特輯 技術解說

암 호

金 大 豪
韓國電子通信研究所

Ⅰ. 암 호

1. 암호학의 정의

정보보호의 필요성은 수천년 전부터 매우 중요한 개념으로 인식되어 왔으며, 또한 상대방의 비밀 정보를 가로채어 자신에게 유리한 정보를 얻고자 하는 노력 역시 계속 경주되어 왔다. 비밀 정보 보호의 필요성은 정보를 보호하는 가장 좋은 수단인 암호시스템에 관한 연구의 동기가 되었다. 만약 제3자가 결코 획득할 수 없는 전송수단이 존재한다면, 그 정보는 매우 안전하며, 정보를 보호하기 위한 수단의 강구는 필요하지 않을 것이다. 그러나 그러한 전송수단은 현재 존재하지 않으며, 전송로상의 정보는 항상 제3자가 획득할 수 있다고 가정해야 한다. 이런 가정하에서 정보를 보호할 수 있는 최선의 방법은 암호시스템을 구성하여 제3자가 정보를 획득하더라도 그 의미를 분석할 수 없도록 하는 것이다. 이것이 바로 암호시스팀을 이용하는 가장 큰 이유라고 할 수 있다.

암호학(cryptology)은 정보보호 수단인 암호와 그 해독에 관한 제 문제를 취급하는 학문으로 그 어원은 그리스어의 "Kryptos logos"인데 이는 숨겨진 말(hidden words)이란 뜻을 지니고 있다.

그림 1의 모델을 이용하여 살펴보기로 한다.

평문(plaintext 혹은 clear text)은 보호의 대상이 되는 본래의 통신문으로, 그 의미를 제3자가 이해할 수 없도록 변형한 것이 암호문(ciphertext 혹은 cryptogram)이다. 이 변환을 암호화(encryption 혹은 encipherment)라고 하고, 역으로 암호문을 본래의 평문으로 복원하는 과정을 복호화(decryption 혹은 decipherment)라고 한다. 이러한 변환을 정하는 것이

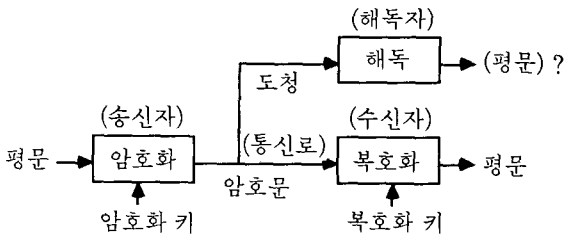


그림 1. 암호 통신의 모델

알고리즘(algorithm)과 그 파라메타가 되는 키(key)이다. 도청자는 알고리즘이나 키의 정보를 가지지 않고 본래의 평문이나 키의 정보등을 알아내려고 하는데, 이것이 암호해독(cryptanalysis)이다.

2. 암호학의 역사적 배경

암호학의 발달과정은 문자 대입방법을 주로 사용하던 시대와 복잡한 기계등을 이용한 시대, 그리고 복잡도가 매우 높은 암호 알고리즘을 사용하는 현대 암호학의 시대등 3단계로 분류된다.

제1단계는 단순한 문자 대입방법을 주로 사용한 시대이며, 고대로부터 19세기 말까지로 분류된다. 이 시대의 암호화 과정에서는 통계적으로 나타나는 평문 문자의 특성을 배제하지 못하고 있으므로, 암호문의 통계적 특성을 분석하여 암호문을 해독할 수 있다. 이 시대를 대표하는 암호시스템으로 시이저 암호(Caesar cipher), Vigenere cipher 그리고 미국 남북전쟁시 남군이 사용한 Beaufort cipher 등을 들 수 있다.

제2단계는 20세기초 전산기가 일반화된 시점으로부터 50년대 말까지로 분류된다. 이 시대의 암호시

스템은 주로 복잡한 기계를 이용하여 암호 알고리즘을 실현하였다. 이런 암호시스템에서 생성된 암호문을 해독하기 위해서는 엄청난 계산량이 요구됨으로 그 당시에는 안전한 시스템이었다. 그러나 컴퓨터의 발달과 새로운 해독 방식이 개발됨으로 인하여 오늘날에는 이런 종류의 암호 시스템을 안전한 시스템이라고 할 수 없게 되었다. 2차 세계 대전중 제 2 단계의 한 암호시스템을 공격하기 위하여 초기 컴퓨터의 일종인 Colossus가 개발되었다는 사실은 컴퓨터의 발달이 암호 해독기법 연구와 밀접한 관계가 있었음을 입증하여 준다. 이 시대에 사용된 복잡한 기계를 일반적으로 Rotor Machine이라고 부른다. 대표적인 기계로는 2 차 대전중 사용된 독일의 ENIGMA, 미국의 M-209등을 들 수 있다.

