초경량 블록 암호 CHAM에 대한 CPA 공격과 대응기법 제안

김현준, 권혁동, 김경호, 서화정

한성대학교 IT융합공학부

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

https://crypto.modoo.at

Contents

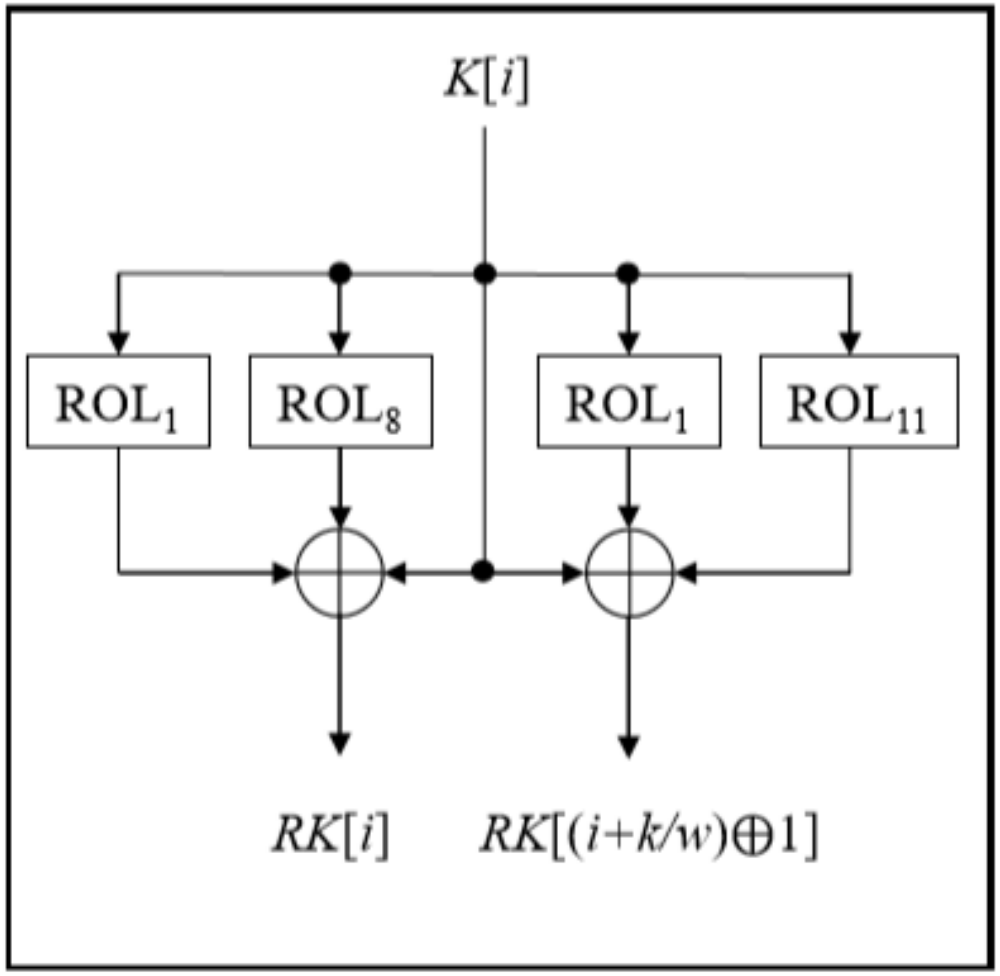
CryptoCraft LAB

CHAM

- 국산 경량 블록 암호로 자원 제약을 받는 저 사양 디바이스 장치에서 효율적인 알고리즘
- ARX (더하기, 회전, XOR) 연산 기반 4- 분기 Feistel 구조
- 8 비트 AVR 마이크로 컨트롤러의 작업 수를 최소화하기 위해 1 비트 및 8 비트 두 가지 유형의 왼쪽 회전을 사용
- CHAM-64 / 128, CHAM-128 / 128 및 CHAM-128 / 256 세 가지

cipher	n	k	r	w	k/w
CHAM-64/128	64	128	80	16	8
CHAM-128/128	128	128	80	32	4
CHAM-128/256	128	256	96	32	8

