데이터 전송 오류에 대한 고장 극복 암호회로

Fault Tolerant Cryptography Circuit for Data Transmission Errors

유영갑, 박래현, 안영일, 김한벼리
충북대학교 정보통신공학과

Younggap You(ygyou@cbnu.ac.kr), Raehyeon Park(rhpark@hbt.cbnu.ac.kr),
Youngil Ahn(yiahn@hbt.cbnu.ac.kr), Hanbyeori Kim(hbkim@hbt.cbnu.ac.kr)

요약

본 논문은 암호문 송신 중 전송 오류에 의한 암복호화의 문제에 대한 해결책을 제시 한다. 블록 암호 알고리즘은 산사태(avalanche) 효과로 인해 단일 비트 오류에 대해서도 많은 비트에 오류를 발생시킨다. 이를 해결하기 위해 재배열 과정과 간단한 오류 정정 코드를 이용해서 산사태(avalanche) 효과에 강인한 방안을 제안한다. 재배열 과정은 간단한 오류 정정 코드를 사용하기 위한 것이다. 재배열 과정은 한 프레임 내에서 전송의 기본 단위인 n-비트 블록 내에 1비트의 단일 오류만이 존재 할 수 있도록 오류를 여러 단위에 분산시키는 역할을 하게 된다. 즉, n-비트 내에서 단일 오류만이 존재하게 되어 단일 오류 정정 코드로 쉽게 복원이 가능하게 된다. 이 방식은 보다 큰 데이터 단위에 확장하여 사용 될 수 있다.

■ 중심어 : | 산사태 효과 | 고장 극복 | 오류 정정 |

Abstract

This paper presented a solution to encryption and decryption problem suffering data transmission error for encrypted message transmission. Block cypher algorithms experience avalanche effect that a single bit error in an encrypted message brings substantial error bits after decryption. The proposed fault tolerant scheme addresses this error avalanche effect exploiting a multi-dimensional data array shuffling process and an error correction code. The shuffling process is to simplify the error correction. The shuffling disperses error bits to many data arrays so that each n-bit data block may comprises only one error bit. Thereby, the error correction scheme can easily restore the one bit error in an n-bit data block. This scheme can be extended on larger data blocks.

■ keyword : | Avalanche Effect | Fault Tolerant |Error Correction |

I. 서 론

컴퓨터와 전기 통신 기술의 발달과 더불어 컴퓨터 통신망의 보급으로 종합 정보 시스템이 구축되고 있다. 컴퓨터 통신이 확대되어 감에 따라 정보에 대한 보안의 중요성이 증대되었다. 암호 알고리즘은 가장 경제적이고 정보 시스템이 요구하는 정보의 보안 수준에 따라 효율적이면서도, 계층적인 보안 대책을 제공할 수 있다.

다양한 분야에 블록 암호 알고리즘이 활용되고 있다. 모든 블록 암호는 평문이 암호문으로 변환되는 과정을

* 본 논문은 2007년도 충북대학교 학술연구지원사업의 연구비지원에 의하여 연구되었습니다.
접수번호 : #080916-004
접수일자 : 2008년 09월 16일
심사완료일 : 2008년 10월 02일
교신저자 : 유영갑, e-mail : gjkim@konyang.ac.kr

포함하며 변환의 결과는 키에 달려있다. 확산(diffusion)은 키를 추론하기 어렵게 하기 위해 평문과 암호문 사이에 통계적인 관계를 가능한 한 복잡하게 한다. 한편 혼돈(confusion)은 키를 발견하기 어렵게 하기 위해 암호문에 대한 통계 값과 암호 키 값 사이의 관계를 가능한 복잡하게 만든다[4].

블록 암호 알고리즘은 암호문에 오류가 발생하면 복호화 할 때 블록 전체에 오류가 번지는 산사태(avalanche)효과를 보인다. 산사태 효과는 평문이나 키의 미소한 변화라도 암호화 및 복호화 과정에서 큰 변화를 일으키는 효과이다. 단일 비트의 변화가 암호문 블록의 반 이상에 변화를 줄 수 있다.

본 논문에서는 데이터 통신 시스템에서 채널상의 노이즈 등으로 인하여 발생 될 수 있는 오류에 대해 간단한 오류 정정 코드를 이용하여 오류에 강인한 모델을 제안 하고자 한다. 제안하는 방식은 오류 정정 코드를 효과적으로 활용하고 산사태 효과를 극복하기 위하여 데이터 재배열 기법을 도입한다. 데이터 재배열은 8비트 내에 단일 오류만이 존재할 수 있도록 오류들을 분산하는 기능을 할 것이다.

