Università degli Studi di Messina, Italia
Dipartimento di scienze matematiche e informatiche,
scienze fisiche e scienze della terra

Soggetto: proposta di tirocinio

| | |
|---|---|
| *ID* | PTI_IT_distefano salvatore_19/02/2026 17.05.06 |
| *Data* | 19/02/2026 17.05.06 |

**Supervisore del progetto**

| | |
|---|---|
| *Cognome* | distefano |
| *Nome* | salvatore |
| *Dipartimento* | mift |
| *Laboratorio* | QUANTUM COMPUTING AND INFORMATION SYSTEMS |
| *E-mail* | sdistefano@unime.it |
| *Numero di telefono* | |

**Co-Supervisore del progetto**

| | |
|---|---|
| *Cognome* | |
| *Nome* | |
| *Posizione* | |
| *Dipartimento* | |

| | |
|---|---|
| *Laboratorio* | |
| *E-mail* | |
| *Numero di telefono* | |

**Dettagli del progetto**

| | |
|---|---|
| *Titolo* | Quantum-Safe by Design: Investigating NIST Post-Quantum Cryptography Standards and Migration Pathways |

*Descrizione dettagliata:*
## 1) Motivation & Context

Large-scale quantum computers will break widely used public-key cryptosystems (RSA, DH, ECC), which motivates an urgent transition to **post-quantum cryptography (PQC)**. Governments and standards bodies have begun to formalize this transition, and organizations are advised to prepare roadmaps now to mitigate “harvest-now, decrypt-later” risks.
[\[pages.nist.gov\]](https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/FAQ/index.html)

On **Aug 13–14, 2024**, the U.S. National Institute of Standards and Technology (**NIST**) published the **first PQC standards**: **FIPS 203 (ML-KEM, from CRYSTALS-Kyber), FIPS 204 (ML-DSA, from CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, from SPHINCS+).**
NIST also selected **HQC** as an additional KEM (Mar 11, 2025) to diversify key-establishment options, with standardization underway, and **Falcon** (FN-DSA) is progressing toward **FIPS 206** for signatures.
[\[csrc.nist.gov\]](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization),
[\[federalregister.gov\]](https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based)
[\[nist.gov\]](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process),
[\[nvlpubs.nist.gov\]](https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf),
[\[digicert.com\]](https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval

-from-nist)

In Europe, the **European Commission** issued a **Recommendation** (Apr 11, 2024) and a **Coordinated Roadmap** (Jun 23, 2025) to synchronize Member States' migration to PQC—making planning and inventories part of "state-of-the-art" cybersecurity under the NIS2 framework.
[\[hardenstance.com\]](https://www.hardenstance.com/wp-content/uploads/2024/04/EU-Commssion-Recommendation-on-PQC.pdf),
[\[digital-st....europa.eu\]](https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography)

## 2) Educational Goals

By the end of the internship, the student will be able to:

* Explain PQC fundamentals and the security assumptions behind **ML-KEM, ML-DSA, SLH-DSA**, and their parameter sets.
[\[csrc.nist.gov\]](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization)
* Read and summarize **FIPS 203/204/205**, track the status of **HQC** and **FN-DSA** (FIPS 206 draft), and map them to real-world use cases (TLS, code-signing, PKI).
[\[federalregister.gov\]](https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based),
[\[nist.gov\]](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process),
[\[digicert.com\]](https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist)
* Evaluate protocol transition patterns (e.g., **hybrid key exchange in TLS 1.3**, **HPKE**), understanding performance/bandwidth trade-offs.
[\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/),
[\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/html/rfc9180)
* Draft a **mini-migration roadmap** aligned with EU guidance (EC Recommendation & NIS-CG Roadmap).
[\[hardenstance.com\]](https://www.hardenstance.com/wp-content/uploads/2024/04/EU-Commssion-Recommendation-on-PQC.pdf),
[\[digital-st....europa.eu\]](https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography)

