# A Data Lifecycle-Aware Risk Assessment Framework for Post-Quantum Cryptography

Sakshyam Panda*, Debasish Jena†, Iakovos Pittaras‡, Vasilios A. Siris‡, Thomas Tsouparopoulos‡, Nikos Fotiou‡, Iordanis Koutsopoulos‡, Jesús García Rodríguez§, José Manuel Merlos Espín§, Antonio Skarmeta Gomez§

*Cylo Labs, UK; s.panda@cylolabs.com — Corresponding author
†International Institute of Information Technology (IIIT - Bhubaneswar), India; debasish@iiit-bh.ac.in
‡Athens University of Economics and Business, Greece; {pittaras, vsiris, tsouparop20, fotiou, jordan}@aueb.gr
§University of Murcia, Spain; {jesus.garcia15, josemanuel.merlose, skarmeta}@um.es

***Abstract*—In the Post-Quantum Cryptography (PQC) era, assessing quantum risk is essential for informing decisions such as prioritising system migration. Emerging identity and authorisation systems, including Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), introduce new challenges due to long-lived assets and multi-actor lifecycle interactions.**

**In this paper, we propose a threat modelling framework and a lifecycle-aware extension to an existing quantum risk assessment methodology. We present a taxonomy of quantum-related threats tailored to DID/VC systems, categorising them by target asset: data (e.g., credentials and DID documents), services (e.g., issuance and verification), and resources (e.g., computation and storage at wallets and verifiers). Building on this, we derive an extended quantum risk formulation that incorporates aggregation risk, sharing exposure, and verified destruction, enabling more informed and context-aware prioritisation of PQC migration strategies.**

***Index Terms*—Threat Modelling, Post Quantum Attacks, Decentralised Identifiers, Verifiable Credentials, Quantum Risk Assessment**

## I. Introduction

Quantum computing substantially extends the space of possible attacks and is expected to have a significant impact on classical cryptography, since quantum algorithms [1], [2] can solve computational problems widely used in cryptographic schemes. As a result, organisations must prepare for a transition to Post-Quantum Cryptography (PQC). This transition is challenging because many digital systems depend on classical cryptographic primitives for authentication, secure communication, and digital signatures, and may also introduce new protocol-level threats within digital ecosystems. A critical challenge in this transition is determining which systems should be migrated first. Migrating all systems simultaneously is often infeasible due to operational complexity, cost, and compatibility constraints [3]–[5]. Therefore, detailed threat analysis and appropriate quantitative methods are essential for prioritising post-quantum migration.

Although early work on quantum risk assessment has focused on traditional infrastructure such as Transport Layer Security (TLS), Virtual Private Networks (VPNs), and data encryption systems, emerging digital identity infrastructures introduce additional challenges. In particular, Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) are used to establish trust relationships between *issuers*, *holders*, and *verifiers* [6]. These assets may remain valid for long periods and be stored across multiple entities, making them vulnerable to long-term quantum attacks such as "harvest now, decrypt later" (HNDL) [7] and "trust now, forge later" (TNFL). Due to their reliance on distributed trust registries and long-lived trust anchors, such risks can extend beyond individual systems and affect entire identity ecosystems [3].

Another important characteristic of DID/VC systems is that credentials often *persist across multiple lifecycle stages*. They may be issued, stored, repeatedly presented, and eventually revoked or replaced. Each stage introduces distinct risks: long-term storage increases the harvesting window, while frequent sharing increases exposure to interception or misuse. These characteristics highlight the importance of considering the *data lifecycle* in evaluating quantum risks. Existing models, including the Quantum Adjusted Risk Score (QARS) framework [8], primarily evaluate risk at the system or asset level. However, in identity systems, risk is closely linked to how credentials are created, stored, shared, and revoked over time.

