2017/01/18 , 2017 보안 기초 세미나

네트워크 보안 에센셜

- 2장 대칭 암호와 메시지 기밀성 (2) -

곽수진(kwaksugin@naver.com)

상명대학교 프로토콜공학연구실

목차

- 스트림 암호와 RC4
  - 스트림 암호 구조
  - RC4 알고리즘
- 암호 블록 운용 모드
  - 전자 코드북 모드
  - 암호 블록 체인 모드
  - 암호 피드백 모드
  - 출력 피드백 모드
  - 카운터 모드

스트림 암호 구조

- 블록 암호
  - 블록 단위로 암호화 처리
- 스트림 암호
  - 비트나 바이트 단위로 입력되는 요소를 연속적으로 처리
- 스트림 암호 구조
  - 스트림 암호를 설계하는 것
  - 전형적인 스트림 암호는 한 번에 한 바이트씩 암호화

스트림 암호 구조

- 평문 바이트와 생성기의 출력(키스트림) 바이트를 XOR
- 의사랜덤 비트 생성기를 이용

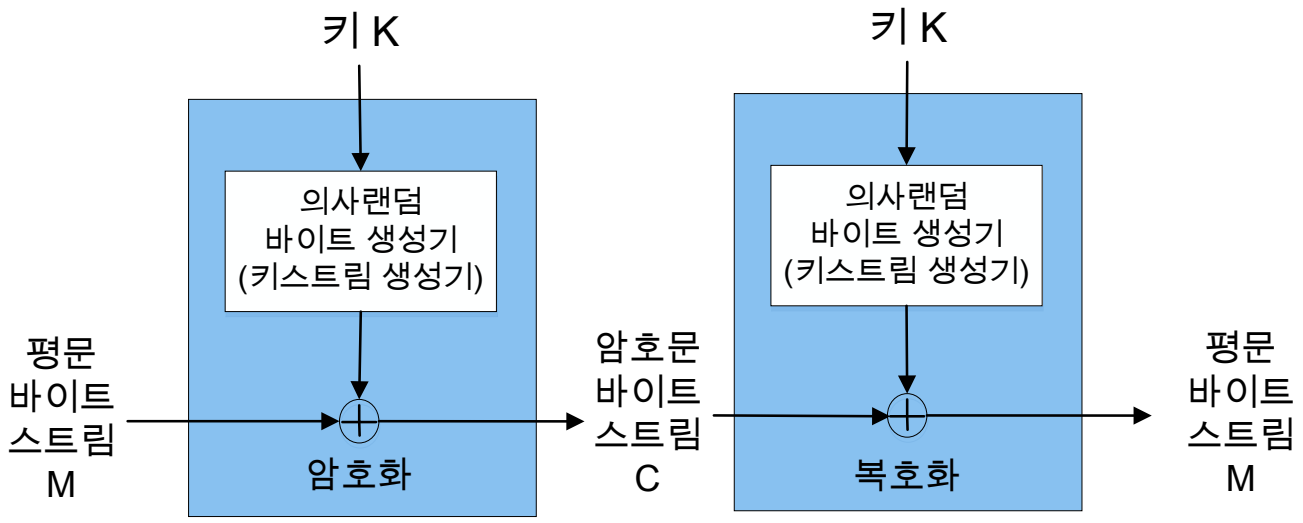
a)암호화

```
  11001100   평문
⊕ 01101100   키스트림
-----------
  10100000   암호문
```

b)복호화

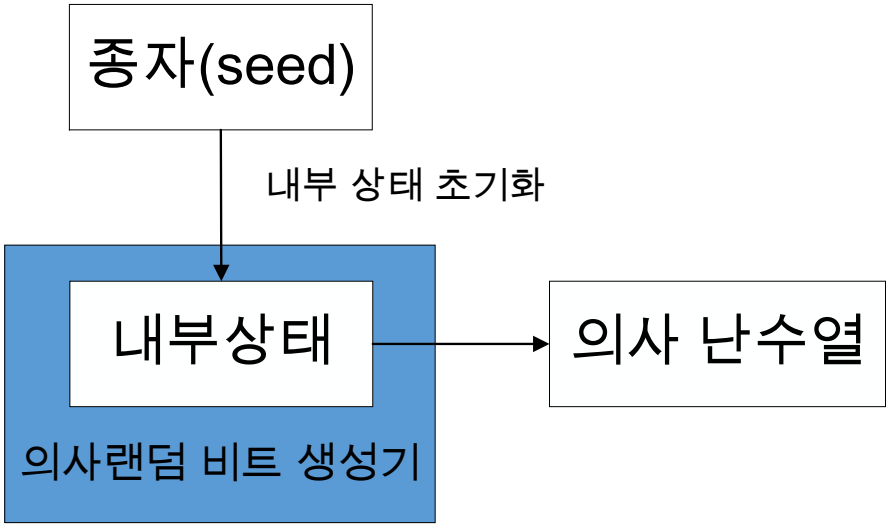
```
  10100000   암호문
⊕ 01101100   키스트림
-----------
  11001100   평문
```

c)스트림 암호 구조



스트림 암호 구조

- 의사랜덤 비트 생성기
  (PRNG : pseudorandom number generator)
  - 입력 되는 값이 종자(seed)라는 고정된 값
  - 종자 값에 따라 난수가 결정됨
  - 같은 입력 값을 넣으면 동일한 결과 값을 출력하는 결정적 알고리즘을 이용해 비트열 생성
  - 무한 비트열을 생성하기 위해 사용되는 알고리즘



스트림 암호 구조

- 스트림 암호 설계 시 고려사항
  - 암호열의 주기는 커야 함
    - 의사랜덤 생성기는 결국 반복적으로 나타나는 비트 스트림을 만들어 냄
    - 반복주기가 길수록 해독이 어려움
  - 키 스트림의 랜덤 스트림화
    - 키스트림이 랜덤하게 구성 될수록 암호문은 더 랜덤 해지고 해독은 더 어려워짐
  - 충분히 긴 키의 길이 (최소한 128bit)
    - 전수 공격을 이용한 해독을 방지

스트림 암호 구조

- 전수공격
  - 전수 공격이란?
    - 암호 해독을 위한 공격유형 중 하나
    - 모든 가능한 경우를 다 시도해보는 방법
    - 키의 길이가 매우 긴 경우 실용적이지 못함

스트림 암호 구조

- 스트림 암호 구조의 특성
  - 장점
    - 패딩 필요 없음
      - 패딩 : 블록의 맨 나중에 공백이나 의미가 없는 기호를 부가하여 고정 길이로 하는 것
    - 실시간 사용 가능
    - 속도 빠르고, 적은 양의 코드 사용
    - 동일한 길이의 키를 사용하는 블록 암호 만큼의 보안성 유지
  - 단점
    - 두 개의 평문을 동일한 키로 암호화 할 시 암호해독이 단순해짐

      → 두 개의 암호문 XOR = 두 개의 평문 XOR

RC4 알고리즘

- RC4 알고리즘 (Rivest Cipher 4)
  - Ron Riveset가 1987년에 RSA Security에서 설계한 스트림 암호
    - 1994년 9월에 한 익명의 제보자가 인터넷의 사이버 펑크 익명 리메일러 목록에 RC4 알고리즘을 올림
  - 바이트 단위로 작동하는 다양한 크기의 키 사용
  - 알고리즘은 랜덤 치환 기법 사용
  - 암호 주기가 10^{100}보다 큼

