Solving the Quantum Threat with Post-Quantum Cryptography on eFPGAs

K. Järvinen, M. Tommiska, *Xiphera Ltd.*

R. Grundler, *Flex Logix Technologies Inc.*

The quantum threat and post-quantum cryptography

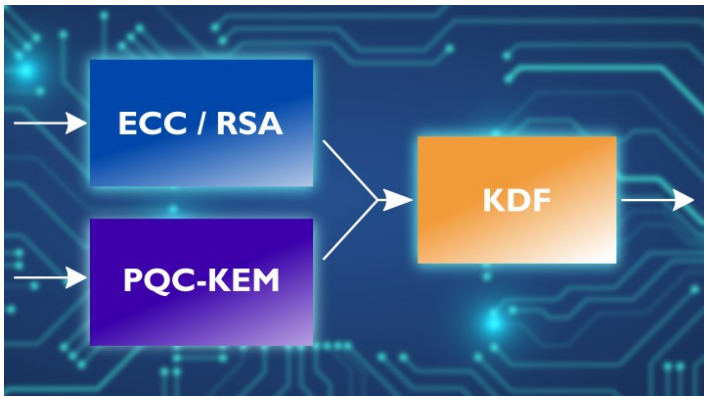
Advances in quantum computing technology threaten the security of current cryptosystems. Asymmetric cryptography algorithms that are used by modern security protocols for key exchange and digital signatures rely on the complexity of certain mathematical problems. Currently, the main problems used for asymmetric cryptography are integer factorization of RSA and elliptic curve discrete logarithm of the elliptic curve cryptography (ECC). Shor's algorithm is a quantum algorithm that can solve these problems if a large enough quantum computer is built. As a consequence, this would break the related cryptosystems and the basis of current computer and communication security. Although quantum computers of cryptographic significance do not exist today, many systems designed now will be in use for decades. It is also possible to record data today and break it in the future when powerful quantum computers will be available.

The international security community woke up to this quantum threat several years ago and developed ways to mitigate it. Post-quantum cryptography (PQC) are algorithms that run on traditional computers but are based on mathematical problems that cannot be solved efficiently with Shor's algorithm, or by any other known quantum computing algorithm. Unique solutions will be required to solve this complex problem and many people are researching it. In 2016, the National Institute of Standards and Technology (NIST) of the United States initiated a competition to find solutions to standardize PQC algorithms. After three rounds, the competition concluded in July 2022 with the publication of four winning algorithms that will be standardized: CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+. Kyber is a so-called Key Encapsulation Mechanism (KEM) that is used for key exchange and the rest are digital signature algorithms. NIST continues the competition with a fourth round to find even further advanced PQC algorithms for a more robust standard in the future. Although the algorithms to be standardized are now known, they may still be tweaked before even the draft standards are written. The final standards are expected to be published in a couple of years and may still change from what is known today.

System designers need to start shifting to PQC immediately, as many organizations and formal requirements mandate security systems to support PQC in the near future. The recent announcement by the National Security Agency (NSA) mandates certain US national systems to support PQC in 2025. These requirements, combined with the still changing PQC landscape, set very high needs for crypto agility: the ability to update and change cryptographic algorithms in deployed systems. There are some solutions being proposed.

Hybrid schemes

New is not equal to secure in cryptography since it takes time to verify trust in a new cryptography scheme. The scheme can be trusted only after it has been subject to years of cryptanalytic research without any identified weaknesses. Because PQC schemes are only a few years old and many are based on new types of mathematical problems, they cannot be fully trusted at this stage or even when the final standards are out. It is entirely possible that previously unknown weaknesses will be discovered and allow breaking them even with classical computers. Indeed, several of the schemes in the NIST competition have been broken, and some of them only at the very late stages of the competition: a third-round finalist algorithm Rainbow was broken in 2020 and SIKE was broken almost immediately after it was chosen for the fourth round in the summer of 2022. These attacks were very effective and allowed for practical attacks, even with a single laptop computer.



To mitigate the risks of a failure of the new PQC schemes, many authorities (e.g. French ANSSI and German BSI), researchers, and security professionals recommend using a hybrid mechanism. A hybrid mechanism combines a PQC scheme with a traditional scheme (ECC in most cases) so that the combination remains secure even if one of them fails under classical or quantum attacks.

Hybrid mechanisms will reduce both risks: the quantum threat and the possible failure of PQC. It is likely that hybrid mechanisms will be widely deployed and used for a long time. This sets high requirements for the implementation of secure systems, as they need to have secure and efficient implementations of both ECC and PQC. They must also be implemented in a crypto-agile manner that permits changes after deployment if some of the algorithms are upgraded or replaced. This is a challenge that reconfigurable computing can answer.

PQC on eFPGAs

The PQC algorithms will evolve over time but their complexity lend themselves to a hardware solution so calculations can be done efficiently in parallel. This uncertainty and complexity point to a unique solution: embedded FPGAs (eFPGAs.) eFPGAs are uniquely qualified for this application because they will provide the ability to change the PQC algorithms but yet provide the performance needed with power and cost savings over other alternatives.

The crypto agility requirement for PQC can be satisfied with eFPGA and provide other benefits to the system. If PQC is implemented on an eFPGA platform, then all forthcoming updates and algorithm modifications can be supported by reprogramming eFPGA. It is also possible to retro-fit PQC into systems that already have eFPGA included in the SoC (System on Chip). By adding reconfigurable computing to the SoC the system can save on power and cost yet still have high-performance encrypting.

Many existing SoC architectures have hardened cryptography modules that include support for a multitude of cryptography algorithms including ECC, but not PQC. Updating such modules to support PQC and hybrid mechanisms after deployment is very hard or even impossible and very expensive without eFPGA. Including cryptography modules with PQC support will be difficult and risky even in new projects in the future as they may not be available in the market at all or come with fixed parameter sets that are impossible to change if the algorithms get tweaked in the final stages of the PQC standardization process or even broken later. eFPGA permits complementing cryptography modules with PQC support that can be updated to accommodate any future changes.

eFPGA may be used also for implementing the entire hybrid mechanism in a resource efficient manner. The eFPGA can be first programmed to implement a PQC KEM and to compute the PQC shared secret, next to implement ECC and to compute the ECC shared secret, and finally programmed to implement the key derivation function that computes the final shared secret from the PQC and ECC shared secrets.

The eFPGA inside the SoC allows for other advantages besides being smaller and generating less heat. One of the problems facing cryptographers is the issue of export laws of various countries and the issue of sensitive information being provided to nefarious people who wish us harm. With the eFPGA inside the SoC, the PQC algorithms remain safe by programming after the SoC is back from manufacturing in a known safe location. The eFPGA binaries can be encrypted using PUF technology to further secure them in case the computing device is stolen or lost in the field.

The quantum threat is a problem that shows we need to not only protect data in the future when quantum computing is powerful enough but also protect data now so that malicious recordings that are stored for the future are not hacked. eFPGA provides a unique opportunity to create an SoC that can support the hybrid model now, and in the future the ability to make it stronger.

For more information, contact Xiphera at info@xiphera.com and Flex Logix at info@flex-logix.com