국산 형태보존암호 FEA의 최적화 및 CTR모드운영

https://youtu.be/x75d3HflNMw

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

역사

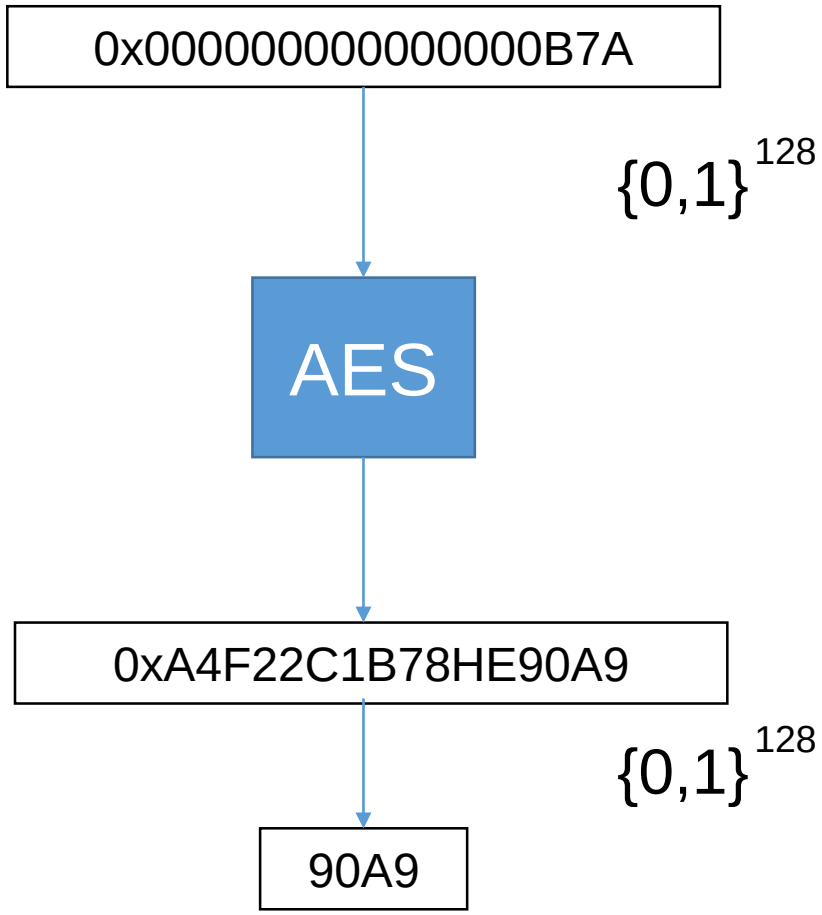
- 1981 년 미국국가표준국(이후 NIST로 이름 변경)은
  임의의 알파벳을 통해 임의의 문자열을 암호화하는 접근법을 설명한 FIPS 74 발명

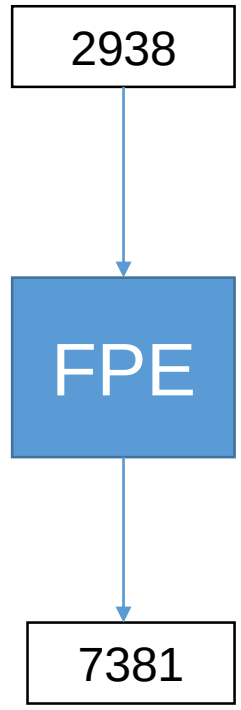
- Brightwell과 Smith가 1997년 FPE 문제와 그 효용성을 구체적으로 언급

