpreted as the resilience of this composition to external interference.

Accordingly, compositional security is defined through a distinguishability metric:

$$\Delta = \| \Phi_{real} - \Phi_{ideal} \|_\diamond . \tag{5}$$

Under these circumstances, the diamond norm is defined as

$$\| \Lambda \|_\diamond = \sup_{\rho_{AR}} \| (\Lambda \otimes \mathbb{I}_R)(\rho_{AR}) \|_1 , \tag{6}$$

guaranteeing that arbitrary correlations of the adversary with an external reference space are taken into account.

Thus, the protocol ε is compositionally secure if:

$$\Delta \leq \varepsilon . \tag{7}$$

The aforementioned formalizes the principle that the protocol maintains its resilience and does not become noticeably more vulnerable, regardless of the integration context.

Furthermore, in the multi-session mode:

$$\| \Phi_{real}^{(n)} - \Phi_{ideal}^{(n)} \|_\diamond \leq n\varepsilon . \tag{8}$$

Thus, composability provides metric control over risk accumulation.

3. Hybridity as a Structural Property of the Channel. The hybrid nature of the protocol implies that the information channel Φ_i consists of two subchannels:

$$\mathcal{K}_{hyb} = \mathcal{K}_{cl} \| \mathcal{K}_{pq} . \tag{9}$$

Therefore, the session key is formed as $K = KDF(\mathcal{K}_{cl} \| \mathcal{K}_{pq})$, which logically corresponds to the principle of cryptographic aggregation.

However, in the quantum adversary model, superposition access to oracles is permitted:

$$\sum_x \alpha_x |x\rangle |0\rangle \to \sum_x \alpha_x |x\rangle |f(x)\rangle, \tag{10}$$

leading to an estimation of the quadratic amplification of the reduction loss:

$$\varepsilon_{hyb} \leq \varepsilon_{cl} + q^2 \varepsilon_{pq} . \tag{11}$$

Thus, the aforementioned implies that hybridity is not a linear superposition of securities but is determined by the nature of the adversary's access.

4. Dynamic Model of a Quantum-Adaptive Adversary. The key element is the formalization of adaptability. It is proposed to describe the adversary's state using the operator:

$$\rho_A(t) \in \mathcal{D}(\mathcal{H}_A) . \tag{12}$$

Furthermore, its evolution is governed by a controlled Lindblad generator:

$$\frac{d\rho_A}{dt} = \mathcal{L}_{s(t),u_{A(t)}}(\rho_A) , \tag{13}$$

where $s(t)$ is the protocol state, $u_{A(t)}$ is the adversary strategy, $\mathcal{L}$ is the Lindblad linear superoperator.

The payoff functional is represented as:

$$J_A = \int_0^T I(Secret; View_A(t))dt . \tag{14}$$

This implies that the adversary optimizes information leakage. The optimal strategy will correspond to:

$$u_A^*(t) = arg \max_{u_A} J_A . \tag{15}$$

Thus, the adversary is modeled as a controlled quantum system with adaptive control.

5. Minimax Security Architecture. Protocol design is formulated as a differential game problem:

$$\min_{\Pi} \max_{u_A} \| \Phi_{\Pi,u_A} - \Phi_{ideal} \|_\diamond . \tag{16}$$

This means that the protocol must minimize the adversary's maximum information gain. Under such conditions, resilience is achieved if the minimax condition for the payoff functional is satisfied

$$\sup_{u_A} \| \Phi_{\Pi,u_A} - \Phi_{ideal} \|_\diamond \leq \varepsilon . \tag{17}$$

Thus, security is interpreted as the invariance of the channel to adaptive control.

6. Systemic Integration of Three Areas. Based on the results of the considered research sequence, covering the properties of composability, hybrid cryptographic structure, and the dynamic adaptability of the adversary, there arises an objective necessity for their systemic alignment within a single formalized model (Fig. 1).

