情報保護學會論文誌
第12券 第6號, 2002. 12

# 송신자에 대한 묵시적 인증을 제공하는 하이브리드 암호 시스템

오 수 현*, 곽 진*, 원 동 호**

# Hybrid Cryptosystem providing Implicit Authentication for sender

Soo-hyun Oh*, Jin Kwak*, Dong-ho Won**

요 약

네트워크상에서 전송되는 메시지의 기밀성을 유지하기 위해 암호 시스템의 사용이 증가하고 있으며, 최근 들어 대칭키 암호 방식과 공개키 암호 방식의 장점을 결합한 하이브리드 암호 시스템이 많이 사용되고 있다. 본 논문에서는 묵시적 키 인증 제공하는 1-pass 키 분배 프로토콜, 해쉬 함수, 대칭키 암호 시스템을 이용하여 암호문을 전송한 송신자의 신분에 대한 묵시적 인증을 제공할 수 있는 새로운 하이브리드 암호 시스템을 제안하고, 대표적인 예로 Diffie-Hellman 기반 방식과 Nyberg-Ruppel 기반 방식을 설명한다. 제안하는 시스템은 기존의 하이브리드 암호 시스템과 같이 실제 메시지 암호화에는 대칭키 암호 방식을 이용하므로 효율적이고, 암호문의 수신자가 송신자의 신분을 묵시적으로 확인할 수 있다는 장점을 갖는다.

ABSTRACT

To provide the confidentiality of messages transmitted over the network, the use of cryptographic system is increasing gradually and the hybrid cryptosystem, which combines the advantages of the symmetric cryptosystem and the public key cryptosystem is widely used. In this paper, we proposes a new hybrid cryptosystem capable of providing implicit authentication for the sender of the ciphertext by means of the 1-pass key distribution protocol that offers implicit key authentication, hash function and symmetric cryptosystem. Also, we describe some examples such as the Diffie-Hellman based system and the Nyberg-Ruppel based system.

The proposed hybrid cryptosystem is an efficient more than general public key cryptosystems in the aspect of computation work and provides implicit authentication for the sender without additional increase of the communication overhead.

**Keyword :** *Hybrid cryptosystem, Implicit authentication, Key distribution protocol, Diffie-Hellman key agreement protocol, Nyberg-Rueppel key agreement protocol*

## Ⅰ. 서 론

네트워크와 통신 기술의 발전으로 인해, 전자 메일을 비롯하여 네트워크를 통한 메시지 전송이 널리 이용되고 있다. 네트워크를 통한 메시지 전송은 시간이나 비용면에서 매우 경제적인 방법이지만, 실생활의 문서 전달에 비해 제 3자에 의해 도청되거나 위·변조되기 쉽다는 문제점이 있다. 따라서, 전송하고자 하는 메시지를 제 3자로부터 보호하기 위해 암호 시스템의 사용이 증가하고 있다.

* 성균관대학교 전기전자 및 컴퓨터공학부 정보통신보호연구실({shoh, jkwak}@dosan.skku.ac.kr)
** 성균관대학교 정보통신공학부 정교수(dhwon@dosan.skku.ac.kr)

암호 시스템(Cryptographic system)이란 송신자가 키(key)를 이용하여 보내고자하는 메시지를 암호화하여 전송하면, 이에 대응하는 키를 가진 수신자만이 암호문으로부터 평문을 얻을 수 있으므로, 네트워크 상에서 전송되는 메시지에 대한 기밀성(confidentiality)을 보장할 수 있다.

암호 시스템은 사용하는 키에 따라 대칭키 암호 시스템(Symmetric cryptosystem)과 공개키 암호 시스템(Public key cryptosystem)으로 나눌 수 있다. 대칭키 암호 시스템은 송·수신자가 동일한 키를 이용하는 방식으로 메시지의 암·복호화가 효율적이라는 장점이 있다. 그러나 송·수신자간에 암호 통신을 하기 위해 반드시 사전에 동일한 키를 설정하는 키 분배 과정이 필요하다는 단점이 있다.

반면에, 공개키 암호 시스템은 송·수신자가 서로 다른 키를 사용하는 방식으로, 메시지의 암호화에 사용되는 키는 공개하고 복호화에 사용하는 키만 비밀로 보관하는 방식이다. 이 방식은 암호화에 사용하는 키를 디렉토리와 같은 공개 장소에 공개하므로 사전에 키 분배 과정이 필요하지 않다는 장점이 있지만, 암·복호화에 많은 시간이 소요되므로 대칭키 암호 방식에 비해 비 효율적이라는 단점이 있다.

따라서, 두 암호 시스템이 갖는 장점만을 이용하여 실제 메시지의 암호화에는 효율적인 대칭키 암호 방식을 이용하고, 대칭키 암호 방식에서 사용한 암호화 키를 암호화하는 데에는 공개키 암호 방식을 이용하는 하이브리드 암호 시스템(Hybrid cryptosystem)이 널리 사용되고 있다.

또한, 기존의 공개키 암호 방식은 누구나 공개된 암호화 키를 이용하여 암호문을 생성할 수 있으므로 암호문의 송신자에 대한 인증(authentication)을 제공할 수 없고 수신한 메시지의 내용에 대한 무결성(integrity)도 보장할 수 없었다.

최근에 활발히 연구되고 있는 안전성 증명이 가능한 공개키 암호 시스템들은 이러한 공개키 암호 시스템의 단점을 해결하기 위해, 대부분이 효율적인 하이브리드 구조를 갖고 있으며 암호문에 평문에 대한 무결성을 검사할 수 있는 검증 정보를 포함하고 있다.

