ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

기밀문서유통을 위한 Weil Pairing IBE 개선 연구☆

Study on Improvement of Weil Pairing IBE for Secret Document Distribution

최 정 현*
Cheong Hyeon Choi

요 약

PKI에 기반을 둔 공개키 방식은 인증성과 비밀성에서 뛰어난 반면 적용된 시스템에서 인증서와 키 관리는 큰 부담이다. 또한 암복호 복잡도(complexity)가 크기 때문에 WSN(Wireless Sensor Network)의 제한된 컴퓨팅 장치에서는 사용하기가 어렵다. 이에 키관리 부담을 없앤 IBE(ID Based Encryption) 방식에서 Bilinear Pairing 방식은 수행속도가 뛰어나고 충분히 안전한 DDH(Decisional Diffie Hellman) 알고리즘으로 인/검증을 처리하는 차세대 암호방식이다. Bilinear Pairing의 이론을 구현한 Elliptic Curve Weil Pairing의 알고리즘은 단순하고 CCA(공격)에 IND/NM의 강력한 보안조건을 만족한다. 동작측면에서 Random Oracle Model을 가정한 IBE PKG는 단일 기밀문서 파일서버로 작동하는 우리의 목적 시스템의 구조에 적합하다. 따라서 본 논문는 Weil Pairing Based IBE 방식을 폐쇄적 기밀문서 유통망(2)에 적합하도록 암복호 및 인검증 알고리즘을 개선하고 본 유통망에 적용된 효율적 프로토콜을 제안한다. 본 논문은 먼저 암호화, 무결성 그리고 사용자 인증을 O(DES) 수준으로 수행하는 개선된 알고리즘을 제안하며 한 번의 암호화 처리에서 비밀성, 무결성과 인증성을 달성하는 정보를 암호문에 포함된다. 둘째 PKI 인증서의 효과를 가진 공개 식별자를 적용하여 키 노출의 위험을 줄인 개선된 IBE 방식을 제안한다.

ABSTRACT

PKI-based public key scheme is outstanding in terms of authenticity and privacy. Nevertheless its application brings big burden due to the certificate/key management. It is difficult to apply it to limited computing devices in WSN because of its high encryption complexity. The Bilinear Pairing emerged from the original IBE to eliminate the certificate, is a future significant cryptosystem as based on the DDH(Decisional DH) algorithm which is significant in terms of computation and secure enough for authentication, as well as secure and faster. The practical EC Weil Pairing presents that its encryption alogorithm is simple and it satisfies IND/NM security constraints against CCA. The Random Oracle Model based IBE PKG is appropriate to the structure of our target system with one secret file server in the operational perspective. Our work proposes modification of the Weil Pairing as proper to the closed network for secret file distribution(2). First we proposed the improved one computing both encryption and message/user authentication as fast as O(DES) level, in which our scheme satisfies privacy, authenticity and integrity. Secondly as using the public key ID as effective as PKI, our improved IBE variant reduces the key exposure risk.

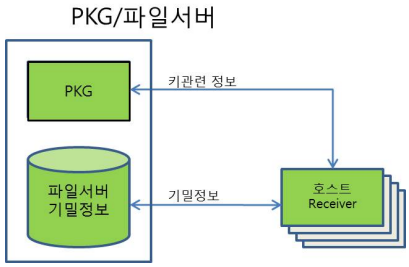
☞ keyword : 네트워크 보안(Network Security), 공개키 암호(Public Key Encryption), 타원곡선 암호방식(ECC-based cryptography), 아이디기반(identity based), 웨일 페어링(Weil pairing)

1. 서 론

경쟁력 있는 기업들은 생산 노하우 등의 기밀정보를 중요자산(proprietary)으로 분류하여 안전한 서버에 디지털 형태로 저장하고, 이 기밀문서는 보안처리 후 네트워크를 통해 유통하는 것이 일반적이다. 그러나 기업 내부 네트워크가 안전성이 보장되지 않은 인터넷 같은 공중 네트워크에 보안성 확보 없이 연결되어 있는 환경이라면 민감한 문서의 노출위험은 상존하고 또 인지하지 못한 사이 경쟁사에게 유출된 사례도 종종 보도된다. 특히 경쟁 핵심 기밀문서는 완벽한 보안성 보장이 필수이다[1].

기밀문서의 보안성은 크게 비밀성(privacy)과 인증성(authenticity)으로 나누며, 인증성이란 합법적 사용자에게만 기밀문서의 접근이 허락되어야 한다는 원칙이고, 비밀성은 유통될 때 문서의 내용은 모든 외부 사용자에게 숨겨져야 하고 인증된 사용자에게만 접근을 허락해야 한다는 원칙이다. 비밀성은 암호화로, 인증성은 전자서명으로 기능을 제공할 수 있다[5,6].

* 종신회원 : 광운대학교 경영정보학과 교수
chchoi@kw.ac.kr
[2011/10/24 투고 - 2011/10/26 심사(2012/01/02 2차 - 2012/02/02 2차) - 2012/03/13 심사완료]
☆ 본 논문은 2009년도 광운대학교 연구년 지원에 의해 작성되었다.



(그림 1) 기밀문서 통신구조

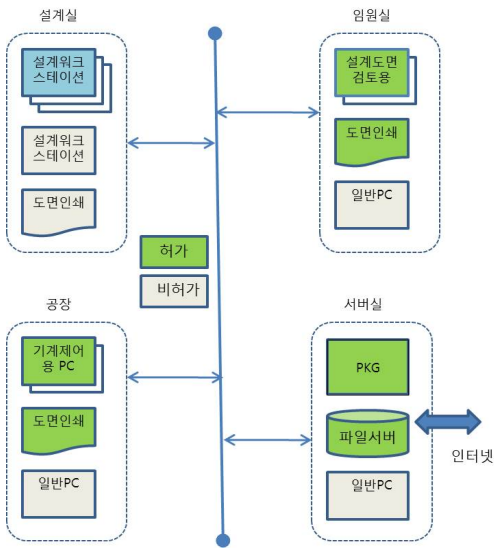
두 조건 모두를 동시에 달성할 수 있는 암호방식은 RSA 공개키 방식이다. 키 크래킹에는 안전하지만 알려진 문제는 첫째 큰 시간복잡도(time complexity)로 처리시간이 길고, 신뢰성 확보를 위한 PKI(public key infrastructure) 기반 인증서는 관리부담을 증가시키고 보안 취약점 발생 빈도가 증가하여 해킹위험이 높아진다. 둘째 키노출 위험을 최소화기 위해 노출이 의심되거나 주기적으로 키변경이 필요하다. 정보 암복호화에 사용할 키셋(i.e. GTEK)과 변경된 키(key)의 안전 분배를 위한 키셋(i.e. GKEK)을 따로 관리해야 하는 키변경(rekey) 절차는 큰 부담을 주므로 프로토콜이 매우 복잡해진다[5,6,10].

이 중 특별히 인증서 관리부담을 낮추기 위해 1984년에 Adi Shamir는 IBE(Identity Based Encryption) 방식을 제안하였다. IBE는 어떤 스트링(string)도 공개키가 될 있어 인증서가 불필요하지만 공개키가 유일해야 하므로 전자우편 주소를 공개키로 사용하는 초기 전자우편의 인증방안으로 제안하였다[24]. 그 후 IBE 방식은 공개키 방식의 하나로서 비밀성과 인증성을 하나의 암호방식으로 달성할 수 있는 방식으로 발전한다. 복잡도가 낮고 안전한 IBE 구현을 위한 변형된 여러 방식이 발표되었으나 그 중 처리부하가 낮고 비교적 구현이 단순한 암복호화 알고리즘이 개발된 Elliptic Curve Bilinear Pairing[17] 방식 Weil Pairing과 Tate Pairing이 대표적이다. 오일러 조건에 기반한 키생성 알고리즘의 Weil Pairing 방식은 기존 공개키 방식의 효과적 대안으로 주목된다[15,16,19].

