論 文

GF(2^n)의 다항식을 이용한 영지식 증명의 인증 기법

正會員 李 元 熙* 正會員 전 문 석* 正會員 李 哲 熙*

An Authenticaton Scheme using Polynomial Equation of GF(2^n) In ZK-Proof Protocol

Won Hee Lee*, Moon Seok Jeon*, Chul Hee Lee* *Regular Members*

要 約

본 논문에서는 정보통신에 있어서 수신자가 송신자 및 송신문을 인증하는 방법으로써 Galois Field에서의 다항식을 이용한 암호화 기법을 적용하여 인증에 걸리는 처리속도를 향상시켰으며, 또한 송신자에대한 인증정보를 대화방식으로 영지식증명 절차를 이용하여 생성하고, 이를 송신문에대한 인증정보에 포함하여 전송하므로써 비밀정보 교환의 안전성을 강화하였다.

ABSTRACT

This paper studies an Authentication sheme which is used polynomial equation over GF(2^n)for reducing time to authenticate sender and his message in secret data communication. Also in order to maintain strong secrecy, this scheme use interactive Zero-knowledge proof protocol for generating information of sender's authentication via unprotected communication channel.

I. 서 론

획기적인 정보통신 기술의 발달로 인한 고도의 정보화 사회에 있어서 점차 컴퓨터 통신망을 이용한 정보교환이 날로 증가되고 있는 추세이다. 교환되는 정보중에는 보호의 필요성이 높은 정보가 있으며, 이러한 정보들을 모두에게 노출되어 있는 통신망을 통하여 교환할수는 없게 되었으며, 따라서 안전하게 이들을 교환할 수 있는 정보보호 방법의 연구가 점차 필요하게 되었다.

통신망을 통하여 전송되는 정보는 어떠한 사람이든지 쉽게 접근이 가능하기 때문에 언제, 어디서, 누구로부터 정보의 위조, 무단절취, 파괴 될 수 있는 위험성을 내포하고 있으며 이러한 위험성을 해결하지 못한다면 개인은 물론 사회전반에 커다란 영향을 미치게 된다. 따라서 컴퓨터 통신망을 통하여 정보를 받은 사람은 정확히 자신이 원하는 송신자부터로 전송된것인가를 증명 할수있어야 하며, 또한 수신한 내용도 위조 되지않은 원래의것인가를 확인할수 있어야한다. 이러한 송신자 및 수신된 내용에 대한 확인을 하는 행위를 인증(Authentication)이라 하며 인증기법의 하나로 이용 되는것으로 암호화(Cryptography)방법을 들수있다.

*崇實大學校 電子計算學科
Dept. of Computer Science Soong Sil Univ.
論文番號 : 93-16(接受1992. 10. 20)

암호화 방법은 인가된 사람만이 허가된 정보를 이해할수 있도록 정보를 변형하는 제반기법으로써 최근에 활발히 연구되고 있다. 현재까지의 암호화 방법은 크게 두가지로 분류하여 볼수있는데 첫째는, 통신 당사자 사이만이 알고있는 비밀키를 가지고 정보를 변형(encrypt)하고, 복원(decrypt)하는 기법의 관용키 암호화 방법이며 둘째는, 모든 통신자에게 제공되는 공개키와 대화 당사자 사이만의 비밀키로써 정보를 변형, 복원하는 기법인 공개키 암호화 방법이다.

관용키 암호화 방법은 송·수신자 둘만이 알고있는 비밀키에 의하여 정보가 보호되는 기법이기 때문에 이러한 비밀키 관리에 문제가 발생하면 안전에 직접 문제가 생기는 단점이 있다. 이러한 단점을 보완하는 기법으로 공개키 암호화 방법에 대한 연구가 활발히 진행되어 왔으며 대표적인 기법으로는 R.S.A 공개키 암호기법을 들수있다.

R.S.A 기법은 비밀키를 송·수신자가 서로 교환하지 않기때문에 안정성은 매우 강하나, 암·복호화 과정에서 비교적 큰수의 지수승 계산을 필요로 하기 때문에 인증에 필요한 정보의 생성에 많은 처리 시간과 기억장소가 필요하기 때문에 실제로 응용하기는 많은 어려움이 따른다는 단점이 있다.

본 논문은 이러한 기존의 기법들의 문제점을 해결하기 위해 다음과 같은 특성을 지니는 전송자및 수신문을 확인하는 인증 기법을 설계하였다.