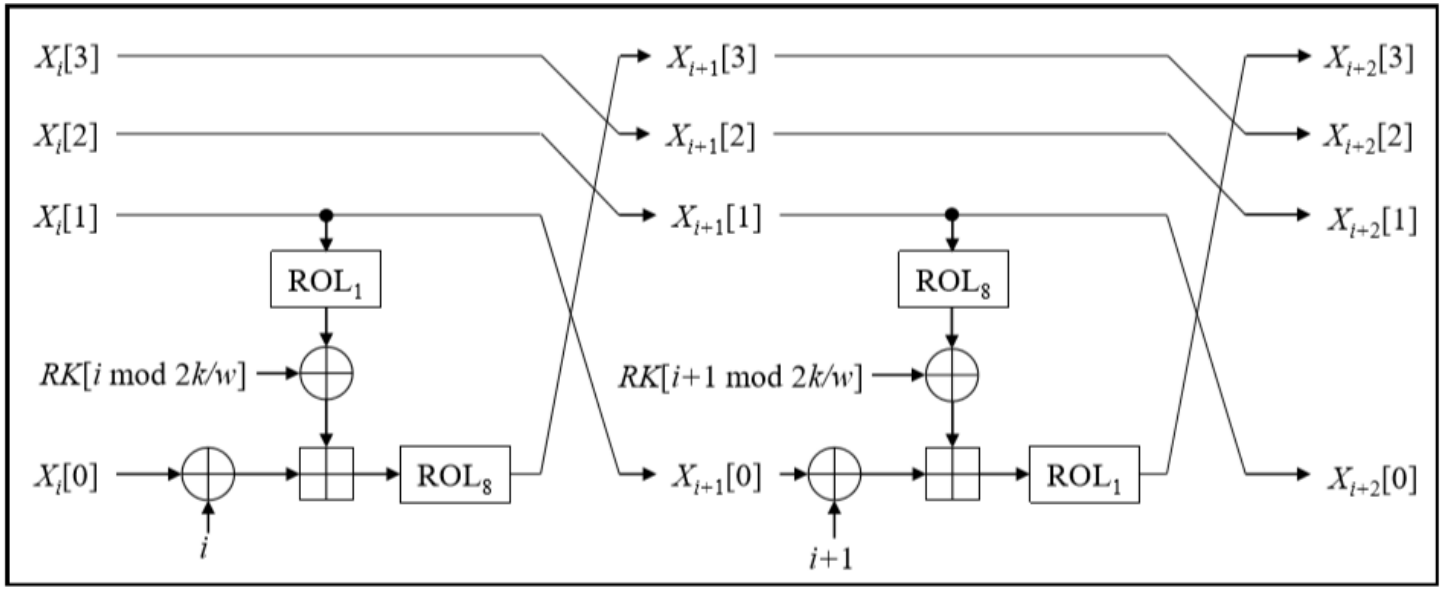
Key schedule 특징



- 하나의 키 워드에 2개의 라운드 키가 겹치지 않게 생성

✓ 둘 중 하나의 라운드키 워드를 획득한다면 전 탐색 기법을 통해서 해당 키 워드를 알아 낼 수 있다.

Encryption 특징



- 2라운드마다 짝수 라운드와 홀수 라운드 연산이 연결되어 반복되어 실행된다.

✓ 공격시 다음 라운드키 값을 찾기 위해서는 전 단계 라운드키를 알아내고 연산 결과 값을 계산 해야 한다.

- 각 라운드마다 해당하는 하나의 라운드 키를 사용한다.
- CHAM은 라운드 키를 저장하는 데 필요한 메모리 크기를 줄이기 위하여 반복적으로 재사용

✓ 공격 시 모든 라운드키를 획득하지 않아도 k/w 만큼의 개수의 라운드키를 알면 모든 키를 알 수 있다.

부채널 공격 기법

- **부채널 공격**이란 분석 구현 과정에서 설계자가 고려하지 못한 정보의 **누출 정보**를 통해 비밀 **정보를 알아내는** 공격 기법

- 이 중 강력한 부채널 공격 방법인 **전력 분석 공격**은
  전력 소비 모델과 **측정된 전력 신호**의 **통계적 특성**을 비교, 분석하여
  암호화에 사용된 키를 찾아내는 공격 방법

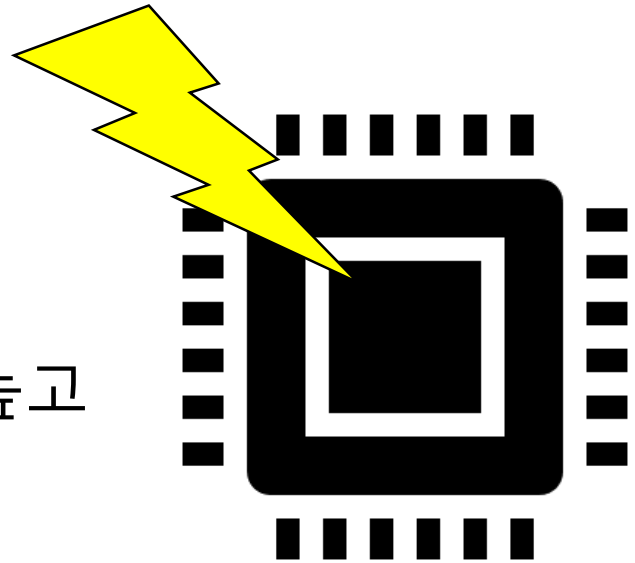
- 상관 전력 분석(Correlation Power Analysis, CPA)

