NFC 보안 채널을 위한 인증 알고리즘에 관한 연구

이선근* · 정우열**

A Study on Authentication Algorithm for NFC Security Channel

Seon-Keun Lee* · Woo-Yeol Jeong**

요 약

현재는 스마트폰의 대중화로 인한 NFC의 응용범위가 확대되고 있다. NFC의 확대는 전자결제의 보편화를 의미한다. 그러므로 NFC의 보안은 매우 중요한 사안이다. NFC에 사용되고 있는 암호기법은 AES-128이므로 안전한 방식이다. 그러나 NFC의 활용범위가 증대될수록 이러한 암호기법은 현재까지만 안전하다는 것을 의미한다. 본 논문에서는 NFC의 발전에 따른 안전성에 문제가 발생되지 않도록 하기 위한 방식을 제안한다. 제안된 A-NFC 방식은 비대칭형 방식의 인증기능을 부가함으로서, NFC, NFC-USIM 칩셋에 적용하기 용이하며 보편적 NFC 환경에 잘 적응할 수 있도록 하기 위한 것이다.

ABSTRACT

Recently, applications range of NFC is widening by popularization of smartphone. Expansion of NFC means generalization of electronic payments systems. So security of NFC is very important. AES-128 is safe cryptographic technique for NFC now in use. But, the more range of applications increases, the more safe cryptographic techniques are necessary. In this paper, we propose the safe method is unaffected by the development of NFC. Proposed A-NFC scheme, adding the authentication of asymmetric cryptographic, is easy to apply for NFC and NFC-USIM chipsets, and it can adapt to the general NFC environment.

키워드

NFC, NFC-USIM, Authentication, Security channel, Symmetric cryptographic algorithm
근거리무선통신, NFC-범용가입자인증모듈, 인증, 보안 채널, 대칭형 암호 알고리즘

Ⅰ. 서 론

스마트폰의 대중화로 인하여 근거리 무선통신망이 각광받고 있다. 이러한 시점에서 최근 부상하고 있는 근거리 무선통신망의 하나가 NFC(Near Field Communication)이다. NFC의 사용 주파수대역은 13.56 MHz이며 단말기 간 데이터 전송은 10cm 이하이다. 즉, NFC는 IC칩과 무선을 통해 식품이나 동/식물, 사물 등 다양한 개체의 정보를 관리할 수 있는 차세대 인식 기술인 전자태그(RFID, Radio Frequency Identification)의 발전된 형태이다. 그러나 단말기의 ON/OFF와 관계없이 항상 결제기(reader)가 있어야 인식이 가능하며 정보를 읽어 들이는 것만 가능한 RFID와 다르게 NFC는 양방향으로 데이터를 전송할 수 있기 때문에 NFC 활성화 상태에서 RFID 태그 정보를 인식하고 휴대폰 자체가 카드 리더기로 작동하기 때문에 읽기와 쓰기 모두가 가능한 것이다.

* 전 원광대학교 전자공학과(caiserisk@googlemail.com) ** 한려대학교 멀티미디어정보통신공학과(wooyeol@paran.com)
접수일자 : 2012. 05. 31 심사(수정)일자 : 2012. 07. 26 게재확정일자 : 2012. 08. 09

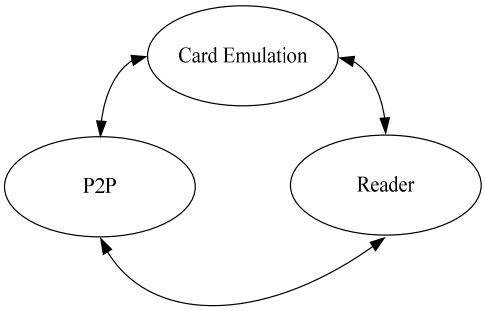

그림 1. NFC 기본 기능
Fig. 1 NFC basic functions

그림 1은 NFC의 기본 기능에 대한 개략도이다. RFID와 유사한 기능을 수행하지만 그림 1과 같이 NFC는 RFID와 기능면에서 엄연한 구별성을 가진다[1].

