PRESS RELEASE

Singapore, 5th November 2024

# Banque de France and Monetary Authority of Singapore conduct groundbreaking Post-quantum Cryptography experiment to enhance communication security

**The Banque de France (BDF) and the Monetary Authority of Singapore (MAS) today announced the successful completion of a groundbreaking joint experiment in post-quantum cryptography (PQC) conducted across continents over conventional Internet technologies. The PQC experiment aims to strengthen communication and data security in the face of quantum computing advancements, and the successful experimentation marks a crucial milestone in the evolution of the protection of international electronic communications against the cybersecurity threats posed by quantum computing.**

The joint BDF-MAS initiative trialled its first use of quantum-resistant cryptographic algorithms for the signing and encryption of emails. The goal was to strengthen the current level of security for electronic communications in the future, while retaining compatibility with existing Internet standards, technologies and communication channels. In this context, emails are particularly sensitive, as they may carry confidential information, making them a prime target for cyberattacks. This experiment not only demonstrates the practical feasibility of these new security methods but also their effectiveness in widely-adopted application environments.

## A hybrid approach for maximum security

The project followed a hybrid approach , combining the robustness of current algorithms with post-quantum algorithms to ensure security and compatibility with existing systems, while preparing for the cybersecurity threats posed by quantum computing.

## An aspiration to be quantum safe

A technical report, which details the results and takeaways from the experiment, was published today. The key findings of the report include:

a) Using Microsoft Outlook as the email client coupled with a PQC email plugin, BDF and MAS successfully exchanged digitally-signed and encrypted emails using PQC algorithms, namely CRYSTALS-Dilithium and CRYSTALS-Kyber.

b) Standardising PQC cryptographic algorithms and libraries for digital signatures and encryption, is not enough. Application protocols and standards like public key infrastructure, digital certificates, key exchanges and secure emails must also be standardised to incorporate PQC cryptographic algorithms to facilitate adoption and interoperability of PQC.

c) There is potential to integrate this technology into payment networks. By integrating PQC algorithms into payment networks, financial institutions can future-proof their security measures against the looming threat of quantum computing, ensuring the long-term integrity and confidentiality of sensitive financial data.

**A strong commitment to the future security of financial systems**

BDF and MAS will continue to collaborate in the next stage of experimentation, to extend PQC to critical financial transactions, particularly cross-border transactions on payment networks.
By collaborating on this pioneering experiment, BDF and MAS affirm their commitment to anticipating future threats and ensuring the security of global financial systems. This initiative also highlights the importance of international cooperation in addressing emerging cyber threats.

Mr Denis Beau, First Deputy Governor, BDF, said, *"Although quantum computing opens up promising new prospects in various fields, it also brings a threat to cyber security, particularly in protecting our communications. In this context, Banque de France, in its role of central bank, has been anticipating and multiplying experiments in post-quantum cryptography with its partners since 2022. The results of this first cooperation with the Monetary Authority of Singapore in the field of post-quantum cryptography reassure us of our ability to make our inter-institutional communications resilient. We are pleased that this cooperation can continue into a second phase."*

Ms Jacqueline Loh, Deputy Managing Director (Corporate Development), MAS, said, *"The looming threat of quantum-powered decryption is transforming cybersecurity strategies in financial services globally. The focus is now shifting towards cryptographic agility and ensuring systems can adapt by integrating with quantum-resistant algorithms. Financial institutions that prepare early for the quantum era will not only mitigate future risks but also position themselves to retain public trust in digital financial services. The collaborative efforts with Banque de France on post-quantum cryptography have been immensely valuable to MAS. We are thankful for this opportunity to work together on such a crucial initiative and look forward to continuing our shared journey in advancing quantum resilience."*

**What is quantum computing?**

Quantum computing uses the principles of quantum mechanics, advanced mathematics, and computer engineering to perform certain types of calculations at a speed unattainable by conventional computers. Unlike current computers, which process information in binary form (bits), quantum computers use qubits. The mathematical principles that apply to qubits enable quantum computers to achieve massive parallelism in information processing. Although still in development, this technology could revolutionise many sectors but also pose a threat to the security of current cryptographic systems.

**What is post-quantum cryptography?**

Post-quantum cryptography refers to a set of techniques and cryptographic algorithms designed to withstand the capabilities of future quantum computers. These machines, far more powerful than classical computers, could break asymmetric cryptography, thereby compromising the security of data and communications. Post-quantum cryptography aims to develop protection methods that remain unbreakable, even by advanced quantum technologies.

**About the Banque de France:** As an independent institution, the Banque de France has three main tasks: monetary strategy, financial stability, and services to the economy. It contributes to the definition of monetary policy in the euro area and its implementation in France; it supervises banks and insurance companies and ensures the sound management of risk; it provides many services to businesses and individuals.
Visit our website: www.banque-france.fr
Follow us

**About Le Lab :** As the Open Innovation centre of Banque de France, Le Lab acts as a catalyst to detect opportunities, experiment and build together with DGSI experts solutions to imagine the Central Bank of tomorrow.

**The Monetary Authority of Singapore (MAS)** is Singapore's central bank and integrated financial regulator. As a central bank, MAS promotes sustained, non-inflationary economic growth through the conduct of monetary policy and close macroeconomic surveillance and analysis. It manages Singapore's exchange rate, official foreign reserves, and liquidity in the banking sector. As an integrated financial supervisor, MAS fosters a sound financial services sector through its prudential oversight of all financial institutions in Singapore – banks, insurers, capital market intermediaries, financial advisors and financial market infrastructures. It is also responsible for well-functioning financial markets, sound conduct, and investor education. MAS also works with the financial industry to promote Singapore as a dynamic international financial centre. It facilitates the development of infrastructure, adoption of technology, and upgrading of skills in the financial industry. For more information, please visit https://www.mas.gov.sg.

Press contacts:

- Press service Banque de France

presse@banque-france.fr | +33 (0)1 42 92 39 00

- Monetary Authority of Singapore

Hidayah Rahim, Deputy Director (Communications)
hidayah_rahim@mas.gov.sg | +65 64225609