이 희 정 (강남대학교)

Cryptanalysis of RSA Criptosystem

1977년 Rivest, Shamir, Adelman에 의해서 개발된 RSA는 현재까지 가장 널리 쓰이고 있는 공개키 암호체계이다. 이러한 RSA암호체계는 20여년 동안 공격에 견디어 왔는데 1999년 Dan Boneh가 "Twenty Years of Attacks on RSA Cryptosystem"이란 논문에서 이러한 공격들에 대하여 조사해 놓았다. 이러한 공격들은 암호체계를 구성하고 있는 파라메타들의 사용상의 부주의에 의해서 가능한 것이었으나 근본적인 RSA 암호체계의 안전성을 위협하는 것은 아니었다. Boneh는 이러한 고찰을 통하여 RSA 암호체계의 안전성을 유지하기 위해서는 메시지의 random padding이 중요하다고 언급하였다. 그후 다시 Dan Boneh와 Antoine Joux, Phong Nguyen이 "Why Textbook ElGamal and RSA Encryption are insecure"에서 파라메타의 사용에 관계없이 메시지의 특성상 메시지를 미리 'preprocessing'하지 않고 쓴다면 안전하지 않다는 것을 보였다. 현재 표준화되어 있는 RSA 암호체계는 OAEP(Optimal Asymmetric Encryption Padding)이다. 결론적으로, 메시지 preprocessing이 RSA 암호체계의 안전성에 결정적 역할을 할 것이라고 주장하고 있다. 본 발표에서는 RSA 암호체계 공격의 핵심논리인 Coppersmith정리에 대해서 알아보도록 한다. Lattice Reduction Theory를 이용하여 증명하였다. Coppersmith정리를 이용한 Coppersmith's short pad attack과 Hastard Broadcasting Attack을 살펴보고 비밀키의 크기가 얼마나 크게 해야 안전한가에 관한 내용과 그곳에 활용된 Coppersmith정리의 miltivariate 경우에 관해서 알아보도록 한다.