Bernstein, Daniel J.; **Lange, Tanja**

Never trust a bunny. (English) Zbl 1337.94093

Hoepman, Jaap-Henk (ed.) et al., Radio frequency identification. Security and privacy issues. 8th international workshop, RFIDSec 2012, Nijmegen, The Netherlands, July 2–3, 2012. Revised selected papers. Berlin: Springer (ISBN 978-3-642-36139-5/pbk). Lecture Notes in Computer Science 7739, 137-148 (2013).

Summary: "Lapin" is a new RFID authentication protocol proposed at FSE 2012 [*E. Kiltz*, Lect. Notes Comput. Sci. 7549, 346–365 (2012; Zbl 1282.94078)]. "Ring-LPN" (Ring-Learning-Parity-with-Noise) is a new computational problem proposed in the same paper; there is a proof relating the security of Lapin to the difficulty of Ring-LPN. This paper presents an attack against Ring-LPN-512 and Lapin-512. The attack is not practical but nevertheless violates specific security claims in the FSE 2012 paper.

For the entire collection see [Zbl 1268.94002].

MSC:

94A62 Authentication, digital signatures and secret sharing

Keywords:

authentication; RFID; LPN; Ring-LPN; attacks; Lapin; bunnies

Full Text: DOI