RC4 알고리즘

- RC4 알고리즘 구현
  - 1. 벡터 S의 초기화, 임시벡터 T 생성
  - 2. S의 초기치환
  - 3. 스트림 생성

RC4 알고리즘

- RC4 알고리즘 구현

1. 벡터 S의 초기화
   - 벡터 S의 성분을 0부터 255까지 오름차순으로 저장
   - 임시벡터 T 생성
     - 키 값의 길이가 256 바이트인 경우
       - K를 그대로 T로 전달
     - 키 값의 길이가 256 바이트 미만일 때
       - 키의 길이 keylen만큼 T에 전달, T가 채워질 때까지 K를 반복하여 채움

❖ **for** i = 0 **to** 255 **do**

```
S[i] = i;
T[i] = K[i mod keylen];
```

RC4 알고리즘

- RC4 알고리즘 구현

2. S 초기치환
   - 벡터 T의 값을 이용해 S[i]를 S의 다른 바이트와 교환

❖ j = 0;

```
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    Swap (S[i], S[j]);
```

RC4 알고리즘

- RC4 알고리즘 구현

  3. 스트림 생성
     - S벡터 초기화 후 입력키는 사용되지 않음
     - 스트림 생성은 S[0]부터 S[255]까지 포함하여 수행
       - 각 S[i]는 S의 현재 상태에 있는 내용에 따라 S의 다른 바이트와 교환
       - S[255]에 도달한 뒤에는 계속하여 S[0]부터 다시 시작
     - 암호화 : K와 평문의 다음 바이트를 XOR 연산 후 리턴
     - 복호화 : K와 암호문의 다음 바이트를 XOR 연산 후 리턴

RC4 알고리즘

- RC4 알고리즘 구현

3. 스트림 생성

❖ i, j = 0

```
while (true)
    i = (i + 1) mod 256;
    j = (j + S[i]) mod 256;
   Swap (S[i], S[j]);
   t = (S[i] + S[j]) mod 256;
   k = S[t];

return text ^ k;
```

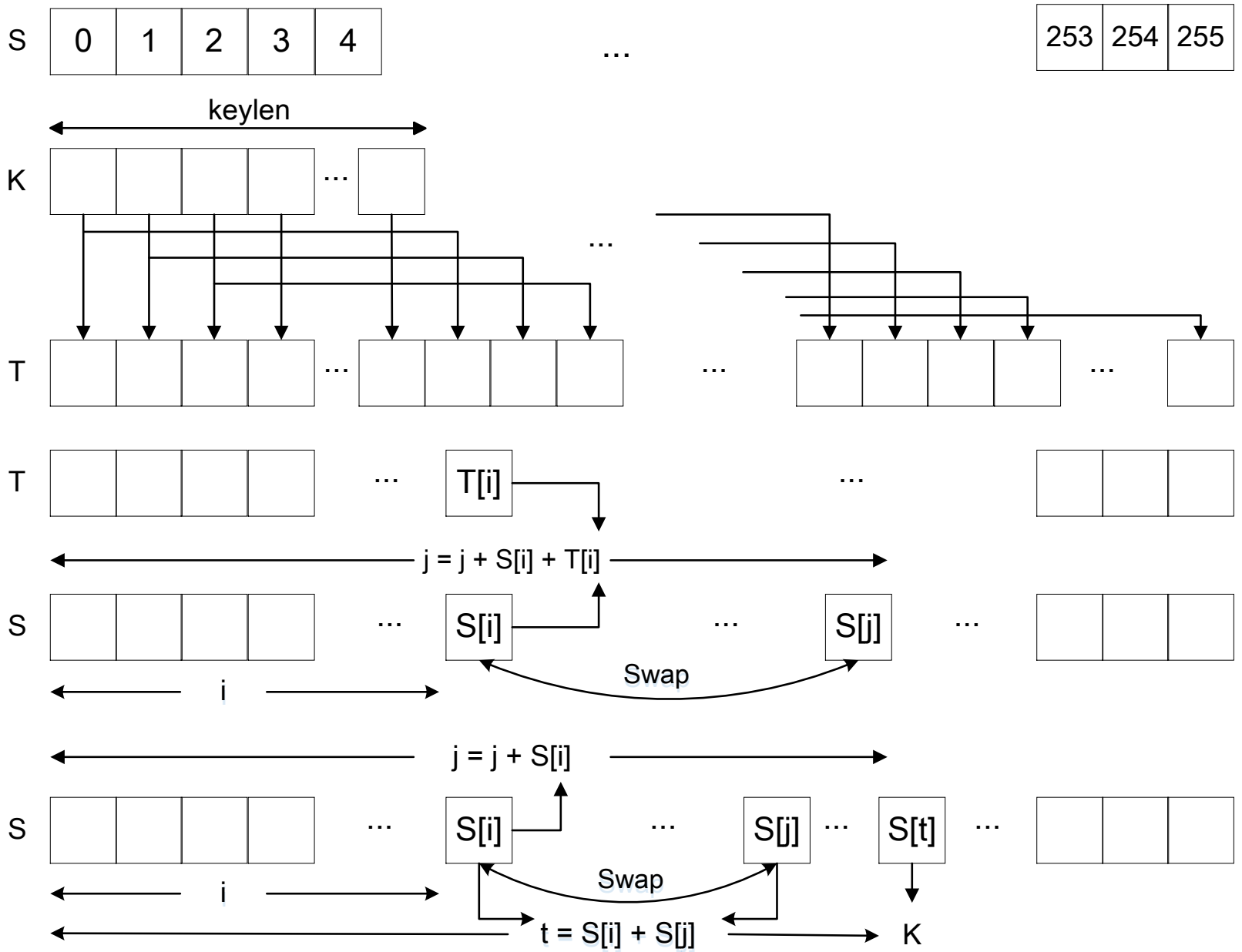
RC4 알고리즘

a) 벡터 S
초기 상태

b) 벡터 T
초기 상태

c) S의
초기 치환

d) 스트림 생성



RC4 알고리즘

- RC4 알고리즘 강도
  - 여러 논문에서 RC4를 공격하는 방법 분석 중
  - 적당한 길이를 갖는 키(128bit)를 사용하는 RC4를 실제적 공격하기 어려움
  - RC4를 이용한 WEP(Wired Equivalent Privacy) 프로토콜의 취약성
    - WEP는 무선 LAN 표준을 정의하는 IEEE 802.11 규약의 일부분으로 무선 LAN 운용간의 보안을 위해 사용되는 알고리즘
    - RC4에 입력으로 사용되는 키의 생성 방법에 문제
      - 24bit인 IV가 5000개의 패킷마다 같은 값을 반복
      - 랜덤으로 생성되는 IV의 값이 같은 경우 같은 키를 사용하기 때문에 키 재사용 됨

