On Reconfigurable Fabrics and Generic Side-channel Countermeasures

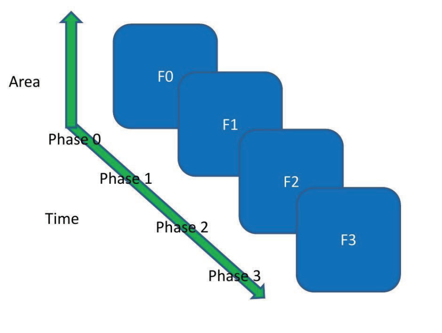
Robert Beat[1], Philipp Grabher[2], Dan Page[2], Stefan Tillich[2] and Marcin Wójcik[2]

[1] Silicon Basis Ltd.; [2] Cryptography Group, Department of Computer Science, University of Bristol

Motivation

The use of **field programmable devices in security-critical applications** is growing in popularity; in part, this can be attributed to their potential for balancing metrics such as efficiency and algorithm agility. However, in common with non-programmable alternatives, **physical attack techniques such as fault and power analysis** are a threat. Investigation of a family of next-generation field programmable devices, specifically those based on the concept of time sharing, can support the premise that extra, inherent flexibility in such devices can offer a range of possibilities for **low-overhead, generic countermeasures against physical attack**.

Time Multiplexed FPGA



The concept of a **Time Multiplexed Field Programmable Gate Array (TMFPGA)** is similar to a conventional FPGA wrt. reconfiguration, but resolves significant technological issues (notably logic density) that count against FPGAs in certain use-cases. At a high level, a TMFPGA can be viewed as time sharing resources (such as LUTs and routing blocks) in order to use them more efficiently. Although the underlying technology is less mature than for FPGAs, concrete implementations are emerging: an example is the **Tabula ABAX family of 3D Programmable Logic Devices (3PLD)** [1].

Soft Gate Array (SGA) [2] is an SRAM-based TMFPGA architecture that aims to overcome the remaining major limitations of TMFPGAs, namely dynamic and static power consumption. These advantages are well aligned to use-cases where physical attacks are most often an issue (embedded or mobile computing devices, for example).

Our work investigated whether the added flexibility afforded by an SGA can be translated into mechanisms for realising generic countermeasures, with particular focus on fault and power analysis, especially **Differential Power Analysis (DPA)** [3].

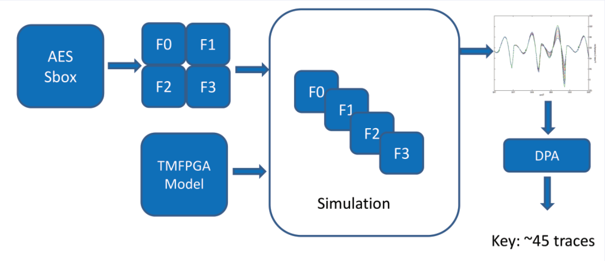
Bibliography

[1] "Tabula Spacetime Architecture", Tabula Inc., Tech. Rep., 2010. http://www.tabula.com/

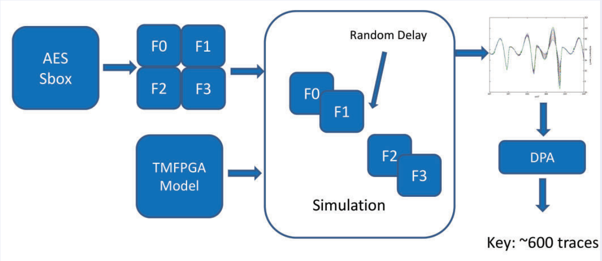
[2] R. Beat, "Programmable Logic Fabric", US Patent Application 2011/0031999 A1, February 2011.

[3] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer-Verlag, 2007.

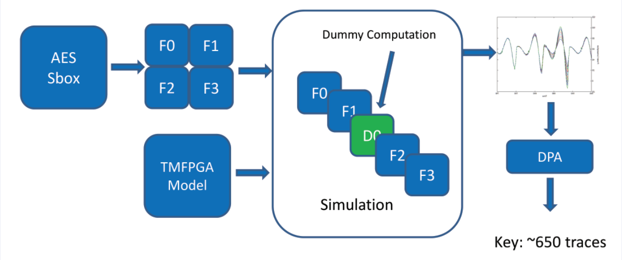
DPA Attack



DPA Countermeasure: Random Delays



DPA Countermeasure: Dummy Computations



Results

Implementation	ρ	Traces	Used	Execution time
		required	slices	(phases)
Vanilla AES S-box	0.66	45	20	12
Buffer randomisation	0.27	300	24	12
Phase skewing	0.19	600	20	13
Dummy computation	0.21	650	20	14

Future Work

1. Investigation of use of **a more accurate power model** to mitigate the use of simulation and improve relevance to physical test devices.
2. Study of **a full AES implementation**.
3. Investigation of **an SGA-specific tool-chain**, in particular whether it is feasible to realise the generic countermeasures in a fully automatic way.

University of BRISTOL