A STUDY ON SECURE MOBILE E-COMMERCE WITH SELF-CERTIFIED PUBLIC KEY CRYPTOSYSTEMS

陳宗保、曹偉駿
E-mail: 9020048@mail.dyu.edu.tw

ABSTRACT


Keywords : ELLIPTIC CURVE CRYPTOSYSTEMS, WIRELESS PUBLIC KEY INFRASTRUCTURE (WPKI), SELF-CERTIFIED PUBLIC KEY CRYPTOSYSTEMS, WIRELESS APPLICATION PROTOCOL (WAP), ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM, AUTHENTICATED ENCRYPTION SCHEME, MOBILE E-COMMERCE
[1] 賴溪松、韓亮、張真誠,「近代密碼學及其應用」,松崗圖書資料公司,民國88年1月。
[2] 高銘智,「使用在WAP協定中的橢圓曲線密碼系統」,電腦與通訊 第85期,第45-48頁,民國88年12月。
[3] 鍾振華,「使用身分基礎之自我驗證公開金鑰的金鑰分配及會議金鑰分配技術」,台灣科技大學資訊管理系碩士班碩士論文,民國88年。
[4] 賴亮智,「電子商務概要」,美商麥格羅.希爾,民國89年10月。
[5] 張瑗玲,「捍衛網際網路的商機」,松崗圖書資料公司,民國86年4月。
[18] ETSI WEB SITE, (URL: HTTP://WWW.ETSI.ORG/).
[23] GSM WEB SITE, (URL: HTTP://WWW.GSM.ORG/).


WAP Forum, (URL: http://www.wapforum.org/).