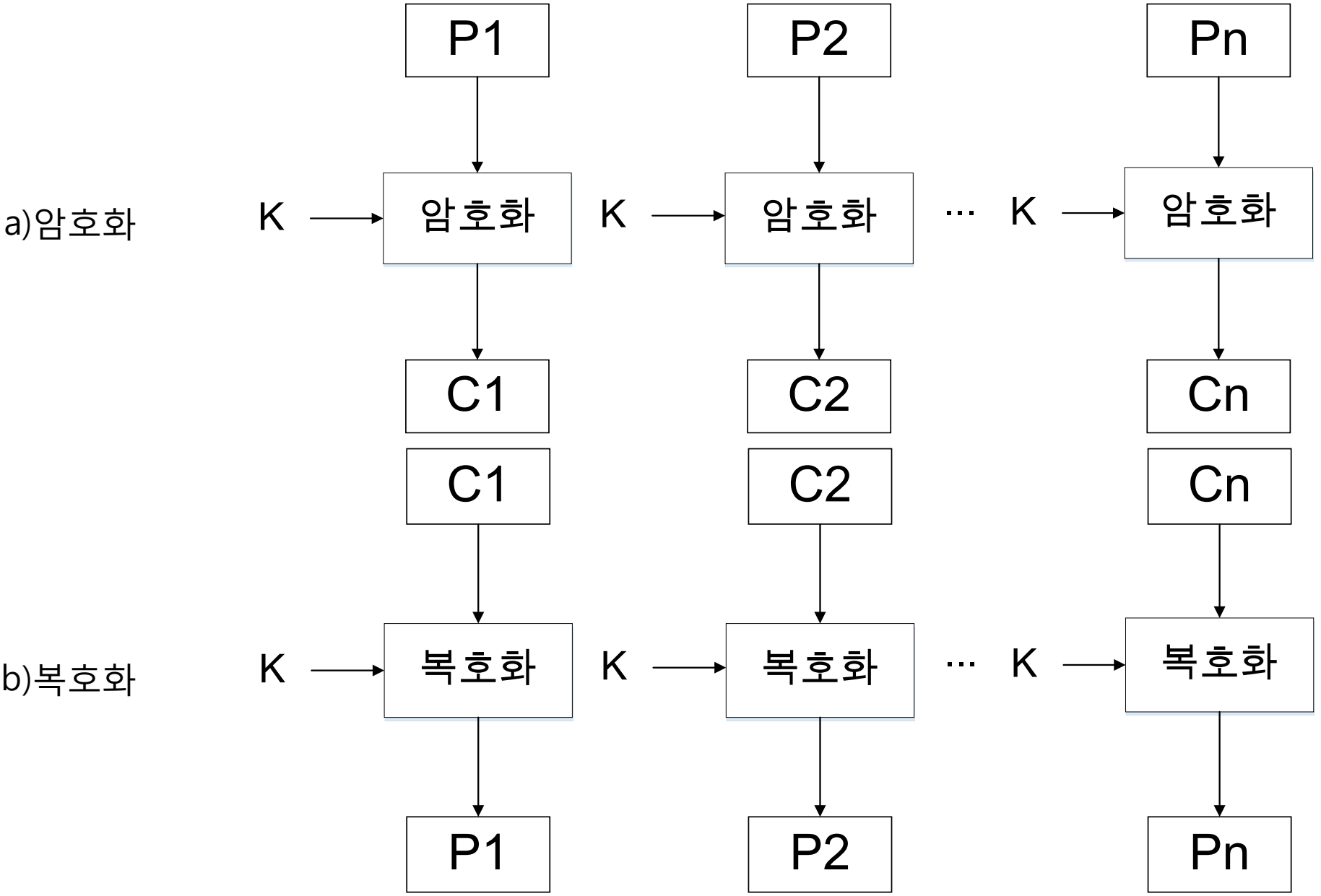
암호 블록 운용 모드

- 블록 암호의 운용
  - NIST(National Institute of Standards and Technology) 에서 5가지 운용 모드 정의
  - 블록 암호방식은 같은 평문 블록에 대해 같은 암호문 블록으로 암호화 함
  - 암호화하려는 정보가 블록 길이보다 긴 경우 적용되는 방법
  - 다양한 응용 환경에 적절한 암호화 도구로 사용할 수 있게 제시된 여러 유형의 효율적인 운영 방식들

전자 코드북 모드

- 전자 코드북 모드(ECB, Electronic CodeBook mode)
  - 가장 간단한 운용모드
  - 가장 기밀성이 낮은 모드
  - 동일한 크기의 블록으로 나눠지는 평문을 동일한 키로 암호화
  - 평문의 마지막 블록이 같은 크기가 아닌 경우 패딩 필요

전자 코드북 모드


P1
P2
Pn
a)암호화
K
암호화
K
암호화
···
K
암호화
C1
C2
Cn
C1
C2
Cn
b)복호화
K
복호화
K
복호화
···
K
복호화
P1
P2
Pn

전자 코드북 모드

- ECB의 특성
  - 장점
    - 간단한 구조
    - 개별적으로 암호화, 복호화 처리하므로 병렬 처리 가능
  - 단점
    - 같은 암호화 키 사용으로 반복공격에 취약
    - 패딩 필요
    - 암호문을 살펴 보는 것만으로도 패턴 반복성 감지 가능

암호 블록 체인 모드

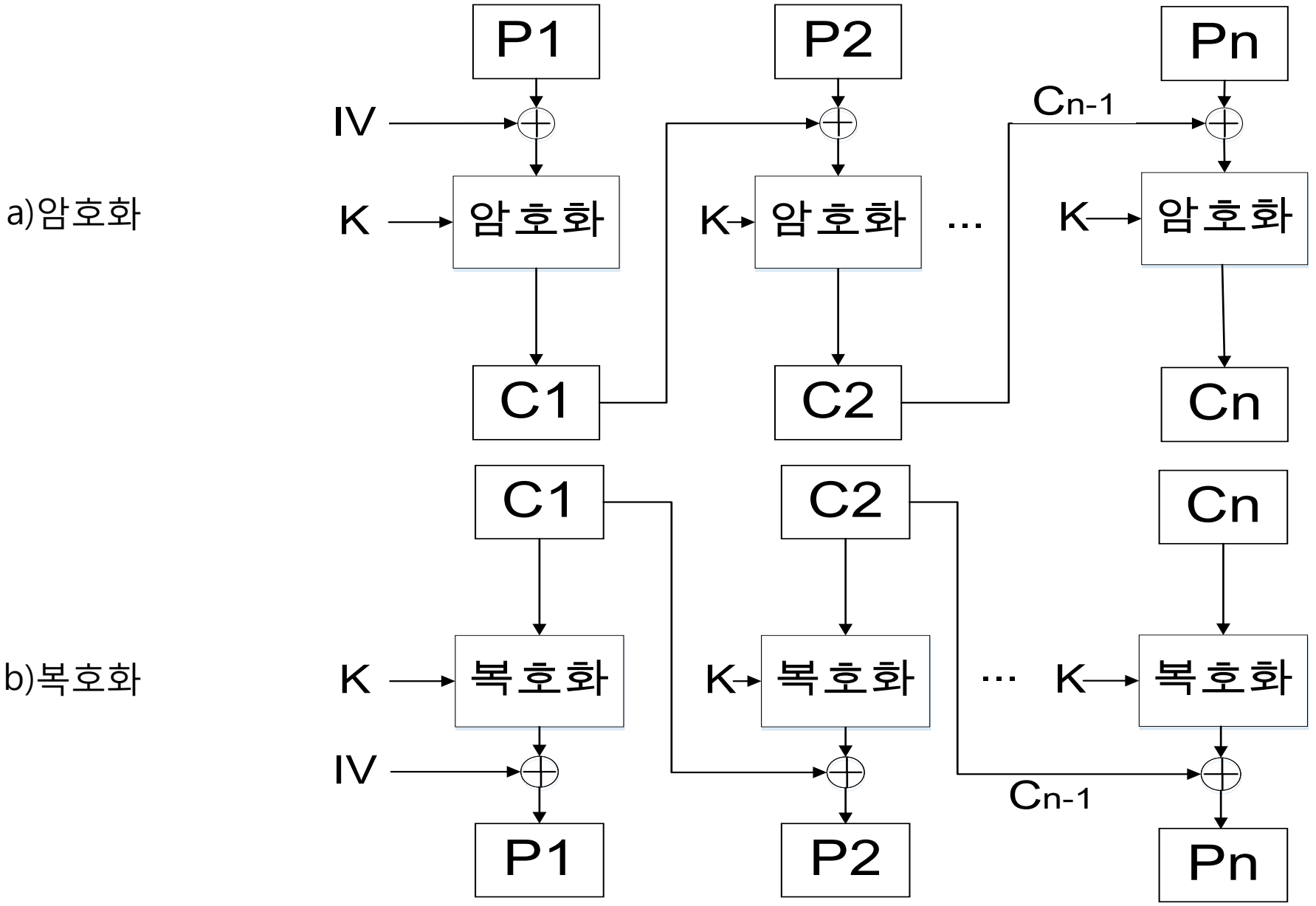
- 암호 블록 체인 모드
  (CBC, Cipher Block Chaining mode)
  - 암호문 블록을 마치 체인처럼 연결시키기 때문에 붙여진 이름
  - 평문 블록과 직전의 암호문 블록과 XOR
  - 첫 번째 블록을 암호화 할 때에는 초기화 벡터(IV) 사용
  - 가장 널리 사용되는 방식