그러나, 지금까지 제안된 대부분의 하이브리드 암호 시스템들은 메시지 암호화에 사용하는 암호화 키를 랜덤하게 선택하므로 송신자의 신분에 대한 어떠한 인증도 제공하지 않는다.

본 논문에서는 묵시적 키 인증(implicit key authentication)을 제공하는 1-pass 키 분배 프로토콜(1-pass key distribution protocol)을 이용하여 암호문 송신자의 신분에 대한 묵시적 인증을 제공하는 하이브리드 암호 시스템을 제안한다.

제안하는 암호 시스템은 하이브리드 구조이므로 계산량 면에서 효율적이고, 1-pass 키 분배 프로토콜을 이용하므로 키 분배를 위한 통신량의 추가없이 암호문의 수신자의 신분에 대한 묵시적 인증을 제공할 수 있다는 장점이 있다.

## II. 연구 배경

1976년 Diffie-Hellman[4]에 의해 공개키 암호 시스템의 개념이 발표된 이후, RSA[16], ElGamal[5]과 같은 여러 종류의 공개키 암호 시스템이 제안되었다.

공개키 암호 시스템은 별도의 키 분배 과정을 필요로하지 않으므로 인터넷과 같은 개방형 네트워크에 적용하기 적합한 방식이지만, 암·복호화에 많은 양의 계산을 요구하고 아직까지 그 안전성에 대한 정확한 증명이 이루어지지 않았다는 등의 문제점이 있다. 이러한 공개키 암호 시스템의 문제를 해결하기 위해 공개키 암호 시스템은 메시지 암호화에 사용되는 키를 암호화하는데만 사용하고, 실제 메시지는 대칭키 암호 방식으로 암호화하는 하이브리드 암호 시스템이 널리 사용되고 있다.

또한, 공개키 암호 시스템에 관한 주요 연구 동향은 안전성 증명이 가능한 암호 시스템을 개발하는 것이다. 즉, 기존의 공개키 암호 시스템들의 안전성이 주로 경험적인 안전성이므로 새로운 공격 방법에 대해서는 그 안전성을 보장할 수 없다는 단점이 있다. 따라서, 최근에는 기존의 공개키 암호 시스템을 선택 암호문 공격에 대한 안전성(CCS : Chosen Ciphertext Security)을 만족하는 공개키 암호 시스템으로 변형하는 방식에 대한 연구가 활발히 진행중이다.

이러한 변형 방식은 각각의 공개키 암호 시스템을 대상으로 하는 방식과 임의의 암호 시스템에 적용 가능한 방식으로 나눌 수 있으며, [7,8,12~15] 등에서 제안되었다. 지금까지 제안된 대부분의 CCS를 만족하는 공개키 암호 시스템은 공개키 암호 시스템, 대칭키 암호 시스템, 해쉬 함수 등을 이용하여 구성하며, 공개키 암호 시스템은 메시지 암호화에서 사용되는 키의 암호화에만 사용되고 대칭키 암호 시스템이 실제 메시지의 암호화를 수행하는 하이브리

드 형태를 나타내고 있다.

즉, 이러한 변형 방식들은 효율성면에서나 안전성 면에서 기존의 공개키 암호 시스템이 가지고 있는 문제점들을 해결한 방식이라 할 수 있다.

지금까지 제안된 CCS를 만족하는 공개키 암호 시스템 중, 최근에 제안된 REACT(Rapid Enhanced-security Asymmetric Cryptosystem Transform)의 암·복호화 과정은 다음과 같다.[12]

**[암호화 과정]**

① 송신자는 랜덤 수 $R$을 선택하고 수신자의 공개키로 암호화하여 암호문 $C_1 = E_{pk}(R)$을 생성한다.

② 송신자는 선택한 랜덤 $R$을 의사 난수 생성기에 입력하여 메시지 암호화에 사용할 세션키 $K = G(R)$를 계산한다.

③ 송신자는 키 $K$를 이용하여 메시지 $m$을 대칭키 암호 방식으로 암호화한다.

$$C_2 = E_K^{sym}(m)$$

④ 송신자는 검증 정보를 생성하기 위해 암호문 $C_1$, $C_2$와 초기 랜덤 수 $R$, 평문 $m$에 대한 해쉬 값 $C_3 = H(C_1, C_2, R, m)$를 계산한다.

⑤ 수신자에게 $m$에 대한 암호문 $(C_1, C_2, C_3)$를 전송한다.

**[복호화 과정]**

① 수신자는 암호문 $C_1$을 자신의 비밀키를 이용하여 복호하여 랜덤 수 $R = D_{sk}(C_1)$을 얻는다.

② 수신자는 $R$을 의사 난수 생성기에 입력하여 메시지 암호화에 사용된 세션키 $K = G(R)$를 계산한다.

③ 수신자는 키 $K$를 이용하여 암호문 $C_2$로부터 평문 $m = D_K^{sym}(C_2)$을 복호한다.

④ 수신한 암호문 $C_1$, $C_2$와 계산한 $R$, $m$을 이용하여 $C_3 = H(C_1, C_2, R, m)$인지 확인하여 메시지의 변경 여부를 확인하고, 일치하는 경우에만 $m$을 정당한 평문으로 출력한다.

