효율적인 키이분배 및 암호시스템의 제안 : 제 I 부 [1]

임 채 훈 . 이 필 중

포항공과대학 전자전기공학과

Proposal of efficient key distribution and encryption systems : Part I [1]

Chae Hoon Lim . Pil Joong Lee

Dept. E.E., Pohang Institute of Science and Technology

요약 본 논문에서는 관용 암호시스템의 세션키이분배방법으로 매우 효율적이며 안전한 새로운 키이분배 시스템을 제안한다. 제안된 시스템은 한번 혹은 두번의 모듈라 멱승 연산만으로 세션키이 공유가 가능하므로 기존의 어떤 방식보다도 효율적이라 할 수 있다. 또한 알려진 어떤 공격에 의해서도 세션키이를 불법 계산하는 것이 불가능함을 보일 수 있으므로 안전성을 확보할 수 있다는 장점도 지닌다.

1. 서론

컴퓨터 통신망을 통한 정보교환이 빈번해짐에 따라 정보보안의 필요성에 대한 인식이 사회적으로 확산되어 가고 있으며 이를 위해 암호시스템 (cryptosystem) 을 사용하는 것이 가장 효과적인 정보보호 대책이라는 사실은 잘 알려져 있다. 전송이나 저장중인 정보를 보호하기 위한 가장 기본적인 도구로서 암/복호화 속도가 빠른 관용 암호시스템

[1] 본 논문은 한국 전자 통신 연구소에서 수탁한 연구의 결과임.

(conventional cryptosystem)이 널리 사용되고 있으나 여기서 가장 문제가 되는 것이 암호키이의 효율적인 관리방법이다. 즉 관용 암호시스템을 이용하기 위해서는 통신하고자 하는 쌍방이 그들만의 비밀키이를 안전하게 공유해야 하며 더우기 안전성을 위하여 매 세션마다 다른 세션키이 (session key)를 사용하는 것이 일반적이므로 암호망 가입자의 수가 증가함에 따라 키이관리 문제가 가장 심각한 과제로 등장하게 된다.

암호키이의 관리방법으로 관용 암호법을 이용하여 중앙의 키이분배센타 (key distribution center : KDC)에서 모든 사용자들의 세션키이를 일괄적으로 분배해 주는 중앙집중형의 키이 관리방법 [1] [2]이 주로 사용되어 왔지만, 이 방식은 모든 사용자들의 세션키이를 KDC에서 발생 분배하므로 KDC에 대한 절대적인 신뢰를 기반으로 해야 하며 또한 각 사용자들의 터미날키이는 여전히 사람에 의해 분배해야 한다는 문제점이 제기된다. 보다 일반적이며 효율적인 키이 관리방법으로 공개키이 암호법 (public key cryptography)을 이용한 Diffie-Hellman형의 공개 키이분배 시스템 (public key distribution system) [3]이 널리 연구되어 왔다.

본 논문의 제 I부에서는 기존에 발표되었던 각종 Diffie-Hellman형의 공개 키이분배 시스템들을 간략히 살펴보고 보다 효율적이면서도 안전성을 잃지않는 새로운 키이분배 시스템들을 제안하고자 한다. 대부분의 기존방식들에서는 각 사용자들이 세션키이 공유를 위해서 시간이 많이 걸리는 모듈라 멱승 (modular exponentiation)을 세번씩은 계산해야 하는 반면 본 논문에서 제안하는 방식은 최소 한번의 모듈라 멱승 연산만으로도 세션키이를 공유할 수 있으므로 기존의 어떤 방식보다도 효율적이라 할 수 있다. 또한 세션키이를 불법 계산하는 것이 이산대수 문제 (discrete logarithm problem)나 소인수분해 문제등과 같이 잘 알려진 어려운 문제를 풀 수 없는 한 불가능하다는 것을 보일 수 있으므로 안전성을 확보할 수 있다는 장점도 지닌다.

