A New Proposal for Lightweight Cryptography: LILLIPUT

Julien Francq

Abstract

This talk proposes to detail some aspects of lightweight cryptography, which has been a very active topic these last years, especially for RFID systems. First, we will discuss about the harsh implementation constraints of RFID tags. We will define the area, power consumption and computation time budgets that a cryptographic implementation has to fit in. Second, we will detail the three main strategies used to implement cryptography in RFID tags: implement standards, adapt them, implement new "ad hoc" intrinsically lightweight algorithms. Related to this last strategy, we will present in avant-premiere in CryptArchi 2014 a new lightweight block cipher proposal: LILLIPUT. This latter has been initially designed by Gael Thomas and Thierry Berger from University of Limoges (France) and Marine Minier from INSA Lyon (France).