태영수, 이만영[2]은 오류 정정 코드를 스트림 암호시스템에 적용함으로써 잡음에 강인한 복원, 오류 전파의 최소화 그리고 인증등과 같은 문제점을 분석 및 해결하고자 했고, 양경철[3]은 wire-tap channel과 함께 부호이론의 응용에 대한 고찰을 했었다. 그러나 본 논문에서는 기존 연구들에서는 논의 되지 않은 오류들의 분산을 통해 간단한 단일 오류 정정 코드만을 이용해 오류에 강인한 암호 회로를 제안 하고자 한다.

이 논문의 구성은 다음과 같다. Ⅱ장에서는 블록 암호 알고리즘에 대해서 소개한다. Ⅲ장에서는 제안하는 방식에 대해서 설명한다. Ⅳ장에서는 제안된 암호 회로의 구현에 대해서 설명한다. Ⅴ장에서는 산사태 극복 과정 및 시뮬레이션 결과에 대해서 기술한다. 마지막으로 Ⅵ장에서는 결론을 서술한다.

Ⅱ. 블록 암호 알고리즘

블록 암호 알고리즘은 암호화와 복호화에 동일한 키를 사용함으로 공통키 암호 알고리즘 대칭 암호 방식이라고도 한다. 본 논문에서는 대표적인 블록암호인 AES(Advanced Encryption Standard) 암호 알고리즘[1]을 사용하였다. 국내에서 개발된 ARIA는 AES를 보다 높은 비도를 갖도록 개량한 것이다. 여기에서 다루는 내용은 ARIA에 그대로 적용가능하다.

처음에 개발된 Rijndael 알고리즘은 암호화에 사용하는 키의 길이와 입력 메시지 블록의 길이가 128비트, 192비트, 256비트 중 하나를 선택 할 수 있었다. 그러나 FIPS-197에 등록된 AES 알고리즘은 입력 메시지 블록의 길이가 128비트로 고정 되었고, 사용하는 암호화 키의 길이만 128비트, 192비트, 256비트 중에서 선택 할 수 있도록 정의하였다.

AES는 지금까지 알려진 블록 암호 알고리즘에 대한 모든 공격 방법들에 대해 안전하도록 설계되었다. 이 알고리즘은 하드웨어나 소프트웨어 구현 시 속도나 코드 압축 면에서 효율적이므로 스마트 카드와 같은 응용분야에 적합하다는 장점이 있다.

Ⅲ. 제안하는 방식

제안하는 방식은 재배열을 이용하여 오류를 분산하고 분산된 단일 오류들은 간단한 오류정정 코드를 이용하여 복원한다.

```
1. 입력(평문)
2. 오류 정정 코드 생성(Hamming code)
3. 재배열 과정
   for i←block number downto 1
     블록 단위의 재배열
   for i←frame number downto 1
     프레임 단위 재배열
4. 암호화(AES 암호 알고리즘)
5. 송·수신
7. 복호화(AES 암호 알고리즘)
8. 역재배열
   for i←frame number downto 1
     프레임 단위 역재배열
   for i←block number downto 1
     블록 단위 역재배열
9. 오류 정정(Hamming code)
10. 출력(평문)
```

그림 1. 제안하는 방식의 pseudo code

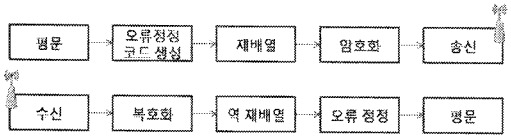
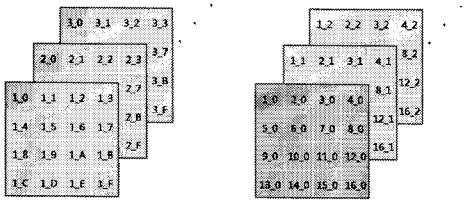


그림 2. 전체 블록도

[그림 1]은 제안하는 방식의 pseudo code 이고, [그림 2]는 제안하는 오류 정정 기능이 포함된 암호 프로세서의 전체 블록도이다. 입력 된 평문은 오류 정정 코드를 생성 한다. 입력된 평문은 재배열 과정을 거친다. 재배열 과정은 블록 단위의 재배열과 프레임 단위 재배열의 2단계를 거친다. 재배열 된 데이터는 암호화 과정을 거친다. 암호화된 데이터는 송신된다. 수신된 데이터는 복호화 과정을 거친다. 복호화 된 데이터는 역재배열 과정을 거친다. 역재배열과정은 재배열 과정의 역으로 진행한다. 이 과정은 프레임 단위 역재배열을 먼저 수행하고 블록 단위 역재배열을 수행한다. 역재배열 된 데이터는 오류 정정을 거치고 출력으로 본래의 평문으로 변환된다.

