論 文

스트림 암호에서 개선된 알고리즘을 이용한 암호 키 발생 방법

正會員 崔 鎭 卓* 正會員 宋 榮 宰**

A Method for Key Generators Using Algorithms in Stream Ciphers

Jin Tag CHOI* Young Jae SONG** *Regular Members*

要 約 데이타와 정보의 전송방법이 급속도로 발전하고 있기 때문에 우리는 허용되지 않은 사용자로 하여금 데이타를 보호하는 것이 오늘날 큰문제점으로 등장하고 있다. 본 논문에서는 이러한 데이타의 보호및 전송방법에 있어서 스트림 부호를 이용한 암호화에 사용되는 키의 비트를 연속적으로 발생시키는 알고리즘에 대하여 다루었으며 특히 중요한것은 긴 난수가 아닌 복합적인 결합 방법에 의하여 계속적인 스트림 비트를 발생 시키는 방법에 대하여 연구하였다.

ABSTRACT As the volume of communication data and information exchange, the protection of data which we want to keep secret from invalid users would be a main topic nowadays. This paper describes the use of an arbitrary bit-sequence generating algorithm as the cryptographic key for a stream cipher. Emphasis is placed on methods for combining stream generators into more complex ones, with and without randomization.

I. 서 론

일반적으로 어떠한 정보를 보호하는 방법에는 크게 두가지로 나눌 수 있다. 첫째로 정보자체의 접근을 통제하는 방법으로 액세스제어(Access control)방법이 있는데 이는 사용자의 신원 또는 공유 자원의 특성을 고려해서 사용자의 접근을 통제 하는 방법이다.[1X2] 둘째로 자원 자체의 사용이나 접근은 통제하지 않으나 내용 자체를 암호화 하여 허락된 사용자만이 그내용의 진의를 파악할 수 있도록 하고 타인은 알 수 없도록 하는 방법이다. 이러한 방법으로 내용을 암호화 하여 정보를 보호하는 것을 Cryptography라고 한다.[1] 여기에는 여러가지 방법으로 내용을 암호화 하여 (Encryption) 특정한 권리를 부여받은 자만이 내용을 전달 받을수 (Decryption)있다. 평문을 암호화 하는 방법에는 블럭 암호방법 스트림 암호방법및 이두가지를 혼합한 방법이 있다. 블럭 암호방법은 평문을 일정 간격마다

*仁川大學校 電子計算學科
Dept. of Computer Science, Incheon Univ.
**慶熙大學校 電子計算工學科
Dept. of Electronic Engineering, Kyunghee University.
論文番號 : 89-58(接受1989. 7. 4)

분할하여 블럭으로 나누고 블럭마다 독립적으로 암호화 하는 방법이고 스트림 암호방법은 암호기에 의해 순차적으로 만들어내는 랜덤키를 사용하여 평문을 암호화 하는 방법을 말한다.[11]

암호화 하는 여러가지 방법중 어떠한 방법을 사용 하던지 내용을 암호화 하는데 꼭 필요한 암호 키 발생 방법및 보관 문제가 암호화 시스템에서 중요한 연구과제중의 하나다.

본 논문에서는 이러한 종래의 방법을 알아보고 특별히 복합 알고리즘을 자체를 키로 사용하여 암호화 하는 스트림암호(stream cipher) 방법에 대하여 연구 하였다.

스트림 암호방법에서 일련의 키를 발생하는데 있어서 종래에는 의사난수(pseudo-random number) 발생법에 의한 랜덤비트나 문자를 연속적으로 발생 시켰는데 여기에는 의사난수 자체로는 미약했고 길때는 반복적일 수도 있다. 스트림 암방법에는 긴 랜덤의 비트가 발생 되기를 원한다. 물론 n개의 비트를 이용하여 n개의 랜덤한 수를 발생할 수 있지만 정보가 길때는 반복적으로 나올 수 있고 키 자체가 노출될 수 있는 보관의 문제점이 있다. 이러한 점을 해결하기 위하여 종래의 사용하던 모든 비트 스트림 발생 알고리즘을 이용하여 하나의 복합 알고리즘 자체를 키로 사용하면 해결될 수 있다. 본 논문은 일반 스트림 암호방법의 XOR에 기본을 둔 비트 스트림 알고리즘이다.

