JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 12 : 2282~2288 Dec. 2016

NAND Flash Memory의 초기 Bad Block 정보 물리주소를 이용한 보안키 설계와 암호화 기법 제안

김성열*

The Proposed of the Encryption Method and Designed of the Secure Key Using Initial Bad Block Information Physical Address of NAND Flash Memory

Seong Ryeol Kim*

Department of Computer & Information Engineering, Cheongju University, Cheongju, 28503, Korea

요 약

보안키 생성기법으로 하드웨어 또는 소프트웨어 관련 생성기법들이 다양하게 제안되고 있다. 본 연구는 기존의 보안키 생성기법들을 분석하여, NAND 플래시 메모리의 Bad Block 정보를 이용하는 새로운 보안키인 NBSK (NAND Bad block based Secure Key)을 설계하고 이를 이용한 암호화기법을 제안한다. NAND 플래시 메모리에 존재하는 Bad Block은 생산중에 발생하기도 하고 사용 도중에 발생하기도 한다. 생산중 발생하는 초기 Bad Block 정보는 변하지 않으며, 사용도중 발생하는 Bad Block 정보는 주기적으로 변할 수 있다는 특성을 가지고 있다. 따라서 본 연구는 NAND 플래시 메모리 생산중에 발생하는 초기의 Bad Block 정보의 물리주소를 이용하여 보안키로 활용할 수 있도록 암호화키를 설계하고 이를 이용한 암호화 기법을 제안한다. 제안 기법을 이용하면 보안키의 생성과 분배의 단순성과 보안키의 인증성과 기밀성 등의 일반적인 보안 특성을 만족할 수 있다.

ABSTRACT

Security key generation method by hardware or software related techniques have been variously proposed. This study analyzed the existing security key generation techniques, and propose the design of a new NAND Bad block based security key(NBSK) using a Bad Block information in the NAND flash memory, and propose a new encryption method using the same. Bad Block present in the NAND flash memory is also generated during production and sometimes occur during operations. Initial Bad Block information generated during production is not changed, Bad Block information that may occur during operation has a characteristic that can be changed periodically. This study is designed of the new secure key using initial Bad Block information physical address generated during manufacturing a NAND flash memory, and proposed of the new encryption method. With the proposed key and method can satisfy the general security characteristics, such as the creation and distribution of the secure key authentication and confidentiality and the simplicity of the security key.

키워드 : 불량 블록, 불량 블록 테이블, 낸드, 보안키

Key word : Bad Block, BBT, NAND, Secure Key

Received 20 July 2016, **Revised** 22 July 2016, **Accepted** 04 August 2016

* **Corresponding Author** Seong-Ryeol Kim(E-mail: srkim@cju.ac.kr, Tel:+82-43-229-8490)
Department of Computer & Information Engineering, Cheongju University, Cheongju, 28503, Korea

Open Access http://doi.org/10.6109/jkiice.2016.20.12.2282 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

보안키 생성기법으로 하드웨어 또는 소프트웨어 관련 보안키 생성기법들이 다양하게 제안되고 있다. 따라서 본 연구는 기존의 보안키 생성기법들을 고찰하고 새로운 하드웨어 보안키 생성기법으로 NAND 플래시 메모리의 특성인 초기 Bad Block 정보(Bad block information: BBI)의 물리주소(BBI physical address: BBA)을 이용하여 새로운 보안키인 NBSK (NAND Bad block Secure Key) 생성기법을 제안하고자 한다.

NAND 플래시 메모리는 일반적인 플래시 메모리 특성과 NAND만의 고유특성을 가지는 메모리로 데이터를 Write하기 전에 Block 단위로 Erase 한다는 일반적인 플래시 메모리 특성과 NAND만의 고유 특성인 Serial 전송 및 Page 단위로 Read/Write하며, 생산중에 Bad Block을 가진다는 특성[1-4]을 가지고 있다.

이러한 NAND 플래시 메모리의 Bad Block은 생산중에 발생하기도 하고 사용 도중에 발생하기도 한다. 생산중에 발생하는 최초의 일반 사용전 초기 Bad Block 정보는 변하지 않으며, 사용도중 발생하는 BBI는 변할 수 있다는 고유 특성[3]을 가지고 있다.

