韓國 컴퓨터情報學會 論文誌
第8卷 第4號, 2003. 12.

2003 8 4 2-7

타원 곡선 상의 Diffie-Hellman 기반 하이브리드 암호 시스템

정 경 숙*, 정 태 충**

Hybrid Cryptosystem based on Diffie-Hellman over Elliptic Curve

Kyoungsook Jung*, TaeChoong Chung**

요 약

본 논문에서는 타원 곡선 상에서의 Diffie-Hellman 기반의 하이브리드 암호 시스템을 제안하고, 구체적인 프로토콜을 설계하였다. 본 논문에서 제안하는 하이브리드 암호 시스템은 기존 하이브리드 시스템과 달리, 송신자와 수신자에 대한 함축적 키 인증성을 제공하는 효율적인 하이브리드 암호 시스템이다. 이 시스템은 암호학적으로 안전한 의사 난수 생성기를 사용하여 세션키를 생성함으로써 안전성을 높였으며, 하이브리드 시스템이기때문에 공개키 시스템과 비밀키 시스템의 장단점을 보완하여 계산량 면에서 더 효율적이다. 또한 위장 공격이 불가능하며, 송신자의 비밀키가 노출되더라도 지정된 수신자 이외에는 정당한 평문을 얻을 수 없다. 그리고 세션키가 노출되더라도 다른 세션의 암호문의 안전성에는 영향을 주지 않는, 알려진 키에 대한 안전성 뿐만 아니라 상호 개체 인증과 재실행 공격에 대한 안전성도 제공한다.

Abstract

In this paper, we proposed hybrid cryptosystem of Diffie-Hellman base in Elliptic Curve, and explained for specific protocol design. The proposed system is efficient hybrid cryptosystems system that offer implicit key authentication about sender and receiver unlike existing hybrid system. This system increased safety generating session key using pseudo-random number generator by cryptographic. Because the system is hybrid system, it is more efficient in calculation amount aspect supplementing merit and fault of public key system and secret key system. Also, the system can not get right plaintext except receiver even if sender's secret key is revealed and impersonation attack is impossible. And the system offers security on known keys without influencing in safety of other session's cryptogram even if session key is exposed. And the system is provided safety about mutual entity authentication and replay attack.

▸ Keyword : hybrid cryptosystem, Elliptic curve, pseudo-random number generator

* 용인송담대학 컴퓨터소프트웨어학과 겸임 교수 ** 경희대학교 컴퓨터공학과 정교수

I. 서 론

네트워크 기술의 발달로 통신 서비스뿐만 아니라 멀티미디어 서비스, 전자 상거래 등 통신 시스템을 이용한 응용 프로그램의 개발과 서비스의 제공이 급증하면서 이용자 신분 및 정보의 노출, 송수신 데이터의 도청 및 변조, 불법적인 서비스의 이용 등 네트워크 환경에서의 보안 문제가 크게 대두되고 있다. 정보의 안전한 통신을 제공하기 위해 요구되는 보안 요소는 로그온 ID, 신분 확인, 접근 제어, 비밀성, 데이터 무결성, 패스워드 보호, 인터넷 연결망의 보호, 부인 봉쇄 등이 있다. 사용자 인증은 사용자의 정당성을 식별하는 기술로 키나 카드 등 본인만이 가지고 있는 것을 식별하는 방법, 패스워드나 비밀키 등 본인만이 알고 있는 정보를 이용하여 식별하는 방법, 지문, 음성 등으로 나눌 수 있다. 이러한 보안 요소를 기반으로 다양한 암호 시스템들이 개발되어 지고 있다.

암호 시스템(Cryptographic system)은 송신자가 전송하는 메시지를 키(key)를 이용하여 암호화하여 전송하면 수신자는 대응되는 키를 이용하여 수신한 암호문을 복호하여 평문을 얻게 된다. 키의 관리는 키의 생성(generation), 저장(store), 분배(distribution), 파기(destroy), 폐기(revoke), 등록(register) 및 해제(deregister), 등록된 키의 확인(certification) 등을 포함한다. 암호 시스템은 사용하는 키에 따라 대칭키 암호 시스템과 공개키 암호 시스템으로 나눌 수 있다.

