다중 블럭 암호 알고리즘을 이용한 에러분산

백 창현, 김 춘수°

한국전자통신연구소

The Error Distribution Using Multiple Block Cipher Algorithm

Chang-Hyun Paek, Choon-Soo Kim

Electronics and Telecommunications Research Institute

요 약 문

본 논문에서는 자동 동기 블럭 암호 시스템에서 발생하는 에러 전파 현상으로 인하여 파생되는 문제를 경감하기 위하여, 다중 암호 알고리즘을 이용한 병렬처리 자동 동기 블럭 암호 시스템을 제안하였다. 제안된 구조는 암호 알고리즘 출력속도를 높일수 있을 뿐만 아니라, 에러전파로 파생된 블럭 단위의 연속적인 에러를 여러 채널로 분산시키는 특성이 있다. 이를 설명하기 위하여 CFB 모드에 적용하여 특성을 분석하였고, 응용 가능성이 높은 분야에 대하여 기술하였다.

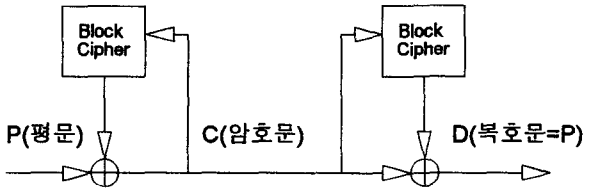
1. 서론

자동 동기 구조를 가지고 있는 Feedback 블럭 암호 시스템은 자동 동기 유지에 대한 뛰어난 특성 때문에 널리 사용하고 있으며, 특히 암호 동기를 위한 Redundancy가 없는 곳에서의 사용이 빈번하다. 그러나 에러 전파(Error Propagation)현상으로 인하여, 특정 구간에서는 이를 사용할 수가 없다. 자동 동기 블럭 암호 시스템의 특성으로 인하여 발생하는 에러 전파 현상에 대한 문제점은 크게 두 가지로 분류할 수 있다[1]. 첫째는 BER(Bit Error Rate) 저하에 따른 데이타 인식에 대한 문제점이고, 둘째는 블럭 에러(Moderate Burst Error) 자체가 가지는 문제점이다. BER 저하를 수용할 수 없는 데이타 링크도 있고 블럭 에러로 인하여 동기 프로토콜이나 선로 동기용 프레임에 심각한 영향을 주어 동기를 상실하는 데이타 링크도 있다. 또한 EDC(Error Detection & Correction) 장치를 사용하는 데이타 링크에 자동 동기 블럭 암호 시스템을 사용할 경우, 에러 전파 현상에 의한 블럭 에러는 EDC 장치를 무용지물로 만들어 버리는 치명적인 결과를 초래할 수도 있다. 본 논문에서는 두 번째 경우, 즉 블럭 에러로 인하여 발생할 수 있는 문제를 해결하기 위하여 다중 암호 알고리즘을 이용한 병렬처리 자동 동기 블럭 암호 시스템을 제안하였다. 블럭 에러에 의하여 동기 데이타 링크의 동기가 상실되는 경우는 유/무선 전송로 상에서 매우 다양하게 실재한다. 특히 무선 전송로에서는 다양한 EDC 장치가 사용되고 있다. 또한 각종 정보산업의 발전과 더불어 정보 보호에 대한 중요성이 더욱더 강조되고 있는 가운데 종전과는 달리 암/복호화기의 사용이 전송구간에서만 제한되고 있지 않고 그 영역이 날로 확산되고 있다[2]. 예를 들면, 인접 시스템간의 데이타 링크나, 한 시스템 안에서 유니트간 연결된 데이타 버스 등 외부로 노출되기 쉬운 곳에서 정보 보호 장치

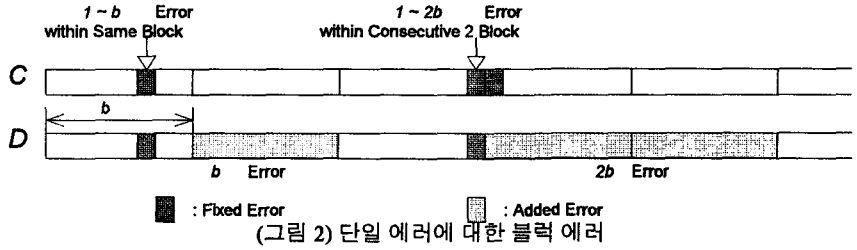
의 필요성이 한층 높아지고 있으며, 심지어 동일 유니트 안에서의 Chip 간 연결되는 데이타 버스에서도 정보보호의 필요성이 대두되고 있다. 이러한 데이터 링크 또는 데이타 Path 에서는 EDC 장치를 기본적으로 사용하고 있는 경우가 많다. 이러한 이유로 본 논문에서 제안한 에러 분산 구조는 상기에서 기술한 분야에서 매우 유용하게 활용될 수 있다[3][4].

