Cryptology ePrint Archive: Report 2011/247

An Ultra-Efficient Key Recovery Attack on the Lightweight Stream Cipher A2U2

Qi Chai, Xinxin Fan, Guang Gong

Abstract: In this letter we report on an ultra-efficient key recovery attack under the chosen-plaintext-attack model against the stream cipher A2U2, which is the most lightweight cryptographic primitive (i.e., it costs only 284 GE in hardware implementation) proposed so far for low-cost Radio Frequency Identification (RFID) tags. Our attack can fully recover the secret key of the A2U2 cipher by only querying the A2U2 encryption twice on the victim tag and solving 32 sparse systems of linear equations (where each system has 56 unknowns and around 28 unknowns can be directly obtained without computation) in the worst case, which takes around 0.16 second on a Thinkpad T410 laptop.

Category / Keywords: Stream Cipher, Key Recovery, RFID

Date: received 17 May 2011, last revised 26 May 2011

Contact author: q3chai at engmail uwaterloo ca