두 암호 시스템은 각각 장단점을 가지고 있기 때문에 이들이 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.

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

본 논문에서는 암호학적으로 안전한 의사 난수 생성기에 의해 암호화에 사용되는 키를 생성함으로써 이전에 사용한 세션키를 재설정하여 공격하는 재실행 공격을 사전에 방지함으로써 시스템의 안전성을 높였다. 뿐만 아니라 이 비밀키로 타원 곡선 알고리즘에 기반한 함축적 키 인증성(implicit key authentication)[1]을 제공하는 키 분배 프로토콜(key distribution protocol)을 설계하여 암호문 송신자의 신분에 대한 함축적 인증을 제공하는 하이브리드 암호 시스템을 제안한다.

제안하는 암호 시스템은 타원 곡선 기반의 하이브리드 구조이므로 계산량 면에서 효율적이다. 또한 키 분배를 위한 통신량의 추가 없이 암호문의 수신자 신분에 대한 함축적 인증을 제공할 수 있고, 안전성도 높일 수 있다는 장점이 있다. 본 논문의 구성은 2장에서는 연구 배경인 암호 시스템의 동향과 타원 곡선 암호 시스템에 대하여 논했으며, 3장은 제안하는 하이브리드 암호 시스템에 대하여 설명하였다. 4장에서는 제안하는 암호 시스템의 안전성에 대하여 분석하였으며, 5장은 결론으로 이루어져 있다.

II. 관련 연구

1. 암호 시스템 동향

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 진행 중이다.

이러한 변형 방식은 각각의 공개키 암호 시스템을 대상으로 하는 방식과 임의의 암호 시스템에 적용하는 방식으로 나눌 수 있으며, [1~6] 등에서 제안되었다.

1) 명시적 키인증성과 같이 프로토콜의 인증성을 보장하는 요인으로 사용됨

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 하이브리드 형태를 나타내고 있다[10].

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

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

〔암호화 과정〕

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

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

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

$$C_2 = E_K^{sym}(m) \quad \cdots\cdots ①$$

④ 송신자는 검증 정보를 생성하기 위해 암호문 C_1, C_2 와 초기 랜덤수 R , 평문 m 에 대한 해쉬값 $C_3 = H(C_1, C_2, R, m)$ 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 랜덤수 $R = D_{sk}(C_1)$ 을 얻는다.

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

2. 타원 곡선 암호 시스템

타원 곡선(Elliptic Curve)에 기반한 암호 시스템은 1985년 Kobliz와 Miller에 의해 제안되었으며, 최근 들어 무선 인터넷 환경이나 스마트 카드와 같은 제한된 계산 능력을 갖는 하드 웨어에 적합한 방식으로 주목 받으면서 활발히 연구되고 있는 분야이다[7][8][9].

타원 곡선 암호 시스템은 동일한 안전성을 제공하는 유한체 상의 이산 대수 문제에 기반한 시스템에 비해 사용하는 키의 길이가 짧고 효율적이라는 장점이 있다. 본 논문에서는 타원 곡선 상에서의 Diffie-Hellman 문제[2]에 기반하여 시스템의 안전성을 보장하고자 하였다.

3. 암호 시스템의 보안 특성

3.1 함축적 키 인증

프로토콜에 참여하는 개체 A와 개체 B가 있을 때, A와 B는 공유키를 생성하는 데, A는 B 이외에 다른 어느 누구도 공유키를 생성할 수 없음을 확신할 수 있다. 이 경우는 A는 B에 대한 함축적 키 인증성(implicit key authentication)을 갖는다고 한다. 그리고 반대로, B는 A 이외에 다른 어느 누구도 공유키를 생성할 수 없음을 확신할 수 있다. 이 경우를 B는 A에 대한 함축적 키 인증성을 갖는다고 한다. 이 두 조건을 만족하는 경우에 인증된 키 합의 프로토콜(authenticated key agreement)이라 한다.

