Technische Universiteit
Eindhoven
University of Technology

# Lattice cryptography and lattice cryptanalysis

Thijs Laarhoven

mail@thijs.com
http://www.thijs.com/

Lecture for Cryptography I
(January 8, 2015)

# Messages

Last lecture: exam coming up!

*"The first exam will take place **January 27, 2015, 13:30 - 16:30**. Please make sure to register on time! Deadline for registering for the first exam is **January 11, 2015**."*

*"The exam will be an **open-book exam**, meaning that you can use any book or notes that you have on paper. I will bring a laptop to display pdf files if you send me the files beforehand. The laptop will have access to the course page incl. blackboard pictures and scripts, but you may not use it to surf the internet. There will be a terminal to run GP-Pari and one to run Python; sage is not allowed. You may use a **programmable calculator** and I expect you to be able to use it for **modular exponentiation and inversion**."*

# Messages

- Tanja is not here today

# Messages

- Tanja is not here today
  - Thijs Laarhoven, fourth year of PhD
  - Working on lattice cryptography and lattice algorithms

# Messages

- Tanja is not here today
  - Thijs Laarhoven, fourth year of PhD
  - Working on lattice cryptography and lattice algorithms
  - Questions about the exam: `tanja@hyperelliptic.org`
  - Questions about old exams: `tanja@hyperelliptic.org`

# Messages

- Tanja is not here today
  - Thijs Laarhoven, fourth year of PhD
  - Working on **lattice cryptography** and **lattice algorithms**
  - Questions about the exam: `tanja@hyperelliptic.org`
  - Questions about old exams: `tanja@hyperelliptic.org`

# Messages

- Tanja is not here today
  - Thijs Laarhoven, fourth year of PhD
  - Working on **lattice cryptography** and **lattice algorithms**
  - Questions about the exam: `tanja@hyperelliptic.org`
  - Questions about old exams: `tanja@hyperelliptic.org`
- Part 1: Lattice cryptography and lattice basis reduction
- Part 2: Algorithms for solving hard lattice problems

Technische Universiteit Eindhoven University of Technology

# Part 1: Lattice cryptography and lattice basis reduction

Thijs Laarhoven

mail@thijs.com
http://www.thijs.com/

Lecture for Cryptography I

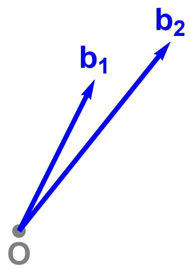
(January 8, 2015)

