論文 98-23-3-26

동기식 스트림암호에 필요한 연속 "0" 억제 알고리듬

正會員 이 훈 재*, 박 봉 주**, 장 병 화**, 문 상 재***

A Zero Suppression Algorithm for Synchronous Stream Cipher

Hoon-Jae Lee*, Bong-Joo Park**, Byung-Hwa Jang**, Sang-Jae Moon*** *Regular Members*

요 약

동기식 디지털 통신에 있어서 수신클럭복구는 중요한 문제 중의 하나이며, 수신 데이터가 매우 긴 비트 간격 동안 연속해서 "0" 또는 "1"을 가질 때 클럭복구가 어려워진다. 본 논문에서는 동기식 스트림암호를 적용함에 있어서 송신암호문에 나타난 연속 "0" 비트수를 k 미만이 되도록하는 연속 "0" 억제 알고리듬을 제안하고, 또한 제안된 알고리듬 적용시 수신된 암호문이 수신단에서 정확히 복호됨을 증명하였다. 평문통신시에는 이진 부호 데이타에 k 비트 연속 "0"이 나타나지 않도록 설계된 통신망에 동기식 스트림 암호를 적용할 경우 송신암호문에 k 비트 연속 "0"이 나타날 확률은 2^{-k}로 크게 늘었으며, 이를 보완한 본 알고리듬 적용시에는 다시 확률이 0으로 떨어졌다. 따라서 제안된 알고리듬은 암호학적 비도수준을 유지하면서 난수동기 문제를 효과적으로 해결할 수 있으며, 연속 "0" 비트의 제약을 갖는 T1 반송시스템($k=16$) 등에 적용이 가능하다.

ABSTRACT

In synchronous digital communications it is important to recover the receiver clock, but this is difficult when received data contains a long sequence of consecutive 0's. We suggest a Zero Suppression (ZS) algorithm, which suppresses sequences of more than k 0's between succesive 1's in a ciphertext at the sender of a synchronous stream cipher system, and recovers original message exactly at the receiver. The probability of k consecutive 0's in ciphertext at the sender is 2^{-k} in a synchronous stream cipher without ZS, but 0 with the suggested algorithm. The ZS algorithm does not affect cryptographic security when compared with a synchronous stream cipher without ZS. It is useful for systems which limit consecutive 0's, such as a T1 carrier system($k=16$).

I. 서 론

디지탈 통신에서 그 성능은 수신측에서 클럭신호를 얼마나 정확하게 복구할 수 있는가에 달려 있으며, 일반적으로 수신 데이터의 "0"-"1" 또는 "1"-"0" 천이로 부터 PLL(Phase Locked Loop)을 이용하여 클럭신호가 복원된다. 그러나 송신 데이타 속에 장시간

*한국산업대학교 컴퓨터공학과
**국방과학연구소 연구원
***경북대학교 전기전자공학부
論文番號:96362-1118
接受日字:1996年 11月 18日

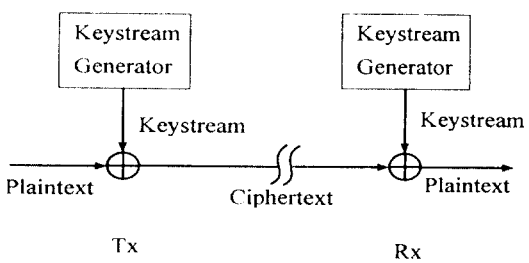
천이가 없을 경우 즉, "0" 또는 "1"이 연속할 경우 수신측에서 클럭복구가 불가능해지는 문제점이 있다. 예를 들면, 이 문제를 해결하기 위하여 T1 반송시스템(1.544 Mbps 전송속도, 24채널 PCM/TDM, AMI부호 및 SF방식)[1]에서는 μ-법칙 음성 부호화시 0-레벨(00000000b)을 배제함으로서 24 채널 TDM 다중화 후에는 16 비트 이상 연속 "0"이 억제되는 특별한 제약이 가해진다. 또한 유선전송 중계시 AMI 방식의 선로 부호화를 이용한 연속 "1" 대비책을 수립함으로서 완벽한 클럭 재생이 강구되어 있다고 볼 수 있다.

