Parcours Recherche – Telecom Paris

Supervisor: *Sébastien Canard*

Contact: *sebastien.canard@telecom-paris.fr, bureau 4C59*

Domain: *Cybersecurity, cryptography*

Keywords: *Authentication, post-quantum, IoT*

Post-quantum authentication for the Internet of Things

Context.

In the context of the Internet of Things (IoT), the security of communications and data is of crucial importance, particularly as some objects are not powerful enough to perform complex calculations. However, such security is only possible if an appropriate authentication mechanism has been put in place to ensure that an entity is indeed the one expected. However, the advent of quantum computers will challenge traditional authentication mechanisms, exposing IoT systems to potential security vulnerabilities. To guarantee the confidentiality and integrity of exchanges in the IoT, it is becoming imperative to develop authentication solutions that are resistant to quantum computers and dedicated to low-power objects.

Objectives.

The main objective of the research project will be to work on a new post-quantum authentication system between, on the one hand, a connected object with little computing power and, on the other hand, a more powerful verification terminal. To achieve this, there are currently various approaches that we can summarise as follows.

- Using an encryption-based mechanism. By using an encryption scheme with the right level of security (IND-CCA for indistinguishability against selected ciphertext attacks) and resistance to quantum computers (such as Kyber), we achieve the desired result.
- Using a hybrid mechanism that relies on a weaker but more efficient version of Kyber (IND-CPA for indistinguishability against chosen plaintext attacks) and additional exchanges, to achieve the same result (see https://link.springer.com/chapter/10.1007/978-3-642-14992-4_11).

In this study, we propose an alternative approach, based on the SPAKE hybrid mechanism. Since it requires a one-way encryption scheme in the face of chosen ciphertext attacks (OW-CCA), the hope is that it will be more effective. However, SPAKE is based on a variant of RSA, which is not secure against quantum computers. We therefore need to find a post-quantum encryption scheme that is OW-CCA to be able to apply it (as we saw earlier, Kyber is IND-CPA or IND-CCA depending on the variant), and then compare the result obtained with the other approaches. To do this, we propose to study the following article: https://link.springer.com/chapter/10.1007/978-3-642-14992-4_11.