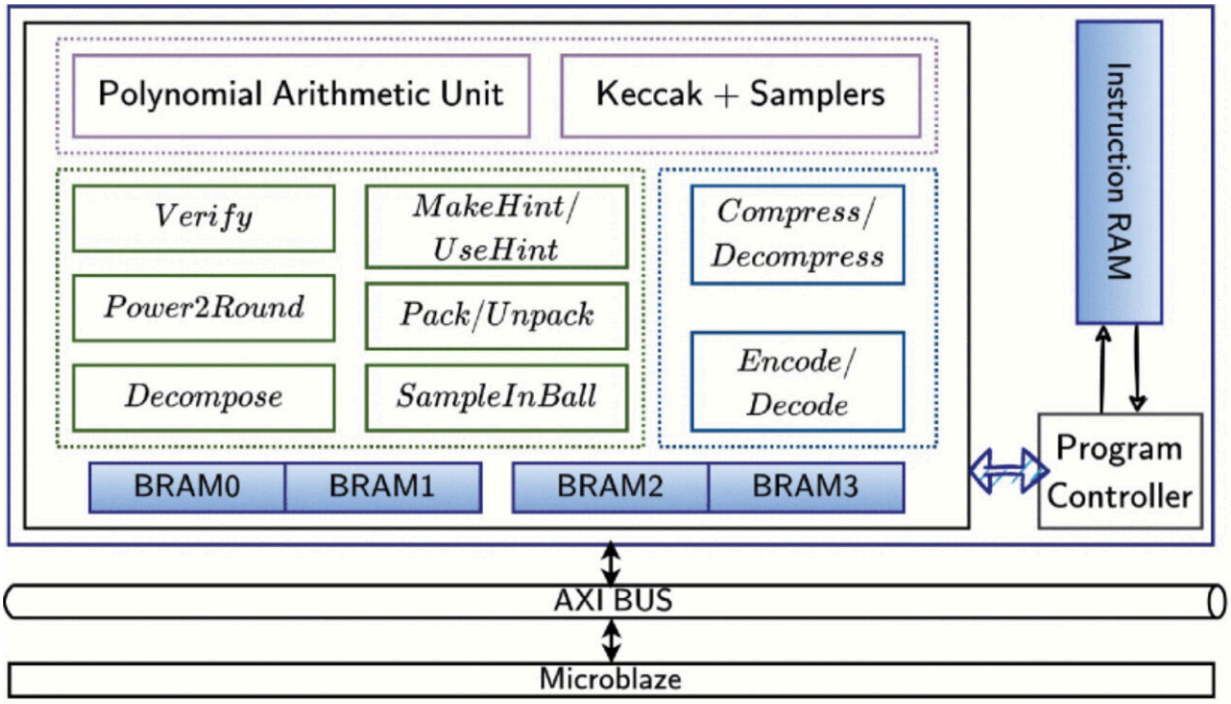
Research team develops hardware architecture for post-quantum cryptography

October 3 2024, by Falko Schoklitsch



The architecture of the KaLi cryptographic coprocessor. Credit: IAIK - TU Graz

Integrating post-quantum security algorithms into hardware has long been considered a challenge. But a research team at TU Graz has now developed hardware for NIST post-quantum cryptography standards with additional security measures for this purpose.

They are not yet a reality, but in the not-too-distant future, sophisticated, high-performance quantum computers will be available. They will revolutionize fields like artificial intelligence, financial modeling, drug development, weather forecasting, and traffic optimization, but they also pose a significant risk to cybersecurity.

A powerful quantum computer will break a subset of widely used cryptographic algorithms that are important in securing the digital world. This is why several quantum-safe, more commonly known as "post-quantum cryptography" (PQC) algorithms, are already being developed. Implementing them into hardware has proven difficult so far, though.

In the PQC-SRC project, a team led by Sujoy Sinha Roy from the Institute of Applied Information Processing (IAIK) and Communications at Graz University of Technology (TU Graz) has developed hardware for these PQC algorithms and implemented additional security measures. During the research, the team was also in contact with companies such as Intel and AMD.

The work is published in the journal *IEEE Transactions on Computers*.

Among the algorithms, those based on computational problems involving mathematical lattice structures are particularly promising. Solving these computational problems is considered an infeasible task even for quantum computers.

In the process of standardizing PQC, the American National Institute for Standards and Technology (NIST) selected one key encapsulation mechanism (KEM) algorithm, namely Kyber, and three digital signature algorithms, namely Dilithium, Falcon, and SPHINCS+, which was partly developed at IAIK, for standardization.

KEM algorithms enable communicating parties to agree on the same

encryption key securely, while digital signature algorithms allow a receiver to verify the authenticity of received messages.

Need for secure and efficient design

Following the publication of standardized PQC algorithms, organizations and industry are gearing up for a transition to quantum-safe cryptography. All devices need to switch from classical KEM and signature algorithms to quantum-safe PQC algorithms. It becomes imperative that the newly standardized PQC algorithms be realizable on a wide range of electronic devices.

There is an urgent need for secure and efficient design and implementation methodologies to enable a smooth transition to quantum-safe cryptography. Researchers of the Cryptographic Engineering team, led by Sujoy Sinha Roy, have been researching such methodologies, especially targeting low-resource electronic devices. The PQC-SRC project has resulted in the development of several new methodologies.

Development of hardware-based coprocessor for standardized PQC

One research result is the construction of a unified cryptographic coprocessor named KaLi, which supports both Kyber KEM and Dilithium digital signature algorithms. Such a unified design is essential in real-life secure communication protocols, such as the widely used Transport Layer Security (TLS), where both KEM and signature operations are performed.

One main research challenge was how to make the unified design very compact. The new PQC algorithms require much larger memory and processing units to store and process the keys compared to the present-

day ones. If the design is not compact, a lot of low-resource computers used in IOT, and smart-card applications will be rendered inoperable.

Another important aspect is the agility or flexibility of architecture—minor changes to the cryptographic algorithms due to potential future threats can be accepted without replacing the hardware resources.

Besides efficiency and compactness, a cryptographic implementation's physical security is important. Although the mathematics behind a cryptographic algorithm may resist known mathematical attacks, the physics of a computing device might leak sensitive information in the form of variations in heat, radiation or energy consumption.

An attacker can try to guess what is happening within an electronic device using an antenna. The researchers investigated techniques to make cryptographic implementations of emerging PQC algorithms resistant to such attacks. They invented a data randomization technique named "Kavach."

The technique optimizes the computation overhead, taking special properties of numbers used in the polynomial operations of PQC algorithms. The results will help cryptographers construct PQC KEM and signature algorithms that are more friendly to countermeasures against physics-based attacks.

Important step for companies and organizations

"We have seen great leaps in the field of quantum processors over the past five years," says Sujoy Sinha Roy.

"When powerful quantum computers are fully developed, they will be able to break encryptions in a few seconds, for which conventional

computers would take years. This would be dangerous for banking transactions, state defense systems and other things. This is often referred to as the quantum apocalypse and we want to prevent it.

"As companies and organizations prepare to move to post-quantum cryptography, our research findings provide an important step towards this transition."

More information: Aikata Aikata et al, A Unified Cryptoprocessor for Lattice-Based Signature and Key-Exchange, *IEEE Transactions on Computers* (2022). DOI: 10.1109/TC.2022.3215064

Provided by Graz University of Technology