Cryptology ePrint Archive: Report 2011/381

A Novel RFID Authentication Protocol based on Elliptic Curve Cryptosystem

Yalin Chen1, Jue-Sam Chou2, Chi-Fong Lin3, Cheng-Lun Wu4

Abstract: Recently, many researchers have proposed RFID authentication protocols. These protocols are mainly consists of two types: symmetric key based and asymmetric key based. The symmetric key based systems usually have some weaknesses such as suffering brute force, de-synchronization, impersonation, and tracing attacks. In addition, the asymmetric key based systems usually suffer from impersonation, man-in-the-middle, physical, and tracing attacks. To get rid of those weaknesses and reduce the system workload, we adopt elliptic curve cryptosystem (ECC) to construct an asymmetric key based RFID authentication system. Our scheme needs only two passes and can resist various kinds of attacks. It not only outperforms the other RFID schemes having the same security level but also is the most efficient.

Category / Keywords: radio frequency identification, RFID, identification protocol, privacy,

Date: received 13 Jul 2011, last revised 17 Jul 2011

Contact author: jschou at mail nhu edu tw

Available formats: PDF | BibTeX Citation

Version: 20110717:071453 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]