2. 블럭 암호 시스템의 에러 전파

(그림 1)는 대표적인 자동동기 암호 장치의 예로서, 블럭 암호 알고리즘을 사용한 CFB(Cipher Feedback) 구조이다. 평문(P:Plain Text)이 블럭 암호 알고리즘의 출력 수열과 Bit-by-bit Exclusive OR되어 암호문(C:Cipher Text)으로 바뀌고, 수신측의 블럭 암호 알고리즘의 출력과 다시 Bit-by-bit Exclusive OR되어 복호문(D:Decipher Text = Plain Text)으로 환원된다. 이 과정에서 특정 크기의 암호문(Block Size = b)이 암호 알고리즘 동기유지를 위하여 블럭 암호기에 피드백 된다. 자동동기 암호 장치로는 블럭 암호 알고리즘을 이용하는 방법과 스트림 암호 알고리즘을 이용하는 방법이 있다. 이와 같은 구조는 암호 알고리즘의 자동동기가 가능하기 때문에 동기 유지를 위한 별도의 암호 알고리즘 동기 프로토콜이나 동기용 Redundancy가 필요 없는 자동동기 암호 장치이다[5]. 이런 이유로 여러 분야에서 응용되고 있다. 그러나 이와 같은 구조를 채택한 암호 장치는 에러 전파 현상을 필연적으로 수반한다. 자동 동기 블럭 암호 장치의 에러 전파 현상은 (그림 2)와 같이 발생한다. 만약 피드백 되는 암호문(수신측: 전송도중 에러 발생)에 에러가 있다면 연속되는 암호기의 출력에 블럭 크기만큼 에러가 전파되어 복호화된 데이타에 블럭 크기만큼의 에러가 발생한다. 즉, 블럭 크기 b 보다 작거나 같은 에러가 동일 블럭 안에서 발생한다면, 연속되는 블럭에 최대 b 에러를 전파시킨다. 추가 되는 블럭 에러는 50% 확률로 발생한다. 즉, 전파된 에러의 크기는 $1 \sim b$ (평균 $b/2$) 만큼 추가된다. 그러나 단순히 평균 BER($b/2$)의 증가만을 고려하기 어려우며, 대부분의 경우 최대 BER(b) 증가를 고려해야 하며, 에러에 대한 에러전파의 크기는 블럭의 크기에 비례하기 때문에, 블럭의 크기가 커지면 단순한 BER 증가 이외에도 Burst 에러에 대한 영향을 고려해야 한다[6].



(그림 1) CFB 모드



(그림 2) 단일 에러에 대한 블럭 에러

3. 다중 암호 알고리즘을 이용한 블럭 암호 시스템

본 장에서는 자동 동기 구조를 채택한 블럭 암호 시스템의 블럭 단위 에러를 단일 에러로 여러 채널에 분산시키는 방법과 그 구조를 제안하고, 이를 CFB 모드에 적용하여 설명한다.

1) 다중 알고리즘 구조

(그림 3)은 다중 알고리즘을 이용한 에러 분산 구조를 CFB에 적용하여 나타낸 것과 같이 여러 개의 알고리즘을 사용하여 평문을 처리하는 방법이다. 즉, 블럭의 크기가 같은 n개의 블럭암호알고리즘을 병렬로 연결한 구조이며, 각각의 암호알고리즘 동기를 위하여 암호문을 S/P Conversion하여 Feedback된다. P/S Converter는 각 알고리즘의 키 수열을 다중화하여 평문(P)의 속도와 정합시킨다. 다중 알고리즘 구조는 암호 알고리즘의 출력 속도, 비도 측면의 개선 효과등 여러 각도에서 분석 및 결과가 제시 될 수 있으나, 본 논문에서는 에러 분산 특성에 대하여만 기술한다.

