단일 전력 파형을 사용한 마이크로 컨트롤러상의 코드 유사도 탐지

https://youtu.be/qihkQB5AlXU

한성대학교 HANSUNG UNIVERSITY

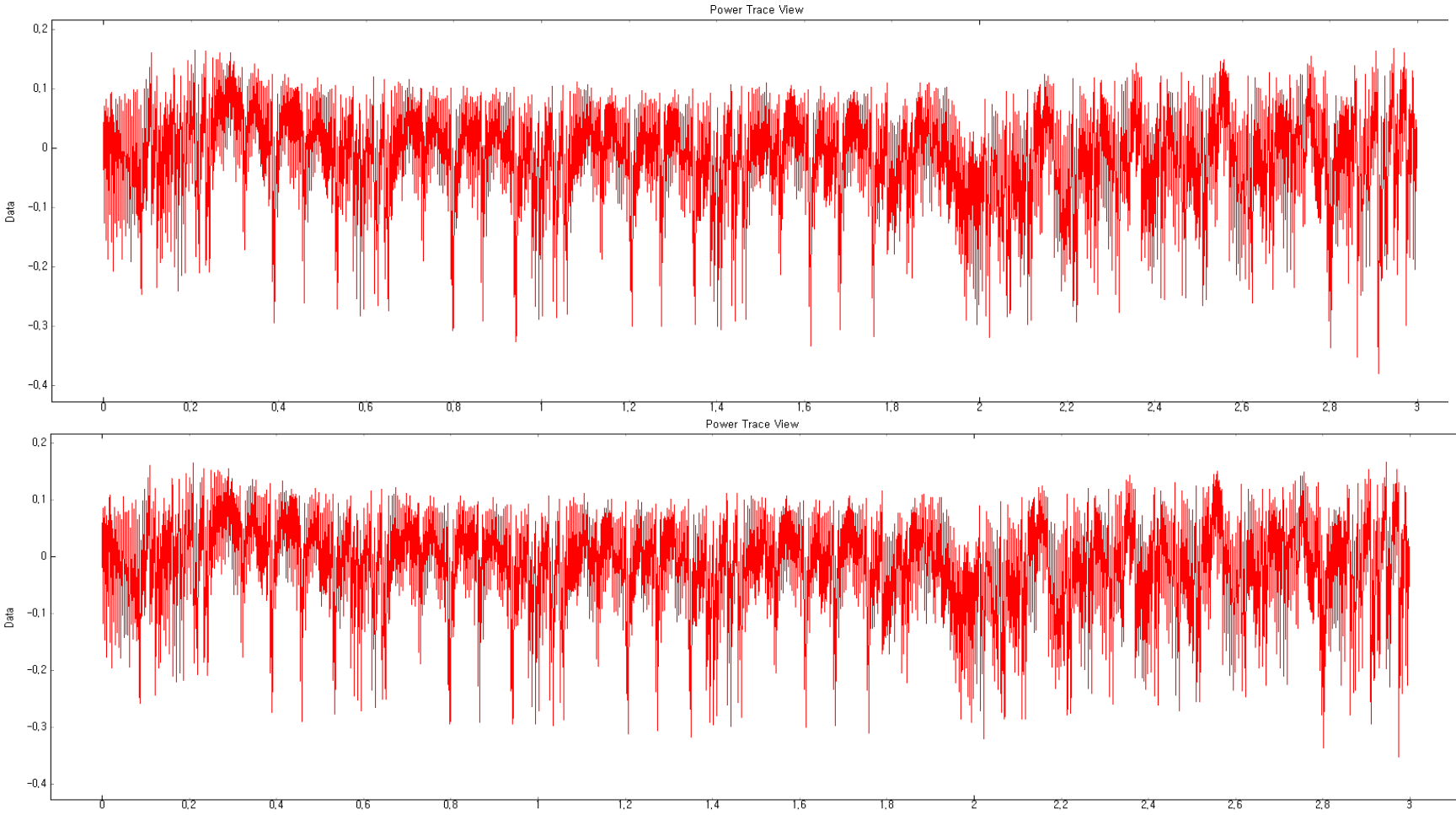
CryptoCraft LAB
https://crypto.modoo.at

배경

- 마이크로 컨트롤러의 소프트웨어를 표절했을 때 지적 재산권 확인 필요
- 부채널 전력 분석으로 두 구현된 프로그램을 비교하여 지적 재산권 확인
- 이전 관련 세미나 발표
  - 공격자의 더미코드 추가도 분류가능 하여 전체적인 표절 뿐 아니라 세부적인 표절 확인 가능
  - 기존 제안된 같은 입력 값을 사용해야 함
  - 10.000개 정도의 다수의 트레이스 사용
- 목표
  - 파형을 통해 표절 여부 판단
  - 원래 코드에 약간의 수정이 적용된 경우에도 감지

배경

- 코드의 입력 값이 다르더라도 파형의 모양은 유사
- 마이크로 프로세서가 수행하는 명령어는 각각 다른 전력 소비 프로파일을 갖음
- 파형의 유사도를 비교
  - 기존 논문과 다르게 다른 입력 값에도 코드의 유사도 분석가능