- 2002년에 Black and Rogaway 가
  접두사 방식, 사이클 워킹 암호, 파이스텔 구조 등 세 가지 방법을 제안하는 논문을 발표

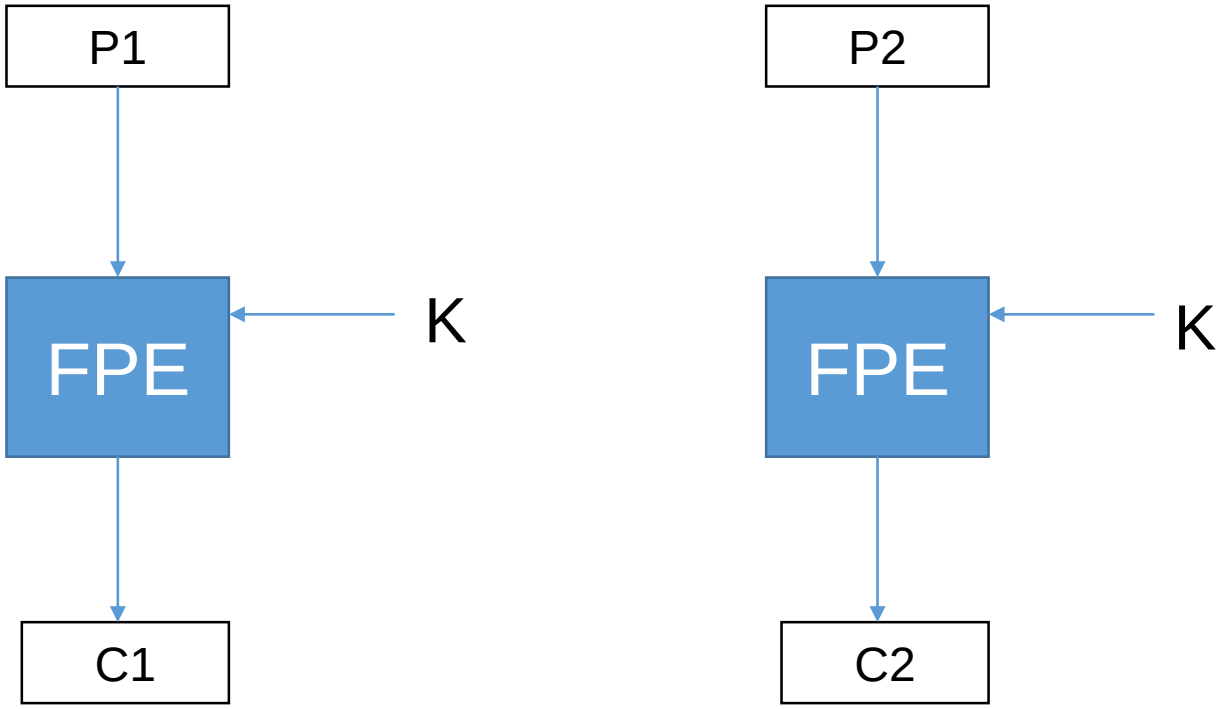
- FPE는 보안을 염두에 두고 설계되지 않은 기존의 중요한 인프라 시스템에 잠재적으로 보안을 제공
  (비 IP 네트워크에서 전송되거나 저장된 정보, 레거시 데이터베이스)

AES와 비교


0x000000000000000B7A
{0,1}128
AES
0xA4F22C1B78HE90A9
{0,1}128
90A9

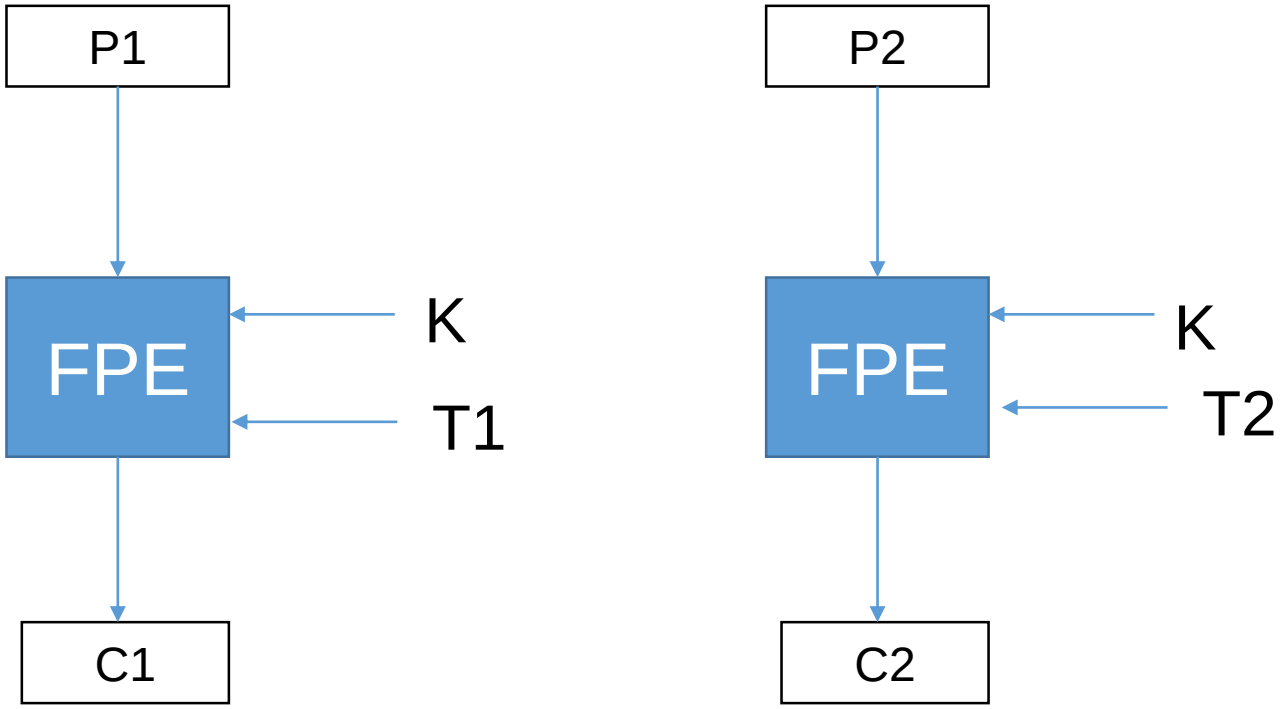

2938
FPE
7381

트윅



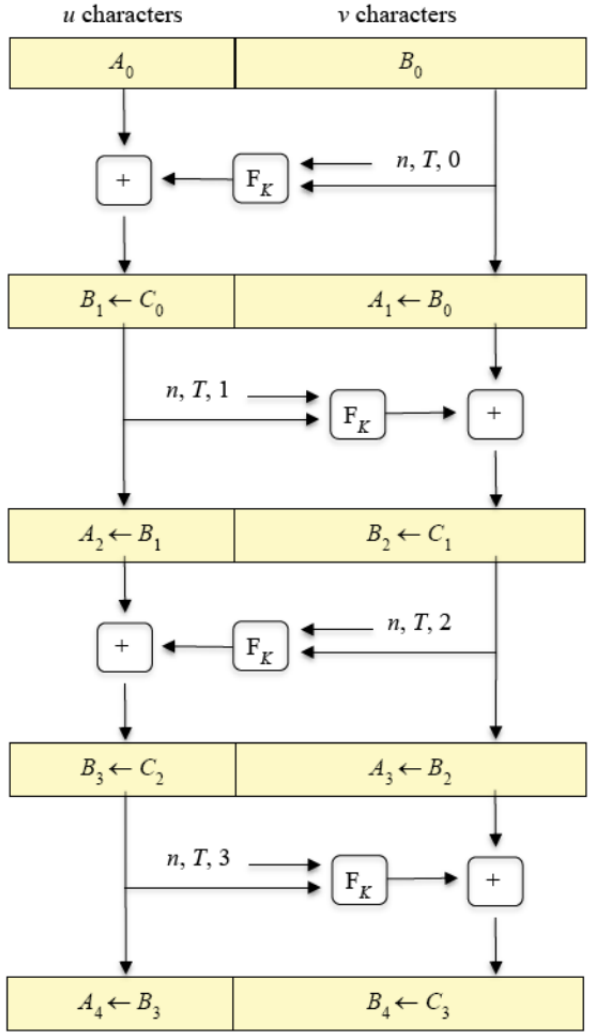
P1=P2, C1=C2

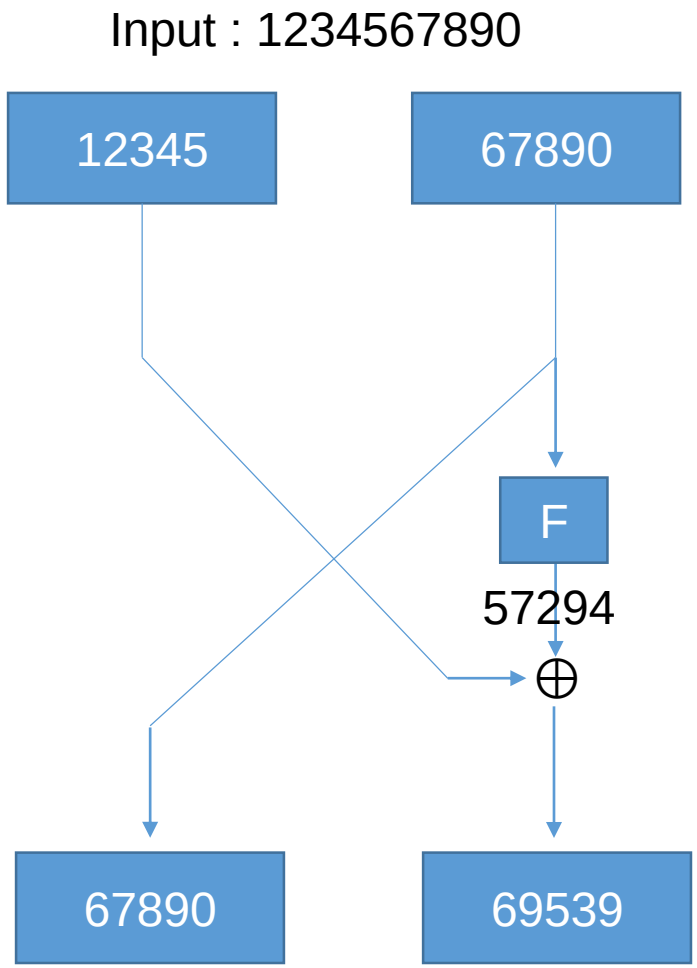
트윅



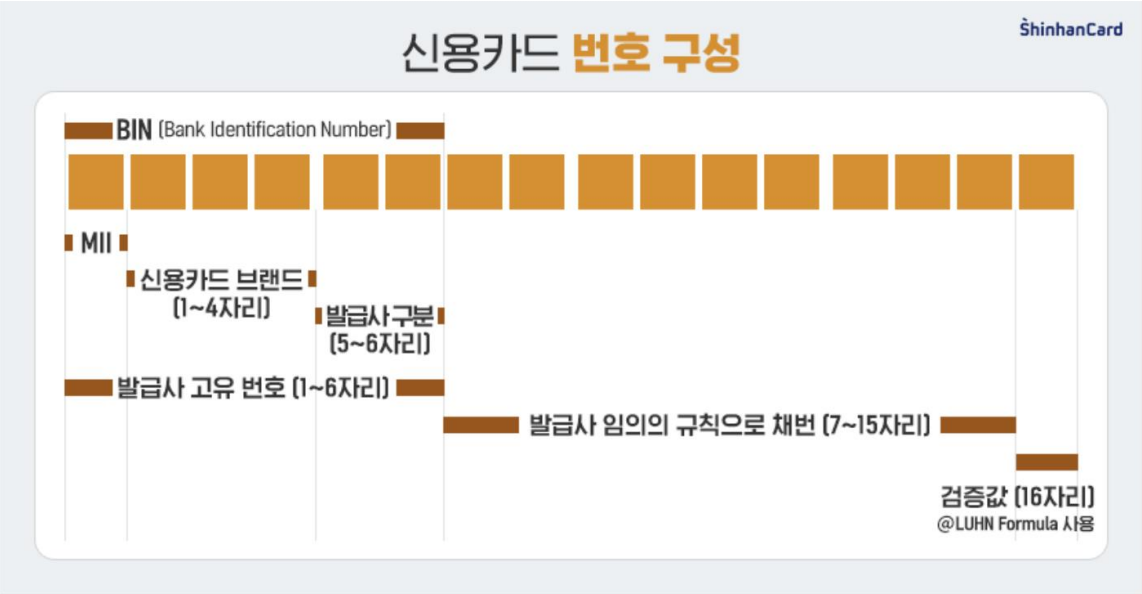
$P1=P2, T1 \neq T2 \quad C1 \neq C2$

파이스텔 기반 FPE


u characters
v characters
A_0
B_0
+
F_K
n, T, 0
$B_1 \leftarrow C_0$
$A_1 \leftarrow B_0$
n, T, 1
F_K
+
$A_2 \leftarrow B_1$
$B_2 \leftarrow C_1$
+
F_K
n, T, 2
$B_3 \leftarrow C_2$
$A_3 \leftarrow B_2$
n, T, 3
F_K
+
$A_4 \leftarrow B_3$
$B_4 \leftarrow C_3$

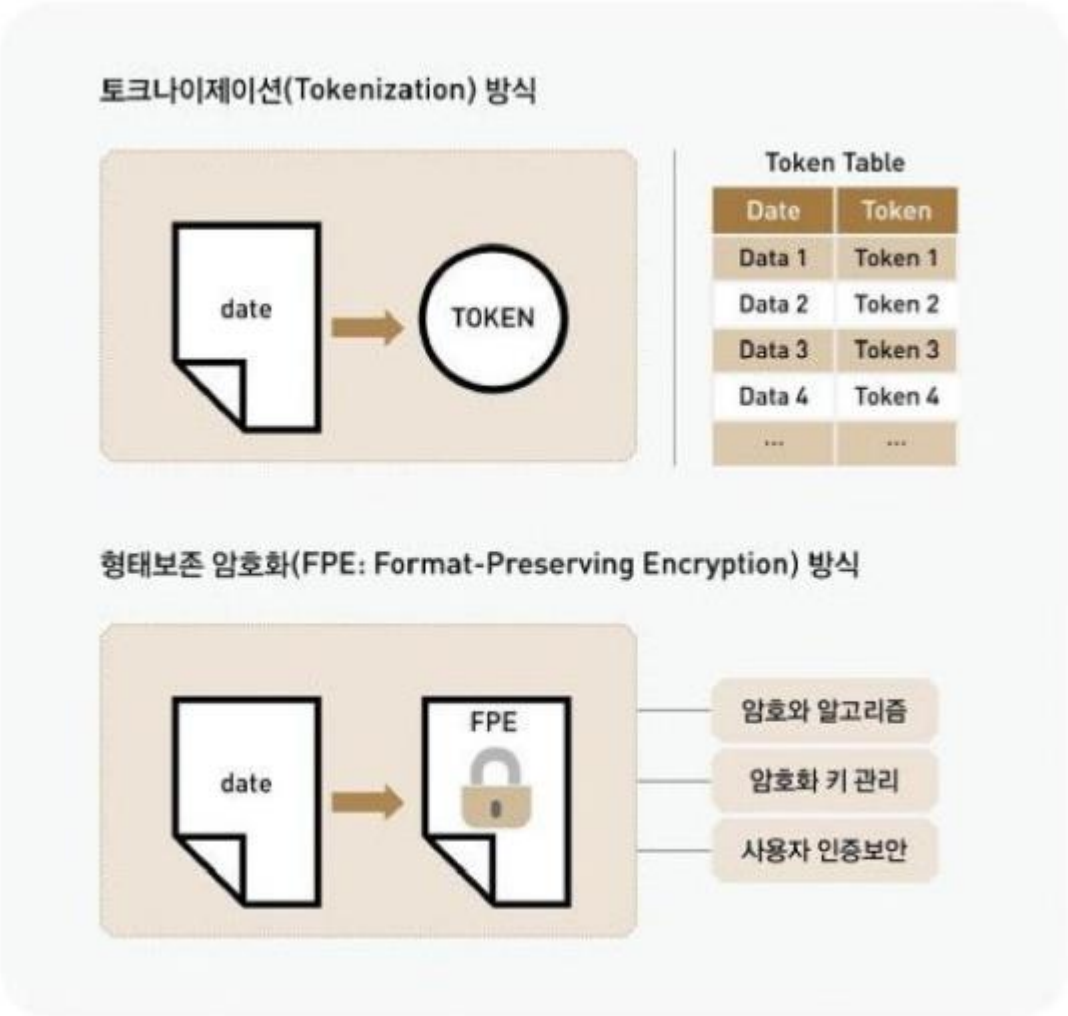

Input : 1234567890
12345
67890
F
57294
67890
69539

개인정보



- 건강관리 기록
- 주민등록번호 901111-1******
- 데이터베이스에는 절대 표시되면 안됨
- 알려진 생년월일을 검색하고 기록을 공개

토크나이제이션



- Tokenization
  민감한 실제 데이터 대신 랜덤 토큰으로 대체하여 사용

- 장점
  중요한 데이터만 따로 안전하게 보관 가능
- 단점
  별도의 시스템 사이에 통신이 필요
  1:1 매칭한 테이블이 존재 통신 구간에서 데이터가 오고 감

토크나이제이션

방식	토크나이제이션	FPE
구현 편의성	어려움	비교적 쉬움
키 분배	비교적 간단	어려움
시스템 성능 영향	성능 저하 확연	영향 거의 없음
생성된 토큰	무의미 토큰을 정보에 매핑	정보를 토큰으로 변경
정보 위치	암호화 서버	원래 저장 위치
토큰: 정보 연관성	암호화 서버에서 토큰과 매핑	알리고즘으로 암호화

- 암호화 장치를 내부에 탑재하여 연동
- 빠른 성능과 보안성
- FPE의 경우 토큰 정보가 실제 정보이기때문에 키관리가 중요

용도

Format Preserving JPEG/MPEG encryption https://shodhganga.inflibnet.ac.in/bitstream/10603/79598/18/18_chapter%206.pdf

- 상업적 가치를 파괴하는 정도의 암호화
- 성능 저하 없이 이미지나 비디오를 가리는 방법
- Rc4 사용

Degradation and encryption for outsourced PNG images in cloud storage

https://sci-hub.tw/10.1504/ijguc.2016.073773

- 클라우드 스토리지 환경에서 사용자는 이미지를 자주 저장하고 휴대 전화를 포함한 개인 장치로 이미지를 검색
- 클라우드 서버로 유출되어 사용자가 신뢰 문제 발생
- 민감한 이미지의 개인 정보를 보호하기 위해 PNG (Portable Network Graphics)의 형식 호환 저하 및 암호화 방법을 제안

PEG2000 암호화 https://www.ntu.edu.sg/home/wuhj/research/publications/2004_ICASSP_JPEG2000.pdf

- 이미지 압축 표준 중 하나 JPEG
- PEG2000이라는 훨씬 더 뛰어난 이미지 압축 표준
- 한 번 압축, 여러 가지 압축 풀기"기능입니다. 즉, 동일한 압축 코드 스트림에서 서로 다른 해상도, 품질 레이어 및 관심 영역 (ROI)을 가진 이미지 추출을 지원
- JPEG2000 구문을 사용하려면 암호화 된 패킷 본문에서 두 개의 연속 바이트가 0xFF8F보다 크지 않아야함
- 마커 스트림 SOP (패킷 시작) 및 마커 EPH (패킷 헤더의 끝)를 제외하고 코드 스트림의 구분 마커 코드 (이들 모두 0xFF90 ~ 0xFFFF 범위에 있음)가 나타나지 않도록

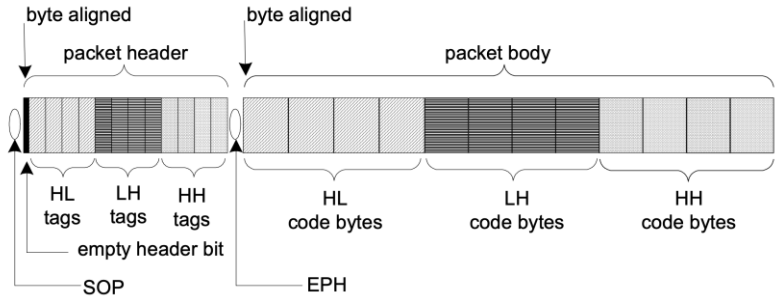
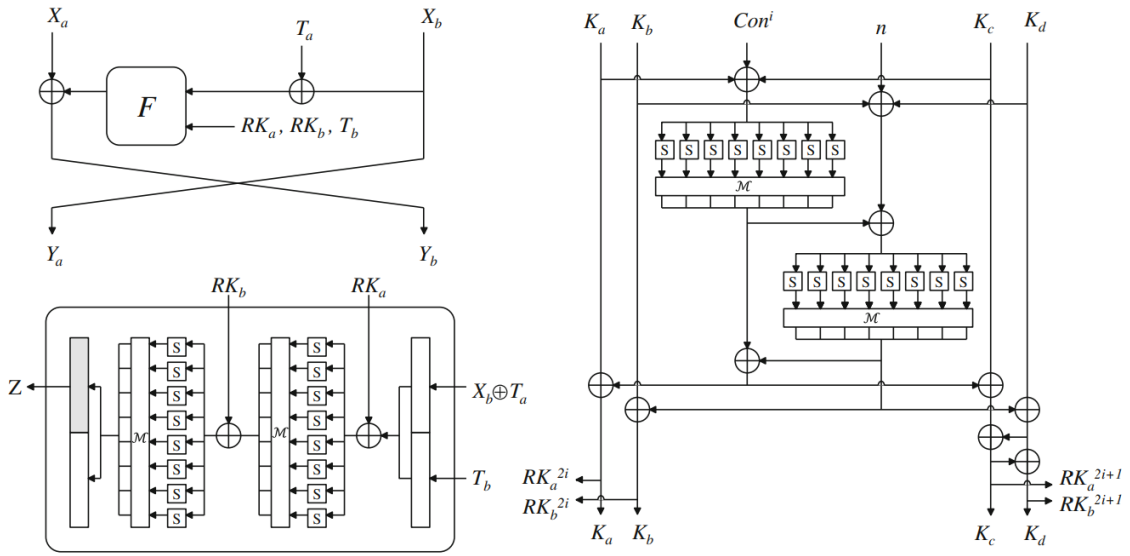
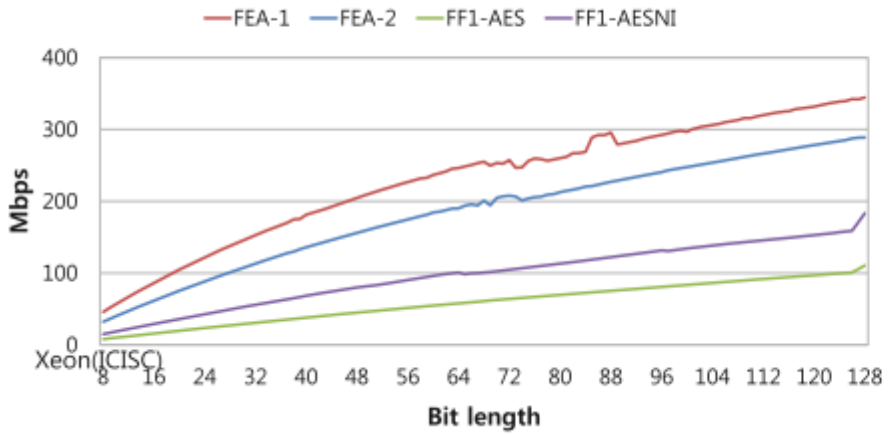
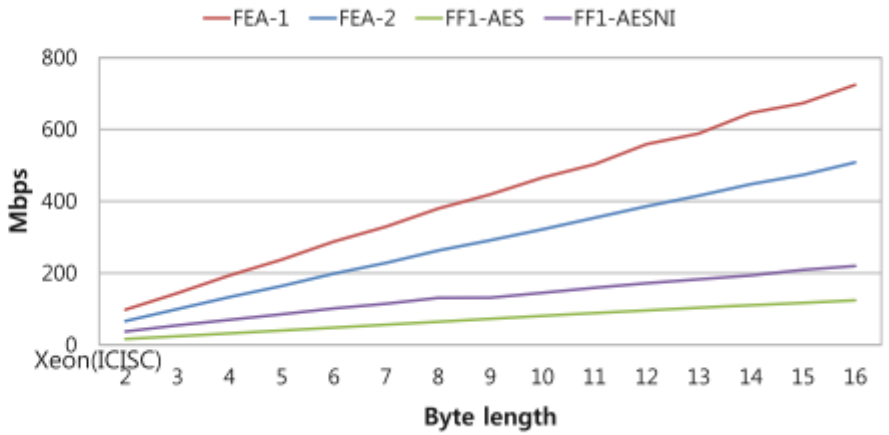


Figure 1.2 JPEG 2000 Packet Structure

국산 형태 보존 암호 FEA







목표

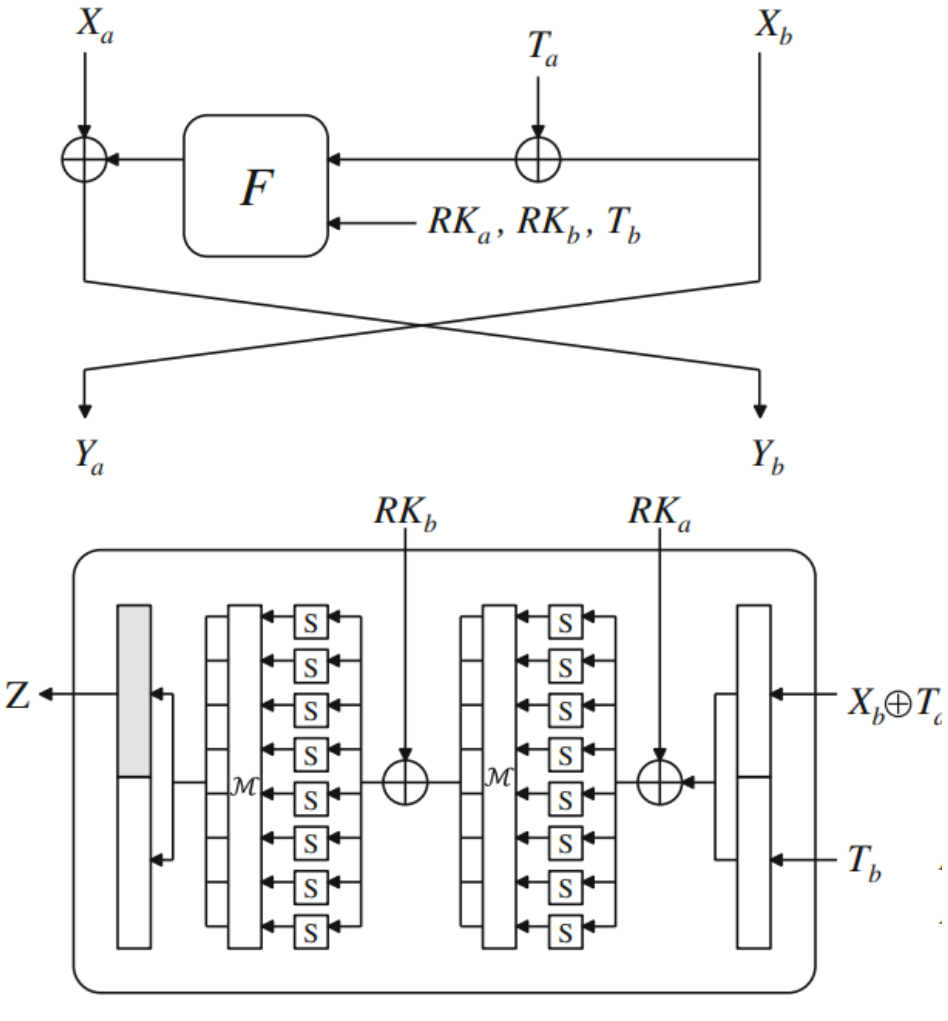
Want

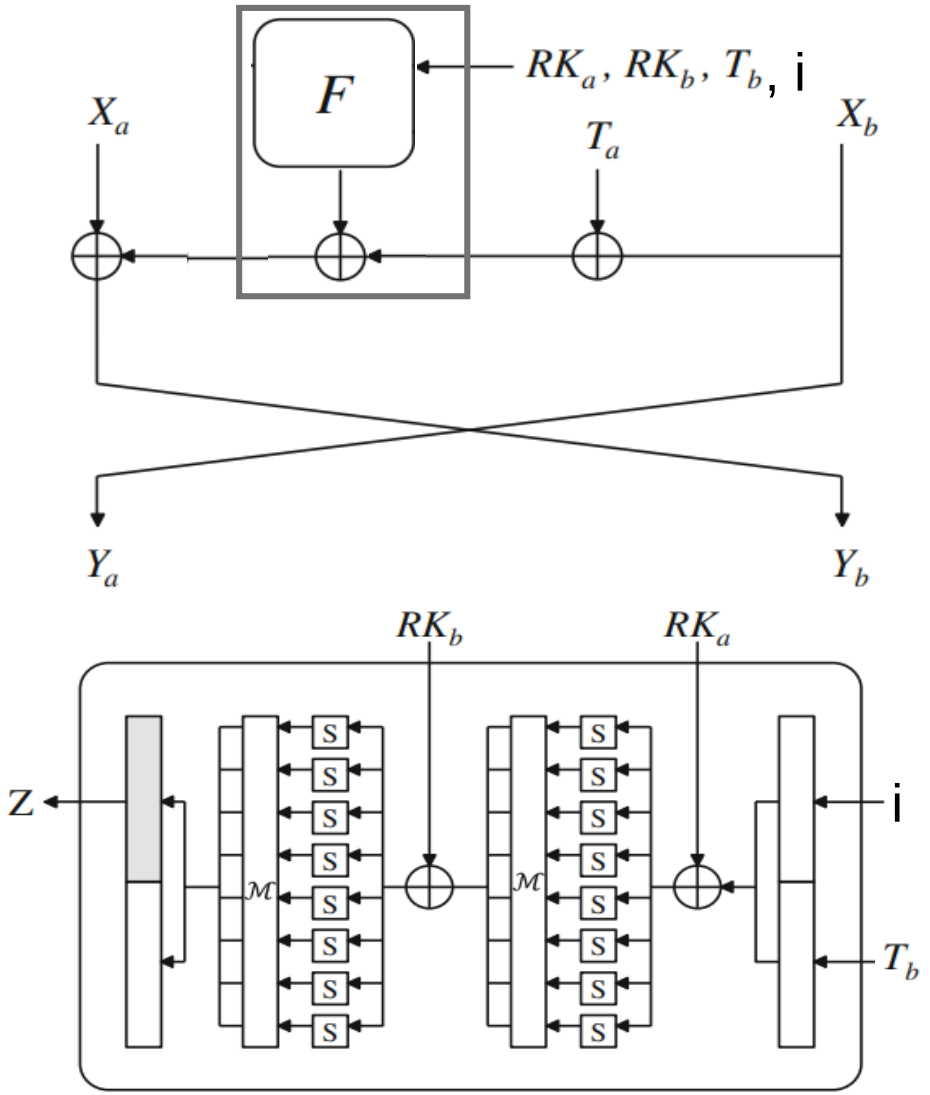
- 작은 크기의 데이터에서 효율적인 저장을 위해서 FEA 사용
- FEA는 2^8보다 크거나 2^128 보다 작은 크기 암호화 더 큰 크기 암호화
- AEAD 기능 추가
- 빠른 연산