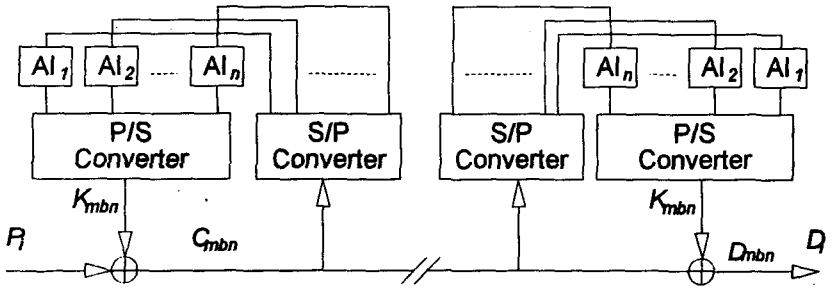


그림 3. 다중 알고리즘 구조

2) 에러분산과정

(그림 3)에 나타낸 다중 알고리즘 구조의 데이타 흐름을 매트릭스로 표현하여 설명하기 위하여, 블럭의 크기를 b(열), 임의의 알고리즘의 갯수를 n (행)이라 하고 다중화하여 출력되는 키 수열을 K_{ij}로 표시하면, bxn 크기의 키 수열을 식(1)과 같이 b by n 매트릭스 구조로 나타낼 수 있다.

$$K_{ij} = \begin{bmatrix} K_{11} & K_{12} & \cdot & \cdot & K_{1n} \\ K_{21} & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ K_{b1} & \cdot & \cdot & \cdot & K_{bn} \end{bmatrix} \quad (1)$$

식(1)의 출력 순서는

for $i = 1$ to b (for $j = 1$ to n (K_{ij}))

이다.

또한 평문(P)과 키 수열을 Bit-by-bit Exclusive OR하여 생성된 암호문도 C_{ij}로 표시하면 식(2)와 같이 나타낼 수 있다.

$$C_{ij} = \begin{bmatrix} C_{11} & C_{12} & \cdot & \cdot & C_{1n} \\ C_{21} & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ C_{b1} & \cdot & \cdot & \cdot & C_{bn} \end{bmatrix} \qquad (2)$$

이 되고, 출력 수열은

for $i = 1$ to b (for $j = 1$ to n (C_{ij}))

와 같으며, C_{ij}는 전송링크를 통하여 수신단에 전달된다.

식(2)에서 각 열은 동일 알고리즘에서 출력되는 키 수열이다. 따라서 임의의 열에서의 에러는 다음번 매트릭스의 동일 열 전체로 전파된다. 이를 설명하기 위하여 암호문의 수열을 일반화 하면 C_{xyz}로 표현할 수 있고 그 출력 수열은 다음가 같이 표현할 수 있다.

for $x = 1$ to m (for $y = 1$ to b (for $z = 1$ to n C_{xyz})) 단 $m = 1,2,3.....$: 매트릭스 출력 번호

(그림 4)는단일 에러가 그 다음 블럭에 전파되는 것을 (그림) 나타내었다.

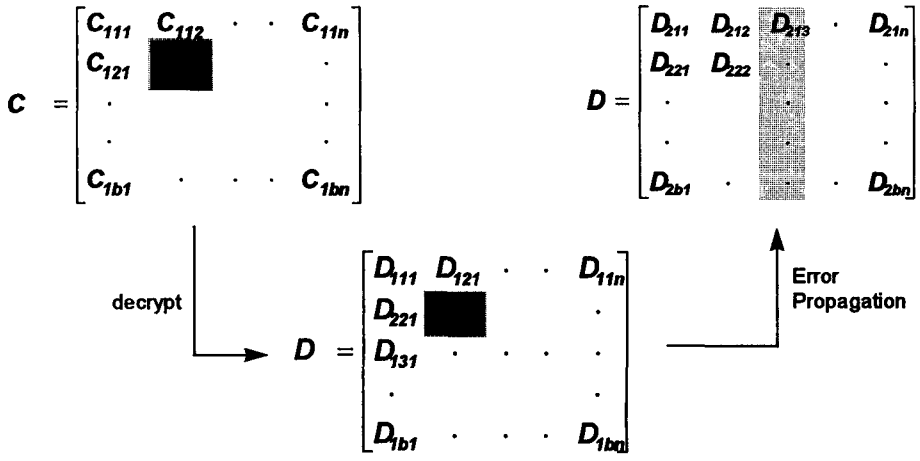


그림 4. 에러 전파 현상

암호화 출력 수열은 b by n 매트릭스 구조이고 , 각 알고리즘의 출력은 매 n Bit 를 주기로 동기되기 때문에 단일 에러에 의하여 추가되는 블럭 에러는 n을 주기로 분산된다. 이를 도식적으로 표현하면 (그림

5)와 같이 되며 D_{mbn}은 출력 수열은 C_{mbn} 출력 수열과 대응되는 수열을 표시하기 위하여 표현한 것이다.

