Lattice-based cryptanalysis

Nadia Heninger, University of California, San Diego

Lecture 1 Background on public-key cryptography in the real world

In this lecture, we will review classical public-key cryptography as used in real-world protocols, including RSA encryption and signatures and common padding schemes, Diffie-Hellman and elliptic curve Diffie-Hellman key exchange, and DSA and ECDSA signatures. This lecture will focus on the mathematical structure of these schemes as it interacts with real-world implementation choices and protocol usage.

Lecture 2 Background on lattices

In this lecture, we will review basic background on lattices necessary for cryptanalysis. A lattice is a discrete subgroup of R^n. Finding the shortest vector in a lattice given an arbitrary basis for this lattice is an NP-hard problem, but this problem is possible to efficiently solve approximately using lattice basis reduction algorithms like LLL and BKZ. This lecture will review some of the basic mathematical structures and properties of lattices such as bases, reduction, and duality that are necessary for cryptanalysis.

Lecture 3 Lattice attacks against RSA

This lecture will cover lattice attacks against RSA. Our basic technique will be Coppersmith's method for finding small solutions to low-degree polynomials modulo integers using lattice basis reduction. We will cover how to formulate problems that arise in the cryptanalysis of RSA as Coppersmith-type problems, such as factoring with partial information, and breaking low-exponent RSA used with weak padding schemes, and show how to solve these problems efficiently in practice.

Lecture 4 **Lattice attacks against discrete log-based schemes**

This lecture will cover lattice attacks against discrete log-based crypto schemes, in particular DSA and ECDSA. Our basic technique will be the hidden number problem. We will show how to formulate the problem of breaking weak DSA/ECDSA signatures as a hidden number problem, and show how to solve the hidden number problem efficiently using lattices.