To address this, this paper proposes a data lifecycle-aware extension of the QARS model. The framework integrates three lifecycle stages: (*i*) creation and storage, (*ii*) usage and sharing, and (*iii*) destruction. This enables organisations to assess how operational practices, such as retention, sharing, and deletion, influence quantum risk. A key component of this extension is the taxonomy of quantum attacks, which enables the classification of abstract long-term threats into structured attack categories based on features and attack levels, including the data traffic level (e.g., TLS) and the DID/VC application level.

Digital identity systems constitute a fundamental pillar of the modern Internet, particularly Self-Sovereign Identity (SSI) frameworks based on DIDs and VCs. Existing work has analysed their trust models and security challenges. Mazzocca et al. [9] provide a survey of DIDs and VCs, Krul et al. [10] analyse trust in SSI systems, Naik et al. [11] propose an evaluation framework for SSI attacks, and Sharif et al. [12] present a threat model for digital identity wallets. While these

works highlight the need for systematic threat analysis, they do not address the attack surface introduced by hybrid and PQC deployments. To our knowledge, this has not yet been explored in this context. Our work also considers threats across multiple issuers and verifiers, capturing ecosystem-level attack vectors overlooked in prior studies.

By systematically classifying attacks by objective, technique, associated threat, vulnerability, and detection features, such a taxonomy, combined with a quantum risk assessment framework, enables organisations to move beyond general awareness towards more specific, informed, and prioritised policies. The contributions of this work are as follows:

- We present a taxonomy of quantum-related threats tailored to digital identity systems.
- We introduce a data lifecycle-aware extension of the QARS model that incorporates lifecycle stages into quantum risk assessment.
- We derive an extended formulation of the QARS score that captures the risk of aggregation, sharing exposure, and verified destruction.
- We propose a lifecycle-adjusted quantum risk methodology that generalises Mosca's quantum inequality.

Although the proposed framework builds on QARS, it introduces a lifecycle-aware perspective where data persistence, sharing practices, and deletion policies influence quantum risk. Unlike static asset-based models, QRAF captures the temporal and operational characteristics of data.

## II. Threat taxonomy

Evaluating quantum-related threats in digital identity systems is essential to identify vulnerabilities, determine mitigation strategies, and ensure a secure transition to PQC. While prior work has assessed the security of SSI systems, limited attention has been given to the implications of quantum-related threats. Recent studies indicate that the transition to PQC, particularly in hybrid deployments, introduces new attack surfaces such as downgrade risks, traffic indistinguishability, and computational amplification effects [3]. Hybrid deployments and PQC algorithms can alter protocol behaviour (e.g., handshake structure and message sizes), affecting how TLS traffic is generated, processed, and analysed, and introducing challenges beyond classical deployments.

To better understand these threats, it is important to consider the structure of digital identity systems, which span multiple architectural layers, notably the transport and application layers. At the transport layer, communication between wallets, issuers, and verifiers is secured using TLS, providing confidentiality, integrity, and authentication. At the application layer, DID/VC frameworks manage identity assertions, credential issuance, and verification. TLS-layer threats primarily target handshakes and protocol negotiations in short-lived sessions, whereas DID/VC-layer threats focus on long-lived identity and credential objects. Moreover, DID/VC threats may involve multiple issuers and verifiers, while TLS threats typically involve a single communication pair.

Consequently, *both layers* must be considered, as each introduces distinct attack vectors. Based on this, we classify quantum-related threats into TLS-specific and DID/VC-specific categories.

### A. TLS threats

The transition to PQC in TLS introduces new attack vectors because hybrid deployments and PQC algorithms can change protocol behaviour, e.g., handshakes, and increase computational cost [13], [14]. These changes affect how TLS traffic is generated, processed, and monitored, creating security challenges beyond those found in classical deployments. One concern is that PQC-based TLS traffic may differ in packet size, handshake structure, and timing behaviour, which can enable traffic analysis and evasion attacks. Attackers may exploit these differences to hide malicious flows within traffic that resembles legitimate post-quantum exchanges, reducing the effectiveness of existing intrusion detection and monitoring tools. Hybrid deployments also introduce the risk of downgrade attacks, where an adversary manipulates the handshake so that the endpoints fall back to classical cryptography instead of PQC.