제 3 단계는 현대 암호학의 시대이며, 1940년대 말 C. E. Shannon이 'Communication theory of secrecy system'이란 논문을 발표한 그 시점을 현대 암호학의 시작으로 간주한다. 70년대 초 전자산업의 획기적인 발달로 인하여, Shannon의 이론과 이로부터 발전된 전반적인 각종 이론 등에 부합되는 복잡도가 높은 암호 알고리즘의 실현이 가능하게 되었다. 이러한 사실때문에 70년대 초를 실질적인 현대 암호학의 시점으로 간주하기도 한다.

Ⅱ. 암호 기술의 기초

암호시스템은 일반적으로 그림 2와 같이 구성되어 있다. 송신자 A는 평문 M을 암호화 키 K_e로 암호화하고, 암호문 $C=E(K_e, M)$을 보낸다. 수신자 B는 K_e와 대응되는 복호화 키 K_d로 암호문을 복호화하여, 본래의 평문 $M=D(K_d, C)$를 얻는다. 그러나 K_d를 알지 못하는 제 3 자는 암호문 C로부터 평문 M을 얻는 일(해독)이 실제적으로 불가능하여야 한다.

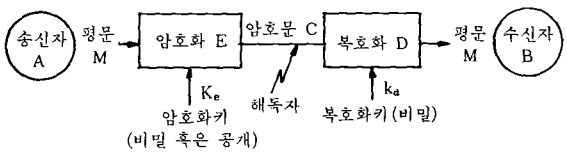


그림 2. 암호시스템

1. 비밀 키 암호시스템(secret key cryptosystem)

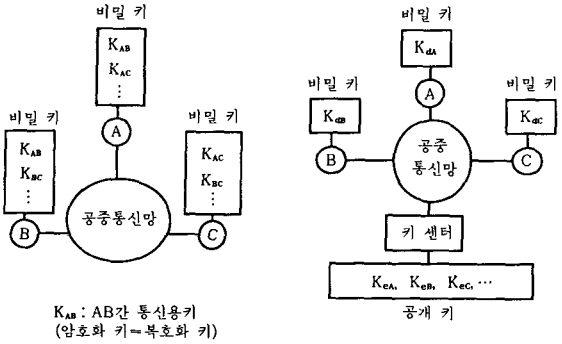
비밀 키 암호시스템이란, 암호화 키 K_e와 복호화 키 K_d가 같고, 송신자와 수신자가 공통의 비밀키를 가지는 암호방식으로, 공통키 암호방식, 대칭 암호방식이라고도 한다. 문자의 순서를 바꾸는 전치식(permutation, 예;KOREA→RAEOK), 문자를 다른 문자로 바꾸는 환자식(substitution, 예;KOREA→TXACQ)이 오래전부터 사용되어지고 있다. 전치와 환자의 대응표가 키가 되고, 제 3 자가 알지 못하도록 송신자와 수신자가 공유한다. 군사나 외교에 있어서는 전치식인가 환자식인가하는 암호의 알고리즘도 비밀로 하고 있다. 예를들어 Veman 암호에서는 키가 되는 난수열의 생성방법은 비밀이다. 그러나 DES나 FEAL등의 상용 암호에서는 암호 알고리즘을 공개하고 키만을 비밀로 한다.

2. 공개 키 암호시스템(public key cryptosystem)

비밀 키 암호시스템은 송-수신자가 동일한 키에 의하여 암호화 및 복호화 과정을 수행하므로, 키를 안전하게 전송하고 보관함에 있어 어려움이 야기됨에 따라 키관리는 필연적으로 요구된다. 실제로 어떤 통신망은 너무 복잡하여 키관리가 곤란할 수도 있다. 키 관리의 이러한 어려움을 해결하기 위하여 제시된 개념이 공개 키 암호시스템이다. 공개 키 암호시스템은 암호화 및 복호화 과정에서 서로 다른 키를 사용하고, 암호화 키를 공개하여 키의 전송 및 비밀 보관등이 필요하지 않은 시스템이다. 1976년 Stanford 대학의 W. Diffie와 M. E Hellman은 논문 'New directions in cryptography'에서 공개 키 암호시스템이란 개념을 최초로 제시하였고, 구체적인 암호 알고리즘으로서 1978년 발명된 RSA암호가 유명하다.