따라서 본 연구는 이러한 NAND 플래시 메모리 생산중에 발생하는 불변의 최초 BBI 즉, 상품화 초기 BBI의 물리주소(BBA)를 이용하여 새로운 보안키인 NBSK 생성기법을 제안 설계하여 보안키의 생성과 분배관리의 단순성과 보안키의 인증성과 기밀성 등의 보안 특성[5, 6]을 만족할 수 있음을 보인다.

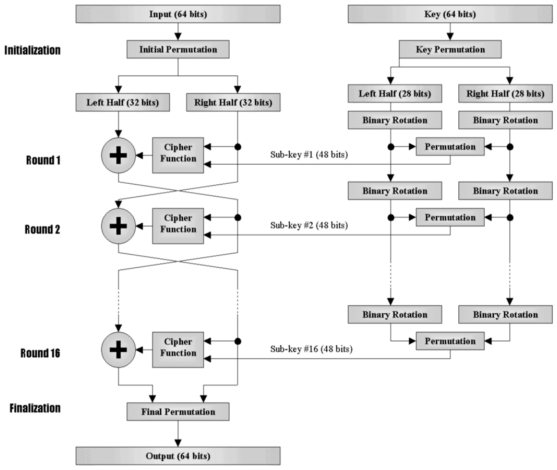
Ⅱ. 관련 연구

2.1. 보안키 암호화 방식

기존 보안키의 암호화 방식은 가장 일반적인 방식으로 DES나 RSA 등의 암호화 알고리즘이 있으며, 이를 응용한 암호화 방식으로는 SSL(Secure Socket Layer), PKI(Public Key infrastructure) 등[7]이 있다.

2.1.1. DES(Data Encryption Standard)

DES 암호는 암호키와 복호키가 같은 대칭 블록암호로서 관련 수식은 암호문(cipher text) C = TK(M) 평문(plain text) 또는 복호문 M = TK-1(C), 알파벳 ei, S = { e0, e1, e2, ... en-1 }, M Î S*, C = { c0, c1, ... }을 이용하여 암호알고리즘[8]을 구현한다. 초기의 DES 알고리즘은 평문의 각 블록의 길이가 64비트이고 키가 64비트(실제로는 56비트가 키이고 8비트는 검사용)이며 암호문이 64비트인 암호였으며, 64비트의 평문이 16라운드의 Feistel 연산을 거쳐 64비트의 암호문으로 암호화하는 것으로 암호화과정은 다음 그림 1과 같다.



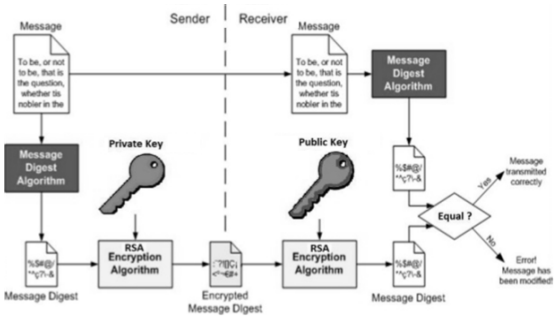
출처: http://homepage.usask.ca/~dtr467/400/

Fig. 1 Block diagram of the DES algorithm

이러한 DES는 전수공격에 취약하여 200년 이후엔 서로 다른 56bit인 암호키 2개를 결합하여 112bit 암호키를 사용하는 3중 DES 암호 방법을 이용하거나 128bit 암호키를 이용하는 IDEA(International Data Encryption Algorithm)을 사용하기도 하며, 미국 NIST에서는 DES의 취약성을 해결하고자 암호키가 128bit이상인 AES (Advanced Encryption Standard) 제정하여 DES를 대신하여 사용되고 있다. 이러한 AES 설계기준은 3중 DES보다 더욱 안전하고 효율적이어야 하므로 암호키의 크기는 128, 192, 256bit, 블록의 크기는 128(64 또는 256 등)bit 이상으로 정의[8]하고 있다.