Another concern relates to availability and implementation security. PQC handshakes require larger keys and higher computational effort, which attackers can exploit to launch DoS attacks by triggering expensive handshake operations. In addition, PQC implementations may introduce side-channel vulnerabilities, where observable characteristics such as execution time or power consumption reveal information about secret keys, including previously unexplored leakage vectors.

### B. DID/VC threats

We now discuss threats at the DID/VC layer, grouped by the asset they target: (i) data assets (e.g., credentials, DID documents, encrypted data, revocation lists), (ii) service assets (e.g., issuing and verification services), and (iii) resource assets (e.g., computation and storage at wallets and verifiers). Within *service assets*, a key threat is the *hybrid cryptographic downgrade attack*. During the PQC transition, protocols may support both classical and post-quantum algorithms. An adversary may exploit this coexistence by forcing a fallback to classical cryptography during credential issuance, presentation, or verification. Such attacks remove post-quantum protection while preserving functionality, making them difficult to detect. Their impact can be greater than at the TLS layer due to the long-lived nature of credentials and DIDs, also affecting *data assets* by exposing them to future quantum attacks.

A second threat to the verification service arises from *cryptographic suite inconsistencies and parameter misconfigurations*. In decentralised identity systems, issuers and verifiers may interpret PQC identifiers, parameter sets, or verification semantics differently. An attacker can exploit these mismatches to bypass checks or induce acceptance of weaker cryptographic settings. Another threat is *verification method manipulation*. By injecting additional methods or reordering

those listed in DID or VC documents, an adversary may exploit verifier selection heuristics and steer verification towards weaker, deprecated, or unintended cryptographic paths.

Another potential threat arises from *cryptographic policy differences between verifiers*. In decentralised digital identity systems, different verifiers may enforce different cryptographic acceptance policies. An adversary may exploit these differences by selectively presenting credentials and proofs to weaker or outdated verifiers, bypassing ecosystem-wide security guarantees, and violating ecosystem-wide consistency. Observe that this threat is not restricted to the verification service at a single verifier, but rather targets the verification service across verifiers of the same ecosystem. This highlights a feature that also exists in other DID/VC threats, such as the *cross-issuer correlation and linkability* threat discussed below, where threats and their corresponding attacks can involve multiple verifiers and issuers.

Another threat vector targeting *resource assets* (computation or storage) at the wallet or verifier relates to *DoS attacks caused by large and computationally expensive PQC artefacts*. Post-quantum keys, signatures, and proofs are typically larger and more computationally expensive to process. An adversary can exploit this by submitting oversized but syntactically valid credentials or proofs, forcing verifiers to perform repeated and costly verification operations before enforcing resource limits, thereby exhausting computational or memory resources. Such DoS threats can also target wallets. In addition to presenting oversized PQC proofs during challenge/response interactions, wallets must generate these proofs, which can further increase computational load and resource exhaustion.

Adversaries may also target *credential status and revocation mechanisms*. By replaying stale but valid status information, manipulating freshness, or exploiting timeouts during PQC-heavy checks, they may cause verifiers to misclassify credentials as valid or revoked. Large PQC-signed status lists can further amplify this by increasing verification costs and causing failures. Privacy threats may also arise through *cross-issuer correlation and linkability*. Repeated credential presentations across multiple verifiers can enable adversaries to infer user identities or behaviour patterns. These observations align with prior studies on privacy impact assessment, highlighting how repeated exposure and interaction patterns can lead to unintended information leakage [15]. By observing interactions, attackers may identify supported cryptographic algorithms and target weaker verifiers or protocol paths.

