MASKING COUPLING EFFECT 최신 동향

권 혁 동, 권 용 빈, 서 화 정
한성대학교 IT응용시스템공학과

Technology trends of Masking Coupling Effect

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

요 약

부채널 공격은 장비 자체를 공격하지 않고 장비에서 발생하는 빛과 소음, 전기적 신호등을 분석하여 비밀 정보를 유추하는 강력한 보안 위협이다. 이러한 부채널 공격에 대응하기 위해서 마스킹 기법이 개발되었다. 마스킹 기법은 평문에 적절한 마스크 값을 씌워서 부채널 정보를 변형하는 것으로 정확한 값 유추를 어렵게 한다. 하지만 일정 조건 하에서 마스크 값이 소실되는 현상이 발견되었다. 마스킹이 해제된 값은 부채널 공격에 취약하기 때문에 이러한 현상을 커플링 현상이라 명명하고 여러 가지 원인 분석에 역량을 기울이기 시작했다. 따라서 현 시점까지 밝혀진 커플링 현상에 대해 조사해보며 이를 완화할 수 있는 방법에 대해 살펴본다.

ABSTRACT

The Side Channel Attack is a strong security threat to guess confidential information by analyzing the light, noise, and electrical signals has generated from equipment without attacking the equipment itself. The Masking Technique has been developed to counter this Side Channel Attack. The Masking Technique modifies the side channel information by covering with an specific mask value, which makes it difficult to guess an accurate value. However, the mask value can be lost under certain conditions. The value has lost mask value is vulnerable to Side Channel Attack. This phenomenon called as Coupling Effect and started to study the cause analysis. We will investigate the Coupling Effect revealed up to now and discuss how to mitigate it.