## Ⅲ. 제안하는 하이브리드 암호 시스템

### 3.1 제안하는 암호 시스템의 개요

제안하는 하이브리드 암호 시스템은 메시지 암호화에 사용하는 세션키를 전송하기 위한 키 전송 시스템, 랜덤한 수를 입력받아 메시지 암호화 키를 생성하는 의사 난수 생성기, 실제 메시지의 암·복호화에 사용하는 대칭키 암호 시스템, 암호문의 무결성을 보장하는 검증 정보 생성하는데 사용하는 해쉬 알고리즘으로 구성된다.

#### 3.1.1 키 전송 시스템( $KTS$)

키 전송 시스템 $KTS$(Key Transport System)는 $KPG$, $SKG$, $SKR$의 세 개의 알고리즘으로 구성되며, 각 알고리즘은 다음과 같다.

$$KTS = (KPG, SKG, SKR)$$

- $KPG(1^k)$ : 공개키 암호 시스템에서 사용하는 사용자의 키 쌍을 생성하는 알고리즘(Key-Pair Generation algorithm)으로, 안전성 계수 k를 입력으로 랜덤한 공개키-비밀키 쌍 $(pk, sk)$를 출력하는 확률론적 알고리즘. (단, $k \in N$)
- $SKG(pk_R, sk_S, R, r)$ : 메시지 암호화에 사용하는 세션키를 생성하는 알고리즘(Session Key Generation algorithm)으로, 수신자의 공개키 $pk_R$과 송신자의 비밀키 $sk_S$ 그리고 랜덤 수 $R$, $r$을 입력으로 하여 암호화된 세션키 $\Sigma$를 출력하는 확률론적 알고리즘.
- $SKR(sk_S, pk_R, \Sigma)$: 메시지 암호화에 사용된 세션키를 복구하는 알고 알고리즘(session Key Recovery algorithm)으로, 수신자의 비밀키 $sk_S$와 송신자의 공개키 $pk_R$ 그리고 암호화된 정보 $\Sigma$를 입력으로, 랜덤 수 $R$을 출력하는 결정론적 알고리즘.

#### 3.1.2 의사 난수 생성기( $G$)

의사 난수 생성기 $G$는 송신자가 선택한 랜덤 수 $R$을 입력으로 하여 실제 메시지 암호화에 사용하는 세션키 $K = G(R)$를 생성하는 알고리즘으로 SHA-1[19], MD5[9]등과 같은 해쉬 함수를 이용하여 구현할 수 있다.

#### 3.1.3 대칭키 암호 시스템( $\Pi$ )

의사 난수 생성기에서 생성된 세션키 $K$를 이용하여 실제 메시지의 암·복호화를 수행하는 대칭키 암호 시스템으로, exclusive-OR 연산을 수행하거나 AES (Advanced Encryption Standard)[6]와 같은 블록 암호 알고리즘을 이용하여 구현할 수 있다.

#### 3.1.4 해쉬 함수( $H$ )

수신한 암호문의 변경 여부를 확인할 수 있는 검증 정보를 생성하는데 사용하는 알고리즘으로, 키 전송 시스템의 출력 값, 대칭키 암호 시스템의 출력 값, 초기 랜덤 수, 평문을 입력으로 하여 이에 대한 해쉬 값을 출력하는 알고리즘이다. SHA-1, MD5와 같은 해쉬 알고리즘을 이용하여 구현할 수 있다.

### 3.2 암 · 복호화 과정

제안하는 암호 시스템의 암 · 복호화 과정은 다음과 같다.([그림 1] 참조)

**[암호화 과정]**

① 송신자는 랜덤 수 $R$, $r$을 선택하고 수신자의 공개키, 송신자의 비밀키를 이용하여 $C_1$을 계산한다.

$$C_1 = R \oplus KAP(pk_R,\ sk_S,\ R,\ r)$$

단, $KAP()$는 묵시적 키 인증을 제공하는 1-pass 키 분배 프로토콜이다.

② 송신자는 선택한 랜덤 수 $R$을 의사 난수 생성기에 입력하여 메시지 암호화에 사용할 세션키 $K = G(R)$를 계산한다.

③ 송신자는 $K$를 대칭키 암호 방식 $ENC$의 키로 사용하여 메시지 $m$을 암호화하여 암호문 $C_2$를 생성한다.

$$C_2 = ENC_K(m)$$

④ 송신자는 메시지의 변경 여부를 확인할 수 있는 검증 정보를 생성하기 위해, $C_1$, $C_2$와 초기 랜덤 수 $R$, 평문 $m$을 이용하여 해쉬 값 $C_3$를 계산한다.