Finally, *key rotation and state desynchronisation* introduce additional risks for DID documents and verifiable credentials, especially during the transition to hybrid or PQC. Inconsistencies between issuers, wallets, and verifiers during key updates could lead to validation failures or the acceptance of credentials signed with weaker algorithms.

The taxonomy shows that quantum-related threats in digital identity systems span multiple layers and contexts, with varying vulnerabilities, attack paths, and impacts. This underscores the need for systematic risk assessment and prioritisation, and provides a basis for linking threat characteristics to lifecycle-aware factors. The next section introduces the proposed lifecycle-aware quantum risk framework.

## III. Lifecycle-integrated Quantum Risk Assessment Framework (QRAF)

The proposed model extends the QARS framework by introducing lifecycle-aware parameters while preserving its core dimensions of timeline, sensitivity, and exposure. These dimensions are consistent with established risk assessment paradigms (e.g., ISO/IEC 27005 and NIST frameworks), where risk is characterised by impact, likelihood, and exposure. These lifecycle extensions capture operational factors, such as data retention, sharing behaviour, and deletion practices, that are particularly critical in decentralised identity systems.

### A. Data Lifecycle Model

This lifecycle comprises three stages: **Creation and Storage**, **Usage and Sharing**, and **Destruction**. Each stage interacts with the core QARS dimensions (timeline, sensitivity, exposure), influencing overall quantum risk. The lifecycle perspective highlights that the quantum risk is determined not only by the cryptographic algorithms used by the systems. Operational practices related to data storage, transmission, and retention also influence the likelihood and potential impact of quantum attacks. In particular, long-term storage increases the window during which encrypted data may be harvested, frequent sharing increases exposure to interception, and secure deletion reduces the persistence of sensitive information.

*1) Creation and Storage:* During the creation and storage stage, data is generated and retained within systems such as databases, archival repositories, and cloud storage platforms. Security frameworks, including ISO/IEC 27040, emphasise the protection of stored information and the management of long-term data retention. In the context of quantum risk, long-term storage introduces Harvest-Now-Decrypt-Later (HNDL) risks. Even if the encryption cannot be broken immediately, the ciphertext may be stored until quantum computers are capable of breaking the underlying cryptographic algorithms, which is expected within the coming decade.

Large datasets also introduce aggregation risk, in which the cumulative value of many records makes a dataset an attractive target for adversaries. Aggregated datasets could contain sensitive information when compromise could lead to significant operational, financial, or societal consequences. This stage therefore affects both the timeline and sensitivity dimension of quantum risk. Longer retention periods increase the effective confidentiality requirements of the data, while larger datasets amplify the potential impact of compromise.

*2) Usage and Sharing:* The second stage corresponds to the usage and sharing of data. During this stage, data might be accessed by users, transmitted between systems, or exchanged between organisations. Security standards such as ISO/IEC 27002 emphasise the need to protect data during transmission and communication. In the quantum threat model, this stage is particularly relevant because it enables HNDL attacks.

| Symbol | Description |
|---|---|
| $a$ | Cryptographic asset or system under assessment |
| $\delta(a)$ | Destruction offset representing lifecycle termination of data |
| $\Lambda(a)$ | Lifecycle adjusted confidentiality burden |
| $q_{int}$ | Internal harvesting factor |
| $q_{shr}$ | External sharing harvesting factor |
| $\rho_L(a)$ | Lifecycle-aware vulnerability ratio |
| $\sigma(a)$ | Sharing exposure proportion of the asset's data |
| $\vartheta(a)$ | Cryptographic visibility of asset $a$ |
| $w_T, w_S, w_E$ | Weighting coefficients for timeline, sensitivity, and exposure |
| $E'(a)$ | Lifecycle-aware exposure component |
| $S(a)$ | Base sensitivity score of the asset |
| $S'(a)$ | Aggregation-aware sensitivity score |
| $T'(a)$ | Lifecycle-adjusted timeline risk |
| $V(a)$ | Dataset size associated with asset $a$ |
| $X(a)$ | Confidentiality lifetime of asset $a$ |
| $Y(a)$ | Time required to migrate asset $a$ to PQC |
| $Z(a)$ | Time until quantum attacks become feasible (threat horizon) |