At this stage, it is fundamentally important to transition from local mathematical descriptions of individual mechanisms to a systemic interpretation. Within this framework, protocol security is viewed as an integral property of interacting subsystems [17]. This approach corresponds to the modern paradigm of universally composable security, formulated within the Universal Composability (UC) framework [18], where each cryptographic primitive is analyzed not in isolation, but as an element of a more complex compositional structure.

From a methodological standpoint, each of the three areas fulfills a clearly defined functional role within the overall model architecture.

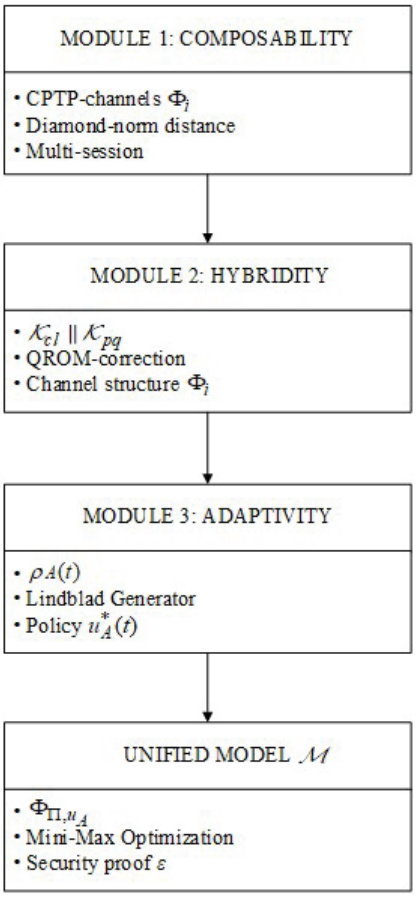

Fig. 1. Structural block diagram of the integration of composability, hybridity, and adaptability into a unified model

First, composability provides metric control over the correctness of protocol integration into an arbitrary external environment. Formally, this is implemented through constraints on the distinguishability of real and ideal channels, defined by an upper bound in the diamond norm. Thus, a global deviation metric is formed, ensuring that any system expansion or the addition of new sessions does not lead to uncontrolled error accumulation. In multi-session mode, the compositional property ensures the additivity or subadditivity of the security parameter, allowing for the establishment of clear upper bounds on the total risk of compromise [19]. Consequently, composability acts as an external stabilizing mechanism that defines the global boundary for permissible system deviations from the ideal specification.

Secondly, hybridity defines the internal structural architecture of channel Φ_i, as it is the combination of classical and post-quantum primitives that shapes the informational state space, the structure of cryptographic dependencies, and the reductionist security bounds. The integration of classical schemes with post-quantum algorithms creates a multi-layered cryptographic mechanism where the security parameter is determined not only by the resilience of individual primitives but also by the nature of their interaction. In the Quantum Random Oracle Model (QROM), reductionist estimates are modified to account for QROM corrections, which directly influence the magnitude of the permissible deviation between real and simulated environments. Thus, the hybrid block defines the internal geometry of the attack space and forms the structural foundation of the entire security system.

Thirdly, adaptability introduces temporal and strategic variability, transforming the adversary into a controlled quantum system with dynamic control. In this context, the adversary is modeled as a system with variable parameters, capable of adjusting its strategy based on intermediate results of interaction with the protocol. Accordingly, the channel Φ_{Π,u_A} acquires a parametric dependence on the control strategy, which shifts security analysis into the domain of dynamic systems and optimal control. This formulation allows for accounting for scenarios of sequential or conditional information disclosure, multi-step adaptive oracle queries, and the strategic optimization of attacks. As a result, protocol security is interpreted as the resilience of the system to all permissible controlled trajectories of the adversary.

Ultimately, it is the integration of these three mentioned areas that forms the hierarchical security structure. Composability establishes the global metric framework and guarantees the invariance of properties during composition. Hybridity defines the internal structural organization of the cryptographic channel and its reductionist bounds. Adaptability accounts for the temporal evolution of the attacking strategy and the strategic optimization of the adversary.

