Cryptology ePrint Archive: Report 2011/424

Cryptanalysis of AZUMI: an EPC Class-1 Generation-2 Standard Compliant RFID Authentication Protocol

Masoumeh Safkhani and Nasour Bagheri and Majid Naderi

Abstract: In this paper, we analyze the security of AZUMI protocol which is compliant with the EPC-Class-1 Generation-2 standard and recently has been proposed by Peris \textit{et al.} This protocol is an improvement to a protocol proposed by Chen and Deng which has been cryptanalysed by Peris \textit{et al.} and Kapoor and Piramuthu. However, our security analysis clearly shows that the designers were not successful in their attempt to improve the Chen and Deng protocol. More precisely, we present an efficient attack to disclose the tag and the reader secret parameters. In addition, we present a simple tag impersonation attack against this protocol. The success probability of all attacks are almost ``1" and the cost of given attacks are at most eavesdropping two sessions of protocol. However, the given secrets disclosure attack also requires $O(2^{16}) $ off-line evaluation of a $PRNG$ function.

Category / Keywords: cryptographi protocols/ RFID, EPC-C1 G2, Mutual Authentication, Secret Disclosure, Tag Impersonation.

Date: received 7 Aug 2011, last revised 28 Aug 2011

Contact author: na bagheri at gmail com