Abstract

On the basis of Vaudenay's untraceability model, this paper describes cryptanalyses of recently proposed Zhuang et al.'s ultralightweight RFID authentication protocol for low cost tags R2AP and Dehkordi and Farzaneh's improved hash based RFID mutual authentication protocol. This paper formally demonstrates that R2AP is insecure and does not attain even Narrow Forward privacy level of security. Additionally, R2AP protocol is traceable and suffers from impersonation attack. Also Dehkordi and Farzaneh's proposed protocol is impractical formally as it does not attain even Narrow Forward privacy level of security.
Security Flaws in Two Recently Proposed RFID Authentication Protocols

References


Index Terms

Computer Science
Security

Keywords

Rfid  Privacy  Authentication  Cryptanalysis