

Cryptology ePrint Archive: Report 2011/691

Yet Another Ultralightweight Authentication Protocol that is Broken

Gildas Avoine and Xavier Carpent

Abstract: Eghdamian and Samsudin published at ICIEIS 2011 an ultralightweight mutual authentication protocol that requires few bitwise operations. The simplicity of the design makes the protocol very suitable to low-cost RFID tags. However, we demonstrate in this paper that the long-term key shared by the reader and the tag can be recovered by an adversary with a few eavesdropped sessions only.

Category / Keywords: cryptographic protocols / Authentication, Ultralightweight protocol, RFID

Date: received 20 Dec 2011, last revised 9 Jan 2012

Contact author: xavier carpent at uclouvain be

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: Removed double line spacing

Version: 20120109:111606 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]