**Team Name:** **Code Crafters**

**Members:**

- **Amanpreet Singh Gandhi(Student)**
- **Anjika Bahl (Student)**
- **Dr. Mahamuda Sultana(Professor)**

**Problem Statement:** **Post-Quantum DNSSEC Testbed under a Delegated .IN Domain**

# TABLE OF CONTENTS

**Blog link**

# Introduction

- **Theme:** Post-Quantum Cryptography (PQC) in DNSSEC Infrastructure
- **Focus Areas:** DNSSEC – Quantum-Resistant Key Algorithms
- **Organized by:** Advanced Internet Operations Research in India (AIORI)
- **Collaborating Institutions:** Guru Nanak Institute of Technology, Kolkata(GNIT)
- **Date:** 05/11/2025
- **Prepared by:**

| Name | Designation | Institution |
|---|---|---|
| Amanpreet Singh Gandhi | Student | Guru Nanak Institute of Technology, Kolkata |
| Anjika Bahl | Student | Guru Nanak Institute of Technology, Kolkata |
| Dr. Mahamuda Sultana | Professor | Guru Nanak Institute of Technology, Kolkata |

**Contact:** amanfromgnit@gmail.com

- ## Executive Summary

This sprint implemented a unified benchmarking framework to evaluate the performance of post-quantum cryptographic algorithms (SQIsign, Falcon512, Dilithium2, and SPHINCS+) within DNSSEC signing and validation workflows on the PowerDNS platform. Using containerized environments, the benchmark measured query latency, response size, and key/signature length metrics, contributing valuable data for PQC integration feasibility in Internet DNS infrastructure.

- ## Overview

This sprint successfully established a unified benchmarking framework designed to stress-test the viability of Post-Quantum Cryptography (PQC) within the critical infrastructure of DNSSEC. By integrating cutting-edge algorithms—specifically SQIsign, Falcon512, Dilithium2, and SPHINCS+—into the PowerDNS ecosystem, we moved beyond theoretical security to practical performance analysis.

The methodology relied on a high-fidelity, containerized testbed managed via Podman, ensuring environment parity and reproducible results. Our primary focus was quantifying the "quantum-readiness" of DNSSEC workflows by measuring three critical vectors: query latency, response payload size, and cryptographic overhead (key/signature lengths).

The findings provide a data-driven foundation for navigating the trade-offs between signature size and computational speed—a core challenge defined in RFC 8624 and emerging PQC drafts. By automating the data logging and metric aggregation phases, we have produced a transparent, open-source-aligned research tool that evaluates how these algorithms behave under real-world DNS resolution constraints, directly informing future transitions to quantum-resistant internet protocols.

## Objectives

- Integrate and benchmark PQC algorithms under DNSSEC (RFC 4033–4035, RFC 8624).
- Evaluate DNS response behavior, latency, and signature overhead with PQC-based signing.
- Automate testbed setup using container orchestration (Podman).
- Contribute reproducible benchmarking scripts to open-source DNSSEC research.

## Scope and Focus Areas

| Focus Area | Relevant RFCs / Drafts | Open Source Reference | AIORI Module Used |
|---|---|---|---|
| DNSSEC (with PQC extensions) | RFC 4033–4035, RFC 8624, draft-ietf-lamps-pq-hybrid-sigs | PowerDNS, BIND Test Environments | |

## Sprint Methodology

- **Workflow:**
  - RFC & Algorithm Selection (PQC for DNSSEC)
  - Environment Setup via Container Automation (Podman)
  - Implementation and Query Benchmarking
  - Data Logging and Metric Aggregation
  - Open Source Documentation and Report Submission

## Activities and Implementation

| Date | Activity | Description | Output / Repository |
|---|---|---|---|
| 01/11/2025 | Sprint 1: PQC Integration | Implemented SQIsign, Falcon512, Dilithium2, SPHINCS+ into PowerDNS configuration files | [GitHub Repo Link] |
| 02/11/2025 | Sprint 2: Automated Benchmark | Automated container builds, DNSSEC signing, and query latency measurement | [GitHub Repo Link] |
| 03/11/2025 | Sprint 3: Result Aggregation | Generated latency, key-size, and response metrics in CSV and TXT reports | [GitHub Repo Link] |

## Results and Findings

- Average DNS query times increased moderately (5–15%) with PQC-enabled keys.
- SPHINCS+ exhibited the largest signature size (~40–50 KB), impacting response size.
- Falcon512 and Dilithium2 provided the best trade-off between key size and latency.
- Podman-based isolation proved effective for reproducible DNSSEC test environments.

## Open Source Contributions

- No upstream open-source contributions were made during this sprint.
- However, all benchmarking scripts and configurations have been prepared for future release under the AIORI open repository once validation and review are complete.

- **Collaboration with IETF WGs**
    - No direct collaboration or communication with IETF Working Groups took place during this sprint.
    - However, our work aligns with ongoing discussions in DNSOP and LAMPS related to post-quantum DNSSEC, and the team intends to share findings in future AIORI-IETF outreach sessions.
- **Impact and Future Work**

This work demonstrates practical PQC deployment viability within DNSSEC and provides baseline data for hybrid PQC-RSA signing. Future work includes:

- Integration into AIORI-IMN PQC module.
- Extending tests to PQ-hybrid key exchanges (RFC 9555 drafts).
- Publishing results as an Internet-Draft.

