2023/02/03, 2023 겨울방학 보안 기초 세미나

Network Security Essentials

- Chapter_2 대칭 암호와 메시지 기밀성(2) -

김 지 혜(jihye@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

보충

- 암호 개념
  - 암호화 유형
    - 사용되는 키의 수에 따른 암호 방식
      - 대칭 암호(Symmetric Encryption)
        - 송수신자가 동일한 키를 가지고 암호화/복호화하는 방식
      - 비대칭 암호(Asymmetric Encryption)
        - 송수신자가 서로 다른 키를 가지고 암호화/복호화하는 방식

특징	대칭 암호	비대칭 암호
속도	상대적으로 빠름	상대적으로 느림
키 관계	암호 키 = 복호 키	암호 키 != 복호 키
키 전송	필요	불필요
키 길이	키 길이가 짧음	키 길이가 김
대표 알고리즘	e.g., DES, AES	e.g., Diffie-Hellman, RSA

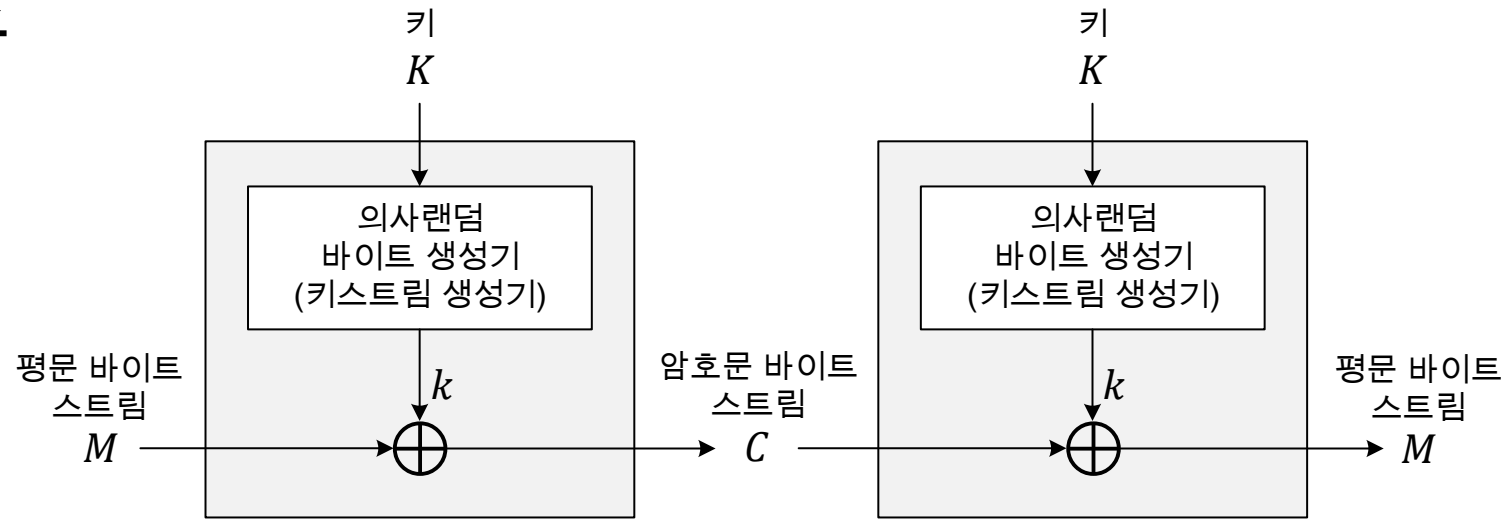
목 차

스트림 암호와 RC4

- 스트림 암호(Stream Cipher)
  - 정의
    - 연속적인 비트/바이트/워드를 순차적으로 암호화/복호화 하는 방식
  - 특징
    - 한 번에 한 비트 혹은 바이트씩 암/복호화
    - 패딩(Padding) 처리 불필요
    - 실시간 처리 가능하여 오디오 및 비디오 스트리밍에 사용
    - 대표적으로 RC4 알고리즘 사용

스트림 암호와 RC4

- 스트림 암호(Stream Cipher)
  - 구조



	11001100	평문
⊕	01101100	키스트림
	10100000	암호문

	10100000	암호문
⊕	01101100	키스트림
	11001100	평문

스트림 암호와 RC4

- 스트림 암호(Stream Cipher)
  - 설계 요구사항
    - 암호열의 주기가 길어야 함
      - 의사랜덤 바이트 생성기를 통해 생성되는 키스트림에 의한 주기
    - 키스트림은 진성 랜덤 스트림의 특성에 근사해야 함
      - e.g., 0이나 1의 개수가 거의 동일해야 함(무작위성)
    - 키의 길이는 충분히 길어야 함
      - 최소 128비트 이상 권장

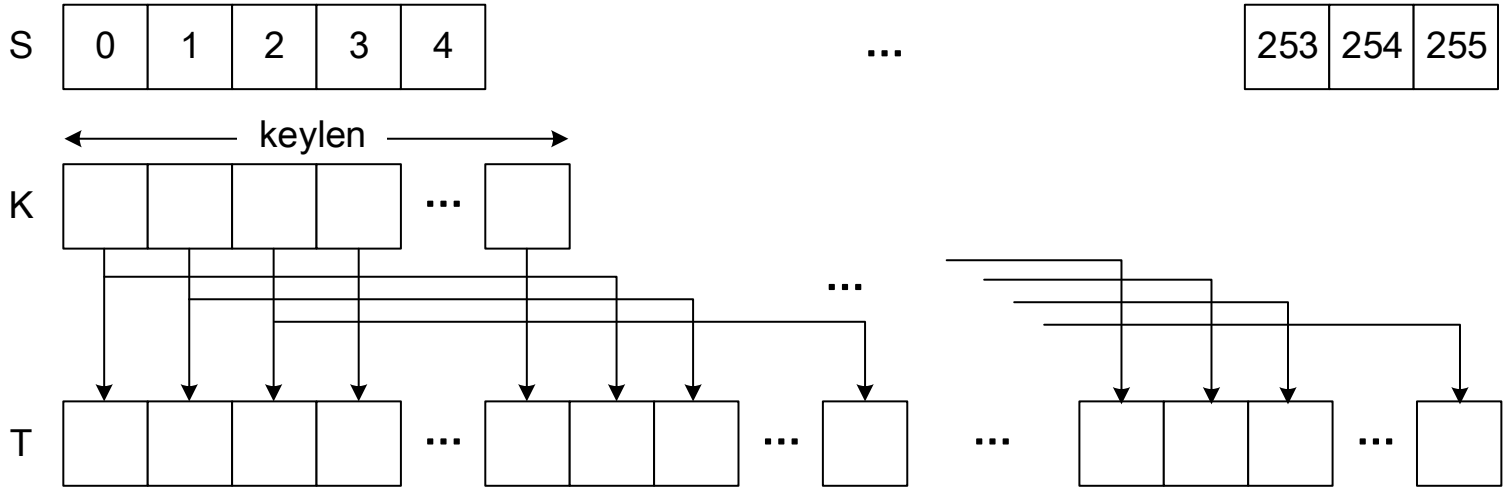
스트림 암호와 RC4

- RC4 알고리즘
  - 정의
    - Ron Rivest가 설계한 바이트 단위의 가변적인 키를 사용하는 스트림 암호 알고리즘
  - 특징
    - 연산 속도가 빠름
      - 한 바이트 출력을 위해 8~16번의 연산 수행
    - SSL/TLS(Secure Socket Layer/Transport Layer Security) 표준에서 사용
      - 웹 브라우저와 서버 간 통신 표준
    - WEP(Wired Equivalent Privacy)프로토콜과 WPA(WiFi-Protocol Access) 프로토콜에서 사용
      - 무선랜 표준(IEEE 802.11)