배경

- 추측
  - 카피한 코드의 경우 같은 명령어의 구조로 되어있으므로
    파형을 푸리에 트렌스폼을 적용하여 비교하면 카피여부를 구분 가능

- 하나의 파형을 푸리에 트렌스폼을 적용 한 후에 상관관계 비교

- 유의미하게 나왔지만 이미 논문이 있음

- 그러나 푸리에 트랜스폼을 사용한 논문의 경우 세부적인 분석이 불가능

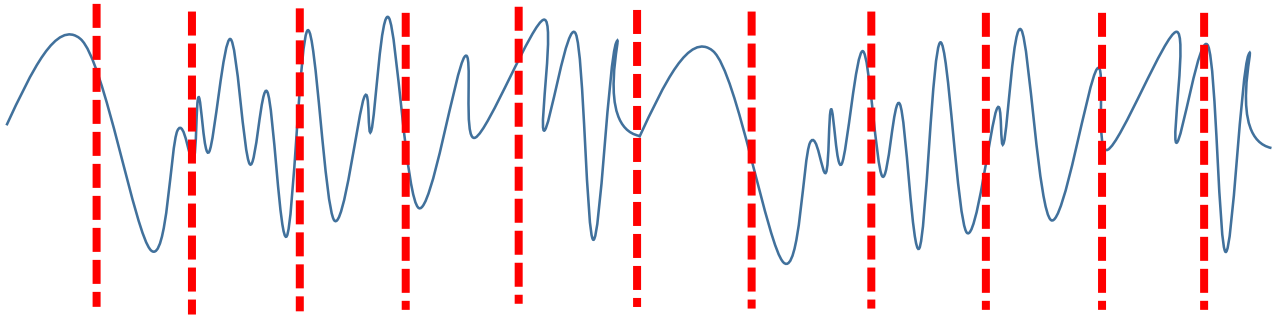
제안 기법

✓파형을 구간으로 나누어 비교

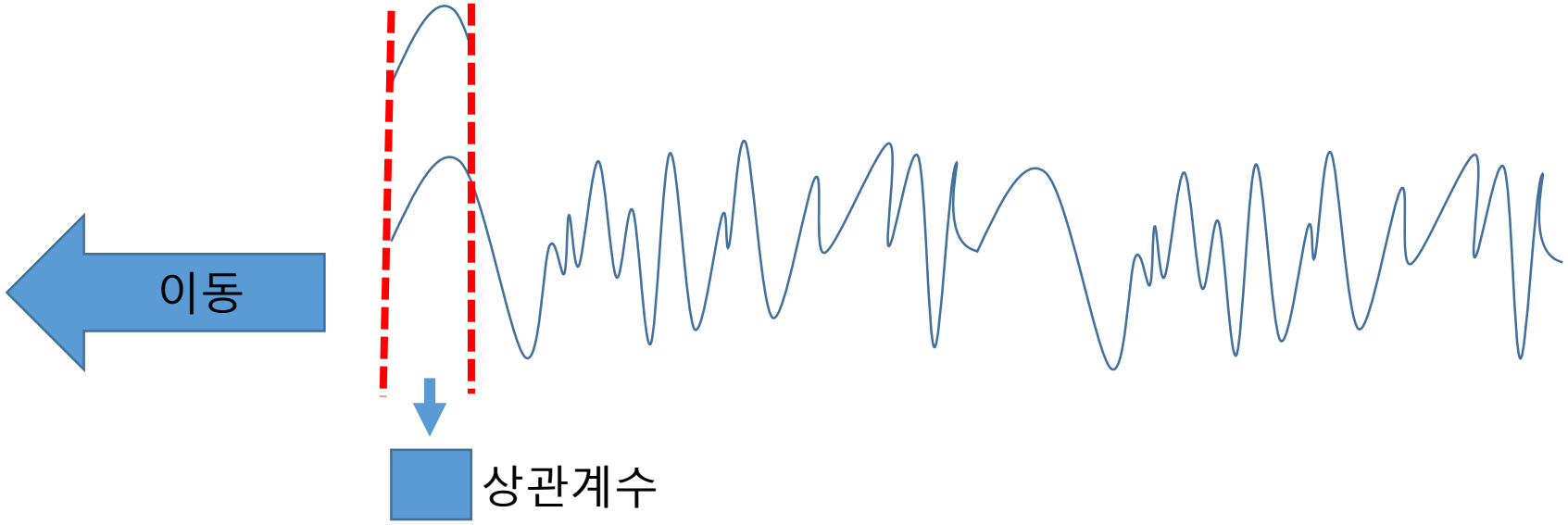
- 서로 다른 입력 값을 사용하여도 분석 가능
- 파형을 구간으로 나누어 분석 세부적인 코드의 카피를 분석가능
- 각각 하나의 파형 필요 기존보다 빠른 속도 비교

