NXP Helps Standardize Next-Generation Security with Post-Quantum Cryptography

July 6, 2022

- *The U.S. Government's National Institute of Standards and Technology (NIST) selects specialized NXP Crystals-Kyber algorithm for post-quantum cryptography standard development*
- *Second NXP submission advances to fourth round for further analysis ahead of possible standardization*
- *Designed for use by traditional computers, the new standard for public key encryption will help secure data around the world against attacks from quantum computers*

EINDHOVEN, The Netherlands, July 06, 2022 (GLOBE NEWSWIRE) -- NXP Semiconductors (NASDAQ: NXPI) today announced that a specialized security algorithm co-authored by NXP security experts has been selected by NIST to become part of an industry global standard designed to counter quantum threats. A second algorithm co-authored by NXP will also advance to the fourth and final round for further analysis and consideration for standardization. As the dangers of quantum computers become more clear, this effort anticipates the need to protect encrypted data and connected devices. The selected post-quantum cryptography (PQC) algorithms will be used to develop a new public key encryption standard that is secure against both traditional and quantum computers.

Many cyber security experts believe that when large-scale quantum computers come to fruition, the sheer computing power of these machines will be able to "solve" encryption challenges in a fraction of the time, breaking today's public key encryption systems and leaving data, digital signatures and devices vulnerable. This creates substantial security risks for online devices and data, including financial transactions, critical infrastructure, over-the-air update mechanisms, and more.

To combat this, NIST announced an effort to standardize PQC algorithms that would allow the industry to transition to new, secure systems in advance of the quantum threat. The Crystals-Kyber lattice-based cryptography algorithm, submitted by NXP with security experts from IBM, will serve as the foundation for this new standard. The Classic McEliece, another co-authored NXP submission that belongs to the family of code-based cryptography, advances to an additional round of analysis and consideration for standardization.

"As the world becomes more connected and more data-driven, ensuring data and devices remain secure, even against quantum computers, is crucial," said Joppe Bos, Senior Principal Cryptographer at NXP. "As NIST moves forward with developing a new post-quantum standard, NXP will offer our deep knowledge in security, and specifically our algorithmic expertise, to fortify our products for a post-quantum future. We aim to contribute to the common standard so that our customers can achieve long-term security in their own products."

"The industry security experts of IBM, NXP and Arm®, together with their academic partners (ENS, RAB, CWI and RUB) have created an industry-leading submission that will help shape the way we think about encryption and security for decades to come," said Michael Osborne, Principal Research Scientist Manager for Foundational Cryptography at IBM. "Kyber is not only faster than current standards, it provides our clients with strong security to protect systems and data as we enter the quantum era."

For more information on PQC, please visit NXP.com/PQC.

About NXP Semiconductors
NXP Semiconductors N.V. (NASDAQ: NXPI) enables a smarter, safer and more sustainable world through innovation. As a world leader in secure connectivity solutions for embedded applications, NXP is pushing boundaries in the automotive, industrial & IoT, mobile, and communication infrastructure markets. Built on more than 60 years of combined experience and expertise, the company has approximately 31,000 employees in more than 30 countries and posted revenue of $11.06 billion in 2021. Find out more at www.nxp.com.

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/e90f7643-8605-4880-abe2-76bf21c19f2d

For more information, please contact:

Americas & Europe
Phoebe Francis
Tel: +1 737-274-8177
phoebe.francis@nxp.com

Greater China / Asia
Ming Yue
Tel: +86 21 2205 2690
Email: ming.yue@nxp.com

NXP Helps Standardize Next-Generation Security with Post-Quantum Cryptography

The U.S. Government's National Institute of Standards and Technology (NIST) selects specialized NXP Crystals-Kyber algorithm for post-quantum cryptography standard development. A second NXP submission advances to fourth round for further analysis ahead of possible standardization.

Source: NXP USA, Inc.