2.1.2. RSA(Rivest, Shamir, Adleman)

RSA 암호법은 공개키 암호방식으로 1978년에 Rivest와 Shamir, Adleman에 의해 개발[9]되었으며, 공개키(public key)와 개인키(private key)를 사용하여 암호화/복호화(encryption/decryption) 한다. 이러한 키생



출처: http://www.slideshare.net/srilalb/presentation-about-rsa

Fig. 2 RSA encryption flow diagram

성 방법은 p와 q라는 서로 다른($p \neq q$) 소수(prime number)를 선택하여 두수의 곱인 N=pq와 $\Phi(N) = (p-1)(q-1)$를 구한다. 그리고 $\Phi(N)$ 보다는 작고 $\Phi(N)$와 서로 소인 e를 찾아 공개키로 선택하고 e와 N을 공개한다. 사용자가 p, q를 알고 있다면, 확장된 유클리트 호제법을 이용하여 $e*d \equiv 1 \pmod{\Phi(N)} = \pmod{(p-1)(q-1)}$ 즉, 나머지가 1인 정수 d를 비밀키로 선택하여 암호화와 복호화[9, 10]에 사용하고 두 개의 키를 생성한 후에는 p와 q는 삭제하는 것이 안전하다.

RSA 암호화/복호화 과정은 그림 2와 같으며, 암호화 과정은 임의의 송신자가 메시지 M을 전송하려면 평문 M을 N보다 작은 숫자로 변환(padding scheme)하고 공개키 <N, e>를 획득하여 암호문 $c = me \bmod N$를 계산하여 이 암호문 c를 수신측에 전송한다. 또한 복호화 과정은 수신자는 암호문인 c를 수신하고 이미 알고 있는 <N, d>를 이용하여 $m = cd \bmod N$을 계산하여 메시지 M으로 복원[9, 10]할 수 있다. 이러한 RSA는 N이 충분히 큰(200자리 이상) 숫자라면 수퍼컴으로 계산하여도 1 만년 이상이 걸린다고 알려져 있기 때문에 이러한 RSA가 거의 완벽한 암호법[10]이라 할 수 있어 널리 사용되고 있다.

2.2. 보안키 생성과 관리

현존하는 다양한 보안위협으로부터 데이터를 보호하기 위해서는 강력한 암호화 알고리즘(예: DES, RSA, PKI 등)을 이용하여 암호화하여 사용하지만 이러한 암호화된 데이터의 저장장소가 노출된다면 아무리 고강도의 암호 알고리즘으로 암호화한 데이터라고 하더라도 암호키 즉, 보안키를 안전하게 관리하지 못한다면 무용지물이 될 수 있다. 따라서 상존하는 각종 보안 위협으로부터 철저한 보안공격으로부터 피해를 최소화하고 안전한 암호키 또는 보안키 관리를 위하여 다음과 같은 보안정책[5, 6]이 필수적이라 하겠다.

첫째 데이터 암호키는 암호화된 데이터와 물리적인 공간에 분리보관 관리되어야 한다.

둘째 데이터 암호키를 안전하게 저장해야 한다. 키 저장소는 공격자에게 제1순위 공격 대상이 됨으로 키 저장소는 한층 더 높은 보안 수준이 요구된다.

마지막으로 주기적으로 데이터 암호키의 생성·폐기하는 생명주기 관리가 필요하다.

암호화 기술과 암호키 관리는 다양한 보안 사고로부터 데이터를 보호할 수 있어야 하며 데이터 유출 사고를 미연에 방지할 수 있어야 하는 것만이 완벽한 보안대책[5, 6]이 될 수 있다. 그러나 대부분 현존하는 보안키들의 관리방법은 소프트웨어적으로 보안서버에 저장하여 관리하는 방식들이 사용되고 있으나, 키 생성과 관리시 상존하는 보안위협에 대처하기에는 완전한 방식이 될 수 없다. 따라서 이에 대처하기 위하여 최근에 개발된 하드웨어 보안 모듈(Hardware Security Module : HSM)[11]들이 활용되고 있으나, 보안키 생성과 분배는 소프트웨어적으로 처리하거나 이를 각종 디바이스에 탑재하여 관리 보안성을 높인 하드웨어 보안키 관리 방식이다.