In aggregate, this enables a transition from the static analysis of individual primitives to a systemic model, where security is viewed as an integral function of structural, metric, and dynamic parameters.

Thus, the coordinated combination of composability, hybrid architecture, and adaptive adversary dynamics forms a closed formalized construction $\mathcal{M} = (\mathcal{H}, \Phi^{(n)}, \mathcal{K}_{hyb}, \mathcal{L}_{sec})$, ensuring the integrity, scalability, and mathematically grounded resilience of the protocol within a classical-quantum computing environment.

In performing a quantitative assessment of security metrics, it is proposed to consider a typical hybrid session key establishment protocol. In this protocol, a classical exchange mechanism based on Elliptic Curve Diffie-Hellman (P-256 curve) is combined with the

ISSN 2786-9024

post-quantum key encapsulation mechanism CRYSTALS-Kyber (Kyber-768 parameter level) [20]. Such an architecture is representative of modern TLS-like hybrid implementations focused on long-term cryptographic resilience.

First and foremost, it is necessary to formalize the initial assumptions. Let the system serve $N = 10^6$ independent sessions during a specific analyzed period, and let the adversary possess the capability to make adaptive quantum queries to oracles in the QROM model. Under these conditions, the integral assessment must account for four interrelated factors: (1) classical resilience, (2) post-quantum resilience, (3) compositional error accumulation, (4) adaptive reduction loss.

In the first stage, the classical component is evaluated. For ECDH P-256, the nominal security level is approximately 128 bits, which is equivalent to a successful attack probability of $\varepsilon_{cl} \approx 2^{-128} \approx 2.9 \cdot 10^{-39}$.

However, in multi-session mode, additive risk accumulation occurs. Applying the union bound, we obtain $\varepsilon_{cl,total} \le N \cdot \varepsilon_{cl}$, $N = 10^6$, $\varepsilon_{cl,total} \le 10^6 \cdot 2^{-128}$, $\varepsilon_{cl,total} \approx 2^{-108}$. Thus, even without considering other factors, the effective level of classical resilience is reduced to approximately 108 bits.

In the second stage, the post-quantum component is evaluated analogously. For Kyber-768, the claimed quantum security level corresponds to approximately 128 bits, yielding $\varepsilon_{pq} \approx 2^{-128}$. Taking into account the same 10^6 sessions, we obtain: $\varepsilon_{pq,total} \le N \cdot \varepsilon_{pq}$, . $\varepsilon_{pq,total} \le 10^6 \cdot 2^{-128}$, $\varepsilon_{struct} \le 2 \cdot 2^{-108}$, $\varepsilon_{pq,total} \approx 2^{-108}$.

Consequently, both classical and post-quantum components exhibit the same order of effective security degradation under multi-session conditions.

The next step is the structural integration of the hybrid scheme. Under the assumption of independent mechanisms, protocol compromise can occur via the breach of either component; thus, the integral structural bound is defined as $\varepsilon_{struct} \le \varepsilon_{cl,total} + \varepsilon_{pq,total}$, $\varepsilon_{struct} \approx 2^{-107}$.

Thus, hybridity ensures that the security level remains above 100 bits, yet it does not compensate for the losses resulting from system scaling.

Further analysis requires accounting for compositional complexity. Let the protocol consist of $k = 5$ cryptographically significant submodules. Within the framework of the Universal Composability (UC) model, the global distinguishability bound increases proportionally to the number of compositional elements, yielding: $\varepsilon_{comp} \le k \cdot \varepsilon_{struct}$, $\varepsilon_{comp} \le 5 \cdot 2^{-107}$, $\varepsilon_{comp} \approx 2^{-105}$.

Thus, the compositional architecture leads to an additional reduction in effective resilience by approximately two bits.

Finally, it is fundamentally important to account for the adversary's adaptability. Let the adversary make quantum queries to the oracles. In the QROM, the reduction loss scales as $\sqrt{q} = 2^{16}$. Accordingly, $\varepsilon_{adapt} \le \sqrt{q} \cdot \varepsilon_{comp}$, $\varepsilon_{adapt} \le 2^{16} \cdot 2^{-105}$, $\varepsilon_{adapt} \approx 2^{-89}$.

