Using lattices for cryptography

For Gymnasium Neufeld

De Kaag

1 July 2025

Ludo Pulles

Cryptology Group, CWI, Amsterdam

Morning schedule

- What are lattices and why should I care?
- Work yourself
  - Reduce lattices yourself
  - Dive in theory: high-dimensional operations $\rightarrow$ linear algebra
  - Write your own dim-2 lattice reduction!

Quantum Apocalypse

All currently used cryptography are breakable by quantum computers!

With a quantum computer, you could:

- Impersonate Google:

- Read encrypted data on public WiFi,
- ...

But, ..., we still have time before a quantum apocalypse!

New cryptographic standards

NIST writes new cryptographic standards

that resist *quantum-attackers*

developed by international researchers

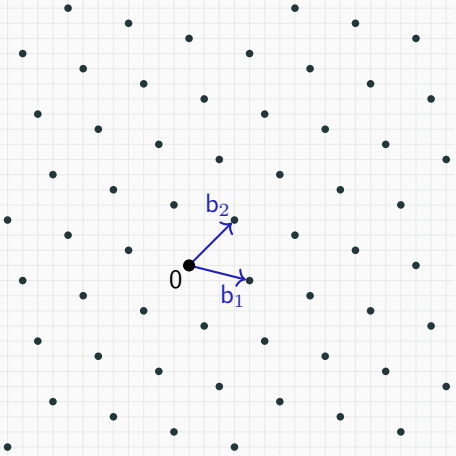
to be used **worldwide**

by **2035**

replacing **RSA** (and **ECC**).

Most promising cryptoschemes are based on lattices: ML-KEM, ML-DSA.

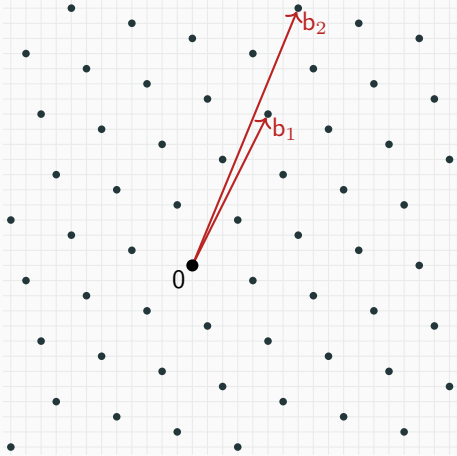
Lattice bases



Good basis
(short vectors)

Easy: randomize basis

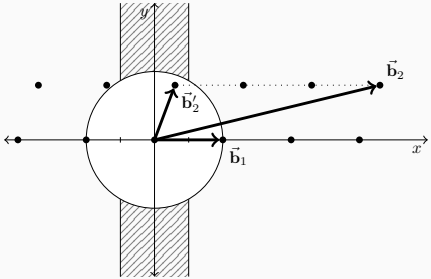
Hard: lattice reduction



Bad basis
(long vectors)

Lattice bases

Lattice reduction is hard, but not in dimension 2.

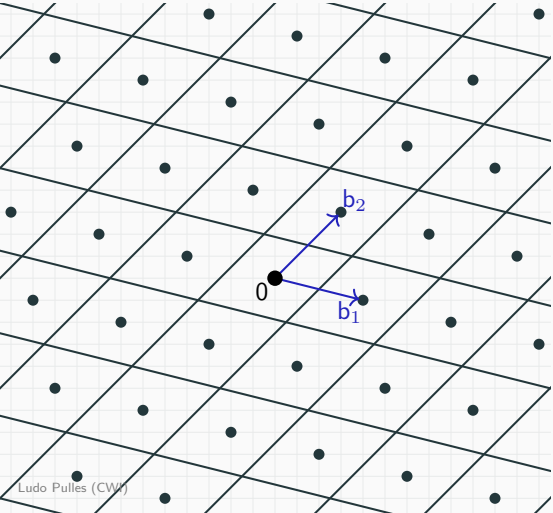


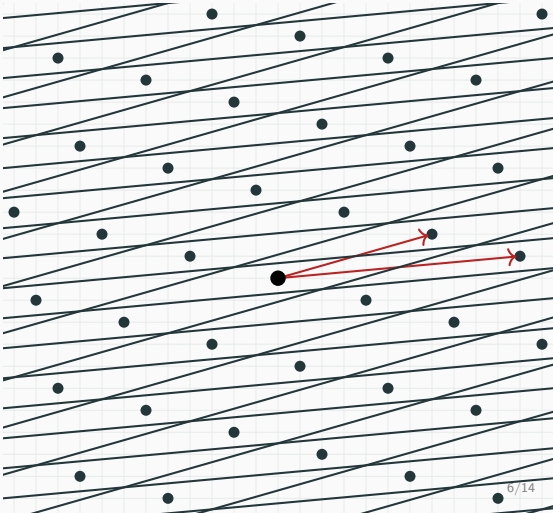
Best algorithm runs in exponential time: runtime $\approx 2^{.292n}$, as function of dimension n.