# Lattices

## What is a lattice?

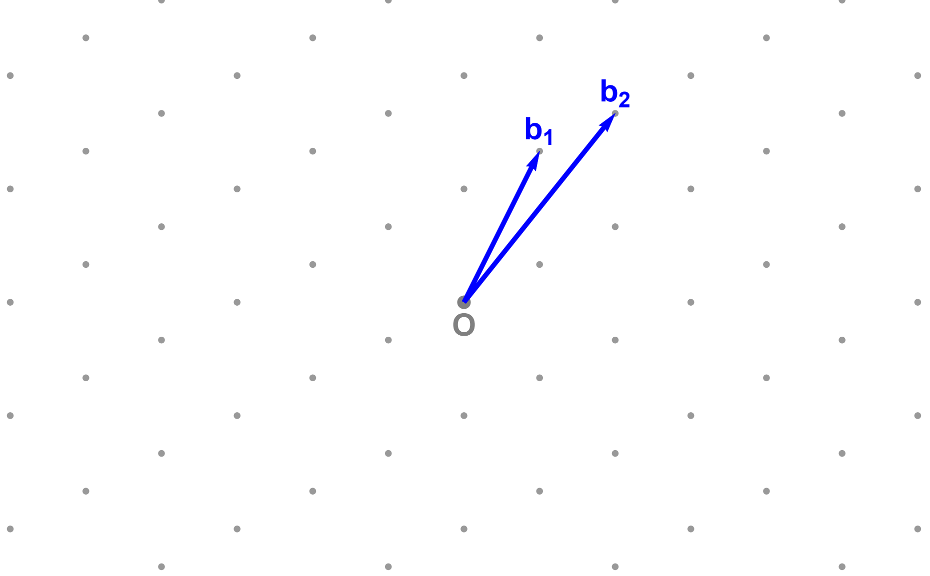
# Lattices

## What is a lattice?



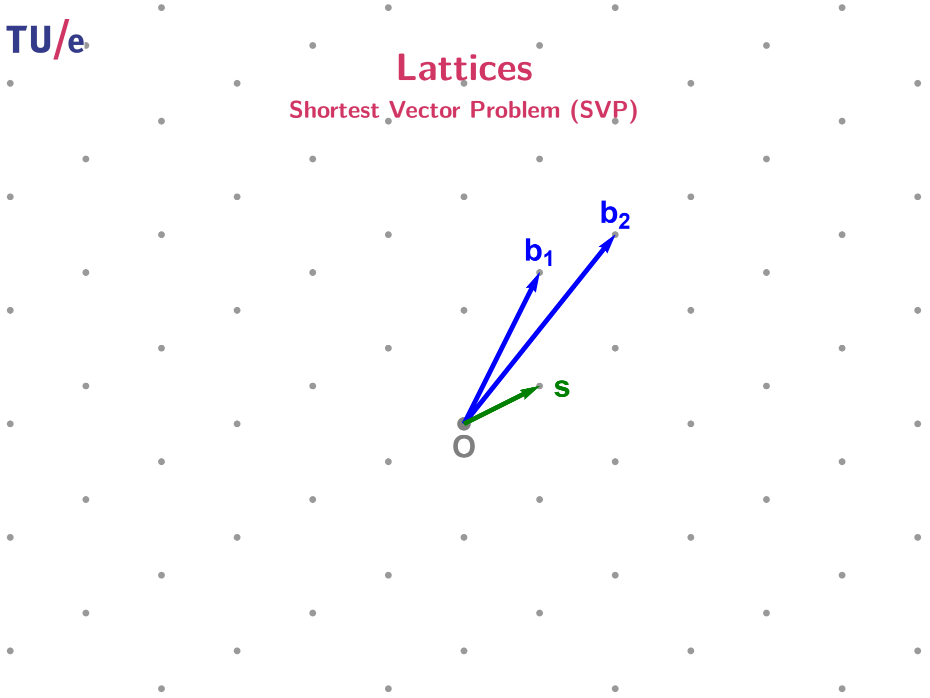
# Lattices

## What is a lattice?



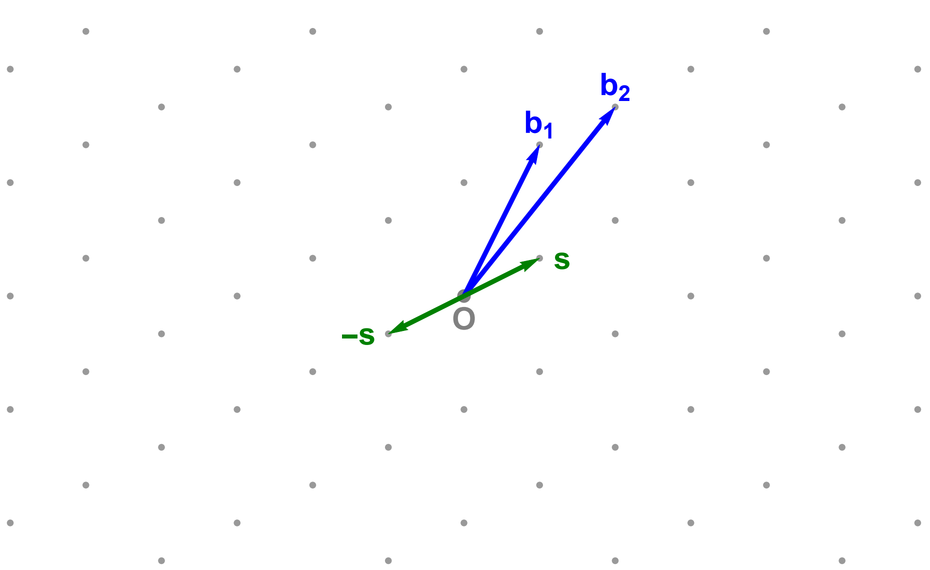
# Lattices

## Shortest Vector Problem (SVP)



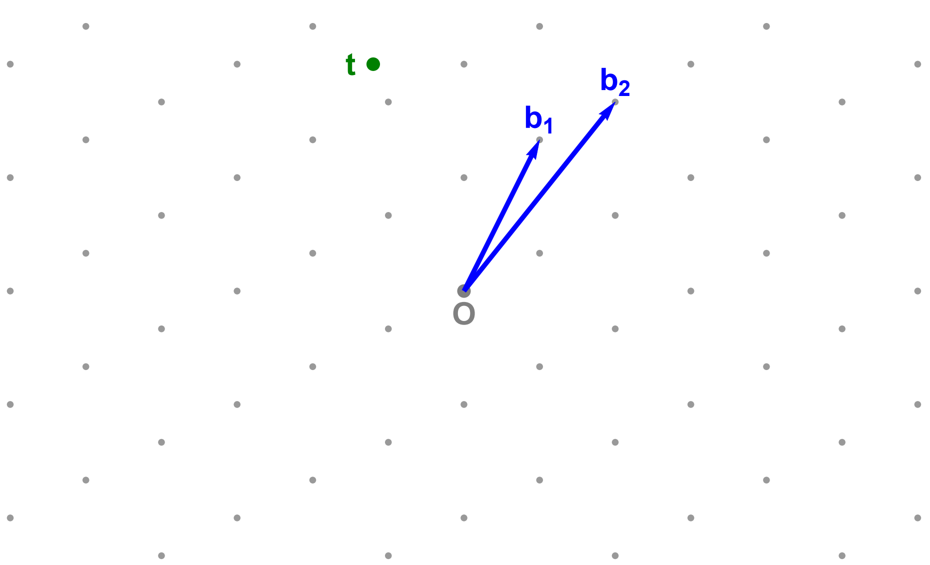
# Lattices

## Shortest Vector Problem (SVP)



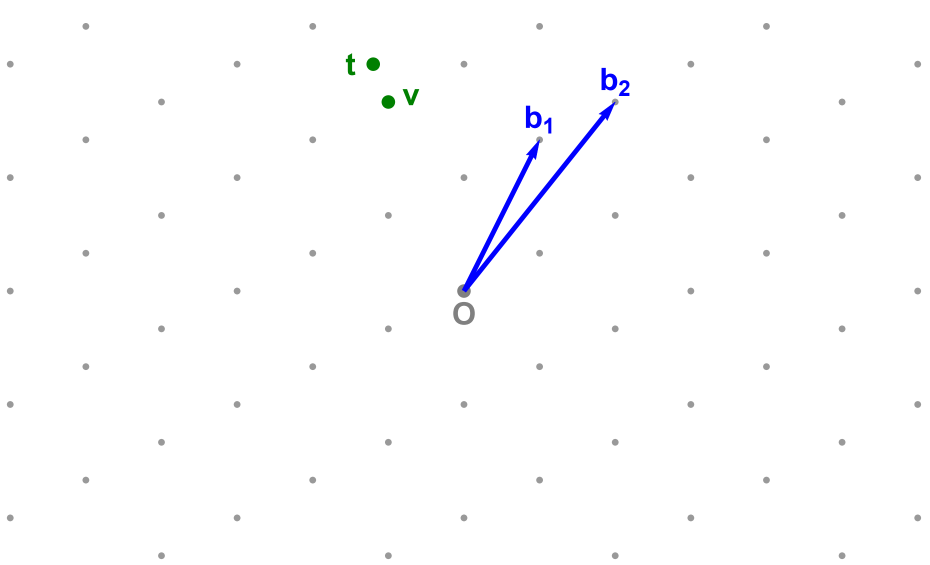
# Lattices

## Closest Vector Problem (CVP)



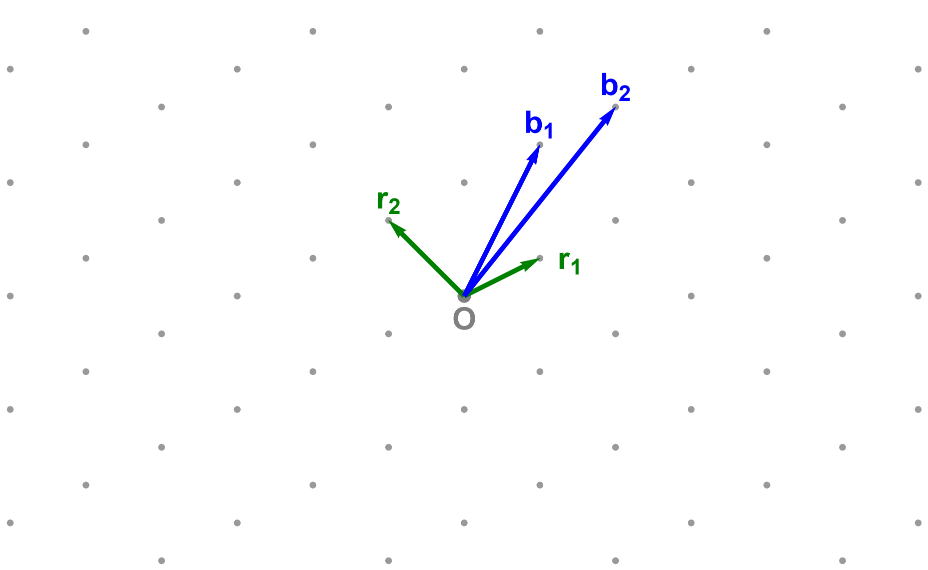
# Lattices

## Closest Vector Problem (CVP)



# Lattices

## Lattice basis reduction



# GGH cryptosystem

## Overview

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$

# GGH cryptosystem

## Private key

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

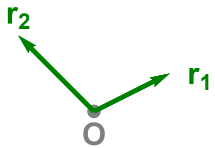
$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}'B^{-1}$$

## GGH cryptosystem

### Private key

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$




Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

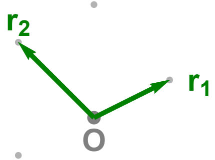
$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$

# GGH cryptosystem

## Public key

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$




Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}'B^{-1}$$

# GGH cryptosystem

## Public key

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

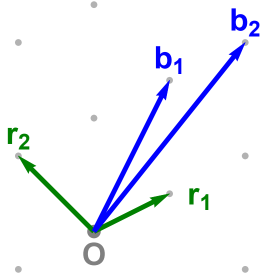
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$



# GGH cryptosystem

## Encryption

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

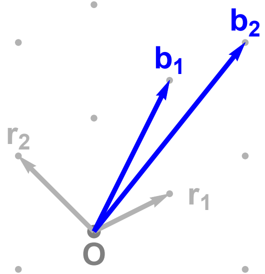
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}'B^{-1}$$



# GGH cryptosystem

## Encryption

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

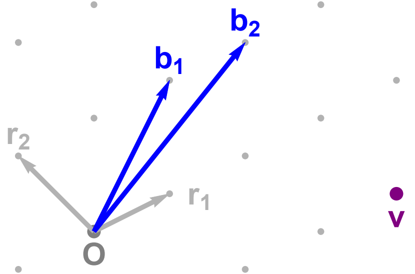
$\boldsymbol{v} = \boldsymbol{m}B$

$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$

Decrypt $\boldsymbol{c}$:

$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$

$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$



# GGH cryptosystem

## Encryption

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

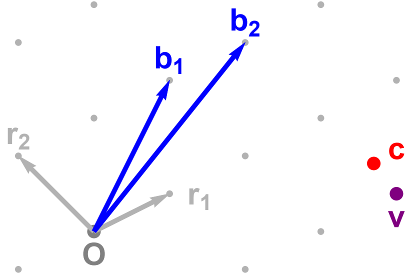
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$



# GGH cryptosystem

## Decryption with good basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

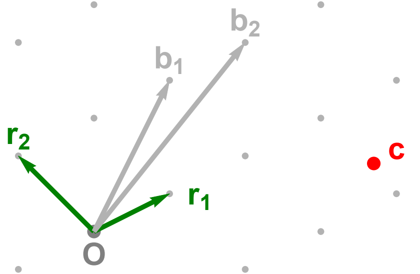
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$



# GGH cryptosystem

## Decryption with good basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

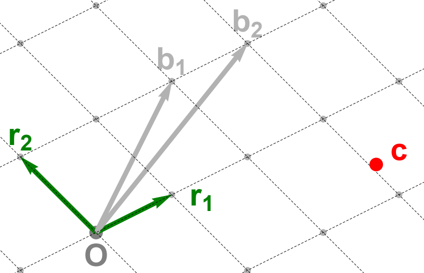
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$



# GGH cryptosystem

## Decryption with good basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

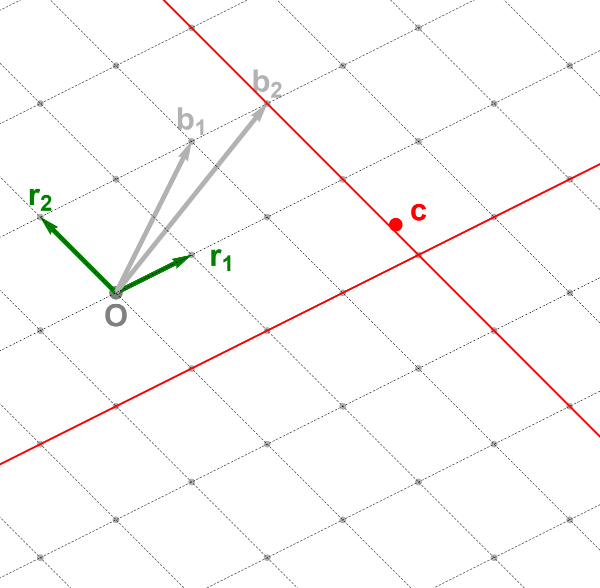
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$



# GGH cryptosystem

## Decryption with good basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

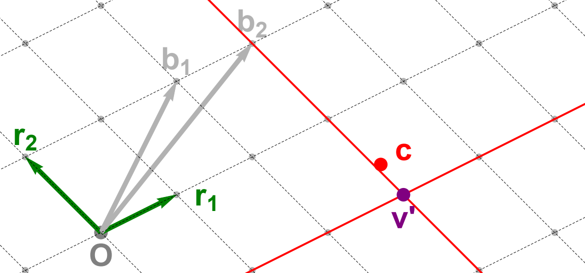
$\boldsymbol{v} = \boldsymbol{m}B$

$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$

Decrypt $\boldsymbol{c}$:

$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$

$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$



# GGH cryptosystem

## Decryption with bad basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

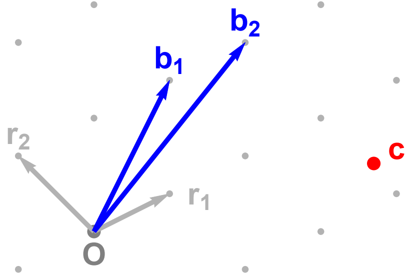
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}'B^{-1}$$



# GGH cryptosystem

## Decryption with bad basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

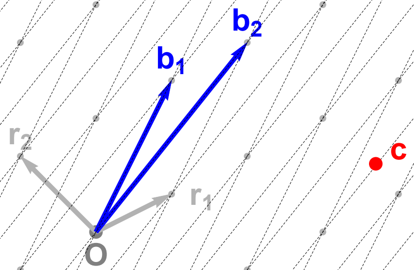
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$



# GGH cryptosystem

## Decryption with bad basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

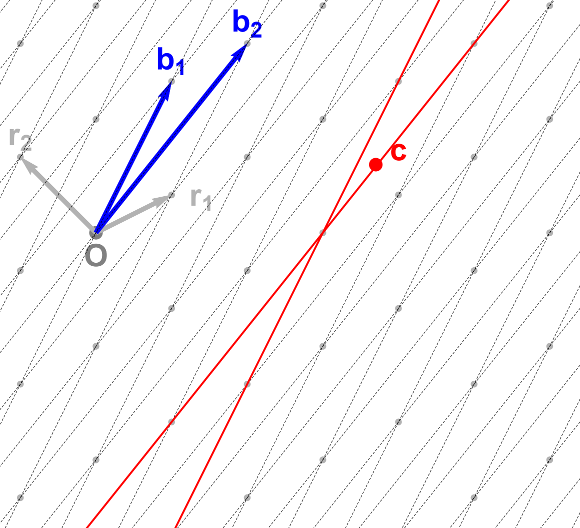
Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

$$\boldsymbol{v} = \boldsymbol{m}B$$
$$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$$

