웹상에서의 CHAM 성능 측정

유튜브 주소 : https://youtu.be/M05bQVvQ2vw

CHAM / Ajax / API

구현 과정

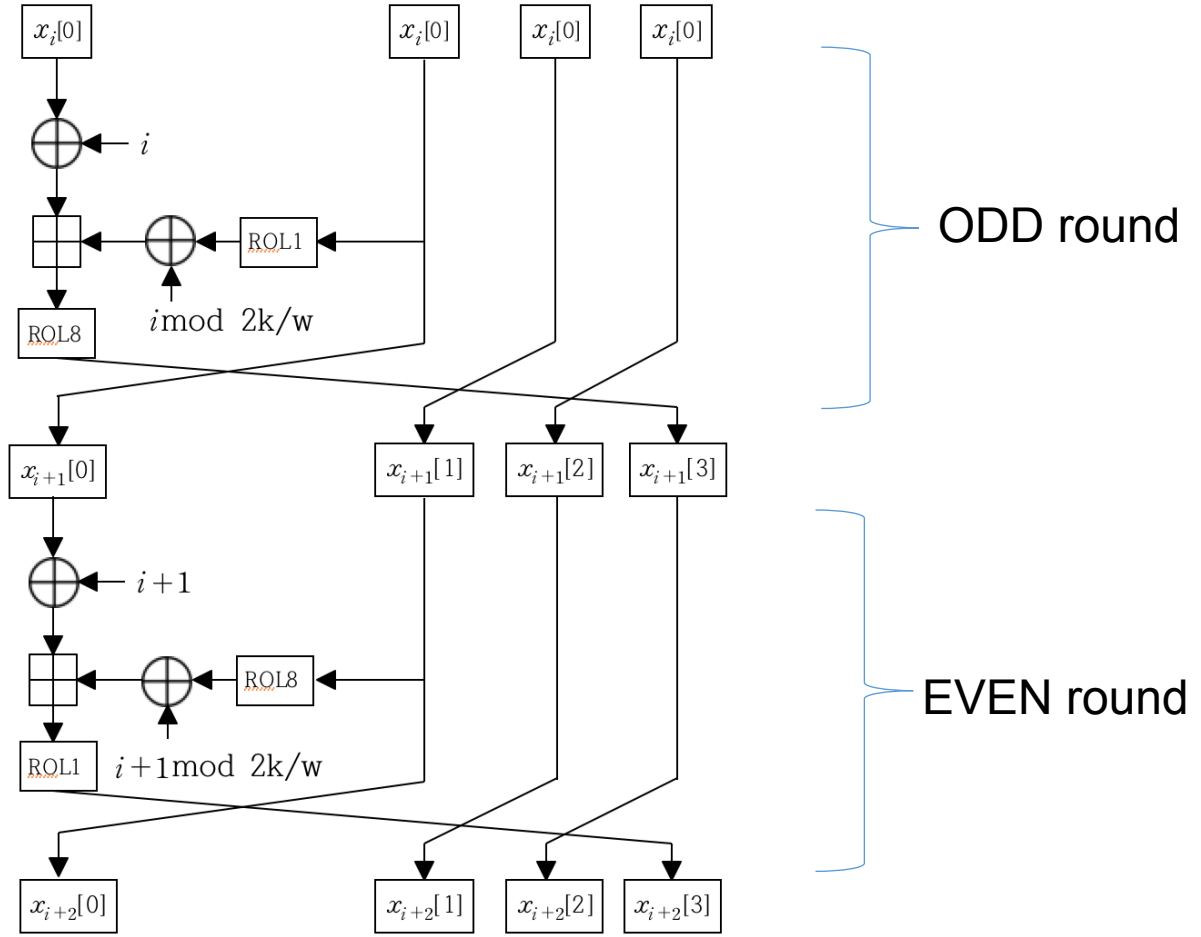
성능 측정 결과

CHAM

- IoT 환경에서 사용되는 것을 목적으로 개발된 국산 경량암호알고리즘

- 세가지 타입 존재
  - 64/128, 128/128, 128/256

- 라운드 횟수
  - 64/128 : 88 round
  - 128/128 : 112 round
  - 128/256 : 120 round



Ajax

Ajax – Asynchonous Javascript And Xml(비동기식 JS와 xml)

- JS 라이브러리 중 하나임

- JS를 이용해 클라이언트-서버간 XML 데이터(혹은 JSON)를 주고 받는 기술

- Ajax로 주로 하는 작업
  - 웹 페이지 새로고침 없이 서버에 요청(Request) -> 비동기 서버 통신 방식
    - 웹 페이지의 속도 향상
  - 서버로부터 데이터를 받고 작업을 수행

API

API - Application Programming Interface

- 응용 프로그램에서 기능을 사용하거나 데이터를 주고 받기 위한 기능

- API 구성 요소
  - 요청정보(요청 URL, 요청 방식(GET/POST…))
  - 서버가 제공할 기능(회원 데이터 조회, 게시판 생성 등)
  - 응답데이터(어떤 key로 데이터를 줄지?)
    - E.g. return render_template('main.html', data=results)

- E.g. 은행에서 돈을 인출한다고 할 때
  - 고객 - 클라이언트, 은행 – 서버, 창구 – API
  - 고객은 정해진 창구를 통해 은행에 인출을 요청함

구현 과정

- 키 생성 및 암호화 알고리즘 테스트 웹 페이지 구현
  - 간단한 웹 페이지로 각 알고리즘 수행에 소요된 시간 출력
  - 다양한 브라우저에서 테스트 진행

- Python으로 구현된 CHAM 알고리즘을 API 형식으로 작성
  - 웹 상에서 Python 성능 테스트를 하기 위함
  - Python 기반 웹 프레임워크인 Flask 사용해 웹 서버 및 페이지 구축

- 각 알고리즘 수행 시간을 측정 후 Cpb 계산
  - Cpb 공식: 밀리초 / 반복횟수 / 1000(초로 환산) * 동작 주파수 / 입력 바이트

성능 측정 결과

Cipher	browser	KeyGen	Encrypt
CHAM 64/128	Chrome	10171,08	48761,23
	Safari	9202,68	46976,32
	Opera	10055,29	47318,69
	Firefox	10313,39	46754,94
	Whale	9276,79	47280,96
CHAM 128/128	Chrome	2759,21	29485,92
	Safari	2682,73	28062,88
	Opera	2634,27	28155,29
	Firefox	2622,82	27952,48
	Whale	2620,49	27895,76
CHAM 128/256	Chrome	5228,29	30170,31
	Safari	4764,26	28776,02
	Opera	5101,94	28736,92
	Firefox	5054,84	28535,91
	Whale	4743,31	28567,38

Q & A