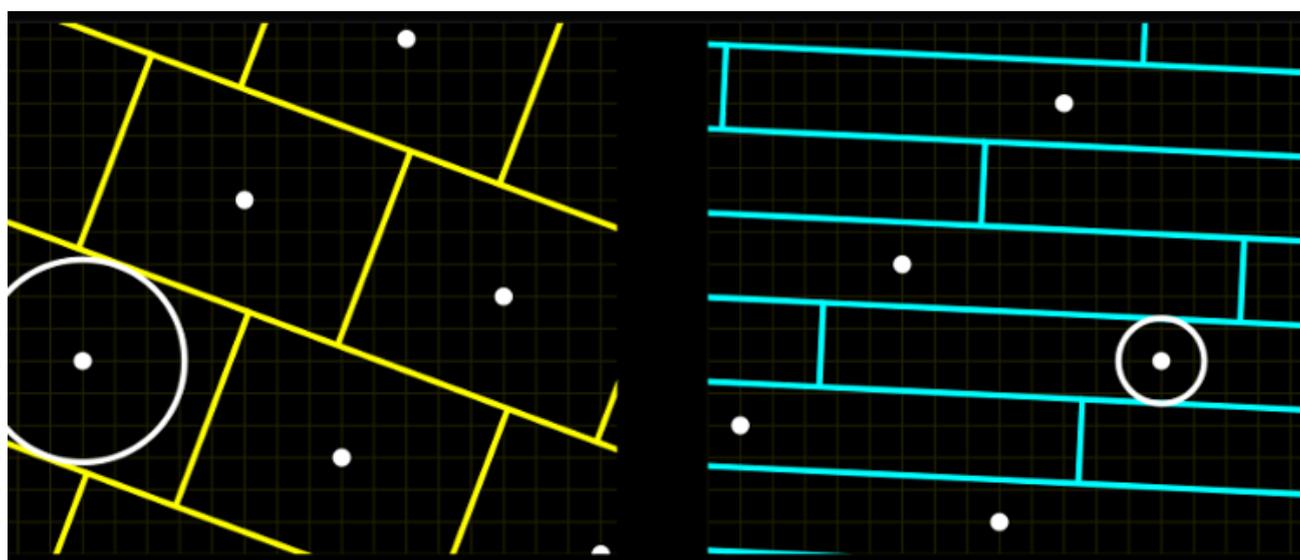


[Home](#) > [Academics](#) >



[ACADEMICS](#) [INTERNATIONAL NEWS](#) [UNIVERSITY NEWS](#)

## Leiden University's Ducas Co-Designs Key Quantum-Safe Cryptography Methods

By [lednewsdesk](#)

On [Aug 22, 2024](#)

Three quantum-safe cryptography methods have been standardised for worldwide use since this week. Léo Ducas co-designed the two primary PQC methods selected for this standardisation. Ducas is part of the Cryptology group at Centrum Wiskunde & Informatica (CWI) and is also

professor of Mathematical cryptology at Leiden University.

From competition to standardization: three quantum-safe cryptography methods are now standardized for global use. The US National Institute of Standards and Technology (NIST) announced this on 13 August 2024. Quantum-safe cryptography is also called post-quantum cryptography (PQC). Léo Ducas from CWI's Cryptology group co-designed the two primary PQC methods selected for this standardization. The new standards have been finalized eight years after the competition was first announced, and a boost in adoption rates is expected soon.

## Why do we need quantum-resistant encryption methods?

Current advances in quantum computing threaten the security of our digital communications. Classical encryption methods are designed to be secure against attacks via existing (classical) computers. Their security depends on difficult mathematical tasks such as prime factorization: breaking down a large number into its prime factors. When executed by classic computers, this would require an immense amount of energy and tens of thousands of years.

Sensitive data can be deciphered when using a quantum computer.

However, future quantum computers can solve specific mathematical tasks like these very efficiently, meaning they could break classical methods in a relatively short time. This implies that sensitive data that are being sent or stored in encrypted form today, can be intercepted and deciphered at a later time when using a quantum computer.

## Competition for new encryption methods

To mitigate these risks, the National Institute of Standards and Technology published in 2016 its Post-Quantum Cryptography Standardization competition. Scientists from all over the world submitted proposals for new encryption and signature methods that were designed to be immune to quantum attacks. The 82 submitted proposals were reviewed in several rounds by the cryptography scientific community. In 2022, one encryption method and three methods for digital signatures were chosen for standardization: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ and FALCON.

## Standards help implementation

Now, NIST published the standards with new official names for CRYSTALS-Kyber (ML-KEM), CRYSTALS-Dilithium (ML-DSA), and SPHINCS+ (SLH-DSA). A fourth standard, Falcon (FN-DSA), is expected to be finalized later, and further standards are expected to be added to the portfolio in the coming years. These standards are intended to help implement the new encryption methods into online applications smoothly without the risk of disrupting current security safeguards.

These standards are intended to help implement the new encryption methods smoothly

Many companies had already recognized the importance of implementing these new secure encryption methods before the standards have been published. The adoption of CRYSTALS-Kyber has started in 2023 and has been implemented by 17.1% of the clients using Cloudflare (as of 5

August 2024, according to Cloudflare). This translates to more than half a trillion connections per day terminating at Cloudflare secured using PQC. The biggest early adopters are services such as iMessage (Apple), Google Chrome, Signal, Zoom, and Cloudflare.

## Protecting privacy of billions of users

Together with international colleagues from numerous institutions (listed below), Léo Ducas co-designed what are now the two primary standards CRYSTALS-Kyber (ML-KEM), CRYSTALS-Dilithium (ML-DSA).

Ducas: 'The standardization of our scheme means that it will be deployed globally, protecting the privacy of billions of users; fundamental research rarely gets such a direct and broad impact. The credit should go to the whole cryptographic research community; the schemes we proposed are merely the crystallization of decades of scientific effort.'



Leiden University

**lednewsdesk** - 82131 Posts - 0 Comments

© 2024 - India Education | Latest Education News | Global Educational News | Recent Educational News. All Rights Reserved.

Powered By: [Suryanandan.net](https://suryanandan.net)

---

[Privacy and cookie settings](#)

Managed by Google. Complies with IAB TCF. CMP ID: 300

---