# Cryptology ePrint Archive: Report 2013/066

**Analysis and Improvement of the securing RFID systems conforming to EPC Class 1 Generation 2 standard**

*Amin Mohammadali; Zahra Ahmadian; Mohammad Reza Aref*

**Abstract:** Radio Frequency IDentification (RFID) technology is a wireless identification method in which security and privacy are important parameters for public acceptance and widespread use. In order to thwart such security and privacy problems, a wide variety of authentication protocols have been proposed in the literature. In 2010, Yeh et al's proposed a new RFID authentication protocol conforming to EPC Class 1 Generation 2 standard. They claimed that this protocol is secure against DoS attack, replay attack, DATA forgery attack, and provides untraceability and forward secrecy. In 2012, Yoon showed that this protocol does not provide forward secrecy and DATA integrity. He improved the protocol and tried to eliminate the weaknesses and claimd that the improved protocol does not have the weaknesses of the primary protocol. In this paper, we show that the improved protocol has some weaknesses including DoS attack, back-end server impersonation, tag impersonation and DATA forgery attack. We also show that it can not provide forward secrecy of the reader and untraceability. We improve the protocol, which offers a high level of security and provides mutual authentication, untraceability and forward secrecy as well as resistance to DATA forgery, replay and DoS attacks, while retaining a competitive communication cost.

**Category / Keywords:** cryptographic protocols / RFID authentication protocol, EPC, Forward secrecy, integrity.

**Date:** received 12 Feb 2013

**Contact author:** zahraahmadian at yahoo com