제 4장 블록 암호 모드

4.0 주요 내용

- 블록 암호의 **모드**(Mode)에 대해 설명하도록 한다
- 임의의 길이의 평문을 암호화하기 위해서는 평문을 일정한 길이를 갖는 블록으로 나누고 각 블록에 블록 암호를 반복 적용하여 암호화를 할 필요가 있다.
- 블록 암호를 반복하는 방법을 블록 암호의「모드」라고 한다.
- 블록 암호의 주요 모드인 ECB, CBC, CFB, OFB, CTR에 대해서 차례대로 설명하도록 한다.

4.1 블록 암호 모드

- 평문의 길이가 블록 암호의 블록 크기보다 클 경우에는 어떻게 블록 암호를 적용할 것인가?
- 이런 문제점을 해결하고 다양한 응용 환경하에 적절한 암호화 도구로 사용할 수 있는 여러 유형의 효율적인 운영 방식들을 제시하고 있다.
- 이러한 방식들을 블록 암호 모드라고 한다.

4.1.1 블록 암호와 스트림 암호

- **블록 암호**(block cipher)
  - 어느 특정 비트 수의「집합」을 한 번에 처리하는 암호 알고리즘
  - 이「집합」을 **블록**(block)이라고 한다.
  - 블록의 비트 수를 **블록 길이**(block length)라고 한다.
- **스트림 암호**(stream cipher)
  - 데이터의 흐름(스트림)을 순차적으로 처리해 가는 암호 알고리즘
  - 스트림 암호에서는 1비트, 8비트, 혹은 32비트 등의 단위로 암호화와 복호화가 이루어진다.

4.1.2 모드란

- 긴 평문을 암호화하기 위해서는 블록 암호 알고리즘을 반복해서 사용하여 긴 평문 전부를 암호화할 필요가 있다.
- 이와 같이 반복하는 방법을 블록 암호의 **모드**(mode)라고 부른다.

블록 암호의 주요 모드

- ECB 모드 :
  - Electric CodeBook mode(전자 부호표 모드)
- CBC 모드 :
  - Cipher Block Chaining mode(암호 블록 연쇄 모드)
- CFB 모드 :
    - Cipher-FeedBack mode(암호 피드백 모드)
- OFB 모드 :
  - Output-FeedBack mode(출력 피드백 모드)
- CTR 모드 :
  - CounTeR mode(카운터 모드)

4.1.3 평문 블록과 암호문 블록

- **평문 블록**
  - 블록 암호 알고리즘에서 암호화의 대상이 되는 평문을 말한다.
  - 평문 블록의 길이는 블록 암호 알고리즘의 블록 길이와 같다.
- **암호문 블록**
  - 블록 암호 알고리즘을 써서 평문 블록을 암호화한 암호문을 말한다.

평문 블록과 암호문 블록

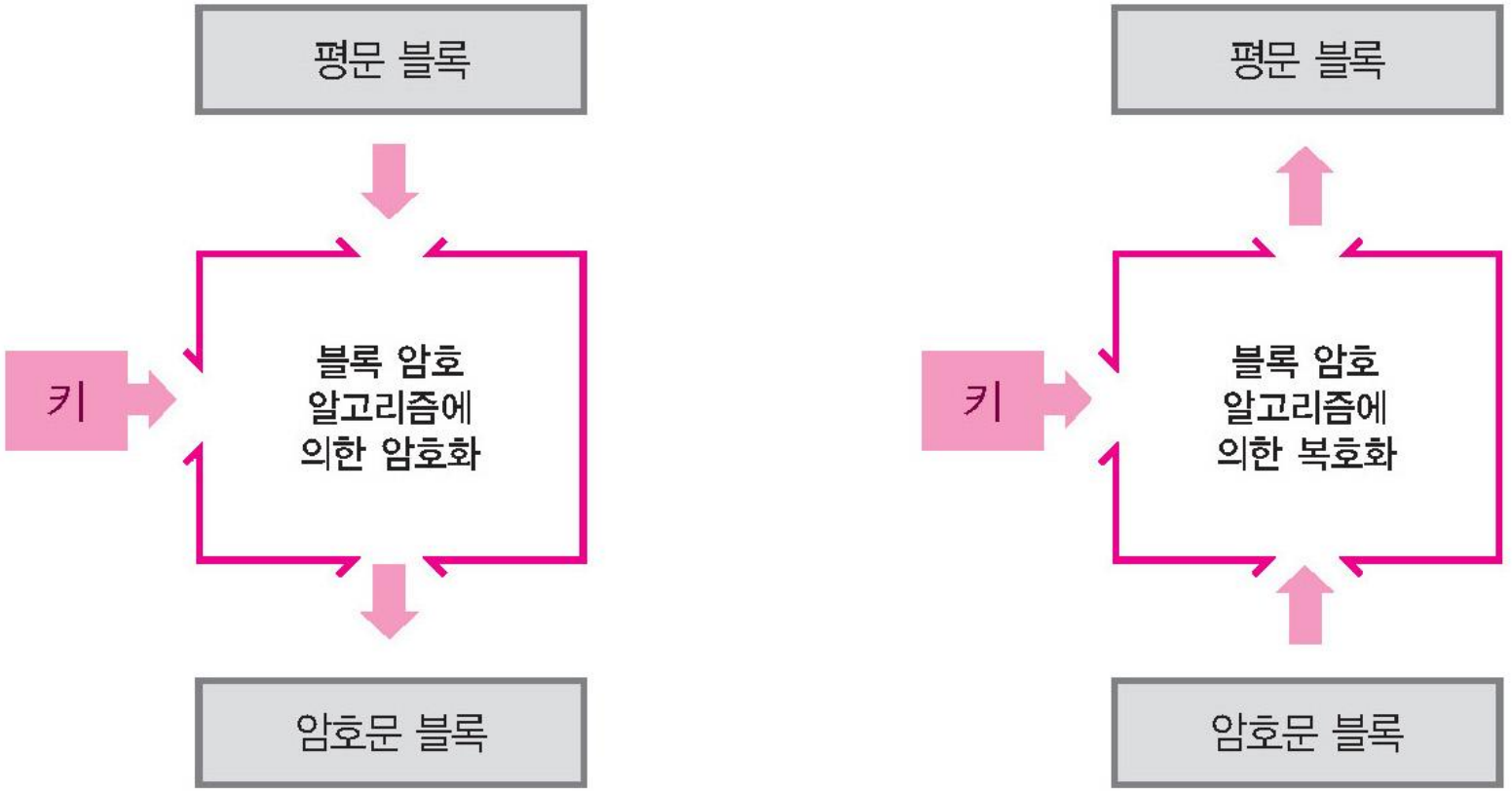


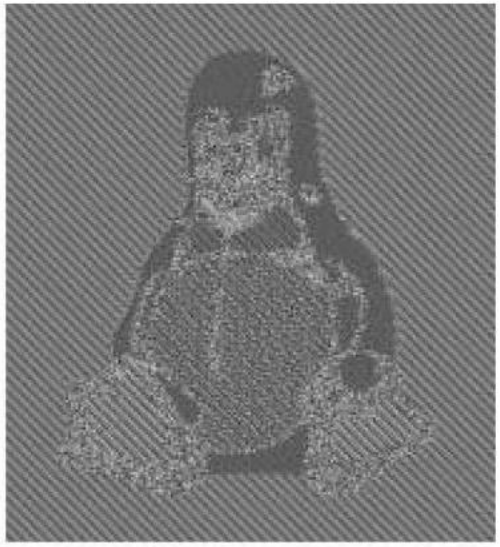
그림 4-1 평문 블록과 암호문 블록

4.2 ECB 모드

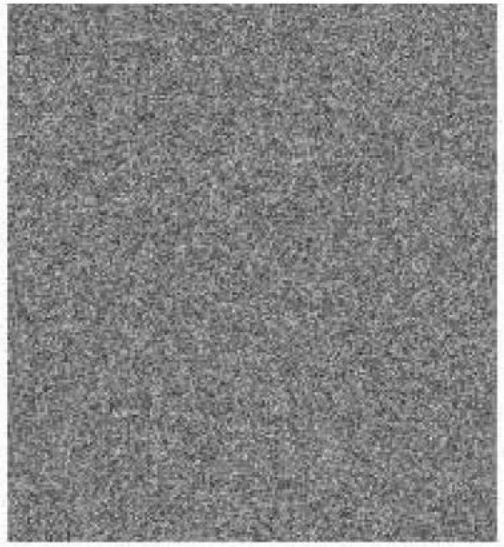
- 평문 블록을 그대로 암호화하는 것이 ECB 모드이다.
- 간단하지만 약점이 있어서 별로 사용되지 않는다.

ECB 모드와 다른 모드의 차이

원자료



ECB 모드를
이용한 암호화



다른 모드를
이용한 암호화

그림 4-2 ECB 모드와 다른 모드의 차이

4.2.1 ECB 모드란

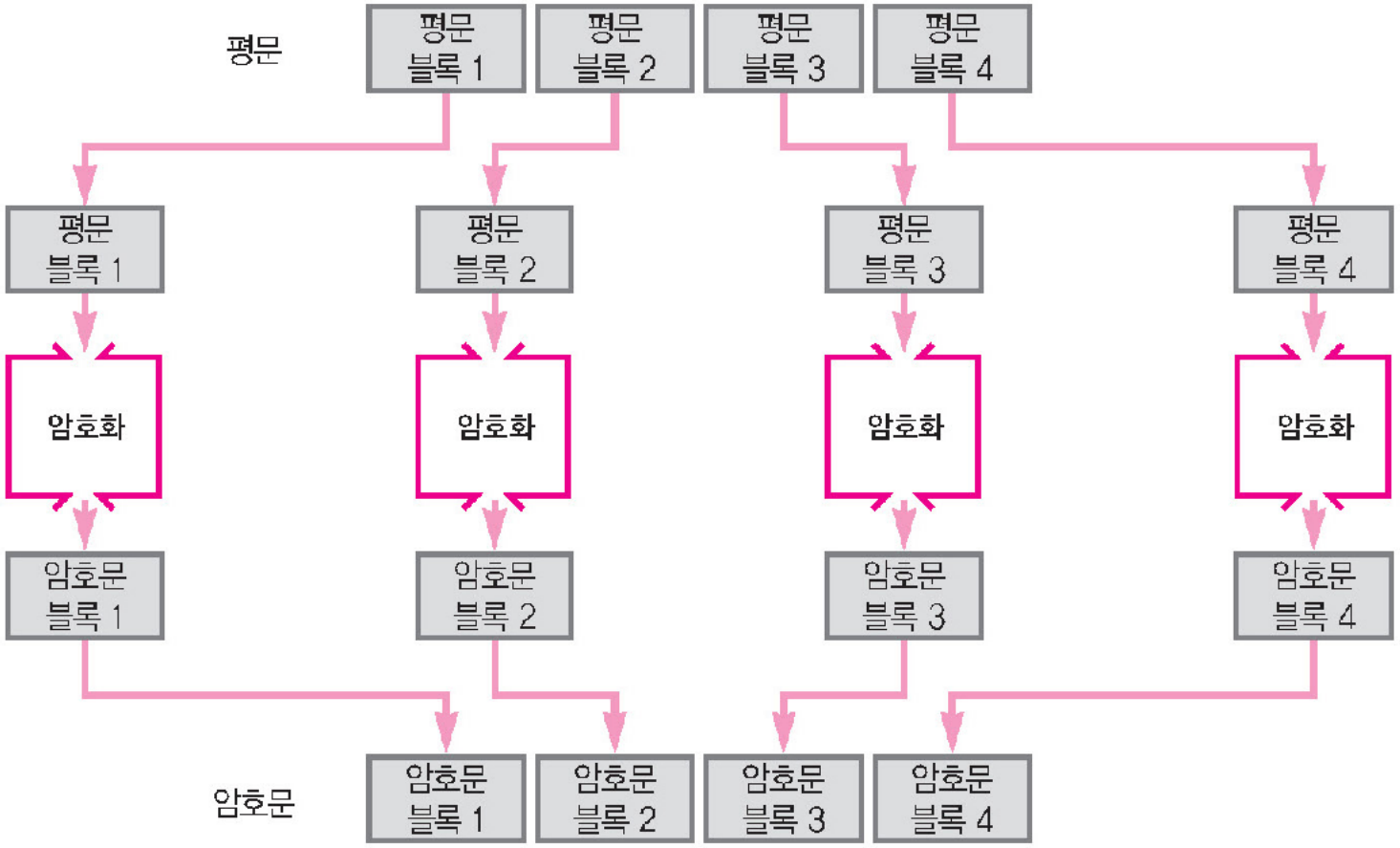
- ECB 모드에서는 평문 블록을 암호화한 것이 그대로 암호문 블록이 된다
- 동일한 내용을 갖는 평문 블록은 이에 대응되는 동일한 암호문 블록으로 변환된다

ECB 모드의 특징

- 가장 간단한 것이다
- 가장 기밀성이 낮은 모드이다.
- ECB 모드에서는 평문 블록과 암호문 블록이 일대일의 관계를 유지하게 된다.
- 암호문을 살펴보는 것만으로도 평문 속에 패턴의 반복이 있다는 것을 알게 되며, 이것을 실마리로 암호 해독을 할 수 있게 된다.
- 이 모드는 안전하지 않다.