The obtained result demonstrates that the adaptive quantum factor constitutes the dominant contribution to the degradation of the integral security parameter.

Summarizing the presented stages, it should be noted that the integral resilience metric takes the value $S_{total} \approx 2^{-89}$, which is thus equivalent to approximately 89 bits of effective security. At the same time, the nominal 128 bits declared for individual cryptographic primitives are transformed into a significantly lower integral indicator in a real multi-session, compositional, and adaptive model.

Thus, the sequential transition from local reductionist assessments to a systemic integral metric allows for the identification of critical sources of resilience degradation and provides an engineering-correct basis for selecting protocol parameters [21]. Such a multi-level evaluation methodology is a necessary condition for designing cryptographic systems oriented toward functioning in a classical-quantum computing environment with a high level of compositional complexity.

Results

The conducted system analysis of modern hybrid cryptographic protocols has identified key aspects for enhancing their resilience within a quantum-adaptive environment. It was established that composability, multi-session security, and the integration of classical and post-quantum components remain critical risk areas, particularly in multi-layer and multi-user infrastructures such as 5G/6G and scalable IoT systems. It was found that the compromise of a single session or Security Association (SA) can degrade the entropy of adjacent elements, creating potential secondary attack vectors. Such scenarios transcend classical security notions and necessitate the implementation of integrated methods for evaluating and controlling protocol resilience.

Further analysis of adversary models in the Quantum Random Oracle Model (QROM) highlighted the need to account for the adaptive behavior of attackers capable of performing superposition queries to oracles and correlating leakage across sessions. This factor introduces additional reduction losses and significantly complicates the construction of formally rigorous security proofs, especially in composable and multi-session scenarios. In this context, the development of a formalized Quantum-Adaptive Adversary (QAA) model serves as a key step, enabling the integration of three domains composability control, hybridity of cryptographic primitives, and dynamic adversary adaptability into a single systemic framework.

The integration of these aspects paves the way for building next-generation hybrid protocols capable of maintaining resilience in multi-session environments, adapting to changes in adversary behavior in real-time, and guaranteeing security in composable scenarios.

A comprehensive approach allows not only for the formalization of protocol component interdependencies but also for the quantitative assessment of their interaction through integral metrics that account for classical and post-quantum elements, the effect of adversary adaptability, and compositional complexity.

Future research perspectives include several interconnected directions:

1. Development of integral resilience metrics that consider multi-session effects and composable influence to improve the accuracy of protocol analysis and optimization.

2. Enhancement of proof constructions in the QROM, accounting for dynamic adversary adaptability and multi-level scenarios to ensure formal security clarity at the system level.

3. Research into dynamic protocol parameter management strategies, including key lengths and cryptographic primitive configurations, to establish a basis for building effective adaptive protocols in environments with high network activity and powerful quantum attacks.

Thus, a comprehensive integrated approach to the analysis, modeling, and resilience evaluation of hybrid cryptographic protocols opens opportunities for creating reliable, scalable, and adaptive security systems capable of countering modern quantum threats and ensuring the effective operation of next-generation networks.

Conflict of Interest

The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship-related, or any other type of conflict that could have influenced the research or its results presented in this article.

Funding

This research was conducted without any financial support.

Data Availability

This manuscript has no associated datasets.

BIBLIOGRAPHY

[1] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, “Post-quantum cryptography and quantum-safe security: A comprehensive survey,” ACM Comput. Surv., vol. 1, no. 1, Art. 1, pp. 1–33, Oct. 2025. DOI: 10.48550/arXiv.2510.10436.

[2] National Institute of Standards and Technology, “Post-quantum cryptography Standardization.” csrc.nist.gov. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[3] Y. Zhyvylo and Y. Kuchma, “Mathematical modeling of intellectual and cryptographic protection of authentication keys,” ITS, vol. 13, no. 2, pp. 162–177, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344591.