일반적으로 동기식 스트림암호 방식으로 디지탈 데이타 신호를 암호화하려면 디지탈 평문 데이타에 PN(randomness) 특성[2]을 갖는 2진 난수열(keystream)을 XOR시키게 되는데, 이 때 출력되는 암호문 데이타는 "1"과 "0"이 균일 분포되는 특성을 갖는다. 이러한 암호화방식을 T1 반송시스템에 적용하게 되면, 수신 데이타중 연속 "0"이 나타날 때 클럭 재생이 불안정하게 되는 문제가 발생된다. 이 문제를 해결하기 위해서는 암호화 후에도 16개 이상의 "0" 연속이 억제되는 암호 방식이 필요하다.(PCM 중계기는 15개까지의 "0"연속에 견디도록 설계되어 있음)

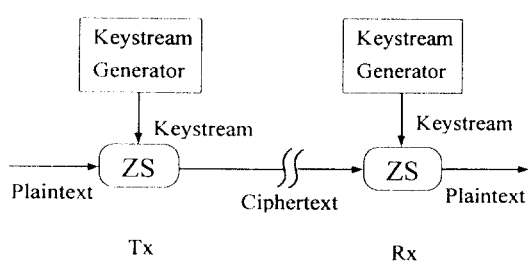
본 연구에는 이와 같은 수신클럭복구상의 문제점을 해결할 수 있는 연속 "0" 억제 알고리듬(Zero Suppression, 이하 "ZS" 알고리듬)을 제안한다. 평문통신시에는 이진 부호 데이타에 k 비트 연속 "0"이 나타나지 않도록 설계된 통신망에 동기식 스트림 암호를 적용할 경우 송신암호문에 k 비트 연속 "0"이 나타날 확률은 2^{-k}로 크게 늘었으며, 이를 보완한 본 알고리듬 적용시에는 다시 확률이 0으로 떨어진다. 즉, ZS가 없는 일반적인 동기식 스트림 암호의 경우 암호문 출력에 k-비트 연속 "0"이 2^{-k}확률로 나타나게 되지만, ZS 알고리듬을 적용함으로서 k-비트 이상 연속 "0"이 완전히 억제되어 확률이 0이 됨으로서 평문통신에서 약정된 규격을 암호통신에서도 유효하게 한다. 예를 들어, 동기식 스트림암호로 T1 회선을 암호화함에 있어서 ZS 또는 다른 대안이 없을 경우 수신 클럭이 불안정하여 난수동기가 이탈하게 되고 그로 인하여 동기를 재확립(resynchronization)하여야 하는 데, 이는 Daemen등[3]이 지적한 바와 같이 암호학적 비도저하의 한 원인이 될 수 있다. 이와 같이 본 알고리듬을 적용할 경우 잦은 재동기로 인한 비도저하를 막을 수 있을 뿐 아니라, 난수열 발생기의 비도수준을 유지하면서 난수동기를 효과적으로 보존하는 장점 때문에 T1 반송시스템등 여러형태의 통신망에 적용이 가능하다.

Ⅱ. Zero Suppression 알고리듬

그림 1 a)는 출력단에 연속 "0" 비트가 상한선 없이 확률적으로 나타날 수 있는 기본적인 동기식 스트림 암호를 나타내었고, b)는 제안된 ZS 알고리듬(그림 2)과 동기식 스트림 암호와의 삽입 위치를 나타내었다.



a) Synchronous stream cipher



b) Synchronous stream cipher with ZS

그림 1. 연속 "0" 억제 알고리듬 삽입위치
Fig. 1 Insertion of zero suppression algorithm.

ZS 알고리듬은 연속 "0" 억제 최소 비트수(k)와 연관 있는 블록크기(n) 만큼의 연속 "0"이 나타나는지 검출하는 검출부와 검출이 일어난 후 정해진 블록크기만큼 다른값으로 대체시키는 대체부로 나눌 수 있으며, 본 알고리듬은 블록단위로 검출하고, 블록단위로 대체시키는 방식이다.

