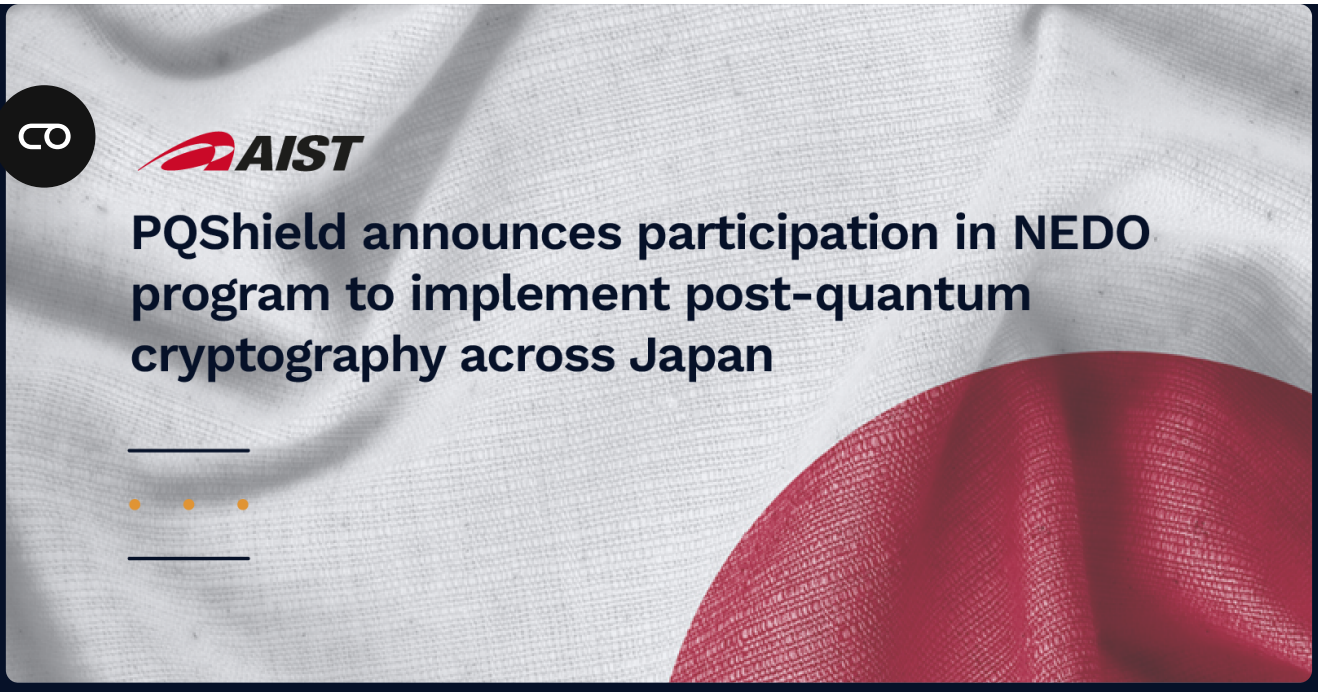
PQShield announces participation in NEDO program to implement post-quantum cryptography across Japan

‹ Back

Author: Dr Shuichi Katsumata

Topics: News

Date: 21/01/2025



- ***PQShield has been named a supporting member of the Cyber Research Consortium (CRC), which is receiving a grant from Japan's New Energy and Industrial Technology Development Organization (NEDO).***
- ***NEDO is funding the CRC for a major project to enhance Japan's defenses against cyber attacks, improve its situational awareness, and establish a common cybersecurity infrastructure.***
- ***As part of the CRC, we have been subcontracted to design and deliver new PQC primitives and protocols across Japan, and to conduct R&D towards the ongoing global development of PQC standards.***

We are proud to announce that we have joined the Cyber Research Consortium (CRC) in Japan to participate in its program with the Japanese government's New Energy and Industrial Technology Development Organization (NEDO) to enhance Japan's defense against quantum-enabled cyber attacks. As a supporting member of the CRC, we will design and deliver PQC protocols that can be implemented across Japan's technology supply chain, and contribute to the ongoing global PQC

standardization process. NEDO is providing a funding grant to CRC to support this project.

The publication of NIST's finalized PQC standards in August 2024 gave businesses, governments, and institutions globally a defined route to modernizing their cryptography, safeguarding their data, and protecting themselves from future quantum attacks. In July 2024, to kick-start this process in Japan, NEDO announced that research into PQC implementation technologies would take place as part of its "Enhancement of situational awareness and defense capabilities to counter cyber attacks", a newly-established project within Japan's K Program funded by NEDO and delivered by the CRC. The goal of this research is to achieve advanced functionality in quantum-resistant cryptography, such as ring signatures, threshold signatures, and threshold encryption. The K Program is an R&D initiative that builds on the collaboration between public and private organizations in Japan to investigate critical technologies for civil and defense purposes.

