Abstract

RFID (Radio Frequency identification) is emerging as an important tool in the field of Automatic Identification Technologies. The universal deployment of RFID devices may expose new security and privacy risks. These risks are the main obstacle for successful deployment of RFID tags. Since, the traditional cryptographic approach is not suitable for the RFID tags due to its
limited computation resources and small storage capacity. This paper proposes an effective and efficient ultralightweight mutual authentication protocol, to achieve stronger security and privacy by using only simple bitwise operations (e.g. XOR, modulus addition). The proposed protocol is inspired by the Gossamer protocol of ultralightweight protocol family and by using its existing Rotation and Mixbit function. The proposed protocol provides better solution for security and privacy risk as compared with Gossamer and other relevant protocols. The comparative security and performance analysis shows that proposed protocol provides better security and privacy from the other solutions as well as reduces the computation, communication and storage cost.

Reference


Index Terms

Computer Science | Security

Key words

Authentication | Traceability | Applicability
Ultra-lightweight protocol
privacy
radio frequency identification (RFID)
security
active attacks
denial of service
de-synchronization