Documentation of Xoodyak_TI_first_order (v0.1.0)

Shuohang Peng Shuying Yin Cankun Zhao

April 18, 2022

1. Protection Method
   (a) Name of the applied countermeasure: **Threshold Implementation (TI).**
   (b) Corresponding primary reference describing this countermeasure (when applied to an arbitrary cryptographic algorithm): **Primary reference about TI is the paper by Nikova et al. [NRR06]. Technique about resharing is introduced in [BDN^{+}13].**

2. Results of the Preliminary Security Evaluation
   (a) Attack/leakage assessment type: **Fixed vs. random t-test at first order [GGR11] and second order [SM15].**
   (b) Number of traces used: **One million traces for the protected and 10,000 for the unprotected implementation.**
   (c) Experimental setup
      i. Measurement platform and device-under-evaluation: **Design-under-evaluation was instantiated on the Xilinx Spartan-6 (XC6SLX75-2CSG484C) FPGA on SAKURA-G board. The other Xilinx Spartan-6 (XC6SLX9-2CSG225C) FPGA on SAKURA-G was used for control.**
      ii. Description of measurements: **The design-under-evaluation power consumption is measured at the output of the SAKURA-G's on-board amplifier (AD8000YRDZ), that amplifies the voltage drop across the on-board 1 Ω shunt resistor.**
      iii. Usage of bandwidth limiters, filters, amplifiers, etc. and their specification: **N/A.**
      iv. Frequency of operation: **3 MHz.**
      v. Oscilloscope and its major characteristics: **Teledyne LeCroy WaveRunner 8404M with 4 GHz bandwidth was used to collect traces.**
      vi. Sampling frequency and resolution: **Sampling rate of 100 MS/s and 8-bit sample resolution were used.**
      vii. Are sampling clock and design-under-evaluation clock synchronized? **No.**
   (d) Attack/leakage assessment characteristics
      i. Data inputs and performed operations: **Tested operation is the Xoodoo permutation with 12 rounds. Input test vectors are initially shared on the control FPGA. The data input for the fixed data-set is chosen to make the state bits after the third round all zero.**
      ii. Source of random and pseudorandom inputs: **Trivium-based DRBG.**
      iii. Trigger location relative to the execution start time of the algorithm: **Scope trigger is set at the beginning of the algorithm execution.**
      iv. Time required to collect data for a given attack/leakage assessment: **Unfinished.**
      v. Total time of the attack/assessment: **Unfinished.**
      vi. Total size of all traces (if stored): **Unfinished.**
      vii. Availability of raw measurement results: **Unfinished.**
   (e) Attack-specific characteristics
      i. Power model: **N/A.**
      ii. Attack point: **N/A.**

(f) Documentation of results

i. Graphs illustrating the obtained results: **Unfinished.**

ii. Attack scripts: **N/A.**

3. The handshake of random data input (rdi) is not actually working in this version of implementation, i.e., the rdi should always be valid to ensure correctness. This will be fixed soon in the next version, which will be uploaded to our Github repository.

References

[BDN+13] Begül Bilgin, Joan Daemen, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen, and Gilles Van Assche. Efficient and first-order DPA resistant implementations of keccak. In Aurélien Francillon and Pankaj Rohatgi, editors, *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*, volume 8419 of *Lecture Notes in Computer Science*, pages 187–199. Springer, 2013.

[GGR11] Josh Jaffe Gilbert Goodwill, Benjamin Jun and Pankaj Rohatgi. A testing methodology for side-channel resistance validation. In *NIST Non-Invasive Attack Testing Workshop*, Nara, Japan, 2011.

[NRR06] Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold implementations against side-channel attacks and glitches. In Peng Ning, Sihan Qing, and Ninghui Li, editors, *ICICS 06*, volume 4307 of *LNCS*, pages 529–545. Springer, Heidelberg, December 2006.

[SM15] Tobias Schneider and Amir Moradi. Leakage assessment methodology - A clear roadmap for side-channel evaluations. In Tim Güneysu and Helena Handschuh, editors, *CHES 2015*, volume 9293 of *LNCS*, pages 495–513. Springer, Heidelberg, September 2015.