## 3) Scope & Activities (what the student will do)

1. **Standards Scouting & Briefing Notes (≈20–30 h)**
   * Create concise digests of **FIPS 203/204/205**: security categories, key/signature sizes, and typical application patterns (e.g., ML-KEM for key exchange, ML-DSA for general signatures, SLH-DSA as conservative fallback). [\[csrc.nist.gov\]](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization)
   * Note the status of **HQC** (selected 2025) and **FN-DSA/Falcon** (draft FIPS 206) and why diversity matters. [\[nist.gov\]](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process), [\[digicert.com\]](https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist)

2. **Protocols & Deployment Patterns (≈20–30 h)**
   * Study **TLS 1.3 hybrid KEX** (IETF draft) and **HPKE (RFC 9180)** to understand how PQ KEMs integrate into today's stacks. [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/), [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/html/rfc9180)
   * Identify practical deployment issues (handshake size, MTU, cert chains) using best-practice notes (e.g., ETSI TR on hybrids). [\[etsi.org\]](https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf)

3. **Hands-on Measurements / Mini-Lab (≈30–40 h)**
   * Collect **reference sizes** from the standards (e.g., ML-KEM-768: PK 1184 B, CT 1088 B; Dilithium3: PK 1952 B, SIG ≈3293 B; SPHINCS+ signatures are larger—7–30 KB, depending on parameters). Build a small dataset and discuss implications for TLS and PKI. [\[pq-crystals.org\]](https://pq-crystals.org/kyber/data/kyber-specification.pdf), [\[pq-crystals.org\]](https://pq-crystals.org/dilithium/), [\[pqcvisualizer.com\]](https://pqcvisualizer.com/)
   * (Optional stretch) Compare classical vs. hybrid handshake sizes using public data points and published drafts/guidance. [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/), [\[etsi.org\]](https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf)

4. **Policy & Migration Roadmapping (≈20–30 h)**
   * Map UniMe-relevant use cases (web services, VPNs, internal PKI,

software/firmware signing for lab devices) to **EU Roadmap** milestones and **CISA/NSA/NIST** migration guidance (crypto inventory, risk triage, vendor engagement).
[\[digital-st....europa.eu\]](https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography), [\[cisa.gov\]](https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf)
* Produce a 2–3 page **PQC Migration Starter Plan** for the department (inventory template, pilot suggestions, evaluation metrics).
[\[hardenstance.com\]](https://www.hardenstance.com/wp-content/uploads/2024/04/EU-Commssion-Recommendation-on-PQC.pdf)

## 4) Deliverables

* **D1. Standards Brief (8–10 pages)**: Executive summary of FIPS 203/204/205; status notes on HQC and FN-DSA; glossary.
[\[csrc.nist.gov\]](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization), [\[nist.gov\]](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process), [\[digicert.com\]](https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist)
* **D2. Protocol Note (3–4 pages)**: TLS-hybrid overview and HPKE integration, with a one-page risk/benefit sheet for hybrid vs. pure PQ.
[\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/), [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/html/rfc9180)
* **D3. Mini-Dataset + 1–2 page Analysis**: Key, ciphertext, and signature sizes (ML-KEM, ML-DSA, SLH-DSA) and implications for UniMe services.
[\[pq-crystals.org\]](https://pq-crystals.org/kyber/data/kyber-specification.pdf), [\[pq-crystals.org\]](https://pq-crystals.org/dilithium/), [\[pqcvisualizer.com\]](https://pqcvisualizer.com/)
* **D4. PQC Migration Starter Plan (2–3 pages)**: Inventory template, pilot proposal, and alignment with EU Roadmap.
[\[digital-st....europa.eu\]](https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography)
* **D5. Final Presentation (12–15 slides)** for staff/students summarizing findings and recommended next steps, including references.