비밀 키 암호시스템을 공중통신망에서 이용하도록 하면, 통신상대마다 다른 키를 제 3 자가 알지못하도록 사전에 알려줄 필요가 있고, 그림 3(a)에서 나타내듯이 통신상대가 늘어남에 따라 공중망에 의한 암호사용자는 통신 상대 전원의 많은 키를 가져야 한다. 이러한 다수키의 배포와 보관이 비밀 키 암호의 최대문제였으나, 공개 키 암호시스템을 이용하면 이러한 키 관리문제는 해결할 수가 있다.

각 이용자의 비밀 키에 대응하는 공개 키를 전화부와 같은 공개 파일에 보관하면 된다. 공개 키 암호에서는 각 이용자는 그림 3(b)와 같이 자기만의 1종류의 복호화 키를 보관하면 된다. 예를들어 이용자 B와 비밀 통신을 행할 경우 B의 공개키 K_{eB}로 부터 암호문 $C=E(K_{eB}, M)$을 생성하여 B에게 보낸다. B는 자기만이 알고있는 비밀의 복호화키 K_{dB}로 부터 $M=D(K_{dB}, C)$를 계산하여 평문을 복호한다. 임의의 사



K_{AB} : AB간 통신용키
(암호화 키=복호화 키)

(a) 비밀 키 암호시스템

K_{eA} : A의 암호화 키
K_{dA} : A의 복호화 키 ($K_{eA} \neq K_{dA}$)

(b) 공개 키 암호시스템

그림 3. 비밀 키 암호와 공개 키 암호의 키의 배치

표 1. 비밀 키 암호와 공개 키 암호의 비교

항목 \ 암호방식	비밀 키 암호		공개 키 암호
암호키의 관계	암호화 키=복호화 키		암호화 키≠복호화 키
암호화 키	비밀		공개
복호화 키	비밀		비밀
암호 알고리즘	비밀	공개	공개
대표 예	Vernam암호	DES 암호	RSA 암호
비밀키의 분배	필요(×)		불필요(○)
비밀키의 보관수	많음(×) 통신상대수 만큼 필요		적음(○) 자기 키만 가지면 됨
안전한 인증	곤란(×)		용이(○)
암호화 속도	빠름(○)		느림(×)

*○ : 장점 × : 단점

용자가 비밀 통신의 송신자가 될 수 있음에 특징이 있다.

공개 키 암호가 비밀키 암호보다 뛰어난 또하나의 점은, 통신문 발신자의 인증을 확실히 할 수 있음이다. 예를들어 이용자 A가 통신문 M에 서명하고 싶을 경우, A는 자기만이 알고있는 비밀키 K_{dA}를 이용하여 서명문 $S=D(K_{dA}, M)$을 생성하여 S와 자기이름 I_A의 쌍을 보내면 된다. 수신자는 I_A로부터 A의 공개키 K_{eA}를 검색하여 $M=E(K_{eA}, S)$를 계산한다. 복호된 M이 문장으로 의미를 가지면 A가 송신자로서 도중에 수정이 없었다는 것을 인증한다. 임의의 수신자가 인증통신의 확인자가 될 수 있는 점과, 수신자가 A로 위장하려는 것이 불가능하다는 특징을 가지고 있다.

이상을 종합할 때 공개 키 암호시스템은 키의 배송이 용이, 비밀로 보관하는 키의 종류가 적음, 안전한 인증 기능 가능의 특징이 있고, 공중 통신망을 통한 불특정 다수의 상대와 통신을 하는데 있어서 불가결한 기반 기술일 것이다. 비밀 키 암호와 공개 키 암호의 특징을 표 1에서 비교한다.

