POSTER: Exploiting Dynamic Partial Reconfiguration for Improved Resistance Against Power Analysis Attacks on FPGAs

Ghada Dessouky
TU Darmstadt, Germany
ghada.dessouky@trust.cased.de

Ahmad-Reza Sadeghi
TU Darmstadt, Germany
ahmad.sadeghi@trust.cased.de

ABSTRACT

FPGA devices are increasingly deployed in wireless and heterogeneous networks in-field due to their re-programmable nature and high performance. Modern FPGA devices can have part of their logic partially reconfigured at run-time operation, which we propose to exploit to realize a general-purpose, flexible and reconfigurable DPA countermeasure that can be integrated into any FPGA-based system, irrespective of the cryptographic algorithm or implementation. We propose a real-time dynamic closed-loop on-chip noise generation countermeasure which consists of an on-chip power monitor coupled with a low-overhead Gaussian noise generator. The noise generator is reconfigured continuously to update its generated noise amplitude and variance so that is sufficiently hides the computation power consumption. Our scheme and its integration onto an SoC is presented as well as our proposal for evaluating its effectiveness and overhead.

1. INTRODUCTION AND MOTIVATION

Side-channel analysis (SCA) attacks constitute a major threat to the security of embedded devices and sensor nodes. Exploiting information leakage of a cryptographic implementation such as power consumption or timing or electromagnetic radiation can break the theoretic security of the implementation and enable successful key recovery rendering the cryptography useless. It is safe to assume that devices and sensors designed to function autonomously and in-field can easily get into the hands of an adversary, which motivates the necessity of hardening SCA attacks. Hence, this area of research has received plenty of attention and interest over the years, with an outcome of a wide range of potential countermeasures to defeat, or at least harden such SCA attacks.

We focus in this work on counteracting power analysis attacks on FPGA-based systems and network devices. Power analysis attacks are categorized as either simple power analysis (SPA) which is carried out by directly observing of a power trace, where instantaneous power consumption depends on a part and value of the secret key being processed. Differential power analysis (DPA) attacks, as first introduced in [2] rely on the relationship between the switching activities of transistors (due to bits flipping) of a cryptographic module and its instantaneous power consumption. These bit flips depend on the data being processed which may also depend on the secret cryptographic key which establishes a relationship between the secret key and the instantaneous power consumption. Such an attack is carried out by an adversary observing the target's power dissipation during the encryption by targeting an intermediate result of the computation which depends on both a portion of the message and a portion of the secret key. The adversary has to perform multiple measurements and statistical tests to determine if a correlation exists between the power consumption measured and the secret key. Therefore, in designing a secure cryptography module, it is necessary to incorporate countermeasures against SPA and DPA attacks. Such countermeasures aim at making an attack more difficult, and the effectiveness of a countermeasure is measured by the number of power trace samples required to establish a correlation between them and the secret key. In [4] and [3], these countermeasures are divided into mainly two groups: masking and hiding. Masking is usually at the algorithmic level and aims at randomizing the intermediate values processed by the cryptographic module. These have been successfully applied to several encryption algorithms such as in [7]. Hiding aims at removing the relation between the secret data and power consumption. Several hiding countermeasures exist such as power supply filtering, on-chip noise generation [1], wave dynamic differential logic (WDDL) [5] and symmetrical routing [6] and on-chip power regulation, insertion of dummy cycles, random order execution, and on-chip noise generation. In practice, no one countermeasure can guarantee the resistance of the cryptographic system against power attacks, and several countermeasures are often used simultaneously.

In this work, we focus our proposed DPA countermeasure to FPGA-based devices. The re-programmable nature, yet high performance, of FPGA devices have made them increasingly attractive as a choice of platform for embedded devices and an integral component of heterogeneous and wireless networks. Their increasingly wireless interfaces also enable their flexible in-field deployment and remote update and control. Being in-field however, they can easily fall in the hands of an adversary. Various countermeasures and hardening mechanisms against DPA attacks have been pro-

WiSec'16, July 18 - 20, 2016, Darmstadt, Germany

DOI: http://dx.doi.org/10.1145/2939918.2942426.

posed as described above. However, most of them require modifications to the cryptography module itself, its algorithm or implementation technology making them inflexible and specific to a certain cryptography implementations.