스트림 암호와 RC4

- RC4 알고리즘
  - 동작 과정(1/3)
    1. S와 T의 초기 상태
       - 벡터 S에 0~255를 오름차순으로 정렬
       - 임시 벡터 T 생성
       - 키 K를 길이(keylen)만큼 벡터 T로 이동

```
/*Initialization*/
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

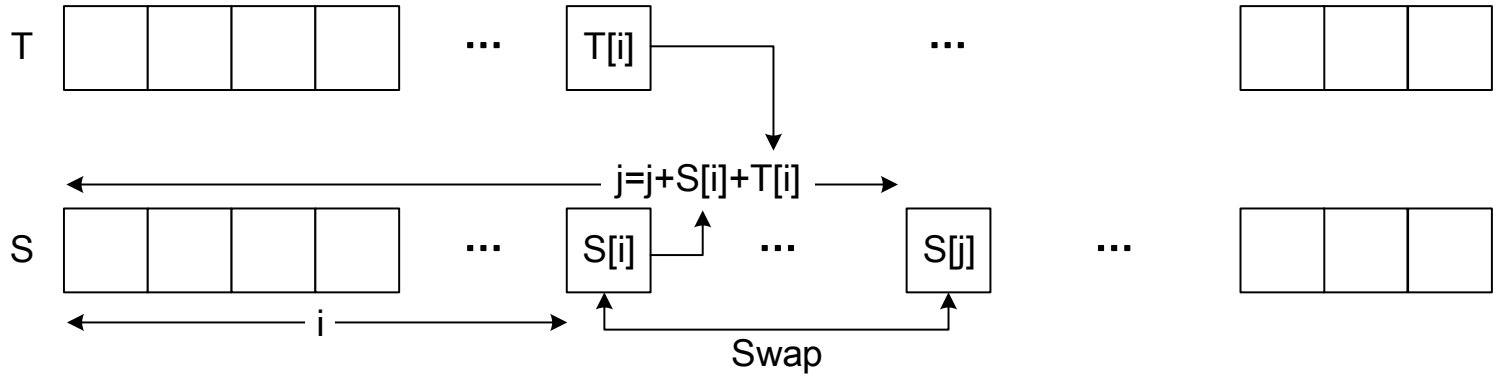


(a) S와 T의 초기 상태

스트림 암호와 RC4

- RC4 알고리즘
  - 동작 과정(2/3)
    2. S의 초기 치환
       - 벡터 T, S의 현재 위치(i)를 이용하여 교환할 위치(j) 계산
       - S[i]와 S[j]의 위치 교환

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

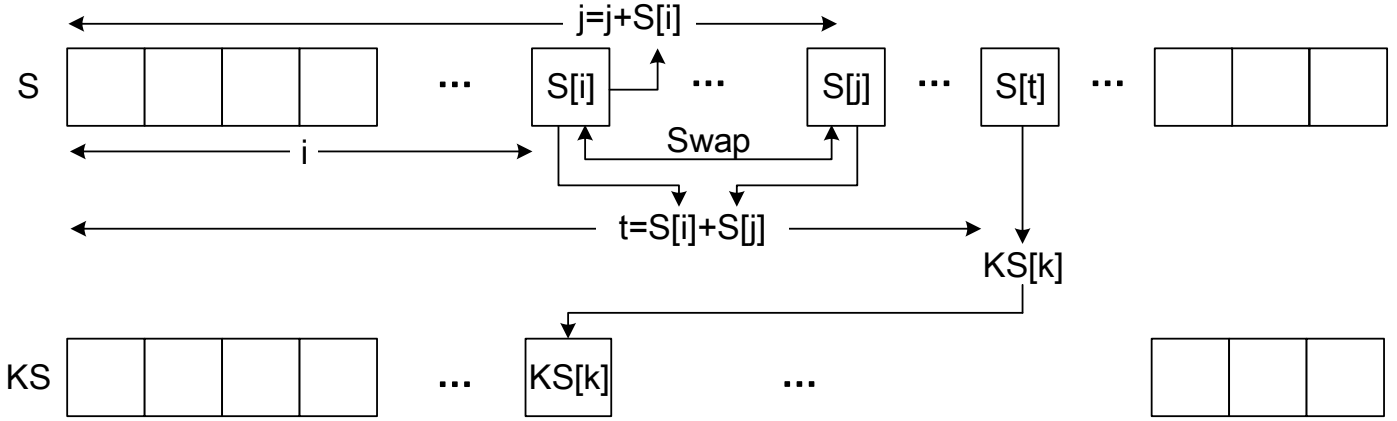


(b) S의 초기 치환

스트림 암호와 RC4

- RC4 알고리즘
  - 동작 과정(3/3)
    3. 스트림 생성
       - 벡터 S의 현재 위치(i)를 이용하여 교환할 위치(j) 계산
       - S[i]와 S[j]의 위치 교환
       - 벡터 S의 i, j를 이용하여 키스트림 KS 값이 될 벡터 S의 위치(t) 계산
       - 현재 키스트림 KS 위치(k)에 S[t] 저장