암호 블록 체인 모드

- 초기화 벡터 (IV, Initialization Vector)
  - 최초 암호화(혹은 복호화) 할 때 1 단계 앞의 암호문 블록이 존재하지 않으므로 대신할 블록
  - 무결성 중요

  ➡공격자가 IV의 비트 값을 변조하는 경우, 첫 번째 블록의 비트 값들이 바뀜
  - 송신자와 수신자 모두 알고 있어야 함

암호 블록 체인 모드

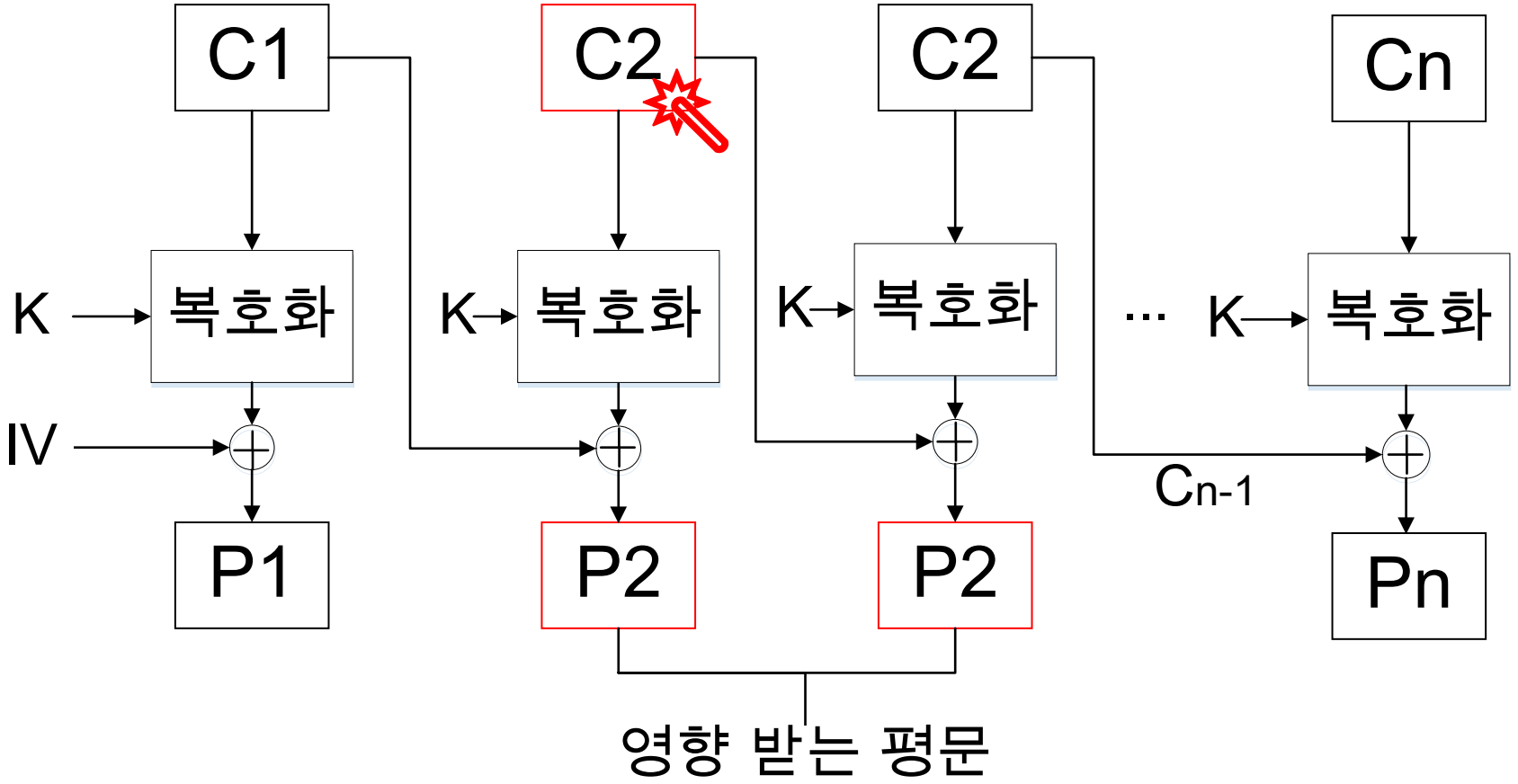

a)암호화
P1
P2
Pn
IV
Cn-1
K
암호화
K
암호화
...
K
암호화
C1
C2
Cn
b)복호화
C1
C2
Cn
K
복호화
K
복호화
...
K
복호화
IV
Cn-1
P1
P2
Pn

암호 블록 체인 모드

- CBC의 특성
  - 장점
    - ECB의 단점을 보완한 모드
      → 평문에 의한 동일한 암호문이 발생하지 않음
  - 단점
    - 암호화시 병렬 처리 할 수 없음
    - 암호블록 사이즈의 배수로 패딩
    - 오류 확산