3.2 명시적 키 인증

프로토콜에 참여하는 개체 A와 개체 B가 있다. 이들 A와 B는 공유키를 생성한다. 이 때, A는 B가 실제로 공유키를 계산해 가지고 있음을 확인할 수 있을 때, B에 대한 명시적 키 인증성(explicit key authentication)을 갖는다. 그리고 반대로 B는 A가 실제로 공유키를 계산해 가지고 있음을 확인할 수 있을 경우에 A에 대한 명시적 키 인증성을 갖는다. 명시적 키 인증성은 함축적 키 인증성에 실제로 상대방이 공유키를 계산할 수 있음을 추가하는 것이다.

2) 키분배 프로토콜의 대표적 알고리즘

3.3 알려진 키에 대한 안전성

개체 A와 개체 B가 인증 및 키 합의 프로토콜에 참여할 때, 세션마다 유일한 개인키를 생성하게 되는데, 이를 세션키(session key)라 한다. 만일 이전에 다른 세션에서 공격자로부터 세션키를 공격 당해 세션키가 노출되더라도 현 프로토콜이 안전함이 보장되는 것을 알려진 키에 대한 안전성(know-key security)이라 한다.

3.4 상호 개체 인증

프로토콜에 참여하는 개체 A와 개체 B가 있다. 상호 개체 인증(mutual entity authentication)은 A는 B의 신분을, B는 A의 신분을 확인하는 과정이다. 이는 서로 다른 개체에 대한 가장을 방지하기 위해 필요한 것이다.

3.5 갱신키 확인

이전에 사용한 메시지를 재사용할 때, 이전의 키를 재설정하는 것을 재실행 공격(replay attack)이라 한다. 이 공격을 방지하기 위해 키를 새롭게 설정해야 한다. 이를 갱신키 확인(confirmation freshness of key)이라 한다.

III. 제안하는 하이브리드 암호시스템

제안하는 타원 곡선 상의 Diffie-Hellman 기반의 하이브리드 암호 시스템은 랜덤한 수를 입력 받아서 세션키를 생성하는 의사 난수 생성기와 세션키를 생성하고 전송한 후 복구하는 알고리즘, 실제 메시지를 암복호화에 사용되는 대칭키 암호 시스템, 암호문의 무결성을 보장하기 위한 해쉬 알고리즘 등으로 구성된다.

1. 의사 난수 생성기

난수 생성기(random number generator)는 통계적으로 독립적(statistically independent)이고 무편향적(unbiased)인 비트들을 생성하는 기기나 알고리즘을 말한다[11]. 의사 난수 생성기는 v 비트의 난수를 근원(seed)으로 하여 난수처럼 보이는 $u(>v)$ 비트의 의사 난수(pseudo-random number)를 생성하는 알고리즘이다. 의사 난수 생성기가 지녀야 하는 보안 요건은 seed로 이용되는 난수의 길이, 즉 v값이 매우 커서 제3자가 모든 가능한 2v개의 수를 시도해 볼 수 없게 해야 한다. 뿐만 아니라 의사 난수 생성기에 의해서 생성되는 의사 난수는 진정한 난수와 통계적으로 구별할 수 있어야 하며, 이미 출력된 여러 의사 난수들이 주어졌을 때, 다음에 출력될 의사 난수를 예측하는 것이 불가능해야 한다.

select a seed x_0, $0 < x_0 < n$;
for $i = 0$ to u {
  $x_i \leftarrow x_{i-1}^T \bmod n$;
  $z_i \leftarrow$ *the least significant bit of* x_i;
}
return $(z_1, z_2, \ldots, z_n)$;

그림1. RSA를 이용한 의사 난수 생성 알고리즘
Fig.1 alg. of pseudo random number generator using RSA

제안하는 시스템에서는 위의 조건을 만족하는 RSA의사 난수 생성기를 사용한다. RSA 의사 난수 생성기는 'RSA 문제'의 어려움에 기반을 둔 암호학적으로 안전한 의사 난수 생성기이다. RSA 공개키 암호에서 사용되는 두 소수 p, q, 법 n=pq 그리고 1 〈 T (n) 범위 내에서 gcd(T, (n)) 조건을 만족하는 난수 T 를 선정한다.

