Cryptology ePrint Archive: Report 2011/563

On the Security of RFID Anti Cloning Security Protocol(ACSP)

Masoumeh Safkhani and Nasour Bagheri and Majid Naderi

Abstract: Recently Qian et al. have proposed a new attack for RFID systems, called counting attack, where the attacker just aims to estimate the number of tagged objects instead of steal the tags' private information. They have stated that most of the existing RFID mutual authentication protocols are vulnerable to this attack. To defend against counting attack, they propose a novel Anti-Counting Security Protocol called ACSP. The designers of ACSP have claimed that their protocol is resistant against counting attack and also the other known RFID security threats. However in this paper we present the following efficient attacks against this protocol:

1) Tag impersonation attack: the success probability of attack is "1" while the complexity is two runs of protocol. 2) Two single tag de-synchronization attacks, the success probability of both attacks are "1" while the complexity is at most two runs of protocol. 3)Group of tags de-synchronization attack: this attack, which can de-synchronize all tags in the range at once, has success probability of "1" while its complexity is one run of protocol. 4) Traceability attack: the adversary's advantage in this attack is almost "0.5", which is almost the maximum of possible advantages for an adversary in the same model. The complexity of attack is three runs of protocol

Category / Keywords: cryptographic protocols /

Date: received 18 Oct 2011, last revised 25 Oct 2011

Contact author: nbagheri at srttu edu