Cryptology ePrint Archive: Report 2011/519

Leakage-Resilient Cryptography From the Inner-Product Extractor

Stefan Dziembowski and Sebastian Faust

Abstract: We present a generic method to secure various widely-used cryptosystems against \emph{arbitrary} side-channel leakage, as long as the leakage adheres three restrictions: first, it is bounded per observation but in total can be arbitrary large. Second, memory parts leak \emph{independently}, and, third, the randomness that is used for certain operations comes from a simple (non-uniform) distribution.

As a fundamental building block, we construct a scheme to store a cryptographic secret such that it remains \emph{information theoretically} hidden, even given arbitrary continuous leakage from the storage. To this end, we use a randomized encoding and develop a method to securely \emph{refresh} these encodings even in the presence of leakage. We then show that our encoding scheme exhibits an efficient additive homomorphism which can be used to protect important cryptographic tasks such as identification, signing and encryption. More precisely, we propose \emph{efficient} implementations of the Okamoto identification scheme, and of an ElGamal-based cryptosystem with security against continuous leakage, as long as the leakage adheres the above mentioned restrictions. We prove security of the Okamoto scheme under the DL assumption and \emph{CCA2 security} of our encryption scheme under the DDH assumption.

Category / Keywords: foundations /

Publication Info: extended version of a paper accepted to Asiacrypt 2011

Date: received 21 Sep 2011

Contact author: stefan at dziembowski net