한편 제 II부에서는 I부에서 제안된 대칭형의 키이분배 시스템을 일방향의 통신 (one-way communication)만을 이용하는 키이분배 시스템으로 변형시켜 보고, 또한 공개키이 디렉토리 및 각 사용자간에 상호인증 (mutual authentication) 기능을 제공할 수 있도록 제안된 시스템을 확장시켜 보기로 한다. 아울러 제안된 키이분배 시스템을 응용하면 키이분배와 동시에 안전한 암호화 기능까지도 제공할 수 있음을 보인다. 따라서 본 논문에서 제안된 시스템들을 통합 구현한다면 특정한 암호시스템을 갖추지 않은 환경에서도 완전한 암호시스템을 구축할 수 있으므로 일석이조의 효과를 거둘 수 있을 것이다.

2. 기존방식들에 대한 고찰

1976 년 Diffie 와 Hellman 이 공개키이 암호시스템의 개념을 제안한 논문 [3] 에서 유한체 (finite field) 상의 이산대수 문제를 푸는 것이 계산상 불가능 (computationally infeasible) 함을 이용한 공개 키이분배 시스템을 최초로 선보인 이래 정수링 Z/mZ 나, 메트릭스링, 허(실)수이차체 (imaginary/real quadratic field) Q(√D) 및 타원곡선 (elliptic curve) 등 이산대수 문제가 어려운 한 어떤 대수적 구조체에서나 이 Diffie-Hellman 의 키이분배 시스템을 변형 적용시킬 수 있다는 사실이 많은 학자들에 의해 연구 발표되어 왔다 [4] - [10]. 특히 RSA 법 (modulus) 과 같은 형태의 합성수 m 에 대해 정수링 Z/mZ 상의 곱셈군 (multiplicative group) 구조를 이용한 Composite Diffie-Hellman 방식이나 음의 합성수 D 에 대해 허수이차체 Q(√D) 상의 클래스군 (class group) 구조를 이용한 Diffie-Hellman 방식은 이들을 깨는 것이 합성수 m 이나 D 를 소인수분해하는 것만큼 어렵다는 것을 증명할 수 있으므로 원래의 Diffie-Hellman 방식에 비해 그 안전성을 보다 확고히 보장할 수 있다는 장점을 지닌다.

한편 원래의 Diffie-Hellman 방식이나 이를 다른 대수적 구조체에 적용시킨 방식들은 모두가 항상 동일한 세션키이를 초래한다는 결함이 있다. 따라서 보다 실용적인 키이분배 시스템으로 사전 통신 (preliminary communication) 을 통하여 랜덤정보를 서로 교환함으로써 매번 다른 세션키이를 얻을 수 있도록 이들을 일반화시킨 방식들에 대한 연구도 활발히 진행되어 왔다. 이들 일반화된 Diffie-Hellman 방식의 각종 변형들에 대해서는 참고문헌 [11] 에 상세히 분석되어 있으며 비록 엄격한 증명은 어려우나 지금까지 알려진 공격방법으로는 깨어지지 않는다는 점에서 안전한 시스템으로 분류될 수 있는 방식들을 소개해 보기로 한다.

우선 시스템 설계 및 안전성 분석의 바탕이 되는 키이분배 시스템에 대한 가능한 공격방법들을 분류해 보면 다음과 같다. 즉 공격자들의 공격양상에 따라서는 passive attack 과 impersonation attack 으로 나눌 수 있고, 또한 공격자들이 보유한 정보량에 따라서는 ciphertext-only attack 과 known-key attack 으로 나눌 수 있으므로 다음의 4 가지 공격방법을 생각할 수 있다 [11] [12].

♦ Ciphertext-Only Passive (COP) attack : 가장 단순한 공격방법으로 공격자는 단지 두 사용자간에 교환되는 정보의 관측만을 통하여 (wire-tapping) 세션키이를 불법 계산하려고

한다.

