Flexible, Opensource workBench fOr Side-channel analysis (FOBOS)

Abubakr Abdulgadir, William Diehl, Rajesh Velegalati, and Jens-Peter Kaps

Cryptographic Engineering Research Group
George Mason University, Fairfax, VA, http://cryptography.gmu.edu

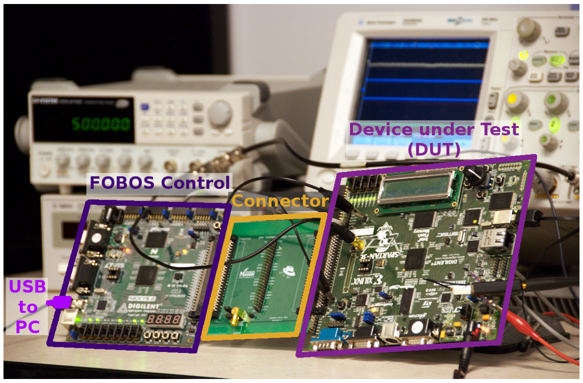
Side-channel analysis attacks pose a grave threat to implementations of cryptographic Algorithms implemented in software as well as in hardware. We started developing FOBOS in 2012 [6, 7, 5] in order to evaluate hardware implementations on Field Programmable Gate Arrays (FPGAs) as integrated evaluation environments were very costly or available only for a few FPGA devices. FOBOS, an "acquisition to analysis" solution, includes all necessary software to control the device under test (attack) (DUT), trigger the oscilloscope, obtain the measurements and analyze them using several power analysis techniques. 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.

At HOST we want to announce our latest release of FOBOS which has significant enhancements over the last release announced at HOST 2016. The most prominent one is the capability of performing Test Vector Leakage Assessment (TVLA) based on Welche's t-test. This is an industry-standard method to evaluate the effectiveness of side-channel countermeasures. This assessment is especially valuable in conjunction with our new profiler which ties each t-test evaluation to the state of the cryptographic function under evaluation. This allows a user to pin-point during which operation information is leaking. Furthermore, FOBOS is now compatible with the CAESAR API, enabling evaluation of implementations on FPGAs of candidates of the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) without changes to FOBOS.

FOBOS results have appeared in four peer-reviewed conference papers and presentations over the last year. This includes the use of FOBOS to verify the effectiveness of countermeasures against DPA in lightweight block ciphers [2], a custom-designed side channel resistant soft core microprocessor [3], and CAESAR Round 3-candidate authenticated ciphers [1]. FOBOS, when combined with the power-sensing capabilities of the eXtended eXternal Benchmarking eXtension (XXBX), has also been used for precise power measurement and computation of energy consumption for block ciphers, authenticated ciphers, cryptographic software, and a hardware accelerator for Pairing-based Cryptography (PBC) [2, 3, 1, 4].

Hardware Demonstration at HOST 2018

We intend to present a complete FOBOS setup to demonstrate TVLA on protected and unprotected CAESAR candidates. The demonstration will include a short overview of the configuration files and the data acquisition using an oscilloscope. We will walk through the analysis of the obtained power waveforms, and identify, using TVLA results and our profiler, the states of the cryptographic algorithm which are leaking information. Knowing which function that the implementation is performing in a given clock cycle allows us to determine if the leaked information is exploitable by a power analysis attack.



Below are examples of viewable products that will be seen by visitors of our demonstration.