이와 같이 정보를 주고받는 NFC의 원리에 기반을 두어 현재 다양한 컨텐츠가 서비스 중에 있다. 즉, NFC를 이용하여 결제, 인증, 의료, 모바일 광고, 전자티켓, 전자명함, 소액거래 등 여러 분야에서 응용 서비스가 확대되고 있는 추세이다[1][2].

삼성전자는 이미 스마트폰용 NFC-USIM 보안칩셋을 상용화 하였으며 KT 역시 다양한 기능을 수행할 수 있도록 하는 NFC 칩셋을 개발해 놓은 실정이다[1].

이와 같이 NFC의 활용성은 스마트폰의 보급과 더불어 그 영역이 급속도로 넓어지고 있다[11]. 표 1은 근거리 무선통신망의 비교 스펙이다. 표에서 보는 바와 같이 NFC는 중요한 전자결제를 수행할 능력을 갖추기 위하여 암호화를 적용하고 있다.

표 1. 근거리 무선통신 기술 비교
Table 1. Comparison of short-range wireless technology

기 술	사용주파수	보안성	표준범위	주 서비스 영역
NFC	13.56MHz	암호화 적용	글로벌	비접촉 결제/RFID/ 파일전송
블루트스	2.4GHz	미적용	글로벌	단말기 파일전송
지그비	2.4GHz	미적용	글로벌	기기제어/RFID
900MHz RFID	900MHz	미적용	국내	RFID

그러나 적용되는 암호화 방식이 AES-128이기 때문에, 향후의 급속한 무선통신망의 발달과 다양한 해킹 및 크래킹의 보안누출에 신경을 써야 할 때이다. 또한 AES는 개방된 암호방식이므로 현재도 매우 안전하다고 보장 할 수 없는 실정이다.

AES는 대칭형 알고리즘이기 때문에 오히려 NFC에 적합할 수 있다. 그래서 AES를 사용하고 있지만 NFC의 사용이 증가 될수록 원하지 않는 접속이 증가될 우려가 있으므로 NFC에 비대칭형 특성을 부가해야 할 필요성이 존재한다는 것이다.

그러므로 본 논문은 비대칭형에 사용되는 인증기능을 대칭형에 부가하여 NFC에 적용할 수 있도록 A-NFC(Authentication-NFC) 암호알고리즘을 연구함으로서 보다 안전한 NFC 보안 채널을 형성하고자 하는 것이다.

II. 기존 인증알고리즘

대칭형 암호알고리즘과 병행하여 사용되던 기존 인증알고리즘은 해쉬함수와 MAC/MDC이다.

해쉬함수를 사용하여 안전한 보안채널을 확보하기 위해서는 해쉬함수에 대한 안전성을 고려해야 한다. n비트의 해쉬함수 값을 갖는 키가 없는 해쉬함수의 경우, 다음 두 가지 조건을 만족할 때 이상적인 해쉬함수에 대한 안전성을 갖는다[3][4][5].

ⓐ 각각의 역상과 두 번째 역상을 생성하는데 2^n번의 연산이 필요

ⓑ 충돌을 생성하는데 $2^{n/2}$번의 연산이 필요

이상과 같은 조건을 만족할 때 t비트 키와 고정된 입력에 대해 임의로 선택된 키가 옳은 MAC 키가 될 확률은 $t > n$일때 2^{-t}이다. 그러므로 n비트 MAC 알고리즘에 대하여 주어진 입력에 대한 MAC 값을 올바르게 추측하거나 주어진 MAC 값에 대한 역상의 안전성을 보장받으며 추측할 확률은 2^{-n}이 된다.