## 5) Tentative Roadmap & Effort (100–150 hours)

* **Week 1 (20–30 h):** Onboarding; read FIPS 203/204/205; draft D1 outline. [\[csrc.nist.gov\]](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization)
* **Week 2 (20–25 h):** Deep-dive on TLS hybrid & HPKE; start D2; compile initial size table for D3. [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/), [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/html/rfc9180)
* **Week 3 (20–25 h):** EU policy review; draft D4 (migration starter plan); refine D3 dataset. [\[hardenstance.com\]](https://www.hardenstance.com/wp-content/uploads/2024/04/EU-Commssion-Recommendation-on-PQC.pdf), [\[digital-st....europa.eu\]](https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography)
* **Week 4 (20–25 h):** Consolidate D1–D4; prepare slides (D5); rehearsal and feedback.
* **Optional buffer / stretch (up to +25 h):** Add Falcon/HQC updates; expand measurements; outreach to vendors about roadmaps (documented Q\&A). [\[nist.gov\]](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process), [\[digicert.com\]](https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist)

## 6) Assessment

* **Work products (D1–D4):** clarity, technical accuracy, and citation quality (60%).
* **Presentation (D5):** communication and critical insight (20%).
* **Professional skills:** planning, versioning, and responsiveness to feedback (20%).

## 7) Prerequisites & Resources

* Basics of cryptography and networks (TLS/PKI).
* Access to standards and guidance: **NIST PQC project page**, FIPS 203/204/205, **NIST IR 8545 (HQC)**, **IETF drafts/RFC 9180**, **EC Recommendation + EU Roadmap**, **CISA/NSA/NIST factsheet** (links in References). [\[csrc.nist.gov\]](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization), [\[nist.gov\]](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process), [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/), [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/html/rfc9180),

[\[hardenstance.com\]](https://www.hardenstance.com/wp-content/uploads/2024/04/EU-Commssion-Recommendation-on-PQC.pdf), [\[digital-st....europa.eu\]](https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography), [\[cisa.gov\]](https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf)

## 8) Risks & Mitigations

* **Standard evolution:** Falcon (FN-DSA) and HQC details may evolve—student will track deltas and update briefs accordingly. [\[nist.gov\]](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process), [\[digicert.com\]](https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist)
* **Protocol churn:** TLS hybrid drafts can change—focus on stable concepts and cite current versions. [\[datatracker.ietf.org\]](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/)
* **Time constraints:** Prioritize D1–D4; stretch items only if time remains.

***

## References (key documents)

* **NIST PQC Standardization (hub & updates):** [Post-Quantum Cryptography | CSRC](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization)
* **FIPS issuance notice (Aug 14, 2024):** [Federal Register – FIPS 203/204/205 approved](https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based)
* **NIST Fourth-Round Status & HQC selection (Mar 11, 2025):** [NIST IR 8545](https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process)
* **Falcon → FN-DSA (FIPS 206) status:** [DigiCert blog update](https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist)
* **IETF HPKE:** [RFC 9180](https://datatracker.ietf.org/doc/html/rfc9180)
* **TLS 1.3 hybrid key exchange:** [IETF draft-ietf-tls-hybrid-design](https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/)

| |
|---|
| * **EU policy & roadmap:** [EC Recommendation on PQC transition (Apr 11, 2024)](https://www.hardenstance.com/wp-content/uploads/2024/04/EU-Commssion-Recommendation-on-PQC.pdf) and [Coordinated Implementation Roadmap (Jun 23, 2025)](https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography)<br>* **Migration guidance (US):** [CISA/NSA/NIST Quantum-Readiness factsheet](https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf)<br>* **Sizing & trade-offs:** Kyber parameter sizes (PK/CT) from the Kyber specification, Dilithium sizes from CRYSTALS site, SPHINCS+ signature sizes via visualizer/benchmarks. [Kyber spec](https://pq-crystals.org/kyber/data/kyber-specification.pdf), [Dilithium perf page](https://pq-crystals.org/dilithium/), [PQC signature size explorer](https://pqcvisualizer.com/)<br>* **Hybrid deployment considerations:** [ETSI TR 103 966](https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf) |

| | |
|---|---|
| *Durata (mesi – max 12)* | 3 |
| *Durata (ore)* | 100 |
| *Numero di posizioni aperte* | 6 |

**Competenze richieste dal tirocinio**

| | |
|---|---|
| *Requisiti tecnici:* | |
| *Altri requisiti* | |