- $GF(2^N)$ 에서의 다항식 연산에 의하여 인증에 필요한 정보를 생성한다.
- 비밀정보의 교환시마다 생성되는 송신자의 인증정보 내용이 각각 다르다.
- 전송자에 대한 인증정보는 대화방식의 영지식 증명 절차에 의하여 생성한다.
- 인증정보의 생성 및 검증은 BLOCK 단위의 이진 연산을 한다.
- 송신자는 자신의 인증정보를 전송문의 암호정보에 포함하여 전송한다.

위의 특징을 갖는 인증기법은 먼저 인증 정보생성에 있어서 $GF(2^N)$상의 다항식을 이용하여 정보를 변형하는 기법을 사용하므로써 처리속도의 개선을 가져올수 있는것은 물론 대화형 방법의 영지식증명 절차에 의하여 송신자의 인증정보를 생성하고 또한 이 정보를 전송문을 변형한 암호문에 포함하여 전송하므로써 수신자는 자신이 수신한 암호문으로부터 송신자에대한 검증 및 수신문에대한 검증을 모두 하기 때문에 정보보호에 있어서 높은 안전성을 유지할 수 있다.

Ⅱ. 인 증

인증(Authentication)이란 어느사람 혹은 어느것이 진짜인지를 확인하는 행위를 말한다. 즉 정보통신에 있어서는 송·수신자 및 전송되는 내용의 정당성을 확인, 증명하는 행위를 말하며 컴퓨터 시스템이나 통신망에 있어서 각통신주체 및 통신내용을 인증하는 것은 데이타 보호에 있어서 중요한 분야이다. 일반적으로 인증이란 하나 혹은 그 이상의 요소들의 유효성(Validity)을 점검함으로써 이루어 진다.

수신자가 송신자로부터 수신한 메세지의 내용을 검증하는데에는 다음과 같은 사항들을 수신자가 확인할 수 있어야한다.

- 수신 내용이 자신이 원하는 진짜 송신자로 부터의 것인가?
- 수신 내용이 송신자가 보낸 내용 그대로 인가?
- 수신 내용이 전송 순서대로 수신되었는가?
- 수신문이 정말 자신에게 보낸것인가?

첫째로 송신자인증(authentication of sender)이란 송신자가 자신에관한 정보를 수신자에게 제공하고 수신자는 그정보를 점검하여 송신자의 진위 여부를 확인하는것을 말한다.

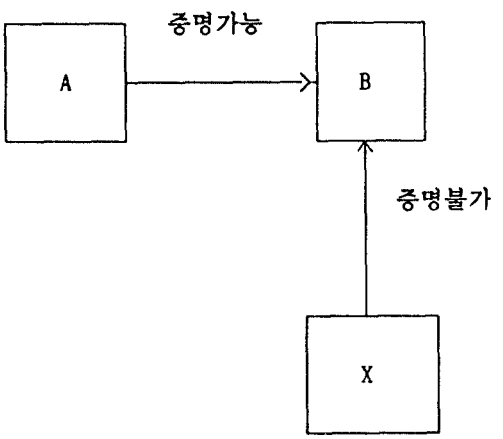

그림 1. 송신자 인증
Fig. 1. Authentication of Sender

즉 그림 1 에서와 같이 송신자 "A"는 수신자 "B"에게 자신이 "A"임을 증명할 수 있으나, "A" 이외의 어떤 제삼자 "X" 도 자신이 "A"라고 "B"에게 증명할 수 없어야 하며, 따라서 수신자는 허위의 송신자로부터 거짓 전송문을 받는 위험으로 부터 보호될 수 있게 된다.

송신자를 인증하는 기법에는 전송문 자체에 자신을 증명하는 인증정보가 포함된 일체형 기법과 전송문과 자신을 증명하는 정보가 별도로 존재하는 분리형 기법이 있다. 일체형 기법은 송신자가 자신에 관한 인증정보를 별도로 생성하지않고 전송문을 암호화하여 전송하고, 수신자는 받은 암호문을 복호화하여 송신자를 검증하는 방법이다. 그림 2 에서 송신자는 전송문(M)을 암호화하는 알고리즘 P로 암호화해서 전송하고 수신자는 받은 암호문을 복호화 알고리즘 P^{-1}을 이용하여 인증하게 된다.

즉 수신자가 P^{-1}을 이용하여 수신한 암호문 C'를 복원한 M'이 의미있는 문장이면 송신자가 확인된 것이며 의미없는 송신자가 적절한 키(Kp)를 모르는 경우로써 적법한 송신자가 아님을 검증하게 된다.

