제목 : G 인증 및 키합의 프로토콜(5G-AKA)의 보안취약점과 PUF 기반의 보안성 향상 방안

1.연구 배경:

-5G 네트워크에서 사용되는 5G-AKA 프로토콜은 인증 및 키 합의를 담당하

-5G-AKA는 사용자 장치와 네트워크 간의 안전한 통신을 보장

-그러나 기존의 5G-AKA 프로토콜은 보안 취약점을 가지고 있어, 이를 해결하기 위한 연구가 필요

-이러한 배경에서 물리적 복제 방지 기능인 PUF를 활용하여 보다 안전한 5G-AKA 프로토콜을 설계하는 것이 필요

2.연구 내용

-PUF를 이용한 새로운 5G-AKA 프로토콜의 설계와 구현을 함.

-PUF를 활용하여 각 장치마다 고유한 응답값을 생성하고, 이를 이용하여 키 합의 및 인증 과정을 수행 또한, 해시 함수를 통해 응답값을 처리하여 보안성을 높임

- 이를 통해 기존의 5G-AKA 프로토콜의 보안 취약점을 보완하고, 화이트리스트 정책을 구현할 수 있게 됨

3.향후 방향:

향후 연구 방향으로는 PUF를 적용한 5G-AKA 프로토콜의 보안성을 더욱 강화하는 방법을 탐구돼야 함.

또한, 효율적인 PUF 구현 방법 및 적용 가능한 환경에 대한 연구를 진행하여 실제 산업 및 서비스에 적용 가능한 기술로 발전시켜야 함.