Schneider, Tobias; Moradi, Amir; Güneysu, Tim

Arithmetic addition over Boolean masking. Towards first- and second-order resistance in hardware. (English) Zbl 1423.94103

Malkin, Tal (ed.) et al., Applied cryptography and network security. 13th international conference, ACNS 2015, New York, NY, USA, June 2–5, 2015. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 9092, 559-578 (2015).

Summary: A common countermeasure to thwart side-channel analysis attacks is algorithmic masking. For this, algorithms that mix Boolean and arithmetic operations need to either apply two different masking schemes with secure conversions or use dedicated arithmetic units that can process Boolean masked values. Several proposals have been published that can realize these approaches securely and efficiently in software. But to the best of our knowledge, no hardware design exists that fulfills relevant properties such as efficiency and security at the same time.

In this paper, we present two design strategies to realize a secure and efficient arithmetic adder for Boolean-masked values. First, we introduce an architecture based on the ripple-carry adder that targets low-cost applications. The second architecture is based on a pipelined Kogge-Stone adder and targets high-performance applications. In particular, all our implementations adopt the threshold implementation approach to improve their resistance against SCA attacks even in the presence of glitches. We evaluated the security of our designs practically against SCA using a non-specific statistical t-test. Based on our analysis, we show that our constructions not only achieve resistance against first- and (univariate) second-order attacks but also require fewer random bits per operation compared to any existing software-based approach.

For the entire collection see [Zbl 1331.94004].

MSC:

94A60 Cryptography

Cited in **2** Documents

Keywords:

side-channel analysis; threshold implementation; Boolean masking; arithmetic modular addition

Software:

ChaCha; Salsa20

Full Text: DOI