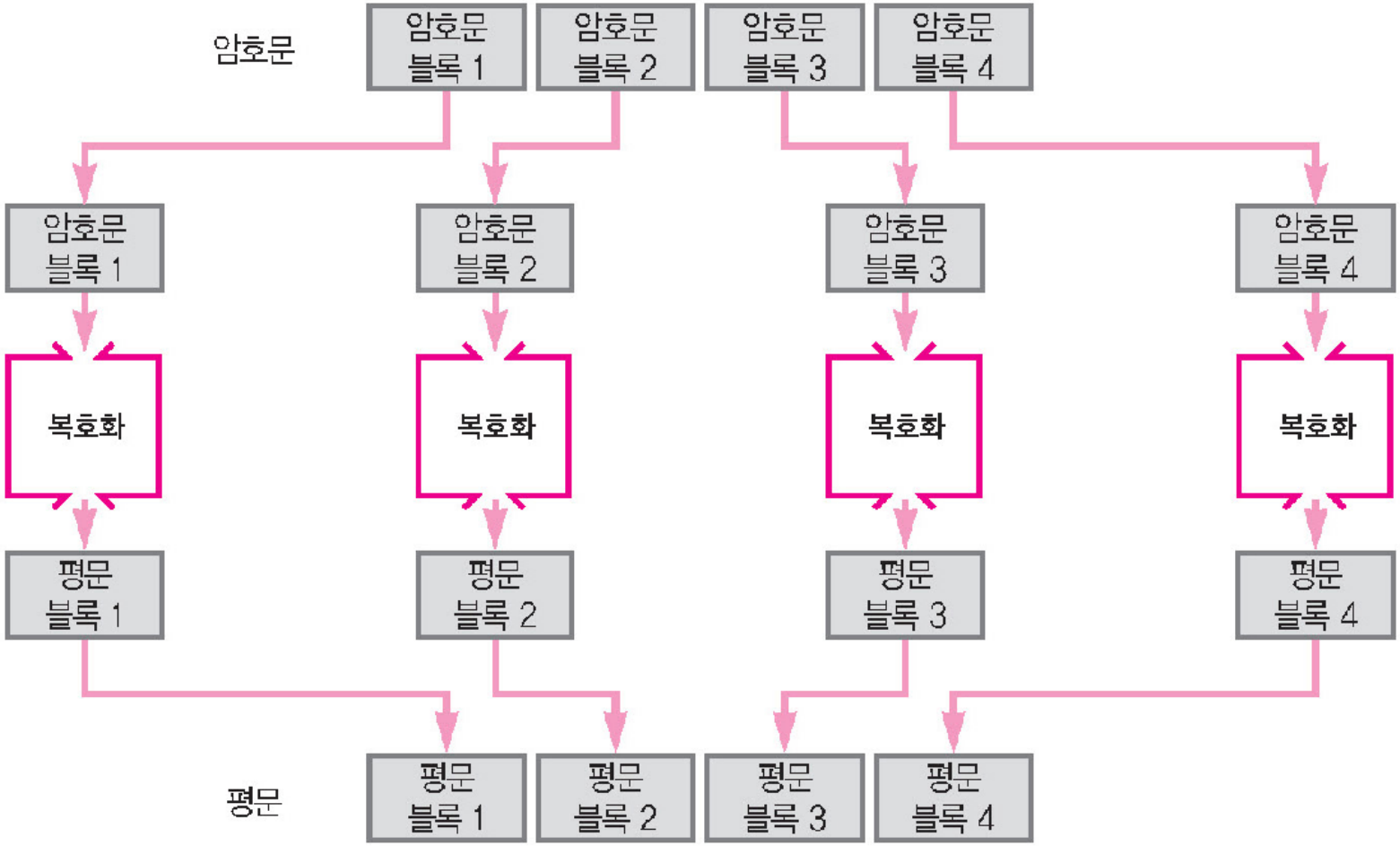
ECB 모드(전자 부호표 모드)

(a) ECB 모드에 의한 암호화



ECB 모드(전자 부호표 모드)

(b) ECB 모드에 의한 복호화



ECB 모드에 대한 공격

- ECB 모드에서는 모든 평문 블록이 각각 개별적으로 암호화되고, 복호화 때에는 개별적으로 복호화된다.
- 적극적 공격자인 맬로리가 악의를 가지고 암호문 블록을 서로 바꾸었다면, 수신자가 그 암호문을 복호화하면 바뀐 암호문 블록에 대응하는 평문 블록도 바뀌게 된다

4.3 CBC 모드

- 블록 암호의 모드로서 다음에 소개하는 것은 CBC 모드이다.
- CBC 모드에서는 1개 앞의 암호문 블록과 평문 블록의 내용을 뒤섞은 다음 암호화를 수행한다.
- 이것으로 ECB 모드의 약점을 회피할 수 있다.

4.3.1 CBC 모드란

- **CBC 모드**는 Cipher Block Chaining 모드(**암호 블록 연쇄 모드**)의 약자이다.
  - 암호문 블록을 마치 체인처럼 연결시키기 때문에 붙여진 이름이다.
- **CBC 모드에서는 1 단계 앞에서 수행되어 결과로 출력된 암호문 블록에 평문 블록을 XOR 하고 나서 암호화를 수행한다**
- 따라서 생성되는 각각의 암호문 블록은 단지 현재 평문블록 뿐만 아니라 그 이전의 평문 블록들의 영향도 받게 된다.

초기화 벡터

- 최초의 평문 블록을 암호화할 때는「1 단계 앞의 암호문 블록」이 존재하지 않으므로 「1단계 앞의 암호문 블록」을 대신할 비트열인 한 개의 블록을 준비할 필요가 있다.
- 이 비트열을 **초기화 벡터(initialization vector)** 또는 앞 글자를 따서 IV라고 부른다.
- 초기화 벡터는 비밀키와 마찬가지로 송신자와 수신자간에 미리 약속되어 있어야 하지만 공개된 값을 사용해도 무방하다.
- 또한 초기화 벡터는 암호화 때마다 다른 랜덤 비트열을 이용하는 것이 보통이다.

패딩

- 실제 CBC 모드를 적용할 경우에 암호화될 평문의 길이는 가변적이기 때문에 마지막 블록이 블록의 길이와 항상 딱 맞아 떨어지지 않게 된다.
- 이 경우에는 부족한 길이만큼을 '0'으로 채우거나 임의의 비트들로 채워 넣는다.