♦ Ciphertext-Only Impersonation (COI) attack : 공격자가 이용 가능한 정보는 COP attack 과 마찬가지로 통신로상에서 관측한 전송정보 뿐이나 여기서는 공격자가 한 사용자를 가장하여 전송정보를 조작함으로써 다른 사용자와 세션키이를 공유하려고 시도한다.

♦ Known-Key Passive (KKP) attack : 과거의 세션키이 및 관련 전송정보를 보유한 공격자가 현재 세션에서 통신로상의 전송정보를 관측하여 세션키이를 불법 계산하려고 하는 공격방법이다.

♦ Known-Key Impersonation (KKI) attack : 과거의 세션키이 및 관련 전송정보를 보유한 공격자가 현재 세션에서 impersonation attack 을 시도하는 경우 (KKP + COI) 와, 과거 세션에서 COI attack 을 시도하여 비록 성공하지는 못하였지만 이때의 합법적인 사용자가 계산했던 세션키이를 어떤 경로로던 입수하여 현재 세션에서 impersonation attack 을 시도하는 경우로 나누어 생각할 수 있다. 특히 후자의 경우는 키이분배 시스템에서 생각할 수 있는 가장 강도 높은 공격방법이나 이에 필요한 정보를 입수하는 것이 또한 그만큼 어렵다는 것을 알 수 있다.

이제 위에서 언급한 어떤 공격방법에 의해서도 합법적인 사용자와 세션키이를 공유하는 것이 불가능하다는 점에서 안전한 시스템으로 생각되는 예들을 소개하기로 한다. 각 시스템은 두 사용자 i, j 에 대해 완전 대칭이므로 한 사용자 i 에 대해서만 기술하기로 하며, 원래 저자들에 의해 제안되었던 방식이 유한체 GF(p), p 는 소수, 상의 연산을 이용하였더라도 가능한 한 합성수 m 을 법으로 하는 정수링 Z/mZ 상의 곱셈군 구조를 이용한 형태로 기술하기로 한다. 이는 앞에서도 언급했듯이 정수링상의 Diffie-Hellman 문제는 이를 깨는 것이 m 을 소인수분해하는 것만큼 어렵다는 사실이 증명되었으므로 공개문제로 남아있는 유한체 GF(p) 상의 Diffie-Hellman 문제에 비해 안전성을 높일 수 있기 때문이다. 공통의 법 m 과 기본원소 g 는 모든 사용자들에게 잘 알려져 있고 각 사용자 i 는 자신의 비밀키이 S_i 에 대응하는 공개키이 $P_i \equiv_m g^{S_i}$ 를 공개하여 모든 사용자들이 이용 가능하게 한다. 여기서 기호 $\equiv_m$ 은 congruence mod m 을 뜻하며 m 으로 나누었을때의 나머지를 나타내는 연산기호이다. R_i 는 사용자 i 에 의해 선택된 랜덤수이다.

• 전송 : $Z_i \equiv_m M^{R_i}$, $M \equiv_m g^{S_iS_j}$; 세션키이 : $K_i \equiv_m Z_j^{R_i} \equiv_m M^{R_iR_j}$ [13]

• 전송 : $Z_i \equiv_m g^{R_iS_i}$; 세션키이 : $K_i \equiv_m (Z_j \cdot P_j^{R_i})^{S_i} \equiv_m g^{S_iS_j(R_i+R_j)}$ [14]

• 전송 : $Z_i \equiv_m g^{R_i}$; 세션키이 : $K_i \equiv_m Z_j^{S_i} \cdot P_j^{R_i} \equiv_m g^{S_jR_i+S_iR_j}$ [15]

• 전송 : $Z_i \equiv_m M \cdot g^{R_i}$, $M \equiv_m g^{S_i S_j}$; 세션키이 : $K_i \equiv_m Z_j \cdot M^{-1} \equiv_m g^{R_i R_j}$ [16]