T1 반송시스템에서는 8-비트 채널데이타는 0-레벨(8-비트 모두 "0")이 허용되지 않는다는 사실에 기초하여 ZS 알고리듬을 제안하였다. 편의상 i번째 n 비트 평문벡터 $\mathbf{P}_i$, i번째 n 비트 난수열 블록 $\mathbf{K}_i$, i번째 n 비트 암호문 블록 $\mathbf{C}_i$, i번째 n 비트 복호평문블록 $\mathbf{Q}_i$라 하고 다음과 같이 정의한다. 그리고 n 비트 0 벡터 $\mathbf{0}$, 블록크기 $n=\lceil(k+1)/2\rceil$이고, $\lceil x\rceil$는 x를 넘지 않는 최대정수이다.

$$\mathbf{P}_i:(p_{in}, p_{in+1}, \cdots, p_{in+n-1}) \quad (1)$$
$$\mathbf{K}_i:(k_{in}, k_{in+1}, \cdots, k_{in+n-1}) \quad (2)$$
$$\mathbf{C}_i:(c_{in}, c_{in+1}, \cdots, c_{in+n-1}) \quad (3)$$
$$\mathbf{Q}_i:(q_{in}, q_{in+1}, \cdots, q_{in+n-1}) \quad (4)$$

ZS 알고리듬을 위해서 다음과 같은 가정을 설정한다.

(1) 송신단 암호 시스템에서 잉여비트를 삽입 또는 삭제할 수 없다.

(2) 모든 $i(i\geq 0)$에 대하여 $\mathbf{P}_i\neq\mathbf{0}$이다.

(3) 난수열 발생기는 높은 비도를 갖는다.

상기의 가정하에 송신단에서의 ZS 알고리듬 동작은 다음과 같다.

(1) $\mathbf{P}_i\oplus\mathbf{K}_i$ 연산된 암호문블록과 $\mathbf{K}_i$를 각각 n단 이동레지스터에 입력시킨다.

(2) $\mathbf{P}_i\oplus\mathbf{K}_i$ 연산된 암호문블록이 $\mathbf{0}$인지 검사한다.

(3) $\mathbf{P}_i\oplus\mathbf{K}_i=\mathbf{0}$일 경우에는 $\mathbf{C}_i=\mathbf{K}_i$를 출력시킨다. 이 외의 경우에는 $\mathbf{C}_i=\mathbf{P}_i\oplus\mathbf{K}_i$를 출력시킨다.

또한 수신단에서의 동작은 다음과 같다.

(1) $\mathbf{C}_i\oplus\mathbf{K}_i$ 연산된 복호문블록과 $\mathbf{K}_i$를 각각 n단 이동레지스터에 입력시킨다.

(2) $\mathbf{P}_i\oplus\mathbf{K}_i$ 연산된 복호문블록이 $\mathbf{0}$인지 검사한다.

(3) $\mathbf{C}_i\oplus\mathbf{K}_i=\mathbf{0}$일 경우에는 $\mathbf{Q}_i=\mathbf{K}_i$를 출력시킨다. 이 외의 경우에는 $\mathbf{Q}_i=\mathbf{C}_i\oplus\mathbf{K}_i$를 출력시킨다.

[정리 1] 임의의 평문블록 $\mathbf{P}_i\neq\mathbf{0}$ 하에서 ZS 알고리듬을 동기식 스트림 암호에 적용할 경우 송신단 암호문 출력에 $2n-1(=k$ or $k-1)$ 비트 연속 "0"이 억제되며, 채널오류가 없을 경우 수신단에서 평문이 완벽하게 복호된다.

(증명) (i) 임의의 $\mathbf{P}_i\neq\mathbf{0}$이기 때문에, 송신단에서 ZS 출력은 $(2n-1)$ 비트 연속 "0"이 허용되지 않는다.

(ii) $\mathbf{P}_i\oplus\mathbf{K}_i=\mathbf{0}$이 검출될 경우, $\mathbf{C}_i=\mathbf{K}_i$이 수신단으로 전송되고, $\mathbf{P}_i=\mathbf{K}_i$이 된다. 이 때 수신단에서는 $\mathbf{C}_i\oplus\mathbf{K}_i=\mathbf{K}_i\oplus\mathbf{K}_i=\mathbf{0}$을 검출함으로서 $\mathbf{Q}_i=\mathbf{K}_i=\mathbf{P}_i$을 출력하게 되고, 결국 평문 블록이 완전히 복호된다.

(iii) $\mathbf{P}_i\oplus\mathbf{K}_i\neq\mathbf{0}$이 검출될 경우, $\mathbf{C}_i=\mathbf{P}_i\oplus\mathbf{K}_i$이 수신단으로 전송된다. 이 때 수신단에서는 $\mathbf{C}_i\oplus\mathbf{K}_i=(\mathbf{P}_i\oplus\mathbf{K}_i)\oplus\mathbf{K}_i=\mathbf{P}_i\neq\mathbf{0}$로 복호하고 $\mathbf{Q}_i=\mathbf{C}_i\oplus\mathbf{K}_i=\mathbf{P}_i$를 출력함으로서 결국 평문블록이 정상 복호된다.