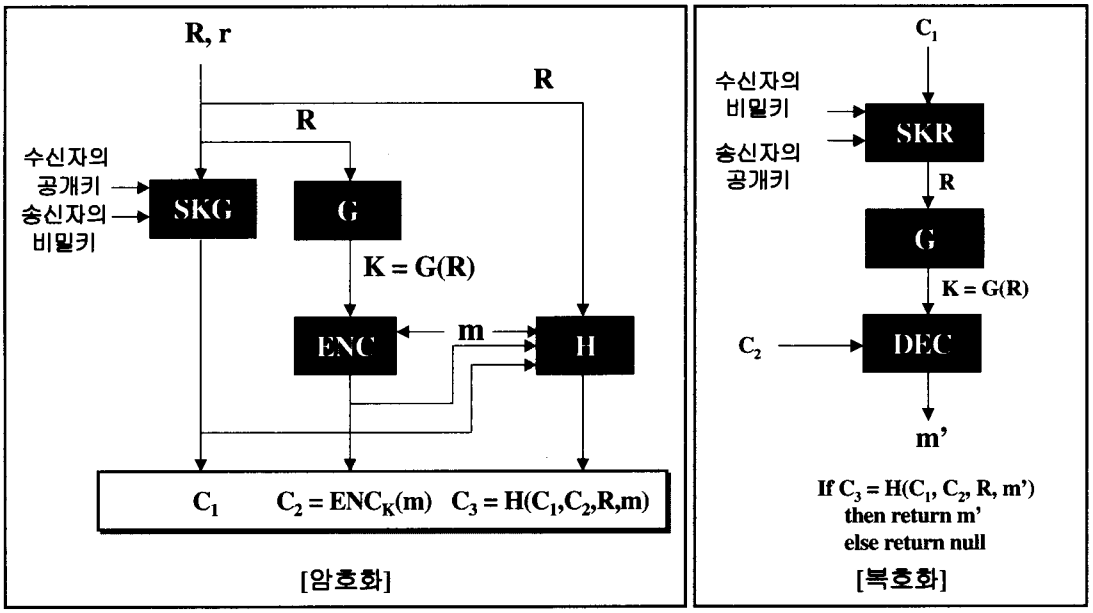
$$C_3 = H(C_1,\ C_2,\ R,\ m)$$

⑤ 송신자는 수신자에게 $m$에 대한 암호문 ($C_1$, $C_2$, $C_3$)를 전송한다.

**[복호화 과정]**

① 수신자는 자신의 비밀키와 송신자의 공개키를 이용하여 $C_1$으로부터 랜덤 수 $R$을 계산한다.

② ①에서 계산한 $R$을 의사 난수 생성기에 입력하




- SKG : 세션키 생성 알고리즘(Session Key Generation algorithm)
- ENC : 대칭키 암호시스템의 암호화 알고리즘
- G : 의사 난수 생성기
- SKR : 세션키 복구 알고리즘(Session Key Recovery algorithm)
- DEC : 대칭키 암호시스템의 복구화 알고리즘
- H : 해쉬 함수

[그림 1] 제안하는 하이브리드 암호 시스템의 암호화/복호화 과정

여 메시지 암호화에 사용된 세션키 $K=G(R)$를 획득한다.

③ ②에서 얻은 $K$를 이용하여 암호문 $C_2$로부터 평문 $m$을 계산한다.

$$m = DEC_K(C_2)$$

④ 수신한 암호문 $C_1$, $C_2$와 계산한 $R$, $m$을 이용하여 $C_3 = H(C_1, C_2, R, m)$인지 확인하고, 일치하는 경우에만 $m$을 정당한 평문으로 출력한다.

## Ⅳ. Some examples

### 4.1 Diffie-Hellman 기반 시스템

Diffie-Hellman은 [4]에서 공개키 암호 시스템의 개념을 처음으로 제안하고 이산대수 문제에 기반한 키 분배 프로토콜을 제안하였다. 이들이 제안한 Basic Diffie-Hellman 프로토콜은 2-pass 키 분배 프로토콜이고 매 세션마다 서로 다른 세션키가 생성된다는 장점이 있지만, 세션키 생성에 랜덤하게 선택한 수들을 이용하므로 프로토콜에 참여하는 사용자들에 대한 어떠한 인증도 제공할 수 없다는 문제점이 있다. 이러한 문제점을 해결하기 위해, 랜덤 수 대신 사용자들의 고정된(static) 비밀키를 이용하는 Static Diffie-Hellman 프로토콜이 제안되었으나, 이 방식은 두 사용자사이에 항상 동일한 세션키가 설정된다는 단점이 있다.

본 논문에서는 1-pass 프로토콜이면서 양방향 묵시적 인증을 제공하기 위해, Basic Diffie-Hellman 프로토콜과 Static Diffie-Hellman 프로토콜의 장점을 결합한 ANSI X9.42[1]의 dhHybridOneFlow 프로토콜을 이용하여 암호 시스템을 구성한다.

ANSI X9.42의 dhHybridOneFlow 프로토콜은 세션키 생성에 필요한 통신 회수는 1이지만 양방향 묵시적 키 인증을 제공하고, 매 세션마다 세션키가 바뀌는 key freshness를 제공한다는 장점이 있다. Diffie-Hellman 키 분배 프로토콜에 기반한 하이브리드 암호 방식의 시스템 파라미터와 암·복호화 과정은 다음과 같다.([그림 2] 참조)

**[시스템 파라미터]**

- $p$ : $2^{511} < p < 2^{512}$인 큰 소수
- $g$ : $Z_p$상의 원시원소 ( $g^{p-1} \equiv 1 \bmod p$)
- $x_{A,B}$ : 사용자 $A$, $B$의 비밀키
- $y_{A,B}$ : 사용자 $A$, $B$의 공개키
- $G$ : 의사 난수 생성기
- $H$ : 해쉬 함수
- $E_k()/D_k()$ : 키 $k$를 이용하는 대칭키 암·복호화 알고리즘

**[암호화]**

① 송신자 $A$는 메시지 $m$에 대한 암호문을 생성하기 위해, 랜덤 수 $R$, $r \in Z_{p-1}$을 선택하고 $t_A$를 계산한다.

$$t_A \equiv g^r \bmod p$$

② 송신자 $A$는 선택한 랜덤 수 $R$, 수신자의 공개키, 자신의 비밀키를 이용하여 $C_1$을 생성한다.

$$C_1 \equiv R \oplus H(y_B^{x_A} \| y_B^r)$$

③ 송신자 $A$는 랜덤 수 $R$을 의사 난수 생성기에 입력하여 메시지 암호화에 사용할 세션키 $K=G(R)$를 계산한다.