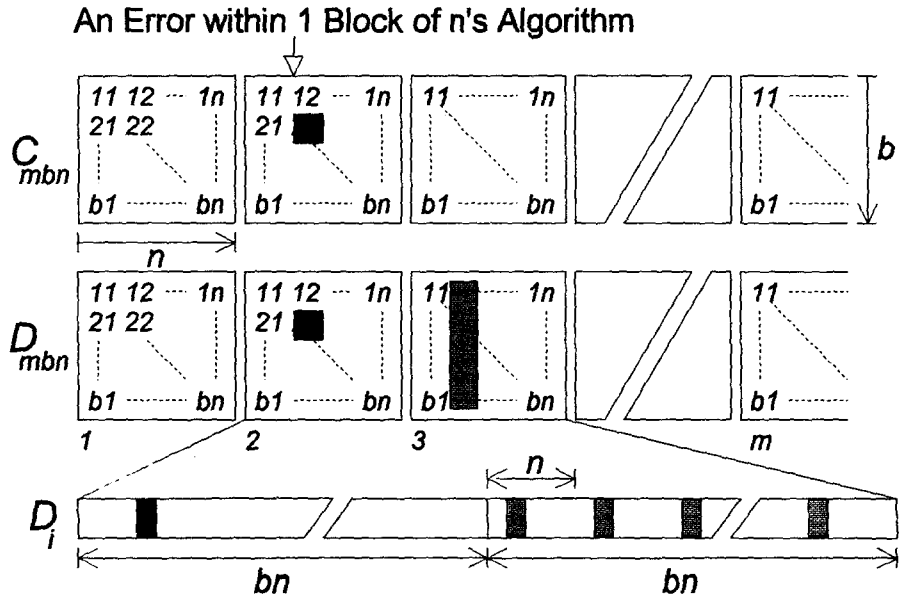


그림 5. 다중 알고리즘 구조에서의 에러 분산

4. 블럭 암호 시스템의 에러 분산 응용

상기에서 기술한 구조의 블럭 암호 시스템은 Burst Error 발생시 b x n Bit이 손실되기 때문에 Burst Error의 확률이 거의 존재하지 않는 데이타 링크에 적합하다. 그러나 이러한 제약 조건에도 불구하고 본 논문에서 제안한 구조의 암호시스템은 여러 가지의 장점이 있기 때문에 적용 가능성이 매우 높다. 에러를 분산을 목적으로 했을 때 에는 다음과 같은 데이타 링크에서 사용하였을 때 그 실용성이 높다.

1) 에러 교정이 가능한 데이타 링크에 삽입되는 경우

특정 구간의 정보 보호를 목적으로 사용하는 경우, 암/복호화기는 기존의 데이타 처리 장치에 부수적으로 삽입되어 사용하는 경우가 많다. 이 구간에서 EDC 장치를 사용한다면 그 장비의 내부에 있는 EDC 전단에 암/복호화기를 설치하기는 어려울 뿐만 아니라 암/복호화기의 특성상 단독으로 관리되는 경우가 많다. 물론 가능하다면 EDC장치를 암/복호화기 사이에 설치하는 것이 더욱 효율적이다. 자동 동기 블럭 암호 시스템을 EDC장치가 설치되어 있는 곳에 사용한다면, EDC 기능이 완전히 상실된다. 그러나 EDC를 사용하고 있는 구간에 본 논문에서 제안한 에러 분산 구조의 블럭 암호 시스템을 사용한다면 에러 전파 현상을 최소화 할 수 있다. 이때 알고리즘의 갯수를 Codeword 의 크기와 일치시키면 더욱 효율적이며, 특히 1 Bit 에러 교정 EDC를 채택한 링크에서는 다중 알고리즘 에러 분산 구조가 적합하다.

2) 다중 Bit 에러 교정이 가능한 데이타 링크

서론에서 언급한 바와 같이 정보 보호의 분야는 더 이상 전송로에만 국한되지 않는다. 특히 대용량 저장 시스템에서의 Data Bus, 근거리 LAN에서의 정보보호는 그 필요성이 점차 증대되고 있다. 또한 높은 신뢰도를 요구하는 시스템에서는 다중 Bit 에러 교정이 기능이 필수적이다. 이런 구간에서는 단일 알고리즘 에러 분산 구조가 적합하며, (그림6)에서 나타낸 것과 같이 1 Bit 에러뿐만 아니라 연속적인 블럭 에러도 교정할 수 있다. EDC 장치가 n Bit 에러를 교정할 수 있다면, 에러 분산 구조에서는 nb 크기의 연속적인 블럭 에러(Burst Error)의 교정이 가능하다.