일반적으로 기존의 cryptography 방법에서는 알고리즘이 공개 되어있고 키값이 비밀 이지만 본 논문에서는 여러가지 복합 알고리즘 자체를 비밀의 키로 사용하여 어떤 정보를 암호화 하는 것이 다른 점이다. 임의로 연속적인 비트를 발생시키는 알고리즘에서 발생한 비트를 암호화 키로 사용된다. 이 비트 스트림 복합 알고리즘이 키의 역할을 하므로 키 공간을 넓게 사용할 수 있고 알고리즘의 조합으로 키를 발생하므로 반복이 아닌 긴 랜덤한 비트를 발생시킬 수가 있으며 키를 발생하는데 소요되는 연산 시간도 많이 걸리지 않으면서 암호키를 발생시킬 수 있어 암호 해독자가 암호문: 평문의 쌍을 입수 하더라도 변환과정이 규칙적이지 않기 때문에 키값을 알아내기가 어렵게 된다. 이와같은 개념을 도식화하면 그림1과 같이 나타낼 수 있다.

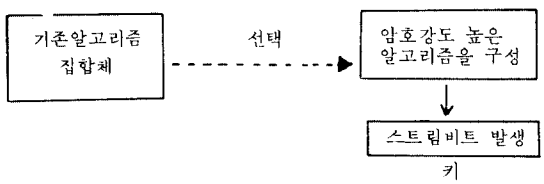


그림 1. 스트림 키 발생과정

Ⅱ. 암호 표기법의 구성

(1) 암호화 과정

암호와(cryptography)하는 과정은 일반적으로 비밀사항의 내용을 작성하고 보관하는데 사용된다. 평문을 암호문으로 변환하는 과정을 특히 encipherment 혹은 encryption이라고 하고 반대로 암호문을 평문으로 변형하는과정을 decipherment 혹은 decryption이라고 한다. 이 두과정 모두가 다음 그림2와 같이 어떤특정한 키값 들에 의하여 결정이 된다.[1,9]

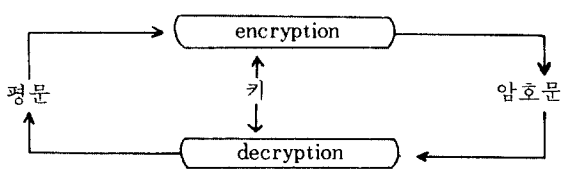


그림 2. 비밀문서

고전적인 정보전달 채널(그림 3)은 메시지의 내용은 일반적으로 개방된 정보채널을 통하여 전송하고 키값은 직접 인편으로 전하거나 개방되지 않은 다른 비밀 정보채널을 통하여 전송 되어야 한다.[8]

Ⅲ. 스트림 암호화

(1) Synchronous 스트림 암호화

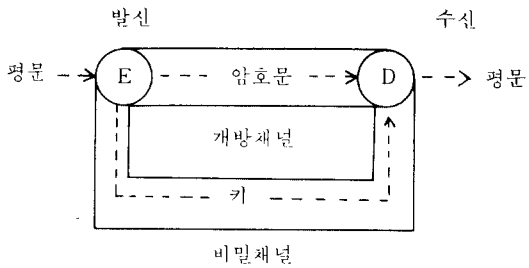


그림 3. 정보 전달채널

synchronous 스트림 암호화는 메시지 스트림에 독립적으로 키를 발생시키는 것의 하나이다. (K=k1, k2, k3,…kn) 키를 발생시키는 키암호 알고리즘과 메시지에 의하여 암호문이 작성된다. 길다란 키를 실제로 기억장소에 저장하여둘 필요는 없다. 약속된 알고리즘에 의하여 암호키를 발생시킨다. 반복되는 스트림 키는 깨어질 수도 있다. 규칙적이지 않는 키로 랜덤하게 연속되는 것은 깨어지기가 어렵다. 스트림 암호화를 그림으로 나타내면 그림4와 같다.[1X10]