대체방법에 대하여 $\mathbf{P}_i\oplus\mathbf{K}_i=\mathbf{0}$이 검출시 출력에 임의의 벡터 $\mathbf{C}_i=\mathbf{R}(\neq\mathbf{K}_i)$를 대체시킬 수 있다고 가정할 수 있겠지만, 이 경우 수신단에서는 $\mathbf{R}$을 검출해서 역대체해야 하는데, 이 과정에서 수신단에서는 암호문벡터 $\mathbf{R}(=\mathbf{P}_i\oplus\mathbf{K}_i)$인지 대체된 값 $\mathbf{C}_i=\mathbf{R}$인지 구별이 불가능하기 때문에 임의벡터의 대체시에는 완전한 알고리듬이 될 수 없으며, 오직 난수열 블록의 대체방법만이 알고리듬을 완전하게 구성한다.

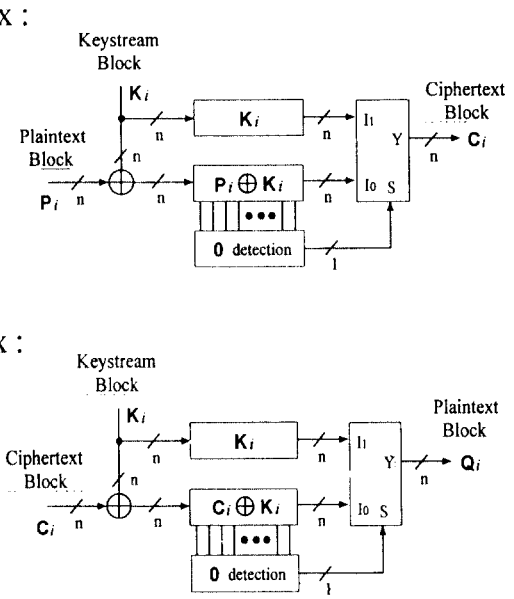


그림 2. ZS 알고리듬

Fig. 2 Zero suppression algorithm.

Ⅲ. 알고리듬 분석

1. 난수동기오류 개선

평문통신에서와는 달리 연속 "0" 비트수가 제한적인 통신망에 동기식 스트림암호방식을 적용하여 암호통신을 할 경우 그림 3에서와 같이 전송데이터 수가 늘어날수록 평균 난수동기오류 횟수는 많아지며, 또한 k값이 작을 수록 이 값은 기하 급수적으로 늘어나 원활한 암호통신을 수행할 수 없고, 난수동기오류가 일어날 때마다 재동기를 시도하여야하므로 통신성능이 크게 저하된다. 그러나 동기식 스트림암호방식을 개선하여 제안된 ZS알고리듬을 적용할 경우 연속 "0"으로 인한 난수동기오류 문제는 완전히 해결될 수 있으며, 암호통신에서의 통신성능이 크게 개선됨을 알 수 있다.

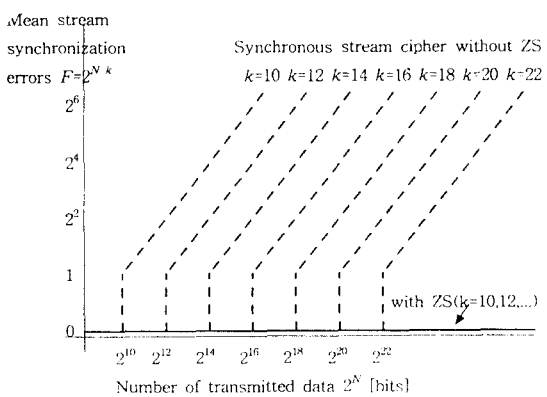


그림 3. 난수 동기 오류 예 (k = 10, 12, ..., 22)
Fig. 3 Examples of keystream synchronization error.