[4] A. Sanz et al., “Extending Quantum-Safe Communications to Real-World Networks: An Adaptive Security Framework,” arXiv preprint arXiv:2511.22416, 2025. [Online]. URL: https://arxiv.org/html/2511.22416v1.

[5] A. Raj and V. Balachandran, “A Hybrid Encryption Framework Combining Classical, Post-Quantum, and QKD Methods,” in Applied Cryptography and Network Security Workshops (ACNS 2025), M. Manulis, Ed. Cham, Switzerland: Springer, 2026, pp. 197–201. DOI: 10.1007/978-3-032-01823-6_14.

[6] Y. Ko, I. W. A. J. Pawana, and I. You, “5g-aka-hpqc: Hybrid post-quantum cryptography protocol for quantum-resilient 5g primary authentication with forward secrecy,” arXiv preprint arXiv:2502.02851, pp. 1–15, 2025. DOI: 10.48550/arXiv.2502.02851.

[7] A. Khutsaeva, A. Leevik, and S. Bezzateev, “A Survey of Post-Quantum Oblivious Protocols,” Cryptography, vol. 9, no. 4, p. 62, 2025. DOI: 10.3390/cryptography9040062.

[8] S. Amador, C. Pardo, and R. Mazo, “Cybersecurity of Cyber-Physical Systems in the Quantum Era: A Systematic Literature Review-Based Approach,” Future Internet, vol. 18, no. 3, p. 125, 2026. DOI: 10.3390/fi18030125.

[9] T. Fesenko and Y. Kalashnikova, “Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection,” ITS, vol. 13, no. 2, pp. 178–191, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344592.

[10] A. Shyshatskyi, Ed., INFORMATION AND CONTROL SYSTEMS: MODELLING AND OPTIMIZATIONS. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024. DOI: 10.15587/978-617-8360-04-7.

[11] T. Fesenko and Y. Kalashnikova, “Predicate logic as the basis for knowledge formalization and logical inference in artificial intelligence systems for cybersecurity,” Science and Technology Today. Series: Engineering, no. 1 (55), pp. 1877–1891, Feb. 2026. DOI: 10.52058/2786-6025-2026-1(55)-1877-1891.

[12] J. Mijalkovic and A. Spognardi, “Reducing the False Negative Rate in Deep Learning Based Network Intrusion Detection Systems,” Algorithms, vol. 15, no. 8, p. 258, 2022. DOI: 10.3390/a15080258.

[13] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.

[14] M. Koval et al., “Improvement of complex resource management of special-purpose communication systems,” Eastern-European Journal of Enterprise Technologies, vol. 5, no. 9 (119), pp. 34–44, 2022. DOI: 10.15587/1729-4061.2022.266009.

[15] S. Kashkevich et al., “The development of management methods based on bio-inspired algorithms,” in Information and control systems: modelling and optimizations, A. Shyshatskyi, Ed. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024, pp. 35–69. DOI: 10.15587/978-617-8360-04-7.

[16] A. Shyshatskyi et al., “Development of a polymodel complex of information systems resource management,” Eastern-European Journal of Enterprise Technologies, vol. 4, no. 4 (136), pp. 58–72, 2025. DOI: 10.15587/1729-4061.2025.335688.

[17] P. Pradeep and K. Kant, “Conflict Detection and Resolution in IoT Systems: A Survey,” IoT, vol. 3, no. 1, pp. 191–218, 2022. DOI: 10.3390/iot3010012.

[18] Y. Zdorenko, A. Yanko, M. Myziura, and N. Fesokha, “Development of a fuzzy risk assessment model for information security management,” TAPR, vol. 4, no. 2 (84), pp. 71–79, Aug. 2025. DOI: 10.15587/2706-5448.2025.334954.

[19] Y. O. Zhyvylo, Y. V. Kuchma, and T. M. Fesenko, “Mathematical modeling of an adaptive anomaly detection system based on hybrid neural network architectures,” in Modern aspects of science: LXII. Part of the international collective monograph. Czech Republic: International Economic Institute s.r.o., 2025, pp. 407–456. DOI: 10.52058/62-2025.