1.1 목적 시스템

본 논문은 현재 기업의 기밀문서 유통시스템[2]에 적용할 목적으로 효율적 암호 알고리즘의 Weil Pairing Based IBE 방식[15]을 변형하여 수행시간 및 안전성을 개선한 방안을 제안한다.

본 기업 기밀문서 유통시스템은 다음과 같은 특성을



(그림 2) 기밀문서 유통망

가지고 있다. 첫째 특정 장소의 특정 호스트에게만 문서가 유통된다. 둘째 문서의 보관 및 관리는 중앙 파일서버에서 이루어진다. 문서는 파일서버에서 특정 호스트의 사용자로 유통되고 문서 생성/갱신 시에 그 역으로도 유통되지만 호스트 사이 문서교환은 없다. 셋째 유통망 닫혀있고 자료교환은 안전채널로 노출로부터 보호되므로 서버와 사용자 사이 정보도청 man-in-the-middle 공격은 불가능하다고 가정한다[1,2].

IBE 방식은, 구조관점에서 보면, Random Oracle Model (ROM) 기반 PKG(Private Key Generator)가 암호 primitive를 서비스하므로 알고리즘과 키정보를 숨기는 것이 일반적이다. ROM에서 암호 primitive 서비스는 적대자(adversary)를 포함한 어떤 사용자에게도 제공되지만 안전성이 입증된 방식이다[29].

본 기밀문서 유통시스템[1]은 파일서버와 ROM IBE PKG의 기능을 변경 없이 적용 가능하므로 ROM IBE 방식에 적합하다고 판단되어, PKG를 안전채널을 통해 기밀정보 유통시스템 파일서버와 1:1 협조하는 구조로 구현하고 암호 primitive: 기밀정보 암호/복호 primitive, 사용자 개인키/공개키 생성 primitive, 사용자 인/검증 primitive 등 를 안전하게 제공할 수 있도록 하였다.

공개키 개선

본 시스템에서 키생성 primitive는 유일하고 시간/공간

적 공개키를 생성하기 위해 사용자 ID에 지역정보를 결합한 공개 식별자에 RO(Random Oracle) 해쉬를 적용하여 무작위(random)로 변형한다. RO 해쉬의 특성은 공개 식별자에 관해 어떤 정보도 역으로 알아낼 수 없도록 하는 비가역성(Onewayness) 조건을 만족한다. 적대자가 특정 공개키를 절취할 수 있다고 해도 그 포함된 어떤 지역정보도 알 수 없다는 보안조건이다[33].

공개키의 시간적 제한은 개체 식별자와 시간정보를 결합하여 해쉬를 적용하여 동적으로 공개키 $Pub_i = (ID_i \| Date\,Time)$ 를 생성한다면 공개키의 유효시간이 경과하면 공개키는 동일 ID에 대해서도 변화되므로 개인키의 적용이 무효가 되어 공개키 폐기(revocation)효과와 같다[21]. 유효기간은 몇 초부터 분, 시간, 달, 년까지 여러 유형이 가능하고 개인키 생성에서 협상에 의해 결정될 경우 적대자는 유효기간 유형에 대한 어떤 정보도 얻을 수 없다.

사용자 ID U_i와 장치 ID D_j를 결합하여 공개키 $Pub_{ij} = Hash(U_i \| D_j \| Time)$ 의 생성이 가능하고 장치 D_j에 로그인 한 사용자 U_i만이 사용할 수 있는 제한적 동적 공개 ID가 되고, 인증 다이제스트로 사용될 수 있다.

요약하면 ROM IBE를 통해서 사용자 ID와 장치 ID를 제공하면 다양한 사용자 지역정보를 결합한 공개 식별자는 공개키의 유효성을 공간적/시간적으로 제한하는 특성을 가지면서도 키관리가 필요 없는 장점을 가진다.

RO 해쉬 구현

ROM IBE의 보안성을 위해 RO 해쉬는 강력한 보안조건인 Randomness와 Onewayness로 모두 만족해야 한다. 그러나 이 조건은 SHA-1와 같은 기존 해쉬로는 불가능하고, 기존 해쉬함수에 더 긴 결과값을 허락하도록 변형하거나 DES를 변경하여 해쉬함수를 구현해야 가능하다[29,30,32].

1.2 PKG 특성

ROM IBE PKG의 주요 암호 primitive는 시스템 파라미터 생성 *Setup()*, 메시지 암호화 *Encrypt()*, 암호문 복호화 *Decrypt()*, 공개 식별자에 대한 공개키/개인키 생성 *Key_Extract()*이다[24].

(그림 1)에서 파일서버는 PKG와 1:1 협조하면서 문서요청 호스트의 공개키로 암호화하여 전송하고, 배포된 개인키로 복호화한다. 각 호스트는 (사용자 ID, 장치 ID)로 PKG에게 키생성을 질의하여 개인키를 얻는다[14]. 본 목적 시스템에서는 일반 공개키 방식과 다르게 PKG에서 사용자 지역정보를 결합과 RO 해쉬를 적용하여 공개키와 개인키를 만들어 공개키는 파일서버에 저장되고개인키는 호스트에 전달한다.

1.3 논문 구성

본 논문의 2장에서 관련 연구로서 Weil Pairing의 수학적 모델, ROM IBE의 주요 primitive 정의, 그리고 ROM IBE의 수학적 안전조건을 기술한다. 3장에서 본 목적 시스템[1,2]에서 문서유통 프로토콜에 적용 가능하도록 Weil Pairing 기반 ROM IBE PKG primitive 알고리즘을 변형하고 성능을 개선한다. 4장에서 개선된 알고리즘을 기밀문서 유통시스템의 문서생명주기의 처리 프로토콜에 적용한다. 5장에서 ROM IBE의 공격에 대한 강력한 안전조건 IND/NM-CCA(Chosen Ciphertext Attack)를 논의하고, 본 논문의 개선된 IBE 방식의 복잡도 분석과 수행성능 분석을 한다. 결론으로 6장에서 미래 연구방향에 대해 언급한다.

2. 관련 연구

Pairing based cryptosystem은 DHP(Diffie Hellman Problem) 문제 Three-party one-round agreement의 효과적인 프로토콜의 존재여부에서 출발한다[19]. 세 개체가 Diffie-Hellman 키교환으로 세션키를 계산해내기 위해서는 최소 두 번의 교환(round)이 필요하다. 세 사용자 Alice, Bob, Chris는 g^a, g^b, g^c를 계산 후 Alice->Bob, Bob->Chris, Chris->Alice 방향으로 그 값을 상대에게 보내어 g^{ac}, g^{ab}, g^{bc}를 계산 후 다시 같은 방향으로 그 값을 보내면 모든 사용자가 g^{abc}라는 최종 비밀키를 얻게 된다.

이를 Computational DHP(CDHP) 문제라고 하며, 적대자가 중간에서 얻은 일부 값을 가지고 비밀키를 알아내는 것은 매우 어려운 문제(hard problem)에 속하므로 키 크래킹이 어렵지만 CDH의 비밀키 계산속도가 매우 느리다. 따라서 크래킹은 여전히 어렵지만, 한 번의 교환으로 비밀키의 계산을 매우 빠르게 한 Bilinear Pairing 방식을 제안한다[31].

이론적 Bilinear Pairing에는 Additive 그룹(group) G_1와 Multiplicative 그룹 G_2에서 다음 Map $\hat{e}: G_1 \times G_1 \rightarrow G_2$이 존재하며 그룹 G_1은 그 기표가 $G_1 = <P>$이고 다음 세

가지 성질을 만족하는 방식이다. 여기서 q는 G_1의 *order*이고 P는 G_1의 *generator*이다.