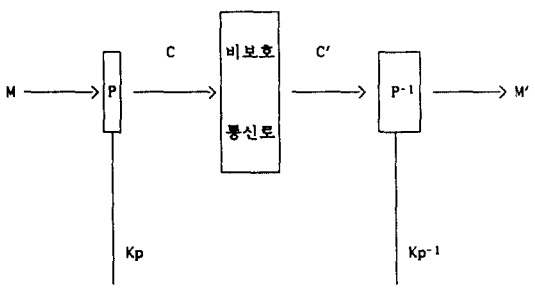

그림 2. 일체형 기법
Fig. 2. Combined Scheme

분리형 기법이란 송신자의 인증정보와 전송문이 별도로 변형되어서 수신자에게 전송되고 수신자는 먼저 수신된 인증정보에 대한 검증을 하여 송신자가 확인이 되면 수신된 전송문이 진짜임을 확인하는 기법이다.

그림 3 에서는 송신자는 전송문(M)을 임의의 hash function(h)에 적용한 결과를 변환알고리즘 P에 의해 암호화하여 인증정보를 생성 S'를 생성하여 송신하며, 또한 전송문 M'은 별도로 변형없이 그대로 송신하는것을 볼수있다.

수신자는 먼저 인증정보 S'를 역변환 알고리즘 P^{-1}

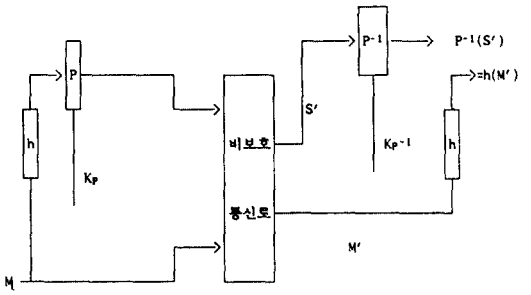

그림 3. 분리형 기법
Fig. 3. Distribute Scheme

을 이용 복원하여 $P^{-1}(s')=h(M')$인가를 검증하여 송신자를 확인한다.

이제까지의 검토된 방법에서 보면 첫째 일체형 방법에서는 변환에 이용된 비밀키 Kp와 Kp^{-1}의 유지관리가 안정성의 유일한 보장이 되기 때문에 취약하며, 두번째 방법인 분류형 방법에서는 전송문 자체는 그대로 평문으로 전송되므로써 전송문 자체에 대한 인증이 결여되는 단점이 있다.

결국 수신자로 하여 전송자에대한 인증 및 수신문에대한 인증이 병행될 수 있는 인증기법이 필요하며 또한 비밀키의 유지만으로 안정을 유지하는 대신, 영지식 증명절차에 의한 인증정보의 송·수신으로 안정성을 높이는 기법이 필요함을 알 수 있다.

Ⅲ. 변환 다항식 f의 구현

송신자가 인증정보 생성시에 적용하는 변환 다항식 f는 이진수로된 전송문을 암호화하는 변환 다항식으로써 한번에 n-bit 씩의 block 단위로 변환시킨다. 즉 전송문을 n-bit로 block화하여 대응되는 암호문인 n-bit block을 생성하게 된다.

따라서 전송문이 n-bit보다 적으면 추가정보를 생성하여 n-bit를 구성하여 연산에 참여하며 만약 n-bit 보다 길면 복수의 block으로 나뉘어 연산하게된다.

1. 다항식 f의 생성

변환다항식 f의 생성은 먼저 임이의 솟수(prime number) P, Q, R을 선정한후 $GF(2^Q)$와 $GF(2^P)$사이에 존재하는 임이의 요소 K개를 선정하여 비밀정보 B_i, C_i를 생성한다.

$$GF(2^Q)<B_i, C_i<GF(2^P)(i=1..K) \quad \text{----------(1)}$$

또한 $GF(2^Q)$과 $GF(2^P)$사이에 존재하는 임이의 요소 T개를 선정하여 비밀정보 D_j를 생성한다.

$$GF(2^R)<D_j<GF(2^Q)(j=1..T) \quad \text{----------(2)}$$

먼저 식(2)의 D를 연산하여 식(1)의 B를 생성하는 함수 S1과 S2를 생성한다.

$$S1(D_j)\equiv B_j(MOD\ 2^N) \quad \text{----------(3)}$$
$$S2(D_j)\equiv B_{j+2}(MOD\ 2^N) \quad \text{----------(4)}$$

또한 식(1)의 C를 연산하여 식(2)의 D를 생성하는 함수 P1, P2를 생성한다.