```
/*Stream Generation*/
i,j,k = 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;
  KS[k] = S[t];
```



(c) 스트림 생성

목 차

- 보충
  - 암호 개념
- 스트림 암호와 RC4
- 암호 블록 운용 모드

암호 블록 운용 모드

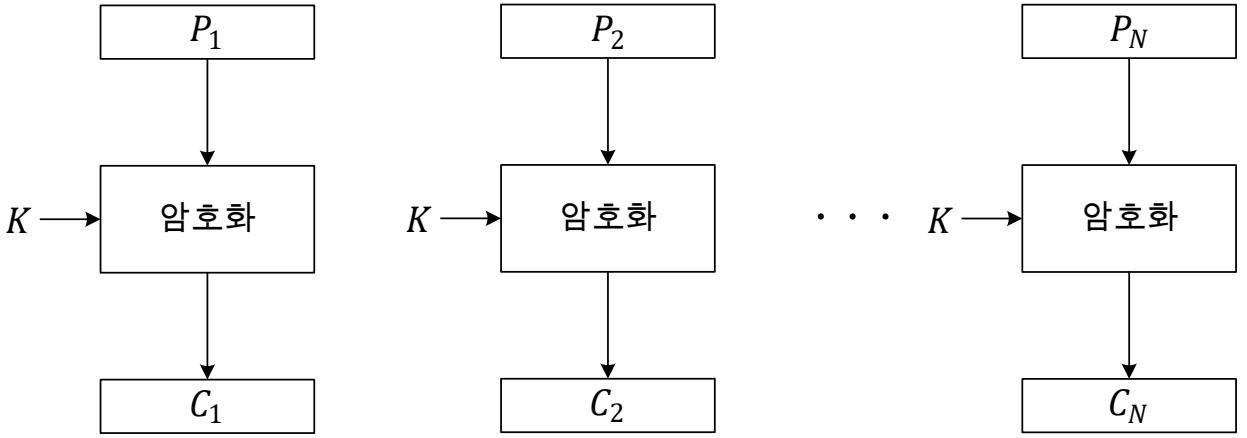
- 개요
  - 정의
    - 평문 길이가 블록 암호의 블록 크기보다 큰 경우를 해결하기 위해 NIST에서 정의한 블록 암호 사용 방식
  - 종류
    - 전자 코드북(ECB, Electronic CodeBook) 모드
    - 암호 블록체인(CBC, Cipher Block Chaining) 모드
    - 암호 피드백(CFB, Cipher FeedBack) 모드
    - 출력 피드백(OFB, Output FeedBack) 모드
    - 카운터(CTR, Counter) 모드

암호 블록 운용 모드

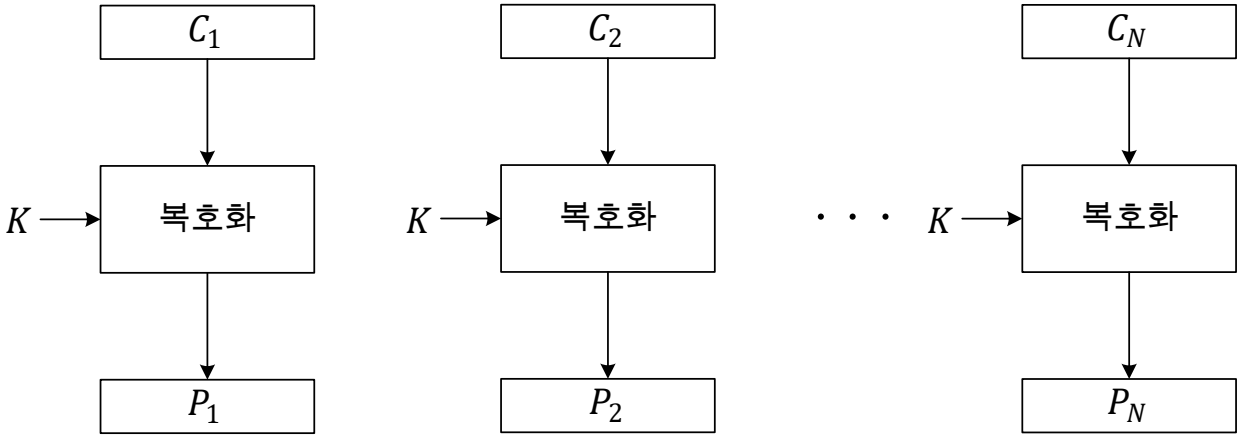
- ECB(Electronic Codebook)
  - 정의
    - 평문 블록을 그대로 암호화하는 방식
  - 특징
    - 평문 크기가 블록 크기의 정수배가 아닌 경우, 패딩(Padding)
    - 각 블록은 동일한 암/복호화 키 사용
    - 각 블록은 독립적, 순차적으로 암/복호화 수행
      - 한 블록에서 오류가 발생해도 다른 블록에 영향을 주지 않음

암호 블록 운용 모드