④ 송신자 $A$는 세션키 $K$를 이용하여 메시지 $m$에 대한 암호문 $C_2$를 생성한다.

$$C_2 = E_K(m)$$

⑤ 송신자 $A$는 해쉬 함수 $H$를 이용하여 암호문에 대한 검증정보 $C_3$를 생성한다.

$$C_3 = H(C_1, C_2, t_A, m)$$

⑥ 송신자 $A$는 수신자 $B$에게 $m$에 대한 암호문 $C=(t_A, C_1, C_2, C_3)$를 전송한다.

**[복호화]**

① 암호문 $C=(t_A, C_1, C_2, C_3)$를 수신한 수신자 $B$는 자신의 비밀키와 송신자의 공개키를 이용하여 랜덤 수 $R$ 값을 계산한다.

$$R = C_1 \oplus H(y_A^{x_B} \| t_A^{x_B})$$

② 수신자 $B$는 ①에서 얻은 랜덤 수 $R$을 이용하여 메시지 암호화에 사용한 세션키 $K=G(R)$를 계

| 송신자 A | | 수신자 B |
|---|---|---|
| $m$ : 평문<br>$R, r \in Z_{p-1}$ 선택하고 다음을 계산<br><br>$t_A \equiv g^r \bmod p$<br>$C_1 \equiv R \oplus H(y_B^{x_A} \| y_B^r)$<br>$K = G(R)$<br>$C_2 = E_K(m)$<br>$C_3 = H(C_1, C_2, t_A, m)$ | $C = (t_A, C_1, C_2, C_3)$<br>----------> | $R = C_1 \oplus H(y_A^{x_B} \| t_A^{x_B})$<br>$K = G(R)$<br>$m = D_K(C_2)$<br>If $C_3 = H(C_1, C_2, t_A, m)$<br>return m. |

〔그림 2〕 Diffie-Hellman 기반 하이브리드 암호 시스템

산한다.

③ 수신자 $B$는 세션키 $K$를 이용하여 암호문 $C_2$로부터 평문 $m$을 복호한다.

$$m = D_K(C_2)$$

④ 수신자 $B$는 $C_3 = H(C_1, C_2, t_A, m)$인지 확인하고 성립할 경우에만 $m$을 정당한 평문으로 출력한다.

Diffie-Hellman 기반 암호 시스템에서 $y_B^{x_A}$값은 모든 세션에 동일한 값이므로 자주 암호 통신을 하는 상대방에 대해 사전 계산하여 저장해두는 것도 가능하다. 그리고 $y_B^{x_A}$ 값이 노출되더라도 매 세션마다 선택한 랜덤 수 $r$이 포함되므로 암호문의 안전성에는 영향을 주지 않는다.

또한, 수신자는 세션키를 생성하는데 사용한 초기 랜덤 수 $R$을 계산하기 위해, 자신의 비밀키와 송신자의 공개키를 이용하므로 송신자의 신분을 묵시적으로 인증할 수 있다. 즉, 송신자가 아닌 제 3자는 정당한 암호문을 생성할 수 없음을 확인할 수 있게 된다.

### 4.2 Nyberg-Rueppel 기반 시스템

K. Nyberg와 R. Ruppel은 〔10, 11〕에서 처음으로 이산대수 문제를 이용하는 메시지 복원형 디지털 서명 방식(Message recovery digital signature scheme)을 제안하였다. 그리고 R. Ruppel과 P. C. Oorschot는 K. Nyberg와 R. Ruppel의 서명방식을 이용하여 양방향 묵시적 키 인증을 제공하는 1-pass 키 분배 프로토콜을 제안하였다.〔17〕

이 방식은 기존의 Diffie-Hellman 방식이 양방향 묵시적 키 인증을 제공하기 위해 2-pass의 통신량을 필요로 하는 것에 비해, 한번의 통신으로 양방향 묵시적 키 인증을 제공할 수 있고, 키 토큰에 타임스탬프(time stamp)나 일련 번호(sequence number)를 포함하는 경우에 수신자에게 송신자의 신분에 대한 명시적 개체 인증(explicit entity authentication)을 제공한다는 장점이 있다.

따라서, 제안하는 하이브리드 암호 시스템의 키 전송 시스템에 Nyberg-Ruppel의 키 분배 방식을 적용하면 송신자의 신분에 대한 인증을 제공할 수 있게 된다.

Nyberg-Ruppel 키 분배 방식에 기반한 하이브리드 암호 시스템의 시스템 파라미터는 Diffie-Hellm 기반 방식과 동일하며 암·복호화 과정은 다음과 같다.(〔그림 3〕 참조)

**[암호화]**

① 송신자 $A$는 메시지 $m$에 대한 암호문을 생성하기 위해, 랜덤 수 $R, r \in Z_{p-1}$을 선택하고 $e, y$ 값을 계산한다.

$$e \equiv g^{R-r} \bmod p$$
$$y = r + x_A e \bmod p$$

② 송신자 $A$는 선택한 랜덤 수 $R$, 수신자의 공개키를 이용하여 $C_1$을 생성한다.

$$C_1 \equiv R \oplus H(y_B^R)$$

③ 송신자 $A$는 랜덤 수 $R$을 이용하여 메시지 암호화에 사용할 세션키 $K = G(R)$를 계산한다.