• 전송 : $Z_i = S_i + R_i$; 세션키이 : $K_i \equiv_m (g^{Z_j} \cdot P_j^{-1})^{S_i} \oplus g^{R_j S_j} \equiv_m g^{R_i S_i} \oplus g^{R_j S_i}$

지금까지 두번 이하의 모듈라 멱승 연산만으로 세션키이 계산이 가능한 것으로 깨어지지 않은 방식은 발표된 적이 없으며 위의 방식들은 모두 각 사용자들이 세션키이를 계산하는데 세번씩의 모듈라 멱승이 필요하다는 것을 알 수 있다. 위의 방식들 중 출처가 표시되지 않은 마지막 방식은 Yacobi등의 방식 [17] 을 약간 변형하여 본 저자들이 개발한 것이나 다른 방식들에 비해 별다른 잇점이 없으므로 위의 예들에 포함시켰다.

3. 제안방식 및 안전성 분석

키이분배 시스템은 대규모의 암호망에서 각 사용자들이 필요할 때마다 원하는 상대방과 안전하게 세션키이를 공유할 수 있도록 해야 하므로 첫째는 안전성을 보장할 수 있어야 한다. 또한 매 세션마다 키이를 공유해야 하므로 가능한 적은 전송량과 계산량으로 키이 공유에 걸리는 시간을 최소화해야 한다. 대부분의 키이분배 시스템이 공개키이 디렉토리와의 접속외에 양방향으로 1회씩의 전송을 기본으로 하므로 전송량에 있어서는 거의 차이가 없으나 문제는 안전성을 잃지 않으면서도 계산량을 최소화하여 속도를 높이는 것이다.

따라서 본 논문에서는 안전성 보장 및 효율성 향상을 주 목표로 하여 전송함수 및 세션키이 계산함수에서 시간이 많이 걸리는 모듈라 멱승의 수를 최소화하고 보다 간단하면서도 안전성을 확보할 수 있는 연산들을 사용하고자 한다. 본 논문에서 제안하고자 하는 키이분배 시스템은 다음의 몇가지 사실들에 바탕을 둔다.

♦ 예비전송 단계에서는 각 사용자들이 발생시킨 랜덤수 자체를 공개적으로 교환하도록 한다. 이같은 전송은 추가의 연산이 필요없을 뿐더러 ciphertext-only (COP, COI) attack 하에서는 공격자가 추가로 얻을 수 있는 정보가 아무것도 없기때문에 known-key (KKP, KKI) attack 하에서만 시스템의 안전성을 고려하면 되므로 가장 간단하면서도 효율적인 방법이라고 할 수 있다.

♦ 시간이 많이 걸리는 모듈라 멱승의 수를 최소화하기 위해서 세션키이 계산시 두 사용자간의 고정된 비밀 공유키이 $M \equiv_m g^{s_i s_j}$ 을 계산하는 것 이외의 모듈라 멱승 연산은 가능한 피하도록 한다.

♦ KKP attack 하에서 시스템이 안전하기 위해서는 과거의 세션키이들이 알려진다 하더라도 이로부터 M 을 구하는 것이 계산상 불가능하도록 세션키이 계산함수를 선택해야 한다. 예비통신 단계에서 단순히 랜덤수 자체를 공개적으로 교환하도록 한 전송함수의 특성상 이 M 이 시스템의 유일한 비밀정보가 될 것이다.

♦ KKI attack 하에서 시스템이 안전하기 위해서는 공격자가 전송정보를 조작하여 그가 알고있는 과거의 세션키이를 합법적인 사용자로 하여금 다시 계산하도록 하는 것이 계산상 불가능하도록 세션키이 계산함수를 선택해야 한다.

위의 설계지침들을 바탕으로 하는 간단하면서도 효율적인 방식으로 다음과 같은 키이분배 시스템을 제안한다. 사용자 i가 통신을 시작하는 것으로 가정하며 프로토콜은 완전 대칭이므로 한 사용자 i 에 대해서만 기술한다.