- ECB(Electronic Codebook)
  - 암호화 방식
    - $C_i = E(K, P_i)$

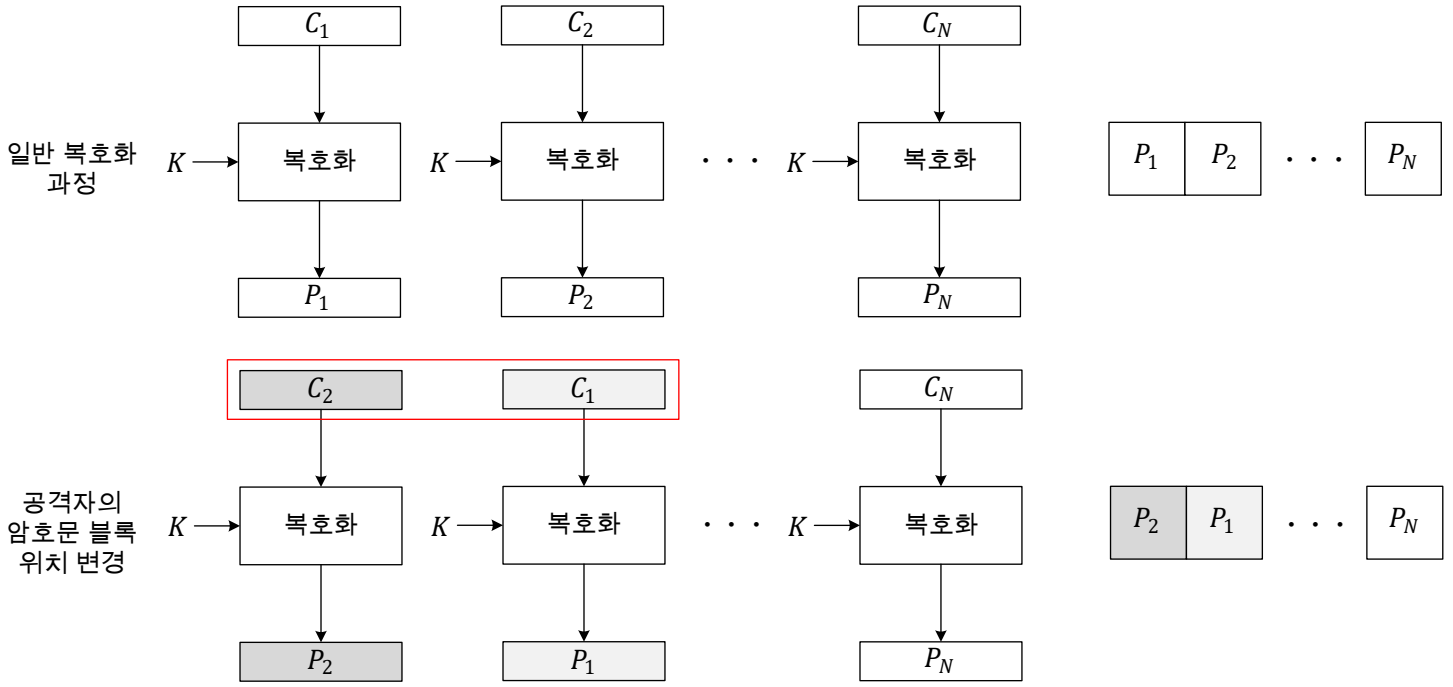


  - 복호화 방식
    - $P_i = D(K, C_i)$



암호 블록 운용 모드

- ECB(Electronic Codebook)
  - ECB 모드에 대한 공격
    - 공격자가 암호문 블록을 서로 바꾸는 경우, 수신자가 복호화 한 평문 블록 구조도 변경됨
      - 공격자는 한 블록의 내용만 알고 있어도 공격 가능

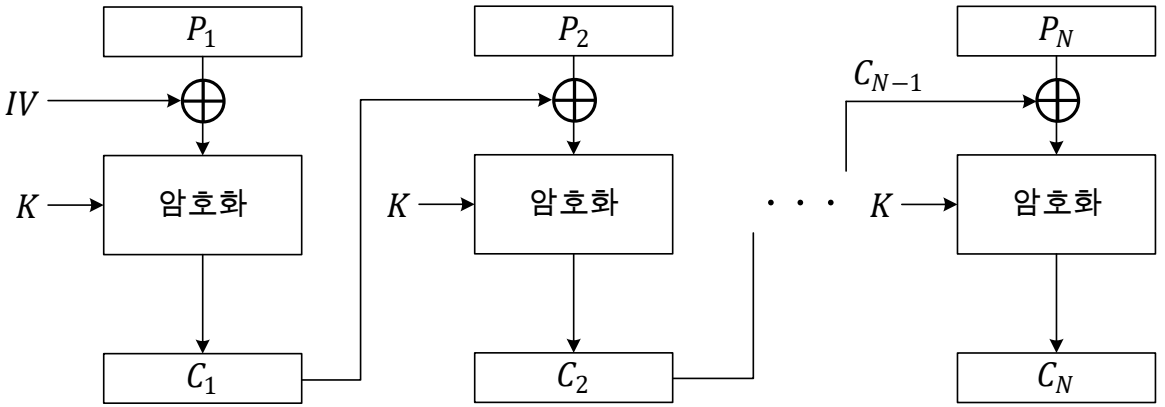


암호 블록 운용 모드

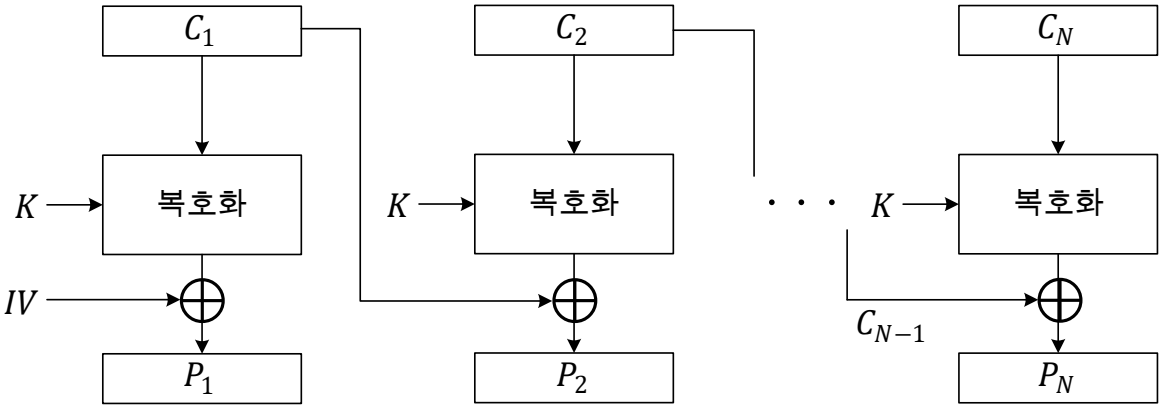
- CBC(Cipher-Block Chaining)
  - 정의
    - 이전 암호문 블록과 평문 블록을 XOR 연산한 후 암호화하는 방식
  - 특징
    - 초기화 벡터(IV, Initialization Vector)를 가짐
      - 최초의 암호화 시, 암호문으로 사용
    - 암호화는 순차적, 복호화는 병렬적 처리
    - 평문 블록이 동일한 경우, 암호문이 같아짐
    - 패딩(Padding) 필요함
    - 오류가 확산됨

암호 블록 운용 모드

- CBC(Cipher-Block Chaining)
  - 암호화 방식
    - $C_0 = IV$
    - $C_{i+1} = E\left(K, (C_i \oplus P_{i+1})\right)$