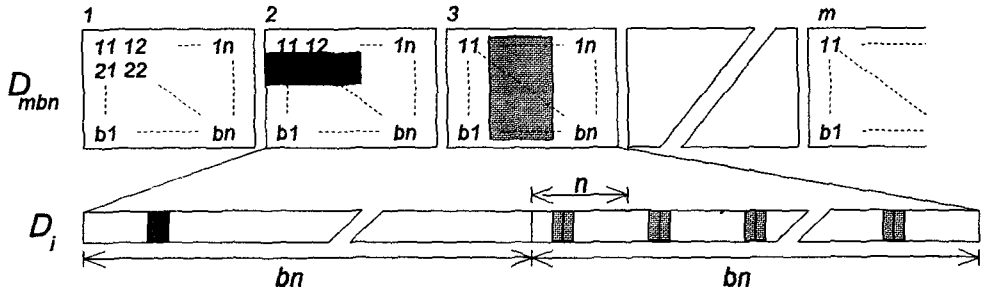


그림6. 연속적인 블럭 에러 분산

3) 블럭 에러를 수용하지 못하는 데이타 링크

블럭 에러는 일종의 Burst 에러 특성을 가지며, 특히 블럭 크기가 클수록 Burst Error에 가깝게 된다. 블럭 에러로 인하여 데이터 링크의 동기가 상실되거나 데이타 서비스에 심각한 문제를 초래할 수도 있다. 특히 연속되는 n 개의 블럭에서의 분산되어 발생하는 단일 Bit 에러는 데이타 서비스를 순간적으로 중시 시킬 수도 있으며, 블럭의 크기가 큰 블럭 암호 시스템을 사용 또한 동일한 결과를 초래한다. 블럭 에러는 $1 \sim b$ (평균 $b/2$)에러 단순히 추가한다. 그러나 데이타 링크의 특성으로 볼 때, 에러로 처리해야 하는 블럭의 크기는$b/2$ 보다는 크며, 항상 b 인 경우도 있다. 에러를 분산 시켰을 때는 동일 블럭 안의 1 Bit 에러에 대하여 평균 $b/2$ 배의 단순 에러 증가만을 고려하면 되므로, 본 논문에서 제안한 다중 블럭 암호 알고리즘을 적용하면 블럭 에러로 인하여 생기는 문제를 해결할 수 있다.

5. 결론

본 논문에서 제안한 에러 분산 구조는 자동 동기 블럭 암호 시스템의 에러 전파 현상에 대한 대책으로서, 다중 블럭 암호 알고리즘을 이용한 병렬처리 자동 동기 블럭 암호 시스템을 제시하였으며, 그 구조와 특성을 CFB 모드에 적용하여 설명하였다. 또한 블럭 에러에 취약한 데이타 링크중 세 가지 분야에 적용한 결과와 문제점을 기술하였다. 예를 든 세 가지 분야에 현실적인 응용이 가능하다는 것과 특히 다중 Bit 에러 교정 기능을 지원하는 데이타 링크에서의 유용성이 매우 크다는 것을 보여주었다. 본 논문에서는 자동 동기 암호 시스템중 대표적인 CFB 모드에서만 적용하였으나, 다른 자동 동기 모드에서도 적용이 가능하리라 생각하며, 본 논문에서 제안한 구조에 대한 최적 적용 분야 발굴에 대한 연구가 필요하며, 향후 보다 효율적이고 완벽한 에러 분산 구조에 대한 연구가 요구된다.

참고문헌

[1] Lars Ramkilde Knudsen, *Block Cipher- Analysis, Design and Applications, DAIMI PB, Denmark,* pp.13-21, 1994.

[2] G. Robert Redinbo, Leonard M. Napolitano, Jr., and David D. Andaleon, "Multibit correcting data interface for fault-tolerant systems," *IEEE Trans, Comput.*, vol. C-42, pp. 433-446,1993.

[3] Richard W. Hamming, *Coding and Information Theory, PRENTICE-HALL, Englewood,* pp. 138-148, 1986.

[4] C S Kim, J W Han, H S Lee, E S Kim, H J Jun, "The Reliable Data Bus for Fault-Tolerant System," *ISITA '94 Proceedings,* vol.1, pp. 389-394, 1994.

[5] Henry Beker, Fred Piper, *Cipher systems The Protection of Communications, A Wiley-Interscience Publication, New York,* pp. 285-288, 1982.

[6] William Stallings, *Network and Internetwork Security Principles and Practice, PRENTICE-HALL, New York,* pp.45-74, 1995.