nano-tera.ch
swiss scientific initiative in health / security / environment systems

SEC-WEAR NTF

FNSNF

Building secure nodes for wearable sensor networks

Konstantinos Padarnitsas, Nikolaos Christianos, Francesco Regazzoni and Mariagiovanna Sami

ALaRi Institute - University of Lugano

Motivation

Body area sensor networks will pervade our life collecting a large amount of sensitive data

Data stored and transmitted by wireless body sensor nodes need to be secured

SEC-WEAR focuses on two threats:

- Eavesdropping data transmitted from the node to the body central unit
- Tampering with a node and illegitimately accessing the data stored on it

Goal and Methodology

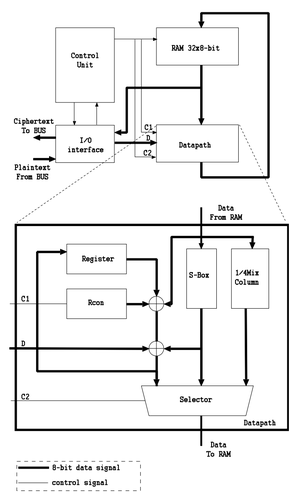
- To provide security complying with the energy constraints imposed by a wireless body sensor node

How?

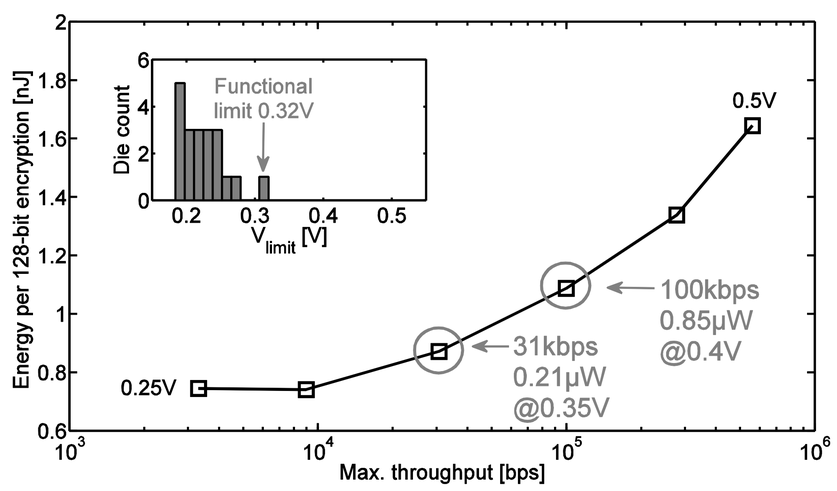
- Using standard algorithms rather than designing new ones
- Exploring the potential of novel libraries for realizing secure BASN nodes
- Examine the behavior of new libraries against fault attacks
- Examine the challenges of realizing a DPA resistant library using new libraries