제안하는 방식에서 암호화 및 복호화는 블록 암호 알고리즘을 사용한다. 본 논문에서는 AES 암호화 알고리즘을 사용하여 검증 하였다. 오류 정정 코드는 단일 오류 정정이 가능한 Hamming code를 사용하였다.

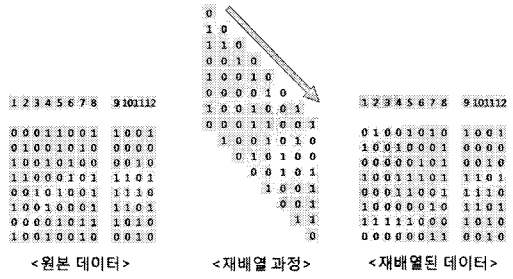
데이터 재배열은 제안하는 오류 정정이 가능한 암호회로에서 가장 중요한 블록이다. 재배열 과정은 크게 2단계로 나누어진다.



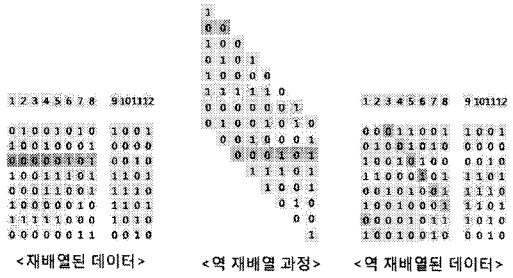
(a) 재배열 전 (b) 재배열 후

그림 3. 프레임 단위 재배열

첫 번째는 프레임 단위의 데이터 재배열이다. [그림 3]에서 4*4배열은 프레임 단위 블록을 나타내고 있다. 프레임 단위 블록은 블록 암호화 알고리즘의 1회 데이터 입•출력 길이를 가진다. 프레임 단위의 재배열은 각 블록의 첫 번째 데이터만을 모아서 새로운 하나의 첫 번째 블록을 생성한다. 다시 각 블록의 두 번째 데이터만을 모아서 새로운 두 번째 블록을 생성한다. [그림 3]a에서 색칠된 각 블록의 첫 번째 데이터들은 [그림 3]b에서 첫 번째 블록으로 재배열 된 것을 확인 할 수 있다. 새로운 프레임 블록은 이와 같은 방법을 반복해서 구성된다. 프레임 단위의 역재배열은 반대의 과정이다.



(a) 재배열과 해밍코드 생성



(b) 역재배열과 해밍코드를 이용한 오류 정정

그림 4. 블록 단위 재배열

두 번째는 블록 단위의 재배열이다. 블록 단위의 재배열은 데이터를 전송단위로 나누고 전송단위별로 오류 정정 코드를 생성한다. [그림 4]a에서는 8*8의 64비트 블록에 대한 재배열과 해밍 코드 생성을 보여준다. 재배열 과정은 가로방향으로 정렬된 데이터를 대각선 방향으로 재배열을 하고 해밍코드를 생성한다. [그림 4]b는 역재배열 과정을 보여준다.

예를 들어 전송할 데이터가 64 비트이고 전송단위가 8비트라 가정한다. 위의 [그림 4]에서 원본 데이터는 가로 방향으로 정렬된 2차원 배열로 표현한다. 대각선 방향으로 전송을 실행하게 되면 실제 재배열된 데이터는

[그림 4]에서 보이는 것처럼 정렬이 이뤄진다. 재배열된 데이터는 원본 데이터의 한 바이트의 내용이 가로 혹은 세로 열에서 겹치지 않도록 정렬된 것이다.

이와 마찬가지로 데이터의 역재배열이 이루어진다. [그림 4]에서 만약 재배열된 데이터의 색칠된 8비트에 오류가 있다고 가정 한다면 역재배열 된 데이터에서는 각각의 오류 비트들이 분산되어서 가로 혹은 세로 열에서 겹치지 않는 것을 확인 할 수 있다. 제안하는 방식은 이렇게 분산된 단일 오류를 간단한 오류 정정 기술을 이용하여 복원 가능하게 한다.

