# COLLOQUIUM

## 부채널분석(Side Channel Attack) 최신연구동향

▣ 연 사 : 한동국 교수님(국민대)

▣ 일 시 : 2010년 4월 8일 (목) 4:30~5:30

▣ 장 소 : 수학전공 강의실 (31316호)

▣ 대 상 : 수학전공 학부생 및 대학원생

▣ 다 과 : 4시 15분부터 31316호실 앞

# Abstract

암호학자들은 종래의 **수학적인 공격에 안전한** 암호 알고리즘의 설계에 매우 성공적이었다. 그러나 이러한 알고리즘이 현실에 사용되는 암호장비, 예를 들면 스마트카드나 모바일에 구현되는 경우, 암호시스템의 안전성에 문제가 생길 수 있음이 증명되었다. 즉 암호 알고리즘을 보안장비에 구현할 때, 알고리즘을 개발할 때에는 예상하지 못했던 취약점을 가질 수가 있다는 것이다. 이와 같은 분석들을 총칭해서 처음으로 "**부채널 분석 (side channel attacks)**" 이라는 이름을 사용했다. 스마트카드와 같은 물리적 보안 장비에서 의도되지 않게 발생되는 부가정보를 총칭해서 "부채널 (side channel)" 이라는 이름으로 사용되고 있다. 본 발표에서는 부채널 분석의 개념 및 최근 연구동향을 소개한다.