2. 비도측면 분석

송신암호문의 난수특성이 뛰어나다는 가정하에서 ZS 알고리듬을 갖는 스트림암호에 대하여 암호문을 이용한 공격(ciphertext-only attack)을 취할 경우 도청자(eavesdropper)는 암호문으로부터 송신단에서 대체시킨 난수열 블록과 그렇지 않은 블록을 구별할 방법이 없다. 왜냐하면 스트림 암호의 원리상 n 비트 난수열 블록이 연속 "0"(000...000b)이면 평문블록이 암호문에 그대로 나타남에도 불구하고 도청자는 암호문 속에 섞여있는 평문을 구별해낼 수 없는 것과 마찬가지로, 난수특성이 뛰어날 경우 ZS에서 대체된 난수블록도 역시 구별해 낼 수 없기 때문이다. 한편, ZS 알고리듬에 대하여 기지 평문 공격(known-plaintext attack)과 선택적 평문 공격(chosen-plaintext attack)을 할 경우에도 암호학적 안전성의 주된 요소는 난수열 발생기(keystream generator)의 강도에 달려있기 때문에 ZS의 적용으로 인한 비도저하요인은 없음을 알 수 있다. 결과적으로 ZS 알고리듬의 적용으로 일반 동기식 스트림암호의 경우에 비하여 암호학적인 비도수준의 저하는 없으며, 난수열 발생기의 비도가 안전성에 가장 중요한 역할을 담당하기 때문에 ZS 적용시에도 안전성이 뛰어난 난수열발생기의 설계가 요구된다.

3. 오류 특성

ZS 알고리듬은 채널오류가 없는 이상적인 채널에서는 문제가 없지만, 그렇지 않은 채널에서는 블록대체로인한 비트오류확산(bit error propagation)이 발생되며, 블록크기(n)와 채널오류율(B)에 따른 전체비트 오류율이 어느정도로 나타나는지 알아볼 필요가 있다. ZS 알고리듬 적용시 송신단에서 균일분포를 갖는 암호문 입력으로부터 송신블록대체가 일어날 확률은 2^{-n}이며, 그 반대 확률은 $1-2^{-n}$이다. 마찬가지로 수신단에서 균일분포를 갖는 복호문 입력으로부터 수신블록대체가 일어날 확률은 2^{-n}이며, 그 반대 확률은 $1-2^{-n}$이다. 이 때 임의의 n에 대하여 P_M은 송신대체시에 수신단에서 미검출되는 미검출확률(miss-detection probability), P_F는 송신 비대체시에도 채널오류로 인하여 수신단에서 대체블록으로 검출되는 오검출확률(false-detection probability), 채널의 비트오류율(BER, bit error rate)을 B라 둘때 ZS적용시 전체 비트오류율 P_E는 다음과 같이 계산된다.

P_M = (송신단에서 블록대체될 확률)×(수신단에서 대체블록을 미검출할 확률)×(미검출에 따른 블록내 평균 오류확산비트 수)

$$= (2^{-n})[1-(1-B)^n](n/2) = (n)\,2^{-(n+1)}[1-(1-B)^n] \quad (5)$$

P_F = (비대체블록에 채널오류가 발생될 확률)×(수신단에서 대체블록으로 판단할 오검출확률)×(오검출로 인한 블록내 평균 오류확산비트 수)

$$= [1-(1-B)^n](2^{-n})(n/2) = (n)\,2^{-(n+1)}[1-(1-B)^n] \quad (6)$$

$$P_E = P_M + P_F + B = 2P_M + B = (n)\,2^{-n}[1-(1-B)^n] + B \quad (7)$$

$k=16$, $n=8$인 T1 반송시스템($P_i \neq 0$에 링크 암호화(link encryption)로 암호시스템을 설계할 경우 전체 비트오류율은 표 1의 왼쪽 결과와 같아지며 $n=8$일 때 전체 비트오류율은 BER에 비하여 평균 1.25배 정도 증가하였음을 알 수 있다. 그러나 이러한 증가는 표 1의 오른쪽 결과에서 알 수 있는 바와 같이 n이 커질 경우 전체 비트오류율은 1에 근사하게 되므로 ZS 적용에 따른 오류확산은 무시된다.

표 1. ZS 알고리듬의 전체 비트오류율(BER 또는 n에 따른)
Table 1. Total Bit Error Rate of ZS Algorithm(by BER or n).