2.3. 하드웨어 보안 모듈

HSM은 보안키를 생성하여 강화된 위조 방지 장치 내에 보안키를 안전하게 관리, 처리 및 보관 가능하도록 핵심적인 보안 역할을 수행한다. 아무리 안전하게 보안키를 생성/보관한다고 해도 소프트웨어적으로 보안키를 다루는 것은 잠재적 보안위협 요소가 너무도 많기 때문에 독립적인 하드웨어 장치 내부에서 보안키를 생성하고 보관 관리하는 방식을 채택하고 있는 것이 HSM인 것이다. 또한 HSM은 장비 내부에서 보안키로 암호화, 복호화, 전자서명을 할 수는 있지만 보안키 자체를 절대로 외부로 가져갈 수 없도록 설계[11]되어 있다. 이러한 HSM은 USB를 이용한 보안토큰 이외에도 칩 형태, PCMCIA 토큰 형태, PCI카드 또는 네트워크 서버의 형태를 가질 수도 있다.

HSM는 RSA의 PKCS#11 (Public Cryptography Standards#11), MS의 MSCAPI(Microsoft Cryptography

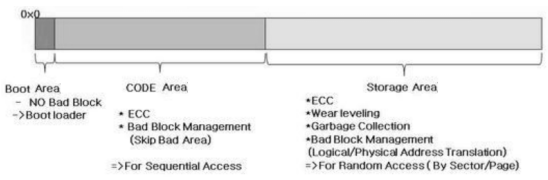
API), JAVA의 JCE(JAVA Cryptographic Engine) 등의 표준 API[11,12]를 통해 PC와 통신한다. HSM의 유형이 USB, PCI 또는 네트워크 서버형이나 동일한 방식으로 정해진 API를 통해서만 HSM과 통신할 수 있고 이 API는 한정된 동작만 허용한다.

이러한 HSM도 소프트웨어 보안키 생성과 분배에 적용된 보안용 SW를 하드웨어에 탑재하여 관리함으로 완벽한 보안키 생성과 분배가 될 수는 없어 향상 복제와 재사용 가능성을 내포하고 있다. 따라서 이러한 문제점들을 해결하기 위하여 NAND Flash Memory의 초기 BBI를 이용한 새로운 보안키인 NBSK 생성과 관리 방법을 제안하고자 한다.

2.4. NAND 플래시 메모리 구조와 Bad Block 정보

NAND 플래시 메모리는 데이터 Write하기 전에 Block 단위로 Erase 한다는 일반적인 플래시 메모리 특성과 NAND만의 고유 특성인 Serial 전송과 Page 단위로 Read/Write하며, 생산중에 Bad Block을 가진다는 특성[1-3, 13]을 가지고 있다. NAND는 Cell이 Page 단위로 구성되며 메모리가 해당 Cell에 접근하기 위해서는 선택하는 Word Line과 전송을 위한 Bit Line이 필요하다. 일반 메모리들은 각 Cell에 대해 접근이 가능하도록 Word Line과 Bit Line을 연결하나, NAND의 경우 Page라고 하는 Bit Line 블록으로 전송하도록 설계되어 있다. 기본적인 Page 단위는 Small Block의 경우 512Byte, Large Block의 경우 2Kbyte 또는 4Kbyte로 구성된다. NAND 메모리 파티션 영역[1-3]은 다음 그림과 같이 2개 또는 3개의 영역으로 구성되며, 각 영역의 기능과 특성은 다음 그림 3과 같다.

- Boot 영역 : 이 영역은 Booting을 위한 Boot Code가 저장되는 영역으로 이 영역엔 절대로 Bad Block이 없어야 하며, 메모리 공급업체에서 이를 보장하여 출하한다. 그러나 단순한 데이터 저장용 NAND에서는 이 영역은 사용하지 않는다.



출처 : http://pastime0.tistory.com/entry/NAND

Fig. 3 NAND partition area

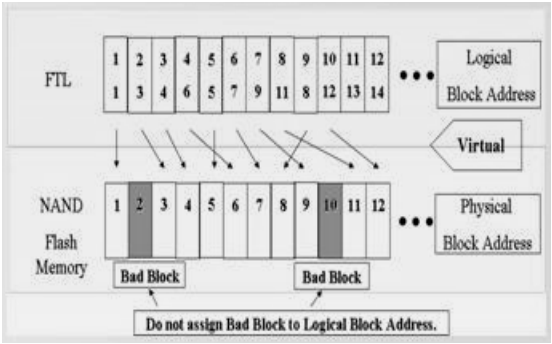


Fig. 4 Relation diagram of Bad Block

- Storage 영역 : 대부분의 사용자가 실제 사용하는 공간으로 Data를 자유롭게 저장하는 공간이다.