(2) 선형귀환 이동레지스터 (LFSR)

n단계의 LFSR은 이동 레지스터 R(r1, r2,… rn) 과 tap sequence T(t1,t2, …tn)로 구성되어 있다. ri, ti는 하나의 2진수 0나 1로 구성되어 있다. 그림5에서와 같이 r1이 키 스트림으로 나타나고 rn,…,r2는 오른쪽으로 한 비트씩 옮겨지고 제일 왼쪽 rn비트는 R과T에 의하여 하나가 삽입된다. R의 다음단계를 R' 라하자.

R'=(rn', r_{n-1}', …,r1')은 다음과 같이 계산된다.

ri'=r_{i+1} (i=1,2,…,n-1)

rn'=TR =$(\sum_{i=1}^{n} tiri) \bmod 2$

=t1r1 ⊕ t2r2 ⊕… ⊕ tnrn

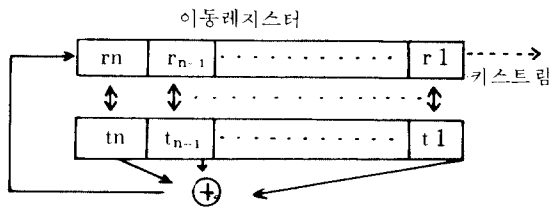


그림 5. LFSR

간단한 예를 그림6의 4단계 LFSR tap sequence T=(1,0,0,1) R=(0,0,0,1)일때 taps의 r1과 r4만 생각하면 된다.