[제안방식 1]

❶ 사용자 i 는 공개키이 디렉토리로부터 사용자 j 의 공개키이 $P_j \equiv_m g^{s_j}$ 를 얻고 이를 이용하여 j 와의 공유키이 $M \equiv_m P_j^{s_i} \equiv_m g^{s_i s_j}$ 를 계산한다.

❷ 사용자 i 는 랜덤수 $R_i \in [0,m)$ 를 선택하여 비밀통신을 요구하는 메세지와 함께 사용자 j 에게 전송한다.

❸ 사용자 i 는 자신이 선택한 랜덤수 R_i, j 로부터 받은 R_j, 그리고 ❶ 에서 얻은 공유키이 M 의 함수로 계산된 $R = f(R_i, R_j, M)$ 을 이용하여 세션키이 $K_i \equiv_m R^E$ 혹은 g^R 를 계산한다. 여기서 $E(\geq 2)$ 는 모든 사용자들에게 알려진 공통의 수로 계산량을 줄일 수 있도록 2 나 3 정도의 작은 수가 적당할 것이다. 그리고 $R = f(R_i, R_j, M)$ 은 다음 방법들 중의 하나로 계산될 수 있다.

$$\text{i) } R \equiv_m R_i^E \oplus R_j^E \oplus M, \quad \text{ii) } R \equiv_m (M \oplus R_i) \cdot (M \oplus R_j), \quad \text{iii) } R \equiv_m (M \cdot R_i) \oplus (M \cdot R_j)$$

위의 제안방식은 앞에서도 언급했듯이 ciphertext-only attack 하에서는 zero-knowledge protocol 이므로 known-key attack 하의 안전성만을 고려하면 될 것이다. 이 중 KKP attack

에 대해서는 세션키이 계산함수가 $K_i \equiv_m R^E$ 혹은 g^R 의 형태이므로 알려진 세션키이로부터 비밀정보 M을 얻기 위해서는 최소한 mod m 으로 E-제곱근을 구하거나 이산대수문제를 풀어야하는 어려움에 직면하게 된다. 따라서 제안방식은 KKI attack 하의 안전성만을 고려하면 충분할 것이다.

한편 KKI attack 하에서는 공격자가 교환되는 랜덤수 중의 하나를 조작하여 그가 알고 있는 과거의 세션키이를 합법적인 사용자로 하여금 다시 계산하게 하는 방법 (replay attack) 이외에는 아무런 이득이 없다는 것을 알 수 있다. 즉 예비전송 단계에서 랜덤수 자체를 누구나 알 수 있게 공개적으로 교환하고 있으므로 공격자가 자신이 마음대로 선택한 임의의 랜덤수를 전송한다 하더라도 위와 같은 replay attack 의 경우를 제외하면 KKI attack 은 KKP attack 과 다를 것이 없게 된다. 특수한 경우로 사용자 i와 세션키이를 불법 공유하려고 하는 공격자가 사용자 i로부터 오는 랜덤수를 그대로 사용자 j가 전송한 것처럼 하여 되돌려 보낸다면 제안방식에서 사용된 mod-2 addition 의 성질상 프로토콜이 실패하게 되는 경우가 생길 수 있으므로 상대방으로부터 받은 랜덤수를 점검하여 이같은 경우는 검출해 낼 필요가 있을 것이다.

이제 R 을 계산하는 세 함수 각각에 대하여 랜덤수를 조작하여 과거의 세션키이를 재계산하게 하는 것이 불가능함을 증명해 보기로 한다. 공격자는 사용자 j를 가장하여 사용자 i와 세션키이를 불법 공유하려고 하며 또한 KKI attack 이 가정하는 것처럼 공격자는 과거의 전송정보 및 해당 세션키이를 소유하고 있는 것으로 가정한다. 과거의 해당정보들은 홑따옴표(') 를 써서 표기하기로 한다.

