Department of Electrical Engineering
香港城市大學
City University of Hong Kong

CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series

Revealing the Weakness of Addition Chain-based Masked SBox Implementations

Dr. Jingdian MING, Doctoral Researcher
Jiaxing Research Institute, Zhejiang University

Abstract:

Addition chain is a well-known approach for implementing higher-order masked SBoxes. However, this approach induces more computations of intermediate monomials, which in turn leaks more information related to the sensitive variables and may consequently decrease its side-channel resistance. Thus, we investigate the resilience of monomial computations with respect to side-channel analysis. We select several representative addition chain implementations, based on their theoretical resilience, that demonstrate the strongest and weakest resistance to side-channel analysis. In practical experiments based on an ARM Cortex-M4 architecture, we collect power and electromagnetic traces, considering different noise levels. The results reveal that the weakest masked SBox implementation exhibits a side-channel resistance nearly identical to an unprotected implementation. Moreover, we find that some monomials with smaller output size leak more sensitive information than the SBox output. This finding applies to various other masking schemes, including inner product masking.

Biography:

Jingdian MING received the Ph.D. degree in 2022 from the School of Cyber Security, University of Chinese Academy of Sciences. He is currently an Associate Researcher at Jiaxing Research Institute, Zhejiang University. His main research interests include hardware security, cryptographic engineering, and side-channel analysis. Over the years, he has published multiple papers in hardware security, including TIFS, TCHES, and DATE.

14 May 2024 (Tue); 9:00am - 10:00am; https://cityu.zoom.us/j/96742093029