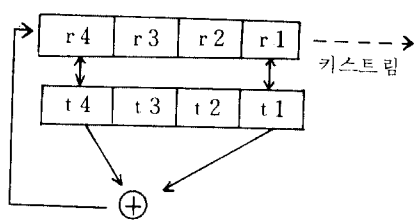


그림 6. 4단계 LFSR

r4'=r1t1 ⊕ r4t4

그림6을 적용하면 키 스트림 K=100011110 101100가 발생된다. 메시지 M의 스트림 m1,

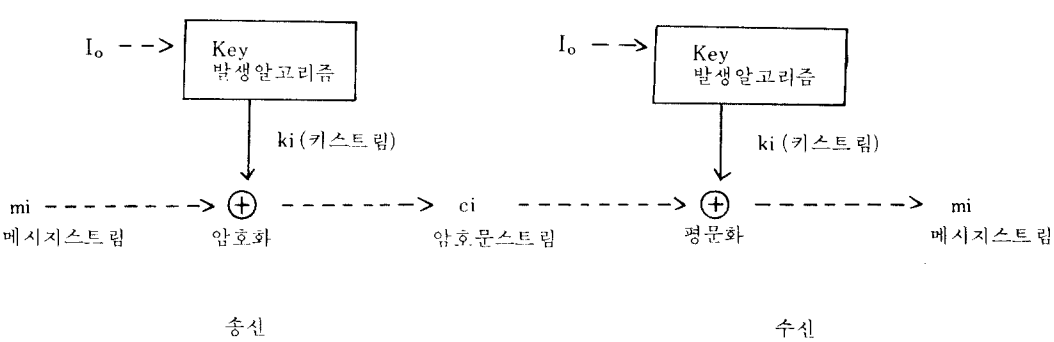


그림 4. Stream 암호화 과정

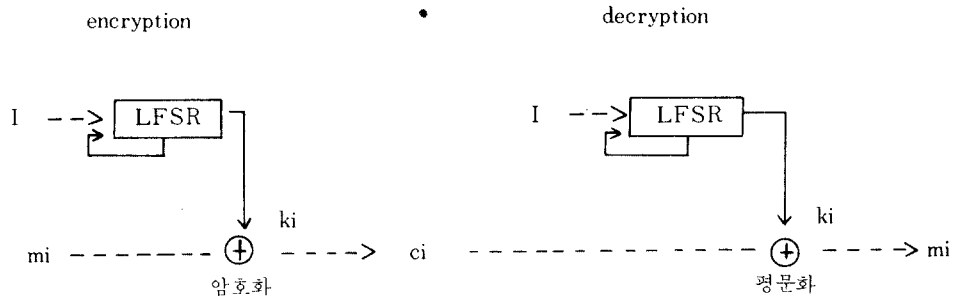


그림 7. 자체 동기화 스트림 암호화

m2, m3,…의 암호화는 ei=mi ⊕ ki 해독방법 역시 그림7과 같은 방법으로 ci ⊕ ki=mi 하면 된다[9X10].

(3) 자동키 암호화

자동키 암호화는 메시지를 이용하여 암호화 하는 것이나 키는 기본키와 메시지 M=m1, m2,… 에 대하여 $ki=m_{i-1}$

ex) 기본키 D이고 메시지가 RENAISSANCE 일때 다음과 같이 암호화 한다[6].

M= R E N A I S S A N C E
K= D U Y L L T L D D Q S
Ek(M)=U Y L L T L D D Q S W

ex) 키는 기본키와 암호문의 각글자가 다음 글자의 키가 된다. 즉 $ki=c_{i-1}$ 메시지 M= RENAISSANCE 이면 기본키 D와 메시지 M에 의하여

다음과 같이 암호문이 작성된다.

M= R E N A I S S A N C E
K= D U Y L L T L D D Q S
Ek(M)=U Y L L T L D D Q S W

물론 이러한 것들은 요즘 표준이되고 강한것은 아니나 특징은 반복 키의 스트림이 아니라는 것이다.

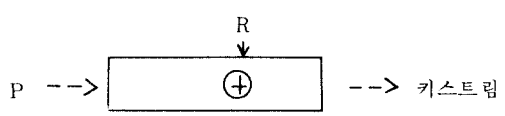
Ⅳ. 복합 알고리즘을 이용한 새로운 암호 키 발생방법의 제안

스트림 암호방식은 외부동기방식과 자기동기방식이 있으며 외부동기방식은 스트림방생기의 내부 상태는 송수신에서 동일하게 되도록 외부에서 동기를 맞추어야하고 자기동기방식은 내부상태(레지스터)의 상태가 도중에 일그러 지더라도 일정시간후에는 자동적으로 동일하게 회복되는 것을 말한다. 스트림 암호방식에서 암호강도를 향상시키기 위해서 복합 알고리즘을 키로 사용하는 개념을 도입한 여러가지 복합적인 방법을 이용하면 아주 복잡한 함수식을 사용한 것보다 더좋은 효과를 얻을 수 있으며 유용한 키를 발생시킬 수 있다. 암호 강도에 맞추어 둘혹은 그이상이 비트스트림을 발생시킬 수 있으며 다음과 같은 여러방법을 사용할 수 있다.

(1) 단순 결합방법에 의한 비트 스트림

a. Exclusive OR.

: 가장 보편적인 방법으로 부호가 같으면 0 서로 다르면 1을 발생시킨다.

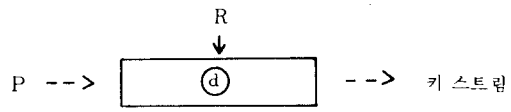


P: 의사난수(pseudo random number)

R: 알고리즘 혹은 메시지

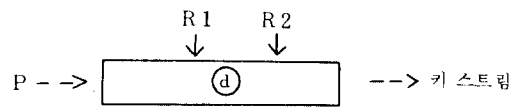
b. 의사난수에 의한 삭제

;의사난수를 이용하여 다른 스트림을 삭제하는데 사용되는 것으로 다음 그림에서 알 수 있듯이



위의 예에서 만약 P='0101010101…' 이면 R에서 나오는 비트를 1이면 삭제하고 0이면 발생시키는 방법으로 결국 하나 건너서 출력한다.

