Towards a Flexible, Opensource BOard for Side-channel analysis (FOBOS)

Rajesh Velegalati and Jens-Peter Kaps

Abstract

Side-channel analysis attacks pose a growing threat to implementations of cryptographic algorithms implemented in software as well as in hardware. Current standard side-channel evaluation boards with Field Programmable Gate Arrays (FPGAs), that allow for exploring the vulnerability of cryptographic implementations on FPGAs, are expensive and available only for a few FPGA devices. Furthermore, a complete open source software package that includes drivers that run test cases on the board, control the measurement equipment, and contain several side-channel analysis techniques is not readily available. Each user has to assemble their own setup based on software packages from multiple sources, written in multiple languages and write parts themselves. Additionally, this complexity and cost makes it very difficult, if not impossible, to educate students on side-channel analysis through hands-on laboratory exercises. We introduced FOBOS, an open-source framework for conducting side-channel attacks on FPGAs, at the work in progress session of COSADE 2012, and it was met with a lot of interest from universities and research groups. We expect to release the first version this Summer. It will feature support for multiple FPGA devices and include all necessary software to run differential power analysis attacks, which are the most prominent kind of side-channel attacks. Furthermore, FOBOS integrates with the low cost OpenADC board to form a complete low-cost SCA solution for less than $200, which will be ideal for educational use. The components of FOBOS are build in a modular fashion so that it can easily be adapted for new FPGA boards, oscilloscopes, and attack techniques. Our next steps are integrating support for fault analysis, including circuitry to cause power and clock faults, and adding new targets, such as ASICs and smart cards.