마지막 블록 채우기

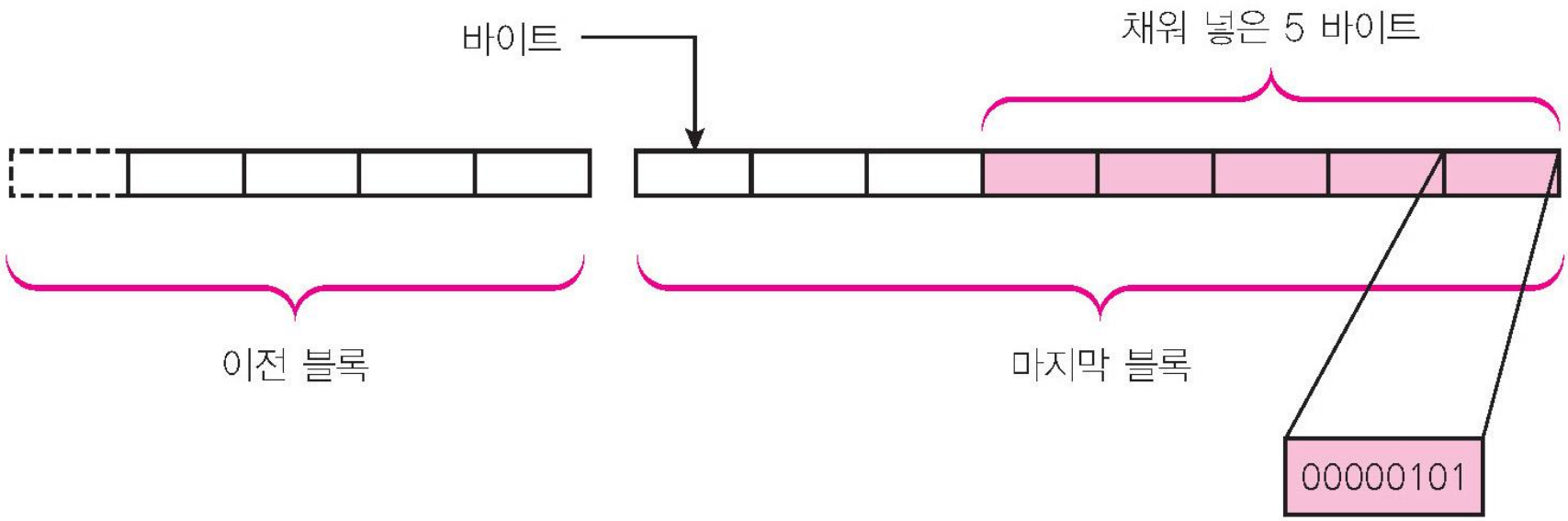
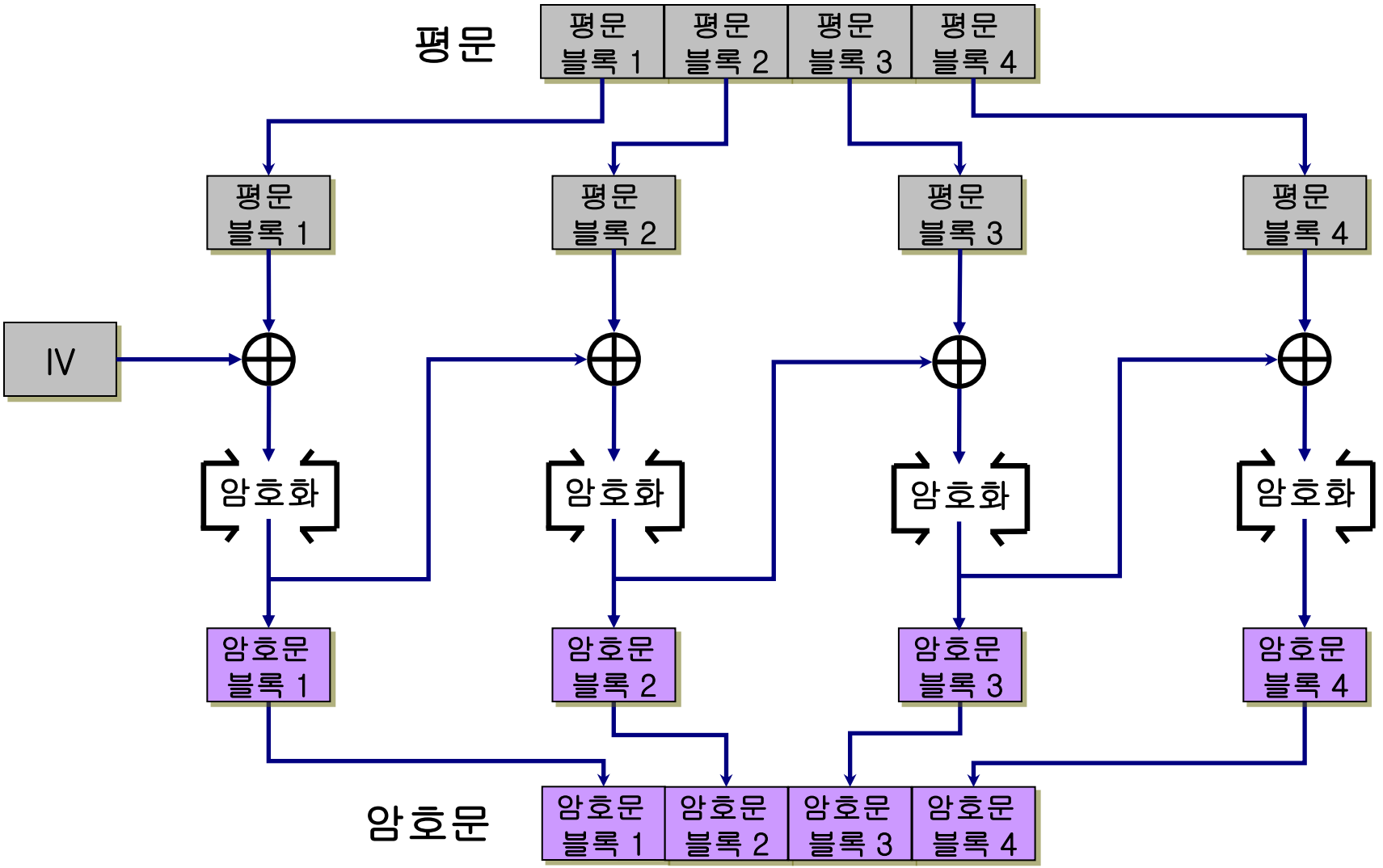
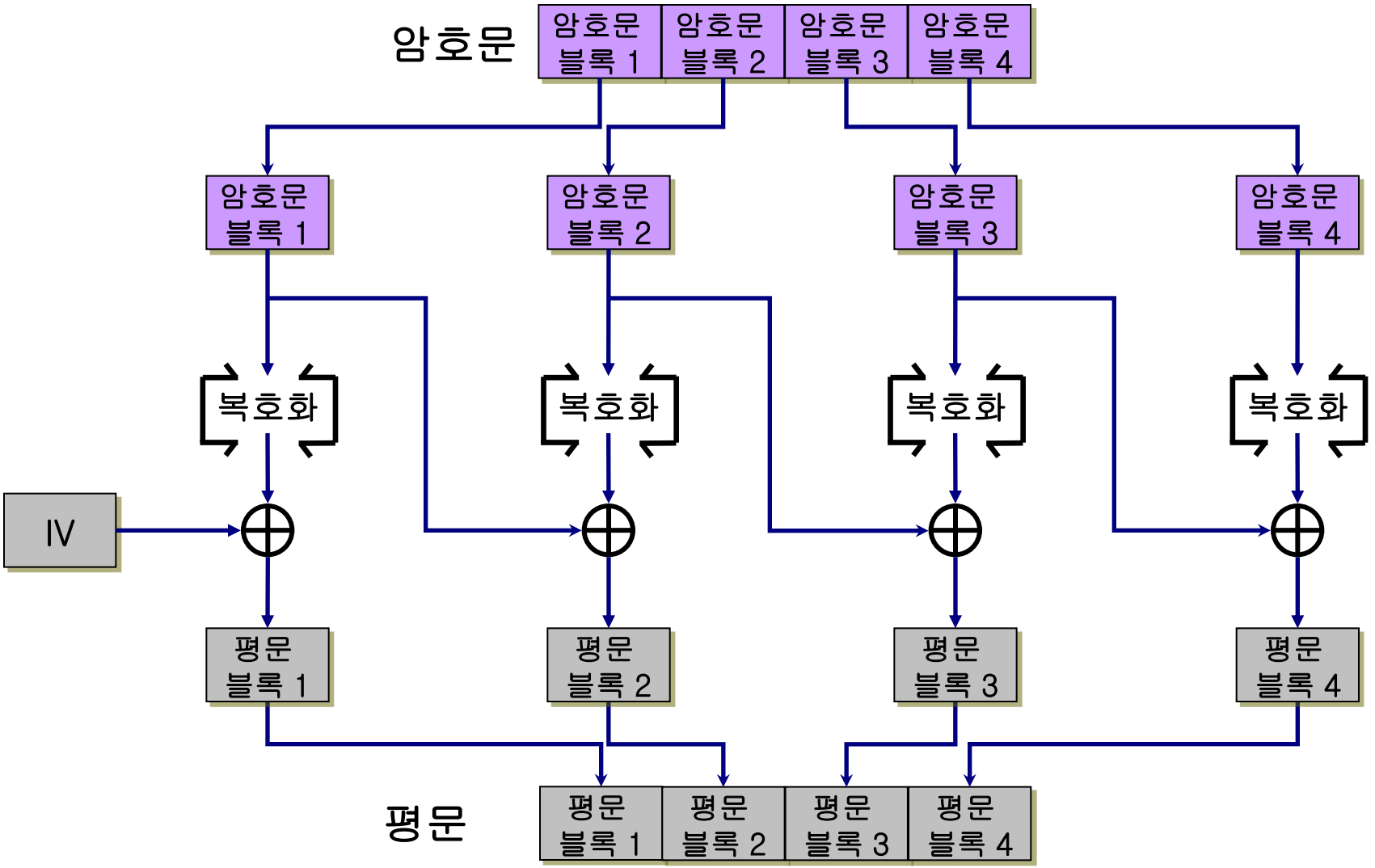


그림 4-4 마지막 블록 채우기

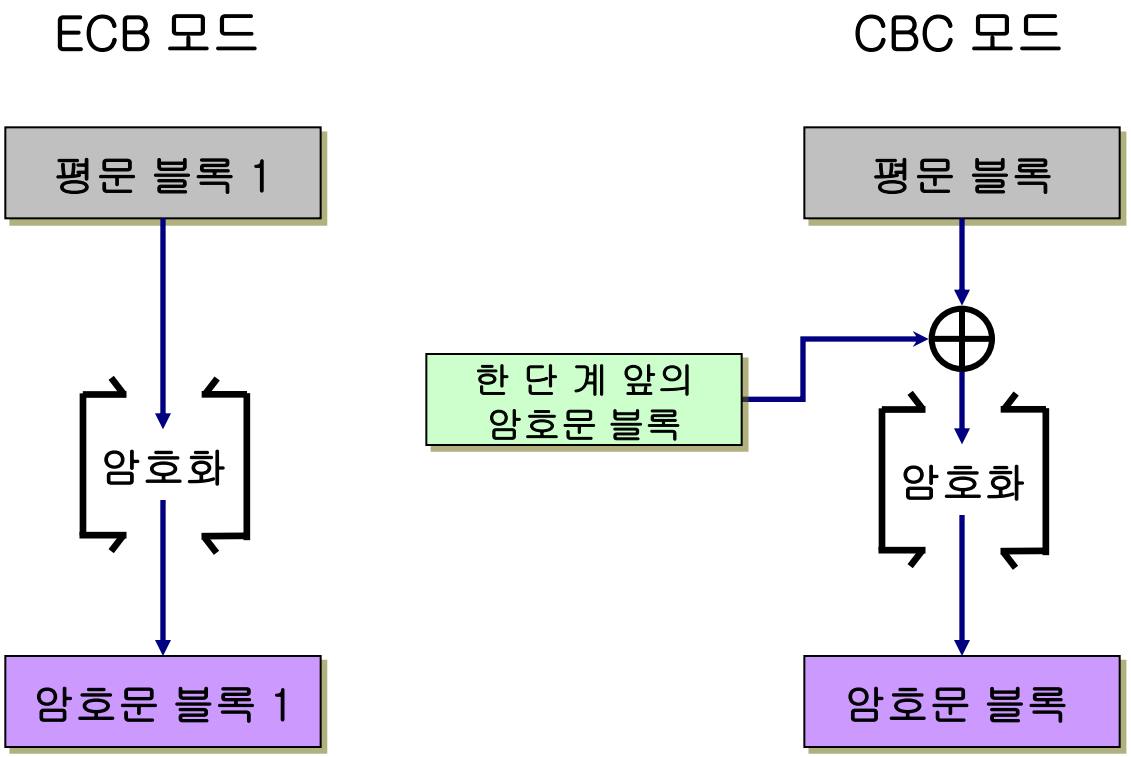
CBC 모드(암호 블록 연쇄 모드)



CBC 모드(암호 블록 연쇄 모드)