For security, we use lattices in dimension ≥ 1000.

Lattice bases

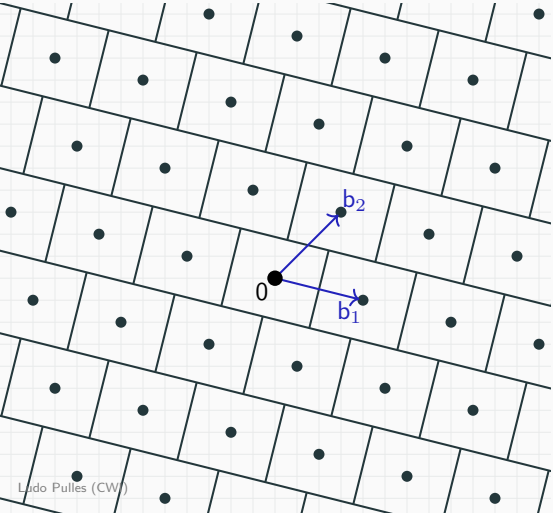
A basis tiles the space nicely or poorly.

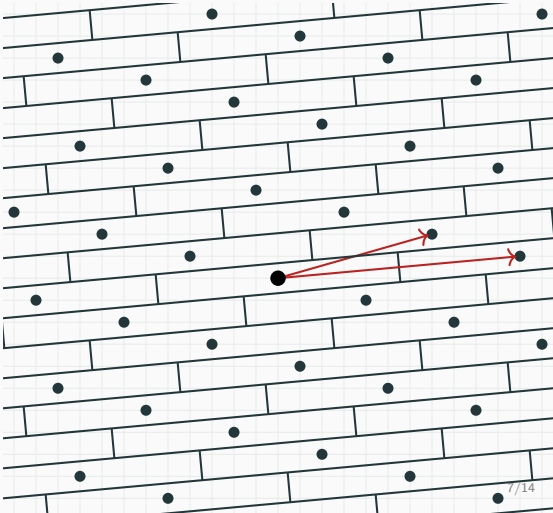




Lattice bases

A basis tiles the space nicely or poorly.



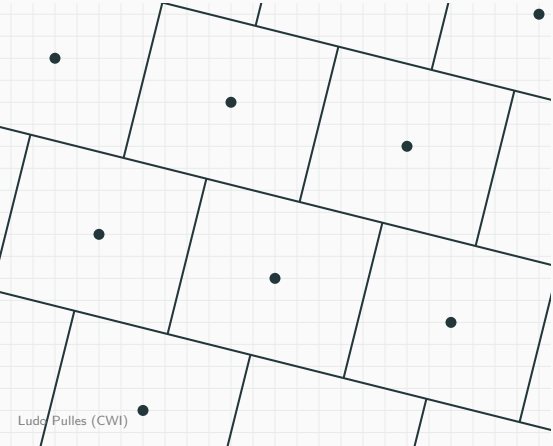


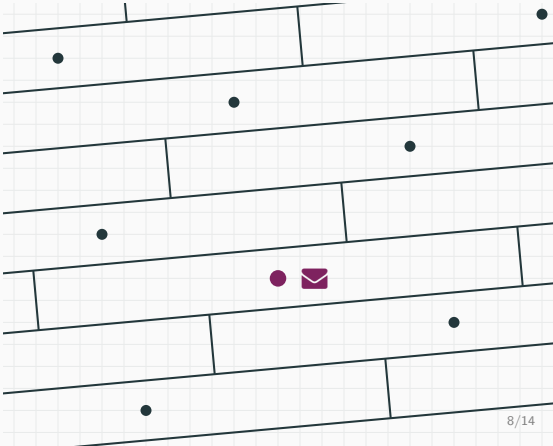
Encrypting with Lattices

Encrypting with Lattices

Situation: Bob wants to send a message confidentially to Alice.

