Postquantum cryptographic schemes in cloud computing services

Gina Gallegos-García

Instituto Politécnico Nacional (IPN), Mexico

As emerging technologies increase, the need to maintain user privacy without compromising the utility that cloud services provide becomes critical. This, coupled with the arrival of quantum computing, has caused modern public key cryptographic schemes used today to become insecure. Consequently, in 2016, the NIST began a standardization process of new cryptographic schemes and algorithms which must be secure against attacks mount from quantum computers. In August 2024, three schemes were standardized because of the third round and in March 2025 one algorithm was selected to be standardized because of the fourth round. All these schemes and algorithms, better known as post-quantum or quantum resistant, have emerged as a promising solution in cloud computing service scenarios. In this talk, we will discuss the impact of post-quantum schemes currently used in that kind of scenarios, and we also give future directions in this sense.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T03