*ASCA: Comparing Horizontal Side-Channel Attacks

Vincent Grosso

Abstract

Side-channel attacks exploit information leaked during the execution of a cryptographic implementation. All operations leak information about the data they manipulate. Hence, a side-channel attack generally consists in attacking one operation that manipulates a part of a secret and a public data. Since the amount of information leaked is small compared to the size of the secret, an attacker generally measures multiple calls of the targeted operation with different public data.

In this scenario, most of the computations performed by the cryptographic implementation are not exploited. To overcome this problem, horizontal attacks have been proposed. The different propositions were proposed to deal with measurement error. However, applying such attacks on microcontrollers with large registers was an open problem.

This presentation will compare different horizontal attacks, algebraic side-channel attacks, tolerant algebraic side-channel attacks, and soft analytical side-channel attacks. We discuss the advantages and inconveniences of each method according to the attributes of the target device, depending on noise level and register size. We develop a technique to apply algebraic side-channel attacks to microcontrollers with large registers (≥ 8).