(1) *bilinearity*: $\hat{e}(aP,bP)=\hat{e}(P,P)^{ab}$
(2) *non-degeneracy*: $\hat{e}(P,P)\neq 1$
(3) $\hat{e}()$의 효과적 알고리즘이 존재한다.

Bilinear Pairing 정의로 보면, 네 값 $A=aP$, $B=bP$, $C=cP$, P이 주어졌을 때, DDH는 $abP\equiv cP$를 알아내는 것이고 CDH는 g^{abc}를 계산하여야 한다. 그러므로 CDHP는 그룹 G_2에 속한 곱셈 기반 문제로서 크래킹은 어려운 문제이고 비밀키 계산은 매우 높은 문제이다. 반면에 G_1에 속하여 덧셈 기반 Decisional DHP(DDHP) 문제는 크래킹에서는 CDHP와 동일 수준의 어려운 문제이지만 비밀키 계산은 덧셈 후 비교하는 매우 빠른 성능을 보인다.

CDHP와 DDHP의 관계는 Map $\hat{e}()$를 통해서 전환된다. DDH에서 $\hat{e}(aP,bP)\equiv\hat{e}(P,cP)$ 는 그 의미가 $abP\equiv cP$ 이므로 CDH의 g^{abc}를 계산하는 것과 동일하다. 매우 빠른 계산 문제가 된다. 이는 Bilinear Pairing 방식의 중요한 특성이다.

그러나 이론적 Bilinear Pairing의 성질을 만족하는 그룹, Map, 알고리즘을 실현 가능하게 한 것은 ECC(Elliptic Curve Cryptosystem)의 Tate Pairing[16]과 Weil Pairing[14] 이었고 ECC는 Bilinear Pairing 기반 구현 가능한 IBE 암호방식이다.

좀 더 간단한 수식이면서 키생성 알고리즘이 개발된 Weil Pairing IBE 방식에 대한 서명방식과 암호방식을 살펴보자.

2.1 Bilinear Pairing 서명

DDH 문제에 기반을 둔 서명과 검증(Verification) 과정은 매우 간단하다. 다음은 [19]에서 기술된 것을 참조하였다.

서명과정

(1) 임의 정수 $a\in Z_q$를 일시 개인키로 한다.
(2) 일시 공개키 $A=aP$을 생성한다.
(3) 메시지 m을 해쉬함수 $H()$를 통해 다이제스트 $M=H(m)$을 생성한다.
(4) 다이제스트를 일시 개인키로 서명 $S=aM$을 생성한다.
(5) 인증 DH-quadruple (P,A,S,M)을 보낸다.

검증과정

(1) 인증 DH-quadruple (P,A,S,M)를 수신한다.
(2) $\hat{e}(P,S)\equiv\hat{e}(A,M)$ 여부를 검사한다.
(3) 일치하면 검증 성공, 아니면 검증 실패.

위 검증과정을 수학적으로 보면, $\hat{e}(P,S)\rightarrow\hat{e}(P,aM)\rightarrow\hat{e}(aP,M)\rightarrow\hat{e}(A,M)$이므로 $\hat{e}(P,S)\equiv\hat{e}(A,M)$은 성립된다.

검증과정은 느린 CDH 비밀키 계산을 $\hat{e}()$을 통해 빠른 DDH로 변환한 것이다. 일반적으로 개인키 기반 서명 과정은 RSA의 높은 복잡도를 보이지만 단지 메시지 다이제스트 길이는 짧고 고정되어 있으므로 서명의 복잡도는 O(1)로 무시된다. 위 서명은 메시지 m에 해쉬 적용이 복잡도를 결정하므로 RO 해쉬 구현 DES의 복잡도로 수렴된다고 할 수 있다.

성능분석을 고려할 때 ECC 기반 $A=aP$의 계산은 RSA의 지수계산 P^a에 비해 빠르지만, 복잡도 관점에서 메시지 크기 $n=\|m\|$가 충분히 크다고 전제하므로, 짧은 ID에서 일시 공개키 계산시간은 O(1)로 무시된다. 이는 상세하게 5장에서 논의한다.

2.2 Bilinear Pairing 암호화

Bilinear Pairing 암호화 과정은 다음과 같이 이루어진다[17][19].

(1) PKG는 초기 *Setup*에서 두 그룹 G_1, G_2, *Map* $\hat{e}: G_1\times G_1\rightarrow G_2$, 두 해쉬 $H_1:\{0,1\}^*\rightarrow G_1$과 $H_2:G_2\rightarrow\{0,1\}^l$ 등을 생성한다. 여기서 해쉬 H_1, H_2는 임의 스트링(string)을 두 그룹 G_1, G_2의 원소로 매핑한다. $G_1=<P>$에서 P는 그룹 G_1의 generator이고, 그 order는 q이며 $G_2=<\hat{e}(P,P)>$이다. 여기에 시스템 마스터 키 $t\in Z_q$ 선정하고 그 공개키 $T=tP$를 생성하여 (t,T)를 PKG에 보관하고, PKG 시스템 파라미터 (G_1, G_2, $\hat{e}$, P, T, q, H_1, H_2)를 생성하여 보관한다.

파일서버와 호스트 간 암호 통신으로 파일서버가 공개 사용자 ID_i를 가진 특정 장치의 사용자 i가 요청한 기밀파일 m을 암호화 전송하는 경우를 보면 다음과 같다.

파일서버의 평문 암호화 전송

(1) PKG가 사용자 i의 ID_i에 대한 키 생성질의에 따라 먼저 공개키 $Q_i = H_1(ID_i, h^*)$을 생성 후 개인키 $d_i = tQ_i$를 계산하여 사용자 i에게 d_i를 안전채널로 보낸다. 여기서 h^*는 사용자 i의 지역정보로서 길이에 제한이 없고 반복 적용이 가능하다.

(2) 임의 정수 $r \in Z_q$를 선정 후 $R = rP$를 생성 후 암호문(ciphertext) $c = m \oplus H_2(\hat{e}(Q_i, T)^r)$ 을 생성하고 암호문 쌍 (R, c)를 사용자에게 전송한다.

사용자의 암호문 복호화

(1) $\hat{e}(Q_i, T)^r = \hat{e}(Q_i, tP)^r = \hat{e}(tQ_i, rP) = \hat{e}(d_i, R)$이므로 복호화는 $c \oplus H_2(\hat{e}(d_i, R))$ 이고 $H_2(\hat{e}(Q_i, T)^r) \oplus H_2(\hat{e}(d_i, R)) = O$이므로 $m \oplus H_2(\hat{e}(Q_i, T)^r) \oplus H_2(\hat{e}(d_i, R)) = m$이다. 결과적으로 복호화가 성공적으로 완료된다.

이상 IBE 암복호 과정을 수학적으로 보면 간단한 *Map* $\hat{e}(d_i, R)$을 통해 복호화가 가능하고 XOR $\oplus$ 연산으로 복잡도는 O(n), $n = \| c \|$ 이다. RSA 방식과 비교하면 개인키 d_i을 암호문에 c^{d_i} 하는 복호화 수행 복잡도 O($k^3 n$) ($k = \lceil \log M \rceil$ M 모듈러 값)과 비교할 수 없게 빠르다.

2.3 Weil Pairing 키생성

Bilinear Pairing 특성을 보이는 *Map* $\hat{e}()$와 두 그룹 G_1, G_2의 결정은 Elliptic Curve E 위의 점들을 Finite Field $F_p = Z/Z_p = \{1, 2, ..., p-1\}$로 한정시킨 $E(F_p)$를 구하고 Weil Pairing의 계산법 (*exp-1*)을 적용하면 Cyclic 그룹 G_1을 생성하게 된다[17][19]. 본 논문에서 Weil Pairing Elliptic Curve $y^2 = x^3 + 1$으로 G_1 원소를 계산하는 알고리즘 (*exp-1*)이 다음과 같다.