$$P1(C_j)\equiv D_j(MOD\ 2^R) \quad \text{----------(5)}$$
$$P1(C_j)\equiv D_{j-2}(MOD\ 2^R) \quad \text{----------(6)}$$

여기에서 식(5)의 함수 T1은 j가 1에서 T까지만 $T+1$부터 K까지는 0값을 가지는 함수이고 식(6)의 함수 T2는 j가 1에서 T까지는 0값을 갖고 $T+1$부터 K까지만 적용되는 함수이다. 이제 변환 다항식 f는 앞에서 생성된 함수들의 곱으로 생성된다.

$$f(x)=S_i(T_i(x))(MOD\ 2^N)(i=1,2) \quad \text{----------(7)}$$

2. 다항식 f^{-1}의 생성

수신자 V는 다음의 절차로써 f의 역인 f^{-1}을 생성 인증정보를 복호화하는데 이용한다. 먼저 식(5,6)의 함수 P1, P2의 역함수로써 식(2)의 D를 연산하여 식(1)의 C가 생성되는 함수 U1, U2를 생성한다.

$$U1(D_j)\equiv C_j(MOD\ 2^N) \quad \text{----------(8)}$$
$$U2(D_j)\equiv C_{j+2}(MOD\ 2^N) \quad \text{----------(9)}$$

또한 식(3,4)의 함수 S1, S2의 역함수로써 식(1)의 B를 연산하여 식(2)의 D가 생성되는 함수 V1, V2를 생성한다.

$$V1(B_j)\equiv D_j(MOD\ 2^R) \quad \text{----------(10)}$$
$$V2(B_j)\equiv D_{j-2}(MOD\ 2^R) \quad \text{----------(11)}$$

여기에서 식(10)의 함수는 j가 1에서 T까지만 적용되고 $T+1$부터 K까지는 0의값을 가지는 함수이고 식(11)의 함수 V2는 j가 1에서 T까지의 0값을 가지며 $T+1$부터 K까지만 적용되는 함수이다

이제 f의 역함수인 f^{-1}은 앞에서 생성된 역함수들의 곱으로 생성되어진다.

$$f^{-1}(x)=U_i(V_i(x))(MOD\ 2^N)(i=1,2) \quad \text{---------(12)}$$

3. 다항식 f의 평가

다항식 f의 생성에 사용되는 솟수 P, Q, R은 충분히 큰수이어야 하며, 비밀정보의 갯수인 식(1)의 K와 식(2)의 T는 $K=2T$의 조건이 만족하도록 선택하여야 한다. 결국 K값의 크기에 따라서 비밀유지의 강도에 변화를 가져올수 있다. 가령 3급 비밀정보에는 $K\leq 4$를 택하여 다항식을 생성하며, 2급에는 $4\leq K\leq 8$로 하며, 1급에는 K값을 더 크게 하므로써 정보의 보호강도를 높일수 있다. 특히 생성된 다항식은 공개할 수 있으며 다만 식(1)의 K개의 정보들과 식(2)의 T개의 정보만 송·수신자의 비밀정보로 유지하면 된다.

Ⅳ. 제안 인증 기법

1. 용어 정의

본 논문에서 제안 하는 인증기법은 송신자가 자신을 증명하는 송신자 인증정보를 생성하여 전송문의 인증정보인 암호문에 포함시켜 수신자에 전송하는 기법으로써 2장에서 소개한 일체형 방법과 분리형 방법을 통합한 기법으로 설계하였다.

인증에 사용한 변환 알고리즘은 $GF(2^n)$상에서의 다항식을 이용한 변환을 하므로써 처리속도의 향상을 기하였고 또한 통신 절차로는 영지식 증명절차에 따라 송신하는 방법을 적용하여 보다 높은 안정성을 갖도록 설계하였다. 먼저 인증기법에서 사용되는 용어를 표 1과 같이 정의한다.

표 1. 용어 정의

기호	내용	기호	내용
P	송신자	f	변환 다항식 $\in GF(2^n)$
V	수신자	S	송신자의 비밀 정보(bit vector)
M	전송문	f^{-1}	변환 다항식 f의 역 다항식
C	송신문의 인증정보	T	송신자의 인증정보

2. 인증 정보의 생성절차

송신자가 자신을 증명하는 인증정보를 영지식 증명절차에 의하여 수신자와 대화방법으로 인증에 필요한 정보를 교환하여 다음과같은 순서에의하여 생성한다.