❑ $R \equiv_m R_i^E \oplus R_j^E \oplus M$ 의 경우

이 경우에는 공격자가 $K_i' \equiv_m R'^E$ 혹은 $g^{R'}$, $R' \equiv_m R_i'^E \oplus R_j'^E \oplus M$ 을 소유하고 있으며 현재 세션에서 사용자 i가 전송하는 R_i 에 대하여 이 K_i' 를 사용자 i로 하여금 재계산하게 하려고 한다. 따라서 공격자는 $R_a^E \oplus R_i^E \equiv_m R_i'^E \oplus R_j'^E$ 을 만족하는 랜덤수 R_a 를 사용자 i에게 전송해야 하나 이와같은 R_a 를 전송하려면 공격자는 mod m 으로 E-제곱근을 구해야 하므로 이 공격은 성공할 수 없음을 알 수 있다.

❑ $R \equiv_m (M \oplus R_i).(M \oplus R_j)$ 와 $R \equiv_m (M.R_i) \oplus (M.R_j)$ 의 경우

이 두 함수의 경우는 비밀수와 알려진 랜덤수의 mod-2 addition 이나 modular

multiplication 의 결과 역시 랜덤한 비밀수가 되며 또한 mod-2 addition 이 비트단위의 연산이므로 modular multiplication 과의 사이에 아무런 상관관계가 성립하지 않음을 이용한 것이다. 공격자가 조작할 수 있는 랜덤수는 R_j 하나 뿐이며 R_i 는 매 세션마다 사용자 i 에 의해 랜덤하게 선택될 것이므로 어떤 경우에도 과거의 값과 같은 R 을 재발생시키는 것은 불가능함을 알 수 있다.

한편 제안방식에서 $R \equiv_m (M \oplus R_i).(M \oplus R_j)$ 나 $R \equiv_m (M . R_i) \oplus (M . R_j)$ 의 경우는 다음과 같이 변형하여도 원래의 방식과 동등함은 쉽게 알 수 있다.

[제안방식 1 의 변형]

❶ 사용자 i 는 j 와의 공유키이 M 과 자신이 발생시킨 랜덤수 R_i 를 이용하여 전송정보 $Z_i = M \oplus R_i$ 를 계산하여 j 에게 보낸다.

❷ 사용자 i 는 j 에게서 받은 Z_j 로부터 $Z_j \oplus M = R_j$ 를 얻고 세션키이로 $K_i \equiv_m R^E$ 혹은 g^R 을 계산한다. 여기서 $R \equiv_m R_i . R_j$ 나 $(M . R_i) \oplus (M . R_j)$ 이다.

(만일 전송정보로 $Z_i \equiv_m M . R_i$ 를 사용한다면 $R = R_i \oplus R_j$ 혹은 $R \equiv_m (M \oplus R_i).(M \oplus R_j)$, $R_j \equiv_m Z_j . M^{-1}$ 로 하여 세션키이로 K_i 를 계산할 수 있을 것이다.)

이상에서 살펴보았듯이 제안된 키이분배 프로토콜은 단지 한번이나 두번의 모듈라 멱승 연산이면 세션키이 공유가 가능하며, 또한 알려진 어떤 공격에 대해서도 세션키이를 불법 계산하는 것이 불가능하므로 매우 효율적이면서도 안전한 방식이라고 할 수 있다. R 을 계산하는 함수는 위에서 예로들었던 세가지 대표적인 방식 이외에도 이를 변형한 $R = f(R_i, R_j, M) \equiv_m (R_i \oplus M)^E \oplus (R_j \oplus M)^E$, $[M . (M \oplus R_i)] \oplus [M . (M \oplus R_j)]$ 혹은 $E_M(R_i) \oplus E_M(R_j)$ ($E_M(.)$ 는 M 을 키이로 하는 관용 암호시스템의 암호화 알고리즘) 등과 같이 함수 f(.) 가 known-key attack 하에서 파라독스 (paradox) 를 피할 수 있도록 비밀정보 M 을 랜덤화시켜 주고 또한 어느 한 랜덤수의 조작에 의해 같은 값을 반복 계산하게 하는 것이 불가능한 함수이면 R 을 계산하는 함수로 안전하게 사용될 수 있을 것이다.