Setup Algorithm --- (exp-1)

Weil Pairing은 $E(F_p)$에서 $x \in G_1$값을 선정하고 그 해(root) y는 $y = \sqrt[3]{x^3 + 1} \pmod p$을 만족하는 $y \in E(F_p)$이다. $p = 12q - 1 \rightarrow p + 1 = 12q$ 이 성립하고 F_p의 *order*는 $p+1$이다. 이런 정수를 quadratic residue modular p라고 부르며 Euler criteria를 사용하여 다음과 같이 계산된다[14].

(1) 만일 p가 소수(prime)이고 GCD(a,p)=1이면, $a^{\frac{p-1}{2}} = 1 \pmod p$을 만족하는 a는 quadratic residue modular p이고 그 역도 성립한다.

(2) 여기서 만일 $p = 3 \pmod 4$ 이라면 a의 제곱근은 $r_{\{1,2\}} = \pm a^{\frac{p+1}{4}} \pmod p$이다.

여기서 개인키 $d_i = tQ_i$을 위한 공개키 Q_i를 계산하는 알고리즘은 다음과 같다[14].

Key_Extract Algorithm --- (exp-2)
j=0
while (j < $\left\lceil \log_2(\frac{1}{\delta}) \right\rceil$) {
  $x_i = H_1(ID_i, h^* \| j) \subseteq G_1$
  $a = x_i^3 + 1 \pmod p$
  if ($a^{\frac{p-1}{2}} = 1 \pmod p$) then {
    $y_i = \min(\pm a^{\frac{p+1}{4}} \pmod p)$
    $Q_i = 12(x_i, y_i)$
    exit
  } else
    j=j+1
}

알고리즘 (*exp-2*)의 복잡도는 해쉬 H_1의 복잡도와 일치한다. 강력한 RO 해쉬는 DES로 구현되므로 $O(cH_1) = O(cDES) = O(DES)$이다. 그러나 $O(DES) = O(n)$이고 $n = \| ID_i \| = c$ 이므로 $O(KeyExtract) = O(1)$ 이다.

2.4 보안성 조건

본 Weil Pairing 방식의 보안성은 DLP(Discrete Logarithm Problem)와 CDHP에서 출발한다. Cyclic Additive 그룹 $G_1 = <P>$에서 $a \in Z_q$ 선정하여 $Q = aP$ 라면 값 (P, Q)를 가지고 a를 알아내는 것이 DLP라는 어려운 문제이다. 이는 Cyclic Multiplicative 그룹 $G_2 = <P>$에서 $b \in Z_q^*$ 선정 후 $Q = P^b$ 에서 b를 구하는 DLP 문제 $b = \log_P Q$와 동일한 어려운 문제이다. 따라서 적대자의 크래킹 알고리즘 A가 해를 발견할 확률은 무시될 만큼 작다[26,27,33].

ROM IBE 방식에서 어떤 사용자도 암호 primitive 질의를 보낼 수 있고 적대자도 암호분석을 위해 질의를 보

내어 필요한 정보를 얻으려고 한다고 가정한다. 그러므로 ROM IBE 보안성은 암호분석에 이용할 만한 한 비트의 정보라도 얻을 수 없도록 하는 조건인 Semantical Security와 관련된다. 이는 일반 평문 x와 해당 암호문 y 사이에서 어떤 관계 정보도 알아낼 수 없는 강력한 조건인 IND(Indistinguishability)와 평문 x과 암호문 y의 쌍 (x, y)의 관계는 알더라도 이를 통해 새로운 변형 쌍 (x', y')을 생성할 수는 없다는 조건 NM(Non-Malleability)이다. 다른 의미로는 IND는 비밀성 확보 조건이고 NM은 불법적 조작이 불가능하다는 무결성 조건이다[32].

ROM IBE에서 primitive $f()$에 대한 보안성 조건은 $f(x)=y$ 에서 y 값으로 x를 알아낼 수 없어야 하고 이것은 $f()$가 Trapdoor permutation이어야 한다는 조건이다. Trapdoor permutation은 $f()$에 강력한 해쉬가 사용되어야 가능하다.

강력한 해쉬란 비가역성(Onewayness)과 무작위성(Randomness)을 만족해야 한다. 해쉬 결과로는 입력정보를 전혀 알아 낼 수 없다는 의미이다. 또 해쉬는 확률적 함수이어야 하고 같은 입력에 결과는 언제나 동일해야 한다는 조건도 가진다. 목적을 가지고 만든 Adaptive 정보조각도 암호분석에서 무작위 추측 수준 이상의 성공확률을 가질 수 없다는 조건이다.

2.5 암호 Primitive

ROM IBE의 암호 primitive의 안전성을 보장하기 위해 신뢰할 수 있는 PKG가 서비스 한다고 가정한다. 질의에 항상 응답해야 하는 ROM을 가정하지만 사용자의 질의 내용과 그 응답 내용은 타인이 도청하거나 절취할 수 없어야 한다. 즉 man-in-the-middle 공격이 불가능해야 한다. 이는 질의/응답 전송은 안전채널을 통한다는 가정이다[11].

일반적 ROM IBE PKG는 다음 네 개 primitive 서비스를 수행한다.

(1) *Setup()* 시스템 파라미터 셋업함수: 언급한 (G_1, G_2, $\hat{e}$, P, T, q, H_1, H_2)를 생성하고, 시스템 마스터 키 t는 PKG에 저장한다. H_1, H_2는 강력한 해쉬이다.

(2) *Key_Extract()* 키생성 함수: 사용자 ID_i로부터 공개키 Q_i를 만든 후 해당 개인키 d_i를 생성하여 사용자에게 전송한다.

(3) *Encrypt()* 암호화 함수: 메시지 m을 수신자 ID_i로부터 생성한 공개키 Q_i로 암호문(ciphertext) c를 생성한다.

(4) *Decrypt()* 복호화 함수: 암호문 c를 공개키 Q_i의 대응 개인키 d_i로 복호하여 메시지 m을 복원한다.

2.4절에서 논의한 보안조건 IND/NM를 만족하는 암호화 방식은 다음 조건을 만족해야 한다.

Encrypt Secure Model --- (exp-3)

(1) $E^{G,H}(x)=f(r)\parallel G(r)\oplus x\parallel H(rx)$ [32]

$f()$는 Trapdoor permutation이고 $f^{-1}()$은 그 역이고, $H:\{0,1\}^{*}\rightarrow\{0,1\}^{k}$ 는 RO 해쉬이고, $G:\{0,1\}^{*}\rightarrow\{0,1\}^{\infty}$ 는 Random Generator이다[32].

본 논문의 개선된 암호화 primitive는 (*exp-3*)와 일치한다.

3. 기밀문서 유통에 적합한 변형 방안

이중 서명

기밀문서 통신은 허락된 장치에서 허락된 사용자가 기밀문서에 대해서 요청할 때 파일서버에서 처리된다(그림 1). 이 때 장치와 사용자의 인증정보를 서명하면 파일서버가 검증한 후 처리가 허락된다. 여기서 장치와 사용자의 이중 인증서명은 두 ID를 결합하여 키생성 질의로 개인키를 얻어 개인키로 ID를 서명하면 장치와 사용자의 쌍의 개인키이므로 이중 서명과 같은 효과를 주고 이를 파일서버가 검증 후 기밀문서의 암호화 전송이 허락된다.

서명과 암호화 병용

본 시스템에서 사용자와 파일서버는 상호 인증을 수행해야 한다. 특별히 Weil Pairing 기반 인증방식은 DDHP에 근거한 효율적 방식이고, 동시에 서명과 암호화의 병행이 가능하다. 본 변형안은 강력한 보안성을 만족하는 서명과 암호화가 혼합된 방식으로 개선하여 암호 primitive에도 적용하였다.

