Chapter 2.4
A SEEP (Security Enhanced Electronic Payment) Protocol Design using 3BC, ECC (F_{2^m}), and HECC Algorithm[1]

ByungKwan Lee
Kwandong University, Republic of Korea

SeungHae Yang
Kwandong University, Republic of Korea

Tai-Chi Lee
Saginaw Valley State University, USA

ABSTRACT

Unlike SET (Secure Electronic Transaction) protocol, this paper proposes a SEEP (Security Enhanced Electronic Payment) protocol, which uses ECC (Elliptic Curve Cryptosystem with F_{2^m} not F_p) (Koblitz, 1987; Harper, Menezes, & Vanstone, 1993; Miller, 1986), 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 & Lee, 2002; Cho, Shin, Lee, & 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 paper, the processing time is reduced substantially. In addition, the use of multiple signatures has some advantages, such as reducing the size of transmission data as an intermediate payment agent and avoiding the danger of eavesdropping of private keys.

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 hardly can 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, and 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 paper proposes a SEEP (Security Enhanced 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 the second section. 3BC algorithm and the structure of SEEP protocol are proposed and defined in the third section. The advantages of SEEP protocol vs. SET are concluded in the fourth section.

BASIC CONCEPTS

Encryption and Decryption Algorithm

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

Figure 1. Concept of encryption/decryption of ECC