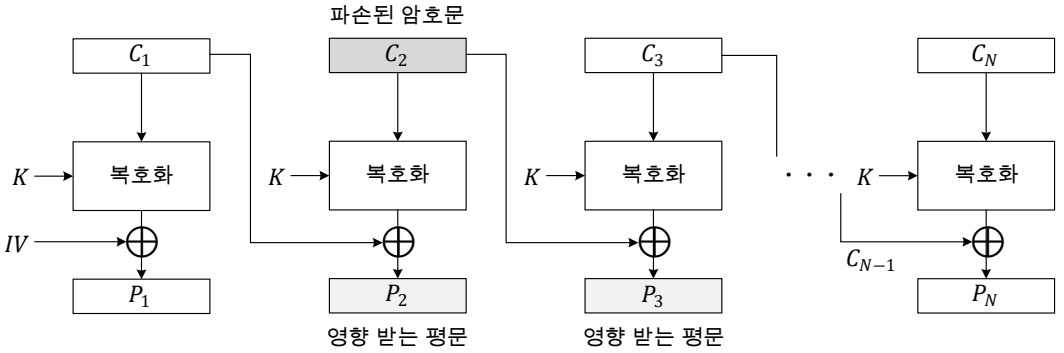


  - 복호화 방식
    - $C_0 = IV$
    - $P_{i+1} = D(K, C_{i+1}) \oplus C_i$

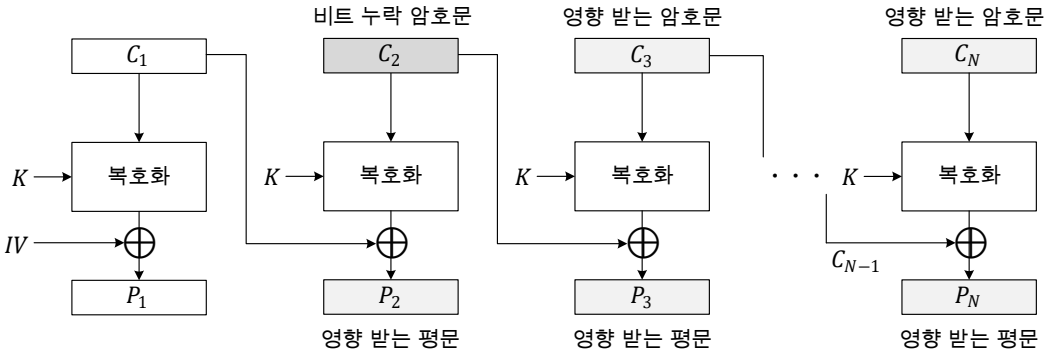


암호 블록 운용 모드

- CBC(Cipher-Block Chaining)
  - CBC 모드에 대한 공격
    - 암호문 블록 1개가 파손된 경우, 평문 블록 2개에 영향을 줌



    - 비트 누락된 암호문을 복호화하는 경우, 이후의 블록 전체에 영향을 줌

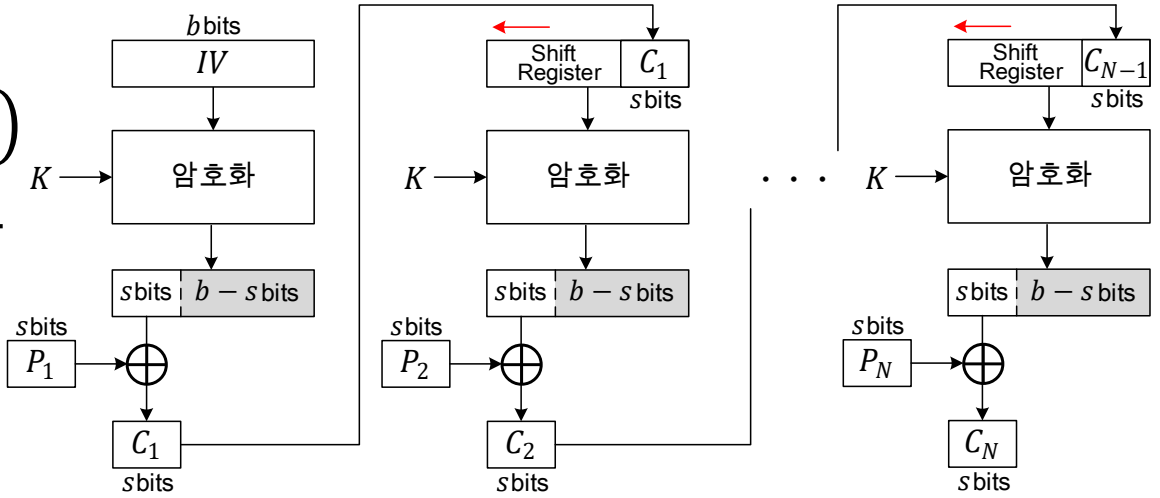


암호 블록 운용 모드

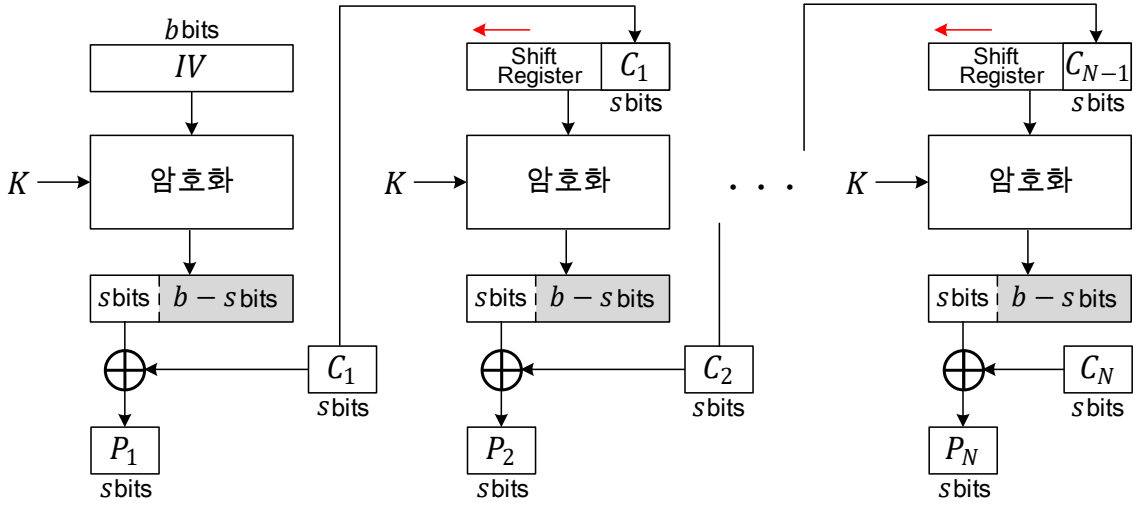
- CFB(Cipher-FeedBack)
  - 정의
    - 이전 암호문 블록을 암호화한 후 평문 블록과 XOR 연산하는 암호화하는 방식
  - 특징
    - 초기화 벡터(IV, Initialization Vector)를 가짐
    - 패딩(Padding) 불필요함
      - 스트림 암호화처럼 구성하므로 평문과 암호문 길이 동일
    - 암호 알고리즘만 사용
    - 암호화는 순차적, 복호화는 병렬적 처리
    - 오류가 확산됨

암호 블록 운용 모드

- CFB(Cipher-FeedBack)
  - 암호화 방식
    - $C_{i+1} = P_{i+1} \oplus S_s\left(E(K, C_i)\right)$
    - $S_s(X) =$ X의 가장 왼쪽 비트

