A Study of PQC Migration Frameworks

Eunisse Nzetchuen, Marc Stöttinger, Alexander Wiesmaier,
Elif Yeşilbek

Faculty of Design Computer Science Media
RheinMain – University of Applied Sciences and Arts
Wiesbaden, Germany

Eunisse.Nzetchuen@hs-rm.de

May 10, 2026

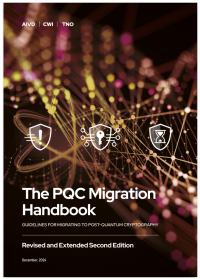
hsrm

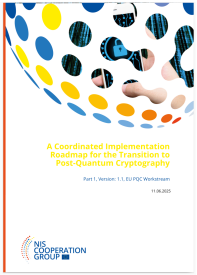
Agenda

Motivation

- Today, cryptography is used everywhere in computer systems
- Current asymmetric algorithms such as RSA and ECC are vulnerable to quantum computers
- Shor's algorithm can break these systems because due to recent advancements in the field of quantum computing it efficiently solves the exact mathematical problems those systems rely on for security.
- So, it is necessary to move to post-quantum cryptography

- NIST is working on standardizing post-quantum algorithms
- Some algorithms have already been standardized
- Current algorithms will be phased out around 2030–2035.
- This leaves little time to migrate because migration es very low and complex.
- There are already exist guideline for how to migrate, but is it enough?





Core Issue with Migration to PQC

- Migration is not only algorithm replacement because, cryptography affects protocols.
- Cryptography is deeply embedded in systems e.g., in TLS.
- Distributed architectures increase complexity because, multiple interconnected components must be updated consistently.
- Hidden dependencies create unexpected risks because, of indirect uses of cryptography.
- Lack of structured methodologies increases failure probability because, without systematic processes, migrations may be incomplete.
- Without a clear methodology, the transition can fail because due partial migration leaving systems insecure.

Paper Objectives

- Analyze and compare existing Post-Quantum Cryptography (PQC) migration frameworks
- Identify how these frameworks address key aspects of migration:
  - Identification of cryptographic components
  - Dependency analysis
  - Risk evaluation and prioritization
  - Cryptographic agility (Crypto agility)
  - Key management
- Evaluate how complete and mature these approaches are
- Highlight the main limitations of current solutions
- Identify open challenges and research gaps for a more reliable PQC migration

- **RQ1 Methodology Maturity**
  - What methods within existing frameworks for PQC migration are used and are they suitable enough for the steps in the migration phases?
- **RQ2 Cryptographic Agility**
  - Do existing frameworks for migration methods take cryptographic agility into account, and if so, to what extent in terms of their properties and a common definition?
- **RQ3 Key Management**
  - What migration stages consider key management and to what extent?

- Survey was done via a systematic literature review following the PRISMA approach
- Search Query: “PQC AND migration AND framework” for academic publications from 2020 to 2026.
- Out of 3760 papers we select 22 relevant papers describing migration frameworks and strategies
- Then we analysed and compared them based on defined criteria.

RESEARCH METHODS AND REPORTING

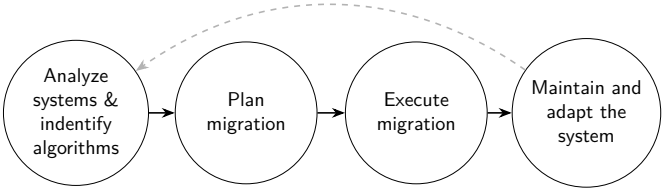
The PRISMA 2020 statement: an updated guideline for reporting systematic reviews

3760 ⟶ 51 ⟶ 22

Initial Filtered Selected

Typical Stages of a Migration Framework

- Most frameworks focus on the identification stage.
- Few frameworks cover the entire migration process [ets24, NHG+24, VNWAH24, WAB+].
- The execution and maintenance phases are often neglected.



