NTNU | Norwegian University of Science and Technology

RANDOMNESS 2

TTM4205 – Lecture 3

Caroline Sandsbråten

29.08.2023

Contents

Contents

Caroline Sandsbråten

- 2nd year PhD student at IIK
- Tjerand is my PhD supervisor
- Researching lattice-based PQC
- I finished KomTek in 2022, thesis on ECC
- I volunteer at Samfundet. Previously in Fotogjengen, currently in ITK.

Contents

Elliptic Curves

Definitions

- (Elliptic Curves) Let K be a field. An elliptic curve over K is a non-singular cubic curve whose points satisfy the equation $Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0$.

- (Elliptic Curves over $\mathbb{F}_p$) Let $\mathbb{F}_p$, where $p \neq 2, p \neq 3$ be a finite field. An elliptic curve over $\mathbb{F}_p$ is a non-singular cubic curve whose points satisfy the equation $y^2 = x^3 + Ax + B$, and the non-singular condition $4A^3 + 27B^2 \neq 0$.

Why Elliptic Curves?

Hard problems

- (DLP) Let p be a prime, and let a, b be integers such that $a \mod p \neq 0$ and $b \mod p \neq 0$. Assume there exists an integer x such that $a^x \equiv b \mod p$ The DLP is then to find x such that $a^x \equiv b \mod p$. More generally, we have the following. Let G be any multiplicative group, and let $a, b \in G$. Assume that $a^x = b$ for some integer x. The DLP is then to find x such that the above equation is satisfied.

- Using Elliptic Curves, the same problems becomes the ECDLP:

- (ECDLP) Let $P_1, P_2 \in E(\mathbb{F}_p)$, where $E(\mathbb{F}_p)$ is an elliptic curve over a finite field $\mathbb{F}_p$ and p is a prime, and P_1, and P_2 is points on the elliptic curve $E(\mathbb{F}_p)$. The ECDLP is then to find an integer x satisfying the equation $xP_1 = P_2$.

Contents

ECDSA Signature Algorithm

(Input): Message m, private key α, the elliptic curve $E(\mathbb{F})$, and the domain parameters, G, and p.

(Output): Digital signature r, s.

(Algorithm):

$h \leftarrow hash(m)$
$k \leftarrow random(0, n)$
$(x, y) \leftarrow kG$
$r \leftarrow x \mod n$
$s \leftarrow k^{-1} \cdot (h + r \cdot \alpha) \mod p$
return r, s

- What would happen if k is not random?

ECDSA Signature Verification

(Input): Message m, public key Q, the elliptic curve E, and domain parameters of the elliptic curve G, and p.

(Output): Boolean value. True if the signature is verified as being correct, False if not.

(Algorithm):

if $Q = O$ or Q is not on E **then**
  return False
end if
$h \leftarrow hash(m)$
$u_1 \leftarrow h \cdot s^{-1} \mod p$
$u_2 \leftarrow r \cdot s^{-1} \mod p$
$(x, y) \leftarrow u_1 \cdot G + u_2 \cdot Q$
if (x, y) = O **then**
  return False
end if
if $r \equiv x \mod p$ **then**
  return True
end if
return False

Contents

What mistakes do we see in practice?

- Using a hash as a nonce
- "Smart" software made to trick people
- People trying and failing to do everything "by hand"
- And more? Let’s discuss

Two methods

- One utilizing Fourier Analysis
- One utilizing the Hidden Number Problem and lattice basis reduction
- Today: The Hidden Number Problem (HNP)

Lattices

Definition

Let $B = [b_1, \ldots, b_k] \in \mathbb{R}^{n \cdot k}$ be a linearly independent set in $\mathbb{R}^n$. The lattice $L(B)$ generated by matrix B is the set of all linear combinations of the columns of B with integer coefficients. B is thus a basis for lattice $L(B)$.

$$L(B) = \left\{ Bx : x \in \mathbb{Z}^k \right\} = \left\{ \sum_{i=1}^{k} x_i \cdot b_i : x_i \in \mathbb{Z} \right\}$$

Lattice Problems

Definition (Shortest Vector Problem.)
Given a lattice L, find a vector $v \in L \setminus \{0\}$ such that $||v|| \leq ||u_i|| \forall u_i \in L \setminus \{0\}$

Definition (Closest Vector Problem.)
Given a lattice L, and a vector u, find the lattice vector v such that $||u - v|| \leq ||u - v_i||, \forall v_i \in L$.

Solving Lattice Problems

1. The Lenstra-Lenstra-Lovàsz Algorithm (LLL)
2. The block Korkine-Zolotarev Algorithm (BKZ)

The Hidden Number Problem (HNP)

$$\begin{aligned}&\text{Adversary is given } d \text{ pairs of integers } \{(t_i, u_i)\}_{i=1}^{d}\\&\text{Such that } t_i x - u_i \mod p = b_i\\&\text{Where } |b_i| < B\text{, for some } B < p\end{aligned} \tag{1}$$

Contents

Lets try our attack

Lets write some code!

Contents

Biased Nonce Sense: Lattice Attacks against Weak ECDSA Signatures in Cryptocurrencies

Links

https://eprint.iacr.org/2019/023

Authors

- Joachim Breitner
- Nadia Heninger

The curious case of the half-half Bitcoin ECDSA nonces

Links

https://eprint.iacr.org/2023/841

Authors

- Dylan Rowe
- Joachim Breitner
- Nadia Heninger

Fast Practical Lattice Reduction through Iterated Compression

Links

Paper: https://eprint.iacr.org/2023/237
Implementation: https://github.com/keeganryan/flatter

Authors

- Keegan Ryan
- Nadia Heninger

Books

- Elliptic Curves: Number Theory and Cryptography

  https://people.cs.nctu.edu.tw/~rjchen/ECC2012S/Elliptic%20Curves%20Number%20Theory%20And%20Cryptography%202n.pdf

- Bitcoin and Cryptocurrency Technologies

  https://bitcoinbook.cs.princeton.edu/