## Technical Blog Series & Dev Diary

- **Lead Paragraph**

In the AIORI-2 Hackathon, our team benchmarked post-quantum digital signature algorithms within DNSSEC to assess operational overhead and interoperability using the AIORI Secure DNS Testbed.

- **Background and Motivation**

As quantum threats emerge, DNSSEC's RSA and ECDSA keys will become vulnerable. We explored replacing them with post-quantum algorithms (Falcon, Dilithium, SPHINCS+) and tested their performance using containerized PowerDNS instances.

- **Technical Implementation**
    - **Setup and Tools:**
        - OS: Ubuntu 24.04 LTS
        - Software: PowerDNS (ghcr.io/sidn/pqc-auth-powerdns), Podman, dig, lsof
        - Measurement Tools: dig, awk, Wireshark, CSV log parser
    - **Implementation Steps:**
        - Automated Dockerfile creation for each PQC algorithm.
        - Configured PowerDNS with default-ksk-algorithm and default-zsk-algorithm.
        - Launched isolated containers and queried DNSKEY/A/NS records.
        - Collected query latency, response sizes, and base64 key lengths.
        - Exported aggregated results in .txt and .csv format.
    - **Challenges Faced:**
        - Some containers failed on initial build due to missing zone rectification.
        - Signature parsing for large SPHINCS+ records required optimized buffer handling.
        - Port conflicts during multiple runs required dynamic cleanup scripts.
- **Results and Observations**

| **Test** | **Metric** | **Observation** | **Note** |
|---|---|---|---|
| Falcon512 | Avg Query Time | 8–12 ms | Stable response |
| Dilithium2 | Avg Query Time | 10–15 ms | Balanced key/signature size |
| SPHINCS+ | Response Size | 40–50 KB | Very large signature overhead |
| SQIsign | Build Time | ~45s | Smallest base64 key size |

- **Lessons Learned**
  - PQC algorithms impose significant DNS payload size increases.
  - Automated containerization ensures reproducibility.
  - Hybrid approaches (PQC + classical) are operationally feasible.
- **Open Source and Community Contributions**
  - No upstream open-source contributions were made during this sprint.
  - However, all benchmarking scripts and configurations have been prepared for future release under the AIORI open repository once validation and review are complete.
- **Future Work**
  - Extend tests to hybrid PQC-RSA trust anchors.
  - Publish technical note in IETF DNSOP WG.
  - Develop visualization dashboard for benchmark comparison
- **Reporting and Standards Mapping**

## AIORI-2: Reporting and Standards Mapping

| Team Name | Institution | Project Title | Focus Area |
|---|---|---|---|
| [Your Team Name] | [Your Institution] | Post-Quantum DNSSEC Benchmarking on PowerDNS | ☑ DNSSEC □ RPKI □ QUIC □ Encrypted DNS □ Other |

Date: 5th November 2025

- **Standards Reference**

| RFC / Draft No. | Title / Area | Lifecycle Stage | How This Work Relates |
|---|---|---|---|
| RFC 4033–4035 | DNSSEC Protocol Framework | Internet Standard | Base DNSSEC functionality under PQC test |
| RFC 8624 | Algorithm Implementation Requirements | Internet Standard | Guidance for algorithm selection in DNSSEC |
| draft-ietf-lamps-pq-hybrid-sigs | PQC Hybrid Signatures | Internet-Draft | Provides baseline for hybrid PQC-DNSSEC design |

- **Impact on Standards Development**

| Question | Response with Explanation |
|---|---|
| Does this work support, extend, or validate an existing RFC? | Supports and stress-tests DNSSEC RFCs (4033–4035, 8624) with post-quantum |
| Could it influence a new Internet-Draft or update sections of an RFC? | Potentially contributes empirical data for PQC hybrid key management in DNSSEC. |
| Any feedback or data shared with IETF WG mailing lists (e.g., DNSOP, SIDROPS, DPRIVE, | No direct feedback or WG interaction occurred during this sprint. |
| Planned next step (e.g., share measurement dataset / open PR / draft text). | Plan to publish benchmark dataset and share findings with AIORI and DNSOP in follow-up |

- **References**

  - RFC 4033–4035 – DNSSEC Protocol Framework
  - RFC 8624 – Algorithm Implementation Requirements
  - draft-ietf-lamps-pq-hybrid-sigs
  - AIORI Testbed Documentation: [aiori.in/testbed]
  - IETF DNSOP WG: https://datatracker.ietf.org/wg/dnsop

- **Acknowledgments**

We thank AIORI mentors, and our institution's research node for infrastructure and guidance.

- **Reflections from the Team**
  - **Amanpreet Singh Gandhi:** "Integrating PQC algorithms into DNSSEC made us appreciate the importance of DNS payload optimization. We started out to integrate PQC algorithms into DNSSEC, and ended up with newfound respect for Internet engineering precision"
  - **Developer:** "Container automation simplified benchmarking across multiple PQC implementations."

- **About the Authors**

Code Crafters represent Guru Nanak Institute of Technology, Kolkata, participating in the AIORI-2 Hackathon (Nov 2025) to advance PQC-based Internet security standards.

- **Contact**

  - **Lead Author:** Amanpreet Singh Gandhi
  - **Email:** amanfromgnit@gmail.com
  - **Mentor:** Dr. Mahamuda Sultana