HELLENIC REPUBLIC
UNIVERSITY OF THE PELOPONNESE

ELECTRICAL AND COMPUTER ENGINEERING DEPARTMENT

Megalou Alexandrou 1 str., Koukouli, Patras Greece

Paris Kitsos, Professor
Pnone.: 6944757238
Email: kitsos@uop.gr

Patras, 02-04-2024

Subject: Doctoral Thesis Review - Differential Power Analysis Countermeasures in Programmable Hardware, submitted by Stanislav Jeřábek

The thesis has been submitted to the Faculty of Information Technology, Czech Technical University in Prague in the Ph.D. study program Informatics.

1. **Up-to-dateness of the dissertation**

This dissertation thesis deals with the threat of side-channel attacks to all implementations of cryptographic algorithms, which is an extensively researched area. The author have secured AES and Serpent by countermeasures proposed for PRESENT cipher. The implementations have no leakage being evaluated by first-order Welch's t-test and have resisted second-order DPA/CPA attacks.
A very important is a new countermeasure proposal that is called Dummy Runds, and it is straight-forwardly applicable to any round-based cryptographic algorithm. Dummy Rounds are a hardware scheme for the implementation of shuffling when shuffling is a common countermeasure for software implementations.

2. **Formal structure and organization of the dissertation**

The submitted dissertation thesis is up to 60 pages, and it is organized in 5 chapters. The first chapter, introduction, is briefly describe the research problems and the results of the thesis. The second one, the necessary background and state-of -the-art about side channel analysis is explained. The main contribution of the candidate. In chapter 3, he have implemented countermeasures previously presented for PRESENT cipher for two of the Advanced Encryption Standard (AES) and Serpent. Leakage of our implementations was evaluated using the non-specific univariate first-order Welch's t-test. Next, in chapter 4, he present his novel hardware SCA countermeasure scheme called Dummy Rounds, which combines software hiding in time, shuffling and common hardware hiding of the circuitry power consumption. There are more parts of hardware design which are executed but their outputs are randomly used or not used for computation in every single clock cycle. So, the structure of the design is the same for every clock cycle and power consumption stays the same, while the algorithm flow changes, which is typically called Shuffling. Also an analysis of the

countermeasure and its leakage assessment are presented. Finally, chapter 5 conclude the thesis.

3. Completion of the dissertation objectives

I denote that the candidate clearly set the below goals:

- Implementation of two complex block ciphers using efficient countermeasures.
- Propose a new countermeasure that can offer competitive and many cases better results in security and overhead in implementation.
- Evaluation of countermeasures in hardware implementation

I feel that the objectives of the dissertation have been met.

4. Assessment of the methods used in the dissertation

The scientific methods, tools, and techniques employed adhere to the latest advancements. The focus of the thesis lies on standard symmetric cryptography algorithms. While AES serves as a common benchmark due to its establishment as a standard in 2002, its implementation costs and associated countermeasures prompt an examination of lightweight ciphers. Specifically, the limited number of rounds renders AES less suitable for dummy round countermeasures.

The designs are executed on the SAKURA-G board featuring the Xilinx Spartan 6 FPGA. SAKURA boards are prevalent in side-channel evaluations, designed to facilitate such analyses. They enable efficient utilization of external oscilloscopes crucial for assessing high-frequency implementations. Widely utilized in security labs, SAKURA boards ensure reproducible outcomes.

5. Evaluation of the results and contributions of the dissertation

The original and valuable contributions of this thesis extend to the domain of side-channel resistant implementation. By integrating masking with random decomposition and incorporating dummy rounds, the proposed approach offers efficient protection against side-channel attacks. Through leakage assessments, the authors validate the effectiveness of this countermeasure.

In addition, the number of published works by the authors serves as evidence of the efficiency of the proposed methods.

6. Remarks, objections, notes, and questions for the defense.

I believe that publishing some more research results in a journal, along with a comparative analysis of other countermeasures, would enhance its value significantly.

7. Recommendation Statement

The author of the dissertation proved the ability to conduct research and achieve scientific results. In accordance with par. 47, letter (4) of the Law Nr. 111/1998 (The Higher Education Act) I do recommend the thesis for the presentation and defense with the aim of receiving the Ph.D. degree.

Patras, 02/04/2024 Paraskevas (Paris) Kitsos