1. Bob: convert message to lattice point $\mathbf{m}$.

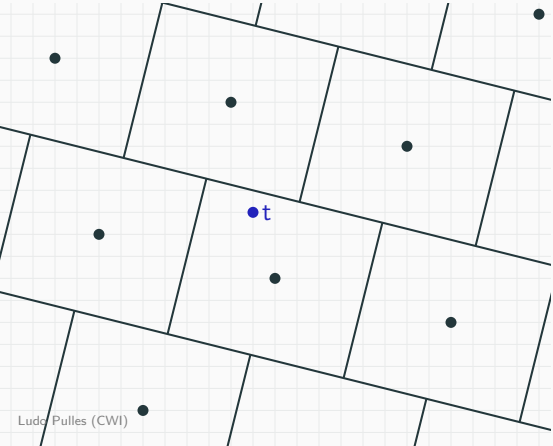


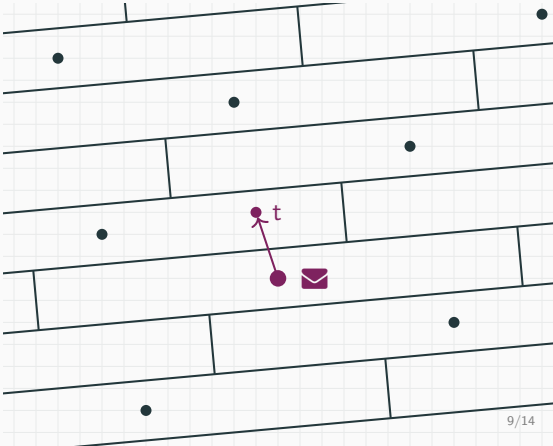


Encrypting with Lattices

Situation: Bob wants to send a message confidentially to Alice.

1. Bob: convert message to lattice point $\mathbf{m}$.
2. Bob: take random, small error $\mathbf{e}$, and send $\mathbf{t} = \mathbf{e} + \mathbf{m}$ to Alice.

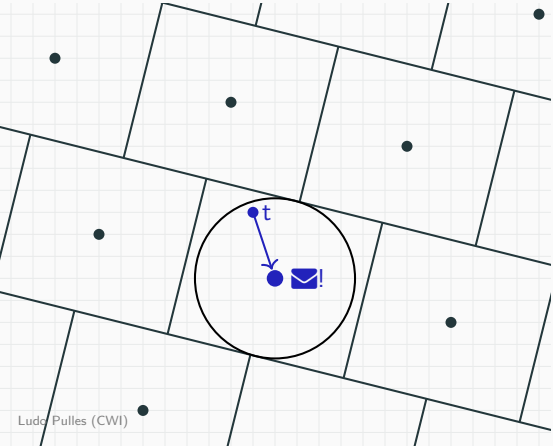




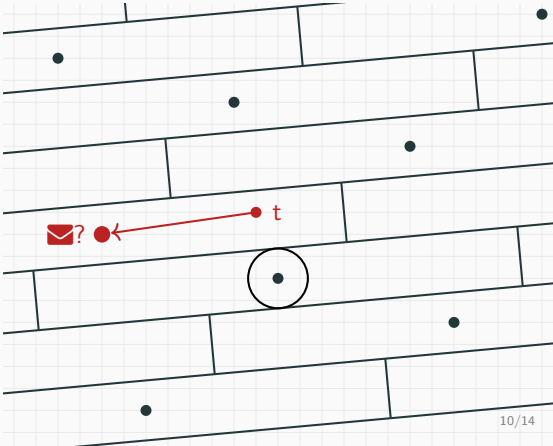
Lattice bases

Decryption:

Alice: find nearest lattice point.



Eve: cannot decrypt
(no good basis available).



Signatures with Lattices

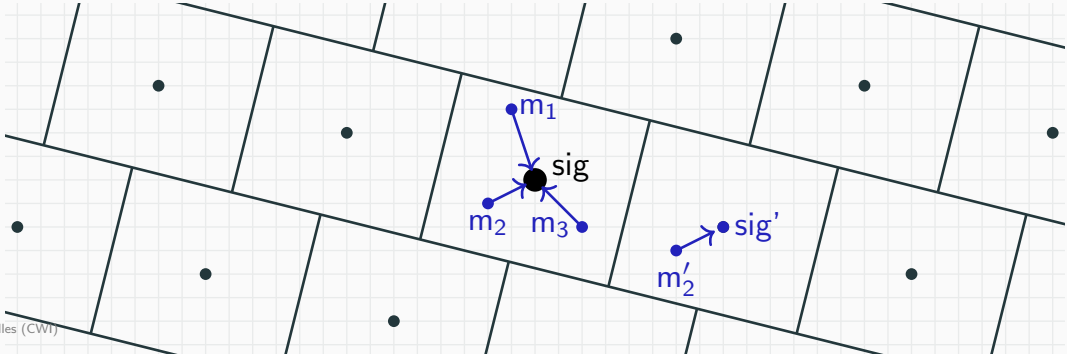
RSA strategy

RSA signatures → lattice signatures?

Signature: $\text{sig} := \text{RSA-Dec}_{\text{secret}}(\text{m})$.

