Cryptology ePrint Archive: Report 2011/418

An efficient RFID mutual authentication scheme based on ECC

Jue-Sam Chou, Yalin Chen, Cheng-Lun Wu, Chi-Fong Lin

Abstract: Recently, Radio Frequency Identification (RFID) technique has been widely deployed in many applications, such as medical drugs management in hospitals and missing children searching in amusement parks. The applications basically can be classified into two types: non-public key cryptosystem (PKC)-based and PKC-based. However, many of them have been found to be flawed in the aspect of privacy problem. Therefore, many researchers tried to resolve this problem. They mainly investigated on how low-cost RFID tags can be used in large-scale systems. However, after analyses, we found those studies have some problems, such as suffering physical attack or de-synch attack. Hence, in this paper, we try to design an efficient RFID scheme based on Elliptic Curve Cryptography (ECC) to avoid these problems. After analyses, we conclude that our scheme not only can resist various kinds of attacks but also outperforms the other ECC based RFID schemes in security requirements, with needing only little extra elliptic curve point multiplications.

Category / Keywords: applications / RFID, location privacy, forward secrecy, mutual authentication

Date: received 3 Aug 2011

Contact author: jschou at mail nhu edu tw

Available formats: PDF | BibTeX Citation

Version: 20110805:134942 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]