2. 암호 시스템의 암·복호화 과정

제안하는 하이브리드 암호 시스템의 암·복호화 과정은 다음과 같다. 제안하는 시스템에서 사용하는 파라메터들이다.

표 1. 시스템 파라미터
Table 1. System parameter

Symbol	Notation
x, y	송신자와 수신자의 비밀키
A(=xP), B(=yP)	송신자와 수신자의 공개키
R	랜덤 수
T	의사 난수 생성기
S	의사 난수 생성기에 의해 생성된 세션키
H	해쉬 함수
Es()/Ds()	세션키 S를 이용한 대칭키 암호화 알고리즘

〔암호화 과정〕

① 송신자는 랜덤수 R과 타원 곡선 상의 점 A=xP의 x를 선택하고, 수신자의 공개키인 B(=yP)와 송신자의 비밀키 x를 이용하여 A1을 계산한다.

$$A = xP, A_1 = H(xB) \oplus R \quad \cdots\cdots ②$$

② 송신자는 랜덤수 R을 암호학적으로 안전한 의사 난수 생성기를 이용하여 메시지 암호화에 필요한 세션키 $S = T(R)$ 를 생성한다.

③ 송신자는 S를 대칭키 암호 시스템의 키로 사용하여 메시지 m을 암호화하여 암호문 A2를 계산한다.

$$A_2 = E_S(m) \quad \cdots\cdots ③$$

④ 송신자는 메시지의 변경 여부를 확인할 수 있는 정보를 생성하기 위해 A1 와 A2, 그리고 랜덤 값 R, 평문 m을 이용하여 해쉬값 A3 을 계산한다.

$$A_3 = H(A_1, A_2, R, m) \quad \cdots\cdots ④$$

⑤ 송신자는 수신자에게 m에 대한 암호문 A_1, A_2, A_3 을 전송한다.

〔복호화 과정〕

① 수신자는 자신의 비밀키 y와 송신자의 공개키를 이용하여 A1으로부터 랜덤수 R을 계산한다.

$$\begin{aligned} R &= A_1 \oplus H(yA) \\ &= H(xB) \oplus R \oplus H(yA) \\ &= H(xyP) \oplus R \oplus H(yxP) \\ &= R \end{aligned}$$

② ①에서 계산한 R을 의사 난수 생성기에 입력하여 메시지 암호화에 사용될 세션키 $S = T(R)$ 을 생성한다.

③ ②에서 얻은 세션키를 이용하여 암호문 A2,을 이용하여 평문 m을 얻을 수 있다.

$$m = D_S(A_2) \quad \cdots\cdots ⑤$$

④ 수신되어진 암호문 A1 와 A2, 그리고 랜덤 값 R, 평문 m을 이용하여 $A_3 = H(A_1, A_2, R, m)$ 인지 확인하고, 일치하는 경우에만 m을 정당한 평문으로 출력한다.

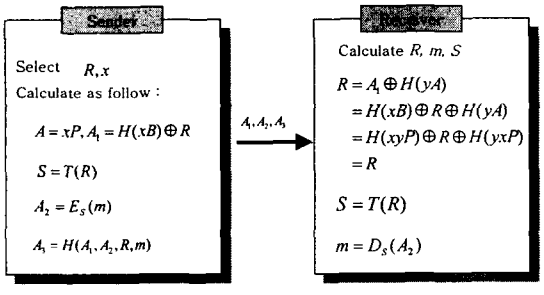

그림2. 하이브리드 암호 시스템의 암복호화 과정
Fig.2 Encrypt and Decrypt Process of Hybrid System

3. 대칭키 암호 시스템

의사 난수 생성시에서 생성된 세션키 S를 이용하여 실제 메시지의 암,복호화를 수행하는 대칭키 암호 시스템으로, exclusive-OR 연산을 수행하거나 AES(Advanced Encryption Standard)[6]와 같은 블록 암호 알고리즘을 이용하여 구현한다.