암호 블록 체인 모드

- 오류확산
  - CBC 모드에서 암호문 블록이 파손되면 2개의 평문 블록에 영향을 미침

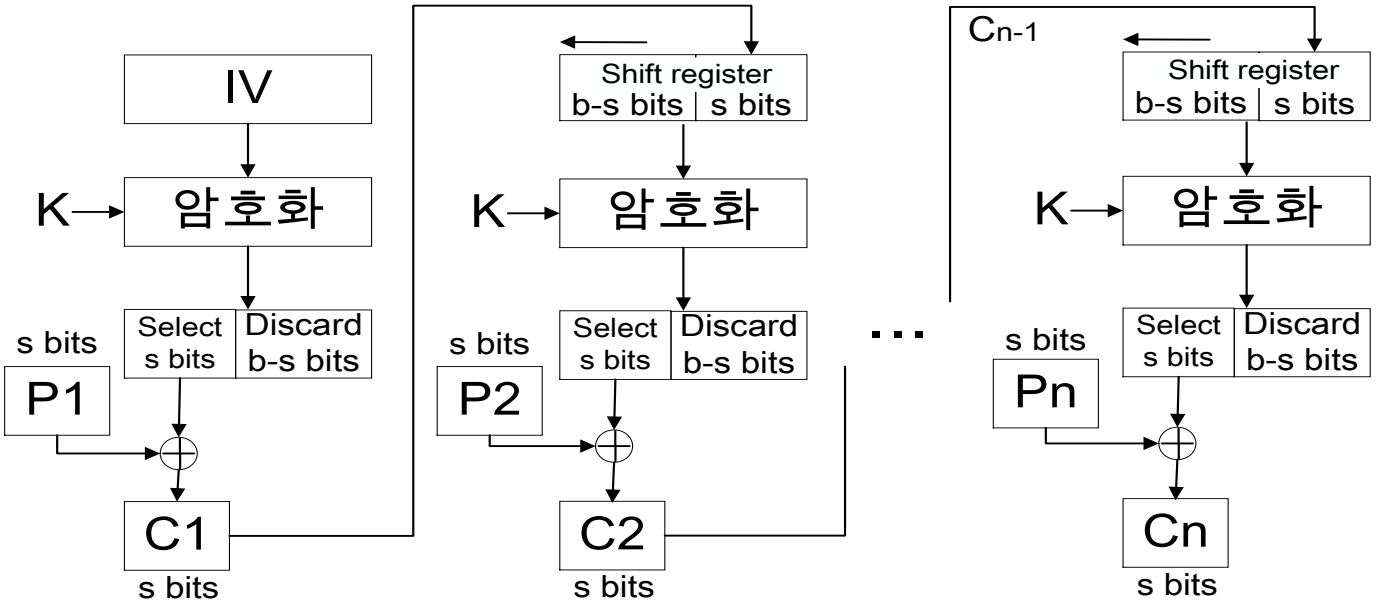


암호 피드백 모드

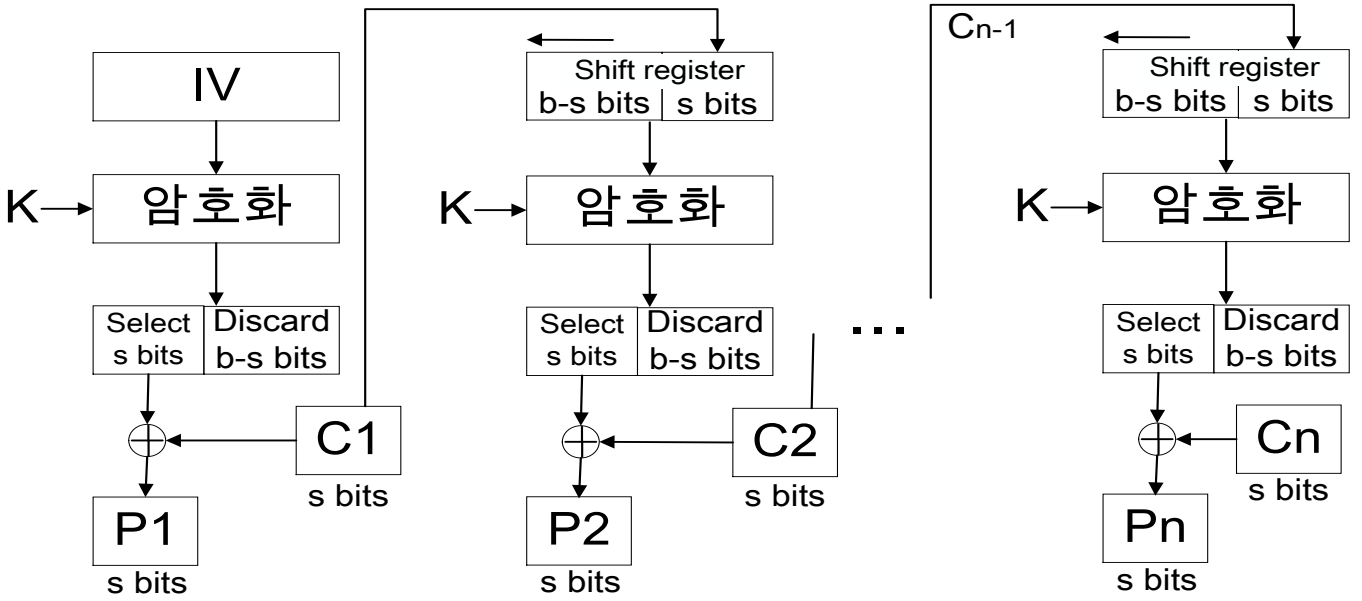
- 암호 피드백 모드 (CFB, Cipher FeedBack mode)
  - 피드백은 암호화의 입력으로 사용한다는 것을 의미
  - 블록 암호를 스트림 암호로 바꿔줌
  - 블록 크기가 n비트 보다 작은 경우
  - 평문이 모두 암호화될 때까지 과정 반복
  - 암호 피드백 모드의 IV는 64비트 시프트 레지스터
  - 암호화 함수 출력의 가장 왼쪽 s개 비트와 평문(s비트)을 XOR 연산