[20] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.

[21] Т. Фесенко та Ю. Калашнікова, «Федеративна GNN-XAI модель прогнозу компрометації облікових записів у ZERO TRUST-середовищі», Кібербезпека: освіта, наука, техніка, вип. 3, № 31, с. 602–619, груд. 2025. DOI: 10.28925/2663-4023.2025.31.1049.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КВАНТОВО-АДАПТИВНОЇ БЕЗПЕКИ ГІБРИДНИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ У МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

Тетяна Фесенко, Аліна Янко, Владислава Магалецька, Максим Плахтій

У статті досліджуються методи забезпечення квантово-адаптивної безпеки гібридних криптографічних протоколів у мережах наступного покоління. Мережі 5G/6G та IoT потребують інтеграції класичних і постквантових алгоритмів. Однак стандартні протоколи, що поєднують ECDH з CRYSTALS-Kyber або CRYSTALS-Dilithium, потребують формальної оцінки безпеки. Сучасні підходи переважно розглядають неадаптивних квантових опонентів, що обмежує їхнє практичне застосування в багатосесійних і динамічних середовищах.

У роботі запропоновано модель квантово-адаптивного зловмисника. Ця модель інтегрує класичні та квантові ресурси зловмисника, стратегію адаптивної атаки та квантовий оракул. Це дає змогу формалізувати суперпозиційні запити та багатоступеневу взаємодію з протоколом. Представлено математичну модель гібридного протоколу рукостискання, де сесійний ключ формується шляхом поєднання класичних і постквантових компонентів через функцію формування ключа (KDF). Виведено верхню межу переваги зловмисника, що враховує як класичну, так і постквантову складову протоколу.

Для підвищення стійкості запропоновано три основні методи. Перший – фіксація параметрів протоколу із захистом від пониження рівня безпеки та криптографічним підтвердженням. Другий – динамічне управління ключовими параметрами та криптографічними примітивами на основі інтегральної функції ризику, яка враховує квантові ресурси противника, навантаження на мережу й активність атак. Третій – композиційна верифікація протоколів з урахуванням багатосесійних і багаторівневих фаз рукостискання, що дає змогу формалізувати композиційність та оцінити багаторівневу стійкість. Запропоновано інтегральну метрику квантово-адаптивної стійкості, що враховує безпеку, складність та адаптивність. Результати створюють наукове підґрунтя для аналізу ризиків harvest-now, decrypt-later.

Ключові слова: *квантово-адаптивна безпека, гібридні криптографічні протоколи, постквантова криптографія, Multi-session security, QAA-модель, QROM.*

REFERENCES

[1] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, “Post-quantum cryptography and quantum-safe security: A comprehensive survey,” ACM Comput. Surv., vol. 1, no. 1, Art. 1, pp. 1–33, Oct. 2025. DOI: 10.48550/arXiv.2510.10436.

[2] National Institute of Standards and Technology, “Post-quantum cryptography Standardization.” csrc.nist.gov. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[3] Y. Zhyvylo and Y. Kuchma, “Mathematical modeling of intellectual and cryptographic protection of authentication keys,” ITS, vol. 13, no. 2, pp. 162–177, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344591.

[4] A. Sanz et al., “Extending Quantum-Safe Communications to Real-World Networks: An Adaptive Security Framework,” arXiv preprint arXiv:2511.22416, 2025. [Online]. URL: https://arxiv.org/html/2511.22416v1.

[5] A. Raj and V. Balachandran, “A Hybrid Encryption Framework Combining Classical, Post-Quantum, and QKD Methods,” in Applied Cryptography and Network Security Workshops (ACNS 2025), M. Manulis, Ed. Cham, Switzerland: Springer, 2026, pp. 197–201. DOI: 10.1007/978-3-032-01823-6_14.