4. 해쉬 함수

수신한 암호문의 변경 여부를 확인할 수 있는 정보를 생성하는데 사용하는 알고리즘으로, 초기 키 전송값, 대칭키 암호 시스템의 결과값, 초기 랜덤수, 평문을 입력하여 이것의 해쉬값을 구하는 알고리즘이다. MD5 또는 SHA-1등의 해쉬 알고리즘을 이용하여 구현한다.

Ⅳ. 시스템 분석

1. 제안 시스템의 안전성 분석

1.1 함축적 키 인증성과 위장공격에 대한 안전성

송신자는 랜덤수 R을 공유하기 위해 자신의 비밀키와 수신자의 공개키로부터 $A_1 = H(xB) \oplus R$ 을 계산한다. 그리고 수신자는 $A_1 = H(xB) \oplus R$ 을 자신의 비밀키로 복호화하여 공유키를 생성한다. 그러므로 송신자는 수신자 외에는 어느 누구도 동일한 공유키를 생성할 수 없음을 확신할 수 있다. 따라서 송신자는 수신자에 대한 함축적 키 인증성을 갖는다. 그리고 송신자의 비밀키를 알지 못하는 공격자는 사용자가 보낸 암호문을 정당한 형태로 위장하여 전송할 수 없게 된다.

이것은 Diffie-Hellman 기반의 하이브리드 시스템이므로 공격자가 송신자가 보낸 암호문으로 위장하여 암호문을 전송하기 위해서는, 송신자의 비밀키와 수신자의 공개키로부터 $A_1 = H(xB) \oplus R$ 을 계산해야 한다.

이것은 유한체 상의 Diffie-Hellman 문제를 해결하는 것만큼 어려운 일이다.

1.2 송신자의 비밀키가 노출되는 경우의 안전성

공개키 암호 시스템에서 수신자의 비밀키가 노출되지 않는 한 암호문의 송신자를 포함한 다른 사용자들은 암호문을 복호화 할 수 없다.

제안하는 암호 시스템에서는 메시지 암호화에 사용된 키를 암호화하기 위해 수신자의 공개키뿐만 아니라 송신자의 비밀키가 사용된다. 그러나 송신자의 비밀키가 노출된다 할지라도 제3자는 세션키 생성에 사용한 랜덤수를 알 수 없기 때문에 암호문으로부터 평문을 획득할 수 없게 된다.

Diffie-Hellman 기반 시스템에서 송신자의 비밀키가 노출되는 경우, 누구든지 송신자의 비밀키를 이용하여 $A = xP$ 를 구할 수는 있지만, 세션키 암호화에 사용된 랜덤수 R이나 수신자의 비밀키를 모르는 제 3자는 R 값을 복원할 수 없다. 즉, 랜덤 수 R과 수신자의 비밀키 y를 모르는 제 3자가 R 을 구하는 것은 Diffie-Hellman 문제와 동치이다.

1.3 알려진 키에 대한 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 시스템은 세션마다 서로 다른 랜덤수를 선택하여 암호화하여 전송하므로, 이전의 세션키가 노출되더라도 현재의 암호문의 안전성에는 영향이 없다. 또한, 세션키 생성에 사용한 랜덤수 R 이 노출되더라도 해당 세션 외의 다른 세션의 암호문은 여전히 안전하다.

Diffie-Hellman 시스템에서는 과거의 세션키가 노출되더라도 현재 세션의 랜덤수 R을 구하는 것은 불가능하다. 즉, 매 세션마다 서로 다른 난수를 이용한다면 과거의 세션키나 세션키 생성에 사용된 랜덤수가 노출되더라도 현재 세션의 암호문의 안전성에는 아무런 영향이 없다.

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

1.4 상호 개체 인증

송신자는 랜덤수 R을 공유하기 위해 자신의 비밀키와 수신자의 공개키로부터 $A_1 = H(xB) \oplus R$ 을 계산한다. 그리고 수신자는 $A_1 = H(xB) \oplus R$ 을 자신의 비밀키로 복호화하여 공유키를 생성한다. 따라서 송신자의 비밀키와 수신자의 공개키, 그리고 송신자의 비밀키와 수신자의 공개키로 암호화와 복호화가 이루어지기 때문에 상호 개체 인증(mutual entity authentication)이 가능하다.

