Cryptology ePrint Archive: Report 2011/660

Program Obfuscation with Leaky Hardware

Nir Bitansky and Ran Canetti and Shafi Goldwasser and Shai Halevi and Yael Tauman Kalai and Guy N. Rothblum

Abstract: We consider general program obfuscation mechanisms using ``somewhat trusted'' hardware devices, with the goal of minimizing the usage of the hardware, its complexity, and the required trust. Specifically, our solution has the following properties:

\begin{itemize}

\item The obfuscation remains secure even if all the hardware devices in use are {\em leaky}. That is, the adversary can obtain the result of evaluating any polynomial-time computable function on the local state of the device, as long as this function has short output. In addition the adversary also controls the communication between the devices.

\item The number of hardware devices used in an obfuscation and the amount of work they perform are polynomial in the security parameter {\em independently} of the obfuscated function's complexity.

\item A ({\em universal}) set of hardware components, owned by the user, is initialized only once and from that point on can be used with multiple ``software-based'' obfuscations sent by different vendors.

\end{itemize}

Category / Keywords: Obfuscation, Hardware, Leakage-Resilience

Publication Info: An extended abstract of this paper appears in the proceedings of ASIACRYPT '11

Date: received 6 Dec 2011, last revised 21 Dec 2011

Contact author: nirbitan at tau ac il