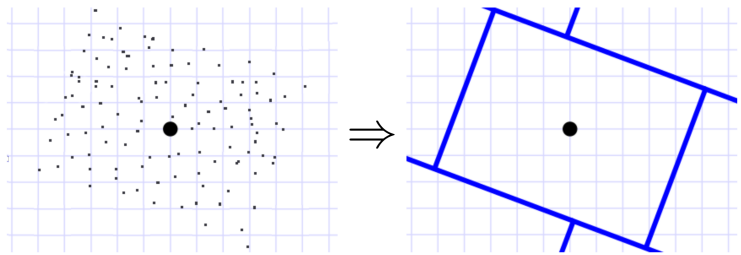
Verification: Check $\text{RSA-Enc}_{\text{public}}(\text{sig}) = \text{m}$.

Do signatures leak information on the secret basis?



Signature leakage!

⚠ Signatures leak information on the secret basis:



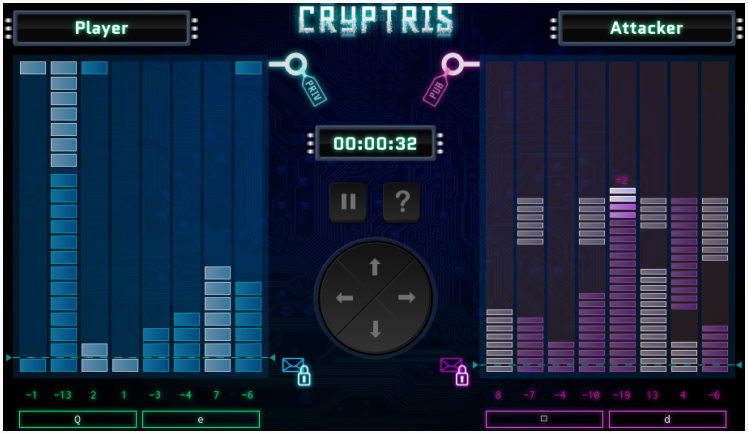
[Nguyen–Regev '06]: parallelogram is leaked, and secret basis.

💡 Solution in 2008 [Gentry–Peikert–Vaikutanathan]:
sample a **somewhat nearby** lattice point, not closest.

A game and a project

Lattice Reduction Game

Serious game for intuition:

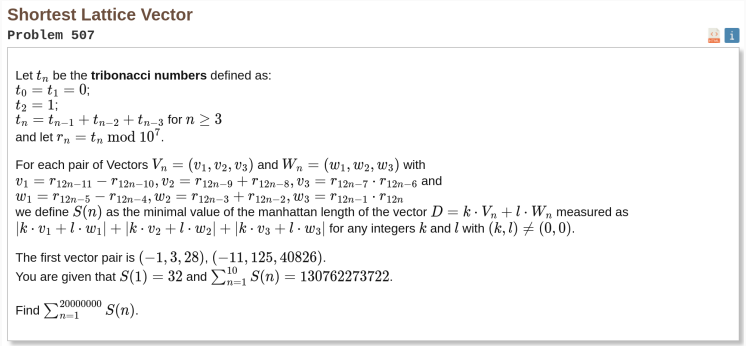


https://cryptris.nl

Assignment: Project Euler

Two basis vectors: $\mathbf{V}_n, \mathbf{W}_n$ (in dimension 3).

Goal: find shortest lattice vector (Manhattan distance).



Shortest Lattice Vector

Problem 507

Let t_n be the **tribonacci numbers** defined as:
$t_0 = t_1 = 0$;
$t_2 = 1$;
$t_n = t_{n-1} + t_{n-2} + t_{n-3}$ for $n \geq 3$
and let $r_n = t_n \bmod 10^7$.

For each pair of Vectors $V_n = (v_1, v_2, v_3)$ and $W_n = (w_1, w_2, w_3)$ with
$v_1 = r_{12n-11} - r_{12n-10}, v_2 = r_{12n-9} + r_{12n-8}, v_3 = r_{12n-7} \cdot r_{12n-6}$ and
$w_1 = r_{12n-5} - r_{12n-4}, w_2 = r_{12n-3} + r_{12n-2}, w_3 = r_{12n-1} \cdot r_{12n}$
we define $S(n)$ as the minimal value of the manhattan length of the vector $D = k \cdot V_n + l \cdot W_n$ measured as $|k \cdot v_1 + l \cdot w_1| + |k \cdot v_2 + l \cdot w_2| + |k \cdot v_3 + l \cdot w_3|$ for any integers k and l with $(k, l) \neq (0, 0)$.

The first vector pair is $(-1, 3, 28)$, $(-11, 125, 40826)$.
You are given that $S(1) = 32$ and $\sum_{n=1}^{10} S(n) = 130762273722$.

Find $\sum_{n=1}^{20000000} S(n)$.

https://projecteuler.net/problem=507