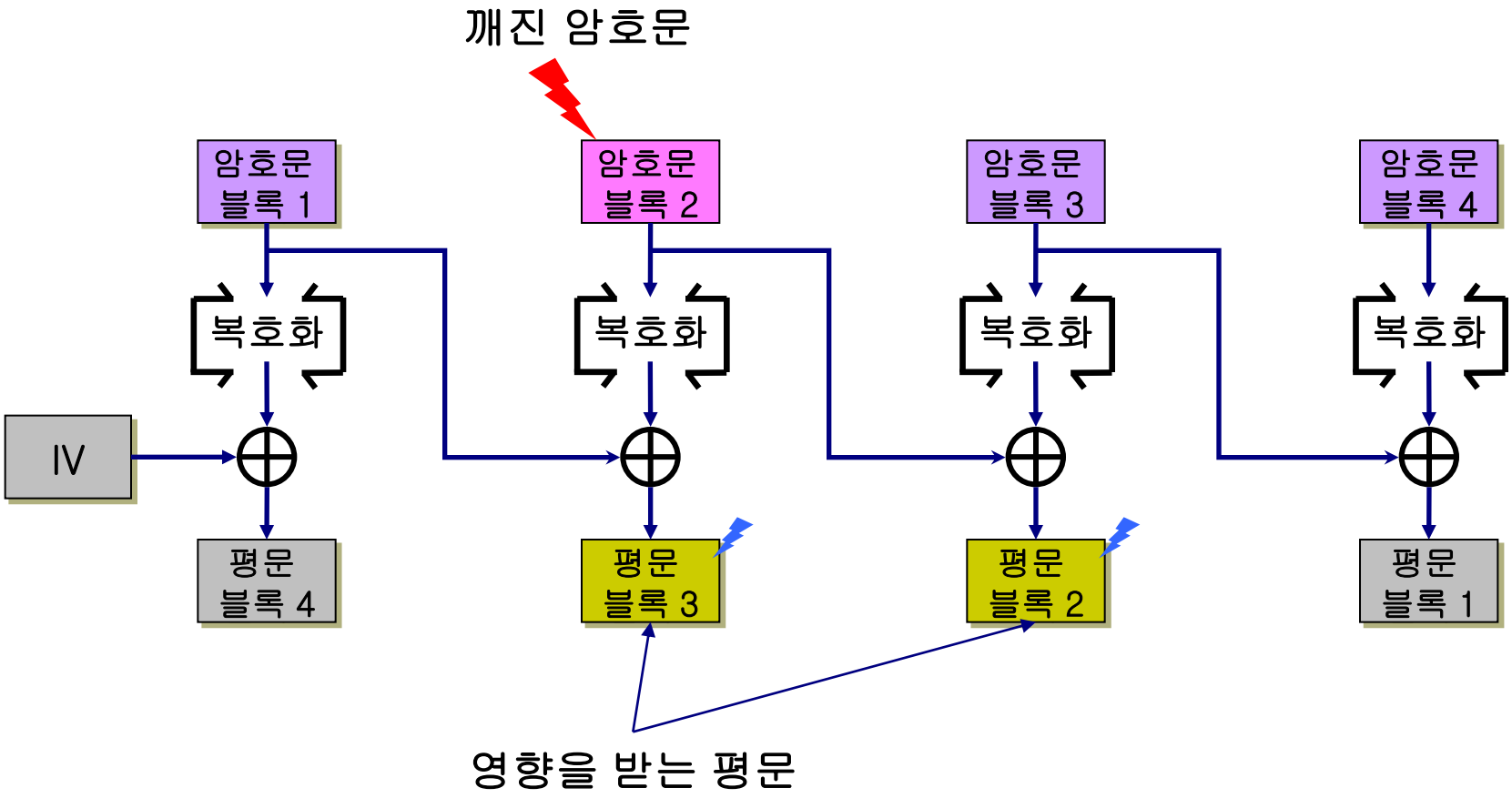
ECB 모드와 CBC 모드의 비교



CBC 모드의 특징

- 평문 블록은 반드시 「1 단계 앞의 암호문 블록」과 XOR을 취하고 나서 암호화된다.
  - 따라서 만약 평문 블록1과 2의 값이 같은 경우라도 암호문 블록1과 2의 값이 같아진다고는 할 수 없다.
  - 따라서 ECB 모드가 갖고 있는 결점이 CBC 모드에는 없다.
- CBC 모드에서는 도중의 평문 블록만을 뽑아내서 암호화할 수는 없다. 암호문 블록3을 만들고 싶다면 적어도 평문 블록의 1, 2, 3까지가 갖추어져 있어야만 한다.
- CBC 모드의 암호문 블록이 1개 파손되었다면, 이 때 암호문 블록의 길이가 바뀌지 않는다면 복호화 했을 때에 평문 블록에 미치는 영향은 2블록에 머문다

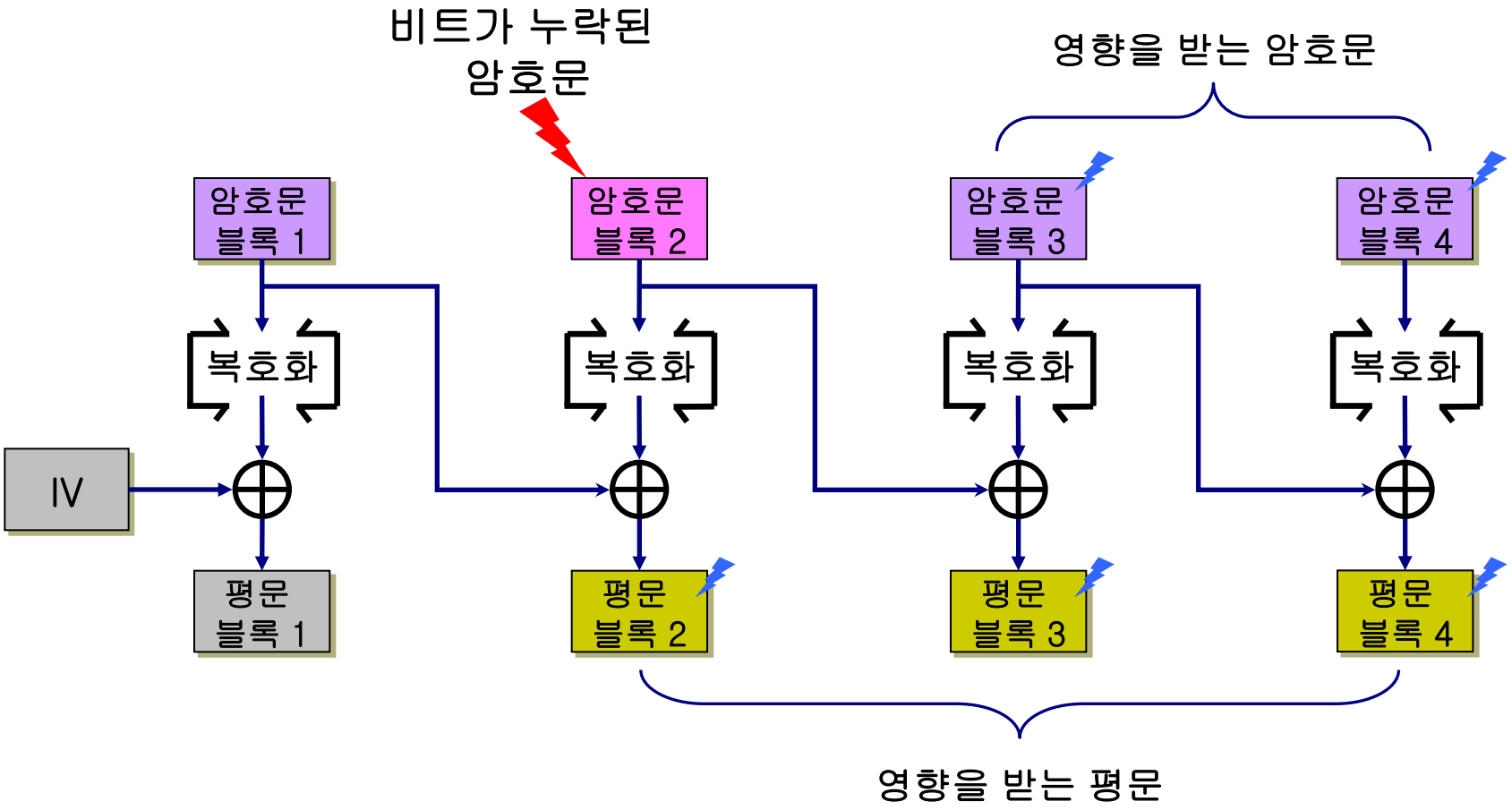
CBC 모드에서 암호문 블록이 파손되면 2개의 평문 블록에 영향을 미친다 __암호문 블록이 파손된 암호문을 복호화한 경우(CBC 모드)



CBC 모드에 대한 공격

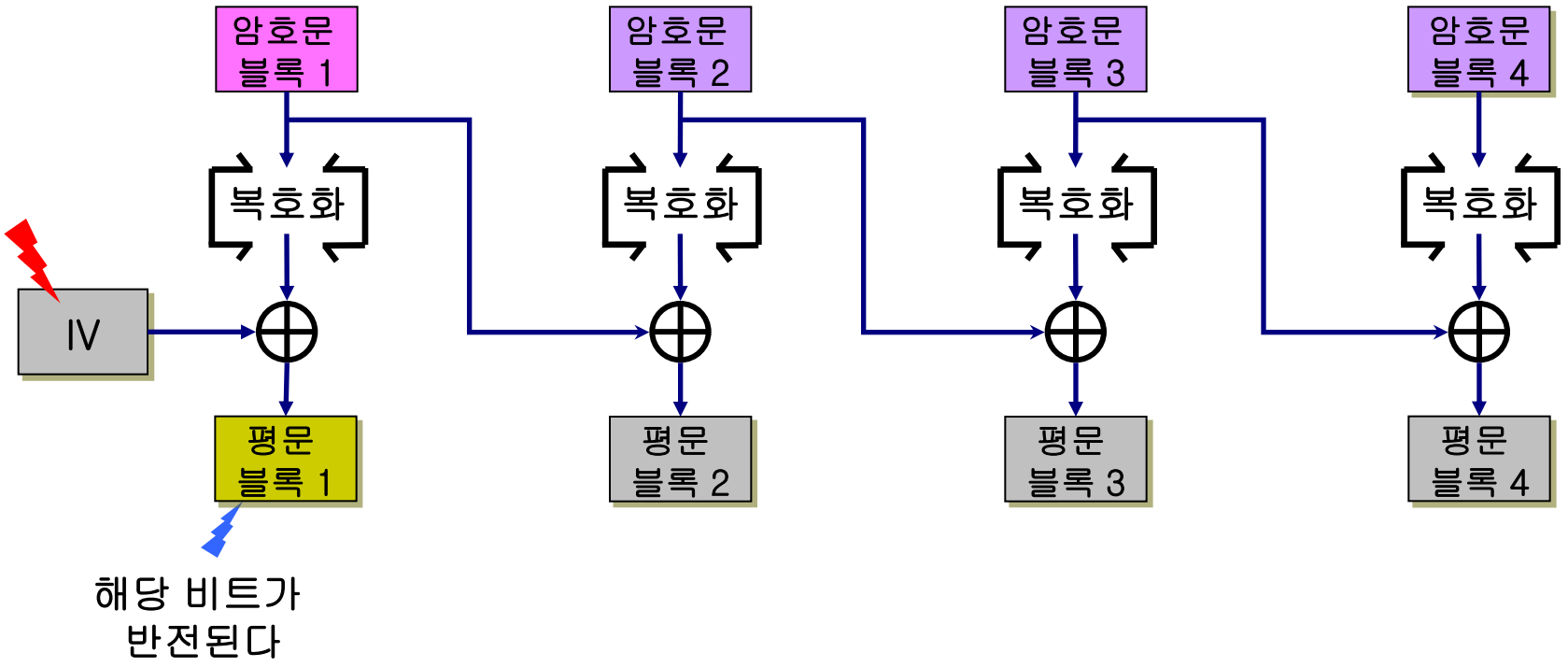
- 적극적 공격자 맬로리가 암호문을 고쳐 써서 수신자가 암호문을 복호화했을 때의 평문을 조작하고 싶어 한다고 해보자.
- 만약 맬로리가 초기화 벡터의 임의의 비트를 반전(1이라면 0, 0이라면 1로)시킬 수 있다면, 암호 블록1에 대응하는 평문 블록1(복호화되어 얻어지는 평문 블록)의 비트를 반전시킬 수 있다.

