Chapter XIII

A SEEP Protocol Design
Using 3BC, ECC(F_2^m) and HECC Algorithm

Byung Kwan Lee, Kwandong University, Korea
Seung Hae Yang, Kwandong University, Korea
Tai-Chi Lee, Saginaw Valley State University, USA

Abstract

Unlike SET (secure electronic transaction) protocol. This chapter proposes a SEEP (highly secure electronic payment) protocol, which uses ECC (elliptic curve cryptosystem with F_2^m not F_p) (Koblitz, 1987; Miller, 1986; Harper, Menezes, & Vanstone, 1993), SHA (secure hash algorithm) and 3BC (block byte bit cipher) instead of RSA and DES. To improve the strength of encryption and the speed of processing, the public key and the private key of ECC and HECC (Hyper Elliptic Curve Cryptosystem) are used in 3BC (Cho, Shin, Lee, & Lee, 2002; Cho & Lee, 2002) algorithm, which generates session keys for the data encryption. In particular, when ECC and HECC are combined with 3BC, the strength of security is improved significantly. As the process of the digital envelope used in the existing SET protocol is removed by the 3BC algorithm in this chapter, the processing time is substantially reduced. In addition, the use of multiple signatures has some advantages of reducing the size of transmission data as an intermediate payment agent and avoiding the danger of eavesdropping of private keys.

Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
Introduction

Today, electronic data exchange is part of our everyday life. The EC (electronic commerce) has been expanding rapidly in quantity and quality since it started on the Internet. The reason is that it can be done by increasing the reliability of EC with the new development of security technique. The SSL, a security socket layer, which is currently used in EC is being considered the only stable access to the Internet during the transportation, but it can hardly ensure the problem of information security. To some extent, the SET (secure electronic transaction) protocol based on electronic payment has improved message integrity, authentication, and non-repudiation. Such a protocol is related directly to cryptography for security and consists of an asymmetric key algorithm, RSA for authentication and non-repudiation, DES for the message confidentiality, Hash algorithm and SHA for message integrity. But the disadvantage of this protocol is that the speed of processing is slow because of long key size. From this standpoint, ECC (elliptic curve cryptosystem) technique is very important to Cryptography. This chapter proposes a SEEP (highly secure electronic payment) protocol, which uses ECC instead of RSA. To improve the strength of encryption and the speed of processing, the public key and the private key of ECC and HECC are used in the 3BC (block byte bit cipher) algorithm, which generates session keys for the data encryption. Therefore, the digital envelope used in the existing SET protocol can be removed by the 3BC algorithm, which makes SEEP protocol better than SET by simplifying the complexity of dual signature. Some basic concepts of encryption and decryption, ECC, and SET are introduced in a later section. 3BC algorithm and the structure of SEEP protocol are proposed and defined in a following section. The advantages of SEEP protocol vs. SET are discussed in the conclusion.

Basic Concepts

Encryption and Decryption Algorithm

As shown in Figure 1, the user A computes a new key $k_A(k_B P)$ by multiplying the user B’s public key by the user A’s private key $k_A$. The user A encodes the message by using this key and then transmits this cipher text to user B. After receiving this cipher text, the user B decodes with the key $k_B(k_A P)$, which is obtained by multiplying the user A’s public key, $k_A P$ by the user B’s private key, $k_B$. Therefore, as $k_A(k_B P) = k_B(k_A P)$, we may use these keys for the encryption and the decryption (Harper, Menezes, & Vanstone, 1993).

SET (Secure Electronic Transaction) Protocol

With digital signatures, encryption for message, and digital envelope, SET offers confidentiality, data integrity, authentication, and non-repudiation over an open network. But the public key cipher algorithm, which is used in digital signature and digital envelope of SET is slow in processing data. In general, SET uses SHA and RSA for a digital signature and
Integration of Optimization Approach Based on Multiple Wordlength Operation Grouping in the AAA Methodology for Real-Time Systems: LVQ Implementation