암호학의 역사 - 차세대 암호

KAIST 정보보호대학원

20225494 손민철

Contents

1. 현대 암호

A. 대칭키 암호

- **대칭키 암호**는 암호화와 복호화를 할 때 동일한 키가 사용되는 암호 시스템
- 암호를 생각할 때 쉽게 떠올릴 수 있는 카이사르 암호, 에니그마 등은 모두 대칭키 암호
- 1975년 미국 국립표준기술연구소(NIST)는 DES를 제시, DES가 키 길이의 부족으로 인해 점차 안전하지 않게 되자 전세계를 대상으로 한 공모를 거쳐 1997년 AES를 대칭키 암호의 표준으로 새롭게 선정

1. 현대 암호

B. 공개키 암호

- **공개키 암호**는 암호화 키와 복호화 키가 다른 암호 시스템
- 대칭키 암호 시스템에서는 송신자와 수신자가 동일한 키를 공유해야 하기 때문에 암호 통신을 하기 전에 반드시 한 번은 만나서 키를 교환해야 함. 반면 공개키 암호에서는 암호화 키와 복호화 키가 다르기 때문에 송신자는 복호화 키를 비밀리에 가지고 있고 수신자에게 암호화 키를 공개. 이 암호화 키는 공격자에게 공개되어도 상관 없음
- 소인수분해($n(=pq)$으로부터 p, q를 복원)의 어려움을 기반 문제로 둔 RSA, 타원 곡선에서 이산 로그 문제($P, Q(=tP)$로부터 t를 복원)의 어려움에 기반을 둔 ECC가 널리 쓰이고 있음
- RSA, ECC 모두 양자 컴퓨터로 다항 시간에 풀이를 하는 방법이 알려져있기 때문에 양자 컴퓨터의 상용화 이후로는 사용 불가

2. 차세대 암호

A. 양자 내성 암호

- 현재 주로 쓰이는 RSA, ECC는 모두 정수론 혹은 대수학적인 문제를 기반 문제로 사용하는데 이들은 양자 컴퓨터로 다항 시간에 해결됨이 증명됨
- NIST에서는 2017년에 전세계의 공모를 받아 양자 컴퓨터가 나온 후에도 안전할 **양자 내성 암호**를 선정 중, 2022년 11월 현재는 4라운드에 도달
- 처음에 제안된 82개의 암호 중 `CRYSTALS-KYBER`, `CRYSTALS-DILITHIUM`, `FALCON`, `SPHINCS+` 총 4개가 남아 표준화 작업이 예정됨
- `SPHINCS+`를 제외한 나머지는 격자 문제에 기반을 두고 있어 격자 문제에 대한 효율적인 해결 방법이 나온다면 무용지물이 될 위험성이 있는 반면 `SPHINCS+`는 암호학에서 굉장히 널널한 가정이라고 여겨지는 오로지 해시 함수의 역상 저항성만 기반 문제로 두고 있기 때문에 성능이 비교적 좋지 않음에도 불구하고 표준화에 포함

2. 차세대 암호

B. 다자간 연산

- **야오의 백만장자 문제**(1982) : 두 명이 서로의 재산을 비교하고 싶다. 그런데 이 때 상대방에게 자신의 재산이 얼마인지 공개 하지 않고 누구의 재산이 더 많은지 비교하고 싶다.
- 제 3자가 있다면 쉽지만 제 3자가 없다면..?
- **다자간 연산** : 두 사람이 각자의 입력 x, y를 가지고 있을 때 함수 $f(x, y)$를 계산하면서도 서로 상대방의 입력을 모르게 하는 연산
- 대표적인 응용 사례 : 프라이버시 보존 머신 러닝

2. 차세대 암호

C. 동형 암호

- **동형 암호** : 암호문을 복호화 없이 연산할 수 없는 기술,
  $E(x+y) = E(x) + E(y), E(xy) = E(x)E(y).$
- 1970년 처음 개념이 제시된 이후 2009년 최초로 방법이 현실화됨, 처음에는 연산에 각 비트당 30분이 필요했던 반면 지금은 0.5ms로 속도가 급속도로 개선됨

ex) 연구팀에서 각 권역별 40대의 평균 소득을 구하기 위해 통계청에 자료를 요청하고 싶음. 소득 데이터는 너무 민감한 데이터라 그대로 데이터를 넘겨주기는 힘들고(심지어 법적 문제가 있을 수도 있고), 그렇다고 이런 요청이 들어올 때 마다 통계청에서 직접 계산을 해서 값만 알려주는건 힘듬

이럴 때 동형 암호를 사용하면 소득 데이터 평문 $m_1, m_2, \ldots, m_n$를 주는 대신 $E(m_1), E(m_2), \ldots, E(m_n)$을 알려주고 연구팀은 이를 토대로 $E(m_1 + m_2 + \cdots + m_n) = E(m_1) + E(m_2) + \cdots + E(m_n)$을 계산한 후 통계청에 복호화를 요청