암호 피드백 모드

a)암호화



b)복호화

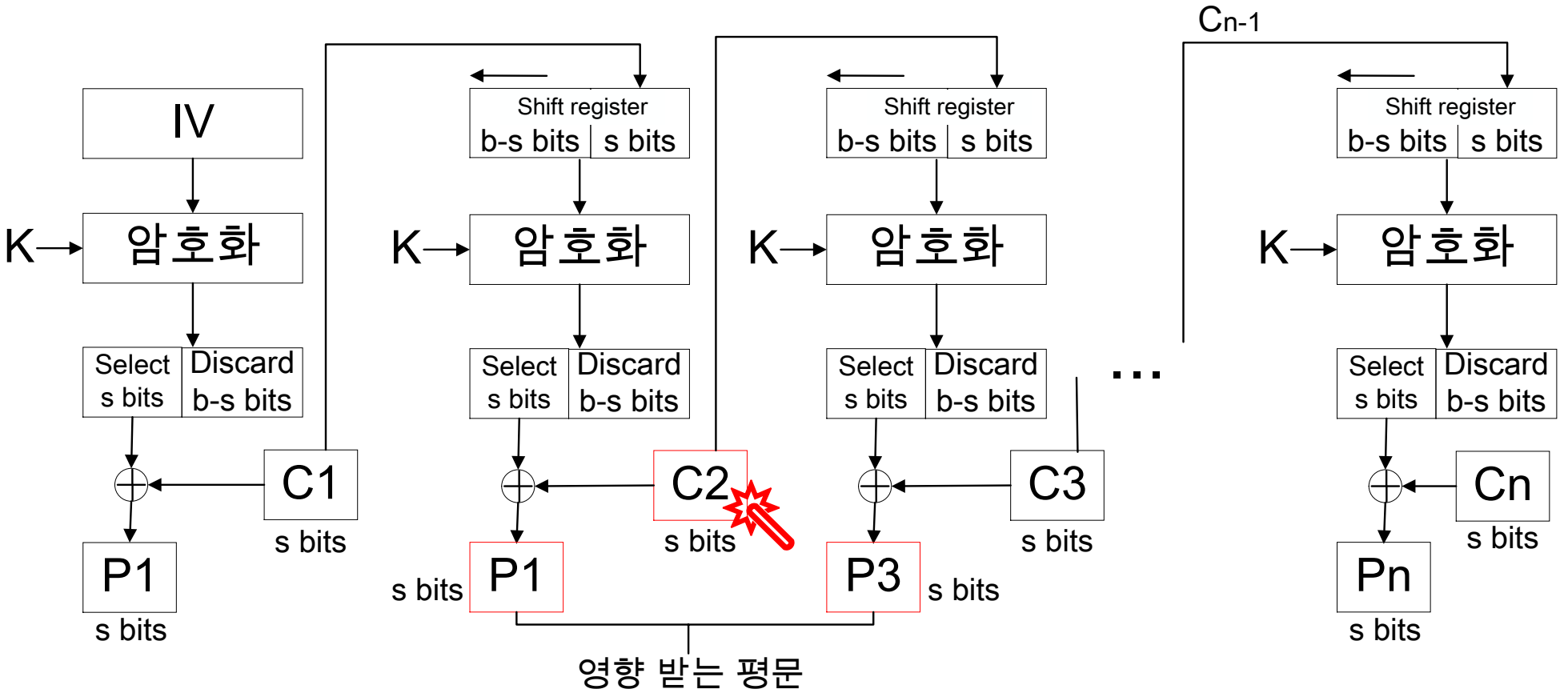


암호 피드백 모드

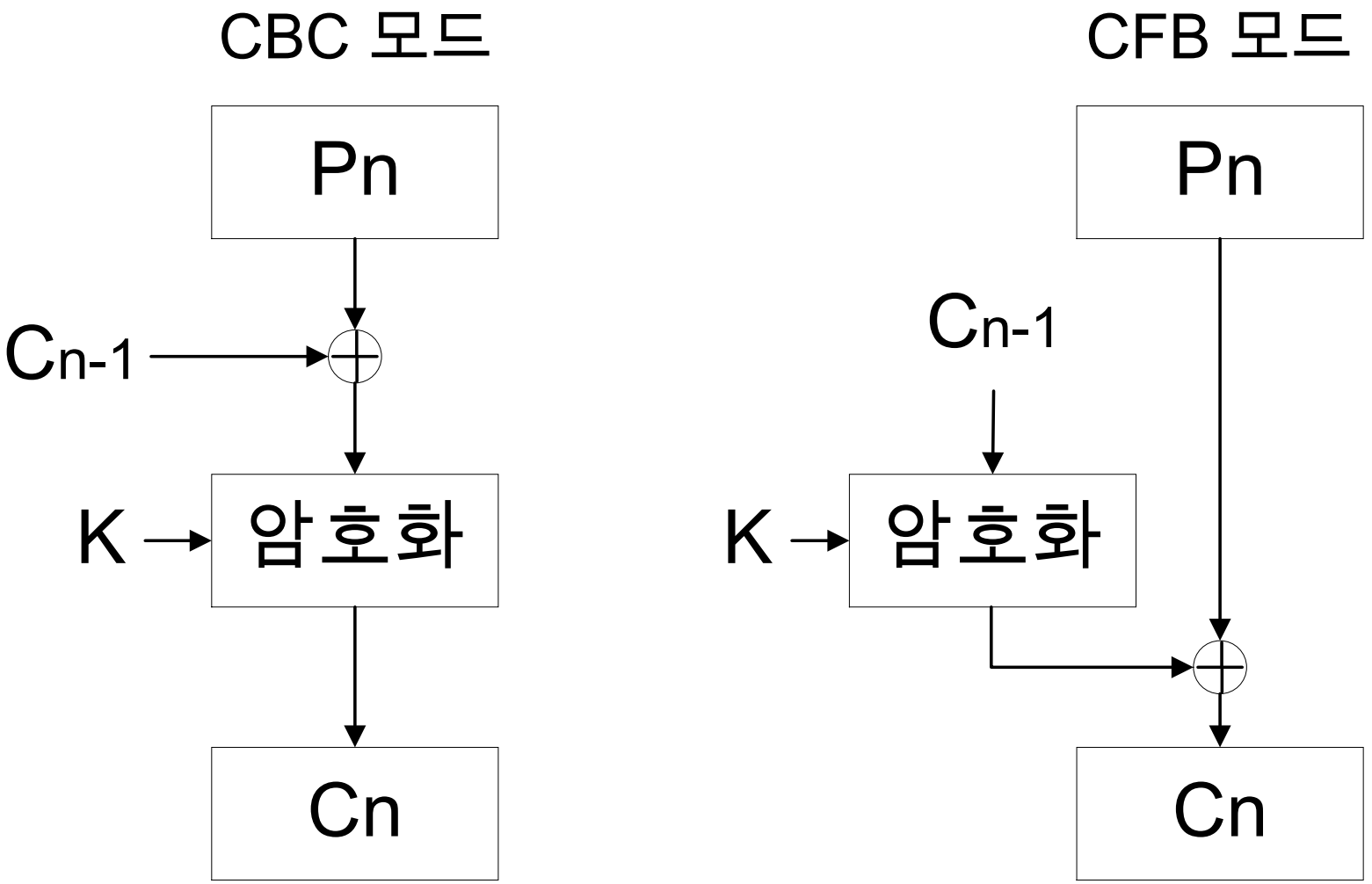
- CFB의 특성
  - 장점
    - 스트림 암호이므로 패딩이 필요 없음
    - 복호화 병렬 처리 가능
  - 단점
    - 암호화시 병렬 처리 할 수 없음
    - 오류 확산