CBC 모드에서 암호문 블록에서 비트 누락이 생기면 그 이후의 평문 블록 전체에 영향을 미친다

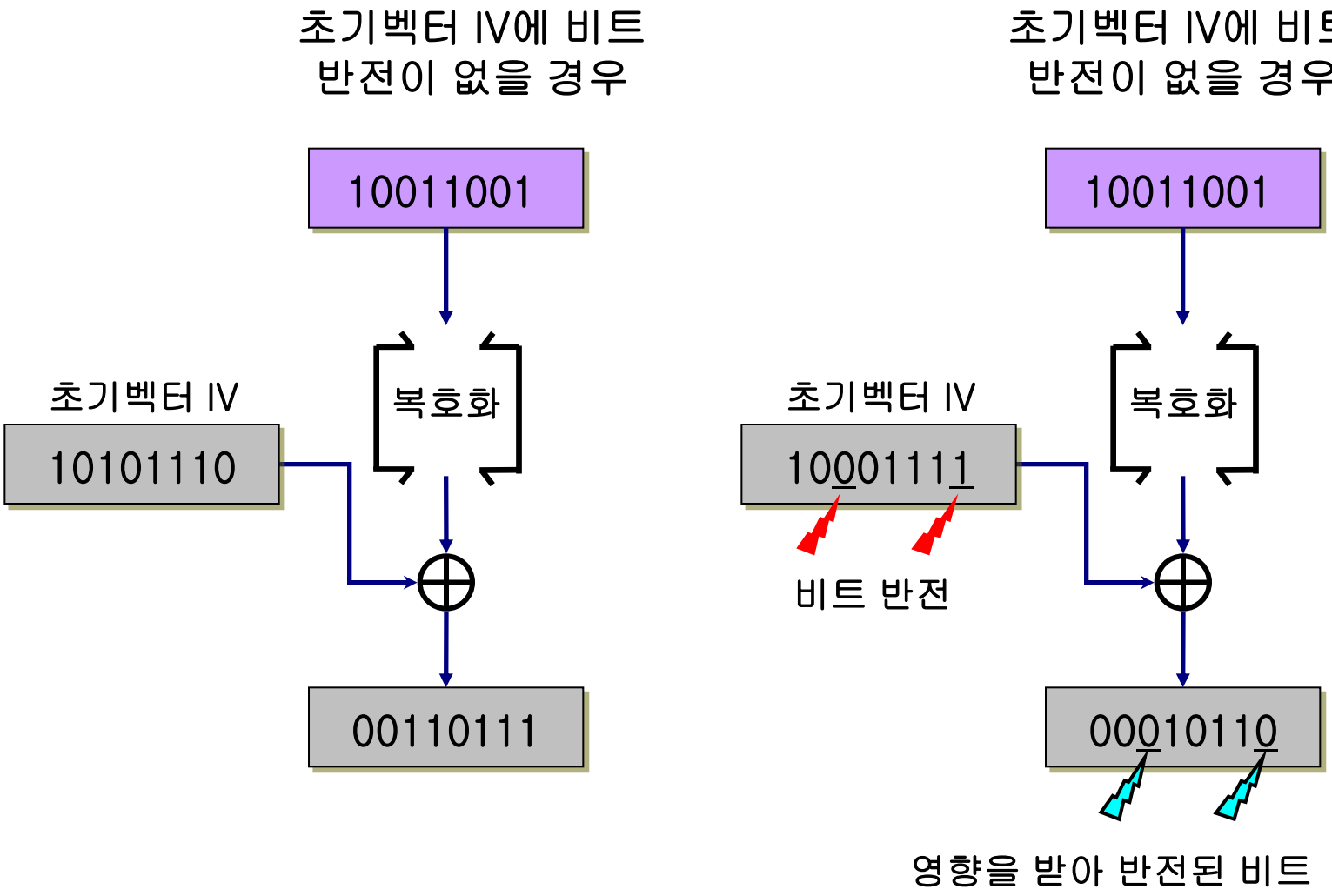


CBC 모드에 대한 공격(초기화 벡터의 비트 반전)

- 초기화 벡터의 비트를 반전시켜 평문 블록의 비트를 반전시키는 공격(CBC 모드)



CBC 모드에서 초기벡터의 비트반전에 대한 영향

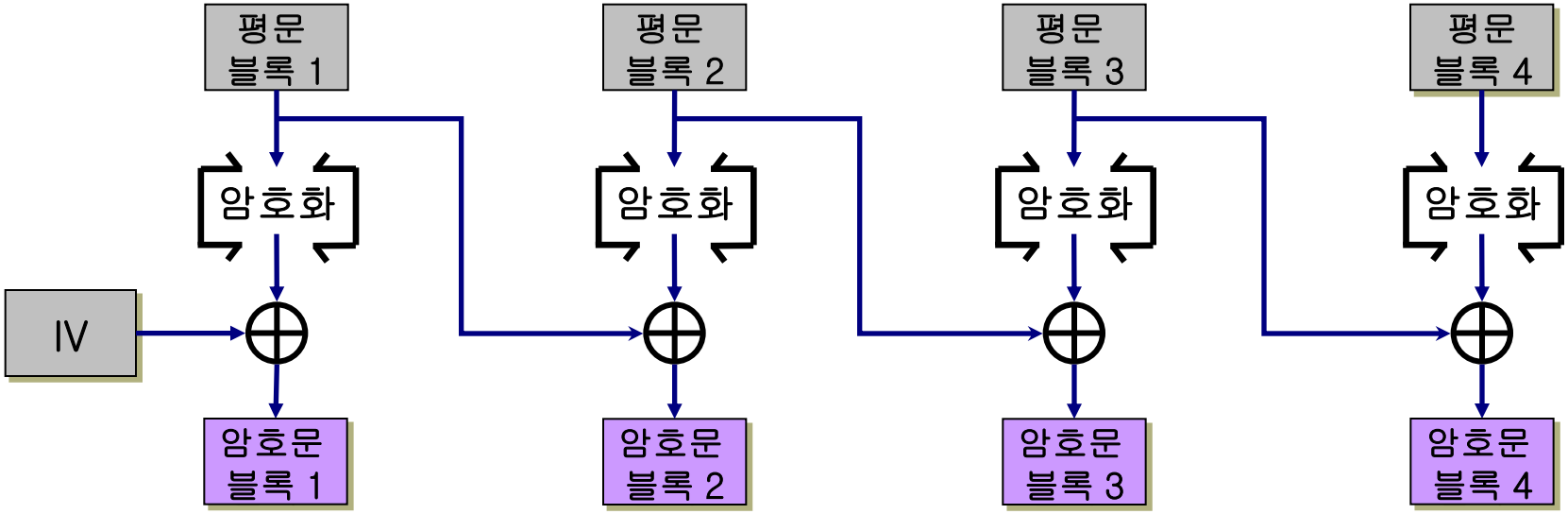


CBC 모드 활용의 예

- IPsec에는 통신의 기밀성을 지키기 위해 CBC 모드를 사용하고 있다.
  - 예를 들면 트리플 DES를 CBC 모드로 사용한 3DES-CBC나, AES를 CBC 모드로 사용한 AES-CBC 등이 여기에 해당된다.
- 인증을 수행하는 대칭암호 시스템의 하나인 Kerberos version 5에서도 사용하고 있다.

앨리스가 만든 CBC 모드 비슷한 것

- 앨리스가 생각해 낸 CBC 모드 비슷한 것은 어떤 성질을 가지고 있는가?



4.4 CFB 모드

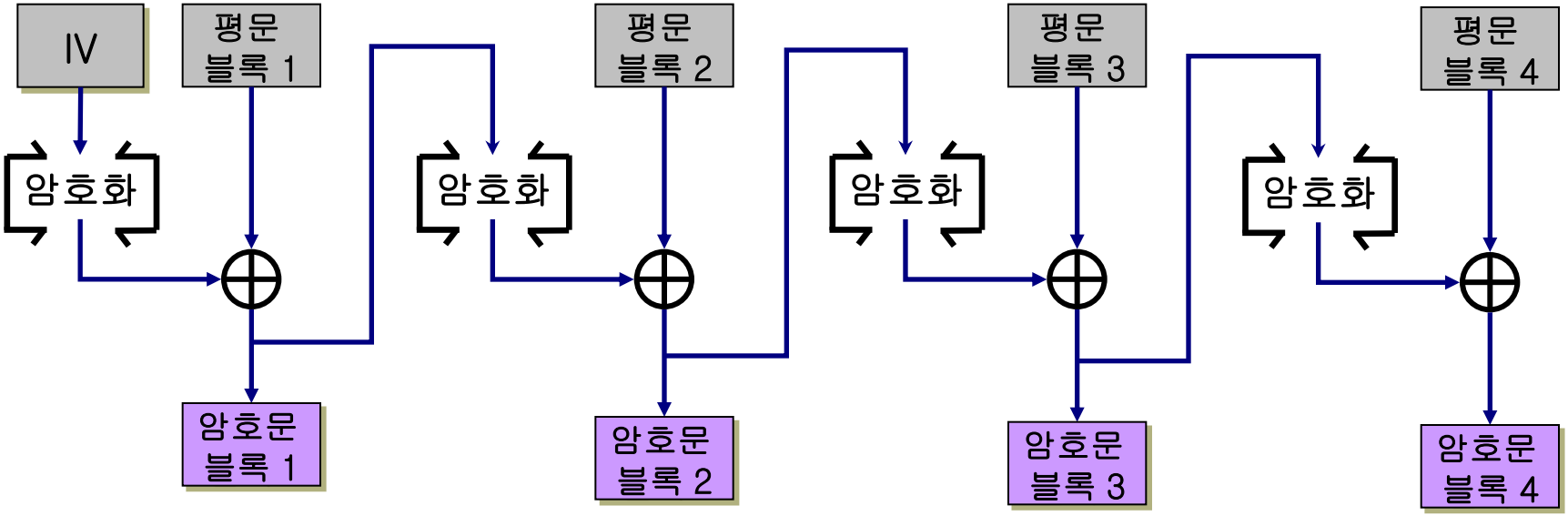
- 절대로 해독할 수 없는 암호인 일회용 패드라는 암호를 XOR의 연습을 겸해서 소개하도록 한다

4.4.1 CFB 모드란

- **CFB 모드**는 Cipher FeedBack 모드(**암호 피드백 모드**)의 약자이다.
- CFB 모드에서는 1 단계 앞의 암호문 블록을 암호 알고리즘의 입력으로 사용한다.
- 피드백이라는 것은, 여기서는 암호화의 입력으로 사용한다는 것을 의미한다

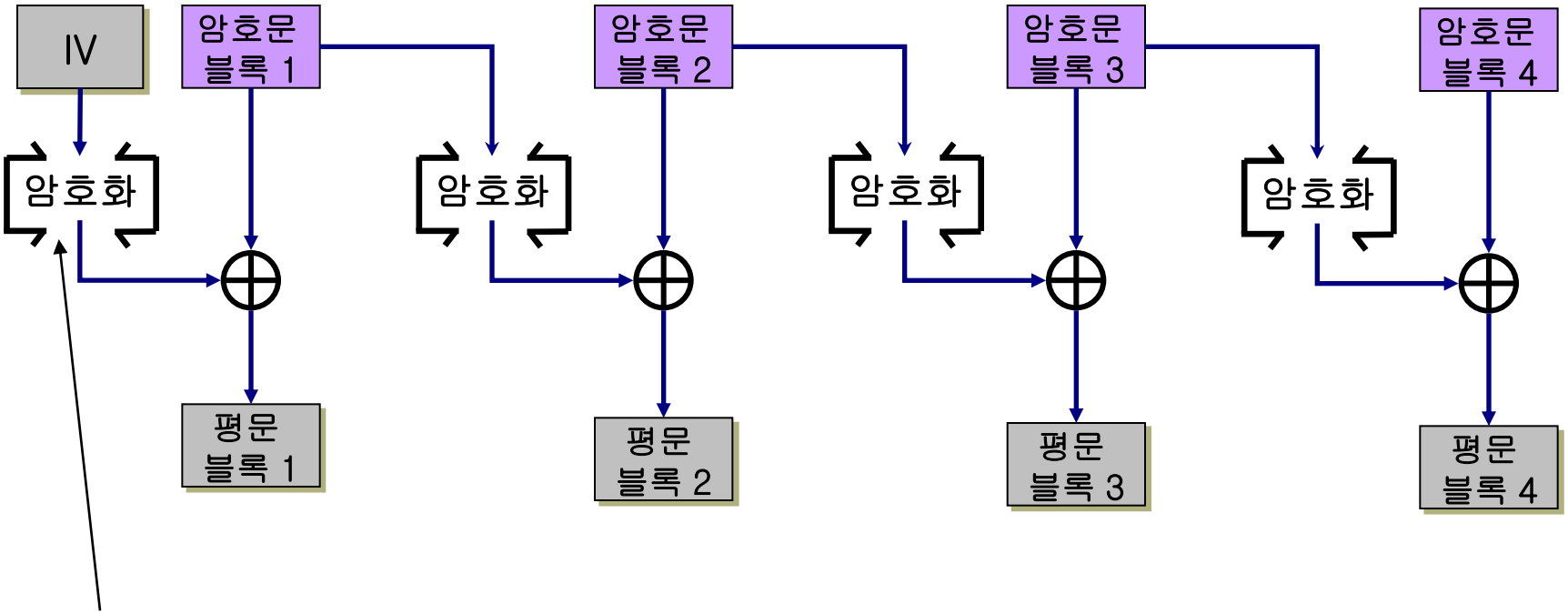
CFB 모드(암호 피드백 모드)