한편 랜덤수를 공개적으로 교환하고 공유키이 M 을 유일한 비밀정보로 하여 랜덤한 세션키이를 안전하게 계산할 수 있는 또다른 방법으로 다음과 같은 시스템을 생각할 수 있다.

[제안방식 2]

❶ 각 사용자 i 와 j 는 공개키이 디렉토리로부터 상대방의 공개키이를 얻어 그들간의 공유키이 $M \equiv_m g^{S_i S_j}$ 를 계산하고 각자가 선택한 랜덤수 R_i 와 R_j 를 공개채널을 통하여 서로 교환한 후 $R \equiv_m R_i^E \oplus R_j^E \oplus M$ 을 각각 계산한다.

❷ 각 사용자는 R, M 을 각각 R_o 와 R_e, M_o 와 M_e 로 나누고 $I_1 \equiv_m (R_o + M_e)^E$, $I_2 \equiv_m (R_e + M_o)^E$ 를 계산한다. 여기서 X_o 는 X 의 홀수번째 비트는 그대로 두고 짝수번째 비트를 0 으로 한 결과이며 X_e 는 그 반대이다. 따라서 $R_o + M_e$ 는 홀수번째 비트값은 R 에서 짝수번째 비트값은 M 에서 취한 결과가 된다.

❸ 이제 두 사용자는 세션키이로 $K_s \equiv_m (I_1 \oplus I_2)^E$ 를 계산한다.

(제안방식 1 의 변형에서와 마찬가지로 과정 ❶ 에서 랜덤수 R_i 대신에 $M \oplus R_i$ 나 $M . R_i$ 를 교환하고 R 을 $R \equiv_m R_i^E \oplus R_j^E$ 이나 $(R_i . R_j)^E$ 으로 계산할 수도 있을 것이다.)

위의 제안방식 역시 제안방식 1 과 마찬가지로 어떤 공격하에서도 안전함을 쉽게 알 수 있다: I_1 과 I_2 를 계산하는 과정에서 R 과 M 의 비트단위의 혼합을 멱승함으로써 M 이 충분히 랜덤화되어 I_1 과 I_2 는 거의 독립된 두 비밀수의 역할을 할 것이고 이들을 mod-2 addition 한 결과를 E-제곱하여 세션키이를 계산하였으므로 세션키이가 노출된다 하더라도 이로부터 M 을 계산하는 것은 불가능하다. 또한 KKI attack 하에서 과거의 세션키이를 재발생시키기 위해서는 mod m 으로 E-제곱근을 구해야하므로 이 공격 역시 성공할 수 없음은 명백하다. 따라서 이 제안방식 역시 한번의 모듈라 멱승과 소수의 모듈라 곱셈이면 안전하게 세션키이를 공유할 수 있을 것이다.

이상에서 가능한 적은 계산량으로 세션키이를 안전하게 분배할 수 있는 시스템들을 제안하였다. 제안된 시스템들은 시간이 많이 걸리는 모듈라 멱승의 수를 줄이기 위해 예비전송 단계에서는 랜덤수 자체를 공개적으로 교환하는 방법을 택하였으며, 또한 세션키이 계산시에도 모듈라 멱승보다는 관련된 두 수를 비트단위에서 혼합시킬 수 있는 빠른 연산들을 주로 사용하여 두 사용자간의 비밀 공유키이 M 을 가능한 랜덤화시킨 후 그 결과를 멱승하는 방법으로 세션키이를 계산하도록 하였다. 이같은 접근방법으로 설계된 시스템들은 세션키이를 불법 계산하는 것이 소인수분해 문제나 이산대수 문제 등과 같이 잘 알려진 어려운 문제들을 푸는 것만큼 어렵다는 것을 증명할 수 있거나 혹

은 증명은 어렵더라도 그것이 불가능함을 보일 수 있으므로 그 안전성을 보장할 수 있었다. 본 논문에 연결된 제 II 부에서는 이들을 일방향 키이분배 시스템으로 변형시키거나 이들을 응용하여 상호인증 및 암호화 기능을 제공할 수 있음을 보일 것이다.

