ETSVL002- 2017- Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications

Abstract

In this work we focus on Power Analysis Attacks (PAAs) which exploit the dependence of the static current of sub-50 nm CMOS integrated circuits on the internally processed data. Spice simulations of static power have been carried out to show that the coefficient of variation of nanometer logic gates is increasing with the scaling of CMOS technology. We demonstrate that it is possible to recover the secret key of a cryptographic core by exploiting this data dependence by means of different statistical distinguishers. For the first time in the literature we formulate the Attack Exploiting Static Power (AESP) as a univariate attack by using the mutual information approach to quantify the information that leaks through the static power side channel independently from the adopted leakage model. This analysis shows that countermeasures conceived to protect cryptographic hardware from attacks based on dynamic power consumption (e.g., WDDL, MDPL, SABL) still exhibit a leakage through the static power side channel. Finally, we show that the Time Enclosed Logic (TEL) concept does not leak information through the static power and is suitable to be used as a countermeasure against both attacks exploiting dynamic power and attacks exploiting static power.