TABLE I: Notation used in the lifecycle-aware QRAF

Systems that frequently transmit or share data have a higher probability of exposure. Exposure risk increases in scenarios such as transmission over public network, synchronisation with cloud-based services, integration with external APIs and cross-organisational data sharing. The lifecycle-aware risk model, therefore, incorporates a parameter that represents the frequency of sharing, which captures how often data leave the protected boundary of the system.

*3) Destruction and Data Sanitisation:* Data retention policies require timely deletion once data is no longer needed. In the context of quantum risk, verified deletion reduces the future confidentiality impact of harvested ciphertext by limiting the effective exposure window. This is captured through a binary destruction offset parameter $\delta \in [0, 1]$, which models the extent to which deletion reduces the effective lifetime of data confidentiality. Its primary function is to minimise the harvesting window. $\delta$ must be applied before high-sharing phases, as deletion cannot mitigate data already intercepted. A value of $\delta = 0$ indicates that the destruction does not reduce the exposure window, while $\delta = 1$ represents complete removal before the threat horizon. Using this destruction offset, the lifecycle-aware model captures the effect of data sanitisation policies on long-term quantum risk.

For reproducibility, the lifecycle parameters are derived from observable system characteristics. The confidentiality lifetime $X(a)$ follows regulatory retention and business value, while $\sigma(a)$ represents the proportion of time data are externally exposed, estimated from logs and data flows. Exposure factors $q_{int}$ and $q_{shr}$ are approximated using qualitative scales (e.g., low/medium/high) based on control maturity and system boundaries.

### B. Extended Risk Score

The QARS model formulated the risk using three dimensions: timeline risk $T$, data sensitivity $S$, and exposure $E$. To incorporate lifecycle effects, QRAF is defined as:

$$QRAF(a) = w_T T'(a) + w_S S'(a) + w_E E'(a) \tag{1}$$

where the components $T', S', E'$ extend the original QARS factors by incorporating lifecycle parameters that capture persistence of storage, data aggregation, and sharing behaviour and they are defined in the sequel, and $w_T, w_S, w_E$ are weight parameters that satisfy

$$w_T + w_S + w_E = 1\,. \tag{2}$$

*1) Timeline Extension:* The timeline risk is derived from Mosca's inequality, which relates the confidentiality lifetime of data to the expected arrival time of quantum attacks. The extended timeline component is defined as:

$$T'(a) = f_{time}\left(\frac{(X(a) + Y(a))(1 - \delta(a))}{Z(a)}\right) \tag{3}$$

where the function $f_{time}(.)$ maps the vulnerability ratio to a bounded interval, typically [0,1], allowing the timeline factor to be combined with the other risk components, and:

- $X(a)$ denotes the confidentiality lifetime of the asset. It is calculated by mapping specific data assets to legal retention mandates (e.g., GDPR, HIPAA) and the duration of their competitive business value.
- $Y(a)$ denotes the time required to complete migration to PQC. It is estimated by aggregating the time required for cryptographic inventory, vendor software updates, and the internal deployment of the PQC-compliant infrastructure.
- $Z(a)$ denotes the expected quantum threat horizon. It is determined using consensus-based scientific forecasts and industry roadmaps on the development of a cryptographically relevant quantum computer.
- $\delta(a)$ denotes the destruction offset, a binary variable representing the verified termination of data before the threat horizon $Z$, introduced in the previous section.

The latter reduces the effective confidentiality threshold when secure deletion policies are applied. If $\delta(a) = 1$, data is assumed to be destroyed before the quantum threat horizon, and the effective timeline risk approaches zero. Note that verified data destruction reduces the confidentiality exposure of specific data instances, but does not remove the need for cryptographic migration. Systems continue to generate new data, and complete deletion across distributed environments cannot be guaranteed. Therefore, lifecycle-aware risk reduction through deletion complements, rather than replaces, PQC migration.