[6] Y. Ko, I. W. A. J. Pawana, and I. You, “5g-aka-hpqc: Hybrid post-quantum cryptography protocol for quantum-resilient 5g primary authentication with forward

secrecy,” arXiv preprint arXiv:2502.02851, pp. 1–15, 2025. DOI: 10.48550/arXiv.2502.02851.

[7] A. Khutsaeva, A. Leevik, and S. Bezzateev, “A Survey of Post-Quantum Oblivious Protocols,” Cryptography, vol. 9, no. 4, p. 62, 2025. DOI: 10.3390/cryptography9040062.

[8] S. Amador, C. Pardo, and R. Mazo, “Cybersecurity of Cyber-Physical Systems in the Quantum Era: A Systematic Literature Review-Based Approach,” Future Internet, vol. 18, no. 3, p. 125, 2026. DOI: 10.3390/fi18030125.

[9] T. Fesenko and Y. Kalashnikova, “Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection,” ITS, vol. 13, no. 2, pp. 178–191, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344592.

[10] A. Shyshatskyi, Ed., INFORMATION AND CONTROL SYSTEMS: MODELLING AND OPTIMIZATIONS. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024. DOI: 10.15587/978-617-8360-04-7.

[11] T. Fesenko and Y. Kalashnikova, “Predicate logic as the basis for knowledge formalization and logical inference in artificial intelligence systems for cybersecurity,” Science and Technology Today. Series: Engineering, no. 1 (55), pp. 1877–1891, Feb. 2026. DOI: 10.52058/2786-6025-2026-1(55)-1877-1891.

[12] J. Mijalkovic and A. Spognardi, “Reducing the False Negative Rate in Deep Learning Based Network Intrusion Detection Systems,” Algorithms, vol. 15, no. 8, p. 258, 2022. DOI: 10.3390/a15080258.

[13] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.

[14] M. Koval et al., “Improvement of complex resource management of special-purpose communication systems,” Eastern-European Journal of Enterprise Technologies, vol. 5, no. 9 (119), pp. 34–44, 2022. DOI: 10.15587/1729-4061.2022.266009.

[15] S. Kashkevich et al., “The development of management methods based on bio-inspired algorithms,” in Information and control systems: modelling and optimizations, A. Shyshatskyi, Ed. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024, pp. 35–69. DOI: 10.15587/978-617-8360-04-7.

[16] A. Shyshatskyi et al., “Development of a polymodel complex of information systems resource management,” Eastern-European Journal of Enterprise Technologies, vol. 4, no. 4 (136), pp. 58–72, 2025. DOI: 10.15587/1729-4061.2025.335688.

[17] P. Pradeep and K. Kant, “Conflict Detection and Resolution in IoT Systems: A Survey,” IoT, vol. 3, no. 1, pp. 191–218, 2022. DOI: 10.3390/iot3010012.

[18] Y. Zdorenko, A. Yanko, M. Myziura, and N. Fesokha, “Development of a fuzzy risk assessment model for information security management,” TAPR, vol. 4, no. 2 (84), pp. 71–79, Aug. 2025. DOI: 10.15587/2706-5448.2025.334954.

[19] Y. O. Zhyvylo, Y. V. Kuchma, and T. M. Fesenko, “Mathematical modeling of an adaptive anomaly detection system based on hybrid neural network architectures,” in Modern aspects of science: LXII. Part of the international collective monograph. Czech Republic: International Economic Institute s.r.o., 2025, pp. 407–456. DOI: 10.52058/62-2025.

[20] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.

[21] T. Fesenko and Y. Kalashnikova, “federative GNN-XAI model for predicting compromise of account records in ZERO TRUST environment,” Cybersecurity: Education, Science, Technique, vol. 3, no. 31, pp. 602–619, Dec. 2025. DOI: 10.28925/2663-4023.2025.31.1049.

Дата першого надходження статті до видання: 18.02.2026
Дата прийняття статті до друку після рецензування: 11.03.2026
Дата публікації (оприлюднення) статті: 00.00.00