• 단계 1

송신자 p는 임의의 수 $x \in GF(2^n)$를 선정하여 변환다항식 f를 이용하여 y를 계산한다.

$$y = f(x) \in GF(2^n) \tag{13}$$

여기에서 송신자 P는 수신자 V로부터 임의의 수 g를 수신하여 다음과 같은 k를 계산한다.

$$K = g \cdot y \in GF(2^n) \tag{14}$$

송신자 P는 식(14)의 k와 식(13)의 y를 비교하여서 적은수를 y_0, 큰수를 y_1으로 정의한후 식(2)의 k를 수신자 V에게 전송한다. 수신자 V 역시 송신자 P로 부터 받은 k와 자신이 생성한 g를 비교하여 송신자와 같은 방법으로 두 수중에서 작은것을 y0, 큰수를 y1으로 정의하여 검증을위해 저장한다.

• 단계 2

송신자 p는 자신의 비밀정보인 bit vector S를 이용하여 다음과 같은 알고리즘(Generate-T)에 의해 자신을 수신자에게 증명하는 인증정보 T를 계산한다. 이제 자신이 수신자에게 송신하려고하는 전송문을 암호화하는 송신문에대한 인증정보 생성단계(단계 3)를 실행한다.

```
procedure Generate-T(S,T)
 begin
   i=1;
   while i <= k Do
    begin
      if y = y_s(i) then T_i = 0;
      else y = y_1-s(i) T_i = 1;
      i=i+1;
    end
end
```

• 단계 3

송신자 P는 전송문 M을 변환 다항식 f에 의하여 다음과같이 암호화 해서 송신문에 대한 인증정보 C를 block 단위로 생성하여 단계 2에서 생성한 자신의 인증정보 T(bit vector)와 함께 연결하여 전송한다.

$$C = f(m) \odot T \tag{15}$$

($\odot$: concatenation)

결국 송신자는 자신의 인증정보및 메세지에대한 인증정보가 포함된 전송정보 C를 수신자에게 전송하므로써 송신절차를 마친다.

3. 인증정보 검증절차.

수신자 V는 이제 송신자 P로부터 수신한 전송문 C를 가지고 송신자에대한 인증및 수신문에대한 검증을 다음순서에의하여 실행한다.

• 단계 4

수신자 V는 송신자 P로부터 S(bit vector)와 x를 수신하여 다음과같은 y′를 계산한다.

$$y' = f(x) \in GF(2^N) \tag{16}$$

여기에서 y′와 g를 이용하여 K′를 다음과 같이 계산하여 식(14)의 K값과 같은가를 점검한다.

$$K' = y' \cdot g \in GF(2^n) \tag{17}$$

즉 식(17)의 K′와 식(14)에서 송신자 P에의해 생성되어 수신한 K의 값이 같으면 송신자에대한 인증이 확인되고, 따라서 수신문에대한 검증단계(단계2)를 실행하게되며, 만약 같지 않다면 송신자에대한 인증이 거부되므로 수신문자체를 전부 거부한다.

• 단계 5

단계 1에서 인증된 정보 K와 g및 S를 이용하여 인증정보 생성절차에서의 단계2의 Generate-T 알고리즘을 이용 T′를 계산하여 수신한 전송정보 C를 검색하여 T′를 찾는다. 이때 찾을수 있으면 송신자에대한 인증이 되었으므로 전송정보 C에서 T′를 뺀 나머지 정보를 송신문의 인증정보로 간주하여 다음단계를 실행한다. 만약 찾지 못하면 송신자 인증이 거부되고 수신된 전송정보 자체를 거부한다.

• 단계 6

단계 2에서 송신자에대한 인증이 완료되면 다음과 같은 연산으로 송신문 M을 재생할 수 있다.

$$M = f^{-1}((C-T)) \quad (18)$$

식(18)의 결과로 얻어진 M이 의미있는 문장이면 송신문에 대한 인증도 완료되어서 수신된 정보에 대한 전체적인 검증이 완료된다.

V. 결 론

본 논문에서는 비보호 통신로상에서의 보호가 요구되는 데이타나 메세지의 교환을 안전하게 할수있는 인증기법을 제안하였다.

제안 인증기법에서는 송신자가 전송한 암호문을 가지고 수신자는 송신자에 대한 인증과 송신문에 대한 인증을 함께 할 수 있으며, 특히 인증에 필요한 정보를 생성하는 방법으로 GF(2ⁿ)상에서의 다항식을 이용한 암호화 방법을 제안하였으며, 또한 송신자에 대한 인증정보의 생성은 대화방식에 의한 영지식 증명절차에따라 생성하였다.