*2) Sensitivity Extension:* The sensitivity component of the model captures the potential impact of a quantum compromise. In the lifecycle-aware formulation, the sensitivity score is extended to account for the size of the data set. The refined sensitivity factor is defined as:

$$S'(a) = S(a) \log_{10}(V(a) + 1) \tag{4}$$

where

- $S(a)$ is the base sensitivity level of the asset,
- $V(a)$ is the number of records associated with the dataset.

This formulation reflects the observation that breaches that affect large datasets typically have greater operational and societal consequences than breaches affecting individual records.

Logarithmic scaling ensures that the impact increases with the size of the data set, while preventing unrealistic linear growth.

*3) Exposure Extension:* Exposure risk reflects the probability that encrypted data may be intercepted and harvested by adversaries. In our lifecycle-aware model, exposure risk incorporates both internal storage exposure and exposure due to external sharing. The revised exposure component is:

$$E'(a) = \vartheta(a) \cdot [q_{int}(1 - \sigma(a)) + q_{shr}\sigma(a)] \tag{5}$$

where

- $\vartheta(a)$ represents cryptographic visibility. It is assessed through automated discovery tools and cryptographic inventories to determine if an asset relies on quantum-vulnerable algorithms (assigned as 1 for RSA/ECC or 0 for PQC).
- $q_{int}$ is the degree of harvesting within internal systems. It is calculated based on internal perimeter defences and the ease of accessing the data.
- $q_{shr}$ is the degree of harvesting during external sharing. It is calculated based on the technical accessibility of the transmission channels and the security posture of external third-party environments.
- $\sigma(a)$ is the exposure proportion of the data lifecycle during which the asset is exposed to external environments or transmitted across system boundaries. It is estimated by analysing data flow logs and network traffic to quantify the percentage of the data lifecycle spent in transit or external environments versus isolated internal usage.

### C. Lifecycle risk Theorem

To formalise the life-cycle interpretation of timeline risk, the following theorem extends Mosca's inequality. Let an asset $a$ have confidentiality lifetime $X(a)$, migration time $Y(a)$, quantum threat horizon $Z(a)$, and destruction offset $\delta(a)$. The lifecycle-adjusted vulnerability ratio is defined as:

$$\rho_L(a) = \frac{(X(a) + Y(a))(1 - \delta(a))}{Z(a)}\,. \tag{6}$$

The asset enters the lifecycle-adjusted quantum breach threshold whenever $\rho_L(a) > 1$. Mosca's inequality states that confidentiality cannot be guaranteed when

$$X(a) + Y(a) > Z(a) \tag{7}$$

In this lifecycle-aware model, the effective confidentiality burden is reduced by the destruction offset introduced earlier. The adjusted confidentiality burden is therefore revised to the following:

$$\Lambda(a) = (X(a) + Y(a))(1 - \delta(a))\,. \tag{8}$$

Replacing the confidentiality burden with the adjusted value yields the lifecycle-adjusted condition, substituting the definition of $\Lambda(a)$, and dividing both sides by $Z(a)$ produces the following

$$\Lambda(a) > Z(a) \tag{9}$$

$$(X(a) + Y(a))(1 - \delta(a)) > Z(a) \tag{10}$$

$$\rho_L(a) > 1 \tag{11}$$

Here, the lifecycle-adjusted vulnerability condition is satisfied when the adjusted confidentiality burden exceeds the quantum threat horizon. Mosca's inequality is generalised by incorporating the effect of data destruction. The destruction offset $\delta$ reduces the effective confidentiality window by incorporating verified data deletion into the risk model. Such as