  전력 소비 모델과 수집파형의 포인트별 상관계수를 계산하는 공격
  추측키가 비밀키와 동일 할 경우 가장 높은 상관계수를 보이 점을 사용

부채널 공격 기법

- CHAM과 동일한 ARX 구조의 블록암호 LEA, HIGHT, SIMON, SPECK이 전력분석공격에 취약함이 알려짐

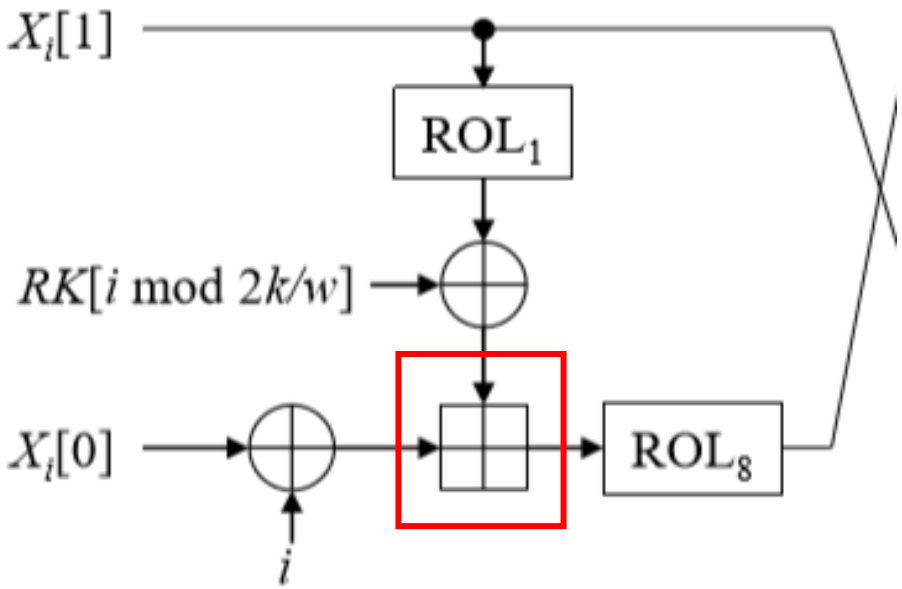
- CHAM 또한 이러한 전력 분석 공격에 취약할 가능성이 높고 대응책이 필요함



마스킹 기법

부채널 분석 공격을 막기위한 일반적인 대책으로 알고리즘 마스킹

- 연산시 발생하는 중간 값을 랜덤하게 만들어 공격자에게 필요한 정보의 누출을 막는 대응기법
- 부울 마스킹 : x'=(x⊕r), 산술 마스킹 : A=x-r mod 2^k
- CHAM과 같은 ARX 구조의 알고리즘에 마스킹 기법이 적용되는 경우 불 마스킹 기법과 산술 마스킹을 상호 변환 하는 과정이 필요
- 불 마스킹된 두 개의 데이터를 더하기 해서는 불-산술 마스킹 변환, 덧셈, 산술-불 마스킹 변환의 3단계 를 거쳐야 한다.



KRJ SA 마스킹 기법

- Karroumi는 기존의 마스킹 변환의 번거로움과 연산량을 개선하기 위해 Secure Addition 마스킹 기법을 처음으로 제안
- 두 개의 불 마스킹된 데이터를 입력받아 불 마스킹된 덧셈 결과를 출력
- 복잡도 5k+8의 연산 소요

Input : x', y', r_x, r_y

Output: z'

1. $C = \gamma$	10. $B = \Omega \ll 1$
2. $T = x' \wedge y'$	11. $C = C \ll 1$
3. $\Omega = C \oplus T$	12. $z' = x' \oplus y'$
4. $T = x' \wedge r_y$	13. $r_z = r_x \oplus r_y$
5. $\Omega = \Omega \oplus T$	14. $T = C \wedge r_z$
6. $T = y' \wedge r_x$	15. $\Omega = \Omega \oplus T$
7. $\Omega = \Omega \wedge T$	16. $T = C \wedge r_z$
8. $T = r_x \wedge r_y$	17. $\Omega = \Omega \oplus T$
9. $\Omega = \Omega \wedge T$	
18. for $i = 2$ to $k-1$ do	
18.1 $T = B \wedge z'$	18.4 $B = B \oplus T$
18.2 $B = B \wedge r_z$	18.5 $B = B \ll 1$
18.3 $B = B \oplus \Omega$	
19. $z' = z' \oplus B$	20. $z' = z' \oplus C$

제안 목적

- ARX 기반 알고리즘 LEA, HIGHT, SIMONE, 그리고 SPECK이
  해당 공격 기법에 취약한 것으로 밝혀짐

- 부채널 공격으로부터 안전성을 갖추기 위한 기법으로 마스킹 기법을 사용 할 수 있다.

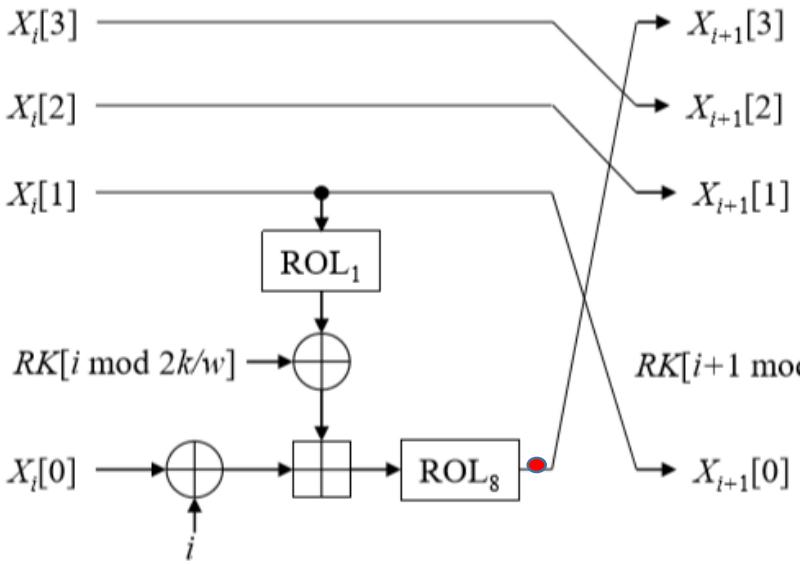
- 8비트 프로세스 상에서 CHAM-64/128에 대한 전력 분석 공격 실험을 통하여
  마스터 키 값을 획득 할 수 있음을 확인한다.