Decrypt $\boldsymbol{c}$:

$$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$$
$$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$$



# GGH cryptosystem

## Decryption with bad basis

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

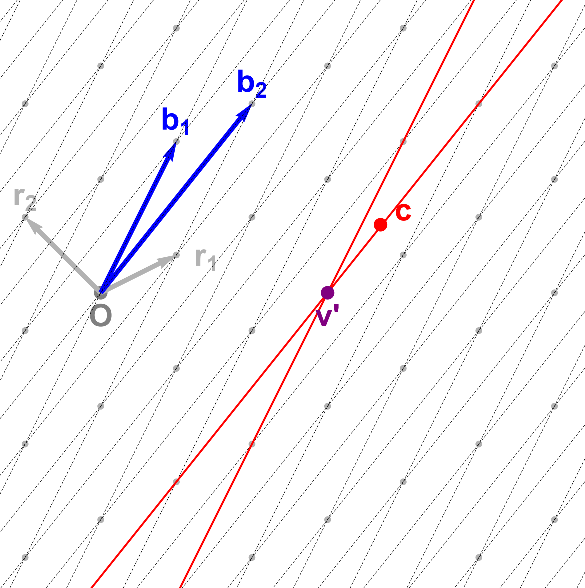
$\boldsymbol{v} = \boldsymbol{m}B$

$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$

Decrypt $\boldsymbol{c}$:

$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$

$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$



# GGH cryptosystem

## Overview

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Encrypt $\boldsymbol{m}$:

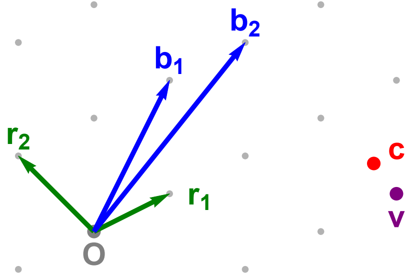
$\boldsymbol{v} = \boldsymbol{m}B$

$\boldsymbol{c} = \boldsymbol{v} + \boldsymbol{e}$

Decrypt $\boldsymbol{c}$:

$\boldsymbol{v}' = \lfloor \boldsymbol{c}R^{-1} \rceil R$

$\boldsymbol{m}' = \boldsymbol{v}' B^{-1}$



# GGH signatures

## Overview

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Sign $\boldsymbol{m}$:

$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \lfloor \boldsymbol{c} R^{-1} \rceil R$

Verify $(\boldsymbol{m}, \boldsymbol{s})$:

$\boldsymbol{s}$ lies on the lattice

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ is small

# GGH signatures

## Private and public keys

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Sign $\boldsymbol{m}$:

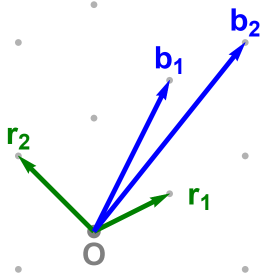
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \lfloor \boldsymbol{c} R^{-1} \rceil R$

Verify $(\boldsymbol{m}, \boldsymbol{s})$:

$\boldsymbol{s}$ lies on the lattice

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ is small



# GGH signatures

## Signing messages

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Sign $\boldsymbol{m}$:

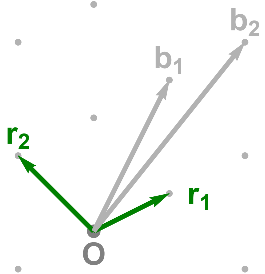
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \lfloor \boldsymbol{c} R^{-1} \rceil R$

Verify $(\boldsymbol{m}, \boldsymbol{s})$:

$\boldsymbol{s}$ lies on the lattice

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ is small



# GGH signatures

## Signing messages

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Sign $\boldsymbol{m}$:

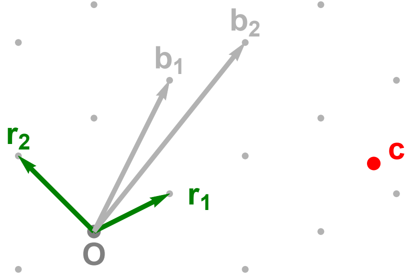
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \lfloor \boldsymbol{c} R^{-1} \rceil R$

Verify $(\boldsymbol{m}, \boldsymbol{s})$:

$\boldsymbol{s}$ lies on the lattice

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ is small



# GGH signatures

## Signing messages

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Sign $\boldsymbol{m}$:

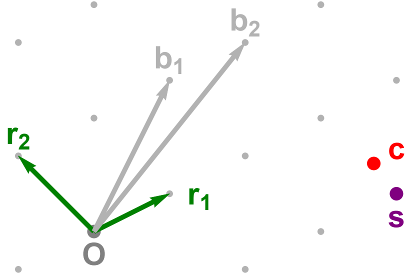
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \lfloor \boldsymbol{c} R^{-1} \rceil R$

Verify $(\boldsymbol{m}, \boldsymbol{s})$:

$\boldsymbol{s}$ lies on the lattice

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ is small



# GGH signatures

## Verifying signatures

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Sign $\boldsymbol{m}$:

