CAA 24-25

Lab #2

04-11-2024

Introduction

In this lab, we are going to study what can go wrong with ECDSA. We will both analyse weird deterministic-ECDSA algorithms and some random ones. The most complex part of the lab is the lattice-reduction attack that allows to recover the private key when part of the nonce is known. A good additional resource for this part is this paper: https://eprint.iacr.org/2019/023.pdf. You will have to submit your code and a small report on cyberlearn.

Lattice Attack on the hidden number problem

In this section, we describe how one can solve the `hidden number problem` using lattice attacks. The hidden number problem is the following problem: Let $\alpha \in \mathbb{Z}_p$ be a secret. Let B be a known bound, with B much smaller than p. Given (t_i, a_i) such that $t_i\alpha - a_i \bmod p = b_i$, with $b_i < B$, find the secret α.

This problem can be solved using lattice reduction, more precisely using the LLL algorithm. Here is how you can proceed:

- Create the following matrix over the rational numbers $\mathbb{Q}$:

$$M = \begin{bmatrix} p & & & & & \\ 0 & p & & & & \\ & & \ddots & & & \\ & & & p & & \\ t_1 & t_2 & \dots & t_m & B/p & 0 \\ a_1 & a_2 & \dots & a_m & 0 & B \end{bmatrix}$$

  Empty elements are zero in this matrix. To do this, define first the matrix space over $\mathbb{Q}$ in Sage using `MatrixSpace(QQ, rows, cols)` and obtain an identity matrix in this space using the method `identity_matrix()`. Let A be this identity matrix. You can modify row i, column j using `A[i,j] = new_val`.

- Call the LLL algorithm (with method `LLL()` on this matrix to obtain a equivalent basis with shorter vectors.

- If it succeeded, the vector $(b_1, b_2, \dots, b_m, B\alpha/p, B)$ is a short vector in this matrix and you can recover α.

1 Questions

It might be easier to answer these questions after having done the practical part of the lab.

1.1. Explain why is the vector $(b_1, b_2, \dots, b_m, B\alpha/p, B)$ is a linear combination of the rows of the matrix M.

1.2. Explain why the vector $(b_1, b_2, \ldots, b_m, B\alpha/p, B)$ is small compared to p.

1.3. Explain what the LLL algorithm does.

2 Challenge 1

In this first challenge, we will use the lattice attack on ECDSA to recover the secret key when some bits of the nonce are known. The implementation is in the function `sign1`.

2.1. First, we need to convert our problem into a hidden number problem. Explain in your report how you convert the problem of recovering the ECDSA private key when the τ most significant bits of the nonce k are set to 0 into a hidden number problem.

2.2. You are given 20 ECDSA signatures for which the last 32 bits are always zero and the public key. Recover the private key.

3 Challenge 2

The function `sign2` shows you an implementation of deterministic ECDSA. You are given 20 ECDSA signatures and the public key. Break the construction, explain your attack and give the private key in your report.

4 Challenge 3

The function `sign3` shows you an implementation of deterministic ECDSA. You are given 20 ECDSA signatures and the public key. Break the construction, explain your attack and give the private key in your report.

5 Challenge 4

The function `sign4` shows you an implementation of deterministic ECDSA. You are given 20 ECDSA signatures and the public key. Break the construction, explain your attack and give the private key in your report.