Securing Sensor Nodes Using Dedicated Cryptographic Modules

Low Cost AES Implementation

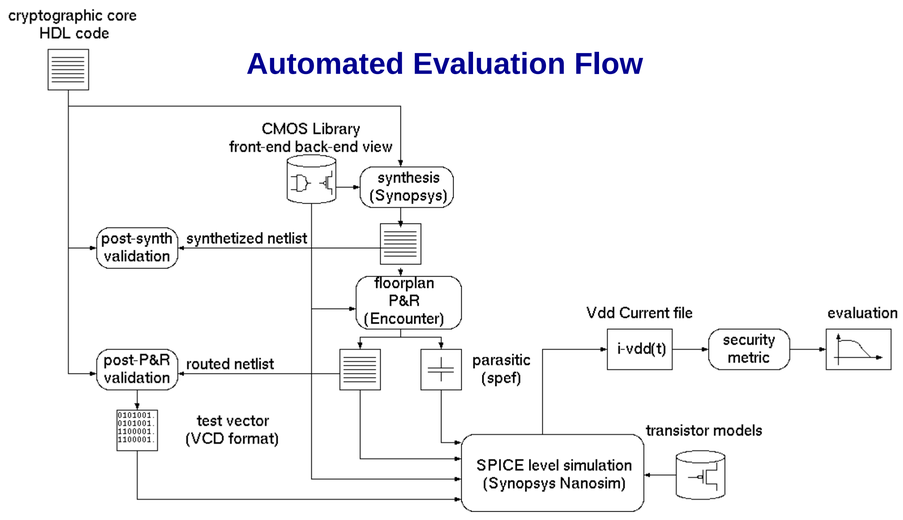


Energy per encryption vs max throughput

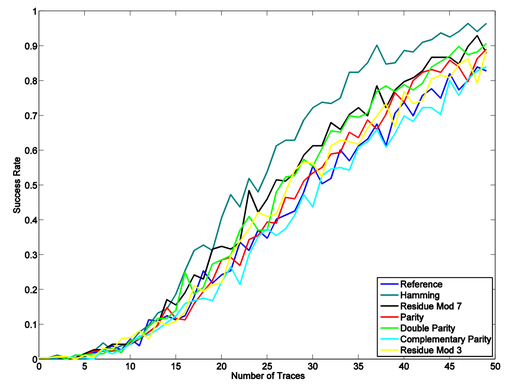


Resistance Against Fault Attacks

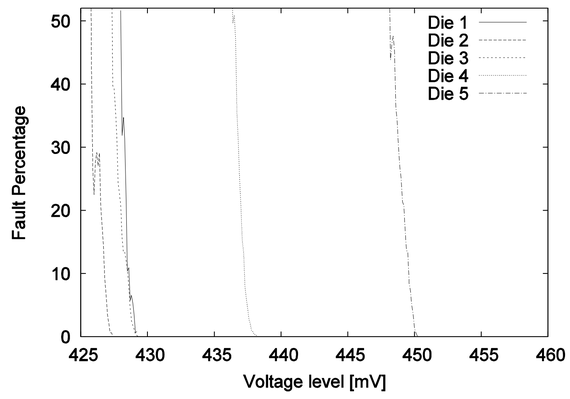
Automated Evaluation Flow



Effects of Error Detection Circuits on DPA

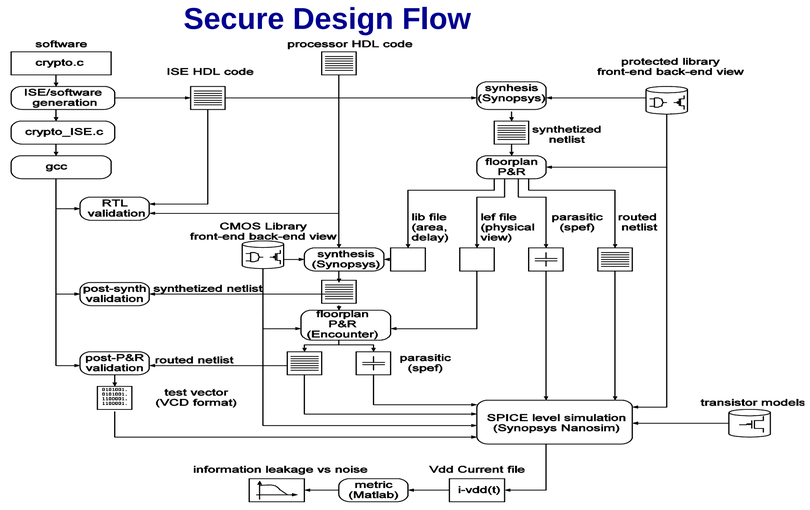


Low Cost Fault Attacks on 65nm sub-threshold AES

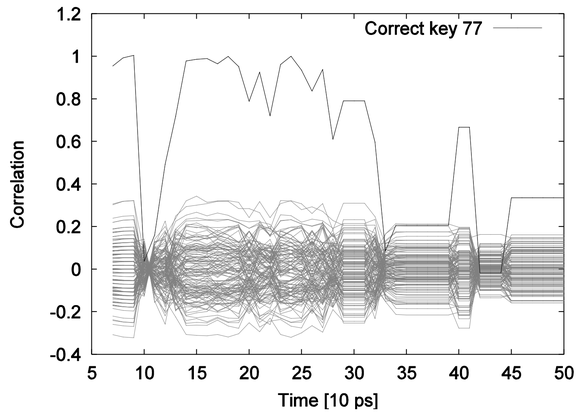


Resistance Against Power Analysis Attacks

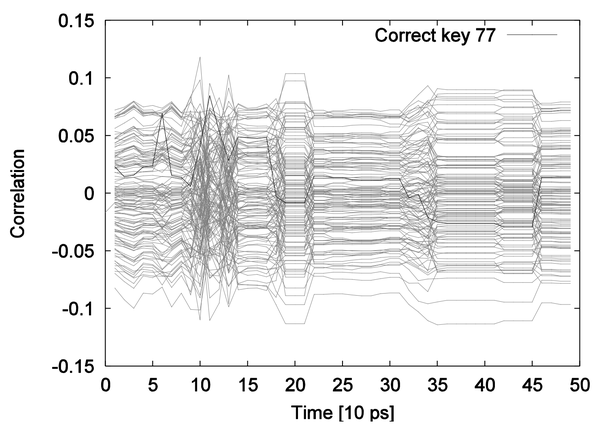
Secure Design Flow



DPA on Unprotected Library



DPA on Protected Library



References

- F. Regazzoni, L. Breveglieri, P. Ienne, and I. Koren, “Interaction between Fault Attack Countermeasures and the Resistance against Power Analysis Attacks”, to appear in Fault Analysis in Cryptography, Springer-Verlag, Editors: Marc Joye and Michael Tunstall
- A. Barenghi, C. Hocquet, D. Bol, F.X. Standaert, F. Regazzoni, and I. Koren, "Exploring the Feasibility of Low Cost Fault Injection Attacks on Sub-Threshold Devices through an example of a 65nm AES implementation", Accepted for publication at 7th Workshop on RFID Security and Privacy 2011, Amherst, Massachusetts, June 26–28, 2011
- C. Hocquet, D. Kamel, F. Regazzoni, J.-D. Legat, D. Flandre, D. Bol, F.-X. Standaert, Harvesting the potential of nano-CMOS for lightweight cryptography: An ultra-low-voltage 65 nm AES coprocessor for passive RFID tags, in the Journal of Cryptographic Engineering, vol 1, num 1, pp 79-86, April 2011, Springer
- B. Lamichanne, S. Mudda, F. Regazzoni, and A. Puiatti "LEXCOMM: a Low Energy, Secure and Flexible Communication Protocol for a Heterogenous Body Sensor Network" , in the Proceedings of IEEE-EMBS International Conference on Biomedical and Health Informatics "Global Grand Challenge of Health Informatics", Jan. 2-7 2012, Hong Kong - Shenzhen, China
- K. Padarnitsas, N. Christianos, and F. Regazzoni, “Exploring the resistance of IMDPL at 65nm”, submitted