해쉬함수가 n비트의 해쉬 함수값을 출력한다고 할 경우, 계산능력을 2^{96}의 연산이 가능하다고 하면 일방향 해쉬함수는 전수 조사 공격에 대항하기 위해서는 n의 값이 96보다 커야 하며 충돌저항 해쉬함수는 birthday 공격으로부터 안전하기 위해서는 n의 값이

192보다 커야 한다[6][7].

메시지 인증코드는 128비트의 키가 사용된다고 가정할 경우 n의 값은 128보다 커야 한다. (n,k,m) 블록암호는 k비트의 키를 이용하여 n비트 크기의 평문을 m비트의 암호문으로 1:1 변환시키는 역변환 가능한 함수를 의미한다. 이때 E를 블록암호함수라 하면 $E_k(n)$라고 표현할 수 있다. 1:1 변환이므로 이와 같은 경우는 $n=m$이다.

블록암호에 적용하기 위한 해쉬함수는 암복호 길이가 평문 n비트, 암호문 n비트와 같이 1:1 변환일 경우의 단일 길이의 해쉬값을 생성하는 것과 평문 n비트에 대한 암호문 $2n$비트를 생성하는 것과 같이 이중길이의 해쉬값을 생성하는 해쉬함수로 나눌 수 있다.

h가 압축함수 f를 갖는 블록암호로부터 생성된 해쉬함수일 경우, h의 해쉬 비율(Hr : Hashing rate)은 $1/r$로 정의된다.

전용 해쉬함수로서는 MD4(Message Digest 4)가 32비트 CPU의 S/W 구현에 적합하도록 설계된 전용 해쉬함수로서 많은 사용되었으나 안전성의 문제로 인하여 지금은 MD5를 기준으로 전용 해쉬함수가 사용되고 있다. MD4에 기반을 둔 SHA-1은 미국 NIST에서 제안한 전용 해쉬함수이며 MD4와 비교하여 160비트를 사용하며 4 라운드를 사용한다는 것이 다른 점이다[8].

데이터 무결성은 인증된 기초자료들을 이용하여 생성, 전송, 저장되는 동안에 인증되지 않은 방법으로 변형되지 않았다는 것을 보장하는 것을 의미한다. 그러므로 데이터 무결성의 판별기준은 제 3자가 임의의 비트를 임의의 길이만큼 추가하거나 삭제 또는 별개의 항목을 추가했는지를 구별하는 것이다[9].

데이터 무결성과 유사한 데이터 고유 인증은 과거에 생성되어 기입된 근거로 데이터 인증에 확신을 주는 부분을 나타낸다. 메시지 인증은 데이터 인증과 비슷하게 사용되는 단어이며 메시지의 근거에 대한 데이터 인증을 포함한다. 데이터 인증은 일반적으로 메시지 인증 코드, 전자서명, 암호문에 추가된 비밀 인증자의 정보를 포함한다.

처리인증은 메시지 인증에 부가적으로 데이터의 유일성과 생성된 시간보장을 포함한 것이다. 유일성과 시간보장 방법으로는 메시지 인증에 시간 변수를 부가적으로 포함시키는 것이다. 암호화과정만을 이용해서는 데이터 무결성을 보장할 수 없다. 만약 임의의 메시지가 A의 키에 의해 복호화 되었을 때 복호화된 메시지가 의미 있는 것이라면 복호화 된 메시지는 A로부터 생성되었다는 가정 하에 발생할 수 있는 보편적 오해는 암호화가 데이터 고유 인증과 데이터 무결성을 제공한다는 것이다. 직관적으로 한 공격자가 메시지들을 조작하기 위해서는 비밀키를 알아야만 한다. 그러나 경우에 따라 공격자가 평문 메시지를 선택할 수 있고 어떤 경우에는 평문을 선택할 수 없음에도 불구하고 평문을 효과적으로 조작할 수 있다[10].