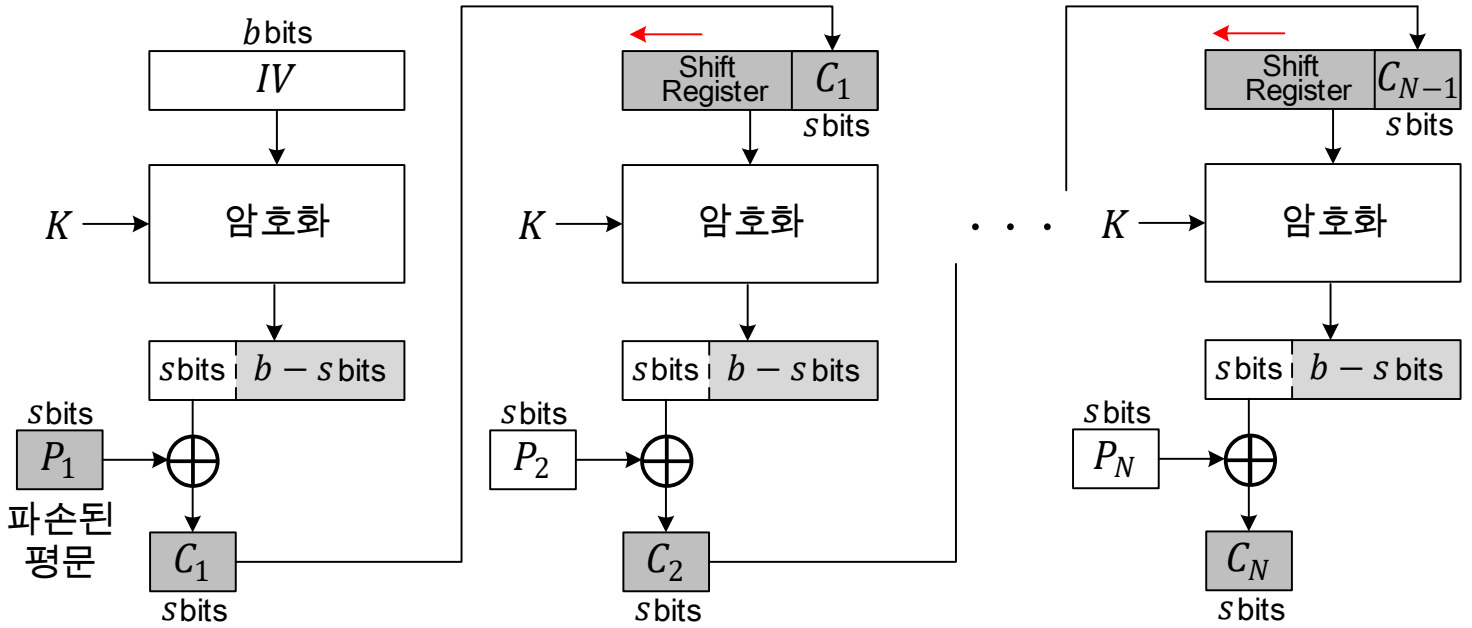


  - 복호화 방식
    - $P_{i+1} = C_{i+1} \oplus S_s\left(E(K, C_i)\right)$



암호 블록 운용 모드

- CFB(Cipher-FeedBack)
  - CFB에 대한 공격
    - 평문 블록 1개가 파손된 경우, 이후의 암호문 블록 전체에 영향을 줌

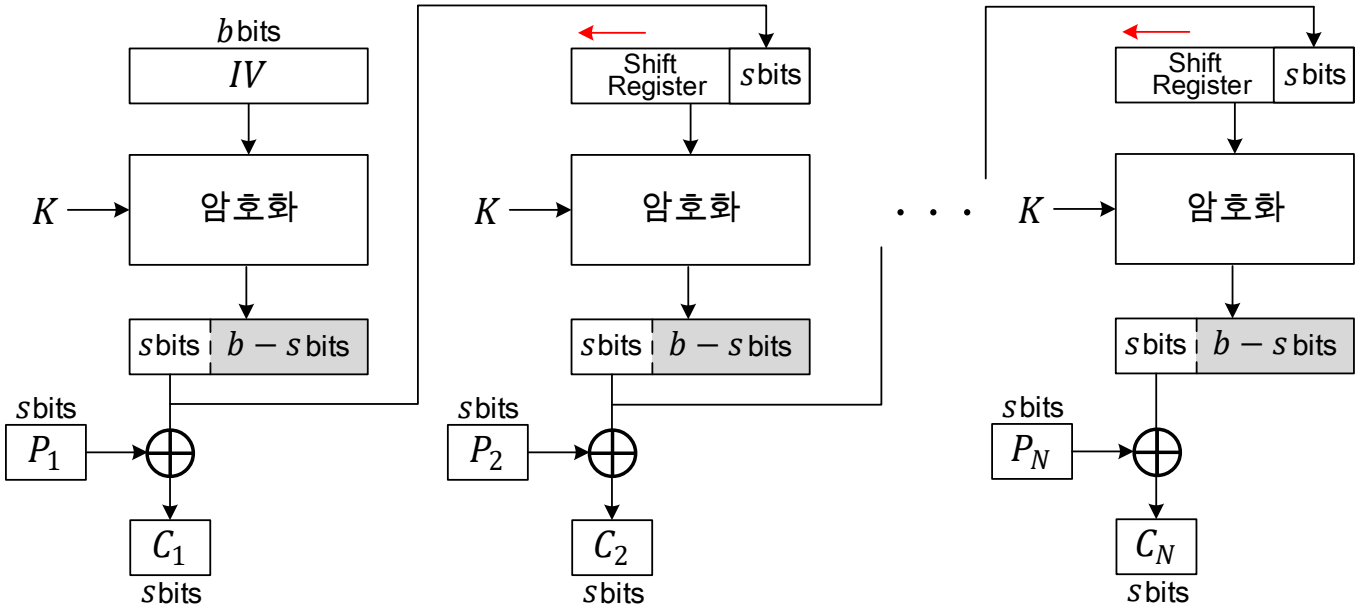


암호 블록 운용 모드

- OFB(Output-FeedBack)
  - 정의
    - 이전 암호 알고리즘의 출력 값을 이용하여 암호화한 후 평문 블록과 XOR 연산하는 암호화하는 방식
  - 특징
    - ECB, CBC, CFB 모드의 한계 개선
    - 초기화 벡터(IV, Initialization Vector)를 가짐
    - 패딩(Padding) 불필요함
      - 스트림 암호화처럼 구성하므로 평문과 암호문 길이 동일
    - 암/복호화 구조가 동일
    - 순차적으로 암/복호화 수행

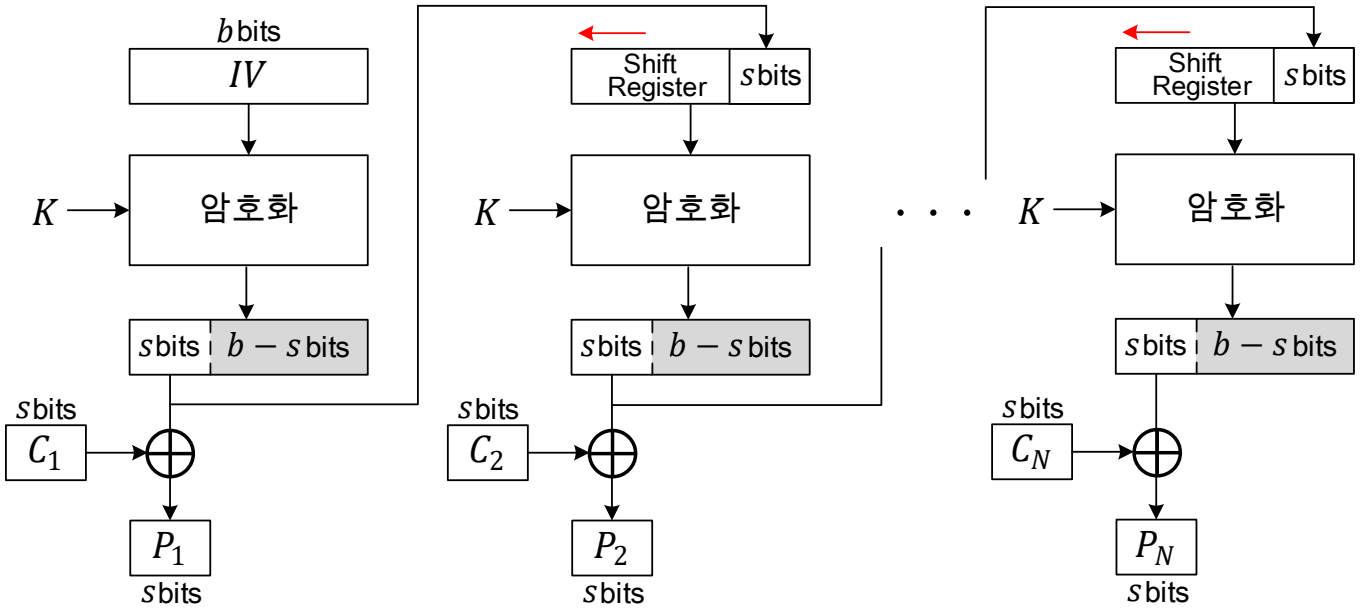
암호 블록 운용 모드

- OFB(Output-FeedBack)
  - 암호화 방식
    - $C_{i+1} = P_{i+1} \oplus (S_s)_i \left(E(K, (S_s)_{i-1}) \right)$



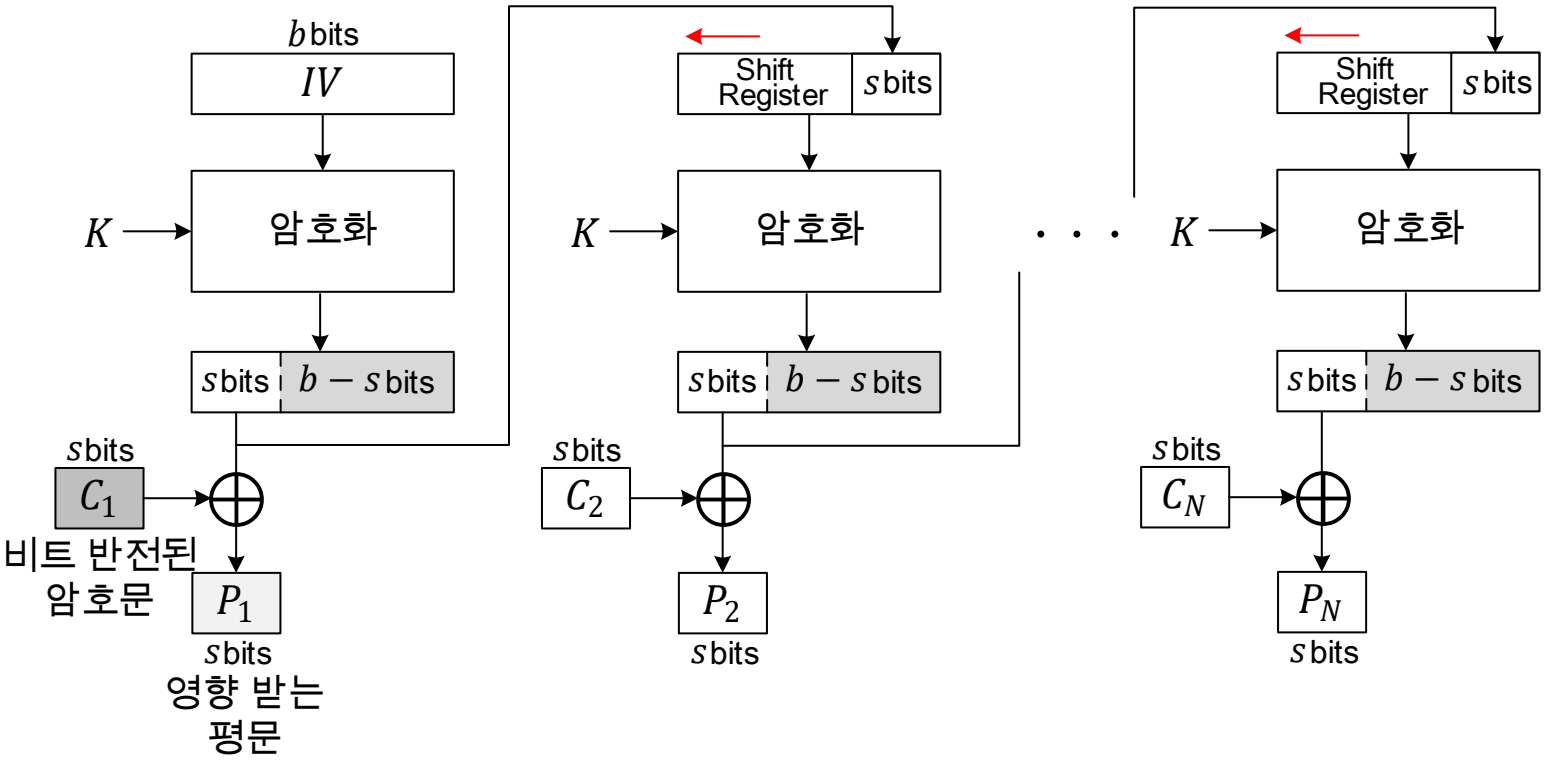
암호 블록 운용 모드

