NXP unterstützt Definition des zukünftigen Sicherheitsstandards für Post-Quantum-Kryptographie

- Das National Institute of Standards and Technology (NIST) der US-Regierung entscheidet sich für den von NXP mitentwickelten Crystals-Kyber-Algorithmus im Rahmen des geplanten Post-Quantum-Kryptographie-Standards

- Eine zweite NXP-Einreichung geht in die vierte Runde zur weiteren Analyse vor einer möglichen Standardisierung

- Der neue Standard für Public-Key-Verschlüsselung wurde für den Einsatz auf herkömmlichen Computern entwickelt und wird dazu beitragen, Daten auf der ganzen Welt gegen Angriffe von Quantencomputern zu schützen

EINDHOVEN, Niederlande, 7. Juli 2022 – NXP Semiconductors (NASDAQ: NXPI) hat einen spezialisierten Sicherheitsalgorithmus mitentwickelt, der von NIST als Teil eines globalen Industriestandards zur Abwehr von Quantenbedrohungen ausgewählt wurde. Ein zweiter, von NXP mitentwickelter Algorithmus wird ebenfalls in die vierte und letzte Runde des Auswahlprozesses kommen. Er wird weiter analysiert, um zu entscheiden, ob er für die Standardisierung in Betracht kommt. Da die Gefährdung durch Quantencomputer immer deutlicher wird, trägt dieses Projekt der Notwendigkeit Rechnung, verschlüsselte Daten und vernetzte Geräte zu schützen. Die ausgewählten Algorithmen der Post-Quantum-Kryptographie (PQC) werden zur Entwicklung eines neuen Public-Key-Verschlüsselungsstandards verwendet, der sowohl gegen Angriffe von herkömmlichen als auch von Quantencomputern geschützt ist.

Viele Cybersicherheitsexperten glauben, dass Quantencomputer, sobald sie im großen Maßstab eingesetzt werden, aufgrund ihrer schieren Rechenleistung heute gängige Verschlüsselungs-Challenges in einem Bruchteil der Zeit „lösen“ können, die bisher dafür nötig ist. Dadurch könnten die heutigen Public-Key-Verschlüsselungssysteme geknackt und Daten, digitale Signaturen und Geräte angreifbar werden. Dies führt zu erheblichen Sicherheitsrisiken für Online-Geräte und -Daten, einschließlich Finanztransaktionen, kritischer Infrastrukturen, Over-the-Air-Updates und mehr.

Um dem entgegenzuwirken, kündigt NIST eine Standardisierung von PQC-Algorithmen an. Diese würde der Industrie den Umstieg auf neue, sichere Systeme bereits ermöglichen, bevor die Gefahr durch Quantencomputer zu groß wird. Der gitterbasierte Kryptographie-Algorithmus Crystals-Kyber, der von NXP zusammen mit Sicherheitsexperten von IBM eingereicht wurde, wird als Grundlage für diesen neuen Standard dienen. Der Classic-McEliece-Algorithmus, ein weiterer von NXP mitverfasster Algorithmus, der zur Familie der codebasierten Kryptographie gehört, geht in die nächste Analyserunde und wird für die Standardisierung in Betracht gezogen.

„Da die Welt immer vernetzter und datengesteuerter wird, ist die Sicherheit von Daten und Geräten von entscheidender Bedeutung, auch gegenüber Angriffen von Quantencomputern“, sagt Joppe Bos, Senior Principal Cryptographer bei NXP. „Während NIST die Entwicklung eines neuen Post-Quantum-Standards vorantreibt, wird NXP sein fundiertes Wissen im Bereich der Sicherheit und insbesondere seine Expertise auf dem Gebiet der Algorithmen einbringen, um unsere Produkte für eine Post-Quantum-Zukunft zu stärken. Unser Ziel ist es, einen Beitrag zum gemeinsamen Standard zu leisten, damit unsere Kunden ihre eigenen Produkte langfristig absichern können.“

„Die Sicherheitsexperten von IBM, NXP und Arm® haben zusammen mit ihren akademischen Partnern (ENS, RAB, CWI und RUB) einen branchenführenden Beitrag geschaffen. Er wird die Art und Weise, wie wir über Verschlüsselung und Sicherheit denken, für die nächsten Jahrzehnte prägen“, sagt Michael Osborne, Principal Research Scientist Manager für Foundational Cryptography bei IBM. „Kyber ist nicht nur schneller als die derzeitigen Standards, sondern bietet unseren Kunden auch eine hohe Sicherheit, um Systeme und Daten zu schützen, während wir in das Quantenzeitalter eintreten.“

Für mehr Informationen über PQC besuchen Sie bitte nxp.com/PQC.

###

NXP Semiconductors
NXP Semiconductors N.V. (NASDAQ:NXPI) entwickelt Lösungen, die eine intelligentere, sicherere und nachhaltigere Welt schaffen. Als ein weltweiter Marktführer bei Lösungen für die sichere Kommunikation in Embedded-Applikationen treibt NXP Innovationen in den Anwendungsfeldern Automobiltechnik, Industrie & IoT, bei Mobilgeräten und Kommunikationsinfrastruktur voran. Das Unternehmen, welches auf eine geballte Erfahrung und Expertise von mehr als 60 Jahren bauen kann, beschäftigt ca. 31.000 Mitarbeiter in mehr als 30 Ländern und konnte 2021 einen Umsatz von US$11,06 Milliarden vermelden. Weitere Details unter nxp.com.

Für weitere Informationen kontaktieren Sie bitte:

Amerika & Europa
Phoebe Francis
Tel: +1 737-274-8177
E-mail: phoebe.francis@nxp.com

China/Asien
Ming Yue
Tel: +86 21 2205 2690
E-mail: ming.yue@nxp.com