IV. 제안된 암호 회로 구현

제안된 모델의 암호회로는 [그림 5]와 같이 구성했다. 이 암호회로는 C언어를 이용하여 구현 및 검증하였다. 이 회로에는 ECC encoder, 재배열, 암복호, 역재배열, ECC decoder 블록을 포함하고 있다. 이 회로블럭은 송신 또는 수신 기능에 따라 선별적으로 사용되도록 multiplexer를 통하여 입력을 공급받는다.

Encoder 블록은 송신 동작일 때 사용된다. Encoder 블록은 입력된 데이터를 오류 정정 회로를 이용하여 인코딩한다. 본 회로에서는 Hamming code를 사용하였다. Decoder 블록은 수신 동작일 때 사용된다. Decoder 블록은 역재배열 된 데이터를 Hamming code를 이용하여 오류 정정을 한다.

재배열(rearrangement) 회로는 송신 동작일 때 사용된다. 재배열 회로는 Encoder 블록을 통과한 데이터를 제안하는 방법에 따라 재배열하는 회로이다. 입력과 출력은 단순한 와이어링 구조이다. 역재배열(inverse rearrangement) 회로는 수신 과정에 사용된다. 역재배열 회로는 재배열의 역방향 회로이다. 재배열된 데이터를 본래의 순서로 되돌리는 회로이다. 입력과 출력은 단순한 와이어링의 구조이다.

Cryptography 회로는 데이터를 암호화하는 블록암호 알고리즘을 사용한다. 본 논문에서는 AES 암호 알고리즘을 사용하였다.

Mode_Sel는 송신측과 수신측의 동작을 선택하는 신호이다. Mode_Sel가 '0'이면 송신측의 동작이 수행된다. 입력 데이터는 오류 정정 코드를 생성하고 재배열 후에 암호 회로를 거친 결과가 출력 된다. Mode_Sel가 '1'이면 수신측의 동작이 수행된다. 수신된 데이터는 복호화 회로를 거치고 역재배열 후에 오류 정정 코드를 이용한 오류 정정 결과가 출력 된다.

V. 산사태 효과 극복 과정 및 시뮬레이션 결과

일반적인 암호알고리즘에서 1비트의 오류가 결과에 미치는 영향은 [그림 6]에서 확인 할 수 있다. [그림 6]에서는 블록 암호 알고리즘의 대표적인 AES암호 알고리즘을 활용하여 1비트 오류로 발생되는 산사태(avalanche)효과를 확인 할 수 있다. [그림 6]의 평문, 암호문, 복호문에서 상단의 굵은 상자는 64비트의 내용을 16진수로 표현하였고, 하단의 상자는 2진수로 표현하였다.

암호문은 평문을 AES암호 알고리즘을 이용하여 암호화함으로써 얻어진다. 얻어진 암호문에서 1비트에 대한 오류를 임의로 발생 시켰다. [그림 6]의 암호문에서 하단 1행 4열에 임의로 오류를 발생시켰다. 오류가 발생된 암호문을 이용하여 복호화 과정을 거친 결과 동그라미로 표시된 부분들은 오류가 발생된 부분들이다. 이 결과로부터 블록 암호 알고리즘에서 1비트의 오류가

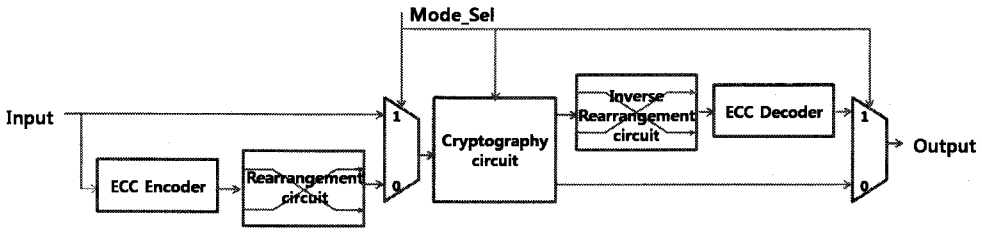


그림 5. 제안하는 암호회로 블록도

산사태(avalanche)효과로 인해 결과에 미치는 영향이 심각하다는 것을 확인 할 수 있다.