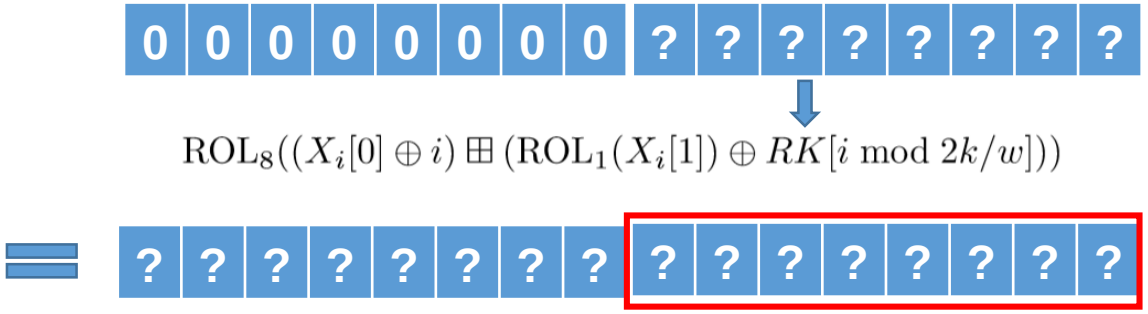
- 1차 전력 분석 공격에 안전하도록 마스킹 기법을 함께 제안

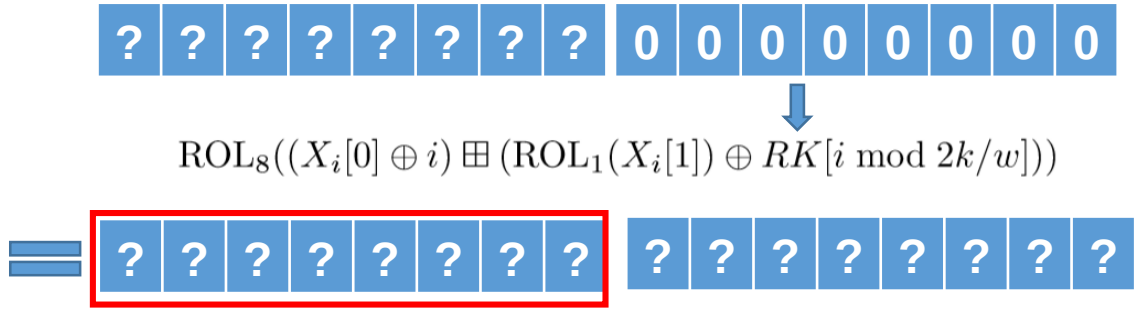
제안 CPA 공격 기법

홀수 라운드 연산

- ROL 연산 후(•) 지점 공격
- 8비트씩 나누어 공격
- RK에 우측부분에 8bit($RK_{8\text{-}15}$)만 추측값를 넣고 결과값 중 가장 상관계수 값이 높은 추측값를 라운드키의 우측 8bit로 선택
- RK에 좌측부분에 8bit($RK_{0\text{-}7}$)만 추측값를 넣고 결과값 중 가장 상관계수 값이 높은 추측값를 라운드키의 좌측 8bit로 선택
- 획득한 라운드키값으로 마스터키값 획득