Ⅲ. 암호화 기술

1. 비밀 키 암호시스템의 알고리즘

1) Vernam 암호

Vernam 암호는 1917년 Vernam이 전신용 암호로서 개발하여 현재까지 오랜 동안 사용되어져 왔고, 키를 충분히 긴 난수로 하면 무조건 안전한 암호를 구성할 수 있는 비밀 키 암호이다. 평문의 각 비트 M_i와 키의 각 비트 K_i의 배타적 윤리합 XOR(eXclusive OR)를 암호문의 각 비트 $C_i=(M_i \oplus K_i)$로 하는 스트림 암호이다. 그림 4는 Vernam 암호의 구성을 나타낸 것이다.

그림 4. Vernam 암호의 구성도

[수치 예]

평문 M이 1011010이고, 키 K가 1000110의 경우,

$C=M+K \bmod 2=0011100$

로써 암호문을 구할 수 있다. ■

2) DES

DES(data encryption standard;데이타 암호화 규격)은 미국 상무성 표준국(NBS;National Bureau of Standard)에서 미국 연방 정부 기관에 있어서 정보처리를 행하는 컴퓨터 데이타 보호를 위하여 1971년 암호의 규격화 검토를 개시하여 1973년 다음의 조건을 제시하여 암호 방식을 공모하였다.

첫째, 애매함이 없이 완전히 규정되어 있을 것.

둘째, 키의 해독에 필요한 시간이나 처리량에 의

한 안전성의 수준을 나타낼 수 있을 것.

셋째, 안전성이 키의 비밀성에만 의존하고, 알고리즘의 비밀성에는 의존 안할 것.

공모 결과 표준국에서는 IBM이 개발 제안한 방식을 채용하여 1977년 데이타 암호화 규격(DES) 으로서 공표하였다. 이러한 DES는 미국 연방 정부 기관의 표준으로 되어 있으나, 민간의 사용을 권장하고 있고 실질적으로는 미국의 표준 방식으로 되어 있다.

DES 알고리즘은 전치식과 환자식을 기본으로 하여, 입력되는 평문을 64비트씩 나누어 64비트의 키를 이용하여 64비트의 암호문을 만들어 낸다. 키에는 8비트의 parity check비트가 포함되어 있기 때문에 실질적인 키의 길이는 56비트로서, 2^{56}(약 10^{17})가지의 키를 사용할 수 있으므로, exhaustive search로써 알고있는 암호문과 평문의 쌍에 대하여 키를 1회씩 변화시켜 검사하는 해독에서는 1회의 검사에 10^{-6}초 걸린다고 하면 전체에 1000년이상의 시간이 필요할 것이다. DES는 16라운드로 구성되며, 동일한 동작과정의 반복으로 이루어진 블럭암호 시스템이다.

DES를 개량하여 고속화를 꾀한 암호로써, 1987년 일본의 NTT가 개발한 FEAL(fast data encipherment algorithm)이 있다.

2. 공개 키 암호시스템의 알고리즘(RSA 암호)

1977년 MIT의 R. L. Rivest, A. Shamir 그리고 L. Adleman이 "A Method for Obtaining Signatures and Public Key Crytosystems"라는 논문을 통하여 새로운 공개 키 암호 알고리즘을 개발하여 그들의 머릿글자를 따서 RSA암호 알고리즘이라 명명하였다. 이 암호 알고리즘은 큰자리수의 소인수분해의 어려움에 안전성의 근거를 두고, 지수승계산에 의해 암호화/복호화를 행하는 암호이다. 암호화 E와 복호화 D는

$C=E(M)\equiv M^e \bmod n$

$M=D(C)\equiv C^d \bmod n$

으로 표시되어진다. 여기서 M은 평문, C는 암호문으로 암호화 키는 e와 n, 대응하는 복호화 키는 d와 n이다. e와 n의 값이 공개되고, d의 값은 비밀로 되어 있다. 모든 $M(0\leq M\leq n-1)$에 대하여,

$D(E(M))=E(D(M))=M$, 즉

$M^{ed}\equiv M \bmod n$

이 성립한다. e, d, n의 키 값은 다음과 같이 생성한다.

(1) 서로 다른 2개의 큰 소수 p와 q를 선택하여, 그 곱을 $n=pq$로 한다.

(2) $(p-1)$과 $(q-1)$의 최소공배수 L을 계산하여, L과 서로소로서 L보다 작은 임의의 정수 e를 구한다.