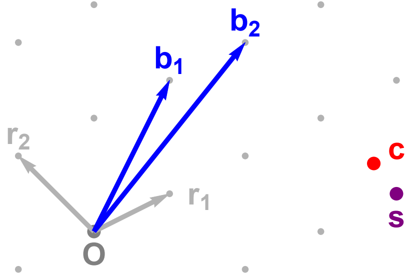
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \lfloor \boldsymbol{c} R^{-1} \rceil R$

Verify $(\boldsymbol{m}, \boldsymbol{s})$:

$\boldsymbol{s}$ lies on the lattice

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ is small



# GGH signatures

## Overview

Private key: $R = \begin{pmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \end{pmatrix}$

Public key: $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$

Sign $\boldsymbol{m}$:

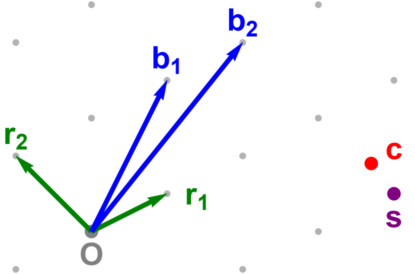
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \lfloor \boldsymbol{c} R^{-1} \rceil R$

Verify $(\boldsymbol{m}, \boldsymbol{s})$:

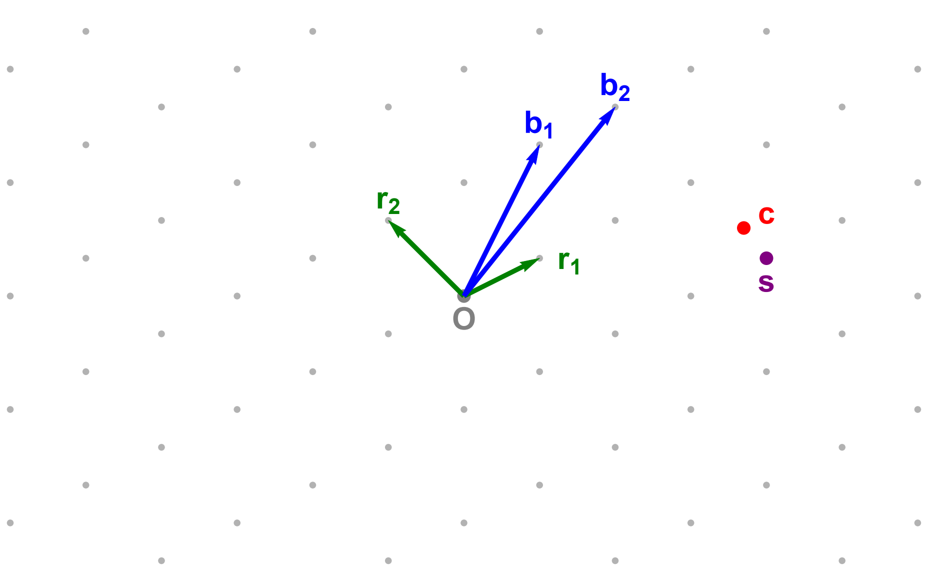
$\boldsymbol{s}$ lies on the lattice

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ is small



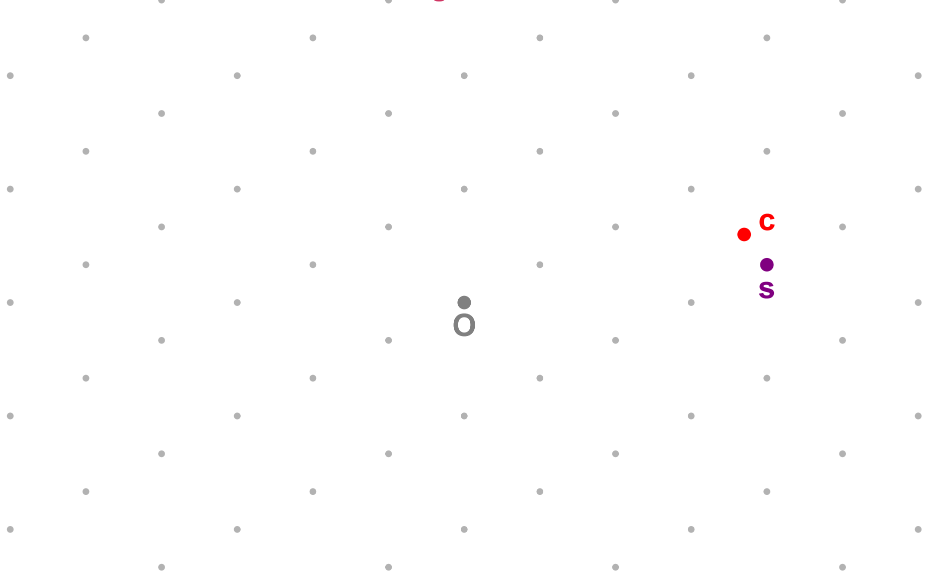
# GGH signatures

## Breaking the scheme



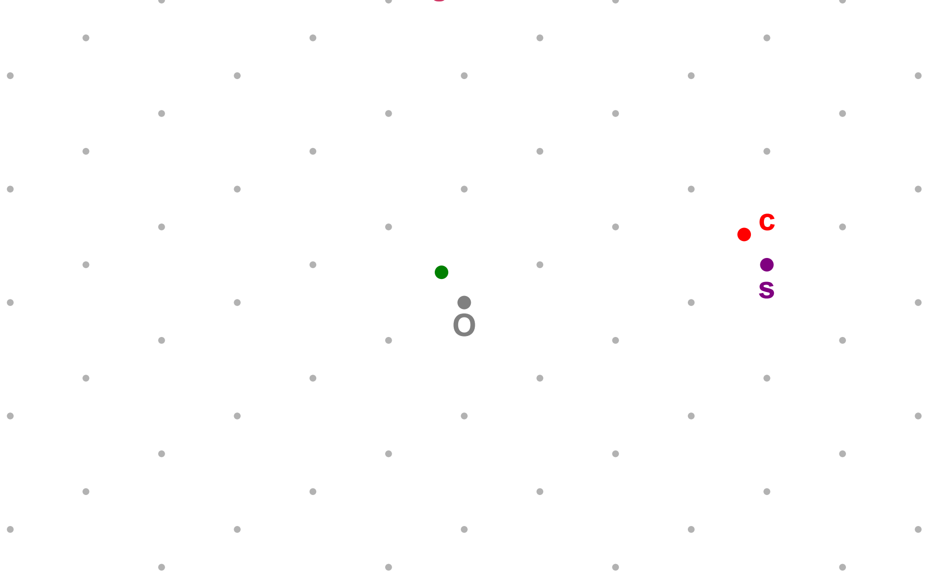
# GGH signatures

## Breaking the scheme



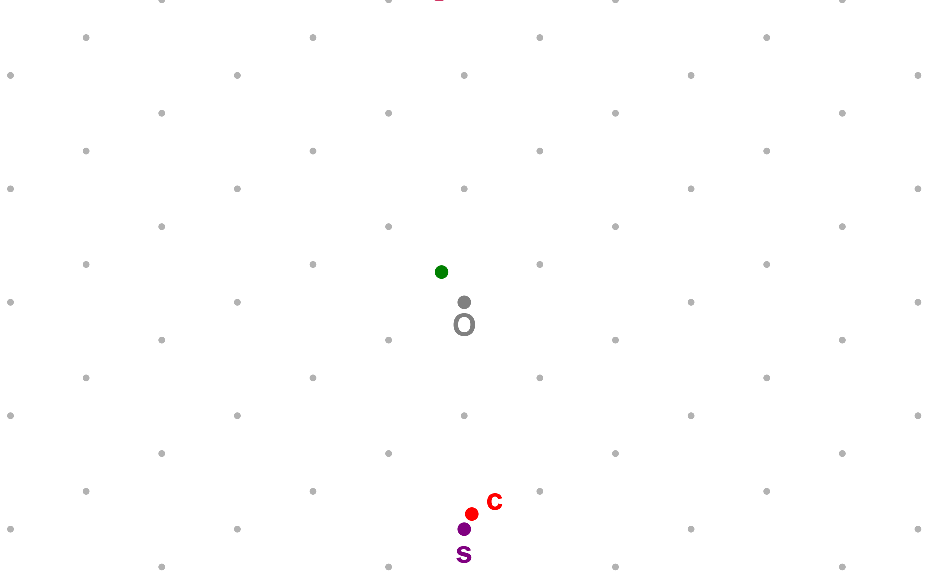