암호 피드백 모드

- 오류 확산
  - 복호화 과정에서 Cn이 손상된 경우 해당 평문과 그 다음 평문에 영향을 미침



CBC 모드와 CFB 모드의 비교

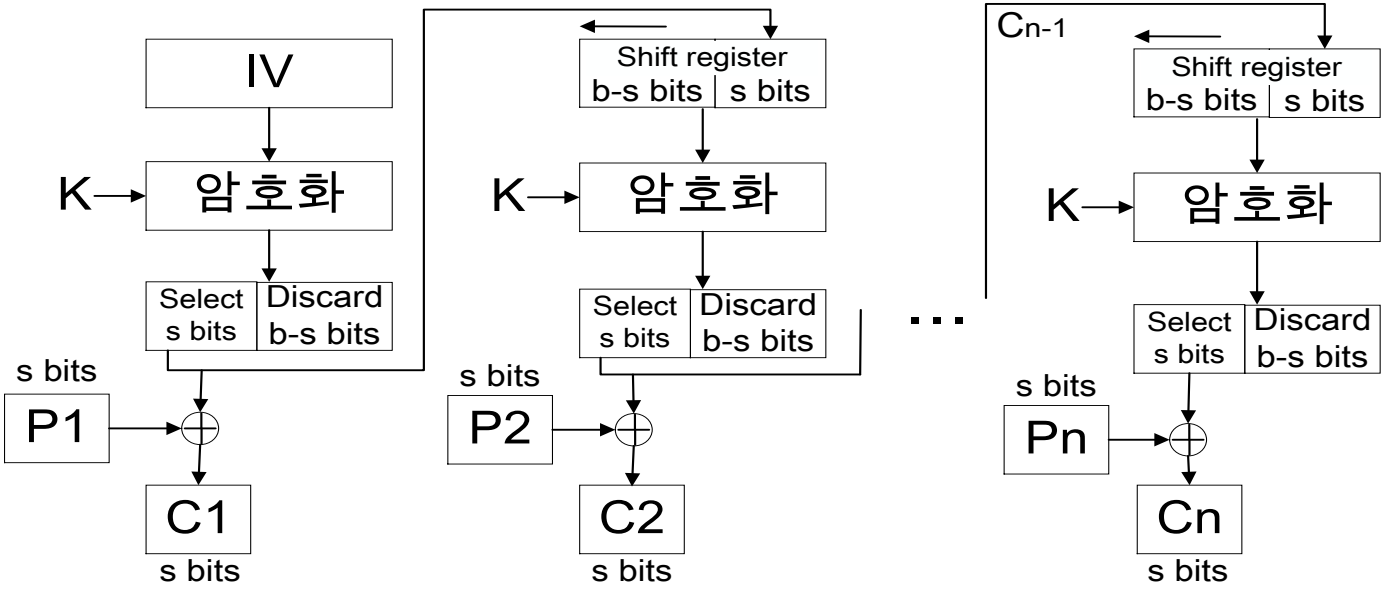


출력 피드백 모드

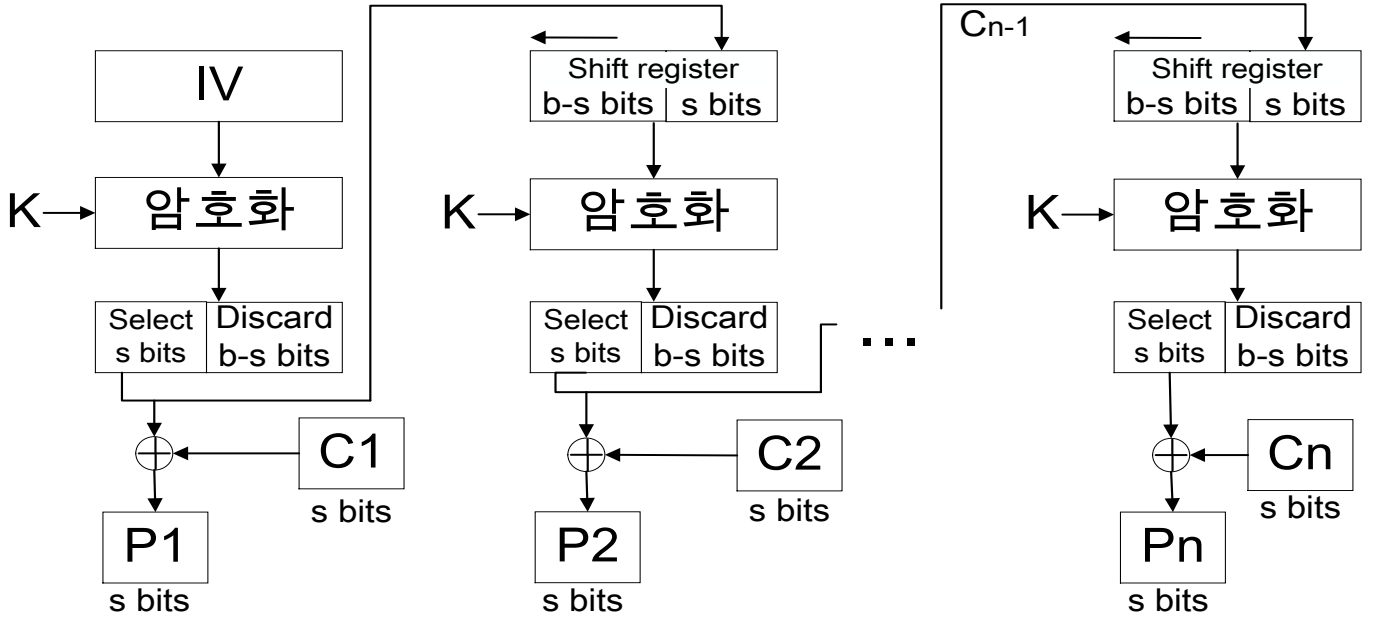
- 출력 피드백 모드 (OFB, Output FeedBack mode)
  - 암호화 함수에서 출력을 다음 암호화 과정 입력으로 넣음
  - 평문 블록과 암호 알고리즘의 출력을 XOR 연산
  - 평문 블록은 암호 알고리즘에 의해 직접 암호화되고 있는 것은 아님

출력 피드백 모드

a)암호화



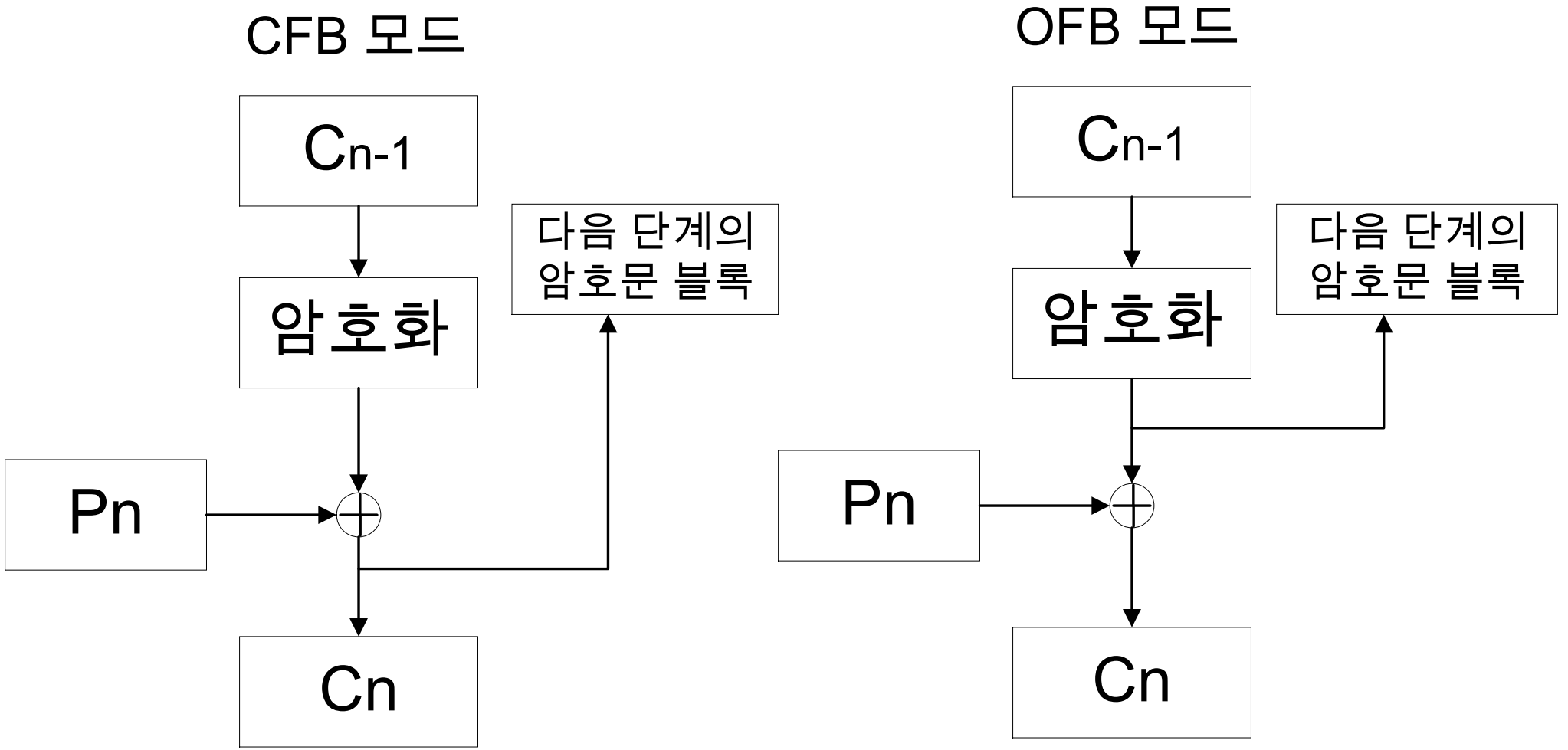
b)복호화



출력 피드백 모드

- OFB의 특성
  - 장점
    - 오류 확산 없음
    - 패딩 필요 없음
    - 암호화와 복호화가 같은 구조
  - 단점
    - 병렬 처리 할 수 없음