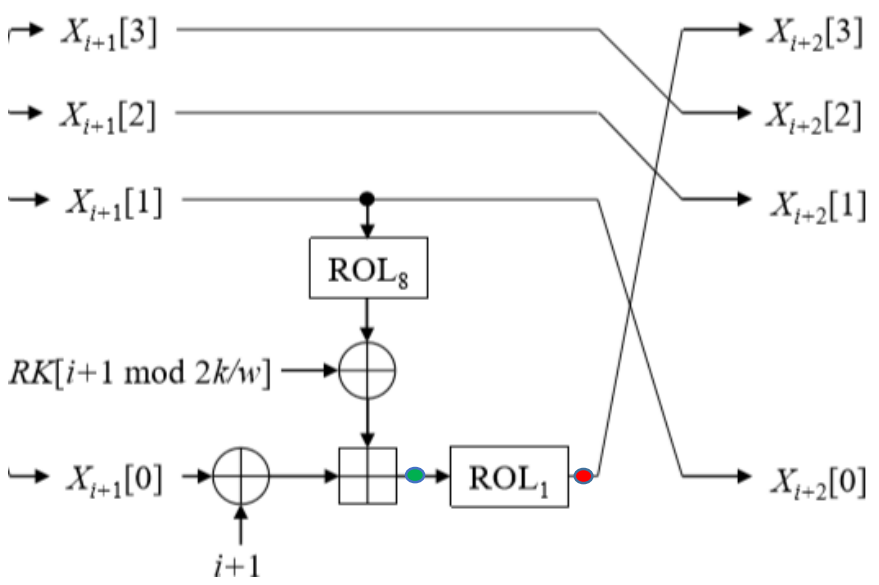


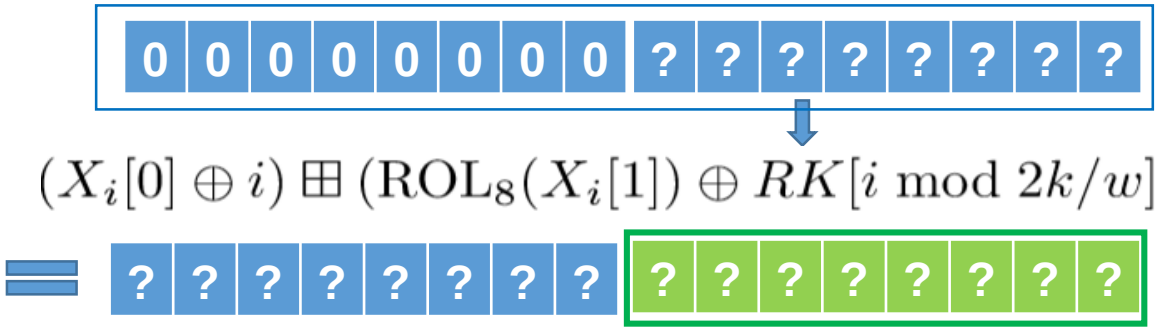


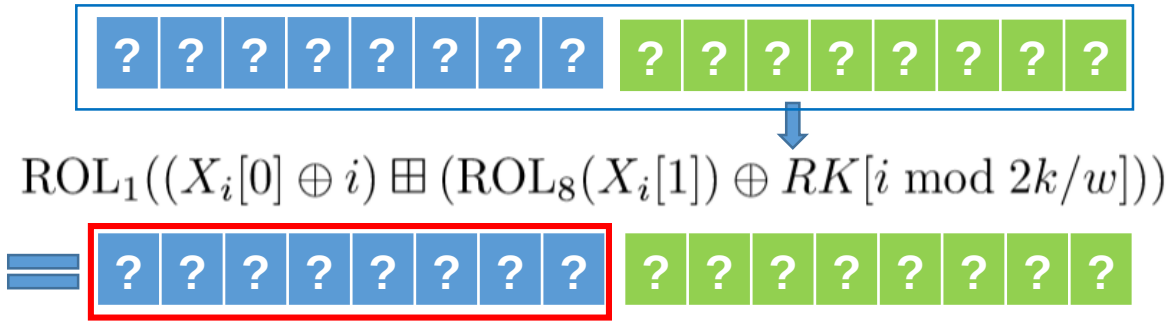
제안 CPA 공격 기법

짝수 라운드 연산

- $RK_{8\text{-}15}$는 ● 지점을 공격, $RK_{0\text{-}7}$은 ● 지점을 공격한다.
- 8비트씩 나누어 공격
- 먼저 $RK_{8\text{-}15}$만 추측 값를 넣고 결과값 중 가장 상관계수 값이 높은 추측 값를 라운드키의 우측 8bit로 선택
- 앞부분에서 구한 $RK_{8\text{-}15}$값과 $RK_{0\text{-}7}$에 추측 값를 넣고 결과값 중 가장 상관계수 값이 높은 추측 값를 라운드키의 좌측 8bit로 선택
- 획득한 라운드 키값으로 마스터키 값 획득

