AES 구현 최신 동향

권 용 빈, 권 혁 동, 서 화 정
한성대학교 IT응용시스템공학과

Technology trends of Implementation of AES

Yongbeen Kwon, Hyeokdong Kwon, Hwajeong Seo
Hansung University Applied IT Department

요약

암호에 대한 관심의 증가와 더불어 IoT와 같은 새로운 인터넷 환경의 등장으로 암호의 최적화 연구의 속도는 더욱 가속화되고 있다. 한편, 암호로서 오랜 역사를 가지고 있는 Advanced Encryption Standard (AES)는 암호 분석이 충분히 진행된 지금에도 쉬운 구현과 그 안전성을 인정받아 여전히 사용되고 있는 블록 암호 알고리즘이다. 본 발표에서는 새로운 환경이 암호 알고리즘에 요구하는 조건들을 알아보고, AES가 이러한 조건을 만족시키기 위해 어떠한 구현 기법이 적용되고 있는지 살펴본다.

The pace of the optimization study on the cipher is accelerating with increasing interest in cipher and appearing on new internet environment such as IoT. Meanwhile, in spite of enough cryptanalysis Advanced Encryption Standard (AES) which has long history as a cipher is still used as a block cipher algorithm because of easy implementation and strong security. In this presentation, we will talk about what conditions new environment requires on cipher and which implementation technique are applied on AES.