Badel, Stéphane; **Dağtekin, Nilay**; **Nakahara, Jorge jun.**; **Ouafi, Khaled**; **Reffé, Nicolas**; **Sepehrdad, Pouyan**; **Sušil, Petr**; **Vaudenay, Serge**

ARMADILLO: A multi-purpose cryptographic primitive dedicated to hardware. (English)

Zbl 1227.94027

Mangard, Stefan (ed.) et al., Cryptographic hardware and embedded systems – CHES 2010. 12th international workshop, Santa Barbara, USA, August 17–20, 2010. Proceedings. Berlin: Springer (ISBN 978-3-642-15030-2/pbk). Lecture Notes in Computer Science 6225, 398-412 (2010).

Summary: This paper describes and analyzes the security of a general-purpose cryptographic function design, with application in RFID tags and sensor networks. Based on these analyses, we suggest minimum parameter values for the main components of this cryptographic function, called ARMADILLO. With fully serial architecture we obtain that 2,923 GE could perform one compression function computation within 176 clock cycles, consuming 44μW at 1 MHz clock frequency. This could either authenticate a peer or hash 48 bits, or encrypt 128 bits on RFID tags. A better tradeoff would use 4,030 GE, 77μW of power and 44 cycles for the same, to hash (resp. encrypt) at a rate of 1.1 Mbps (resp. 2.9 Mbps). As other tradeoffs are proposed, we show that ARMADILLO offers competitive performances for hashing relative to a fair Figure Of Merit (FOM).

For the entire collection see [Zbl 1193.68012].

MSC:

94A60 Cryptography

Software:

Armadillo; ARMADILLO; HIGHT; PRESENT

Full Text: DOI