- Code 영역: 순차적 Write /Read만 수행하며, 특별한 경우를 제외하고는 Write하는 경우가 거의 없어 Read만 수행한다. 이 영역의 Bad Block 처리는 복잡한 FTL(Flash Translation Layer) 처리과정을 수행하지 않고 Bad Block의 위치만 파악하여 해당 Bad Block을 건너뛰는 방식으로 영역을 관리한다. 자체적으로 Bad Block 수를 관리하여 Bad Block이 많아질 경우 동작하지 않도록 관리한다.

이러한 Bad Block 관계도[2,3]는 다음 그림 4와 같다.

이러한 Bad Block은 NAND 플래시 메모리에만 존재하는 불량 블록으로 생산중에 발생하기도 하고 사용 도중에 발생[1-3]하기도 한다. 생산중 발생한 최초 일반사용전의 초기 Bad Block 정보(BBI)는 변하지 않으며, 최초 BBI는 spare 영역의 여섯 번째 바이트에 “0x00”으로 표시되어 있으며, 사용도중 발생하는 BBI는 “0x59”으로 표시[1,3]되며, 주기적으로 변할 수 있다는 특성을 가지고 있다.

이러한 BBI의 구조는 제조사마다 다를 수 있으나, 구체적인 내용은 관련 제품 Sheet를 통해 확인[13-15]할 수 있다. 예로 삼성의 NAND Flash code Information 구조는 다음 그림 5와 같으며, 14번째가 Customer Bad Block 정보내용의 의미를 표현[15]한다.

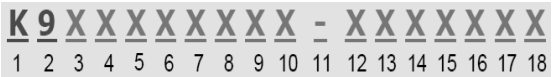


Fig. 5 Samsung NAND Flash code Information

Ⅲ. NBSK 암호화 기법 제안

3.1. NBSK 암호화 개념

제안하는 NBSK 암호화 기법의 개념으로는 1차적으로 기존의 소프트웨어적 암호화 기법인 DES나 RSA 기법을 이용하고 2차적으로 NAND 플래시 메모리 하드웨어 특성으로 생산중에 발생하는 상품화 초기의 BBI는 변하지 않는 최초의 BBI중에 첫번째 BBI 물리 주소(BBI physical Address: BBA)를 이용[1,13]하여 하드웨어 개념인 2차 암호키인 NBSK를 설계하여 이를 이용할 새로운 NBSK 암호화 알고리즘과 기법을 개발 제안한다. 따라서 암호화 기법을 소프트웨어 암화화 기법과 하드웨어 개념의 암호화 기법을 복합적으로 활용한 가능하여 보안강도와 특성을 높이도록 설계 제안한다. 또한 설계 제안한 NBSK와 암호화 기법의 암호키의 생성과 분배관리의 단순성과 보안키의 인증성과 기밀성 등의 보안 특성을 만족할 수 있음을 보인다.

3.2. NBSK 암호화 기법 설계

NBSK 암호화 기법은 기존의 암호화 방법인 DES, RSA 기법 등을 이용하여 1차 암호키로 소프트웨어적으로 사용하고, 새로운 보안키로 NAND 플래시 메모리 Spare 영역[1,13]에 있는 Bad Block 정보(BBI) 물리 주소(BBA)를 이용[4]하여 2차 암호키로 새로운 하드웨어적인 NBSK를 설계하여 이를 이용할 새로운 암호화 알고리즘과 기법을 설계한다.

3.2.1. NBSK 구조

NBSK와 관련된 구조는 다음과 같이 정의하며 암호화에 사용하며, NBSK는 소프트웨어적인 암호키와 하드웨어 특성인 BBA의 순서쌍으로 구성한다. 암호키는 기존의 DES, RSA 암호화에 사용되는 암호키를 1차 암호키로 사용하며, 이를 이용하여 암호화된 암호문에 2차 암호키인 NBSK를 결합하여 NBSK 암호문을 생성하도록 설계한다.

