Abstract: Side-channel attacks have grown into a central threat to the security of nowadays cryptographic devices. The set of implementation countermeasures constantly competes with the set of known attack strategies, however, systematic ways to protect against information leakage are uncommon. Despite many achievements in the field of secure implementations, side-channel countermeasures only offer ad-hoc remedies which do not conform to the idea of provably secure cryptosystems. On the other side, leakage-resilient constructions often hinge on assumptions which can be hardly translated into practice. This work is an attempt to provide a theoretical, yet practical, modeling of side-channels that aids in identifying spots and making design choices towards a comprehensive side-channel security treatment from theoretical proofs down to hardware implementations. More precisely, we illustrate a simple sufficient condition for building physically secure hardware that follows directly from the decomposition of the side-channel into an algorithmic-related part and a physical-related part, and
hardness of inversion. We put forward that our simple modeling allows to commit clear security goals to cryptographers and hardware designers and preserve the security of theoretical constructions all the way down to final chip fabrication. As a showcase application, we consider the security of the Goldwasser-Goldreich-Micali (GGM) construction scheme for efficient pseudorandom functions with and without leakages. These security proofs have been left open in previous literature and here serve to demonstrate the feasibility of our modeling approach.

Stichworte: Leakage, Resilient, Pseudo-Random

Dewey Dezimalklassifikation (Liste): 620 Ingenieurwissenschaften

Kongress- / Buchtitel: Third International Conference on Cryptology and Information Security in Latin America (LATINCRYPT 2014)

Kongress / Zusatzinformationen: Florianópolis, Brazil

Jahr: 2014

Quartal: 3. Quartal

Jahr / Monat: 2014-09

Monat: Sep

Revied: ja

Sprache: en

WWW: http://latincript2014.labsec.ufsc.br/

Occurences:

· Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2014

Entries: