



국산 암호 알고리즘 부채널 분석에 대한 고찰

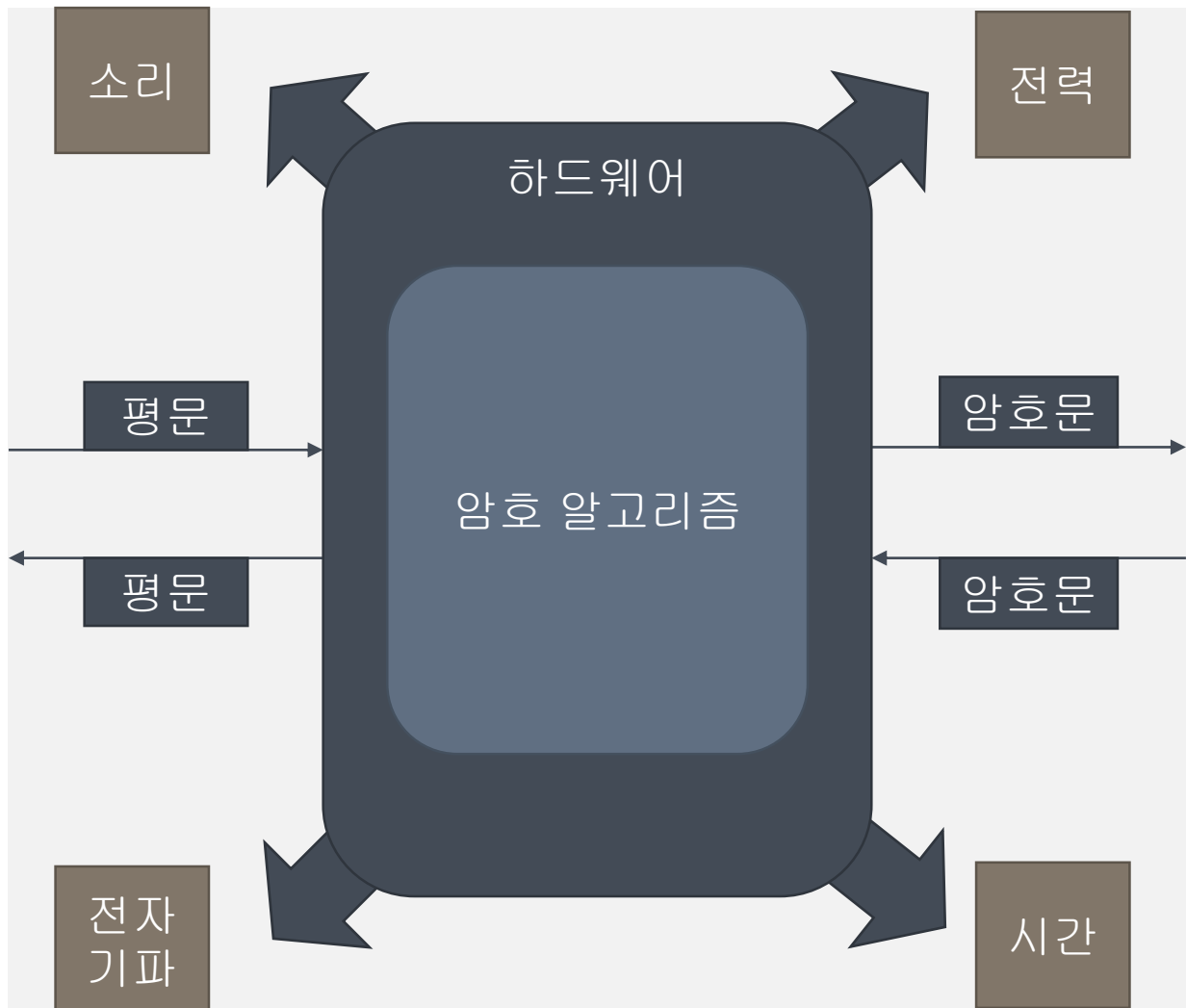


안규황, 권용빈, 권혁동, 서화정



제 1장

부채널 분석



부채널 분석이란?

1. 암호 구동
2. 부가적인 정보 발생
3. 분석



시간 분석



전력 분석



음향 분석



전자기파 분석



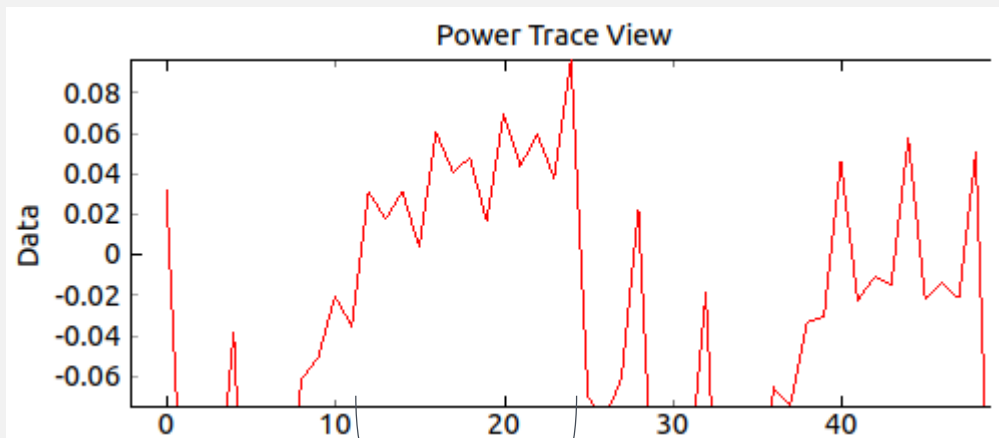
오류주입 분석





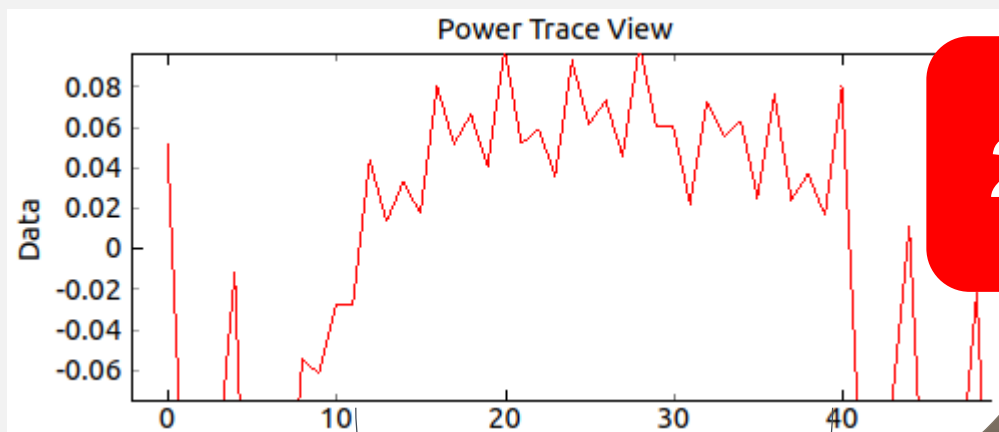
SPA (Simple)

1. 파형 관찰
2. 정보 획득
3. 공격에 활용



4 * NOP

11 to 25 = 14



2배

11 to 40 = 29



AVR Assembler
Instructions

Instructions	Cycles
NOP	1
MUL	2



$$T_{0...N}$$

$H_{0...N}$ by Hamming Weight

$$\begin{aligned} A_0 &< -T \text{ with low } H \\ A_1 &< -T \text{ with high } H \end{aligned}$$

$$D = E(A_0) - E(A_1)$$

$$D \neq 0 \rightarrow \text{Key}$$

DPA (Differential)

1. 올바른 수행 파형 수집
2. 중간값을 전력 모델로 변환한 값 수집
3. 분류함수를 통해 파형 그룹화
4. 평균값을 차분
5. 차분이 0이 아니라면 키

 $T_{0...N}$ $H_{0...N}$ by Hamming Weight

$$p(H, T) = \frac{E(H \cdot T) - E(H) \cdot E(T)}{\sqrt{\text{Var}(H) \cdot \text{Var}(T)}}$$

Highest $p \rightarrow$ Key

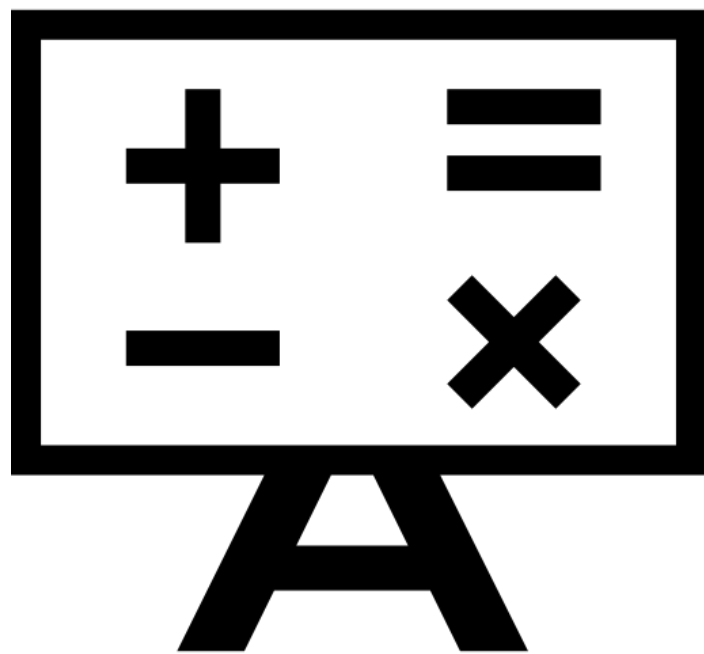
CPA (Correlation)

1. 올바른 수행 파형 수집
2. 중간값을 전력 모델로 변환한 값 수집
3. 상관관계 측정
4. 가장 높은 상관관계를 가지는 키 획득

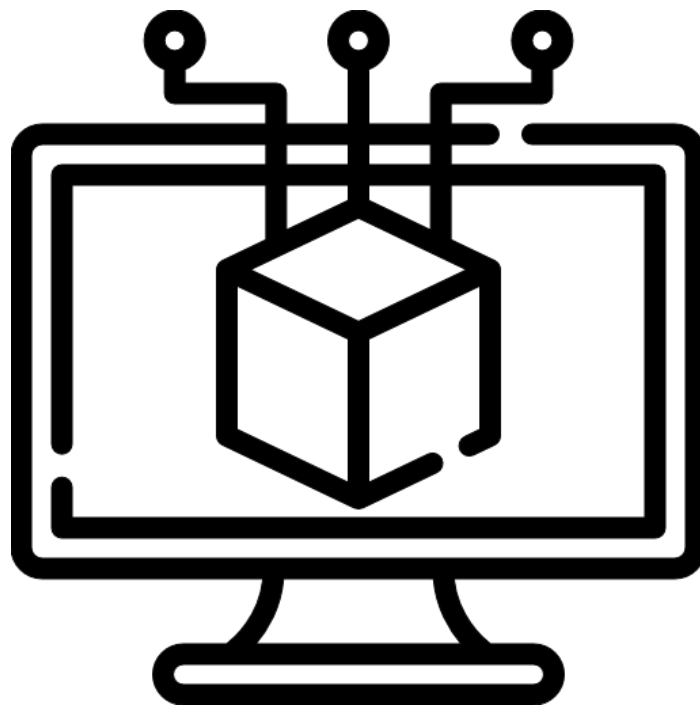
제 2장

전력분석
대응기법

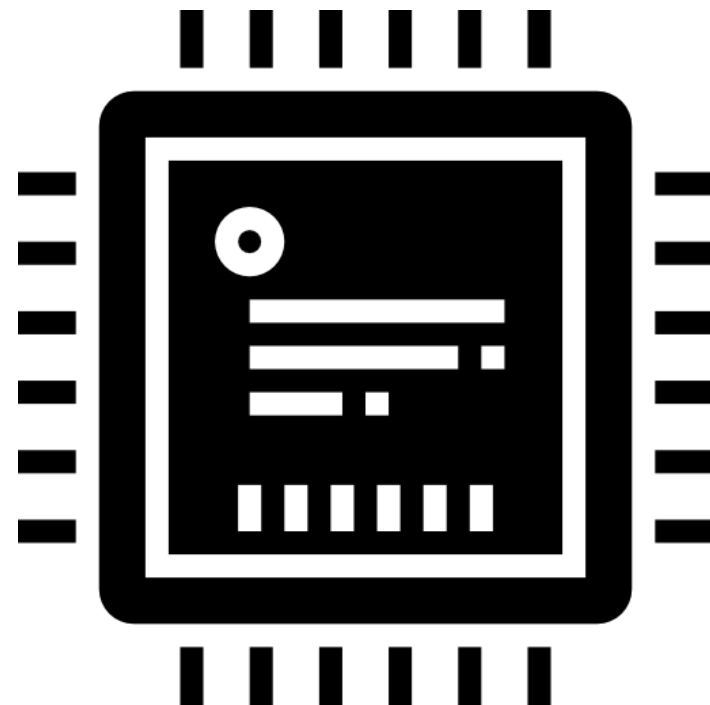




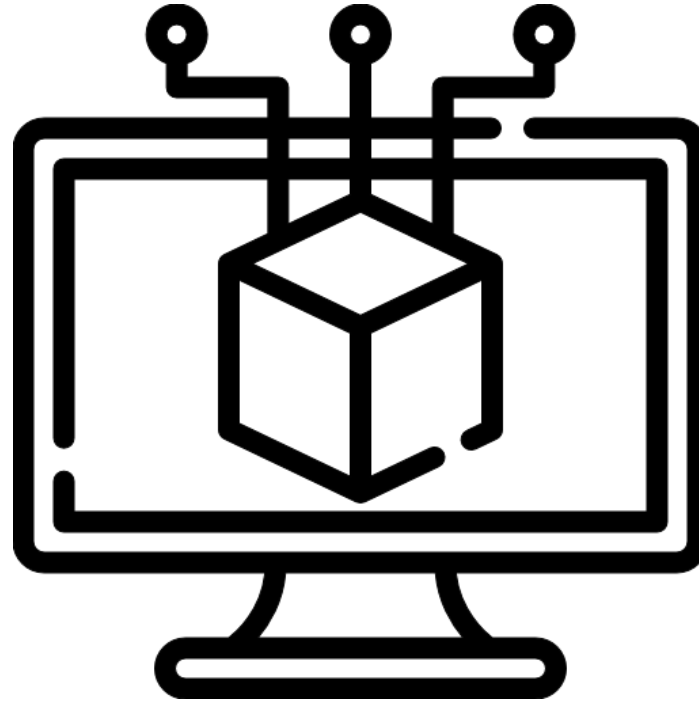
알고리즘 개발자



소프트웨어 개발자



하드웨어 개발자



소프트웨어 개발자

더미 연산
기법



평문

더미 연산

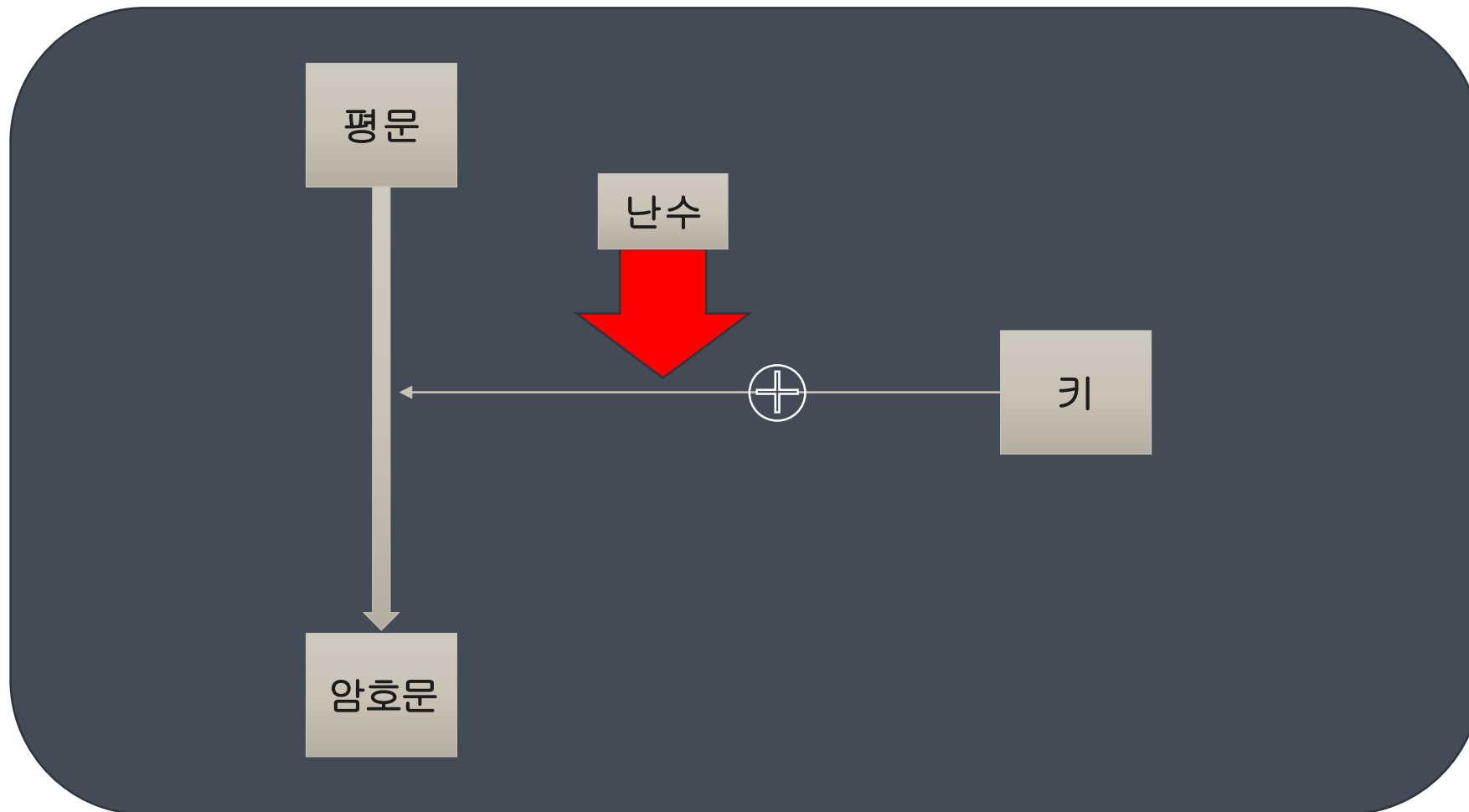


암호문

셔플링
기법



마스킹
기법



제 3장

국산 암호 알고리즘 부채널 분석 동향



SEED

블록암호알고리즘
블록 : 128 비트
키 : 128,256비트
라운드 : 16

특징
Feistel 구조

HIGHT

블록암호알고리즘
블록 : 64비트
키 : 128비트
라운드 : 32

특징
ARX 구조
Feistel 구조

ARIA

블록암호알고리즘
블록 : 128비트
키 : 128/192/256 비트
라운드 : 12, 14, 16

특징
Involutional SPN 구조

LEA

블록암호알고리즘
블록 : 128비트
키 : 128/192/256 비트
라운드 : 24, 28, 32

특징
ARX 구조
Feistel 구조

SEED

블록암호알고리즘
블록 : 128 비트
키 : 128,256비트

특징
Feistel 구조

전력분석

G함수 덧셈

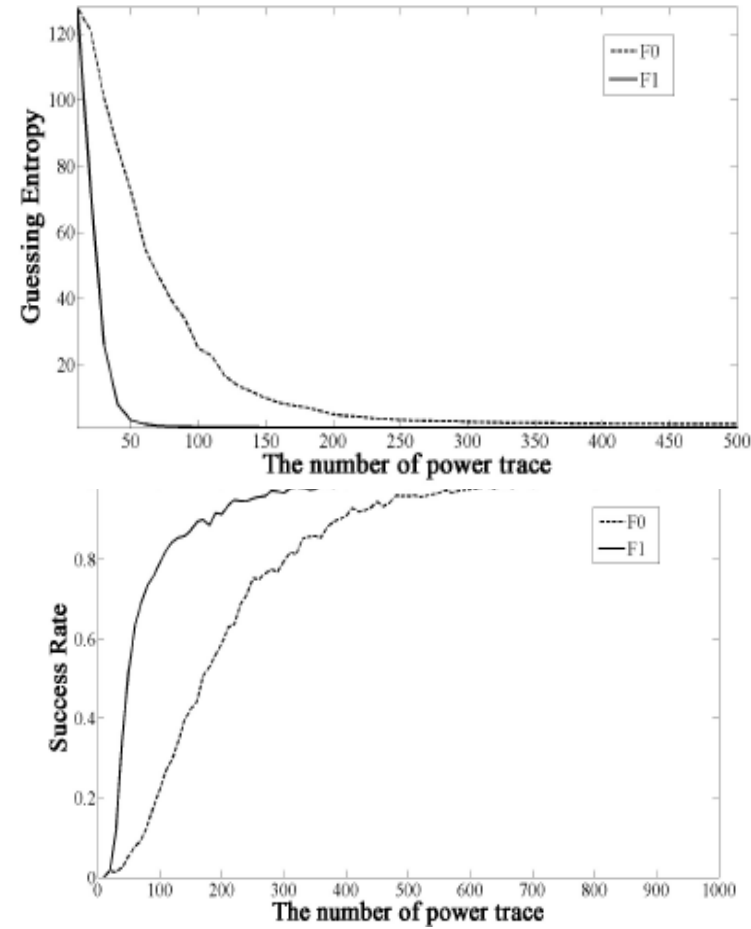
G함수 연산

8000개 파형
공격 성공

HIGHT

블록암호알고리즘
블록 : 64비트
키 : 128비트

특징
ARX 구조
Feistel 구조



원 논문에서 참조한 그래프입니다.

공격 대상 지점 2 곳
(선형, 비선형 연산 부분)
모두 공격이 가능

LEA

블록암호알고리즘
블록 : 128비트
키 : 128/192/256 비트

특징
ARX 구조
Feistel 구조

1차 전력 분석

대응기법 마스킹

안전한 난수 발생기
기반 마스킹

효율적인 마스킹

마스킹 변환 기법

전력 분석 방법 사용

분석 기법의 공격 효율성 향상

적절한 대응 기법의 적용

국산암호의 미래

앞으로 많이 쓰이게 될 암호임

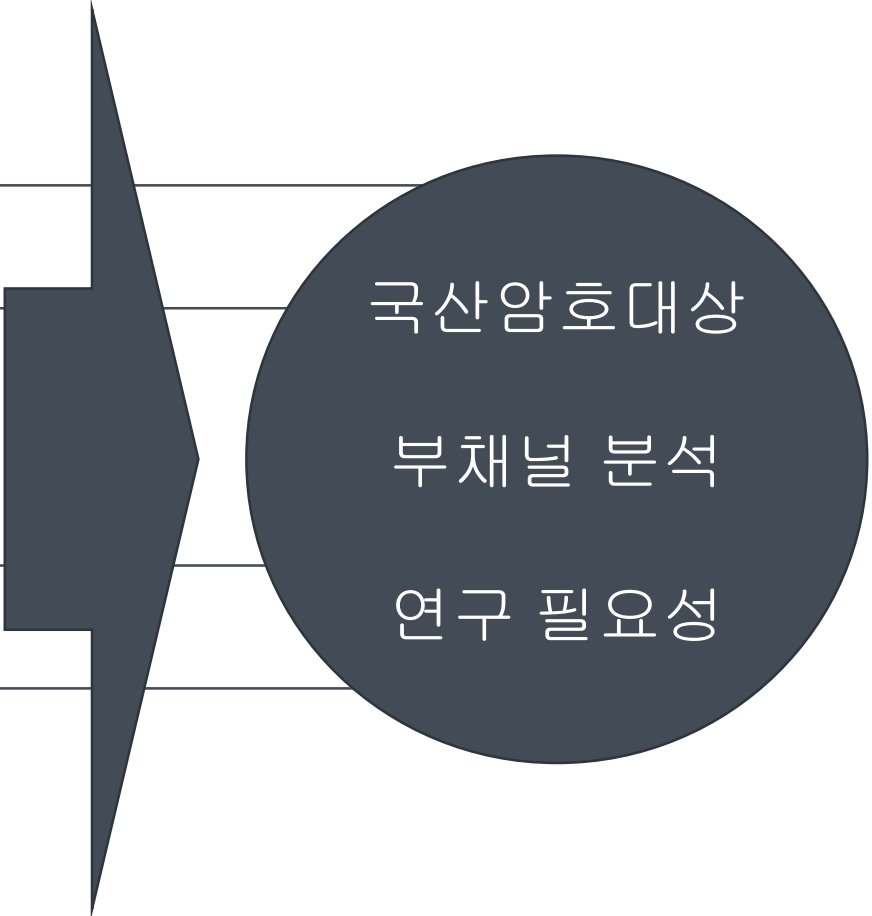
→ 부채널 공격 표면적이 넓어집니다.

복호화 과정이 간단하다.

→ 부채널 공격에 필요한 예측 값을 얻기 쉽습니다.

경량, 고속 환경을 위해 태어남

→ 부채널 공격 대응기법을 마련하기 어렵습니다.



국산암호대상

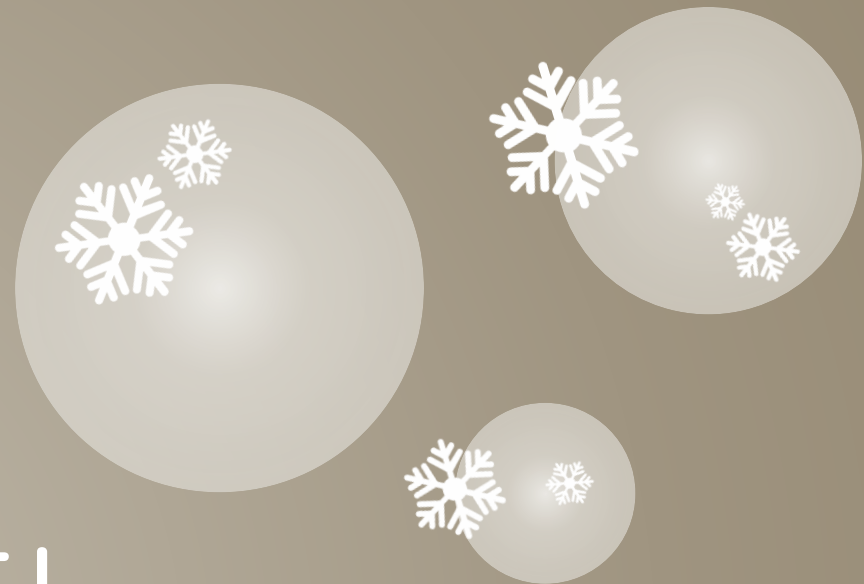
부채널 분석

연구 필요성

국산 암호에 대한 부채널 분석 동향

국산 암호에 대한 부채널 분석과
그 대응기법 연구 필요성 제시

국산 암호에 대해 필요한 연구 제시



감사합니다