본 3장은 Primitive 함수 *Setup()*, *Key_Extract()*, *Encrypt()*, *Decrypt()*을 본 목적 시스템에 적합하도록 변형하였다. 먼저 3.1절 시스템 파라미터에서 개선에 필요한 추가 정보을 설명하고, 3.2절은 인증방식과 공개키 생성방식을 변형하고, 3.3절은 암호/복호화 방식과 개인키 생성방식을 변형하고, 암호 primitive 함수의 수학적 정의를 변경할 것이다.

3.1 시스템 파라미터

시스템 파라미터는 PKG가 유통망 구성 초기에 생성해서 호스트의 질의 처리에 사용할 primitive의 요소이다. 본 시스템은 기본적 IBE 파라미터에 확장된 정보를 추가한 파라미터를 다음과 같이 생성한다.

System Parameter --- (exp-4)

(G_1, G_2, $\hat{e}$, P, T, Q_s, q, k, H_1, H_2, H_3)

G_1, G_2, $\hat{e}$, P, T, q, H_1, H_2는 기존 ROM IBE 방식에서 생성되는 시스템 파라미터(2.2절 참조)와 동일하다. 일반적으로 외부에 공개되는 정보도 있지만 본 시스템의 보안성 때문에 PKG에만 보관된다. 여기에 추가될 정보로 시스템 마스터 키 t와 공개 마스터 키 역할을 할 $T=tP$이다. Q_s는 파일서버 공개키이고, 해당 개인키 $d_s=tQ_s$는 파일서버 서명에 사용된다. 여기서 Q_s는 *Key_Extract Algorithm (exp-2)*에서 입력 $ID_s^{lf}=H_3(D_s)\|lf$은 파일서버 ID의 $H_3(D_s)$에 시간정보를 결합하여 생성된 파일서버 공개 식별자이다.

H_3, k는 메시지 다이제스트를 위한 해쉬함수 $H_3:\{0,1\}^*\rightarrow\{0,1\}^k$로서 k는 길이를 제한하는 정수이다. 해쉬함수 $H_3()$는 2.4절의 IND/NM-CCA을 만족하는 암호화 함수 *Encrypt Secure Model (exp-3)*의 필수요소 $H()$의 역할을 위한 것이다.

3.2 인증방식

IBE 서명은 큰 변형 없이 계산량을 줄이기 위해 최소 변경으로 짧은 다이제스트를 사용한다.

공개 식별자와 공개키 생성

IBE의 초기목적은 개체의 고유 ID를 공개키로 사용하여 인증서 관리부담을 없애는 것이므로 본 목적 시스템에서는 허가된 장치와 사용자에게만 기밀문서 접근을 허락하려고 두 개체의 ID 결합 정보를 전송하고, 서버는 시간정보를 추가한 후 해쉬를 통과시켜 공개 식별자를 생성하여 공개키를 만든다. 이는 두 개체 동시 인증이 가능하게 한다[2].

공개 식별자: $ID_{i,j}^{lt}=H_3(D_i,U_j)\|lf$

(1) D_i: 장치 i 공개 ID

(2) U_j: 사용자 j 공개 ID

(3) lf: 공개키의 유효기간(lifetime)

공개 식별자 $ID_{i,j}^{lt}$를 *(exp-2)*의 $x_k=H_1(ID_{i,j}^{lf})$에 적용하여 공개키 $Q_{i,j}=(x_k,y_k)$를 계산하고 개인키 $d_{i,j}=tQ_{i,j}$가 생성된다.

인증 DH-triple

2.1절에서 보면 호스트와 서버 간 통신 개체의 인증을 위해서 DH quadruple (P,A,S,M) 인증정보를 전송한다. 본 목적 시스템에서는 다음과 같이 인증 프로토콜을 변경한다.

(1) P는 파라미터에 포함된 Cyclic 그룹 G_1의 *generator*이다.

(2) A는 개체인증을 위해 생성한 일시 공개키로서 일시 개인키 $a\in Z_q$로부터 만든다. 전자서명에 포함될 정보지만 (P,A)로 a을 계산하는 것은 DLP로 어렵다.

(3) M은 길이가 k인 다이제스트로서 서명에 적용할 정보로서 $M=H_3(m)$, $\|M\|=k$ 이다.

(4) S는 (2)에서 생성된 일시 개인키 $a\in Z_q$로 다이제스트 M를 서명한 것이다. 개체 인증에서 개체의 공개 ID 합성을 다이제스트로 사용하여 호스트는 $m=(D_i,U_j)$, 파일서버는 $m=ID_s$ 이고 해쉬를 적용한 $M=H_3(m)$ 에 서명한 $S=aM$ 이다.

3.2 암호 및 복호화 방식

Pairing-based IBE 암호화의 조건은 안전모델 *(exp-3)*에 상세히 기술되어 있고 그 모델 구성은 일시 공개/개인키 생성, 암호문(ciphertext) 생성, 서명 생성이다. 세 부분 (R, c, S)이 결합되어 전송된다.

여기서 개선된 암호화 알고리즘 *(exp-5)*을 기술하고 암호화 안전모델 *(exp-3)* 요구에 만족하는지 검증한다.

Encrypt Algorithm --- (exp-5)

(1) 일시 개인-공개키 생성: 개인키 $r\in Z_q$ 선정하고 해당 공개키 $R=rP$을 생성한다.

(2) 암호문 생성: *Key_Extract()*에서 생성된 사용자 공개키는 $Q_{i,j}$, 개인키는 $d_{i,j}=tQ_{i,j}$이라면 메시지 m의 암호문 $c=m\oplus H_2(\hat{e}(Q_{i,j},T)^r)$ 를 생성한다. 여기서 $H_2(\hat{e}(Q_{i,j},T)^r)$은 *Random Generator*로 *(exp-3)*의 $G(r)\oplus m$에 해당된다.

(3) 메시지 서명 생성: 메시지 m의 다이제스트 $M=H_3(m)$이고 서명 $S=rM$을 생성한다.

이에 복호화는 매우 단순하다. 복화화 알고리즘은 다음과 같다.

Decrypt Algorithm --- (exp-6)

(1) $m = c \oplus H_2(\hat{e}(d_{i,j}, R))$

위 암호/복호화 알고리즘으로 비밀성은 충분히 달성되며 동시에 인증서명도 함께 이루어지므로 검증과정 $\hat{e}(P,S) \equiv \hat{e}(R,M)$으로 메시지 인증/검증이 완료되어 메시지 무결성도 달성된다.

본 개선 알고리즘이 보안모델 *exp-3*의 조건과 일치하는지 여부를 증명하자.

Proposition*: *Encrypt Algorithm (exp-5)*은 *암호화 보호 모델 (exp-3)*를 *만족시킨다.

Encrypt Algorithm (exp-5) 세 부분 (R, c, S)는 암호화 보안 모델 *(exp-3)* $E^{G,H}(m)$을 만족시킨다.

Sub-1: $R = rP$는 (exp-3) Trapdoor Permutation $f(r)$을 만족한다.

(증명) Trapdoor permutation란 $y = f(x)$에서 y 값으로 x를 알아내기 어렵게 한 문제이므로 $R = rP$에서 (P,R)로부터 r을 알아내는 것은 DLP $r = \log_P R$ 으로 어려운 문제이고 $f^{-1}(r)$이 존재하므로 $R = rP$는 Trapdoor permutation이다.

Sub-2: 만일 $\Omega(r) = H_2(\hat{e}(Q_{i,j}, T)^r)$ 라고 두면, $\Omega(r)$는 Random Generator이다.

(증명) 만일 $\Omega(r) = H_2(\hat{e}(Q_{i,j}, T)^r)$라면 해쉬 H_2는 Randomness 만족하는 함수이므로 $\Omega(r)$는 Random Generator이다.

Sub-3: S는 (exp-3) $H(rx)$와 같은 역할이다.