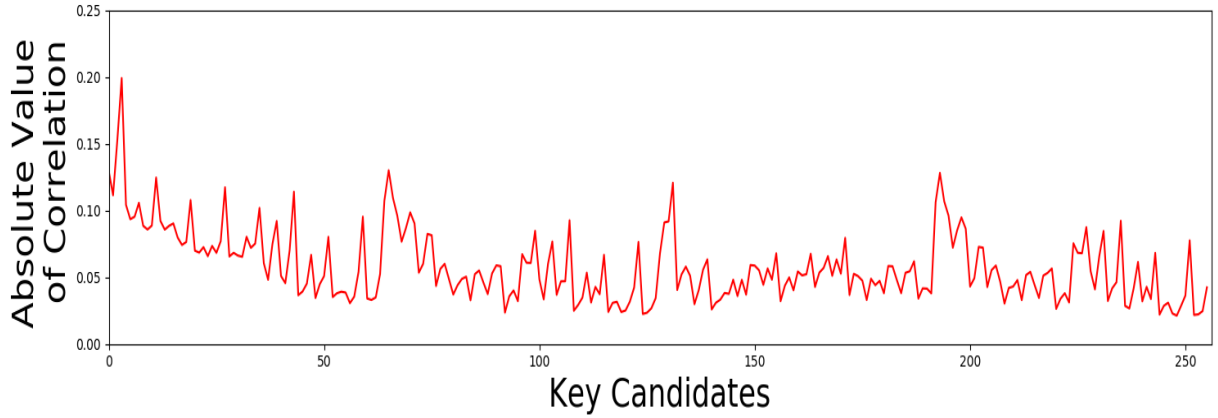


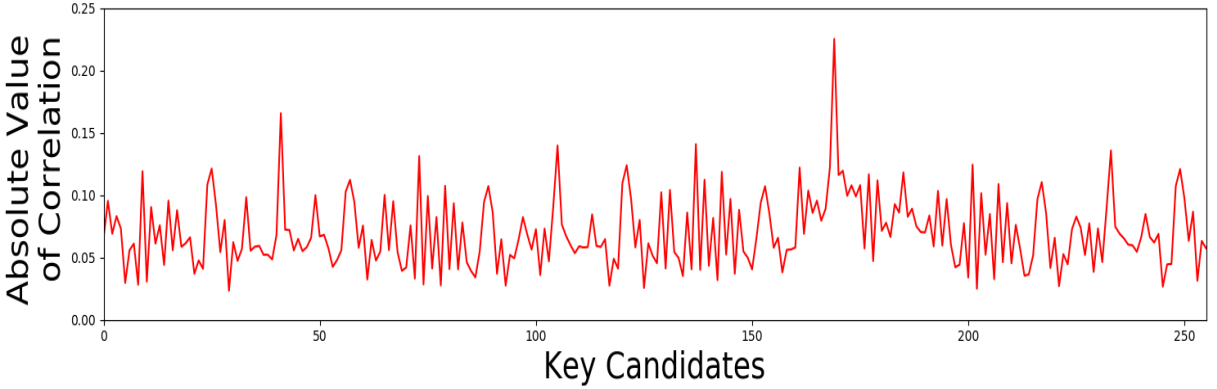




실험 결과

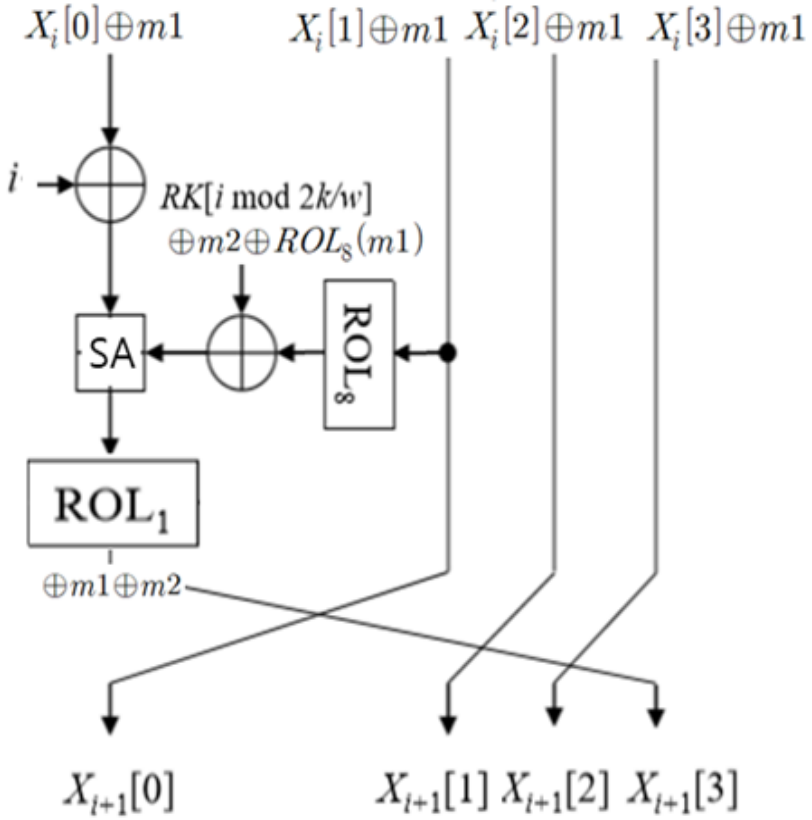
- 8bit 프로세서에서 돌아가는 CHAM-64/128 대상
- 1~8라운드까지의 파형을 5,000개 수집
- 1라운드연산에서 공격을 통해 나오는 가장 높은 상관관계를 가지는 좌측과 우측의 8bit 값은 (0x03, 0xA9) (0x03A9)
- 이 라운드키 값을 통해 사용된 마스터키 값의 일부인 (0x2B7E)을 알아냄
- 동일한 방법으로 나머지 라운드에서도 올바른 마스터키 값을 알아내어 공격에 성공
- 1~8라운드의 전력파형과 입력 값을 알고 있는 경우 5분 이내에 모든 비밀 키를 찾을 수 있었다.