(3) $ed\equiv 1 \pmod L$를 (Euclid호제법으로) 풀어, d를 구한다.

각 사용자 i는 서로 다른 법의 값 $n_i=p_iq_i$와 키의 값 e_i, d_i를 생성하여 사용함에 주의하자.

[수치 예]

$p=5$, $q=7$이라 하면, $n=pq=35$이고 $L=LCM((5-1), (7-1))=12$가 된다. 12와 서로소인 수로서 $e=7$를 선택하면, $d=e^{-1} \bmod 12=7$이 된다. 평문을 $M=2$이라 하면, 암호문 C는

$C=M^e \bmod n=2^7 \bmod 35=128 \bmod 35\equiv 23$

이되고, C로부터 M을 구하는 복호는 다음과 같다.

$M=C^d \bmod n=23^7 \bmod\equiv 2$ ■

RSA암호 알고리즘에서는 암호화 키의 일부로서 공개되어 있는 n이 소인수 분해되면, p 및 q가 알려져 버려 복호화 키 d가 해독되어 버린다. 그러나 n의 값을 크게하면 n을 p와 q로 소인수 분해하는것은 계산량적으로 실행 불가능 하다는 것이 알려져 있다. 실제 Rivest등에 의하면 현재 알려진 가장 빠른 알고리즘을 이용하더라도 실제 n의 소인수 분해에는 EXP((In(n) In(In(n)))1/2)의 연산이 필요하다고 알려져 있다. 1연산의 처리가 10^{-9}초로 가능하다고 할 때 소인수 분해에 필요한 처리시간은 표 2와 같다. 그렇기 때문에 장래 컴퓨터 기술의 진보를 생각하더라도 n을 200자리 정도로 하면 RSA암호 방식은 충분히 안전하다고 생각할 수 있을 것이다.

표 2. 소인수 분해의 처리시간

n의 자리수(10진)	처리 회수	처리 시간
50	1.4×10^{10}	3.9시간
70	9.0×10^{12}	104일
100	2.3×10^{15}	74년
200	1.2×10^{23}	3.8×10^{9} 년
300	1.5×10^{29}	4.9×10^{15}년
500	1.3×10^{39}	4.2×10^{25}년

3. 키 분배 시스템(public key distribution system)

대량의 데이타를 암호화하는 데는 고속의 비밀 키 암호시스템을 이용하는 것이 현실적이다. 그러나 그 비밀 키는 안전하게 분배 되어져야 한다. 키 데이타만

을 RSA암호등의 공개 키 암호로 인증을 행하면서 보내는 것도 가능하나, 키 분배만의 기능을 가진 공개키 분배시스템도 있다. Diffie-Hellman은 1976년 공개키 분배시스템의 개념 및 구체적 알고리즘을 제안하였다. 그 구성을 그림 5에 나타낸다. A와 B는 각각 랜덤한 비밀정보 X_A, X_B를 가지고, 공개의 소수 p와 원시근 a로부터

$Y_A = a^{X_A} \bmod p \quad Y_B = a^{X_B} \bmod p$

를 계산하여 Y_A, Y_B를 공개한다. A와 B는 각각 자기의 비밀정보와 상대의 공개키로 부터

$K_A = Y_B{}^{X_A} \bmod p = a^{X_A X_B} \bmod p$

$K_B = Y_A{}^{X_B} \bmod p = a^{X_A X_B} \bmod p$

를 계산하여 공통의 키 $K(=K_A=K_B)$를 얻는다. 이 방식의 안전성은 이산대수의 계산, 예를들어 Y_A로부터 X_A를 구하는 계산의 어려움에 근거를 두고 있다. 이산대수 계산을 어렵게 하기 위해서는, P는 10진 200자리수 이상의 소수로 하여야 할 것이다.