Cipherkey =< DES, RSA key etc>
BBA() = Initial Bad Block Information physical adress
NBSK() = <Cipherkey, BBA()>
NBSK Ciphertext() = Ciphertext() ‖ BBA()

여기서 첨자()는 식별을 위한 첨자로 송신 암호화 측(S), 복호화 측 (R)을 사용하기 위한 식별자이다.

3.2.2. NBSK 암호화/복호화 알고리즘

NBSK 암호화 알고리즘은 다음과 같이 암호화 알고리즘과 복호화 알고리즘으로 설계한다. 암호화 알고리즘은 기존방식인 DES 또는 RSA 기법으로 암호화한 암호문(S)에 NAND BBA(S)를 첨가하여 NBSK 암호문(S)을 생성하도록 설계한다.

<NBSK Encryption Algorithm>

```
Cipher text(S)= result of  DES or RSA encryption
                                              process
get source NAND BBA(S)
NBSK cipher text(S) = cipher text(S) ‖ source NAND
                      BBA(S)       /*concatenation*/
put NBSK cipher text(S)

Sending or stored NBSK cipher text(S) for user
```

NBSK 암호문을 복호화하는 복호화 알고리즘은 다음과 같으며, 수신된 NBSK 암호문(R)을 기존방식인 DES 또는 RSA 기법으로 암호화한 암호문(R)과 첨가된 NAND BBI(R)를 분리하고, 현재 저장되어 있는 NBSK와 분리된 NBSK(R)와 비교하여 동일할 경우 분리된 암호문을 복호화여 평서문으로 변환하도록 설계한다.

<NBSK Decryption Algorithm>

```
Received or get NBSK cipher text(R)
 cipher text(R) = NBSK cipher text(R)
 NBSK(R) = destination NAND BBA(R)
                 /*splitting cipher text and NBSK */

 get source NAND BBA
NBSK = source NAND BBA

if NBSK = NBSK(R)
  then
    plain text = result of  DES or RSA encrypted
                                          cipher text
    put plain text
  else
    Decryption  Error

Using plain text to user
```

3.3. NBSK 암호화/복호화 동작과정

NBSK 암호화/복호화 동작과정은 평서문을 암호화하는 과정과 암호문을 복호화하는 과정으로 나뉜다.

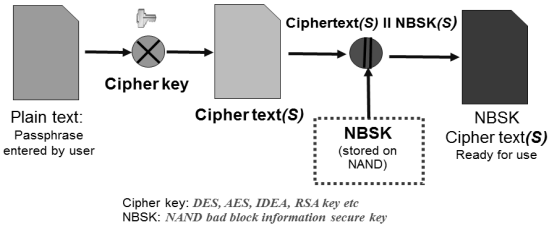


Fig. 6 Encryption process using NBSK

3.3.1. NBSK 암호화 동작과정

NBSK 암호화 동작과정은 설계된 알고리즘에 따라 다음 그림 6과 같이 동작한다.

먼저 평서문을 DES 또는 RSA 기법을 이용하여 암호화하여 암호문(S)을 생성하고, 여기에 자체적으로 가지고 있는 NAND 초기 BBI(S)를 결합 첨가하여 NBSK 암호문(S)을 생성한다. 이러한 암호화 과정을 통해 생성된 NBSK 암호문(S) 형태로 저장하거나 필요에 따라 전송하여 사용자가 활용할 수 있도록 한다.

3.3.2. NBSK 복호화 동작과정

NBSK 복호화 동작과정은 제안설계한 알고리즘에 따라 다음 그림 7과 같이 동작한다.

먼저 저장되어 있거나 수신된 NBSK 암호문(R)을 DES 또는 RSA 기법을 이용하여 암호화된 암호문(R)과 NBSK(R)를 분리한다. 분리된 암호문(R)은 복호화에 사용되며, NBSK(R)는 현재 자체적으로 저장되어 있는 NBSK와 비교하여 복호화를 결정한다. 내장된 NBSK와 수신된 NBSK(R)가 동일하면 수신된 암호문(R)을 DES 또는 RSA 기법을 이용하여 복호화하여 평서문으로 복원하며, 동일하지 않으면 복호화하지 않고 복호오류처리를 수행한다. 복원된 평서문은 사용자 필요에 따라 활용할 수 있도록 한다.

