미래의 암호 해독, 프로그래밍 가능한 암호화

(2024.05.08., 양자정보연구지원센터)

□ 프로그래밍 가능한 암호(Programmable Cryptography), 범용적 도전 과제 해결할 수 있음

○ 암호 기술이 발전함에 따라 그 활용 범위가 늘어나고 복잡해지고 있음

- 단순한 암호 기본 원리로는 많은 것을 할 수 있지만, 그것들이 결합될 때 가장 흥미로운 결과를 얻을 수 있음
- 일부 암호 프로토콜이 하드웨어 설명 능력을 갖추고 있어, 범용적인 도전 과제를 해결할 수 있음
- 이는 수학적 문제를 해결하고 새로운 프로토콜을 설계하는 것을 기존의 것을 결합하는 프로그래밍 문제로 바꾸는 것임(Brian Gu)

○ 프로그래밍 가능한 암호(Programmable Cryptography)가 일상생활에서 어떻게 가장 유용하게 사용될 수 있는지 결정하기 위해서는 암호 응용 프로그램의 다양한 계층을 이해하는 것이 필요함

○ 기초 이해, **프로그래밍 가능한 암호의 단순한 암호 기원**

- 일상에서 데이터 의존도는 높아지고 있으며, 데이터 보호가 중요해지고 있음, 암호학은 데이터 보호를 위한 핵심 역할을 함
- 암호학은 간단한 개념에서 출발하여 복잡한 시스템을 만들어 냄
- 예를 들어, 시저 암호(Cesar cipher)와 비제네르 암호(Vigenère cipher)는 간단한 방법을 결합하여 강력한 보안 시스템 구축에 사용될 수 있음
- 또한, RSA(Rivest-Shamir-Adleman), AES(Advanced Encryption Standard) 같은 암호학적 기본 원리는 다양한 문제에 적용될 수 있음
- 이러한 방법을 결합하여 더 강력한 보안 시스템을 만들 수 있지

만, 한계도 있음

- 항상 새로운 방법을 개발하는 것보다 기존 방법을 결합하여 더 나은 보안 시스템을 구축하는 것이 더 효율적임

○ **중간 프로토콜을 통한 개인 정보 보호 강화**

- 중간 수준의 프로토콜은 더 고급 기능과 기능성을 목표로 함
- 동형 암호화(Homomorphic encryption)는 데이터를 복호화하지 않고 처리할 수 있도록 해주는 프로토콜로, 의료 기록과 같은 민감한 데이터 보호에 사용될 수 있음
- 다중 당사자 계산(MPC, Multi-Party Computation)은 다른 주체들이 협력하여 결과물을 도출할 때 입력을 숨기는 도구로, "백만장자 문제(Millionaire problem)"와 같은 상황에 적용될 수 있음
- 제로-지식 증명(ZKPs, Zero-Knowledge Proofs)은 어떤 것이 사실인지 보여주는 데 사용되며, 대표적인 예로 zk-SNARK 와 zk-STARK 가 있음
- 이러한 고급 프로토콜에 대한 연구는 암호학이 범용 계산을 안전하고 비공개로 수행할 수 있다는 가능성을 보여줌

○ **프로그래밍 가능한 암호학의 미래**

- 프로그래밍 가능한 암호학은 암호학의 새로운 패러다임으로, 기존 시스템을 재구성하거나 완전히 새로운 시스템을 구축하지 않고도 복잡한 문제를 해결할 수 있는 기술임
- 이러한 접근 방식은 고급 언어로 작성된 코드를 해석하고 회로로 변환하여 암호학적 프로토콜에 적용함으로써 실용적인 프로그래밍 환경을 제공함
- 이는 보안 및 개인 정보 보호에 적용할 수 있으며 미래에 더 많은 혁신이 예상됨

(원문)

1. https://thequantuminsider.com/2024/04/23/guest-post-decrypting-the-future-programmable-cryptography-and-its-role-in-modern-tech/