BER	total error rate of ZS($k=16$, $n=8$)	n	total error rate of ZS(BER = 10^{-5})
10^{-1}	1.1779790×10^{-1}	6	1.5632498×10^{-5}
10^{-2}	1.2414228×10^{-2}	7	1.3833208×10^{-5}
10^{-3}	1.2491268×10^{-3}	8	1.2499912×10^{-5}
10^{-4}	1.2499125×10^{-4}	9	1.1584116×10^{-5}
10^{-5}	1.2499912×10^{-5}	10	1.0977844×10^{-5}
10^{-6}	1.2499991×10^{-6}	11	1.0591593×10^{-5}
10^{-7}	1.2499999×10^{-7}	15	1.0068753×10^{-5}
10^{-8}	1.2500000×10^{-8}	20	1.0003819×10^{-5}
10^{-9}	1.2500000×10^{-9}	25	1.0000186×10^{-5}
10^{-10}	1.2500000×10^{-10}	31	1.0000004×10^{-5}

Ⅳ. 결 론

제안된 ZS 알고리듬은 k 비트 이상의 연속 "0"이 암호문 출력에 나타날 때 이를 난수블록을 이용하여 대체시킴으로서 평문통신에서 정의된 연속 "0" 제약성을 암호시스템 적용시에도 그대로 유효하게 만들어주는 알고리듬으로서, 수신단에서 평문이 완전하게 복호될 수 있음을 증명을 통해 확인하였다. 본 알고리듬은 동기식 스트림 암호시스템 적용시에 암호문에서 나타나는 연속 "0" 비트수가 허용된 비트 수를 초과할 경우 나타나는 수신클럭복구의 어려움, 암호시스템의 난수동기이탈과 재확립으로 데이터 손실 및 비도 저하 요인등 여러 가지 문제점들을 해소시켜주는 해결책이 된다. 본 ZS 알고리듬을 T1 반송시스템에 적용시($k=16$, $n=8$), 상기 문제점들이 해소됨을 확인할 수 있었다. 그리고 일반 동기식 스트림암호에 비하여 ZS 알고리듬의 적용으로 인한 암호학적인 비도수준의 저하는 없음을 알 수 있었으며, 난수열 발생기의 비도가 안전성에 가장 중요한 역할을 담당하기 때문에 ZS 적용시에도 안전성이 뛰어난 난수열발생기의 설계가 요구된다.

참 고 문 헌

1. CCITT Recommendation: 'Physical/Electrical Characteristics of Hierarchical Digital Interface', *CCITT red book*, Vol. III, Rec. G. 703, 1985.
2. H. J. Beker and F. C. Piper, *Cipher systems: The Protection of Communications*, Northwood Books, London, 1982.
3. J. Daemen, R. Govaerts and J. Vandewalle, "Resynchronization Weaknesses in Synchronous Stream Ciphers", *Advances in Cryptology-Eurocrypto'93, LNCS 765*, Springer-Verlag, pp. 159-167, 1994.

이 훈 재(Hoon-Jae Lee) 정회원

1985년 2월: 경북대학교 공과대학 전자공학과(전자공학, 공학사)
1987년 2월: 경북대학교 대학원 전자공학과(통신공학, 공학석사)
1987년 2월~1998년 1월: 국방과학연구소 선임연구원
1993년 3월~1998년 2월: 경북대학교 대학원(정보통신, 공학박사)
1998년 2월~현재: 한국산업대학교 컴퓨터공학과(전임강사)
※주관심분야: 정보보호 기술, 디지털 통신, 정보통신망

박 봉 주(Bong-Joo Park) 정회원

1986년 2월: 서강대학교 수학과 졸업(이학사)
1988년 2월: 서강대학교 대학원 수학과 졸업(이학석사)
1988년 2월~현재: 국방과학연구소 선임연구원
※주관심분야: 정수론, 대수론, 암호이론

장 병 화(Byung-Hwa Jang)정회원

1995년 2월 : 연세대학교 공과대학 전기공학과 졸업(공학사)

1978년 2월 : 한국과학기술원 전자공학과 졸업(공학석사)

1988년 2월 : 한국과학기술원 전자공학과 졸업(공학박사)

1975년 11월~1983년 3월 : KIST 연구원

1982년 3월~현재 : 국방과학연구소 책임연구원

※주관심분야 : 암호응용, 디지털 통신

문 상 재(Sang-Jae Moon) 정회원

1972년 2월 : 서울대학교 공과대학 공업교육과(전자공학, 공학사)

1974년 2월 : 서울대학교 대학원 전자공학과(통신공학, 공학석사)

1984년 6월 : 미국 UCLA(통신공학, 공학박사)

1984년 6월~1985년 6월 : UCLA Postdoctor 근무

1984년 6월~1985년 6월 : 미국 OMNET 컨설턴트

1974년~현재 : 경북대학교 공과대학 전기전자공학부 교수

※주관심분야 : 정보보호, 디지털 통신, 정보통신망