Updates on the Implementation Security of ISAP
Proposal for Presentation

Christoph Dobraunig\textsuperscript{1}, Maria Eichlseder\textsuperscript{1}, Stefan Mangard\textsuperscript{1}, Florian Mendel\textsuperscript{2}, Bart Mennink\textsuperscript{3}, Robert Primas\textsuperscript{1} and Thomas Unterluggauer\textsuperscript{1}

\textsuperscript{1} Graz University of Technology, Austria
\textsuperscript{2} Infineon Technologies AG, Germany
\textsuperscript{3} Radboud University, Netherlands
https://isap.iaik.tugraz.at

ISAP v2.0 [Dob+20] is a family of lightweight authenticated encryption algorithms designed with a focus on robustness against implementation attacks. Its instances are based either on ASCON’s permutation [DEMS16] or Keccak-\textit{p}[400] [BDPV11; Nat15]. ISAP v2.0 is of particular interest for applications like firmware updates where robustness against power analysis and fault attacks is crucial and codesize and a small footprint in hardware matters.

In this talk, we focus on the implementation security aspects of ISAP v2.0. First, we revisit ISAP v2.0’s mode-level features such as increased resistance against implementation attacks including DPA [KJJ99], DFA [BS97], SFA [FJLT13], and SIFA [Dob+18].

We then outline the results of the recent CHES paper “Single-Trace Attacks on Keccak”, which is co-authored by one of ISAP v2.0’s designers, and studies the applicability of SPA/Template attacks on cryptographic constructions that are used within ISAP v2.0 [KPP20].

Finally, we discuss a newly released compact co-processor implementing ASCON’s permutation [SP20], which is to appear at CARDIS 2020. This co-processor can be used to significantly speed up ASCON/ISAP v2.0 computations, while providing increased protection against SPA/Template attacks at the same time.

References