Identification of Cryptographic Assets

- Identify all cryptographic assets, e.g., by building an inventory (CBOM):
  - Algorithms
  - Protocols
  - Keys
- Techniques:
  - Manual analysis
  - Automated scanning, cf. [TVSM24] (own tooling *Inventory Generator Tool (IGT)*)
- Challenges:
  - Cryptography hidden in legacy code
  - Third-party libraries are not documented
  - Dynamic usage of cryptographic during runtime
  - Inventory maintenance over time is difficult

Dependency Analysis in PQC Migration

- When we migrate to PQC, we do not change isolated components
- Every system element depends on others (data, crypto, applications)
- These dependencies directly impact:
  - How difficult the migration is
  - In which order components must be updated
  - Whether the migration is even feasible
- All frameworks agree on their importance
- But they differ in how they analyze them:
  - Simple identification vs formal modeling
- Key idea:
  - Complexity comes from the system structure, not just the algorithms [LGH+24]

How Dependencies Are Analyzed

- Some approaches stay at a high level, cf. [GM24]
  - Identify links between systems, data, and organizations
  - Useful to understand global exposure
- Others go deeper and model dependencies explicitly, cf.[HSB+24]
  - Using graphs to represent relationships between assets
  - Helps to reason about security and protection needs
- Some approaches focus on implementation details, cf. [TVSM24]
  - Extract dependencies directly from code (call graphs)
  - Very precise, but harder to scale
- Finally, formal approaches model the system mathematically, cf. [LGH+24, ets24]
  - Identify clusters and constraints
  - Show why migration becomes complex in large systems

Outcomes

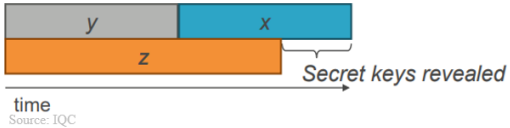
- There is no single “best” approach
- Simpler methods are easier to apply
  - But they miss hidden dependencies
- More formal methods are more powerful
  - But also more complex to implement
- In practice:
  - Small systems $\rightarrow$ simple inventory-based approaches
  - Large infrastructures $\rightarrow$ graph-based models are necessary

Risk Assessment in PQC Migration

- Risk assessment is essential for the planing:
  - What needs to be migrated first
  - What can be delayed
- Risk depends on:
  - Cryptographic vulnerability
  - Value and lifetime of data
  - Migration effort and constraints
- A common approach is based on time:
  - X = data lifetime
  - Y = migration time
  - Z = quantum threat horizon

$$X + Y < Z$$

- If not satisfied $\rightarrow$ high exposure risk, cf. [ets24, TVSM24, GM24]



If the migration is too slow, the risk increases

- Different frameworks assess risk in different ways
- **Temporal and quantitative models**, cf. [TVSM24]
  - Based on time, probability, and exposure
  - Allow prioritization of urgent assets
- **Dependency-based risk**, cf. [HSB+24, LGH+24]
  - Risk appears when sensitive data depends on weak cryptography
  - Influenced by system structure
- **Organizational and strategic risk**, cf. [GM24, NSB+23]
  - Linked to governance and crypto-agility
  - Risk increases if systems cannot evolve quickly

Cryptographic Agility

- The ability to replace or update cryptographic algorithms quickly and safely. (No uniform definition)
- Key requirement for long-term resilience
- Allows hybrid cryptographic deployments

Approach of Cryptographic Agility

- Cryptographic agility is not just technical, it involves design, processes, and organization
- Common approaches:
  - **Architecture and design**
    - Avoid hard-coded cryptography
    - Separate cryptography from application logic
  - **Policies and governance**
    - Integrate cryptographic agility into system design and procurement
- Challenges:
  - Increased complexity and attack surface
  - Performance and storage constraints
  - legacy systems

Key Management in PQC Migration

- Key management is a core part of any cryptographic system
- In PQC migration, it becomes even more critical:
  - New algorithms → new keys
  - Larger key sizes
  - New constraints on storage and performance
- However, most frameworks treat it only at a high level
  - Mainly as part of inventory or asset identification
- Few approaches consider the full lifecycle:
  - Generation
  - Storage
  - Rotation
  - Deprecation

Approach for Key Management

- Inventory-level approaches, cf. [AAB+24, NSB+23, MCD+21]
  - Keys treated as assets
  - Little detail on lifecycle management
- Integrated but implicit approaches, cf. [ets24]
  - Key management appears across all migration phases
  - No dedicated process, but consistent consideration
- Operational and lifecycle-oriented approaches, cf. [WAB+, Rob25]
  - Focus on key rotation, storage, and deployment
  - Consider real-world constraints and tooling