제안 기법

비교 대상 파형을 구간으로 나눈다



원본 파형과 상관관계 분석

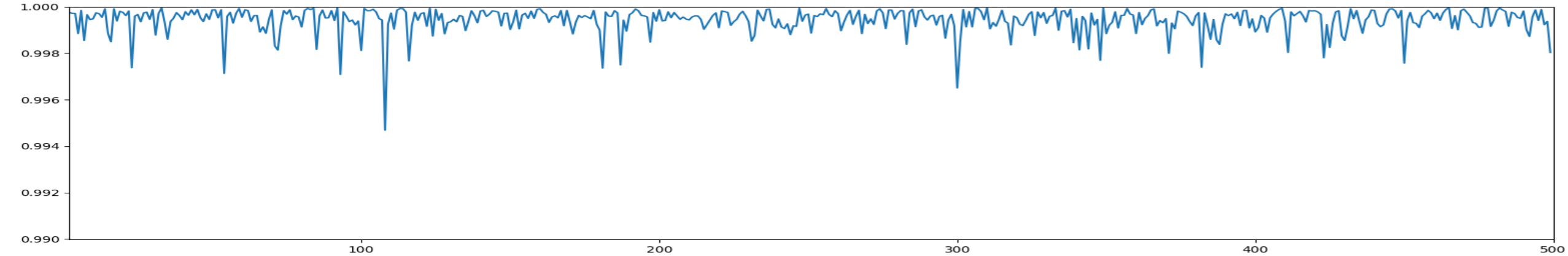


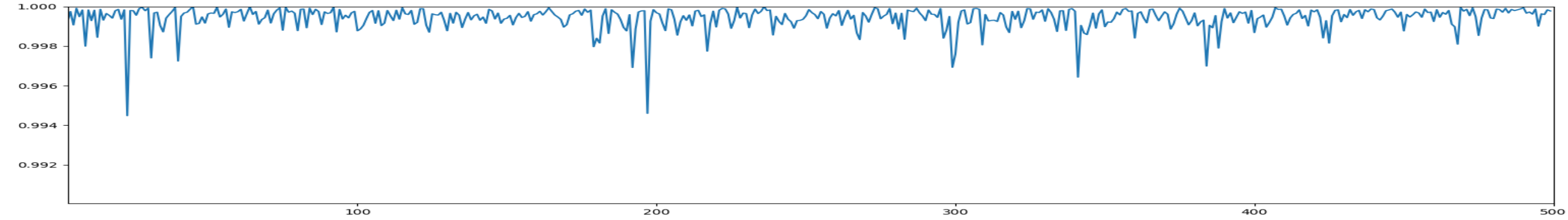
각 구간의 상관계수 중 가장 큰 값을 비교

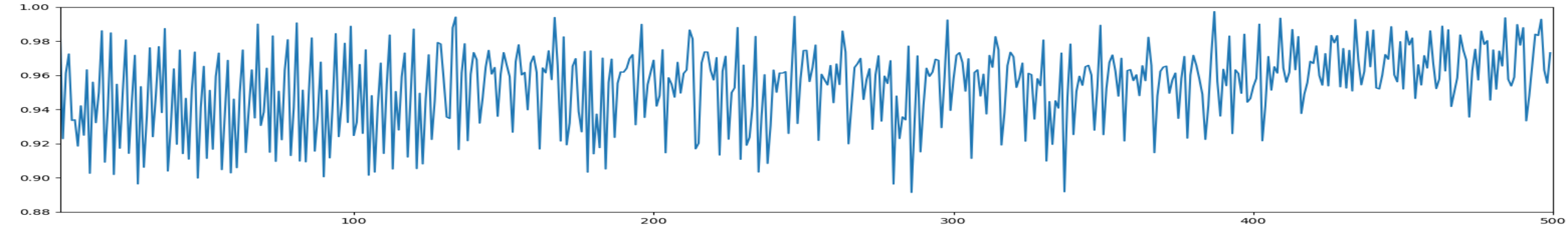
실험

- Chipwisperer Capture로 수집
- Xmaga board
- AES C코드 1라운드 파형 수집
- 7.38 MS/s 샘플링
- 파형을 8 point로 나눔