III. 제안된 A-NFC 암호알고리즘

일반적으로 대칭형 암호알고리즘은 인증기능이 없다. 또한 NFC에 적용된 암호알고리즘인 AES-128인 경우도 마찬가지이다. 그러므로 보안이 보장되지 않는 유/무선 채널에서 대칭형 암호알고리즘의 사용은 네트워크 환경에서 매우 한정되어 사용될 수밖에 없다. 이와 반대로 비대칭형 암호알고리즘은 수학적으로 네트워크 환경에서 키 관리 및 분배, 인증기능이 강화되었다는 점에서 많이 사용된다. 그러나 처리시간이 너무 길고 S/W 또는 H/W 구현상의 어려움으로 인한 제약으로 현실적으로는 많이 사용되고 있지 않다는 단점이 있다. 그러므로 A-NFC 암호알고리즘은 대칭형 기반 암호알고리즘이지만 인증기능을 포함함으로서 NFC 네트워크 환경에 적합하도록 하였다.

기존 대칭형 암호알고리즘은 인증기능이 없기 때문에 인증기능이 필요한 네트워크 환경에서는 해쉬함수 또는 MAC와 더불어 사용된다. 그러나 일반 해쉬함수를 사용해야 할 경우 암호문과 해쉬함수 모두를 관리해야하는 단점이 있다.

A-NFC 암호알고리즘은 해쉬함수와 MAC, MDC를 혼합하여 사용함으로서 기존 인증기능을 강화하였다.

대칭형 암호알고리즘을 사용하면서 인증기능과 무결성 기능을 강화시키기 위하여 해쉬함수의 예측 가능한 관계 또는 입출력 상관관계를 나타내지 않도록 하였고 blocked hand-shake 방법을 적용한 MAC와 MDC를 동시에 사용함으로 N:1, 1:N 그리고 N:N 네트워크 환경에 적합하도록 하는 A-NFC 암호알고리

즘을 개발하였다.

그림 2는 NFC 시스템의 구성도이다.

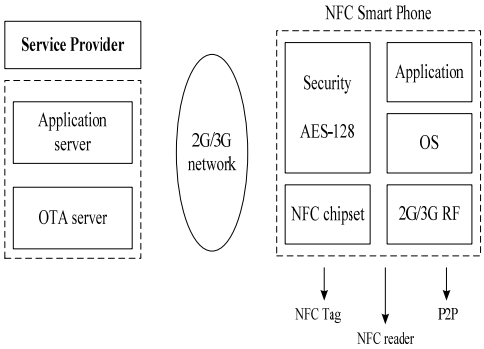

그림 2. NFC 시스템 구성도
Fig. 2 NFC system block diagram

그림 2에서 Security AES-128 부분을 A-NFC로 적용하여 인증기능을 부가함으로서 단순 AES 기능을 수행하는 것이 아니라 보다 안전한 통신채널을 확보하도록 하는 것이다.

즉, 그림 3과 같이 A-NFC 암호알고리즘의 인증기능은 비밀키와 평문 또는 암호문을 이용하여 인증정보를 생산한다.

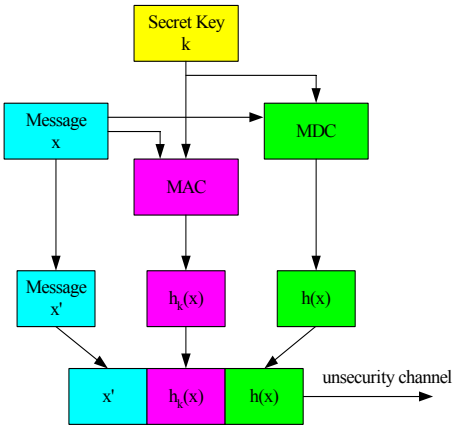

그림 3. NFC를 위한 MAC/MDC 혼합형 인증 구조
Fig. 3 MAC/MDC hybrid authentication structure for NFC

메시지 x'는 x가 암호문인 경우 평문이고 평문인 경우 암호문을 의미한다. A-NFC는 무결성을 제공하며 키 관리를 수행해야 하는 MAC 부분과 해쉬함수를 생성하여 해쉬값을 가지게 되는 MDC를 함께 공유하는 구조로 되어 있다.