CFB 모드와 OFB 모드의 비교

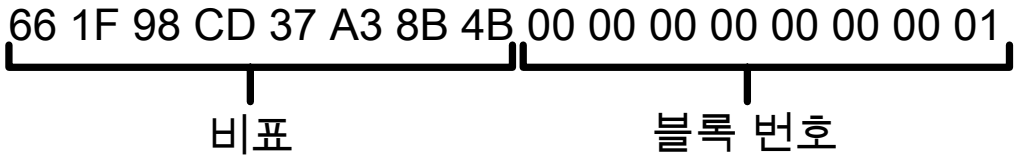


카운터 모드

- 카운터 모드 (CTR, Counter mode)
  - 평문 블록과 동일한 크기의 카운터 사용
  - 카운터가 암호화할 블록마다 값이 달라야함
  - 초기값으로 사용할 카운터 값 결정한 다음, 그 다음 블록은 이전 카운터 값에 1을 더하여 만듦
  - 카운터를 암호화하고 평문 블록과 XOR하여 암호블록 생성
  - 복호화 할 때 동일한 카운터 값 이용

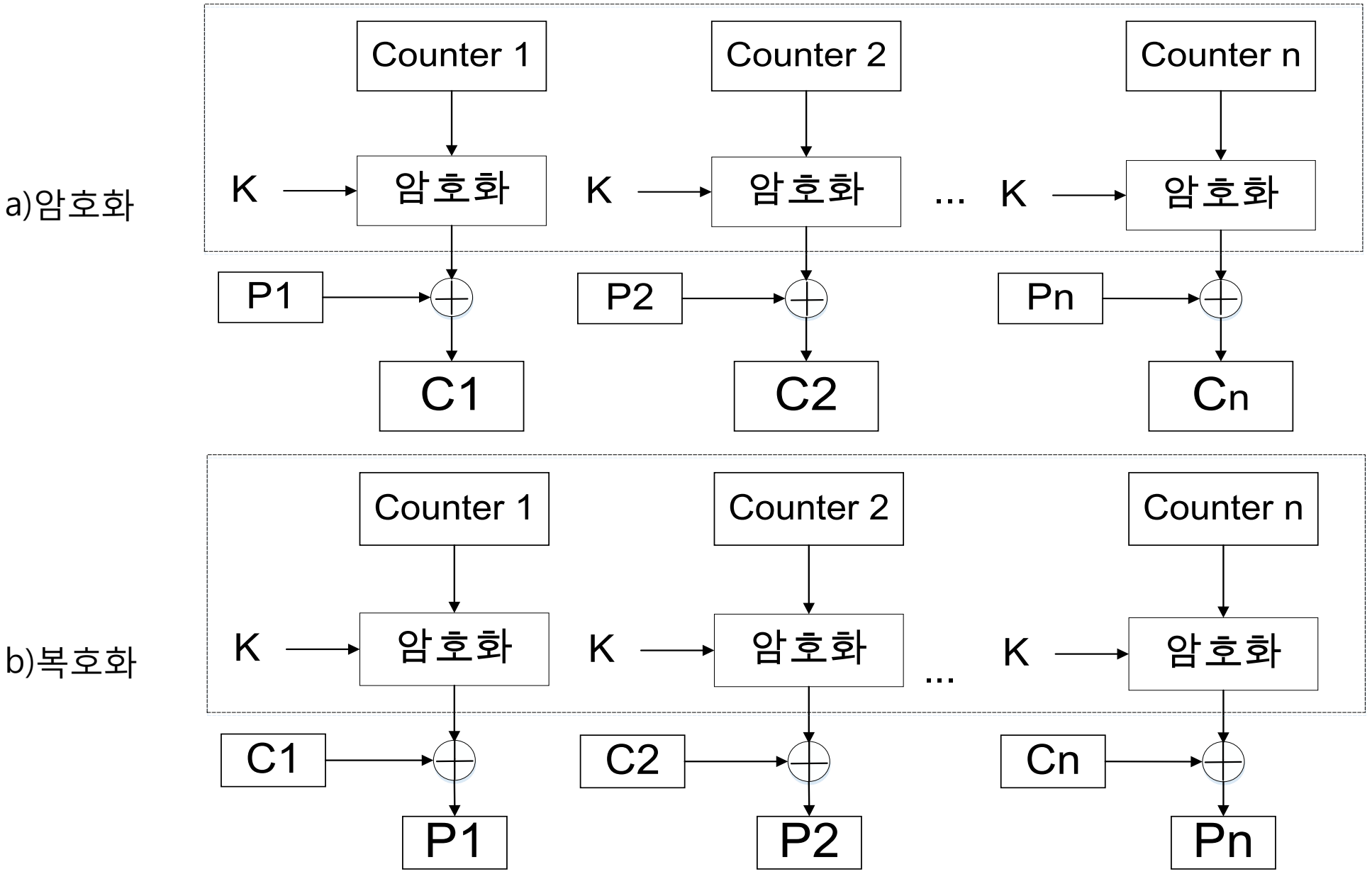
카운터 모드

- 카운터 초기화
  - 암호화 때마다 다른 값을 기초로 해서 작성
  - ex) 블록 길이가 128비트(16바이트)인 경우 카운터의 초기 값



  - 앞부분의 8바이트는 비표로 암호화 때마다 다른 값
    - 비표(nonce) : 한번만 사용하는 랜덤한 값
  - 후반 8바이트는 블록 번호로 하나씩 증가

카운터 모드


a)암호화
Counter 1
Counter 2
Counter n
K
암호화
K
암호화
...
K
암호화
P1
P2
Pn
C1
C2
Cn
b)복호화
Counter 1
Counter 2
Counter n
K
암호화
K
암호화
...
K
암호화
C1
C2
Cn
P1
P2
Pn

카운터 모드

- CTR의 특성
  - 장점
    - 병렬 처리 가능
    - 패딩 필요 없음
    - 랜덤하게 접근하여 처리 가능
    - 카운터 초기값이 실행 할 때 마다 달라 해독이 어려움
    - 오류 확산 없음

암호 블록 운용 모드

- 암호 블록 운용 모드 정리

모드 종류	병렬 처리	랜덤 접근	오류 확산	패딩	초기화 벡터
ECB	암호화, 복호화	암호화, 복호화	대응 블록	필요	불필요
CBC	복호화	복호화	암호화시 전체	필요	필요
CFB	복호화	복호화	복호화시 해당 블록과 다음 블록	불필요	필요
OFB	X	X	대응 블록	불필요	필요
CTR	암호화, 복호화	암호화, 복호화	대응 블록	불필요	불필요

감사합니다!