- OFB(Output-FeedBack)
  - 복호화 방식
    - $P_{i+1} = C_{i+1} \oplus (S_s)_i \left(E(K, (S_s)_{i-1}) \right)$



암호 블록 운용 모드

- OFB(Output-FeedBack)
  - OFB에 대한 공격
    - 비트가 반전된 암호문 블록을 복호화에 사용하는 경우, 대응하는 평문 블록 비트도 반전됨



암호 블록 운용 모드

- CTR(CounTeR)
  - 정의
    - 카운터(Counter)를 암호화한 후, 평문 블록을 XOR 연산하여 암호화하는 방식
  - 특징
    - 평문 블록과 동일한 크기의 카운터(Counter) 사용
      - 카운터 값은 평문 블록별로 달라야 함
    - 패딩(Padding) 불필요함
      - 스트림 암호화처럼 구성하므로 평문과 암호문 길이 동일
    - 암/복호화 구조가 동일
    - 각 블록은 독립적, 순차적으로 암/복호화 수행
    - 임의의 순서로 암/복호화 가능
      - 카운터의 블록 번호 이용

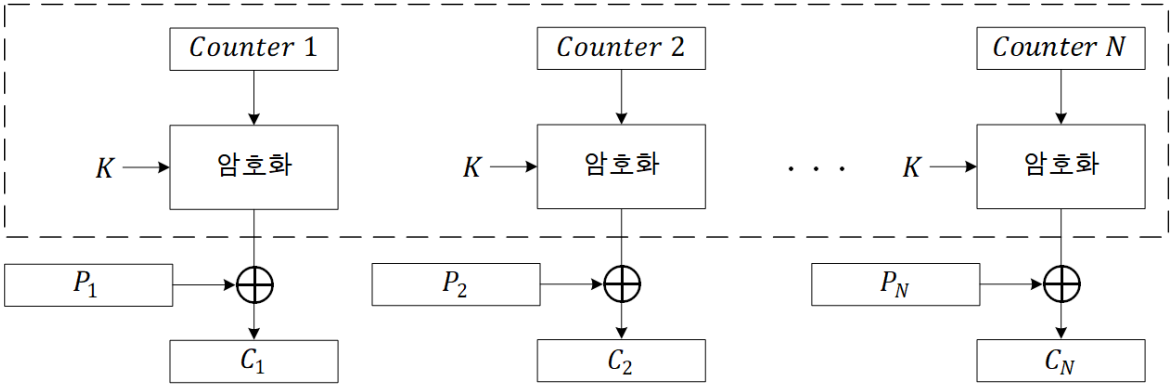
암호 블록 운용 모드

- CTR(CounTeR)
  - 카운터 값 생성 과정
    - 초기 값은 암호화 때마다 다른 값(비표)을 기초로 생성함
      - e.g., 128비트 블록의 카운터 초기값

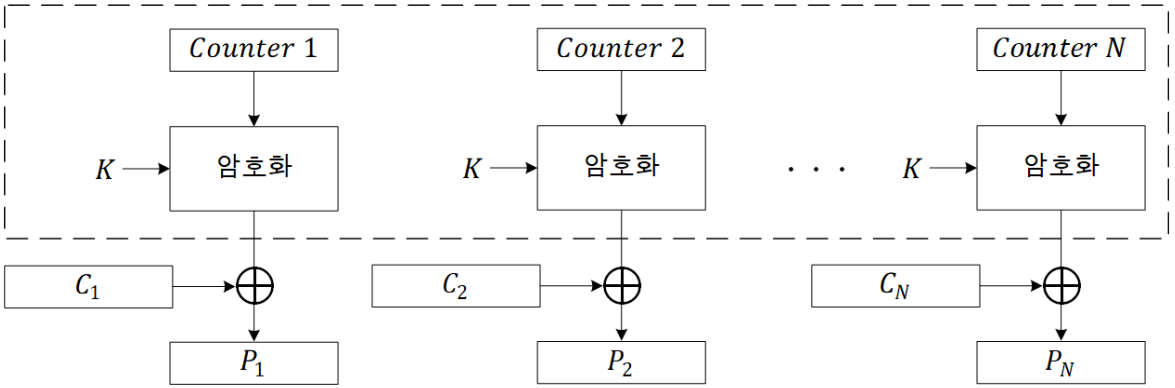
66 1F 98 CD 37 A3 8B 4B	00 00 00 00 00 00 00 01	