관련 없는 코드 간 비교


1.000
0.998
0.996
0.994
0.992
0.990
100
200
300
400
500


1.000
0.998
0.996
0.994
0.992
100
200
300
400
500


1.00
0.98
0.96
0.94
0.92
0.90
0.88
100
200
300
400
500

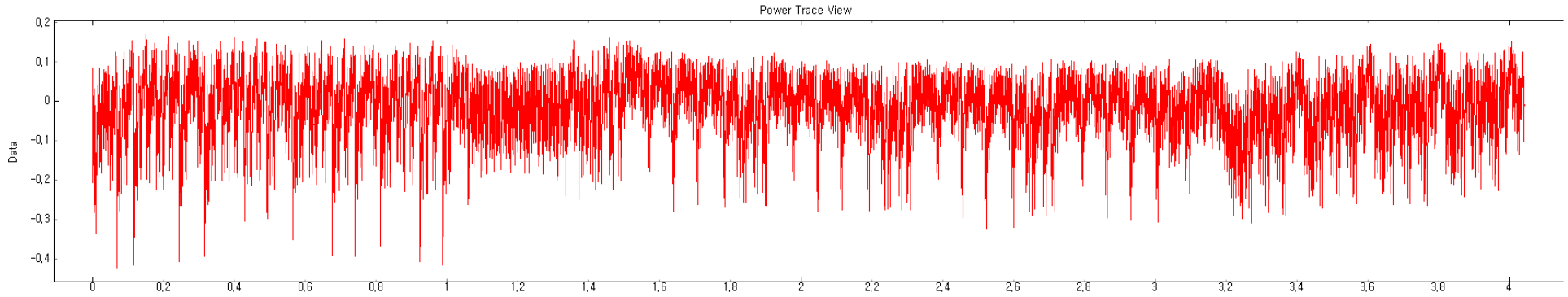
적은 양의 더미 추가

SubBytes

ShiftRows

MixColumns