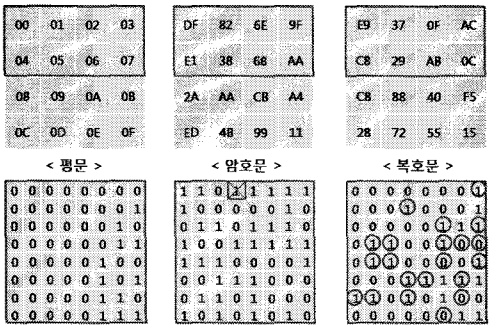
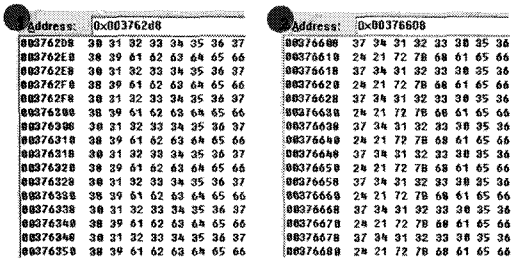
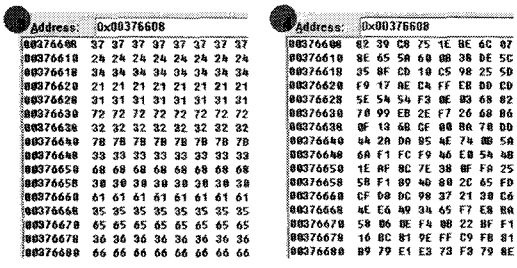


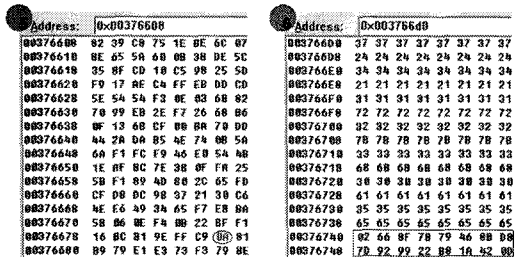
그림 6. 암호회로에서 1비트 오류에 대한 avalanche 효과



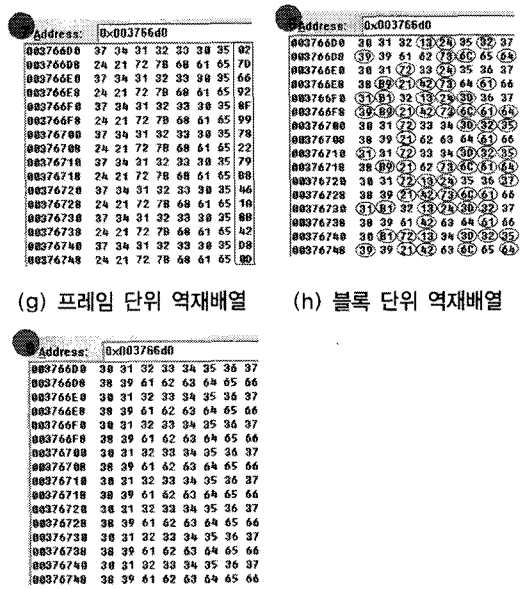
(a) 평문 (b) 블록 단위 재배열



(c) 프레임 단위 재배열 (d) 암호



(e) 1바이트 오류 발생 (f) 복호



(g) 프레임 단위 역재배열 (h) 블록 단위 역재배열

(i) 오류 정정

그림 7. Fault tolerant 암·복호 과정

이 논문에서 제안하는 방식이 AES암호 알고리즘에 해밍코드와 데이터 재배열 블록을 추가하여 오류를 정정할 수 있다는 것을 시뮬레이션을 통해 검증 한다. [그림 7]에서는 제안하는 방식을 이용하여 오류가 정정되어지는 과정을 메모리 맵을 통해 보여준다.

[그림 7]a에서 최초 입력이 이루어진 1024비트를 보여주고 있다. 본 시뮬레이션에서는 이 1024비트가 한 프레임이 된다. 입력된 데이터는 16진수로 표현 되어 있다. [그림 7]b에서는 블록 단위의 재배열 결과를 보이고 있다. 각각의 8*8비트 단위로 재배열이 이루어진 결과를 보여준다. [그림 7]c는 프레임 단위의 재배열이 이뤄진다.