따라서 제안 인증기법은 기존의 인증기법에서와 같이 송신자에 대한 인증과 전송된 내용에 대한 인증을 별도로 하지않고 동시에 하므로써 비도를 높였으며 특히 암, 복호화 과정에서 GF의 고차 이지만 비교적 적은항의 다항식 연산을 하므로써 암복호화에 소요되는 시간 문제를 해결하였으며, 또한 매번 전송시마다 다른 값의 송신자에 대한 인증 정보의 생성및 검증은 전체 인증 시스템의 높은 안정성을 유지할 수 있다. 동시에 영지식 증명 절차에 의한 송신자에 대한 인증정보를 생성하여 전송되는 암호문에 포함시킴으로써, 기존의 암호화 기법의 안정성을 오직 비밀키 관리유지에만 의존하던 점을 보완하므로써 보다 높은 안정성을 유지하게되었다.

향후 연구과제로는 변환다항식에서의 연산을 병행처리 기법을 적용하여 보다 빠른 처리 속도를 유지하는 점과 제안된 인증기법을 전자결제 시스템이나 전자우편 시스템등에 응용하는 연구가 계속되어야 할 것이다.

참 고 문 헌

1. CARL H. MEYER., and STEPHEN M. MATYAS, "CRYPTOGRAPHY : A NEW DIMENSION IN COMPUTER DATA SECURITY," JOHN WILEY & SONS, 1982.
2. Amos Fiat and Adi Shamir, "How to prove yourself : Pratical Solutions to Identification and Signature Problems," Crypto 86 Proceedings.
3. H. Groscot, "Estimation of some encryption Functions implemented into smart card," Eurocrypt 84 Proceedings.
4. Adi Shamir, "Identity-Based Cryptosystems and Signature Scheme," Crypto 84 proceedings.
5. Denning, "CRYPTOGRAPHY AND DATA SECURITY"
6. C.P.Pfleger, "Security in Computing," Prentice Hall, 1989.
7. John D.lipson, "Element of algebra and algebrac computing," prentice hahall, 1989.
8. Gustavus J.Simmons and George B.Purdy, "Zero-Knowledge Proofs of Identity and Veracity of transaction receipts," Crypto 87, proceedings.
9. G.Agnew., R.Mullin., S.Vanstone, "An Interactive data exchange protocol based on discrete exponentiation," Crypto 84, proceedings.
10. John J.cade, "A modification of a broken public-key cipher," Crypto 86 proceedings.
11. Kenji Koyama and Kazuo Ohta, "Security of improved identity-based conference key distribution systems," Crypto 87 proceedings.
12. 한국 전자 통신 연구소, "현대 암호학"

李 元 熙(Won-Hee Lee) 正會員
1954년 1월 28일생
1979년 2월 : 동국대학교 전자계산과 졸업
1983년 6월 : DREXEL UNIVERSITY 전자계산과 졸업(석사)
1989년 9월 ~ 현재 : 숭실대학교 전자계산과 박사과정
1987년 3월 ~ 현재 : 동국대학교 전자계산원 근무(전임교수)

李 哲 熙(Chul Hee Lee) 正會員
1958年 6月 : 陸軍士官學校(理學士)
1962年 8月 : 美 Purdue 大學校 大學院 電氣工學科(工學碩士)
1988年 2月 : 中央大學校 大學院 電子計算學科 (理學博士)
1962年 9月 ~ 1973年 2月 : 陸軍士官學校 電子工學科 敎授
1973年 3月 以後 現在 : 崇實大學校 電子計算學科 敎授
1988年 11月 ~ 1990年 12月 : 韓國情報科學會 會長
1988年 3月 以後 現在 : 崇實大學校 情報科學大學院 院長
※關心分野 : 데이타 通信, 分散 시스템, 프로토콜 工學 等

전 문 석(Moon Seok Jeon) 정회원
1980년 2월 : 숭실대학교 전자계산과 졸업
1986년 12월 : 메릴렌드 대학교 전자계산학과 석사
1988년 12월 : 메릴렌드 대학교 전자계산학과 박사
1989년 8월 : 몰간 주립대학교 조교수
1991년 2월 : 뉴멕시코 주립대학교 부설 Physical Science Lab 책임연구원
1991년 3월 ~ 현재 : 숭실대학교 전자계산학과 조교수
※관심분야 : 병렬처리 알고리즘, 병렬처리 컴퓨터구조, 신경회로