먼저, MDC 계산을 수행하는 방법은 다음과 같다.

입력은 $t \geq 2$, 비트 길이 $l = 128t$인 메시지 x이며 출력은 x에 대한 128 비트의 해쉬 값이다.

i) x를 128 비트의 배수를 기준으로 $x = x_1, x_2, x_3, \cdots, x_t$로 정리한다.

ii) 128 비트의 초기값(IV, $\widetilde{IV}$)을 선택한다.

iii) C_i^L과 C_i^R을 각각 C_i의 왼쪽과 오른쪽 32 비트 값이라고 하면 그림 4와 같은 구조에서 식 (1)과 같은 계산을 수행하여 $h(x) = H_t \| \widetilde{H}_t$를 출력하게 된다.

$$H_0 = IV; \qquad \widetilde{H}_0 = \widetilde{IV}; \tag{1}$$

$$k_i = g(H_{i-1}); \qquad \widetilde{k}_i = \widetilde{g}(\widetilde{H_{i-1}});$$

$$C_i = E_k(x_i) \oplus x_i; \qquad \widetilde{C}_i = E_{\widetilde{k}}(x_i) \oplus x_i;$$

$$H_i = C_i^L \parallel \widetilde{C}_i^R \qquad \widetilde{H}_i = \widetilde{C}_i^L \parallel \widetilde{C}_i^R$$

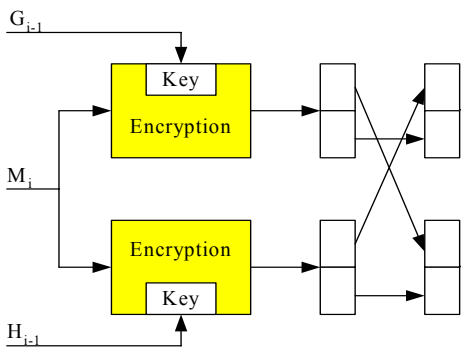

그림 4. MDC 구조
Fig. 4 MDC architecture

다음으로 MAC 계산은 다음과 같다.

입력값은 비트 길이 $32j$인 데이터 x이며 여기에서 $1 \leq j \leq 10^6$이다. 그리고 MAC 128 비트에 대한 비밀키 $Z = Z[1], Z[2], \cdots Z[8]$이다. 이때 출력값은 x에 대한 32 비트 MAC가 된다.

인증을 위한 혼합형 메시지를 만들기 위한 A-NFC 알고리즘은 다음과 같다.

i) 메시지와 무관한 키를 확장한다. 즉 키 집합 Z를 6개의 32 비트로 구성된 X, Y, V, W, S, T 로 확장한다. 이때 X, Y는 초기값(IV)이며 V, W는 주 순환값이며 S, T는 메시지에 첨가되는 padding 값이다.

a) Z의 바이트 0x00나 0xff를 다음에 의해 임의의 바이트로 전환한다.

$P \leftarrow 0;$

for $i = 1$ to 8

$\{P \leftarrow 2P;$

if($Z[i] = 0x00$ or $0xff$)

$\{P \leftarrow P + 1;\ Z[i] \leftarrow Z[i]\ \ OR\ \ P;\}$

$\}$

b) J와 K를 각각 Z의 MSB, LSB 4 바이트라고 할 때 다음을 계산한다.