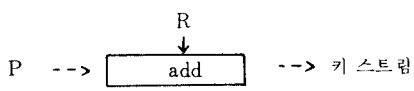
또한 다음 그림과 같다면



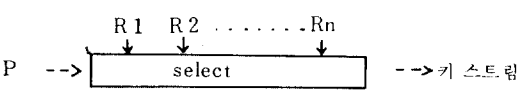
의사난수 P='01010101…'이면 0일때 R1을 출력하고 1이면 R2를 삭제 시키게 된다. 결국 R1만 계속 발생 하게된다.

c. 비트 더하기

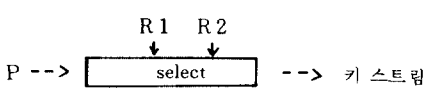
; 두개의 비트를 더하면 0,0면 0이고 0과 1이면 1 그리고 1,1이면 올림수 1을 발생시키는 방법을 말한다.



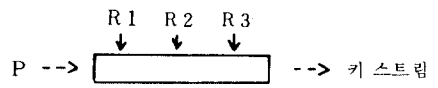
d. 의사난수에 의한 비트 선택



위의 예에서 의사난수 P의 값에 따라서 R1에서 Rn까지 n 스트림으로부터 하나를 선택하여 키를 발생 시키는 방법이다.



만약 위의 예처럼 n=2이고 P='01010101…' 이면 01의 연속이 끝날때까지 계속 R2만 선택이 된다.



위의 예에서도 P='0101010…'이면 연속되는 동안 R2, R1, R3 순으로 계속 선택이 된다.

(2) 복합 알고리즘의 제안

여러가지 결합방법중 한가지를 선택하여 키 스트림 비트를 발생시킬 수 있으나 키공간이 적어서 해독자로 하여금 알고리즘을 알아낼 위험이 있다. 본 논문의 개념인 알고리즘 자체를 키로 실현하기 위해서 한단계 더 보완 하여 복합 알고리즘을 사용한 스트림 비트를 발생시키면 키공간을 넓힐 수 있으며 더욱더 긴 랜덤한 비트의 수를 발생 시킬 수 있다. 기존의 사용가능한 모든 알고리즘을 키공간으로 활용할 수 있으며 어떠한 방법의 알고리즘을 사용해도 좋다. 실예로 블럭 연결 암호문(block chainning cipher)을 포함한 복합 알고리즘으로 그림8과 같이 구현하였다.

P: 의사난수(pseudo random number) 발생

B: 키 스트림

Ri: 알고리즘 혹은 키 스트림

Mi: 메시지

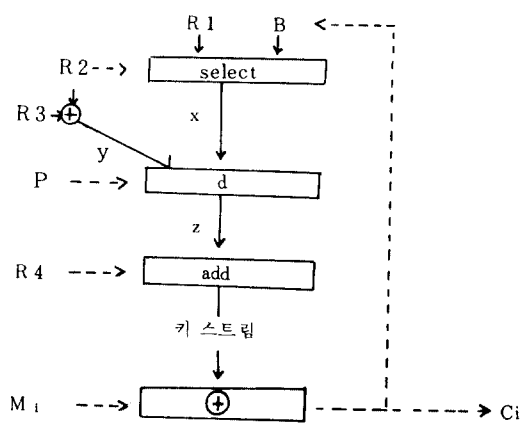


그림 8. 복합 알고리즘의 결합

그림8에서 R1의 알고리즘은 LFSR 방법을 이용하여 그림9와 같이 비트 스트림을 발생한다고 하자.