- No deletion policy ($\delta(a) = 0$) $\rightarrow$ classical Mosca model
- Partial retention reduction ($0 < \delta(a) < 1$) $\rightarrow$ reduced exposure
- Verified destruction before threat horizon ($\delta(a) = 1$) $\rightarrow$ risk eliminated

## IV. Threat Intelligence and Threat Modelling in Lifecycle-Aware Quantum Risk Assessment

### A. Threat intelligence for lifecycle-aware risk assessment in DID/VC systems

Threat intelligence plays an important role in contextualising lifecycle-aware quantum risk assessments within decentralised identity infrastructures. Within the lifecycle-aware QRAF, threat intelligence could inform the evaluation of the timeline and exposure parameters associated with DID/VC architectures. Intelligence reports on advances in quantum computing, cryptanalysis, and national quantum initiatives help organisations establish planning assumptions regarding the timeframe within which classical digital signature schemes may become vulnerable.

Threat intelligence also provides insight into adversarial data collection strategies relevant to identity infrastructures. Credential presentations between holders and verifiers involve the repeated transmission of signed credential data across networks. Observations of large-scale interception campaigns and persistent storage of encrypted communications highlight the relevance of HNDL attacks in such environments. These insights allow organisations to identify identity infrastructures that may be particularly attractive targets for adversaries seeking to collect cryptographic artefacts for future exploitation. Systems supporting large user populations, cross-border digital identity services, or critical infrastructure authentication may therefore require higher priority in post-quantum migration strategies.

### B. Threat Modelling of DID/VC Architecture for Exposure and Lifecycle Analysis

Threat modelling provides a structured method for analysing how adversaries may exploit architectural components of DID/VC ecosystems. Within the lifecycle-aware QRAF, threat modelling supports the identification of exposure points throughout the credential lifecycle and informs the estimation of parameters used in the extended risk model. Each component participating in the lifecycle of credentials introduces potential exposure to adversarial observation. The proposed model therefore examines how data flows through these architectures:

- The issuance of credentials establishes the cryptographic material associated with the credential and corresponds to the initiation stage of the lifecycle.

- The storage of credentials within digital wallets or identity platforms contributes to the confidentiality lifetime parameter $X$, particularly when credentials remain valid for an extended period.
- The presentation of the credential involves repeated transmission of signed credential data between holders and verifiers, increasing the exposure of data interception and harvesting.
- Revocation or deletion of credentials corresponds to the destruction stage, where effective revocation and deletion mechanisms reduce long-term exposure through the destruction offset parameter $\delta$.

Mapping lifecycle interactions enables the estimation of exposure parameters, including internal harvesting $q_{int}$, external sharing $q_{shr}$, and sharing proportion $\sigma$. Systems with frequent cross-border credential exchange exhibit a higher risk of exposure. Threat modelling also reveals architectural factors that affect cryptographic visibility, such as publicly resolvable DID registries and distributed ledgers. These design choices affect the visibility parameter $\vartheta(a)$ within the lifecycle-aware risk model. Compared to QARS, QRAF incorporates lifecycle-aware factors that capture data persistence and sharing dynamics. By accounting for temporal exposure rather than static assets, it enables more precise prioritisation of PQC migration in systems where data longevity drives risk.

## V. Conclusions and Future Work

This paper proposed a lifecycle-aware quantum risk assessment framework that integrates data lifecycle considerations into quantum risk assessment by linking the three core dimensions of the QARS framework (timeline, sensitivity, and exposure) to the stages of data creation and storage, usage and sharing, and destruction. The framework is fuelled by a threat and attack taxonomy in the transport and application layers to demonstrate that quantum risk depends not only on cryptographic algorithms, but also on operational practices such as data retention, sharing frequency, and deletion policies. By incorporating lifecycle considerations, organisations can reduce quantum risk through both cryptographic migration and improved data governance.