1.1 Contribution

We present a generic DPA countermeasure for FPGA-based devices that is both reconfigurable and re-usable with any cryptography module. We exploit the dynamic partial re-configurability of modern FPGA devices to implement a closed-loop real-time Gaussian noise generator which gets configured dynamically to vary the amplitude and variance of noise generated such that it is sufficient to hide the current power consumption. On-chip real-time power consumptions measurements are collected and used to guide the corresponding remote reconfiguration of the Gaussian noise generator. Our scheme is general-purpose, requires no modifications to the cryptographic algorithm or implementation that is to be secured, and therefore incurs no additional overhead on the performance of the cryptography, and aims to harden DPA attacks dynamically by continuously varying the noise amplitude and variance generated. Its estimated area overhead does not exceed 15% of the actual system area.

2. PROPOSED SCHEME

Our scheme extends one of the countermeasures proposed by Güneysu et al. in [1]. Toggling the input signal of a gate is the simplest and most effective way to impacts a gate's power consumption. Extending this to many gates can generate sufficiently high noise to hide the power consumption that is correlated with the current computation. A matrix of rows r and columns c of FPGA look-up tables (LUTs) configured as shift-registers can be implemented as simple Gaussian noise generator. The parameters r, c, the initial random bit patterns input to the matrix, as well as the configuration of the LUTs impact the amount of noise variance and amplitude generated. We propose to exploit the dynamic partial re-configurability of an FPGA device and allow that these parameters are dynamically reconfigured at run-time depending on continuous and real-time power measurements collected from an on-chip power monitor. This ring-oscillator based on-chip monitor measures the on-chip power consumption of the FPGA device at run-time and feeds these into a reconfiguration controller that determines the amplitude and variance of noise level required to sufficiently hide the current power consumption. It then fetches the corresponding bitstream from external memory and reconfigures the noise generator with the newly computed parameters r, c, the initial bit pattern input to the matrix, and the LUT configuration values. This real-time dynamic closed-loop on-chip noise generation countermeasure aims to continuously harden the DPA attack by generating noise amplitude and variance that is continuously changing depending on the current power consumption measured by the on-chip monitor.

3. SYSTEM ARCHITECTURE

Our power measurement and noise generation framework are integrated onto a typical System-on-Chip consisting of one or more cryptographic modules among others for prototyping. A system bus is usually used for the cores to communicate, whether security-critical or not. Along with the Gaussian noise generator matrix and on-chip monitor, a reconfiguration controller is required to receive power measurements from the monitor and compute the required noise amplitude and variance. It then fetches the nearest-match bitstream from external DRAM and reconfigure the Gaussian noise generator via the Internal Configuration Access Port (ICAP) with this bitstream.

4. IMPLEMENTATION AND EVALUATION

We integrate our countermeasure core into an open-core SoC, such as Amber or Sparc-V8 Leon and implement our SoC onto a Xilinx Virtex-7 FPGA board for prototyping our countermeasure and evaluating its effectiveness in resisting DPA attacks and the area and power costs incurred. An oscilloscope operating at a sampling rate of at least 2.5 GS/s and a bandwidth of at least 500 MHz is used to collect the power measurements in order to assess the effectiveness of our countermeasure.

5. CONCLUSIONS

We present a countermeasure against side-channel DPA attacks for FPGA-based embedded devices which exploits dynamic and partial logic reconfiguration of an FPGA. The parameters of an LUT-based Gaussian noise generator are updated continuously at run-time to match real-time on-chip power measurements collected to ensure that a sufficiently high and varying noise is constantly generated. This countermeasure is general-purpose, non-specific to any cryptography implementations, requires no inflexible modifications to the algorithm or its implementation and incurs no overhead on the performance of the cryptographic module.

6. REFERENCES

[1] T. Güneysu and A. Moradi. *CHES 2011 Proceedings*, chapter Generic Side-Channel Countermeasures for Reconfigurable Devices, pages 33–48. 2011.

[2] P. C. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 388–397. Springer-Verlag, 1999.

[3] S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Springer-Verlag New York, Inc., 2007.

[4] N. Mentens, B. Gierlichs, and I. Verbauwhede. *CHES 2008 Proceedings*, chapter Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration, pages 346–362. 2008.

[5] K. Tiri and I. Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Design, Automation and Test in Europe Conference and Exhibition, 2004. Proceedings*, volume 1, Feb 2004.

[6] P. Yu and P. Schaumont. Secure fpga circuits using controlled placement and routing. In *(CODES+ISSS), 2007 5th IEEE/ACM/IFIP International Conference on*, pages 45–50, Sept 2007.

[7] Z. Yuan, Y. Wang, J. Li, R. Li, and W. Zhao. Fpga based optimization for masked aes implementation. In *2011 IEEE 54th MWSCAS*, pages 1–4, Aug 2011.