1.5 갱신키 확인

제안하는 암호 시스템은 세션마다 서로 다른 랜덤수를 선택하여 암호화하여 전송하므로, 이전의 세션키가 노출되더라도 현재의 암호문의 안전성에는 영향이 없다. 또한 세션마다 새로운 세션키를 사용하므로 이전의 키를 재설정하여 공격하는 재실행 공격(replay attack)에 대한 안전성을 보장할 수 있다.

V. 결론

본 논문에서는 타원 곡선 상에서의Diffie-Hellman 기반의 하이브리드 암호 시스템을 제안하고, 구체적인 프로토콜을 설명하였다. 본 논문에서 제안하는 하이브리드 암호 시스템은 기존 하이브리드 시스템과 달리, 송신자와 수신자에 대한 함축적 키 인증성을 제공하는 효율적인 하이브리드 암호 시스템이다. 이 시스템은 의사 난수 생성기, 대칭키 암호 시스템과 타원 곡선 기반의 공개키 암호 시스템의 하이브리드 시스템, 해쉬 함수 등으로 구현 가능하다. 이 시스템은 암호학적으로 안전한 의사 난수 생성기를 사용하여 세션키를 생성함으로써 안전성을 높였으며, 대칭키 암호 시스템과 타원 곡선 기반의 공개키 암호 시스템의 하이브리드 시스템이기 때문에 공개키 시스템과 비밀키 시스템의 장단점을 보완하여 계산량 면에서 더 효율적이다. 또한 위장 공격이 불가능하며, 송신자의 비밀키가 노출되더라도 지정된 수신자 이외에는 정당한 평문을 얻을 수 없다. 그리고 세션키가 노출되더라도 다른 세션의 암호문의 안전성에는 영향을 주지 않는, 알려진 키에 대한 안전성도 제공한다. 또한 상호 개체 인증과 재실행 공격에 대한 안전성도 제공한다.

참고 문헌

[1] E. Fujisaki and T. Okamoto, How to Enhance the security of Public key Encryption at Minimum cost, PKC'99

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

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

[4] T. Okamoto and D. Pointcjeval, OCAC : an Optical Conversion for Asymmetric Cryptosystems, p1363.

[5] D. Pointcjeval, HD-RSA : Hybrid Dependent RSA-a New Public key Encryption Scheme, IEEE p1363

[6] D. Pointcjeval, New Public key Cryptosystem based on the Dependent-RSA Problem, Advances in Cryptology Eurocrypt '99

[7] ANSI X9.42, Agreement of symmetric Key on using Diffie-Hellman Cryptography, 2001

[8] ANSI X9.63, Public Key Cryptography for the financial services industry : key agreement and key transport using elliptic curve cryptography, 2001

[9] Soo-hyun Oh, Seung-Woo Lee, et al, A study on the Security analysis and Applications of standard Key agreement protocols based on Elliptic curve cryptosystem, Journal of the KIISC. Vol. 12. pp 103-118

[10] Soo-hyun Oh, Jin Kwak, Dong-ho Won, Hybrid Cryptosystem providing Implicit Authentication for sender, Journal of the KIISC. Vol 12. pp 71-80

[11] Chang-sub Park, Security and Crypto Theory, Daeyung publish, 2002

저 자 소 개

정 경 숙

1995. 2 경희대학교 수학과 졸업
1997. 8 경희대학교 컴퓨터공학과 석사
1999. 3 ~ 현재 경희대학교 컴퓨터공학과 박사수료
2000. 3 ~ 현재 용인송담대학 컴퓨터소프트웨어학과 겸임교수

〈관심분야〉 정보보호, 인공지능, 전자상거래, 기계학습

정 태 충

1980. 2 서울대학교 전자공학과 졸업
1982. 2 한국과학기술원 전자계산공학과 석사
1987. 2 한국과학기술원 전자계산공학과 박사
1987. 9 ~ 1988. 3 KIST 시스템 공학센터 선임 연구원
1988. 3 ~ 현재 경희대학교 컴퓨터공학과 정교수

〈관심분야〉 인공지능, 자연어처리, 로봇 에이젼트, 정보보호