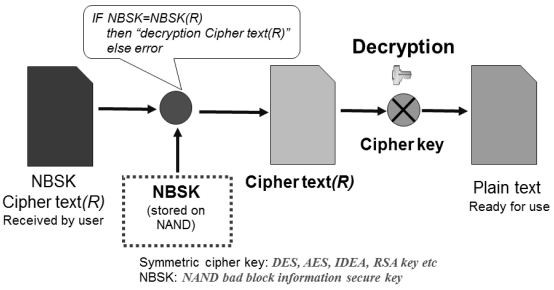


Fig. 7 Decryption process of the NBSK cipher text

3.4. 제안 기법 보안 특성

일반적으로 암호화 기법은 암호키 생성의 견고성, 암호키 분배 관리의 단순성, 보안키의 인증성과 기밀성 등의 보안 특성[5,6]을 만족할 수 있어야 한다.

제안한 NBSK 암호화 기법의 암호키는 1차와 2차의 결합키의 형태로 소프트웨어와 하드웨어 암호화 기법을 복합적으로 이용할 수 있도록 설계하였다. 따라서 기존의 DES 또는 RSA 암호키를 1차키로 소프트웨어적 암호화 기법을 사용함으로써 1차키에 대한 암호키 생성의 견고성, 암호키 분배, 인증성과 기밀성 등은 이미 수많은 검증 연구를 통해 보안특성을 만족함이 보장되고 있다. 따라서 본 연구에서는 하드웨어적 개념을 활용하여 설계한 2차키인 NBSK의 보안 특성만을 고찰 검증한다. 제안한 NBSK 암호화 기법에서 2차키로 사용되는 NBSK 암호키는 하드웨어 특성인 NAND 플래시 메모리 특성상 생산중에 발생하는 최초 BBI 즉, 변하지 않는 상품화 초기의 BBA를 이용함으로 이 또한 정보가 자체적으로 하드웨어에 내장되고 불변한다는 특성을 가지고 있어 암호키 생성과 견고성이 보장될 수 있어 암호키로서 이용에는 보안특성상 전혀 문제가 없다. 또한 NBSK 암호키 분배 관리도 NAND 플래시 메모리에 자체 하드웨어에 내장되어 있는 상품화 초기 불변의 BBIA를 이용함으로 이를 이용한 암호키 분배와 관리가 단순하다. 키의 분배는 암호키가 내장된 NAND 플래시 메모리를 사용함으로 단순하게 분배될 수 있으며, 관리도 불변의 키 정보가 내장되어 있어 별다른 관리가 필요하지 않아 단순하다. 그리고 NAND 플래시 메모리 사용에 문제가 있다면 내장된 NBSK 암호키를 사용할 수 없으므로 폐기관리도 불필요하여 NBSK 암호키 분배관리의 단순성을 보장할 수 있다.

그리고 제안한 암호화 기법은 1차 암호키와 2차 암호키를 함께 사용함으로 보안키의 인증성과 기밀성을 보장할 수 있어 보안강도를 높일 수 있다. 단순하게 1차 키나 2차 키가 노출되었다 하더라도 하나의 키로는 필요한 암호화/복호화 작업을 할 수 없으며, 설상 2개의 키가 함께 노출되었다 하더라도 NBSK 내장되어있는 NAND 플래시 메모리가 활성화되어 있는 경우에만 필요한 암호화/복호화 작업가능하기 때문에 보안 인증성과 기밀성을 보장할 수 있다. 따라서 제안한 NBSK 암호화 기법은 암호키 생성의 견고성, 암호키 분배 관리의 단순성, 보안키의 인증성과 기밀성 등의 보안 특성을 만족한다.