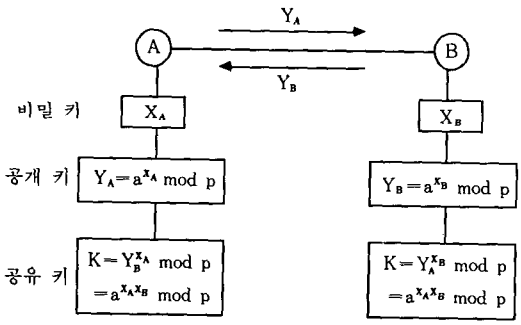


그림 5. Diffie-Hellman의 공개키 분배 시스템의 구성도

4. 인증 (authentication)

인증이란, 사용자 혹은 물건이 정당한가 혹은 진짜인가를 입증하기 위한 처리로서, 암호는 전송메세지, 축적데이타 및 사용자에 대한 인증을 행하기 위한 고도의 안전한 방법을 제공한다. 일반적인 인증의 기능으로 메세지 인증(message authentication), 실체 인증(entity authentication), 디지탈 서명(digital signature)으로 나눌 수 있다. 먼저 메세지 인증이란 정보가 수정되지 않고 본래의 바른 정보임을 보증하는 기능이고, 실체 인증이란 정보 시스템에 있어서 정보의 생성 전송 처리 기억 판단등의 행위에 관여한 실체가 바로 그 실체임을 보증하는 기능이다. 그리고 디지탈 서명이란 이런 메세지 인증 기능과 실체 인증기능을 합한 것으로 생각할 수 있다.

인증 방식의 일반적 개념은 그림 6 과 같다.

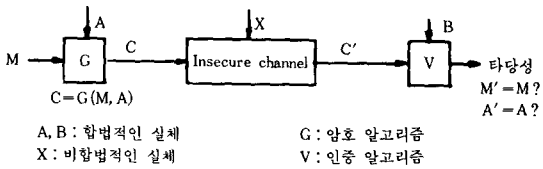


그림 6. 인증 방식의 일반적 개념

먼저 A는 암호 알고리즘 G를 이용하여 메세지 M으로 부터 C를 생성하여 안전성이 보증되어 있지않은 통신로를 통하여 B에게 전송하며, 그때 통신로 출력은 C′가 된다. 통신문 C′를 수신한 B는 인증 알고리즘 V를 이용하여 복원한 메세지 M′와 A가 송신한 메세지 M이 같은가 및 수신측의 실체 B가 생각하고 있는 상대가 확실히 A임을 검사하고 그 타당성을 출력한다.

Ⅳ. 맺음말

컴퓨터와 통신의 결합으로 도래하는 정보화 사회에서는 정보가 매우 중요한 요소를 이루게 된다. 현대사회가 정보화사회로 변환하는 과정에서 정보 security기술의 요구도가 날로 높아지고 있으며, 특히 전자 송금이나 문서 통신등에 있어서 안전성 문제가 이미 우리의 앞에 직면하고 있다. 이러한 안전성 문제와 관련하여 도청이나 정보의 수정을 방지하는 유효한 기술로서 기밀보호와 송신자 인증등의 기능을 가지는 암호의 연구개발이 활발히 진행되고 있다. 본고에서는 암호의 기본적 개념을 간략하게 소개하였으나, 각 부분별 상세한 설명은 다음 기회에 갖기로 한다.

현대 암호학은 전자 계산학, 전자통신 정보 공학, 수학 및 통계학등 여러분야의 학문들과 관련을 갖고 있다. 현대 암호학을 이해하고 암호 시스템을 구성하기 위해서는 위의 분야에 대한 기본적인 이해와 각종 전공자들의 협력이 필수적으로 요구된다.

끝으로 암호에 대한 어두운 선입관을 버리고 밝은 사회를 실현하기 위한 수단으로서의 밝고 건전한 암호가 될 수 있도록 많은 관심을 바라는 바이다.

參 考 文 獻

[1] D.E. Denning, "Cryptography and Data Security," Addison-Wesiey Pub.,1982.
[2] W. Diffier, and M. Hellman, "New directions in cryptography," *'IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.
[3] W. Diffie and M. Hellman, "Privacy and authentication: an introduction to cryptography," *Proc. IEEE*, vol. 67, no. 3, pp. 397-427, March 1979.
[4] FIPS, "Data Encryption Standard," National Burean of Standard, Publication, Jan. 1977.
[5] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Comm. of ACM, pp. 120, Feb. 1978.
[6] C.E. Shannon, "Communication theory of secrecy system," *Bell Sys. Tech. J.*, vol. 28, pp. 656-715, Oct. 1949.

筆 者 紹 介

金 大 豪
1948年 7月 18日生
1977年 2月 한양대학교 전자공학과 졸업
1984年 2月 한양대학교 산업대학원 전자공학과 졸업
1977年～현재 한국전자통신연구소 책임연구원