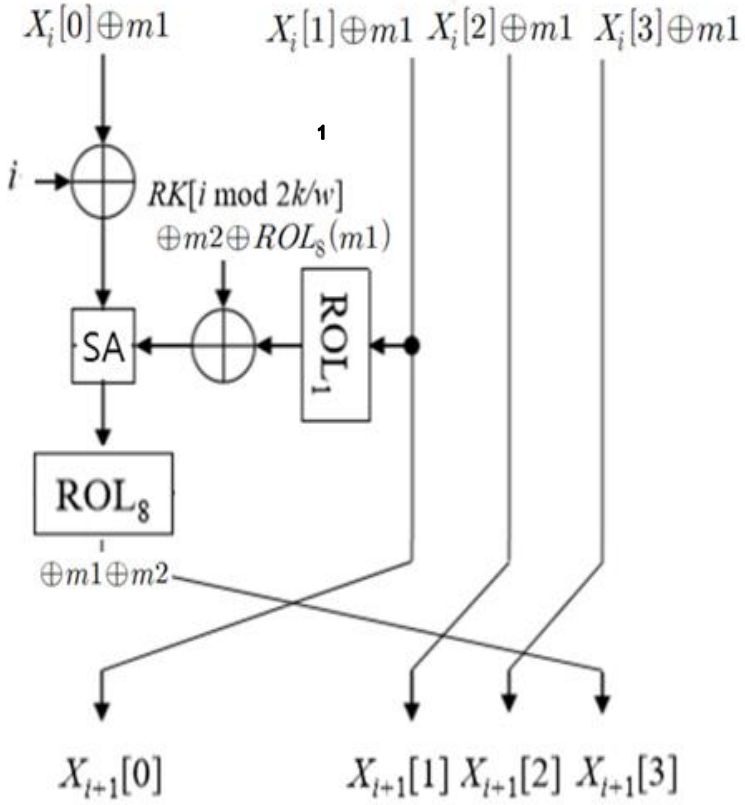




제안 마스킹 적용 기법

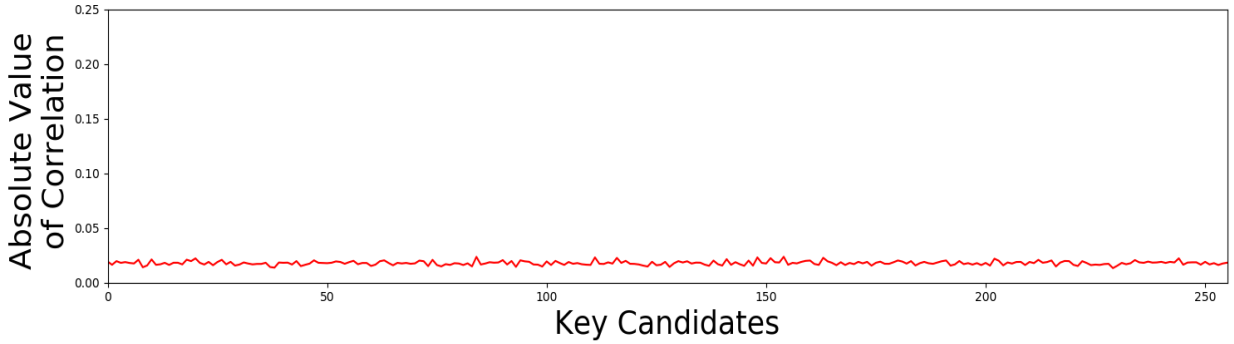
- 입·출력 마스크 값을 동일하게 유지한다.
- 마스크 값은 16비트의 난수를 2개를 사용 하며
- 효율성을 높이기 위해 모듈러 덧셈에 변환 기법 적용을 제외한 부분은 동일한 구조
- 불-산술 마스킹 변환, 덧셈, 산술-불 마스킹 변환 연산을 동시에 수행 할 수 있는 기법 중 KRJ 기법을 사용

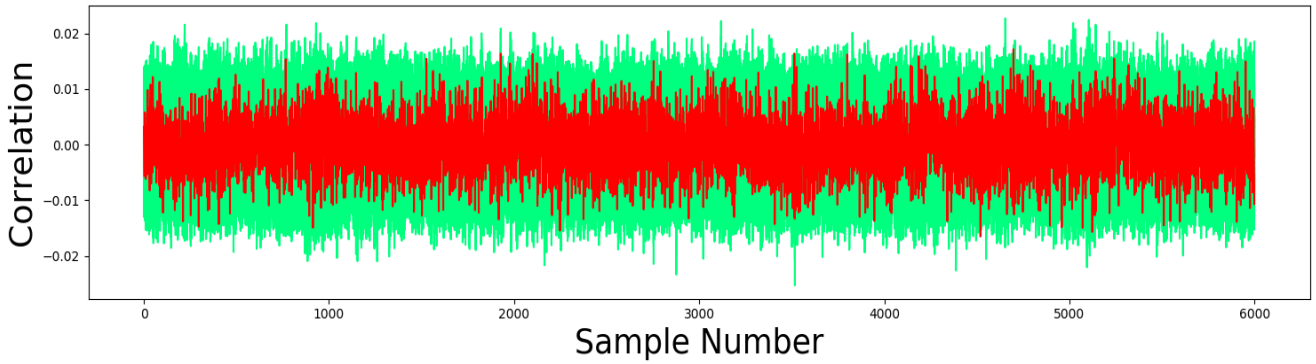




검증

- 제안 기법의 검증을 위해 동일한 환경에 공격을 시도
- 추측 값들에 대하여 전반적으로 낮은 상관계수값이 나옴
- 실제 값에 대한 상관관계가 드러나지 않아 안전한 마스킹이 적용됨을 확인함





Q & A