Automatic derivation of optimal side-channel attacks rounded at a given order

Submission to WRAC'H

Abstract

Masking countermeasure against side-channel attacks consists in randomly sharing sensitive variables. Therefore, such protections consume a lot of randomness (which must be balanced, independent, etc.). Today, many masking protections are constructively designed to be dth-order secure. The parameter $d > 0$ is a design security metric whereby each tuple of strictly less than d shares is independent from the clear sensitive variables.

For masking schemes such as Ishai-Sahai-Wagner (CRYPTO 2003) or Rivain-Prouff (CHES 2010), the security proof is based on composability: it is possible to design widgets for basic operations, e.g., field addition and multiplication, forming a universal set. Subsequently, combining them allows to build arbitrary computations. Reuse of variables shall be dealt with cautiously. In practice, reused variables usually benefit from refresh.

There is one venue of research which consists in checking a complete implementation (Barthe et al., EUROCRYPT 2015). Since the combinatorics of verification is large, the proof employs heuristics taylored for the masking scheme.

Now, in practice, the attacker must perform a dth-order attack. But the attacker will maximize its advantage, and so she is not expected to be satisfied by one combination of d shares. Here we face a paradox: the larger the order d, the more possible combinations, hence it is relevant to study whether in practice, the security level in terms of data complexity (number of traces to recover the key) is still increasing with parameter d.

In this paper, we show how to compute optimal attacks, with tradeoffs regarding data and computational complexities (as in Bruneau et al., J. of Cryptology 2018). We aim at analyzing real-world implementations, irrespective of the source language they are coded in. Moreover, we want to consider optimized code. For this reason, we analyze the intermediate representation generated by a compiler, and generate the formula for the multivariate high-order distinguisher after having simplified the terms.

Results show that monovariate high-order attacks are underestimating the security level by orders of magnitude, especially when the noise level is high.

Key word: Side-channel analysis, masking protection, compositional countermeasure, formal analysis, optimal side-channel attacks, Taylor expansion of distinguishers.