N1에서 열리는 산학협업 소프트웨어 프로젝트 수업이 늦게 끝나 4시 20분 즈음에 착석하였다.

**Physical attacks**

Physical attack의 세 가지 종류로 Correctness attack, Side-channel attack, 그리고 Fault attack이 있다고 말한다. Correctness attack이란 내부를 들여다볼 수 없는 함수에 제작자가 의도하지 않은 입력을 집어넣어 해석하는 것을 말한다. Side-channel attack은 소프트웨어 바깥의 요소를 이용하여 암호를 공격하는 것을 의미한다. 마지막으로 fault attack은 프로그램 실행 도중의 변수를 조작하는 공격을 말하는 것으로 보였다. 마지막 두 공격은 각각 passive, active attack에 속한다.

Side-channel attack의 대표적인 예시는 Kocher의 RSA 공격이 있다(Timing attack, 1996). RSA 암호문을 복호화하는데 사용되는 Fast-exponentiation 알고리즘은 지수 속 1의 갯수에 따라 소모시간이 다르다. 소극적으로는 소모시간의 비교를 통해 1의 개수를 세어 조합적인 접근이 가능하고, 적극적으로는 자릿수가 0일 때와 1일 때의 전력 소모량을 기록하여 암호화 키를 찾을 수도 있다.

앞의 Kocher 공격을 회피하기 위한 변형 계산(RSA-CRT transform)에서 Fault attack의 위험성이 있다. RSA-CRT는 암호화 키를 mod p-1, mod q-1로 쪼갠 뒤 p, q를 법으로 각각 지수계산을 마친 뒤 중국인 나머지 정리를 통해 암호화된 메시지를 얻는 방식인데, 이 과정 중 하나의 암호문(sigma\_q)이 변조될 경우 비밀 키를 복구할 수 있게 된다. 이 때 만들어지는 암호문에 공개 키를 곱하면 N으로부터 p, q를 복원할 수 있게 된다. (Bellcore’s fault attack)

**Physical attack의 최신 기술**

ECDSA 전자기분석 : 소형 전자기기의 주파수 대역 잡음을 통해 key를 찾는 방법이 제시되었다.

급속 메모리 냉각 : 메모리상의 데이터 휘발을 막아 임시 변수를 습득할 수 있게 한다.

이외에도 Lucky thirteen attack, modulus fault attack, PC 등에 대한 acoustic attack이 언급되었다.

**Post-quantum attack**

1993년 Peter Shor가 양자 소인수분해 알고리즘을 제시한 이후, 소인수분해 및 이산로그 문제에 기반한 현대 공개키 암호가 양자 공격에 의해 다항 시간 안에 해독될 수 있게 되었다. 양자컴퓨터 공격에 대해 안전한 체계의 필요성이 대두되면서, 자료구조 수준부터 양자 공격을 회피할 수 있는 암호 시스템이 설계되고 있다.

강의 시간에는 postquantum signature scheme의 예시로 BLISS를 소개하였다. Side-channel attack 및 샘플링 공격을 방어할 수 있다는 점을 언급하였으며, 시간상 알고리즘 내부에 대해서는 간략하게만 설명하고 발표를 마쳤다.