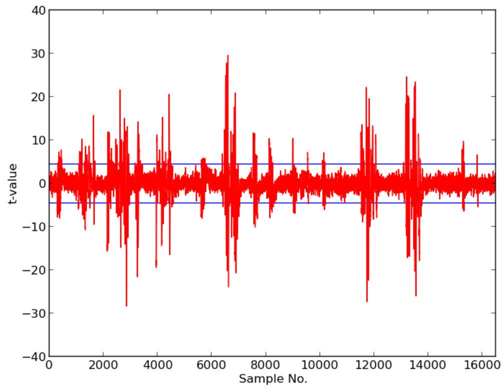


Fig. 1. Failing t-test on unprotected implementation of CLOC-AES

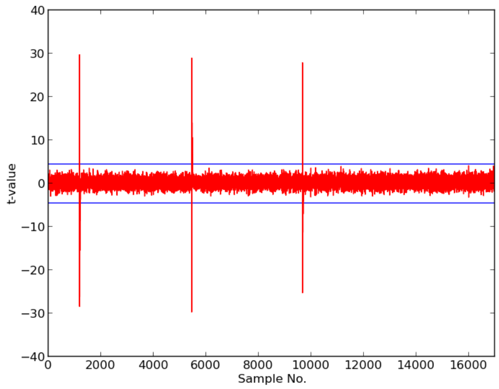


Fig. 2. 3-share Threshold Implementation (TI) of CLOC-AES which passes t-test, except for a data dependent branch condition

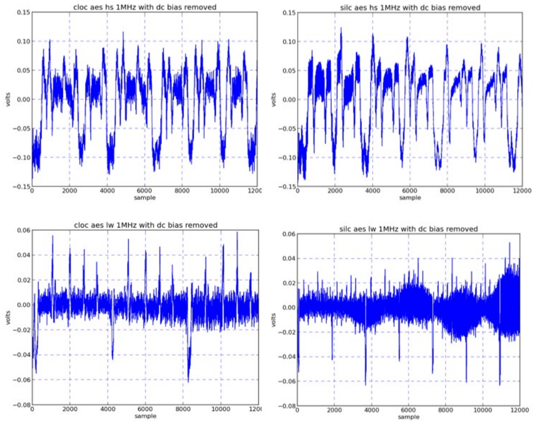


Fig. 3. Power waveforms of high-speed & lightweight implementations of SILC-AES & CLOC-AES

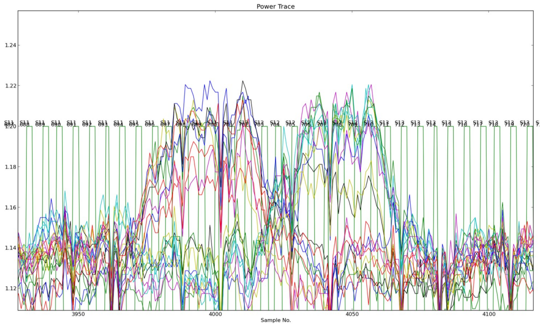


Fig. 4. "Profiler," which correlates sample to precise cipher operation, and indicates possible SPA vulnerability for different test vectors

References

1. Diehl, W., Abdulgadir, A., Farahmand, F., Kaps, J.P., Gaj, K.: Comparison of cost of protection against differential power analysis of selected authenticated ciphers. In: IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (Apr 2018), to appear
2. Diehl, W., Abdulgadir, A., Kaps, J.P., Gaj, K.: Comparing the cost of protecting selected lightweight block ciphers against differential power analysis in low-cost FPGAs. In: International Conference on Field Programmable Technology (FPT 2017) (Dec 2017)
3. Diehl, W., Abdulgadir, A., Kaps, J.P., Gaj, K.: Side-channel resistant soft core processor for lightweight block ciphers. In: International Conference on Reconfigurable Computing and FPGAs (ReConFig) (Dec 2017)
4. Salman, A., Diehl, W., Kaps, J.P.: A light-weight hardware/software co-design for pairing-based cryptography with low power and energy consumption. In: International Conference on Field Programmable Technology (FPT 2017) (Dec 2017)
5. Velegalati, R.: Developing an Integrated Environment for Detecting and Mitigating Side-channel and Fault attacks on Hardware Platforms. Ph.d. dissertation, ECE Department, George Mason University, Fairfax, Virginia, USA (Feb 2015)
6. Velegalati, R., Kaps, J.P.: Introducing FOBOS: Flexible Open-source BOard for Side-channel analysis. Work in Progress (WiP), Third International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012 (May 2012)
7. Velegalati, R., Kaps, J.P.: Towards a Flexible, Opensource BOard for Side-channel analysis (FOBOS). Cryptographic architectures embedded in reconfigurable devices, CRYPTARCHI 2013 (June 2013)