Some problems on Boolean functions posed by side channel attacks

Claude Carlet,
Universities of Paris 8, France and Bergen, Norway.

E-mail: claude.carlet@gmail.com

The implementation of cryptographic algorithms in devices like smart cards, FPGA or ASIC leaks information on the secret data, leading to very efficient *side channel attacks* (SCA) allowing recovering the key with few plaintext-ciphertext pairs in a few seconds if no counter-measure is included in the algorithm. Counter-measures are costly in terms of running time and of memory when they need to resist higher order side channel attacks and there is then a need for minimizing the cost.

The most commonly used counter-measure is a secret-sharing method called *masking*. In this talk, we will address how single-output and multiple-output (i.e. vectorial) Boolean functions play roles in this context.

We shall recall how nonzero correlation immune (CI) functions (keeping the same output distribution when some number of input variables are fixed) play a role, for reducing the overhead due to masking, in two counter-measures against SCA, called *rotating S-box masking* and *leakage squeezing*. In the first method, CI functions need to have low Hamming weights, which poses the question of minimizing the weights of nonzero CI functions. The second method achieves with one mask the same protection as with several ones; it uses bijective vectorial functions, applied to the mask, whose graph indicators need to be correlation immune of highest possible order.

When considering lightweight cryptography, the extra cost due to masking is even more problematic. However, some options are possible like using substitution boxes (S-boxes) that are easier to mask or using S-boxes that possess higher inherent side-channel resilience. We shall see properties of S-boxes allowing them to be more resilient against side-channel attacks, observe the difficulties this poses with respect to the other cryptographic features of the S-boxes, and see the example of the PICARO cryptosystem.

Finally, we will see how minimizing the *masking complexity* of each S-box, that is, the minimum number of nonlinear multiplications needed to implement it, which is an important factor of complexity in masking. In particular, we shall see the Coron-Roy-Vivek method and the CPRR method, based on two different S-box algebraic decomposition principles.