Masking S-Boxes in prime fields

Noémie Akpaki*[1,2]

[1]Thales SIX GTS France – Université Paris VIII Vincennes-Saint Denis – France
[2]Université Paris 8 - Département de Mathématiques – Laboratoire Analyse, Géométrie et Applications, LAGA, CNRS, UMR 7539, F-93430, Villetaneuse, France. – France

Abstract

A widely used countermeasure against side-channel attacks is masking.
While masking in binary fields exhibits reduced security in low-noise scenarios, masking in prime fields has been shown to provide stronger protections, both in low-noise settings and more generally.
In this context, masked implementations of symmetric-key algorithms defined over prime fields have been proposed in the literature. They achieve higher side-channel security than some traditional masked implementations of block ciphers while retaining competitive computational efficiency.

To analyse the security of masking schemes, several leakage models exist.
The masked version of the recently proposed prime-field ciphers are proven secure in the probing model.
However, the random probing model provides a more realistic description of leakage.
This work aims to study how we can obtain secure implementations of prime ciphers in the random probing model.

In addition, all the proposed constructions so far rely on Mersenne primes, mainly because they allow efficient implementations. This work focuses on studying

*Speaker

other prime fields to see whether masked implementations in the associated fields could offer better side-channel security.

Collaboration with Sonia Belaïd and Gaëtan Cassiers