Solution

- FEA 변형
- CTR 모드 사용
- GCM 사용

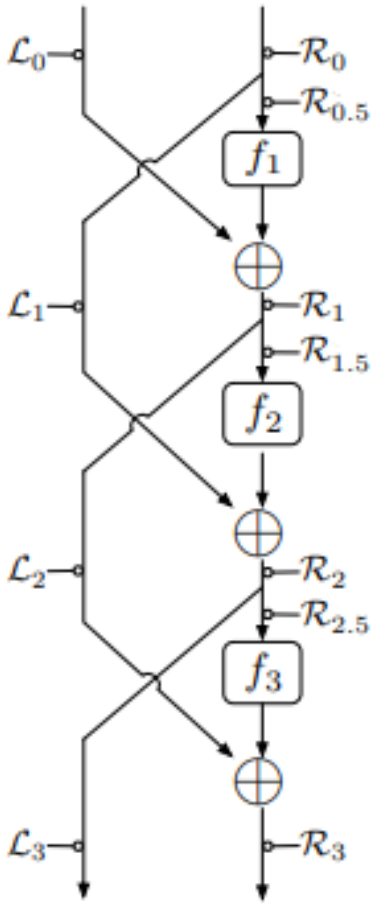
F함수의 스트림화


X_a
T_a
X_b
F
RK_a, RK_b, T_b
Y_a
Y_b
RK_b
RK_a
S
$\mathcal{M}$
Z
$X_b \oplus T_a$
T_b


F
RK_a, RK_b, T_b, i
X_a
T_a
X_b
Y_a
Y_b
RK_b
RK_a
S
$\mathcal{M}$
Z
i
T_b

보안성

- David Goldenberg et al. 의사 난수 함수를 사용하여 안전하게 조정 가능한 Feistel 방식을 연구 [1].
- 라운드 함수의 특정 속성을 사용하지 않는 일반적인 공격에 대해 안전한 조정 가능한 Feistel 구조를 제공

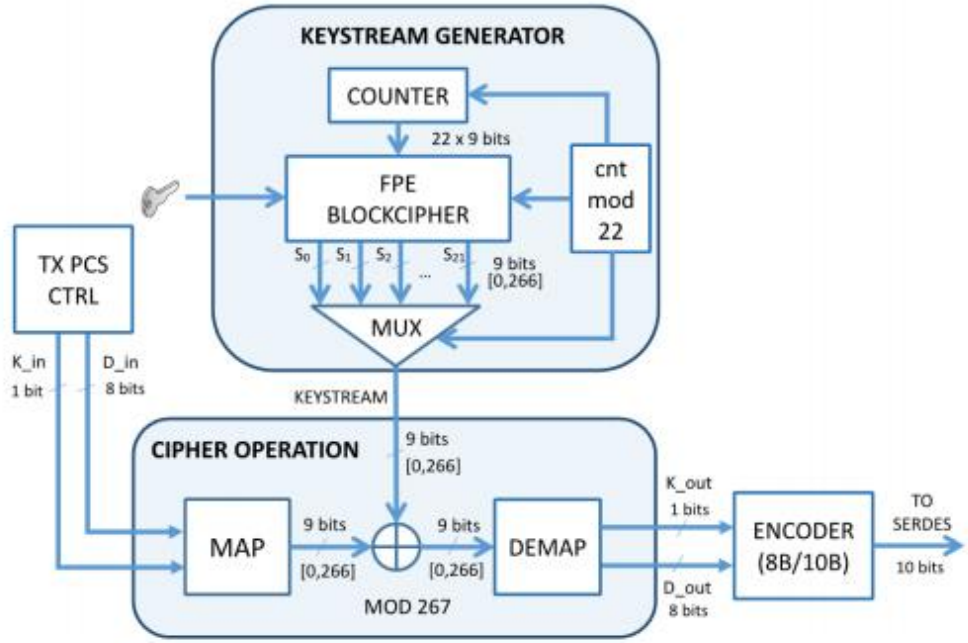


- CPA-secure against polynomial adversaries in 4 rounds (Theorem 3)
- CCA-secure against polynomial adversaries in 6 rounds (Theorem 8)
- CPA-secure against $q \ll 2^k$ queries in 7 rounds (Theorem 4)
- CCA-secure against $q \ll 2^k$ queries in 10 rounds (Theorem 9)

[1] Goldenberg, D., Hohenberger, S., Liskov, M., Schwartz, E.C., Seyalioglu, H.: On tweaking luby-rackoff blockciphers. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 342–356. Springer, Heidelberg (2007)

CTR 모드 적용

- 8b/10b 인코딩 : 8비트 워드를 10비트 심볼로 매핑
- 8b / 10b 데이터 흐름의 암호화 목표
- CTR (카운터) 모드에서 작동하는 FPE 블록 암호 수행



[1]A. Pérez-Resa, M. Garcia-Bosque, C. Sánchez-Azqueta and S. Celma, "Physical layer encryption for industrial ethernet in gigabit optical links", *IEEE Trans. Ind. Electron.*, vol. 66, no. 4, pp. 3287-3295, Apr. 2019.

Q & A