Cryptology ePrint Archive: Report 2011/314

Tamper-Proof Circuits: How to Trade Leakage for Tamper-Resilience

Sebastian Faust and Krzysztof Pietrzak and Daniele Venturi

Abstract: Tampering attacks are cryptanalytic attacks on the implementation of cryptographic algorithms (e.g., smart cards), where an adversary introduces faults with the hope that the tampered device will reveal secret information. Inspired by the work of Ishai et al. [Eurocrypt'06], we propose a compiler that transforms any circuit into a new circuit with the same functionality, but which is resilient against a well-defined and powerful tampering adversary. More concretely, our transformed circuits remain secure even if the adversary can adaptively tamper with every wire in the circuit as long as the tampering fails with some probability $\delta>0$. This additional requirement is motivated by practical tampering attacks, where it is often difficult to guarantee the success of a specific attack.

Formally, we show that a q-query tampering attack against the transformed circuit can be ``simulated" with only black-box access to the original circuit and $\log(q)$ bits of additional auxiliary information. Thus, if the implemented cryptographic scheme is secure against $\log(q)$ bits of leakage, then our implementation is tamper-proof in the above sense. Surprisingly, allowing for this small amount of information leakage -- and not insisting on perfect simulability like in the work of Ishai et al. -- allows for much more efficient compilers, which moreover do not require randomness during evaluation. Similar to earlier work our compiler requires small, stateless and computation-independent tamper-proof gadgets. Thus, our result can be interpreted as reducing the problem of shielding arbitrary complex computation to protecting simple components.

Category / Keywords: foundations / tamper resilience, compiler

Publication Info: An extended abstract of this paper appears at ICALP 2011

Date: received 14 Jun 2011

Contact author: sfaust at cs au dk

Available formats: PDF | BibTeX Citation

Version: 20110617:064659 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]