| 송신자 A | | 수신자 B |
|---|---|---|
| m : 평문<br>$R,\ r \in Z_{p-1}$ 선택하고<br>다음을 계산<br><br>$e \equiv g^{R-r} \bmod p$<br>$y = r + x_A e \bmod p$<br>$C_1 \equiv R \oplus H(y_B^R)$<br>$K = G(R)$<br>$C_2 = E_K(m)$<br>$C_3 = H(C_1, C_2, e, y, m)$ | $C = (e, y, C_1, C_2, C_3)$<br>----------> | $R = C_1 \oplus H((g^y \cdot y_A^{-e} \cdot e)^{x_B} \bmod p)$<br>$K = G(R)$<br>$m = D_K(C_2)$<br>If $C_3 = H(C_1, C_2, e, y, m)$<br>return m. |

〔그림 3〕 Nyberg-Rueppel 기반 하이브리드 암호 시스템

④ 송신자 $A$는 세션키 $K$를 이용하여 메시지 $m$에 대한 암호문 $C_2$를 생성한다.

$$C_2 = E_K(m)$$

⑤ 송신자 $A$는 해쉬 함수 $H$를 이용하여 암호문에 대한 검증정보 $C_3$를 생성한다.

$$C_3 = H(C_1, C_2, e, y, m)$$

⑥ 송신자 $A$는 수신자 $B$에게 $m$에 대한 암호문 $C = (e, y, C_1, C_2, C_3)$를 전송한다.

**[복호화]**

① 암호문 $C = (e, y, C_1, C_2, C_3)$를 수신한 수신자 $B$는 자신의 비밀키와 송신자의 공개키를 이용하여 다음과 같이 랜덤 수 $R$ 값을 계산한다.

$$R = C_1 \oplus H((g^y \cdot y_A^{-e} \cdot e)^{x_B} \bmod p)$$

② 수신자 $B$는 ①에서 획득한 랜덤 수 $R$을 이용하여 메시지 암호화에 사용한 세션키 $K = G(R)$를 계산한다.

③ 수신자 $B$는 세션키 $K$를 이용하여 암호문 $C_2$로부터 평문 $m$을 복호한다.

$$m = D_K(C_2)$$

④ 수신자 $B$는 $C_3 = H(C_1, C_2, e, y, m)$인지 확인하여 성립할 경우에만 $m$을 정당한 평문으로 출력한다.

Nyberg-Ruppel 키 분배 방식에 기반한 암호 시스템에서는 $e, y$가 메시지 $m$에 대한 디지털 서명의 역할을 한다. 따라서, 재전송 공격(replay attack)을 막을 수 있도록 타임 스탬프나 일련 번호를 암호문에 포함한다면 송신자에 대한 명시적 개체 인증을 제공할 수도 있다.

## V. 안전성 분석

### 1) 정당한 사용자로 위장하여 암호문을 전송하는 공격에 대한 안전성

일반적인 공개키 암호 시스템과 달리, 제안하는 하이브리드 암호 시스템은 메시지 암호화에 사용하는 세션키를 생성하기 위해 암호문을 전송하는 송신자의 비밀키를 이용한다. 즉, 송신자만이 해당 암호문을 생성할 수 있다는 묵시적 인증을 제공하게 된다.

따라서, 사용자 $A$의 비밀키 $x_A$를 알지 못하는 공격자는 $A$가 보낸 암호문으로 위장하여 정당한 형태의 암호문을 전송할 수 없게 된다.

Diffie-Hellman 기반 시스템에서 공격자가 사용자 $A$가 보낸 암호문으로 위장하여 암호문을 전송하기 위해서는, 사용자 $A$의 공개키 $y_A = g^{x_A} \bmod p$와 수신자 $B$의 공개키 $y_B = g^{x_B} \bmod p$로부터 $g^{x_A x_B} \bmod p$ 값을 계산해야 한다. 이것은 유한체상의 Diffie-Hellman 문제와 동치이며, 따라서 공격자가 사용자 $A$로 위장하여 암호문을 전송하는 것을 Diffie-Hellman 문제를 해결하는 것만큼 어려운 일이다.

또한, Nyberg-Ruppel 기반 시스템에서 공격자가 사용자 $A$가 보낸 암호문으로 위장하여 암호문을

전송하기 위해서는, 디지털 서명 값 $(e, y)$를 계산해야 한다. 그러나 사용자 $A$의 비밀키 $x_A$를 알지 못하는 공격자가 정당한 형태의 $(e, y)$ 값을 계산하는 것은 계산상 불가능하다. 따라서, 공격자가 다른 사용자로 위장하여 정당한 형태의 암호문을 전송하는 것은 계산적으로 불가능하다.

**2) 송신자의 비밀키가 노출되는 경우의 안전성**

공개키 암호 시스템에서는 수신자의 비밀키가 노출되지 않는 한 암호문의 송신자를 포함한 다른 사용자들은 암호문을 복호할 수 없다.

제안하는 암호 시스템에서는 메시지 암호화에 사용된 키를 암호화하기 위해 수신자의 공개키뿐만 아니라 송신자의 비밀키가 사용된다. 그러나, 송신자의 비밀키가 노출된다 할지라도 제 3자는 세션키 생성에 사용한 랜덤 수를 모르므로 암호문으로부터 평문을 획득할 수 없게 된다.