$X \leftarrow J^4(\mathrm{mod}2^{32}-1) \oplus J^4(\mathrm{mod}2^{32}-2)$

$Y \leftarrow [K^5(\mathrm{mod}2^{32}-1) \oplus K^5(\mathrm{mod}2^{32}-2)](1+P)^2(\mathrm{mod}2^{32}-2)$

$V \leftarrow J^6(\mathrm{mod}2^{32}-1) \oplus J^6(\mathrm{mod}2^{32}-2)$

$W \leftarrow K^7(\mathrm{mod}2^{32}-1) \oplus K^7(\mathrm{mod}2^{32}-2)$

$S \leftarrow J^8(\mathrm{mod}2^{32}-1) \oplus J^8(\mathrm{mod}2^{32}-2)$

$T \leftarrow K^9(\mathrm{mod}2^{32}-1) \oplus K^9(\mathrm{mod}2^{32}-2)$

c) 3개의 결과 쌍 (X, Y), (V, W), (S, T)에서 a)에서와 같이 0x00과 0xff를 제거한다.

d) AND-OR 연산자에 대한 상수를 정의한다.

A= 0x02040801, B= 0x00804021

C= 0x$bfef7fdf$, D= 0x$7dfefbff$

ii) 초기화 및 padding을 수행한다.

a) 초기화 : $v \leftarrow V$, $H_1 \leftarrow X$, $H_2 \leftarrow Y$

b) S, T를 x에 padding한다. 이때 $x_1, \cdots, x_t$를 padding된 32 비트 메시지 블록이라고 표기한다.

iii) 블록을 처리한다.

각 32 비트 메시지 블록 x_i를 다음과 같이 처리한다.

$v \leftarrow (v \hookleftarrow 1)$

$U \leftarrow (v \oplus W)$

$t_1 \leftarrow (H_1 \oplus x_i) \times_1 ((H_2 \oplus x_i) + U)\ \ OR\ A)\ \ AND\ C)$

$t_2 \leftarrow (H_2 \oplus x_i) \times_2 ((H_1 \oplus x_i) + U)\ \ OR\ B)\ \ AND\ D)$

$H_1 \leftarrow t_1, \quad H_2 \leftarrow t_2$

여기에서 $\times_i$는 $\mathrm{mod}2^{32}-i$에서 곱셈연산을, $\oplus$는 $\mathrm{mod}2^{32}$에서의 덧셈연산을, $\hookleftarrow$은 왼쪽으로 1 비트 rotation을 의미한다.

iv) 마지막으로 MAC의 결과값은 다음과 같다.

$$H = H_1 \oplus H_2$$

이상과 같이 MDC, MAC를 구한 후 두 가지 함수에 대한 값을 산출하여 식 (2)와 같이 하나의 frame에 더한다.

$$C = E_k(x \parallel h(x))\ \ \&\ \ E_k(x \parallel h_k(x)) \tag{2}$$

식 (2)에서 $h(x)$를 기준으로 메시지 x를 암호화하여 구해진 MDC 값과 $h_k(x)$를 이용하여 구한 MAC 값을 합하여 하나의 데이터를 만든 것이 암호문 C값이 된다. 이때 MDC와 MAC에 의하여 생성된 값들은 식 (3)과 같이 동일한 IV와 동일한 메시지 x를 사용하여도 항상 상호 독립성을 유지한다.

$$E_k(x \parallel h(x)) \neq (E_k(x),\ E_k(h(x))) \tag{3}$$

만약 식 (3)의 조건을 무시하거나 MDC와 MAC가 종속관계를 가지게 되면 padding을 수행하였다고 하여도 데이터 내부의 MDC, MAC 값을 구별할 수 있는 기준이 사라져 복호화를 수행할 수 없게 된다.

식 (3)과 같이 수행할 수 있기 때문에 A-NFC 암호알고리즘은 기존의 인증 알고리즘과 구별되며, N:N 환경에서 NFC의 안전한 채널을 만족시킬 수 있다. 이러한 특징은 암호 수행 크기가 증가되더라도 비례적으로 증가시킬 수 있다는 장점을 가지므로 AES-128보다 더 큰 수를 가지는 암호방식이라 하더라도 별도의 알고리즘 및 시스템을 구성할 필요성이 없다는 장점을 가진다.