The proposed methodology also supports emerging post-quantum transition initiatives such as the EU Coordinated PQC Roadmap and aligns with the adoption of NIST post-quantum cryptographic standards, including FIPS 203–205. In particular, the lifecycle-aware Quantum Risk Assessment Framework (QRAF) metric enables phased prioritisation of migration activities by identifying assets whose lifecycle characteristics amplify long-term quantum risk.

Future work will focus on empirical validation of the proposed framework through case studies in real-world DID/VC deployments and simulation-based evaluation of parameter sensitivity. In particular, the framework will be applied to representative identity architectures to assess its effectiveness in supporting PQC migration decisions and to allow quantitative comparison with existing risk assessment approaches such as QARS. Further research will also explore the automation of parameter estimation through system monitoring and threat intelligence integration. Such developments could further assist in efficiently tackling the transition toward quantum-resilient digital infrastructures.

## Acknowledgment

This work received funding from the EU Horizon Europe POSEIDON Project[1] under Grant Agreement No. 101225797. All authors, with the exception of Prof. Debasish Jena, were funded by this project.

## References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, p. 1484–1509, Oct. 1997. [Online]. Available: https://doi.org/10.1137/S0097539795293172

[2] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying grover's algorithm to aes: quantum resource estimates," in *International Workshop on Post-Quantum Cryptography*. Springer, 2016, pp. 29–43.

[3] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," *IEEE Access*, vol. 12, pp. 23 427–23 450, 2024.

[4] S. Panda, E. Panaousis, G. Loukas, and C. Laoudias, "Optimizing investments in cyber hygiene for protecting healthcare users," in *From Lambda calculus to cybersecurity through program analysis: Essays dedicated to Chris Hankin on the occasion of his retirement*. Springer, 2020, pp. 268–291.

[5] M. Tsiodra, S. Panda, M. Chronopoulos, and E. Panaousis, "Cyber risk assessment and optimization: A small business case study," *IEEE Access*, vol. 11, pp. 44 467–44 481, 2023.

[6] R. Campbell, "Enterprise migration to post-quantum cryptography: Timeline analysis and strategic frameworks," *Computers*, vol. 15, no. 1, p. 9, 2025.

[7] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, "Post-quantum cryptography and quantum-safe security: A comprehensive survey," *arXiv preprint arXiv:2510.10436*, 2025.

[8] Š. Grigaliūnas and R. Brūzgienė, "Towards a unified quantum risk assessment," *Electronics*, vol. 14, no. 17, p. 3338, 2025.

[9] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 6, pp. 3641–3671, 2025.

[10] E. Krul, H.-y. Paik, S. Ruj, and S. S. Kanhere, "Sok: Trusting self-sovereign identity," in *Proceedings on Privacy Enhancing Technologies Symposium*, 2024.

[11] N. Naik, P. Grace, P. Jenkins, K. Naik, and J. Song, "An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity," *Computers & Security*, vol. 120, p. 102808, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404822002024

[12] A. Sharif, Z. E. Ansaroudi, G. Sciarretta, D. Pöhn, M. Mollaeefar, W. Hommel, and S. Ranise, "Protecting Digital Identity Wallet: A Threat Model in the Age of eIDAS 2.0," in *Risks and Security of Internet and Systems*. Springer Nature Switzerland, 2025.

[13] T. Reddy.K and H. Tschofenig, "Post-Quantum Cryptography Recommendations for TLS-based Applications," Internet Engineering Task Force, Internet-Draft draft-reddy-uta-pqc-app-08, Jul. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-reddy-uta-pqc-app/08/

[14] K. Souvatzidaki and K. Limniotis, "Post-quantum key exchange in tls 1.3: Further analysis on performance of new cryptographic standards," *Cryptography*, vol. 9, no. 4, p. 73, 2025.

[15] S. Panda, E. Panaousis, G. Loukas, and K. Kentrotis, "Privacy impact assessment of cyber attacks on connected and autonomous vehicles," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–9.

[1] https://cordis.europa.eu/project/id/101225797