Call for feedback about the Masked Circuits Project

Text originally posted on 2021-June-21 in the MC-Forum

Comments due by 2021-Sep-06

The NIST Masked Circuits project is interested in masking techniques that can improve resistance of hardware circuit implementations of block-ciphers against side-channel attacks. The newly formed forum MC-forum@list.nist.gov will be used to support open discussion; and the new project webpage https://csrc.nist.gov/Projects/masked-circuits will host relevant material.

It is important to gauge the stakeholders' interest in this effort and on the direction to be taken. We received a proposal "Threshold Cryptography on a Single Device by Means of Threshold Implementations" by S. Dhooghe, S. Nikova, and V. Rijmen, from KU Leuven, see attachment. It describes three first-order masking schemes for AES, requiring a set of algorithmic properties to guarantee security in the (single-probe) glitch-extended probing model. The proposal covers only the logical construction, with the result being specified as a netlist. Using this as a basis, this email serves as a call for feedback on it. We ask the community to comment on the following:

1. Potential interest:

a) Are the glitch-extended probing model and the corresponding masking schemes addressing problems of interest for the industry and government stakeholders?

b) What orders of protection are pertinent to consider for standardization?

c) Will the semiconductor industry adopt this type of schemes in their product lines to supply the market with products implementing them?

2. Feasibility potential:

a) Is there a stack of available design and production tools, widely used by the semiconductor industry, that can transfer the logical netlists into silicon gate layouts, on major hardware platforms of interest (FPGA, ASIC, etc.), while preserving the needed algorithmic properties and ensuring the needed implementation assumptions, so that minimal side-channel testing would be sufficient for the verification of the intended security guarantees?

b) Considering practical attacks, are there identifiable deployment characteristics that justify differentiated security profiles across platforms, masking orders, and other properties?

The MC-forum@list.nist.gov forum can be used for open comments, but please send your formal comments in a PDF file, by September 6, 2021, by email to masked-circuits@nist.gov. The formal comments received by email, in PDF, will be compiled together and made available on the webpage.