An Efficient and Secure Symmetric Cryptosystem for RFID Security

許慶賢,謝杰甫,Hai-Cheng Chu,Jong-Hyuk Park
Computer Science & Information Engineering
Computer Science and Informatics
chh@chu.edu.tw

Abstract

RFID technology introduces new challenging security problems. In this paper, we present an efficient and secure mechanism from identity authentication to data encryption for RFID systems. Given the inadequate of data encryption in current RFID security, the proposed scheme was based on symmetric cryptographic technique to support mutual authentication and data encryption between tags and readers/servers. The ASE (Advanced Encryption Standard) symmetric cryptographic algorithm was employed due to trade-off between hardware complexity and security strength. According to our design, tag only needs to implement an AES engine to be able to perform both identity authentication and data encryption. In addition, the proposed identity authentication scheme provides mutual authentication and key management protocol which is resistant to several known RFID attacks such as Man-in-the-Middle, Denial-of-Service, replay, clone attack and backward/forward traceability. The time computational complexity of our proposed identity authentication scheme is 3Tencrypt+1Tnonce+4Txor in the tag side. In the data encryption phase, we proved that AES is able to provide higher encryption performance than other symmetric cryptographic algorithm in the same level of security strength.

Keyword：RFID security, symmetric cryptographic, identity authentication, data encryption, AES.