Ⅳ. 결 론

본 연구는 NAND 플래시 메모리 생산중에 발생하는 불변의 최초 BBI 즉, 상품화 초기 BBI의 물리주소(BBA)를 이용하여 하드웨어 특성을 이용한 보안키 NBSK를 설계하고 이를 이용 가능한 암호화 기법을 제안하였다. 설계 제안한 NBSK 암호화 기법은 1차적으로 기존의 소프트웨어적 암호화 기법인 DES나 RSA 기법을 이용하고, 2차적으로 NAND 플래시 메모리 특성인 생산중에 발생하는 상품화 초기의 BBI는 변하지 않는 최초의 BBI 중에 첫 번째 BBI 물리 주소(BBA)를 이용하는 하드웨어적 특성을 이용하여 2차 암호키인 NBSK 보안키를 설계하고 이를 이용하는 새로운 NBSK 암호화 알고리즘을 개발하여 암호화 기법을 제안하였다. 또한 설계 제안한 NBSK 암호화 기법의 암호키의 생성과 분배관리의 단순성과 보안키의 인증성과 기밀성 등의 보안 특성을 만족할 수 있음을 보였다. 따라서 본 연구 결과로 설계 제안한 NBSK 암호화 기법을 적용하면 기존의 소프트웨어적인 암호화 방식과 하드웨어 방식의 암호화 방식의 특성을 가질 수 있어 보안강도를 증강 향상시킬 수 있을 것으로 기대한다.

REFERENCES

[1] NAND [Internet], Available: http://pastime0.tistory.com/entry/NAND.

[2] NAND bad blocks [Internet], Available: http://wiki.openmoko.org/wiki/NAND_bad_blocks.

[3] C. H Wu, “A Bad-Block Test Design for Multiple Flash-Memory Chips”, *Journal of information Science and Engineering*, vol. 28, pp.1091-1104, 2012.

[4] S. R. Kim, “Design of a User Authentication System using the Device Constant Information”, *Journal of IT Convergence Society for SMB*, vol. 6, no. 3, pp.29-35, Sep. 2016.

[5] Ho-seok Ryu et al, “Group Key Management Method for Secure Device in Smart Home Environment”, *Journal of The Korea Institute of Information Security & Cryptology*, vol. 25, no. 2, pp. 479-487, Apr. 2015.

[6] KISA “IT Security Evaluation & Certification Guide with Common Criteria (ISO 15408)”, KISA, 4. 2009.

[7] Information Security [Internet], Available: http://m.blog.naver.com/PostList.nhn?blogId=nttkak&categoryNo=19&currentPage=1.

[8] Development and Analysis of Block Ciphers and the DES System [Internet], Available: http://homepage.usask.ca/~dtr467 /400/.

[9] L. M. Adleman, R. L. Rivest, and A. Shamir, “A method for obtaining digital signatures and public-key cryptosystems”, *Communications of the ACM*, vol.21, pp.120-126, 1978.

[10] RSA [Internet], Available: https://ko.wikipedia.org/wiki/RSA_%EC%95%94%ED%98%B8.

[11] HSM(Hardware Security Modules) [Internet], Available: https://handouts.secappdev.org/handouts/2010/Filip%20Demaertelaere/HSM.pdf.

[12] Microsoft CryptoAPI [Internet], Available: https://en.wikipedia.org/ wiki/MicrosoftCryptoAPI.

[13] Micron, “Bad Block Management in NAND Flash Memory”, Micron Technology Inc., TN-29-59, 2011.

[14] Open NAND Flash Interface specification: Block Abstracted NAND [Internet], Available: http://www.onfi.org/~/media/ONFI/specs/BA_NAND_rev_1_1_Gold.pdf.

[15] Samsung NAND Flash Code Information(1/3) [Internet], Available: http://www.samsung.com/global/business/semiconductor/html/common/file/support/part_number_decoder/Nand_Flash.pdf.

김성열(Seong-Ryeol Kim)

1982년 숭실대학교 전자계산학과 공학사
1987년 숭실대학교 대학원 전자계산학과 공학석사
1992년 숭실대학교 대학원 전자계산학과 공학박사
1982년~1984년 한국전력공사 전자계산소 근무
1984년~1990년 오산대학 전자계산과 교수
1997년~1998년 호주 QUT ISRC 객원 교수
1990년~현재 청주대학교 컴퓨터정보공학과 교수
※관심분야 : 컴퓨터 네트워크, 컴퓨터 보안, 사물인터넷