비표	블록 번호	
66 1F 98 CD 37 A3 8B 4B	00 00 00 00 00 00 00 01	카운터 1(초기값)
66 1F 98 CD 37 A3 8B 4B	00 00 00 00 00 00 00 02	카운터 2
66 1F 98 CD 37 A3 8B 4B	00 00 00 00 00 00 00 03	카운터 3
66 1F 98 CD 37 A3 8B 4B	00 00 00 00 00 00 00 04	카운터 4

암호 블록 운용 모드

- CTR(CounTeR)
  - 암호화 방식
    - $C_i = P_i \oplus E(K, Counter)$

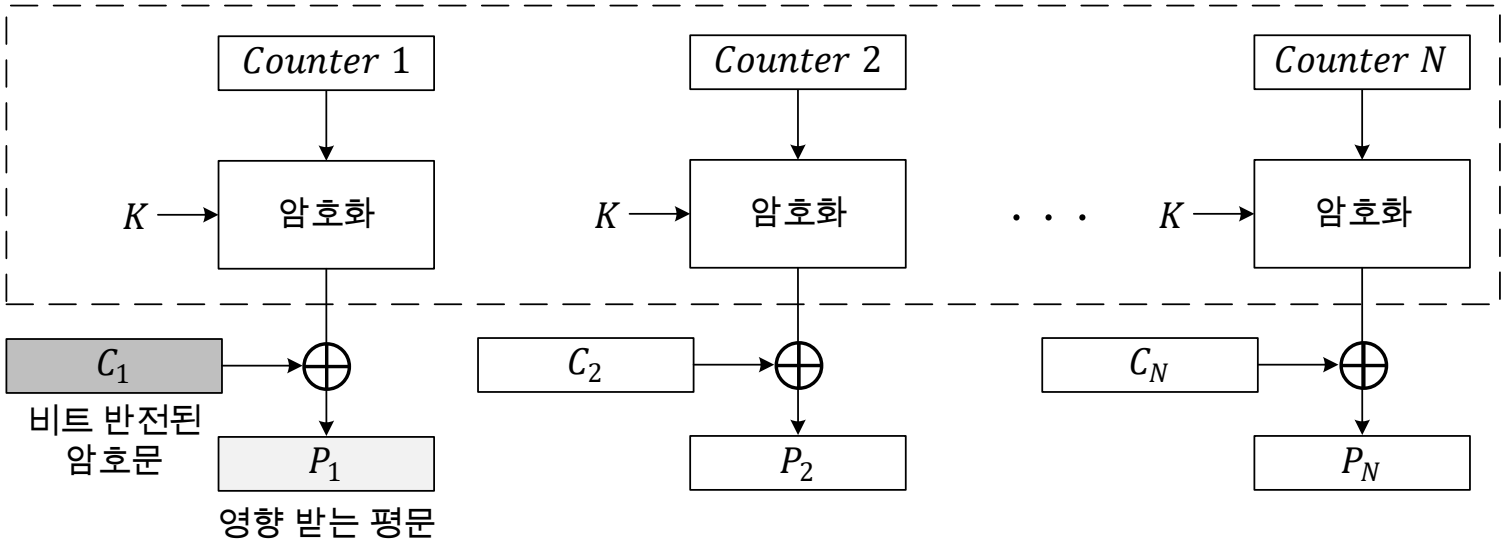


  - 복호화 방식
    - $C_i = P_i \oplus E(K, Counter)$



암호 블록 운용 모드

- CTR(CounTeR)
  - CTR에 대한 공격
    - 비트가 반전된 암호문 블록을 복호화에 사용하는 경우, 대응하는 평문 블록 비트도 반전됨



암호 블록 운용 모드

- 운용 모드 비교

	ECB	CBC	CFB	OFB	CTR
패딩 처리	O	O	X	X	X
병렬 처리	O	복호화만	복호화만	X	O
오류 전파	X	O	O	X	X
암호 알고리즘 입력값	평문 블록	이전 암호문 블록⊕평문 블록	이전 암호문 블록	이전 암호 알고리즘 출력값	카운터 값
복호 알고리즘 사용	O	O	X	X	X
사용 여부	사용하면 안됨	권장	현재 사용 X, CTR 권장	사용 O, CTR 권장	권장

Thanks!

김 지 혜 (jihye@pel.sejong.ac.kr)