We have been named a supporting member of the CRC under its NEDO grant, and will be subcontracted to deliver designs and protocols for PQC implementation technologies. Our Lead Cryptography Researcher Dr Shuichi Katsumata, based in Japan, will lead the company's work under the CRC.

As part of the CRC, we are being subcontracted to carry out two PQC projects for NEDO: designing PQC primitives; and, in collaboration with AIST, constructing new protocols to ensure that non-PQC protocols can be updated to align with NIST's latest standards. Both projects will contribute to the ongoing effort to coordinate robust, global standards for PQC. All results will be published in academic papers, the primitives we have designed will be submitted to NIST's standardization call for multi-party

threshold cryptography, and the protocols constructed with AIST will be shared with the Internet Engineering Task Force to become public RFCs.

We are working directly with AIST on the design and standardization of new PQC protocols, while further support for this project is being provided by CRC subcontractors SCU Inc., Mitsubishi Electronics, and The University of Tokyo. The full list of participants in this project is:

- FFRI Security Inc
- Preferred Networks Inc
- Fujitsu
- NTT
- Powder Keg Technologies
- Ricerca Security
- Mitsubishi Electronics
- Japan Electronics
- Hitachi
- Toppan
- PQShield
- Secafy
- SCU Inc
- Yokohama National University
- Waseda University
- Keio University
- The University of Tokyo

- AIST
- Iwasaki Gakuen

Through this collaborative project we aim to enhance the functionality and security of the technology supply chain across Japan and globally. This includes planned R&D into the difficulty of the lattice problems PQC is based in, opening up avenues to understand the fundamental security of current cryptography standards. We already have a strong presence in Japan, with partners including Mirise Technologies, Sumitomo Electric and NTT Data Group Corporation – the NEDO grant supports the company's growing presence in the market and the expansion of its local team.

Dr Ali El Kaafarani, founder and CEO of PQShield, said: "Securing critical infrastructure from quantum computers requires strong collaboration between governments, universities and the private sector, and this project is an ambitious and necessary step to protect against the quantum threat. Japan is an important market for PQShield and plays a critical role in the global technology supply chain. We are pleased to be working directly with NEDO and the government of Japan to help implement PQC across the country and protect against the cyber threats of the future."

Tsutomu Matsumoto, AIST Fellow / Director of CPSEC said, "The implementation of post-quantum cryptography across Japan is extremely important, and updating existing protocols to support NIST's latest standards will play a significant role in this process. We're pleased to support this vital mission and look forward to collaborating with fellow CRC subcontractors, including PQShield, to design and standardize new protocols which can become public RFCs."
This project with the CRC and NEDO will run from 2024 to 2026, with the final standardization documents to be delivered in 2026.

About AIST

The National Institute of Advanced Industrial Science and Technology (AIST), one of the largest public research organizations in Japan, focuses on the creation and practical realization of technologies useful to Japanese industry and society, and on “bridging” the gap between innovative technological seeds and commercialization.

For this, AIST is organized into 5 departments and 2 centers that bring together core technologies to exert its comprehensive strength.

AIST, as a core and pioneering existence of the national innovation system, has about 2300 researchers doing research and development at 12 research bases across the country, based on the national strategies formulated bearing in mind the changing environment regarding innovation.

AIST is also actively building a global network by, for example, signing memorandums of understanding for comprehensive research cooperation (MOUs) with major research institutes around the world.

About NEDO

NEDO, the New Energy and Industrial Technology Development Organization, is a Japanese national research and development agency that creates innovation by promoting technological development necessary for realization of a sustainable society. NEDO acts as an innovation accelerator to contribute to the resolution of social issues by developing and demonstrating high-risk innovative technologies having practical application. Learn more about NEDO at here.

Please get in touch if you would like a copy of the press release in Japanese.

Sign up for our newsletter

PQShield comprises a world-class collaboration of post-quantum cryptographers, engineers, and operators. We've helped shape all of the first international PQC NIST standards, and we were the first cybersecurity company to develop quantum-safe cryptography on chips, in applications, and in the cloud.

Links

- Team PQShield
- Products
- Markets
- Publications
- News
- Partners
- Careers
- Contact
- Security, Quality & Legal
- Report a Bug or Vulnerability

Markets

- Semiconductors and Manufacturing
- Military and Aerospace
- Identity and Paymentech
- System Integrators
- Network & Telecommunications
- Automotive
- Industrial IoT
- Enterprise Platforms

Products

- PQPlatform – TrustSys
- PQPerform – Lattice
- PQCryptoLib – Embedded
- PQPlatform – Hash
- PQPlatform – Lattice
- PQPlatform – CoPro
- PQPlatform – SubSys
- PQSDK
- PQCryptoLib
- Product Security