Ⅳ. 결 론

NFC 환경에 적용하고 있는 기존 대칭형 암호알고리즘은 인증기능이 자체적으로 없기 때문에 무선 네트워크 환경에 사용되기 위하여 일반적으로 해쉬함수와 MAC 또는 MDC를 병행하여 사용하게 된다. 이때 전송채널은 암호화된 데이터와 인증용 데이터들이 독립적으로 채널을 확보하여 전송하게 된다. 이러한 현상은 점유 대역폭을 증가시키며, 안전성 또한 위험해진다. 이로 인하여 전송률이 저하되고 품질의 안전을 신뢰할 수 없는 현상이 발생하게 된다.

그러므로 본 연구에서는 제한된 대역폭에서 암호화된 데이터에 인증기능을 포함시키기 위하여 NFC 환경에 MAC와 MDC를 결합한 A-NFC 암호알고리즘을 제안하였다.

제안된 A-NFC 암호알고리즘은 기존에 사용되던 MAC와 MDC를 하나의 인증용으로 사용하기 위하여 결합한 알고리즘이므로, 보다 안전한 통신채널의 확보에 따른 인증 및 암호화 과정을 보장하는 기회를 제공할 것이다. 그러므로 향후 NFC 네트워크 환경에서 안전성 및 네트워크 관리측면에서 비효율적인 비대칭형 암호알고리즘의 사용보다 대칭형 암호알고리즘 기반 A-NFC 암호알고리즘이 매우 유용한 알고리즘이라고 생각된다.

참고 문헌

[1] “모바일 지급결제 표준화 추진”, 지식경제부, (http://www.mke.go.kr) 2011. 3. 9.

[2] 카인즈 (http://www.kinds.or.kr)

[3] R. Anderson, "The classification of hash functions", P. G. Farrell, editor, Codes and Cyphers : Cryptography and Coding Ⅳ, Institute of Mathematics & Its Applications, pp. 83-93, 1995.

[4] I. B. Damgard, "Collision free hash functions and public key signature schemes", Advances in Cryptology EUROCRYPT'87, LNCS, Vol. 304, pp. 203-216, 1988.

[5] B. Preneel, "Cryptographic hash functions", European Transactions on Telecommunication Vol. 5, pp. 431-448, 1994.

[6] H. Dobbertin, "Cryptanalysis of MD-4", D.Gollmann, editor, Fast Software Encryption, Third International Workshop, LNCS, Vol. 1039, pp. 71-82, Springer-Verlag, 1996.

[7] M. J. Bach, "The design of the UNIX operating system", ISBN 0-13-201799-7 or ISBN 0-13-201757-1(international ed.). Prentice-Hall 1986.

[8] M. W. Garrett, "A Service Architecture for ATM: From Applications to Scheduling", IEEE Network May/June 1996.

[9] ATM Forum, "ATM User Network Interface (UNI) Specification Version 3.1", ISBN 0-13-393828-X, Prentice-Hall, Englewood Cliffs, NJ, June 1995.

[10] G. C. Sacket and C. Y. Metz, "ATM and Multiprotocol Networking", ISBN 0-07-057724-2, McGraw-Hill 1997.

[11] 나성훈, 신현식, “VoIP 보안 관련 주요기술에 대한 분석”, 한국전자통신학회논문지, 5권, 4호, pp. 385-390, 2010.

저자 소개

이선근(Seon-Keun Lee)

1995년 원광대학교 전자공학과 (공학사)
1997년 원광대학교 대학원 전자공학과 (공학석사)
2003년 원광대학교 대학원 전자공학과 (공학박사)
2006년~2008년 원광대학교 전자공학과 전임강사
※ 관심분야 : 이동통신시스템, 암호시스템, VLSI 설계

정우열(Woo-Yeol Jeong)

1982년 원광대학교 전자공학과 (공학사)
1984년 경희대학교 대학원 전자공학과(공학석사)
1999년 원광대학교 대학원 전자공학과(공학박사)
1995년~현재 한려대학교 멀티미디어정보통신공학과 교수
※ 관심분야 : 이동통신시스템, 암호시스템, VLSI 설계