Report – Security in a Post- Quantum World

Leads:
S. Bai (Florida Atlantic University),
J.-F. Biasse (University of South Florida),
E. Persichetti (Florida Atlantic University)

In this breakout session, we sought to encourage discussion about topics connected to cybersecurity in a world in which, looming on the horizon, is the ever-growing threat of general purpose quantum computers. To begin the session, we played a short 10-minute introductory video, produced by J.-F. Biasse at USF. The purpose of this video was to describe the topic at a high level, including challenges and possible future developments, to make sure all participants started the discussion from a common standpoint. After this, we proceeded with a quick roll call, to get the participants to introduce themselves and specify their background, and possible angles to contribute to the discussion.

The discussion started with a summary of the current state of the art. The notion emerged that current Public-Key Cryptography (PKC) should be regarded as a “first generation” toolbox, which has served us well over the years, but is now due to be replaced. Indeed, NIST has started this process back in 2017, by promoting the first standardization competition for Post-Quantum Cryptography (PQC). The emphasis here is on “first”, as, in fact, even this effort from NIST has to be regarded merely as a first step towards transitioning to quantum-safe algorithms; this was one of the topics which were discussed as well. It was pointed out that, while the NIST competition has now reached a 3rd round, this is far from final; some schemes are now likely to be standardized, yet more analysis will follow in a 4th round (for alternate finalists), as well as new rounds (for example, a re-opening dedicated exclusively to non-lattice signature schemes).

The topic of lattice-based cryptography, in fact, was another major line of discussion in this breakout group. It was recognized that the overwhelming majority of NIST successful candidates belong to this area (3 out of 4 KEMS and 2 out of 3 signatures). The matter of cryptanalysis was then brought up. On one hand, the cryptanalysis of lattice-based schemes needs to really step up, to reach the level of maturity provided, for instance, by code-based schemes such as Classic McEliece (one of the schemes most likely to be among the first standards). On the other hand, a wider cryptanalysis activity is required to correctly analyze the landscape beyond lattices, as demonstrated by the recent, devastating attack on multivariate signature scheme Rainbow. Both of these cryptanalytic efforts are often merely a matter of manpower, and channeling research energies into the task.

A very important type of attack analysis is the one that is devoted to attacks of physical nature, i.e. those that exploit side-channels such as timing, power analysis, fault injection etc. As a consequence, it was suggested that a robust side-channel analysis is necessary to properly evaluate post-quantum schemes.

A second, separate line of discussion verted about performance, in general. For example, hardware implementations are currently only at a very early stage, and need heavy optimization. Also, participants discussed the idea of correctly defining the tradeoff spectrum between security and performance. Then, PQC schemes could be developed by keeping this aspect in mind, i.e. could be tailored to specific security requirements, or applications (lightweight, Internet-of-Things, etc.) . In addition to basic functionalities, this would also drive the development of schemes that satisfy advanced needs, such as identity-based signatures, homomorphic encryption, and similar. Other important aspects that were discussed are regarding the deployment of PQC. This includes “hybrid” schemes, that combine pre-quantum schemes (ECC, RSA) with PQC schemes, and could serve as a “bridge”, to facilitate the transition; as well as the notion of “crypto agility”, which would allow to interchange different PQC schemes, or their parameters, depending on the purpose and requirements of the intended application.

Finally, a portion of the discussion was centered on quantum computing itself, and how this meets PQC. Indeed, to properly analyze the security of PQC schemes, it is necessary to investigate quantum algorithms in the first place. This encompasses several different areas, among which the main ones that were discussed are: quantum resource estimation of existing algorithms; new or improved quantum attacks (that go above and beyond Shor’s or Grover’s, for example); actual implementations of quantum attacks, even if just as a proof of concept; and the possibility of performing a combination of quantum and classical techniques, i.e. some “hybrid” attacks. Research on the above topics would also help revisit the current notions of security and defining them in light of the new quantum adversaries capabilities.