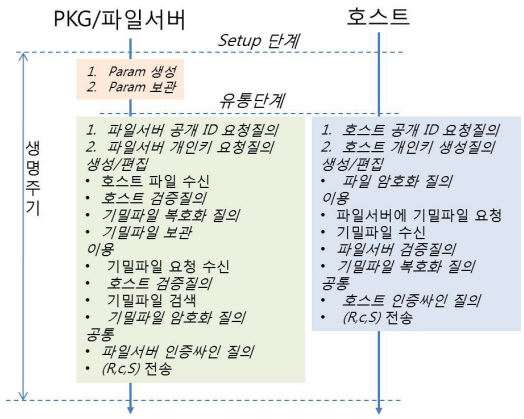
(증명) $S = rH_3(m)$이므로 S는 m, r의 함수 $S = f(r,m)$이므로 $f(r,m) \approx H(r \circ m)$ 이므로 같은 역할이라고 할 수 있다.

결론적으로 본 암호화 방식 (*exp*-5)은 ROM 보안조건 NM과 IND을 만족하는 암호화 모델 (exp-3) $E^{G,H}(x)$와 일치하므로 (*exp*-5)는 IND/NM-CCA 방식이다[32].

3.3 암호 primitive 재정의

ROM IBE는 PKG에서 RO primitive 질의를 처리하고 응답하는 방식이다. PKG를 키-대리자(Key Escrow) 역할을 수행한다[19].

본 시스템에서는 PKG primitive를 *Setup()*, *Key_Extract()*, *Sign()*, *Verify()*, *Encrypt()*, *Decrypt()*의 여섯개 primitive 함수로 확장한다. 단 *Decrypt()*는 일반 ROM에서는 제외하는 primitive이다.



(그림 3) 기밀문서 생명주기

본 논문의 여섯 가지 개선된 암호관련 primitive 함수를 수학적으로 다음과 같이 정의한다.

(1) *Setup()* ::==

$(G_1, G_2, \hat{e}, P, T, Q_s, q, k, H_1, H_2, H_3)$, (d_s, t) where $T = tP$, $d_s = tQ_s$ and q is the order of $G_1 = <P>$and $k = |H_3(\bullet)|$

(2) *Key_Extract*(ID_i) ::==

Q_i in (d_i, Q_i) where $Q_i = H_1(ID_i^{lf}, h^* \| l)$ and $d_i = t\,Q_i$ and $ID_i^{lf} = H_3(ID_i) \| lf$

(3) *Sign*(m) ::==

(R,S,M) when $R = rP$, $r \in Z_q$ and $M = H_3(m)$ and $S = tM$

(4) *Verify*(R,S,M) ::==

if $\hat{e}(P,S) \equiv \hat{e}(R,M)$ then true else false

(5) *Encrypt*(Q_t, m, ID_t) ::==

(R, c, S, M) where Q_t=*Key_Extract*(ID_t) is a public key and $\Omega(r) = H_2(\hat{e}(Q_{i,j}, T)^r)$ is a random generator, thus $c = \Omega(r) \oplus m$., (**R**, **S**, **M**) = *Sign*($ID_t \| m$), $R = rP$, $r \in Z_q$

(6) *Decrypt*(d_t, (R, c, S, M)) ::==

if *Verify*(R, S, M) then m else fail where d_t is a private key and $m = c \oplus H_2(\hat{e}(d_t, R))$.

이미 언급한 것처럼 이상의 primitive 질의와 응답은 안전채널을 통한다고 가정한다.

다음 4장에서 본 시스템이 목적으로 하는 기밀문서 유통의 처리과정 프로토콜을 기술하겠다.

4. 기밀문서 처리 프로토콜

본 목적 시스템에서 기밀문서는 생성/편집/사용이라는 생명주기(그림 3)를 반복한다. 문서의 교환은 사용자와 파일서버 사이에서만 상호 인증과 함께 이루어진다.

시스템의 생명주기는, 크게 PKG *Setup()* 단계와 기밀문서 유통단계로 나누어지고, 유통단계는 다시 생성, 사용, 편집이라는 문서 생명주기로 구성된다. 유통단계에서 문서의 생성과 편집은 호스트가 파일서버에게 생성 또는 갱신된 기밀파일을 전송한다. 이 때 *Encrypt()* 질의로 얻은 (R, c, S, M)을 파일서버에 전송한다. 반면 문서의 사용은 호스트가 기밀문서를 파일서버에게 요청하면 문서를 찾아 호스트 공개키로 질의한 *Encrypt()*의 응답을 호스트에 전송한다.

4.1 기밀문서 생성과 편집

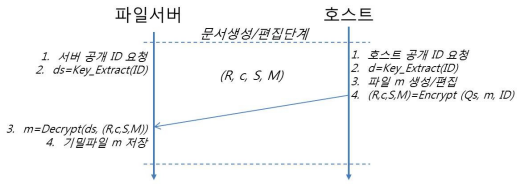
기밀문서는 등록된 장치 i의 D_i에서 합법 사용자 j의 U_j가 생성하거나 편집한다. 호스트 ID=(D_i, U_j)는 장치 i에 접속한 사용자 j를 의미한다. 문서를 파일서버로 전송하기 전에 사용할 개인키를 요청해야 한다.

호스트 $ID_{i,j}$=(D_i, U_j)로 키생성 *Key_Extract*($ID_{i,j}$) 질의를 한다. 3.3절 (2)에서 보면 공개키 $Q_{i,j} = H_1(H_3(ID_{i,j}\ lf), h^* \| j)$ 가 생성되고 개인키 $d_{i,j}$가 계산되어 ($d_{i,j}$, $Q_{i,j}$)가 생성되고 개인키 $d_{i,j}$는 호스트로 전달한다. 공개키에는 유효시간동안만 사용가능하다. 파일서버의 공개키 Q_s와 개인키 d_s는 *Setup()*에서 생성되고 공개키 Q_s는 모든 장치에 분배된다.

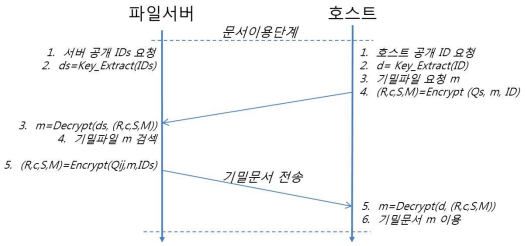
호스트가 갱신한 파일 m과 인증 다이제스트 $ID_{i,j}$로 3.3절 (5) *Encrypt*($Q_s, m, ID_{i,j}$)를 통해서 응답 (R, c, S, M)을 파일서버로 전송한다. 파일서버는 3.3절 (6) *Decrypt* ($d_s, (R, c, S, M)$)를 통해 *Verify*(R, S, M)로 검증하고 $m = c \oplus H_2(\hat{e}(d_s, R))$으로 복호화 한다.

4.2 기밀문서 이용

문서의 이용은 호스트가 문서를 요청하면 파일서버가 호스트로 해당 문서를 전송하는 과정이다. (그림 4)에서처럼 문서요청 메시지 m을 전송한다. 암호화 요청 메시지 c를 복원 후 요청파일을 검색하고 파일서버는 검색파일을 암호화하여 호스트로 전송한다.



(그림 4) 문서 생성(편집) 절차



(그림 5) 문서 이용 절차

파일서버는 검색파일 m과 서버 인증 다이제스트 ID_s로 *Encrypt*($Q_{i,j}, m, ID_s$)를 통해 (R, c, S, M)을 호스트로 전송한다. 호스트는 *Decrypt*($d_{i,j}, (R, c, S, M)$)를 통해서 *Verify*(R, S, M)로 검증하고 $m = c \oplus H_2(\hat{e}(d_{i,j}, R))$ 으로 복호화 한다.