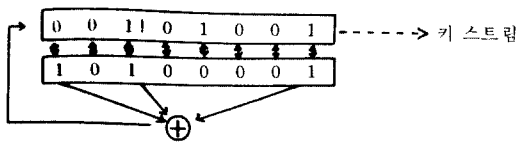
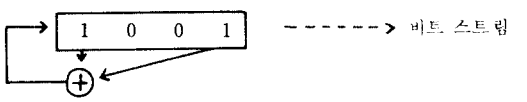


그림 9. R1의 LFSR

그림9에서 발생되는 비트스트림 R1=1001 0100 0001 0100… B는 복합 알고리즘 전체에서 발생되는 비트 스트림 이므로 초기치는 0으로 한다. R4 알고리즘은 seed값을 1001갖는 다음과 같은 방법으로 비트 스트림을 발생한다고 하자.



R4=1001 0001 1110 1011…로 발생된다.
각각 다른 알고리즘에서 발생되는 비트스트림을 다음과 같이 주어질때
R2=0110 1010 1010 0101…
R3=1111 0000 0101 0101…
P =1011 0010 1001 0101…
Mi=1010 0001 1100 1101…

일때 위의 그림에서 알 수 있듯이 R2의 랜덤 한수에 의하여 R1 이나 B나 선택되는데 R2의 값이 0면 R1이, 1이면 B가 선택된다고 하면 x=1이 발생이 된다.

또 R2, R3의 배타적논리합 (Exclusive OR) 값에 의하여 다음 y=1의 값이 발생된다.

의사난수 P에 의하여 방금 발생한 x,y 값중에서 한개는 삭제된다. 여기서 P의 값이 0면 x가 삭제되고 1이면 y가 삭제된다. 다시말하면 P의 값이 0면 y가 선택되고 1이면 x가 선택된다. 이러한 방법으로 Z=1 이 발생된다. 다음 R4와 z를 (add)하여 최종적인 키 스트림의 값 1이 발생하게 된다. 메시지와 다시 XOR 하면 첫번째 암호 C1=0가 발생된다. 다시 반복적으로 B의 값은 C1의 값 0을 가지고 같은 방법으로 반복하면 발생되는 스트림 비트
Ki=1001 1111 1111 1011…Ci =0011 1110 00 11 0110…를 발생한다. 발생된 키 스트림은 특히 반복되지 않는 수이므로 암호문과 평문을 누군가 알더라도 break되기 어려운 강한 암호키의 한 발생법이 된다.

Ⅳ. 결 론

정보화 시대에 각 정보의 보호가 요구됨에 따라서 컴퓨터의 디스크 장치에 보관하고 있는 파일이나 상호간에 정보 전달과정에 있어서 정보의 복사나 도청의 문제등이 있기때문에 정보의 보호는 필연적이라 할 수 있다. 일반적으로 현재 정보의 보호는 액세스 제어리스트(access control list)를 사용하여 사용자의 접근을 제한하는 방법이다. 이는 정보자체를 그대로 보관하고 있다는 문제점이 있다. 이를 교묘하게 dump 나 복사에 의하여 침해될 수 있다.

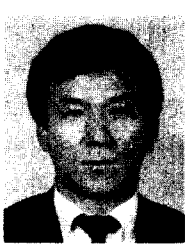
본논문에서는 정보를 얻드라도 사용할 수 없게 정보 자체를 암호화 하여 보관하거나 전달하는 방법인 cryptography에 있어서 특히 복합 알고리즘을 이용하여 스트림 비트를 발생시켜 암호화 하는 방법으로 알고리즘을 키로 사용하므로 서로 키값대신 알고리즘을 같이알고 있으면된다.

이러한 방법은 변환과정에서 키값이 일정하지 않으며 같은 문자라도 변환한 값이 서로 다르므로 키값을 알기가 어렵다. 또한 반복되는 키가 아니므로 예를들어 평문과 암호문을 알아도 알고리즘을 모르면 키를 알아낼 방법이없다. 이리하여 암호 해독자가 암호문의 정보를 입수하더라도 평문으로 변환할 수 없는 secrecy가 보장되며 또한 메시지를 알고 있더라도 키 스트림을 몰라서 평문을 암호문으로 바꾸는 인증(authenticity)도 보장된다. 경우에 따라서는 한 비트가 수만번 다음에 사용되기도 한다. 알고리즘의 결합 방법은 XOR 혹은 addition등 여러가지 알고리즘 방법을 복합하여 사용할 수 있으며 장점으로는 첫째 키의 길이나 값이 고정된 것이 아니므로