Diffie-Hellman 기반 시스템에서 송신자의 비밀키가 노출되는 경우, 누구든지 송신자의 비밀키와 수신자의 공개키를 이용하여 $y_B^{x_A}$를 구할 수는 있지만, 세션키 암호화에 사용된 랜덤 수 $r$이나 수신자의 비밀키를 모르는 제 3자는 $R$값을 복원할 수 없다. 즉, 랜덤 수 $r$과 수신자의 비밀키 $x_B$를 모르는 제 3자가 $y_B^r = t_A^{x_B} = g^{r \cdot x_B} \bmod p$를 구하는 것은 Diffie-Hellman 문제와 동치이다.

또한, Nyberg-Ruppel 기반 시스템에서 송신자 $A$의 비밀키 $x_A$가 노출되면 누구든지 전송정보 $(e, y)$로부터 $r = y - x_A \cdot e \bmod p$와 $g^R = e \cdot g^r \bmod p$를 계산할 수 있다.

그러나, 세션키 생성에 사용된 랜덤 수 $R$을 복구하기 위해서는 $g^R$과 $y_B$로부터 $y_B{}^R = g^{R \cdot x_B} \bmod p$를 구해야 하며, 이것은 Diffie-Hellman 문제의 어려움과 동치이다. 따라서, 송신자의 비밀키가 노출되더라도 수신자를 제외한 다른 사람들이 암호문을 복호하는 것은 계산상 불가능하다.

**3) 이전의 세션키가 노출되는 경우의 안전성**

암호 시스템의 사용에 있어 매 세션마다 동일한 키를 이용하여 암호문을 생성하는 경우에, 한 세션의 키만 노출되면 이전의 모든 암호문이 공개되므로 매 세션마다 서로 다른 키를 사용하여 메시지를 암호화하는 것이 바람직하다.

제안하는 암호 시스템의 키 전송 시스템은 세션마다 서로 다른 랜덤 수를 선택하여 암호화하여 전송하므로, 이전의 세션키가 노출되더라도 현재의 암호문의 안전성에는 영향이 없다. 또한, 세션키 생성에 사용한 랜덤 수 $R$이 노출되더라도 해당 세션 외에 다른 세션의 암호문은 여전히 안전하다.

Diffie-Hellman 기반 시스템에서 과거 세션의 암호문이 $C_1' \equiv R' \oplus H(y_B^{x_A} \| y_B^{r'})$이고 현재 세션의 암호문이 $C_1 \equiv R \oplus H(y_B^{x_A} \| y_B^{r})$이라 하자.

이때, 과거 세션의 랜덤 수 $R'$가 노출되는 경우, 누구든지 쉽게 $C_1' \oplus R' = H(y_B^{x_A} \| y_B^{r'})$을 계산할 수 있지만, $r \neq r'$이면 이를 이용하여 $C_1$으로부터 현재 세션의 랜덤 수 $R$을 구하는 것은 불가능하다. 즉, 매 세션마다 서로 다른 난수를 이용한다면 과거의 세션키나 세션키 생성에 사용된 랜덤 수가 노출되더라도 현재 세션의 암호문의 안전성에는 아무런 영향이 없다.

또한, Nyberg-Rueppel 기반 시스템에서도 세션키 생성에 사용하는 랜덤 수 $R$을 매 세션마다 다르게 사용하면, 과거의 세션키나 랜덤 수가 노출될지라도 다른 세션의 암호문의 안전성에는 아무런 영향을 미치지 않는다.

따라서, 제안하는 하이브리드 암호 시스템은 각 세션마다 다른 랜덤 수를 사용하는 경우에, 이전의 세션키가 노출된다 하더라도, 다른 세션의 암호문의 안전성에는 영향을 미치지 않는다.

**4) 전송중인 암호문을 변경하려는 공격에 대한 안전성**

RSA 공개키 암호 시스템은 multiplicative 특성으로 인해, 공격자가 전송중인 암호문으로부터 전체 평문을 얻을 수는 없지만 정당한 형태의 다른 암호문으로 변경하는 것이 가능하다. 이러한 암호 시스템을 조작 가능한(malleable) 암호 시스템[3]이라 하며, 이러한 RSA의 문제점을 해결하기 위해 암호문의 무결성을 보장하는 검증 정보를 추가하는 OAEP (Optical Asymmetric Encryption)[2]가 제안되었다.

본 논문에서 제안하는 하이브리드 암호 시스템에서도 암호문의 무결성을 검증할 수 있는 해쉬 값이 암호문에 포함되므로, 공격자가 전송중인 암호문을 드러나지 않게 변경하는 것은 불가능하다.

즉, 수신자는 암호문을 복호하고 검증 정보의 정당성을 확인한 후에 정당한 경우에만 평문을 받아들이므로, 공격자가 전송중인 암호문을 변경하기 위해

서는 검증정보인 해쉬 값도 변경해야 한다. 그러나, 해쉬 값을 계산하기 위해서는 초기 랜덤 수와 평문 $m$이 필요하므로, 공격자가 정당한 검증 정보를 생성하는 것은 불가능하다.

따라서, 제안하는 하이브리드 암호 시스템은 조작 불가능(non-malleable)하다.

## Ⅵ. 결 론

최근 들어 암호 시스템의 사용이 증가함에 따라, 대칭키 암호 방식과 공개키 암호 방식의 장점을 결합한 하이브리드 암호 시스템이 널리 사용되고 있다.