5. 성능 및 보안성 분석

Weil Pairing IBE를 채용한 본 유통 시스템은 여러 가지 장점이 있다. 첫째 인증서 관리부담이 없고, 둘째 이중키에 유효기간이 내포되므로 키노출로 인한 위험이 적고, 셋째 암복호화와 인검증의 수행성능이 우수하고 동시에 보안성에서 수행성능에 영향을 미치지 않고 안전을 보장한다.

보안성 분석

일반적으로 IBE는 노출에 취약할 것으로 판단하지만 그 정도는 일반 공개키 방식과 차이가 없다. 키 크래킹에 대한 암호분석 안전도는 Weil Pairing IBE는 DLP 문제로서 일반 RSA 방식 보다 안전하다.

3.2절에서 암복호화 알고리즘 *exp-5,6*은 *exp-3*과 일치

하는 것을 증명하였으므로 이 IBE 기반 알고리즘은 강력한 보안조건 IND/NM 특성을 가진 ID-IND/NM-CCA이다[31].

비밀성, 인증성, 무결성

IBE의 비밀성은 조작된 평문을 이용한 공격 CPA (chosen plaintext attack); 조작된 암호문을 이용한 공격 CCA(chosen ciphertext attack)으로부터 암호분석에 사용될 수 있는 어떤 정보도 노출되지 않아야 한다. ROM IBE에서 적대자는 자신이 임의 생성한 사용자 ID로 질의하여 개인키를 얻을 수 있고 자신이 조작한 암호문의 복호화 질의를 통해 고난도 CCA-2 공격도 가능하다.

Weil Pairing IBE의 알고리즘 *(exp-3)*는 적대자가 얻은 정보를 이용하여 목표 암호문의 해석을 막는 IND-ID-CCA를 보장하므로 비밀성을 만족한다[19]. 동시에 임의 생성한 평문에 대한 암호문 간의 관계 벡터를 만들어 그 패턴을 분석하는 암호화 시뮬레이션을 불가능하게 하는 NM-ID-CCA도 만족한다. 어떤 평문에 대해서 암호문을 유추할 수 없으므로 무결성이 만족된다[33]. 3.3절 (5)에서 사용자 ID와 메시지 m을 결합한 다이제스트에 서명하므로 메시지와 호스트의 인증성도 달성된다.

결론적으로 본 개선안은 비밀성, 무결성 그리고 인증성까지 모두 만족한다.

복잡도 분석

암복호화와 인검증의 수행속도에서 볼 때 성능분석은 시간복잡도와 처리시간 비교로 가능하다. 단 알고리즘의 복잡도가 동일해도 수행속도는 CPU 종류, S/W 구성방법, 전용 H/W 사용에 따라서 차이가 있다. 그러나 수행속도는 복잡도 한계를 넘을 수 없다.

전통적 비밀키 DES 방식과 이중키 RSA 방식은 복잡도에서 큰 차이가 있다. DES 방식은 permutation과 XOR 연산을 16회 라운드의 반복 한다. 반면 RSA 방식은 매우 큰 소수로 매우 큰 메시지를 밑수로 지수승하는 반복적 곱셈을 수행한다.

RSA 기반 암호화의 복잡도가 (mod n)에 의존한다. 만일 $k = \lceil \log_2 n \rceil$ 라면 메시지 m에 대한 RSA 공개키 연산은 $O(k^2|m|)$, 개인키 연산은 $O(k^3|m|)$이다. 그러나 $O(k^4)$ 키생성은 메시지 m과 무관한 계산이고 $O(k^4)$의 연산이 소요되지만 $k^4 \le c$ 이므로 $O(\text{키생성}) = O(1)$ 이다.

반면에 DES 암복호 복잡도는 $O(|m|)$이다. 일반적으로 키생성 수행속도는 고려하지 않는다. 일반 해쉬함수는 그 복잡도가 $O(1) \sim O(\log n)$ 이지만 강력한 해쉬는 DES를 통해서 구현되므로 $O(Hash(m)) = O(DES)$이다.

본 시스템의 해쉬 복잡도는 메시지 m의 크기의 함수이고 DES 입출력 크기가 128비트로 커져야 한다.

$$O(Hash(m)) = O(DES)$$
$$O(Hash(ID)) = O(1)$$

이로 3.3절 primitive 함수의 복잡도를 보면,

(1) $O(KeyExtract) = O(Hash(ID))$
(2) $O(Sign) = O(Hash(m))$
(3) $O(Verify) = O(1)$
(4) $O(Encrypt) = O(\| m \|) + O(Sign)$
(5) $O(Decrypt) = O(\| m \|) + O(Verify)$
따라서
(6) $O(KeyExtract) = O(1)$
(7) $O(Sign) = O(DES)$
(8) $O(Verify) = O(1)$
(9) $O(Encrypt) = O(DES)$
(10) $O(Decrypt) = O(DES)$

결론적으로 ROM IBE 복잡도는 대칭키 DES 복잡도보다 크지 않다.

그러므로 암호화 방식 복잡도는 다음과 같다.

$$O(WIBE) = O(DES)$$

복잡도는 알고리즘의 본질을 분석한 것이고 일반적으로 암복호화 알고리즘의 비교를 목적으로 암호분석에 대한 복잡도로 계산한다. 암호분석에서 전수조사에 요구되는 수행시간을 중심으로 복잡도 비교를 한다.

수행시간 분석

일반 PKI 기반 공개키 방식은 암복호화와 인검증의 수행시간이 길고 인증서 관리로 공간요구가 크지만 현재는 암호방식 비교에서는 수행시간을 중심으로 이루어진다.

암호방식을 하드웨어로 구성할 때 1,000 ~ 10,000 * $t(DES) = t(RSA)$로서 수행시간 차이가 크다[10].

각 암호방식에 따른 수행시간을 $t(DES)$=t_{des}로 표기하고, 또 $t(RSA)$=t_{rsa}로 표기하면, 그 암호화 수행시간은

(표 1) 수행속도 비교표

암호종류	기존 공개키[10]	본 시스템
키생성	10,000 c	c
암호화	100 t_{des}	t_{des}
복호화	1,000 t_{des}	t_{des}
인증	t_{des}+ c	t_{des}
검증	t_{des}+ c	c

t^{e}_{rsa}= 100 t_{des}이고, 복호화 수행시간은 t^{d}_{rsa}=1,000 t_{des}이고, 인증 수행시간은 128비트 다이제스트를 개인키 암호화 하는 것이므로 다이제스트 계산 외 128비트 암호화 수행시간을 상수로 간주할 수 있으므로 t^{s}_{rsa}= t_{hash}+ c = t_{des}+ c이고, 검증 수행시간은 인증과 동일하므로 t^{v}_{rsa}= t_{des}+ c 이다. c는 상수이고 RSA 암복호가 128비트 다이제스트에 적용되므로 $O(Signature) = c$ 이다.

기존 RSA 방식과 본 시스템 방식에서 암복호 및 인검증의 수행시간을 요약 비교를 해보면 (표 1)과 같다.

본 시스템의 암호방식은 공개키 방식보다 높은 안정성을 가지는 반면에 그 수행시간은 대칭키 DES 수준이다. 본 암호방식은 ***Setup()*** 과정에서 다른 방식과 비교해서 많은 처리시간이 소요될 것으로 판단되지만 이는 시스템의 최초 가동에 한 번 이루어지는 과정이므로 암호방식의 수행시간에서 제외해도 무리는 없다고 판단하며, 기밀문서 m이 충분히 크다고 가정하면 (표 2)는 수행시간 비교의 대표성을 가진다.