- CFB 모드에 의한 암호화



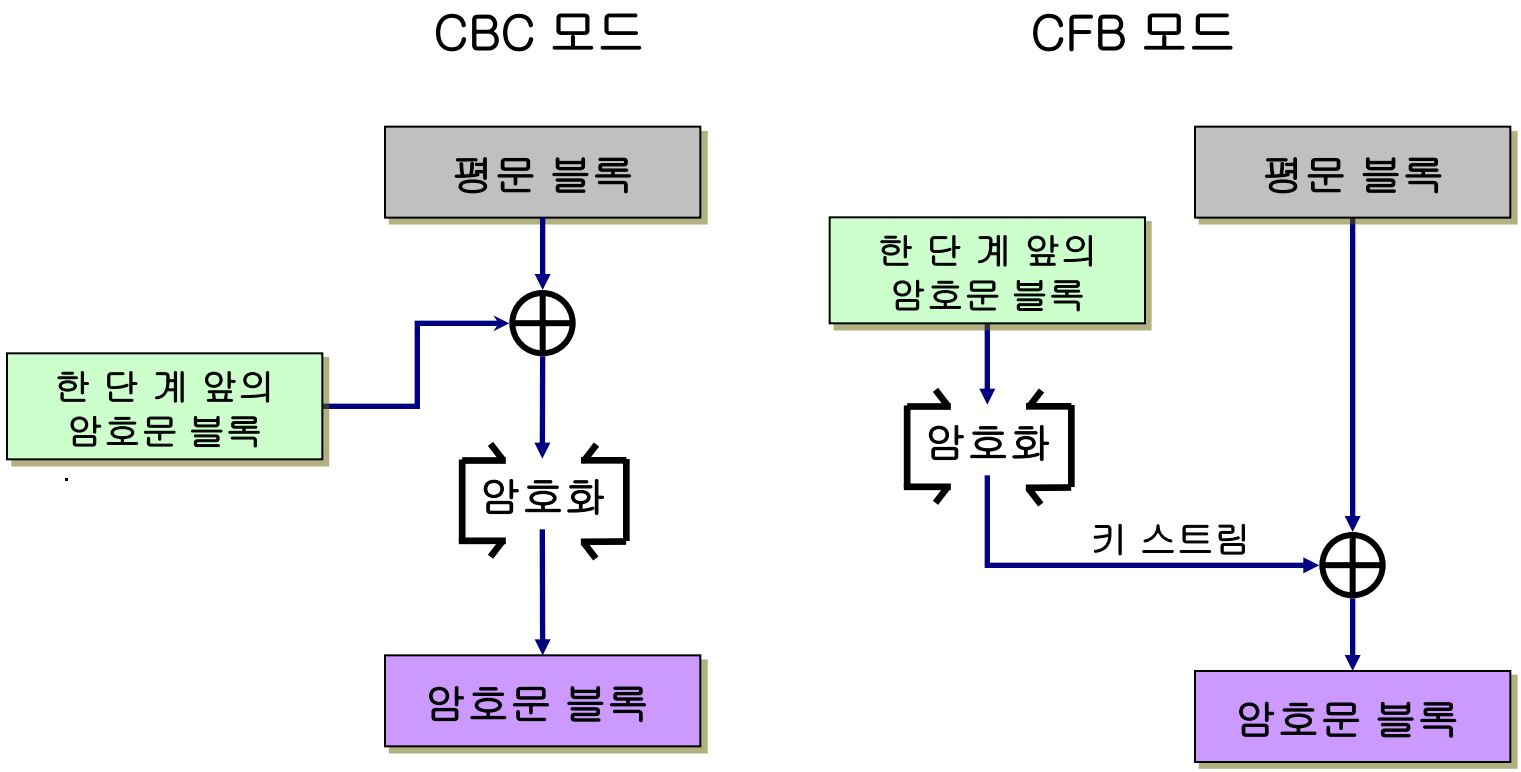
CFB 모드(암호 피드백 모드)

- CFB 모드에 의한 복호화



초기벡터를 복호화 하는 것이 아니라 암호화라는 점에 유의하기 바란다.

CBC 모드와 CFB 모드의 비교



초기화 벡터

- 최초의 암호문 블록을 만들어낼 때는 1 단계 앞의 출력이 존재하지 않으므로 대신에 **초기화 벡터**(IV)를 사용한다
- 이것은 CBC 모드 때와 같다
- 초기화 벡터는 보통 암호화 때마다 다른 랜덤 비트열을 사용한다

CFB 모드와 스트림 암호

- CFB 모드의 구조는 일회용 패드와 비슷하다.
  - 일회용 패드에서는「평문」과「랜덤한 비트열」을 XOR해서「암호문」을 만들어냈다.
  - CFB 모드에서는「평문 블록」과「암호 알고리즘의 출력」을 XOR해서「암호문 블록」을 만든다.
  - XOR에 의해 암호화하는 것이 비슷하다.

CFB 모드와 스트림 암호

- CFB 모드와 일회용 패드를 비교해서 살펴보면 일회용 패드의「랜덤한 비트열」에 대응되는 것을 CFB 모드에서 찾는다면 그것은「암호 알고리즘의 출력」이다.
- 암호 알고리즘의 출력은 계산으로 만들어내고 있는 것이므로 실제 난수는 아니다
- 그러므로 CFB 모드가 일회용 패드처럼 이론적으로 해독 불가능한 것은 아니다.

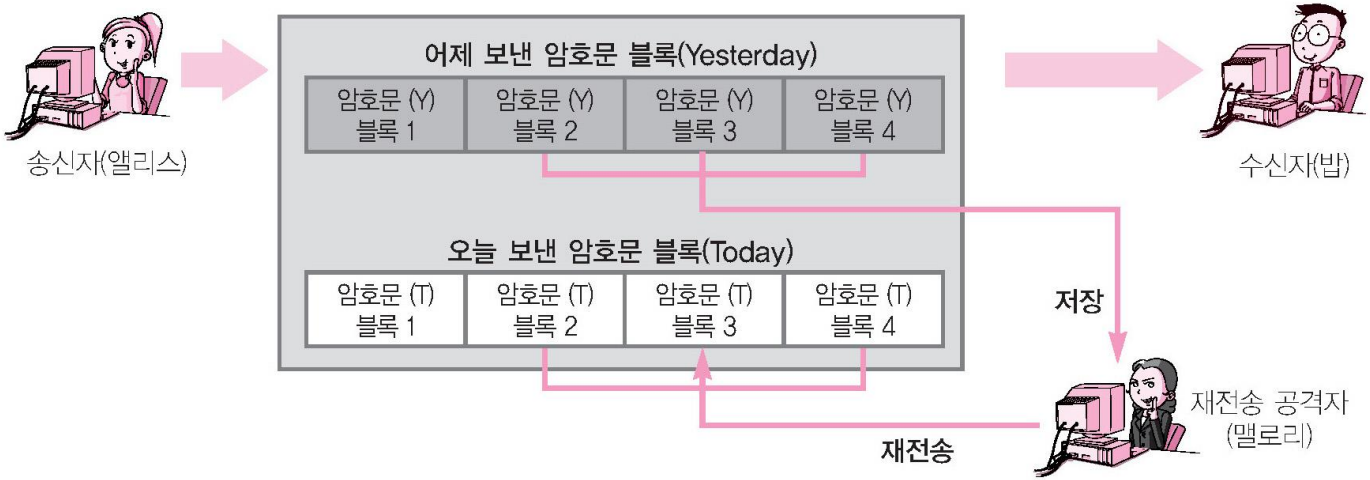
CFB 모드의 복호화

- CFB 모드에서 복호화를 수행할 경우, 블록 암호 알고리즘 자체는 암호화를 수행하고 있다는 것에 주의하라.
- 키 스트림은 암호화에 의해 생성되는 것이다.

CFB 모드에 대한 공격

- CFB 모드에 대해서는 **재전송 공격**(replay attack)이 가능하다.

CFB 모드에 대한 재전송 공격



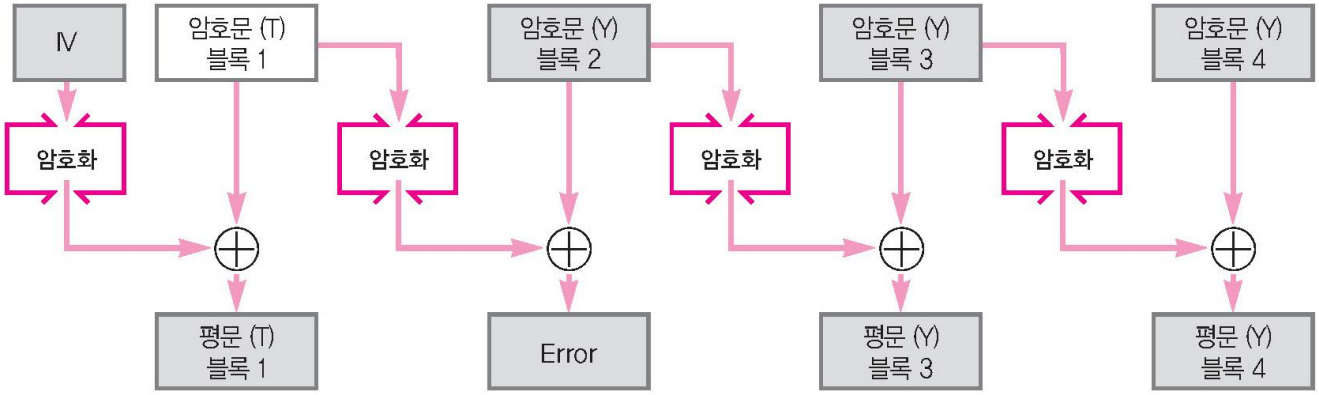


그림 4-14 CFB 모드에 대한 재전송 공격

4.5 OFB 모드

4.5.1 OFB 모드란

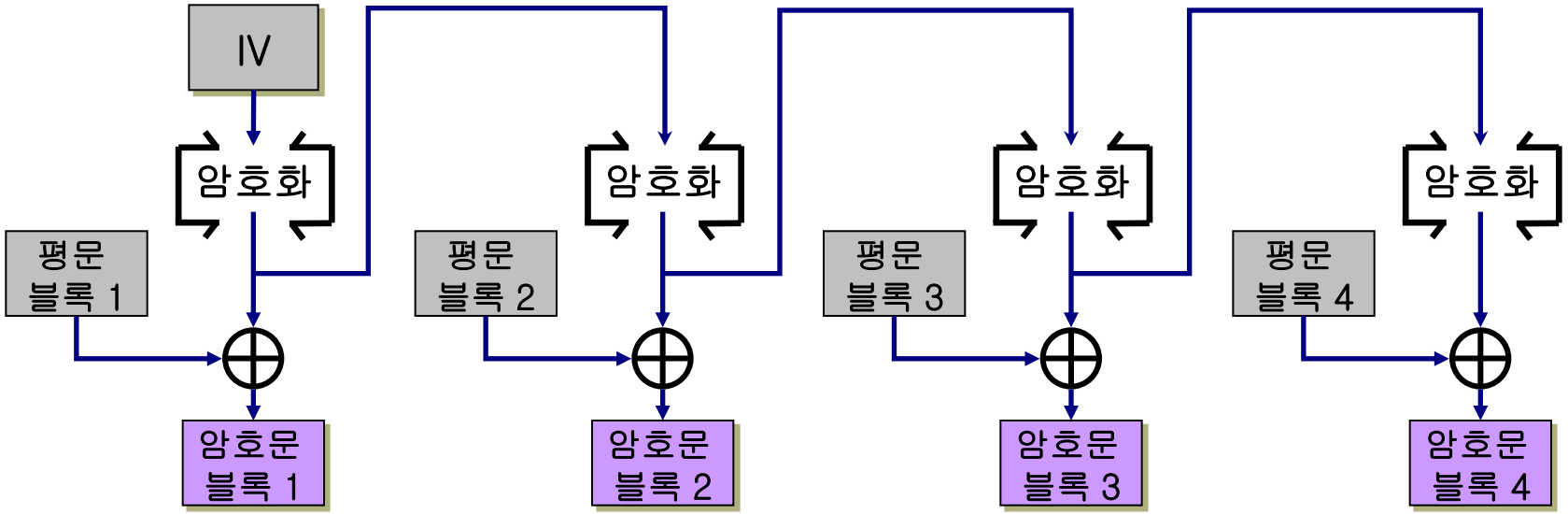
- **OFB 모드**는 Output-FeedBack 모드(**출력 피드백 모드**)의 약자이다.
- OFB 모드에서는 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백한다.
- OFB 모드에서는 평문 블록은 암호 알고리즘에 의해 직접 암호화되고 있는 것은 아니다.
- 평문 블록과 암호 알고리즘의 출력을 XOR해서 암호문 블록을 만들어내고 있다.
- OFB 모드는 이 점에서 CFB 모드와 비슷하다.