AES의 기본 블록이 되는 128비트 단위로 각 8개의 블록에서 특정 부분들을 취합해서 새로운 128비트 단위의 블록을 생성한다. 기본 단위인 128비트(16바이트) 중에서 각 블록의 처음 8비트(1바이트)를 차례로 모아서 새로운 첫 번째 128비트(16바이트)를 생성 할 수 있다. 이와 같은 방법을 반복해서 새로운 AES 암호화 블록 단위의 재배열이 이루어진 1024비트의 데이터를 생성한다. [그림 7]d는 AES 암호화 알고리즘을 거친 결과

이다. AES 암호화 알고리즘의 블록인 128비트 단위로 8번을 반복하게 된다.

[그림 7]e에서는 암호화 결과에 임의로 기본 전송 단위인 8비트(1바이트)에 대한 오류를 발생시켰다. [그림 7]f에서는 오류가 발생한 암호 데이터가 AES 복호화 알고리즘을 거친 결과를 보여준다. 1바이트의 오류를 발생시켰지만 결국 복호의 기본단위인 128비트에서 다수의 비트에 오류가 발생하는 것을 확인 할 수 있다.

[그림 7]g는 AES 암호 알고리즘의 기본 블록 단위인 128비트 단위의 역재배열을 실시한 결과이다. 128비트의 오류가 각각의 블록에 1바이트(8비트)씩 분산되는 것을 보여준다. [그림 7]h에서는 각각의 8*8비트 배열에서 역재배열을 통해 8비트의 오류가 각각의 8비트에 1비트씩 분산 되는 것을 확인 할 수 있다. 결과적으로 역재배열이 완료되면 8비트에서 1비트만의 오류를 갖도록 128비트의 오류가 각각의 바이트로 분산된다. [그림 7]i는 Hamming code를 이용해 8비트 내에서 1비트에 대한 단일 오류 정정을 한다. 정정 과정을 거친 결과 [그림 7i]는 본래의 입력 데이터[그림 7a]와 동일하다는 것을 확인 할 수 있다.

시뮬레이션 결과로 AES 블록 암호 알고리즘에서 단일 비트의 오류는 다수의 비트에 오류를 가져오는 산사태(avalanche)효과를 확인하였다. 제안된 방식을 적용하면 산사태 효과로 인한 다수의 오류가 블록 단위의 재배열과 프레임 단위의 재배열을 통해 분산되는 것을 확인하였다. 즉, 8비트 내에서 단일 오류(1비트의 오류)만이 존재 하게 된다. 단일 오류는 Hamming code를 이용하여 완벽한 정정이 가능하다. 이것은 n*n비트 블록 내에서 연속되는 n비트의 오류를 단일 오류로 분산 가능하며, n*n*n비트의 프레임 블록 내에서는 연속되는 n*n비트 블록의 오류를 단일 오류로 분산 가능 하다는 것을 확인했다. 이러한 규칙은 n비트를 기준으로 지수의 관계를 갖고 있으며, 배수의 법칙이 적용가능하다.

시뮬레이션을 예로 들면 n은 8이 되고, n*n은 64가 된다. AES 블록 암호 알고리즘의 기본 블록이 128비트이기 때문에 n*n블록(64비트)의 2배의 사이즈가 된다. 따라서 프레임 블록의 사이즈는 n*n*n(512비트)의 2배가 되는 1024비트가 되는 것이다.

결과적으로 본 시뮬레이션은 미소 오류로 인한 산사태 효과의 극복이 가능하다는 것을 검증하였다.

VI. 결 론

본 논문은 블록 암호 알고리즘에서 입력 1비트의 오류가 결과적으로 다수의 비트에 오류를 발생하는 산사태(avalanche) 효과에 대한 문제를 해결하기 위한 모델을 제안하였다. 간단한 오류 정정 코드와 데이터의 재배열을 통하여 이러한 문제를 해결하였다. 단일 오류 정정 코드를 사용하기 위해서 본 논문에서는 데이터 재배열을 도입하였다. 데이터 재배열을 통하여 기본 전송 단위인 8비트 내에 1비트의 단일 오류만이 존재 하도록 하였다.