키의 공간을 매우 넓게 사용할수 있다. 둘째는 안전의 수준에 따라서 알고리즘에 사용되는 seed의 길이나 키의 복잡성도 조절할 수 있다. 셋째 기존의 암호 방식을 사용한다는 것이다. 넷째 키의 반복 되지 않는 길이의 크기에 비하면 디스크가 차지하는 부분은 얼마되지 않는다. 이러한 장점은 정보의 전달과정때 외부 침입자로부터 해독을 방지할 수 있을뿐만 아니라 특별히 정보의 보호가 요구되는 사항이나 군대에서 비밀취급에 있어 메시지 전달과정에서 긴요하게 쓰일 수 있다고 볼수있다. 그렇지만 앞으로 암호강도의 측정및 전송과정에서 에러검출 복잡도의 적정 수준도 등이 앞으로의 연구과제다.

參 考 文 獻

1. Dorothy E.Denning, Cryptography and Data Security, Adison Wesley Publishing Company, pp. 101-147, 1982.
2. Dorothy E.Denning and Peter J.denning "Data Security" Computing Surveys Vol.11, no.3, pp. 227-245, Sep.1979.
3. Robert Morris and Ken Thompson, "Password security", Commu. ACM, Vol. 22,No.11, pp.594-597, Nov 1979.
4. R.L.Rivest, A.Shamir and L.Adleman, "A method for obtaining digital signatures and public key crypto systems", Commu. ACM, Vol. 21, No.2, pp.120-126, Feb. 1978.
5. Dorothy E.Denning, "Secure personal computing in an insecure network", Commu.ACM, vol.22, No.8, pp.476-482, Aug.1979.
6. Leslie Lamport, "Password authentication with insecure communication", Commu.ACM, Vol.24, No 11, pp.770-772. Nov.1981.
7. Gio Wiederhold, Database Design, McGraw-Hill, 1985.
8. R.W. Hamming, Coding and Information Theory, Prenticehall, Englewod Cliffs, N.J.,1980.
9. A.G.Konheim, Cryptography, John Wiley and Sons, N.Y., 1981.
10. Bernard Smeets, A note on sequence generated by clock controlled shift registers, Lund univ., 1985.
11. 윤석창, RSA 암호방식의 확장에 관한연구, 성균관대학교 대학원, 1988.



최 진 탁 (Jin Tag CHOI) 正會員
1953年 4月 8日生
1977年 2月 : 東國大學校 數學科 卒業
1982年 8月 : 東國大學校 大學院 電子計算學科 卒業
1987年 2月 : 慶熙大學校 大學院 電子工學科 博士課程 修了
1987年～現在 : 仁川大學校 電子計算學科 助教授로 在職中.

宋 榮 宰 (Young Jae SONG) 正會員
1947年 4月20日生
1969年 2月 : 仁荷大學校 電子工學科 卒業
1972年10月 : 日本 Toyo Seiko研究員
1976年 3月 : 日本Keio Univ. 大學院 卒業
1979年 8月 : 明知大學院 卒業(工學博士)
1980年 1月 : 工業振興庁 工業標準 審議委員
1982年 8月 : 美國Univ. of Maryland 객원教授
1985年 : 韓國情報科學會 平委員
1986年 1月 : 大韓電子工學會 電子計算研究會 專門委員長.
1986年 1月～現在 : IEEE Computer Society 한국지회副會長
1987年 6月～現在 : 全國大學電算所長協議會 總務理事, 副會長
1976年～現在 : 慶熙大學校 電子計算工學科 教授
• 關心分野 : 소프트웨어 엔지니어링, 데이타베이스 시스템 Object-oriented Programming & Systems.