- **RQ1 Methodology Maturity**
  - Frameworks differ in structure and level of detail
  - No unified methodology covering all migration stages
- **RQ2 RQ2 Cryptographic Agility**
  - Widely recognized as essential
  - But no common definition or consistent implementation
- **RQ3 Key Management**
  - Often limited to asset identification
  - Rarely addressed as a full lifecycle process

Conclusion & Future Work

- PQC migration is not optional anymore it is a complex but necessary transition for future security.
- Existing PQC migration frameworks remain fragmented and do not provide a complete solution.
- A unified and systematic methodology is essential to enable a reliable and scalable PQC migration.
- Future work must integrate following dimensions:
  - Develop a unified methodology
  - Better integrate key management
  - Improve dependency analysis
  - Clarify crypto-agility

Thank you!

Let us start to create a sufficient migration framework!

References I

Back to start

[AAB+24] Alessandro Amadori, Thomas Attema, Maxime Bombar, Jo ao Diogo Duarte, Vincent Dunning, Simona Etinski, Daniël van Gent, Matthieu Lequesne, Ward van der Schoot, Marc Stevens, AIVD Cryptologists, and Advisors.
The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography – Revised and Extended Second Edition.
Technical report, TNO, Applied Cryptography and Quantum Algorithms and CWI, Cryptology Group and AIVD, Netherlands National Communications Security Agency, December 2024.

[ets24] A Repeatable Framework for Quantum-Safe Migrations, 2024.

[GM24] Amare Geremew and Atif Mohammad.
Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing.
International Journal on Engineering, Science and Technology, 6(4):338–365, September 2024.

[HSB+24] Khondokar Fida Hasan, Leonie Simpson, Mir Ali Rezazadeh Baee, Chadni Islam, Ziaur Rahman, Warren Armstrong, Praveen Gauravaram, and Matthew McKague.
A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies.
IEEE Access, 12:23427–23450, 2024.

References II

[LGH+24] Daniel Loebenberger, Stefan-Lukas Gazdag, Daniel Herzinger, Eduard Hirsch, Christian Näther, and Jan-Philipp Steghöfer.
On the Formalization of Cryptographic Migration, 2024.
Version Number: 4.

[MCD+21] Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, and Vaibhav Garg.
Caraf: crypto agility risk assessment framework.
Journal of Cybersecurity, 7(1):tyab013, 2021.

[NHG+24] Christian Näther, Daniel Herzinger, Stefan-Lukas Gazdag, Jan-Philipp Steghöfer, Simon Daum, and Daniel Loebenberger.
Migrating Software Systems Toward Post-Quantum Cryptography-A Systematic Literature Review.
IEEE Access, 12:132107–132126, 2024.

[NSB+23] William Newhouse, Murugiah Souppaya, William Barker, Chris Brown, Panos Kampanakis, Marc Manzano, David McGrew, Anne Dames, Vladimir Soukharev, Philip Lafrance, Anthony Hu, David Hook, Raul Garcia, Evgeny Gervis, Eunkyung Kim, and Changhoon Lee.
Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery, 2023.

[Rob25] Amelia Roberts.
Quantum-Resistant Cryptography Migration Strategies for Long-Term Data Security in Healthcare.
Global Journal of Intelligent Technologies, 5(3):13–22, September 2025.

References III

[TVSM24] Meena Singh Dilip Thakur, Kumar Vidhani, Habeeb Basha Syed, and Rajan M.A.
Enterprise post quantum cryptography migration tools.
In *2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pages 327–329, 2024.

[VNWAH24] Nils Von Nethen, Alexander Wiesmaier, Nouri Alnahawi, and Johanna Henrich.
PMMP – PQC Migration Management Process.
In *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, pages 144–154. ACM, 2024.

[WAB+] Bill White, Gregg Arquero, Ritu Bajaj, Anne Dames, Gloria Ho, Richard Kisley, Henrik Lyksborg, Navya Ramanjulu, Jacob Ruwald, and Charu Tejwani.
Transitioning to Quantum-Safe Cryptography on IBM Z.