Cryptology ePrint Archive: Report 2011/704

Security Analysis of a PUF based RFID Authentication Protocol

Masoumeh Safkhani and Nasour Bagheri and Majid Naderi

Abstract: In this paper we consider the security of a PUF based RFID Authentication protocol which has been recently proposed by Bassil et a
The designers have claimed that their protocol offers immunity against a broad range of attacks while it provides excellent performance. Howeve
we prove in contrary to its designers claim that this protocol does not provide any security. We present an efficient secret disclosure attack whic
retrieves all secret parameters of the protocol. Given those secret parameters, it would be trivial to apply any other attack in the context on the
protocol. However, to highlight other weaknesses of the protocol we present extra reader traceability, impersonation and desynchronization atta
that do not require disclosing the secret parameters necessarily. Success probability of all mentioned attacks is almost ``1'' while the complexity
most two runs of protocol.

Category / Keywords: cryptographic protocols / RFID, Authentication, PUF, Traceability Attack, Reader Impersonation Attack, Tag impersonation Attack, Desynchronization Attack

Date: received 26 Dec 2011, last revised 9 Jan 2012

Contact author: nbagheri at srttu edu, na bagheri@gmail com