Abstract:
Over the last few years many systems adopted Radio Frequency Identification (RFID) technology in various business activities and security applications. In RFID technology the system uses radio frequency signal for communication between the tag (object) and the reader. This signal can be easily intercepted or captured using an appropriate electromagnetic signal detector, which makes the system vulnerable to security attacks. Business activities that utilize the RFID technology for access-control, electronic payments, electronic documents (e-documents), etc., require strong security. However, due to limited computational power and memory storage on the tag, powerful security protocols including Public Key Cryptography (PKC) can hardly be implemented in many RFID systems. Based on their memory size, computing power and security features, there exists a variety of RFID systems. MIFARE is one of the most popular ones. MIFARE consists of four different types of contactless cards with MIFARE Classic being the front runner, covering about 85% of the contactless smart card market. MIFARE Classic security scheme uses stream-cipher cryptography with 48-bit secret key. As the cryptanalysis is getting sophisticated, the vulnerability level of MIFARE Classic has significantly increased and security challenges have become a rising concern in many business applications. Multiple studies on the security of MIFARE Classic disclosed significant weaknesses. However, the proprietor claims the security scheme was enhanced with additional bytes for unique identifier (UID), and the system has reliable security. Accordingly, MIFARE Classic is still deployed and being used in large-scale applications. This paper presents a comprehensive survey of currently known attacks on RFID-MIFARE Classic security structure, the potency of 7-Byte UID in enhancing the security scheme, and finally proposes a number of methods to reduce the danger of potential attacks.