본 논문의 시뮬레이션에서는 블록 암호 알고리즘에서 대표적인 AES(Advanced Encryption System)를 사용하였다. 오류 정정 코드로는 단일 오류 정정 코드의 대표적인 Hamming code를 사용하였다. 이렇게 Hamming code와 같은 간단한 오류 정정 코드와 데이터 재배열 과정을 거쳐 통신상 혹은 내부적인 노이즈로 인한 미소한 오류에 의해 발생될 수 있는 산사태(avalanche) 효과를 해결 할 수 있을 것으로 기대된다. 향후 암·복호 알고리즘 뿐 아니라 특히 인증과 관련된 분야에 있어서 데이터의 오류로 인한 재전송 등의 번거로움을 줄임으로써 다양한 활용이 가능 할 것이다.

참 고 문 헌

[1] http://csrc.nist.gov

[2] 태영수, 이만영, "오류정정부호를 이용한 스트림 암호 시스템에 관한 연구", 정보보호학회지, 제1권, 제1호, pp.66-78, 1991.

[3] 양경철, "부호이론을 이용한 암호기법에 관한 고찰", 정보보호학회지, 제3권, 제2호, pp.36-42, 1993.

[4] C. E. Shannon, "Communication theory of

secrecy systems," Bell System Technical Journal, Vol.28, pp.656-715, 1949.

[5] L. Breveglieri, I. Koren, and P. Maistri, "An operation-centered approach to fault detection in symmetric cryptography ciphers," IEEE Transactions on Computers, Vol.56, No.5, pp.635-649, 2007.

[6] 이문호, 김순영, *오류 정정 이론 : 터보코드의 기본 원리와 응용*, 도서출판 영일, 2001.

[7] S. Y. Shin, H. S. Park, S. C.hoi, and W. H. Kwon, "Packet error rate analysis of ZigBee under WLAN and Bluetooth interferences," IEEE Transaction on Wireless Communications, Vol.6, No.8, pp.2825-2830, 2007.

[8] W. Xiao, Y. Sun, Y. Liu, and Q. Yang, "TEA : transmission error approximation for distance estimation between two Zigbee devices," 2006 International Workshop on Networking, Architecture, and Storages, 2006.

[9] Y. Xiao and M. Guizani, "Optimal stream-based cipher feedback mode in error channel," Global Telecommunications Conference 2005, pp.1660-1664, 2005.

[10] P. H. Liu and Y. Lin, "A class of (d,k) block codes with single error correcting capability," IEEE Transactions on Magnetics, Vol.33, No.5, pp.2758-2760, 1997.

[11] R. K. James, T. K. Shahana, K. P. Jacob, and S. Sasi, "Fault tolerant error coding and detection using reversible gates," Tencon 2007 - 2007 IEEE Region 10 Conference, pp.1-4, 2007.

[12] 박성경, 김신령, 강창언, "해밍코드를 이용한 효율적인 Hybrid ARQ 시스템의 성능분석", 한국통신학회논문지, 제13권, 제6호, pp.535-544, 1988.

저 자 소 개

유 영 갑(Younggap You) 정회원

- 1975년 8월 : 서강대학교 전자공학과(공학사)
- 1975년 ~ 1979년 : 국방과학연구소 연구원
- 1981년 8월 : Univ. of Michigan, Ann Arbor 전기전산학과(공학석사)
- 1986년 4월 : Univ. of Michigan, Ann Arbor 전기전산학과(공학 박사)
- 1986년 ~ 1988년 : 금성반도체(주) 책임 연구원
- 1993년 ~ 1994년 : 아리조나 대학교 객원 교수
- 2000년 ~ 2001년 : 오레곤 주립대학교 교환교수
- 2007년 ~ 2008년 : 일리노이 주립대 객원 역구원
- 1988년 ~ 현재 : 충북대학교 정보통신공학과 교수

<관심분야> : VLSI 설계 및 Test, 고속 인쇄회로 설계, Cryptography

박 래 현(Raehyeon Park) 준회원

- 2007년 2월 : 충북대학교 정보통신 공학과(공학사)
- 2007년 3월 ~ 현재 : 충북대학교 정보통신 공학과 석사과정

<관심분야> : 암호, 직접회로, 패키지

안 영 일(Youngil Ahn) 준회원

- 2006년 2월 : 한밭대학교 전자 공학과 (공학사)
- 2008년 8월 : 충북대학교 정보통신 공학과 (공학석사)

<관심분야> : 암호, 직접회로, 패키지

김한벼리(Hanbyeori Kim) **준회원**

- 2008년 2월 : 충북대학교 전자 공학과(공학사)
- 2008년 3월 ~ 현재 : 충북대학교 정보통신 공학과 석사 과정

<관심분야> : 암호, 직접회로, 패키지