AddRoundKey



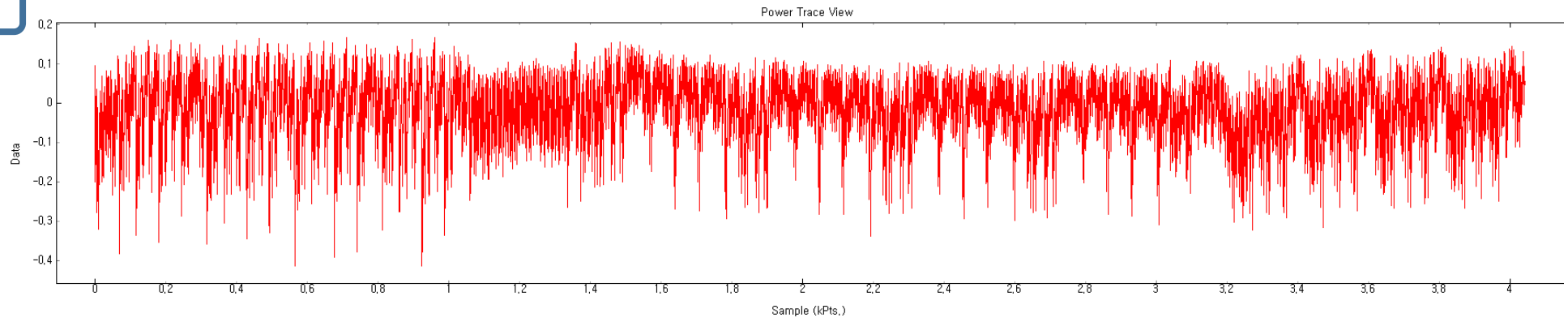
nop

SubBytes

ShiftRows

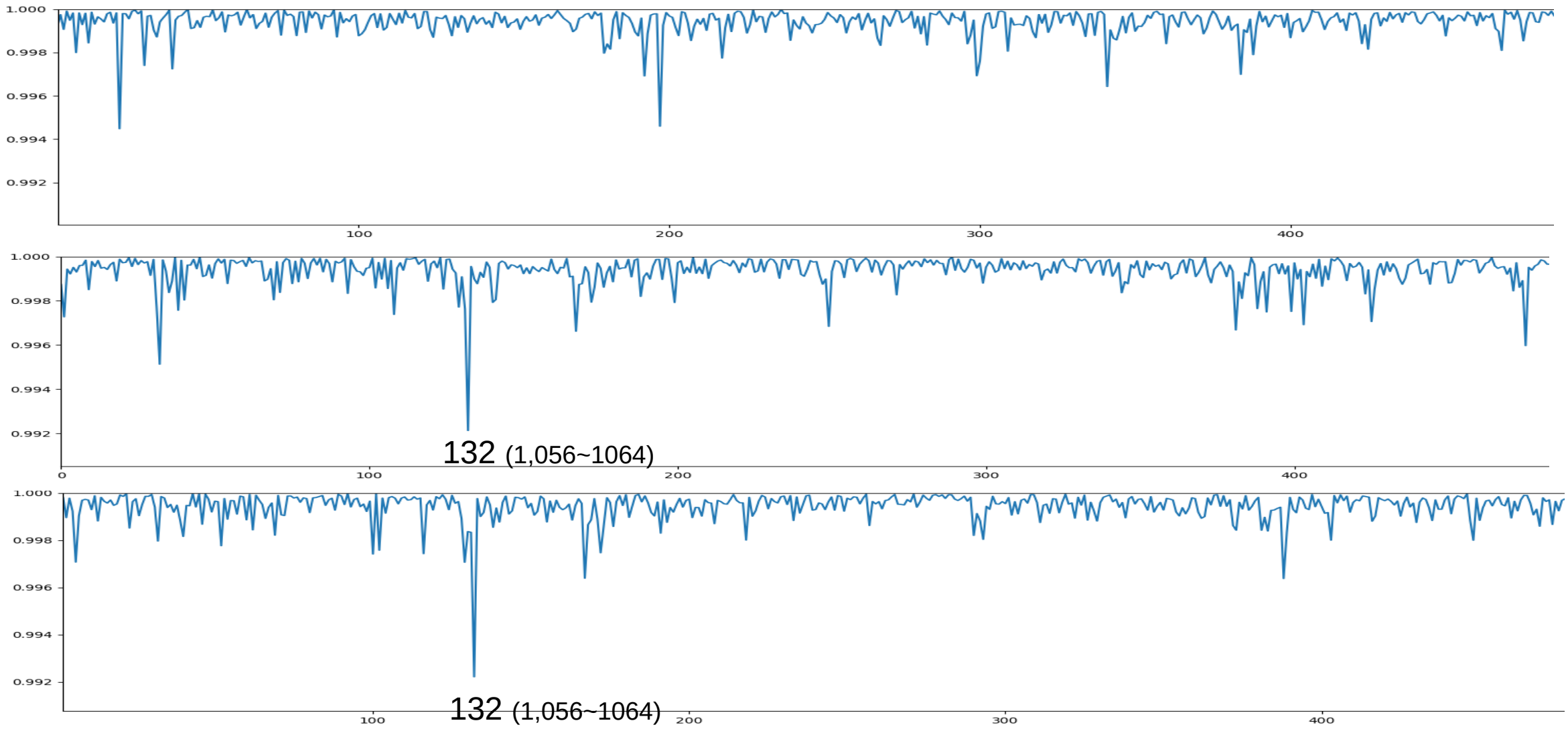
MixColumns

AddRoundKey



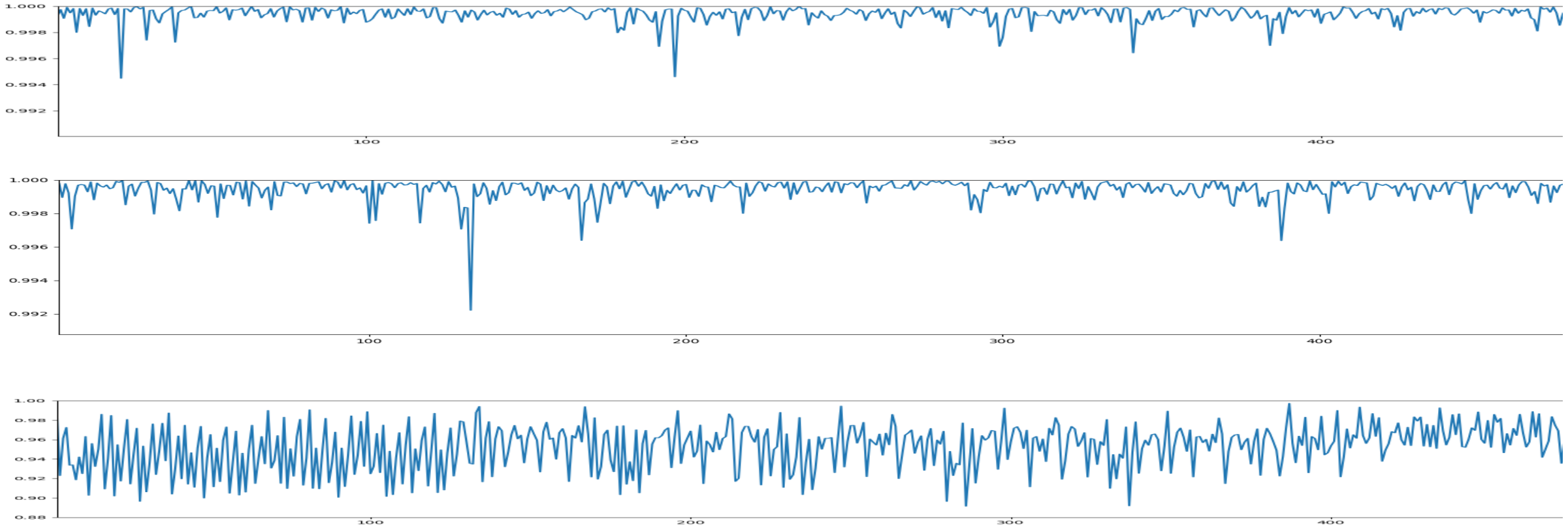
대략 1050~1070 사이

원본 코드와 더미코드와 비교



진행 사항

- 판단 기준 필요


1.000
0.998
0.996
0.994
0.992
100
200
300
400
1.000
0.998
0.996
0.994
0.992
100
200
300
400
1.00
0.98
0.96
0.94
0.92
0.90
0.88
100
200
300
400

진행 사항

- 같은 암호의 다른 구현 비교

- 견고성 테스트
  - 가산기 : 레지스터 또는 SRAM 주소 변경
  - 교환 : 가능한 경우 교환
  - dumo : 라운드 밖에 더미 작업 추가
  - Dumi : 라운드 안에서 더미 작업 추가

- 32비트 보드에서 비교

Q & A