Symmetric cryptanalysis: from primitives to modes

Rachelle Heim Boissier*[1]

[1]Université catholique de Louvain (UCLouvain) – Belgique

Résumé

Cryptology is a fundamental science for the protection of information systems. In a nutshell, it enables secure communication between two parties over an unreliable channel. In this presentation, we will primarily discuss symmetric algorithms, which base their security on a secret key known only to the two parties. In practice, these algorithms require both parties to first share the secret key, which can be done thanks to asymmetric or public-key cryptography. Whilst public-key cryptology offers many functionalities beyond key exchange, symmetric schemes are often more efficient. As a result, a hybrid approach combining both types of cryptography is used in most contexts.

Cryptology, and in particular symmetric cryptology, relies on building blocks called primitives used within modes of operation to build more complex algorithms. To guarantee security, a first approach, provable security, consists in proving that a cryptosystem is secure under some assumptions, which are typically made on the underlying primitive. However, for the vast majority of primitives, the cryptographic community does not know how to guarantee the veracity of these assumptions. We thus rely on a complementary rationale: if the cryptographic community makes a significant effort to break a cryptosystem and fails to do so, then the cryptosystem is most-likely secure. The effort made to break a cryptosystem is called cryptanalysis and is the central topic of my PhD. In this presentation, I will present two families of contributions to cryptanalysis.

We will first start by discussing primitive cryptanalysis, looking at one of the most classical families of attacks, differential cryptanalysis. In particular, I will focus on the key recovery step, and present our dedicated tool, KYRYDI. We will then move on to mode cryptanalysis, which offers a complementary perspective to that of provable security. We will present generic attacks on duplex-based authenticated encryption modes, and show how these can be improved using a new combinatorial tool: the so-called exceptional functions.

*Intervenant