초기화 벡터

- OFB 모드에서도 CBC 모드나 CFB 모드와 마찬가지로 **초기화 벡터**(IV)를 사용한다.
- 초기화 벡터는 암호화 때마다 다른 랜덤 비트열을 이용하는 것이 보통이다.

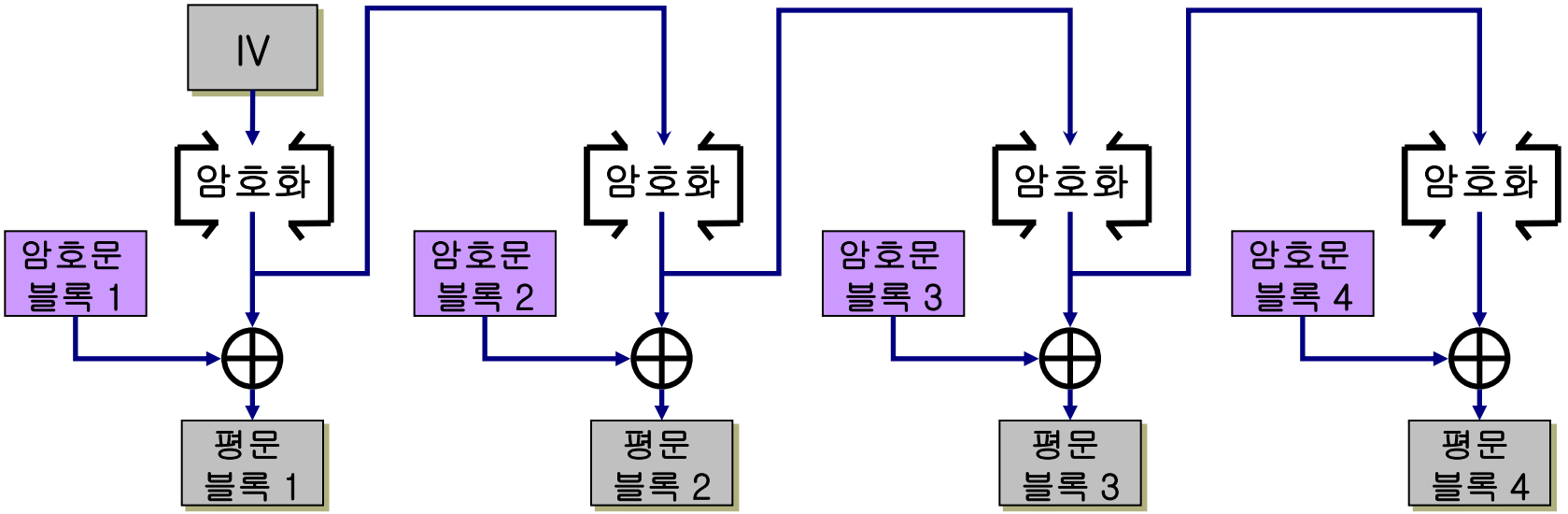
OFB 모드(출력 피드백 모드)

- OFB 모드에 의한 암호화



OFB 모드(출력 피드백 모드)

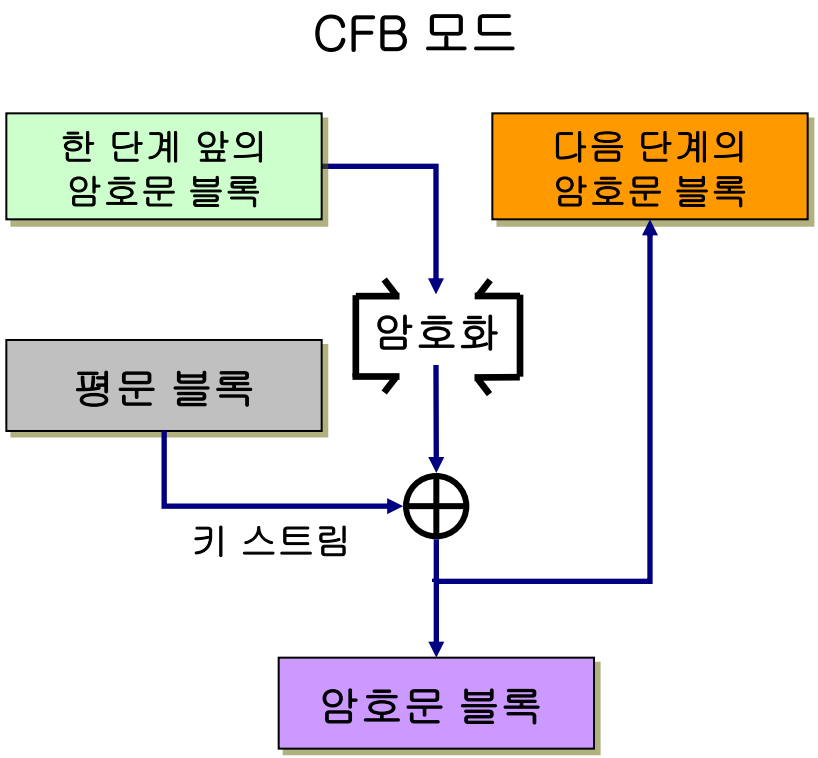
- OFB 모드에 의한 복호화

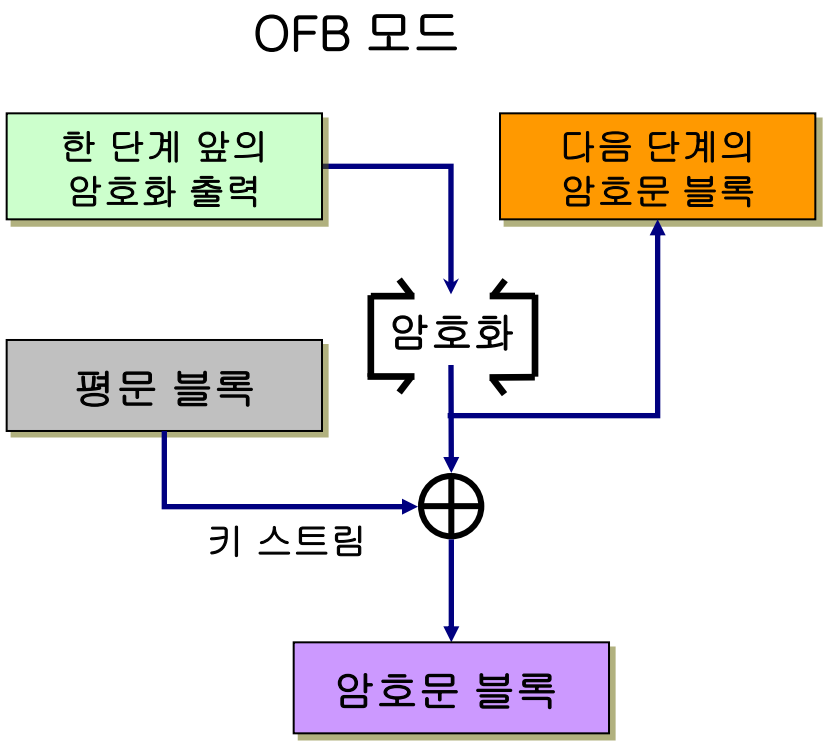


CFB 모드와 OFB 모드의 비교

- OFB 모드와 CFB 모드에서는 암호 알고리즘으로의 입력만이 다르다.
- CFB 모드에서는 1개 앞의 암호문 블록이 암호 알고리즘으로의 입력이었다. 암호문(사이퍼) 블록을 암호 알고리즘으로 피드백한 것이다. 그렇기 때문에「사이퍼 피드백 모드」라는 이름을 붙인 것이다.
- 한편 OFB 모드에서는 암호 알고리즘의 입력으로 사용되는 것은 암호 알고리즘의 한 단계 앞의 출력이다. 출력(아웃풋)을 암호 알고리즘으로 피드백한 것이다. 이것 때문에 「아웃풋 피드백 모드」라는 이름이 붙어 있다.

CFB 모드와 OFB 모드의 비교



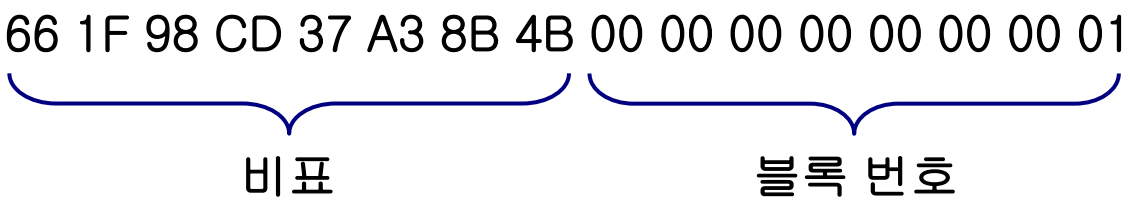


4.6 CTR 모드

- **CTR 모드**는 CounTeR 모드의 약자입니다.
- **CTR 모드는 1씩 증가해 가는 카운터를 암호화해서 키 스트림을 만들어 내는 스트림 암호이다.**
- CTR 모드에서는 블록을 암호화할 때마다 1씩 증가해 가는 카운터를 암호화해서 키 스트림을 만든다.
  - 즉, 카운터를 암호화한 비트열과, 평문 블록과의 XOR을 취한 결과가 암호문 블록이 된다.