본 논문에서는 기존의 하이브리드 암호 시스템과 달리, 묵시적 키 인증을 제공하는 1-pass 키 분배 프로토콜을 이용하여 송신자의 신분에 대한 묵시적 인증을 제공할 수 있는 효율적인 하이브리드 암호 시스템을 제안하고 구체적인 프로토콜을 설명하였다. 제안하는 시스템은 dhHybridOneFlow 프로토콜이나 Nyberg-Ruppel 키 분배 프로토콜과 같은 1-pass 키 분배 프로토콜과 대칭키 암호 시스템, 난수 생성기, 해쉬 함수 등을 이용하여 구현할 수 있다. 제안하는 암호 시스템은 하이브리드 방식이므로 계산량 면에서 효율적이고, 송신자의 신분에 대한 묵시적 인증을 제공하므로 제 3자가 송신자로 위장하여 메시지를 보내는 것이 불가능하다. 또한, 송신자의 비밀키가 노출되더라도 지정된 수신자 외에 다른 사람은 암호문으로부터 평문을 얻을 수 없고, 한 세션의 세션키나 랜덤 수가 노출되더라도 다른 세션의 암호문의 안전성에는 영향을 주지 않는다. 그리고, 메시지의 무결성을 검사할 수 있는 검증 정보를 포함하므로 제 3자가 암호문을 변경하는 것이 불가능하다.

제안하는 암호 시스템은 네트워크 상에서 전송되는 메시지에 대해 기밀성 및 무결성을 제공해야 하는 여러 응용 분야에 효율적으로 사용될 수 있을 것이다. 또한, 본 논문에서 설명한 dhHybridOneFlow 프로토콜이나 Nyberg-Ruppel 키 분배 프로토콜 외에 다른 임의의 묵시적 키 인증을 제공하는 1-pass 키 분배 프로토콜을 이용하여 구현하는 것이 가능하다.

## 참 고 문 헌


[1] ANSI X9.42, "Agreement of symmetric Key on Using Diffie-Hellman Cryptography", 2001.

[2] M. Bellare, P. Rogaway, "Optimal Asymmetric Encryption", Advances in Cryptology-Eurocrypto 94.

[3] M. Bellare, A. Sahai, "Non-Malleable Encryption : Equivalence between Two Notions, And an Indistinguishability -Based Charaterization", Crypto 99.

[4] W. Diffie, M. E. Hellman, "New directions in cryptography", IEEE Transaction on Information Theory, IT-22, 6, pp. 644 ~654, 1976.

[5] T. ElGamal, "A public key crypto system and a signature scheme based on discrete logarithms", IEEE Trans, info, Theory, Vol. 31, pp. 469~472, 1985.

[6] FIPS-197, "Advanced Encryption Standard", 2001.

[7] E. Fujisaki and T. Okamoto, "How to Enhance the Security of Public-Key Encryption at Minimun cost", PKC'99.

[8] E. Fujisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Scheme", Advances in Cryptology-Crypto'99.

[9] Internet Engineering Task Force (IETF) RFC 1321, "Message Digest 5(MD5)".

[10] K. Nyberg, R.A. Rueppel, "A new signature scheme based on DSA giving message recovery", Proc. 1st ACM Conf. on Comput. Commun. Security, pp. 58~61, November 1993.

[11] K. Nyberg, R. Rueppel, "Meessage recovery for signature schemes based on the discrete logarithm problem", Advances in Cryptology-Eurocrypt '94, Springer-verlag, LNCS 950, 1994.

[12] T. Okamoto and D. Pointcheval, "REACT : Rapid Enhanced-security Asymmetric Cryptosystem Transform", RSA '01.

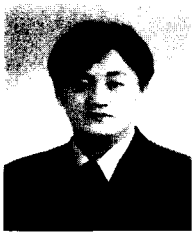
[13] T. Okamoto and D. Pointcheval "OCAC : an Optimal Conversion for Asymmetric Crptosystems", P1363.

[14] D. Pointcheval, "HD-RSA : Hybrid De-

pendent RSA - a New Public key Encryption Scheme", IEEE P1363
[15] D. Pointcheval, "New Public key Cryptosystem based on the Dependent-RSA Problems", Advances in Cryptology-Eurocrypt'99
[16] R. Rivest, A. Shamir and L. Adleman, A method of obtaining digital signature and public key cryptosystem", ACM Communication 21, No. 2, pp. 120~126, 1978.
[17] R. A. Rueppel, P. C. van Oorschot, "Modern Key Agreement Techniques", Computer Communications, 1994, pp. 458~465.
[18] B. Schneier, Applied Cryptography, John Wiley & Sons, Inc., 1994.
[19] "Secure hash standard", National Bureau of Standards FIPS Publication 180, 1993.

## 〈著者紹介〉

**오 수 현 (Soo-Hyun Oh) 학생회원**
1998년 2월 : 성균관대학교 정보공학과 졸업(공학사)
2000년 2월 : 성균관대학교 대학원 전기전자 및 컴퓨터 공학부 졸업(공학석사)
2000년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 박사 과정



**곽 진 (Jin Kwak) 학생회원**
2000년 8월 : 성균관대학교 생물기전공학과 졸업(공학사)
2001년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 석사 과정

**원 동 호 (Dong-Ho Won) 정회원**
성균관대학교 전자공학과 졸업 (학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구소 전임연구원
1992년~1994년 : 성균관대학교 교학처장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
1999년~2001년 : 성균관대학교 전기전자 및 컴퓨터공학부장 정보통신대학원장
현재 : 성균관대학교 정보통신공학부 교수, 성균관대학교 연구지원처장, 한국정보보호학회 회장, 정통부 지정 정보보호인증기술연구센터 센터장
〈관심분야〉 암호이론