확장성

확장성 관련 공간문제에서 만일 호스트 수가 m이고 사용자 수가 l이라고 하면 인증서 수는 $O(m+l)$ 이지만 본 시스템의 이중 인증방식을 채용하면 유지해야 할 인증서 수는 $O(m\times l)$ 이다. 한 항목이 메시지 암복호화에서 사용할 공개키-개인키 쌍을 의미한다. 키/인증서 관리 부담은 호스트 수와 사용자 수가 증가하면 기하급수적으로 커진다. 이것은 전통적 PKI 기반 공개키 방식의 알려진 문제이다. 반면에 본 시스템에서는 메시지 전송세션마다 한 키 쌍만 사용되고 유효시간이 지나고 사용을 마치면 폐기된다. 따라서 확장에 따른 키 관리부담은 전혀 존재하지 않는다.

6. 결론 및 추후연구

본 논문에서는 전통적 암호방식으로 기밀정보 유통시스템의 안전성을 보장하는 것이 가능하지만 수행시간부담이 크므로 좀 더 빠르고 공간요구가 적고 관리부담이 낮은 시스템을 설계하되 단순하여 구축비용을 낮추면서 동일한 안전성 효과를 주는 새로운 해법에 도전하였다.

본 논문은 기 설계된 시스템에 어떻게 보안성을 확보하면서 수행시간을 낮출 것인지에 집중하였다. 추후 여러 공격형태에 따라서 어떻게 안전한지에 대한 증명과 새로운 공격은 발생할 수 없는지를 연구할 것이다.

외부로 기밀문서를 유통해야 할 경우 어떠한 본 논문의 안전성을 어떻게 보장할 수 있는지를 위한 보안조치가 필요하고 IBE 방식을 어떻게 적용하는 것이 좋은지를 연구할 것이다. DRM에서는 이용 허가권을 구입자의 전자우편으로 전송하지만 그것을 장치와 결합하여 저작권이 불법 복사되는 것을 막을 방법에 IBE 방식 적용이 가능하다고 판단되며 새로운 도전이 될 것이다.

참 고 문 헌

[1] 최정현, “전자기밀문서 유출봉쇄 유통시스템 구조 연구”, 인터넷정보학회논문지, 제11권 4호 pp. 143-158, 2010-08-27

[2] 최정현, “기업비밀유통을 위한 MSEC 기반 그룹키관리 프로토콜 설계와 구현 연구”, 인터넷정보학회논문지 제11권 6호, pp.87-110, 2010-12-30

[3] 최정현, “IBE-기반 암복호 모듈기능구조 연구”, 2010년도 한국인터넷정보학회 학술발표대회 논문집, 제주 해비치 호텔 & 리조트, 2010-06-25, pp. 419-422

[4] Cheong H. Choi, “IBE based Mobile IP Security”, Proceedings for ICONI & APIC-IST 2010, Mactan Island, Philippines, 2010-12-17, pp.115-118

[5] R Anderson, ″Two remarks on public key cryptology″, 1997 Advances in Cryptology, Asiacrypt 96, Springer LNCS vol.1163 pp.26~35

[6] SIMON BLAKE-WILSON, ″Information Security, Mathematics, and Public-Key Cryptography″, 2000 Kluwer Academic Publishers, Boston. 2000

[7] 김승주, ″공개키 암호시스템의 안전한 키 길이 권고안 암호기술연구 00-2″, 한국정보보호센터,

2000.2

[8] 아재용, 고영웅, 홍철호, 유혁, "하드웨어 암호화 기법의 설계 및 성능분석", 정보과학회논문지 : 정보통신 제29권 제6호, 2002. 12, pp.625~634

[9] 박영호, "공개키 암호", 물리학과 첨단기술 March 2007,

[10] M. Baugher, R. Canetti, L. Dondeti, F. Lindholm, "The Multicast Security (MSEC) Group Key Management Architecture", RFC 4046, April 2005

[11] Dan Boneh and Matthew Frankliny, "Identity-Based Encryption from the Weil Pairing", SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[12] Victor S. Miller, "The Weil Pairing, and Its Efficient Calculation", J. Cryptology (2004) 17: 235-261

[13] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing", Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science, 2248 (2001), 514-532. Full version: Journal of Cryptology, 17 (2004), 297-319.

[14] Xun Yi, "An Identity-Based Signature Scheme From the Weil Pairing", IEEE COMMUNICATIONS LETTERS, VOL. 7, NO. 2, FEBRUARY 2003

[15] Kenneth G. Paterson, "ID-based signatures from Pairings on Elliptic Curves", http://eprint.iacr.org/2002/004.pdf

[16] S. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", Algorithmic Number Theory: 5th International Symposium, ANTS-V, Lecture Notes in Computer Science, 2369 (2002), 324-337.

[17] S. Galbraith, "Pairings", Ch. IX of I. Blake, G. Seroussi and N. Smart, eds., Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.

[18] Pairing-based crypto lounge. available at http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html.

[19] Alfred Menezes, "An introduction to pairing-based cryptography", Notes from lectures (2005) in http://www.cacr.math.uwaterloo.ca/~ajmeneze/public

[20] B. Libert and J. Quisquater, "New Identity Based Signcryption Schemes from Pairings", IEEE Information Theory Workshop, 2003. http://eprint.iacr.org/2003/023/

[21] Ran Canetti and Ron Rivest, "Pairing-Based Cryptography", Special Topics in Cryptography Instructors: Ran Canetti and Ron Rivest Lecture 25: May 5, 2004 Scribe: Ben Adida

[22] Jason Crampton, Hoon Wei, Lim Kenneth G. Paterson, "What can identity-based cryptography offer to web services?", SWS '07 Proceedings of the 2007 ACM workshop on Secure web services, ACM New York, NY, USA ©2007

[23] Marc Joye and Sung-Ming Yen, "ID-based Secret-Key Cryptography", ACM Operating Systems Review 32(4):33-39, 1998.

[24] Jon Callas, "Identity-Based Encryption with Conventional Public-Key Infrastructure", PGP Corporation Palo Alto, California, USA jon@pgp.com

[25] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, 31 (1985), 469-472

[26] Antoine Joux and Kim Nguyen, "Separating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups" (2001), http://eprint.iacr.org/2001/003.ps.gz

[27] Dan Boneh (1998). "The Decision Diffie-Hellman Problem". ANTS-III: Proceedings of the Third International Symposium on Algorithmic Number Theory (Springer-Verlag): pp 48-63.

[28] R Lu, "ID-based Encryption Scheme Secure against Chosen Ciphertext Attacks", iacr.org, 2008, eprint.iacr.org

[29] Gaetan Leurent1 and Phong Q. Nguyen, "How Risky is the Random-Oracle Model?", Advances in Cryptology - CRYPTO 2009, Lecture Notes in Computer Science, 2009, Volume 5677/2009, 445-464

[30] Claus Peter Schnorr, Serge Vaudenay, "The Black-Box Model for Cryptographic Primitives", J. Cryptology (1998) 11: 125-140

[31] A. Joux, "A one round protocol for tripartite Diffie-Hellman", Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science, 1838 (2000), 385-393. Full

version: Journal of Cryptology, 17 (2004), 263-276.
[32] M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols”, Proc. First Annual Conference on Computer and Communications Security, ACM, 1993
[33] M. Bellare, A. Desaiy, D. Pointchevalz, P. Rogaway, “Relations Among Notions of Security for Public-Key Encryption Schemes “, Advances in Cryptology { CRYPTO ’98, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed., Springer-Verlag, 1998.

◐ 저 자 소 개 ◑

최 정 현

1984년 서울대학교 컴퓨터공학과(공학사)
1988년 미국 조지아공과대학교(GIT) 대학원 컴퓨터학과(이학석사)
1992년 미국 알라바마(Alabama) 주립 어번(Auburn)대학교 대학원 컴퓨터공학과(공학박사)
1994년~현재 광운대학교 경영대학 경영정보학과 교수
관심분야 : 인터넷 프로토콜, 정보보안, 인공지능, 서비스기반기술 etc.
E-mail : chchoi@kw.ac.kr