4.6.1 카운터 만드는 법

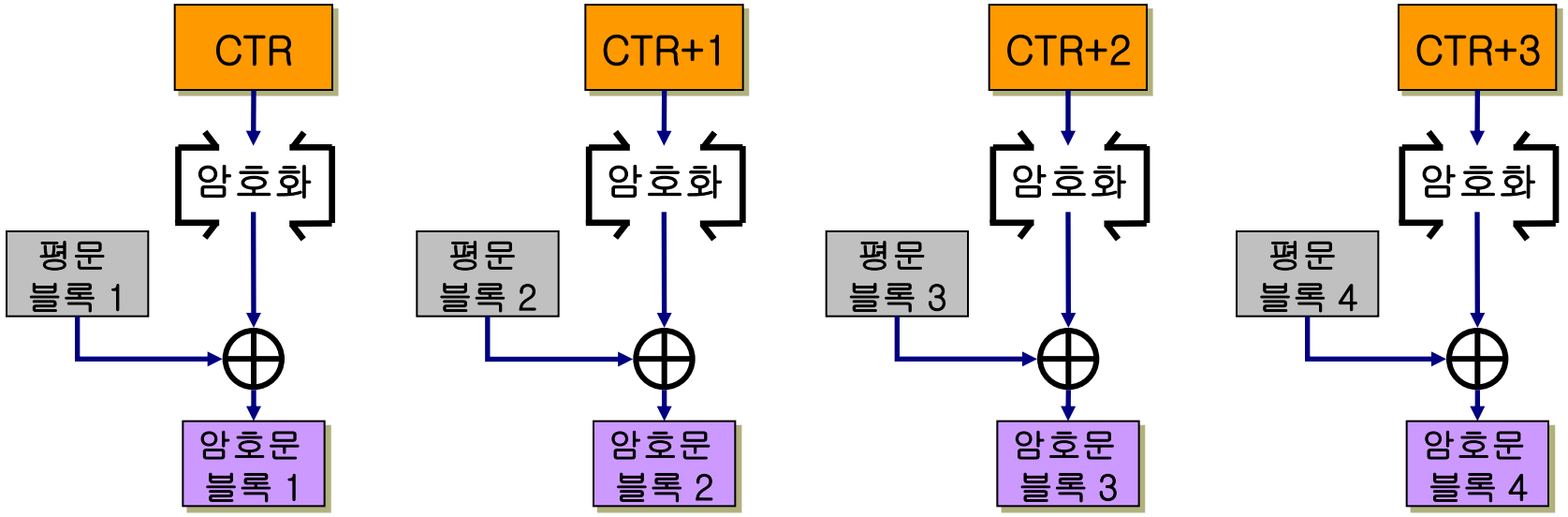
- 카운터의 초기값은 암호화 때마다 다른 값(nonce, 비표)을 기초로 해서 만든다.
- 블록 길이가 128비트(16바이트)인 경우 카운터의 초기값은 예를 들면,



- 와 같은 값을 사용할 수 있을 것이다.

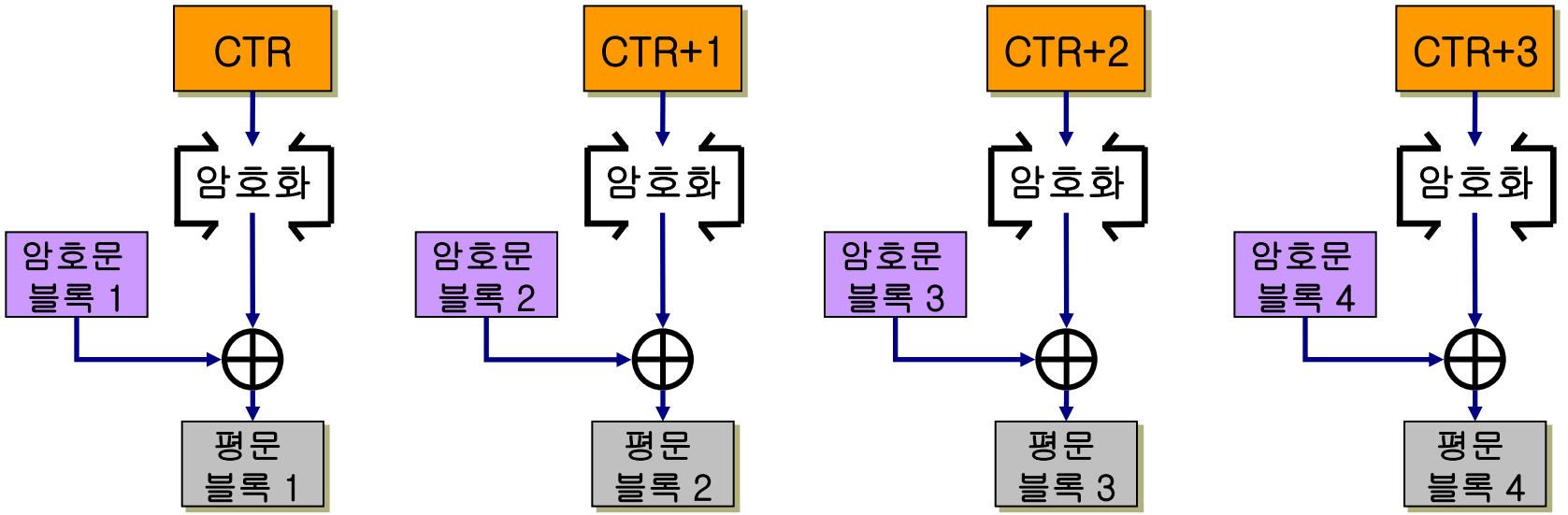
CTR 모드(카운터 모드)

- CTR 모드에 의한 암호화



CTR 모드(카운터 모드)

- CTR 모드에 의한 복호화



카운터 만드는 법

- 앞부분의 8바이트는 비표로 암호화 때마다 다른 값으로 하지 않으면 안 된다.
- 후반 8바이트는 블록 번호로 이 부분을 카운트해서 하나씩 증가시켜가면 된다.
- 암호화가 진행됨에 따라 카운터의 값은 다음과 같이 변환한다.

카운터 값

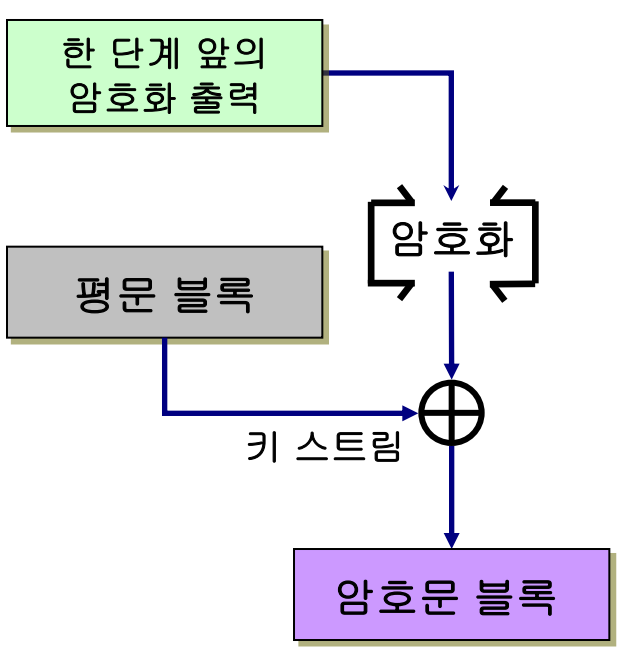
- 66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 01 평문 블록1용의 카운터(초기값)
- 66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 02 평문 블록2용의 카운터
- 66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 03 평문 블록3용의 카운터
- 66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 04 평문 블록4용의 카운터

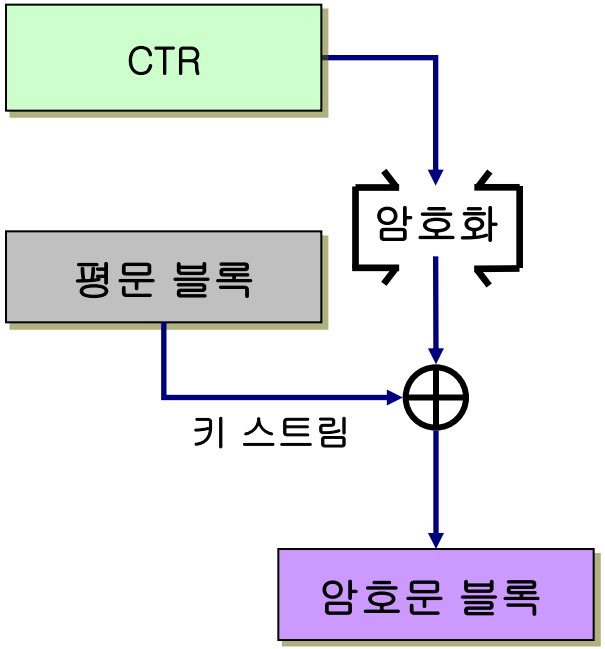
⋮ ⋮

4.6.2 OFB 모드와 CTR 모드의 비교

- CTR 모드는 OFB 모드와 같은 스트림 암호의 일종이다.
- 1개의 블록의 암호화하는 부분만을 추출해서 OFB 모드와 CTR 모드를 비교하면 차이를 잘 알 수 있을 것이다
- OFB 모드에서는 암호화의 출력을 입력으로 피드백하고 있지만, CTR 모드에서는 카운터의 값이 암호화의 입력이 된다.

OFB 모드와 CTR 모드의 비교





4.6.3 CTR 모드의 특징

- CTR 모드의 암호화와 복호화는 완전히 같은 구조이므로, 프로그램으로 구현하는 것이 매우 간단하다.
  - 이것은 OFB 모드와 같은 스트림 암호의 특징이다.
- 또한 CTR 모드에서는 블록을 임의의 순서로 암호화・복화화할 수 있다.
  - 암호화・복호화 때에 사용하는「카운터」는 비표와 블록 번호로부터 금방 구할 수 있기 때문이다.
  - 이것은 OFB 모드에는 없었던 성질이다.

4.6.4 오류와 기밀성

- CTR 모드는 통신 오류와 기밀성에 관해서 OFB 모드와 거의 같은 성질을 가지고 있다.
- CTR 모드의 암호문 블록에서 1비트의 반전이 발생했다고 하자.
- 복호화를 수행하면, 반전된 비트에 대응하는 평문 블록의 1비트만이 반전 되고, 오류는 확대되지 않는다.

오류와 기밀성

- CTR 모드에는 OFB 모드보다도 뛰어난 성질이 하나 있다.
- OFB 모드에서는 키 스트림의 1블록을 암호화한 결과가, 암호화 전의 결과와 우연히 같아졌다고 하면 그 이후 키 스트림은 완전히 같은 값의 반복이 된다.
- 그러나 CTR 모드에서는 그런 걱정은 없다.

4.6.5 모드 선택

	이름	장점	단점	비고
ECB 모드	Electric CodeBook 전자 부호표 모드	• 간단 • 고속 • 병렬 처리 가능(암호화. 복호화 양쪽)	• 평문 속의 반복이 암호문에 반영된다. • 암호문 블록의 삭제나 교체에 의한 평문의 조작이 가능 • 비트 단위의 에러가 있는 암호문을 복호화하면, 대응하는 블록이 에러가 된다. • 재생 공격이 가능	사용해서는안된다

모드 선택

	이름	장점	단점	비고
CBC 모드	Cipher Block Chaining 암호 블록 연쇄 모드	• 평문의 반복은 암호문에 반영되지 않는다. • 병렬 처리 가능(복호화만) • 임의의 암호문 블록을 복호화할 수 있다.	• 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다. • 암호화에서는 병렬 처리를 할 수 없다.	권장

모드 선택

	이름	장점	단점	비고
CFB 모드	Cipher-FeedBack 암호 피드백 모드	• 패딩이 필요 없다. • 병렬 처리 가능(복호화만) • 임의의 암호문 블록을 복호화할 수 있다.	• 암호화에서는 병렬 처리를 할 수 없다. • 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다. • 재생 공격이 가능	• 현재는 사용 안 함. • CTR 모드를 사용하는 편이 나음.

모드 선택

	이름	장점	단점	비고
OFB 모드	Output-FeedBack 출력 피드백 모드	• 패딩이 필요 없다. • 암호화.복호화의 사전 준비를 할 수 있다. • 암호화와 복호화가 같은 구조를 하고 있다. • 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트만 에러가 된다.	• 병렬 처리를 할 수 없다. • 능동적 공격자가 암호문 블록을 비트 반전시키면, 대응하는 평문 블록이 비트 반전한다.	• CTR 모드를 사용하는 편이 나음.

모드 선택

	이름	장점	단점	비고
CTR 모드	CounTeR 카운터 모드	• 패딩이 필요 없다. • 암호화.복호화의 사전 준비를 할 수 있다. • 암호화와 복호화가 같은 구조를 하고 있다. • 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트만 에러가 된다. • 병렬 처리 가능 (암호화.복호화 양쪽)	• 능동적 공격자가 암호문 블록을 비트 반전시키면, 대응하는 평문 블록이 비트 반전한다.	권장