4. 결론

본 논문에서는 관용 암호시스템의 실제 운영에 있어서 가장 문제가 되는 세션키이의 효율적인 분배방법으로 Diffie-Hellman 형의 공개 키이분배 시스템의 일반형에 대한 새로운 키이분배 프로토콜들을 제시하였다. 기존의 방식들에서 보이는 효율성 저하를 극복하기 위해 가능한 시간이 많이 걸리는 모듈라 멱승 연산을 피하고 간단하면서도 빠른 연산들을 이용하여 최소 한번의 모듈라 멱승만으로 세션키이를 안전하게 분배할 수 있도록 하였다.

[참고문헌]

[1] W.F.Ehrsam, S.M.Matyas, C.H.Meyer, and W.L.Tuchman, "A cryptographic key management scheme for implementing the Data Encryption Standards," IBM Systems J., 17, No.2, 1978, pp.106-125.

[2] "Banking-key management (wholesale)," International Standard ISO8732, International Organization for Standardization, Geneva, 1988.

[3] W.Diffie and M.E.Hellman, "New direction in cryptography," IEEE Trans. Inform. Theory, IT-22, 6, 1976, pp.644-654.

[4] Z.Shmuely, "Composite Diffie-Hellman public key generating systems are hard to break," TR.No.356, Computer Science Dept. Technion-Israel Institute of Technology, Feb. 1985.

[5] K.S.McCurley, "A key distribution system equivalent to factoring," J. Cryptology, Vol.1, No.2, 1988, pp.95-106.

[6] R.W.Odoni, V.Varadaharajan, and P.W.Sanders, "Public key distribution in matrix ring," Electronic Letters 20, 1984, pp.386-387.

[7] J.A.Buchman and H.C.Williams, "A key-exchange system based on imaginary quadratic fields," J.Cryptology 1, 1988, pp.107-118.

[8] ___ , "A key exchange system based on real quadratic fields," Proc. Crypto'89 : Advances in Cryptology, Lecture notes in Computer Science 435, Springer-Verlag, 1990, pp.335-343.

[9] V.Miller, "Use of elliptic curves in cryptography," Proc. Crypto'85 : Advances in Cryptology, Lecture notes in Computer Science 218, Springer-Verlag, 1986, pp.417-426.

[10] N.Koblitz, "Elliptic curve cryptosystems," Math. Comp. 48, 1987, pp.203-209.

[11] 이필중, 임채훈, "일반화된 Diffie-Hellman 키이 분배방식의 안전성 분석," 한국통신학회논문지 제 16 권 7 호, 7/91, pp.575-597.

[12] Y.Yacobi, "A key distribution paradox," Proc. Crypto'90, pp.245-255.

[13] T.Yamamoto and R.Akiyama, "A data encryption device incorporating fast PKDS," Proc. IEEE Global Telecom. Conf., Nov.-Dec. 1983, pp.1085-1090.

[14] E.Okamoto and and K.Nakamura, "A note on public key distribution system," 1984 Natl. Conf. Rec. on IECE Japan, 15, Oct. 1984.

[15] T.Matsumoto, Y.Takashima, and H.Imai, "On seeking smart public key distribution systems," Trans. IECE Japan, V0l.E.69, No.2, 1986, pp.99-106.

[16] 문상재, 이필중, "키이분배 프로토콜의 제안," 제 2 회 정보보호와 암호에 관한 workshop 논문집, 1990, pp.117-124.

[17] Y.Yacobi and Z.Shmuely, "On key distribution systems," Proc. Crypto'89, pp.344-355.