# GGH signatures

## Breaking the scheme



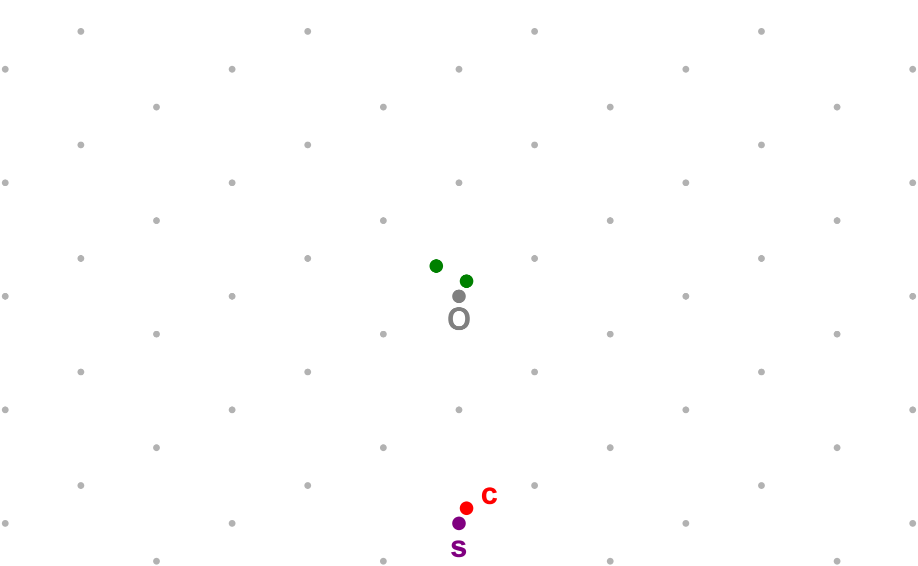
# GGH signatures

## Breaking the scheme



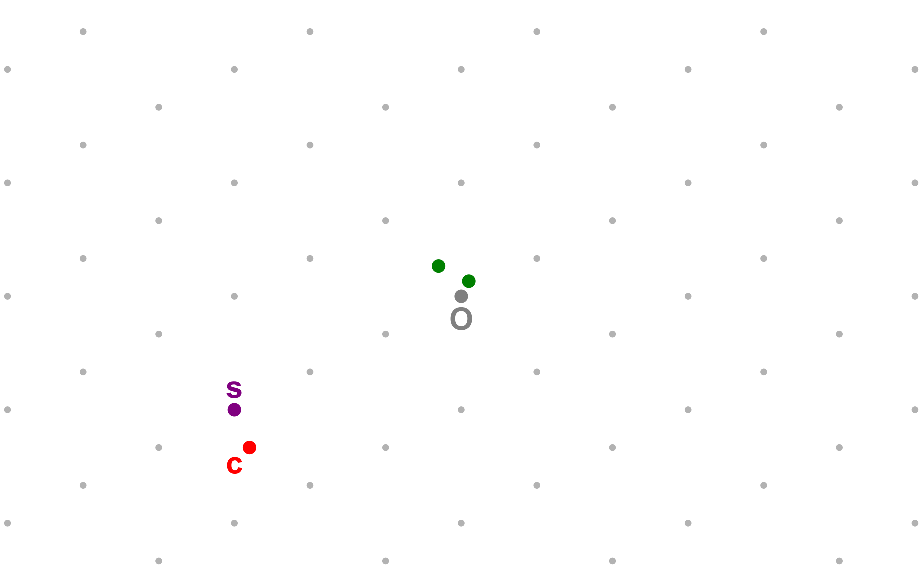
# GGH signatures

## Breaking the scheme



# GGH signatures

## Breaking the scheme

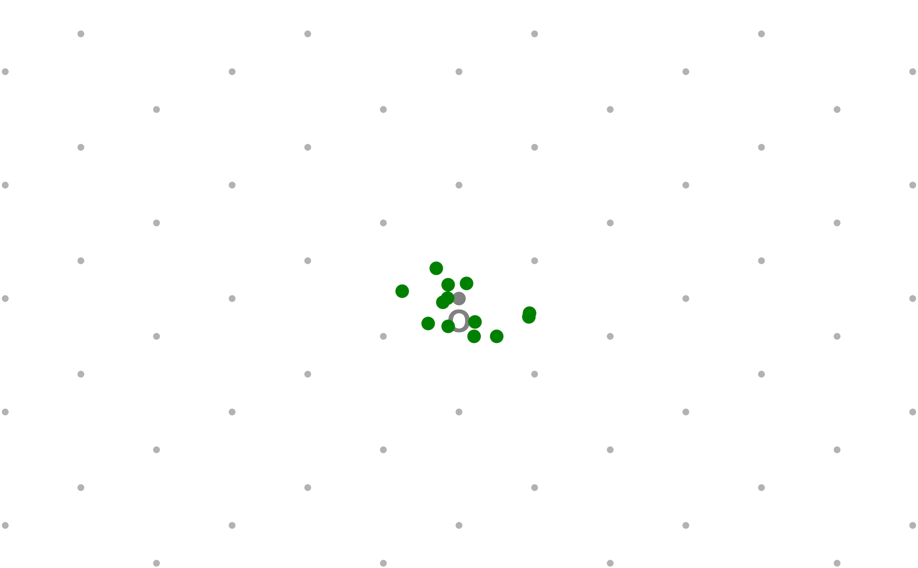


# GGH signatures

## Breaking the scheme

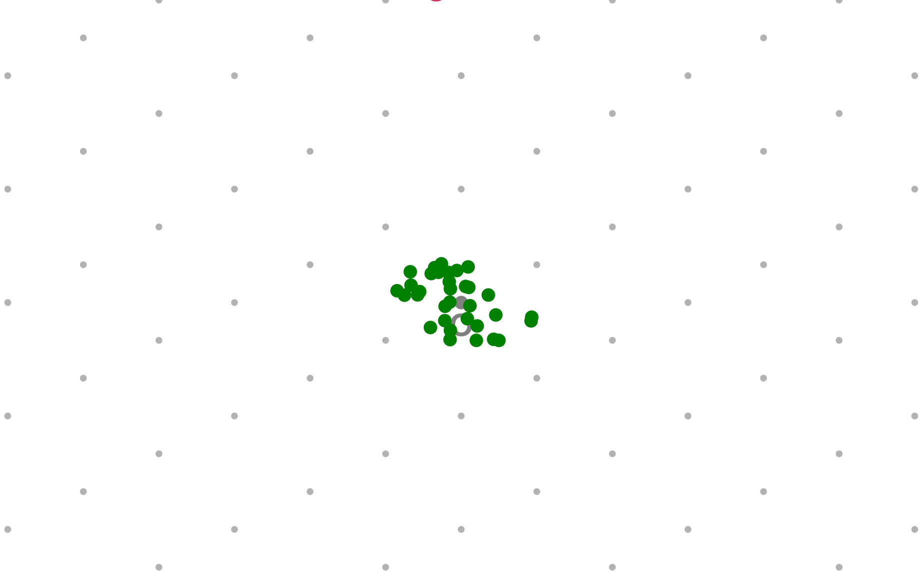
# GGH signatures

## Breaking the scheme



# GGH signatures

## Breaking the scheme

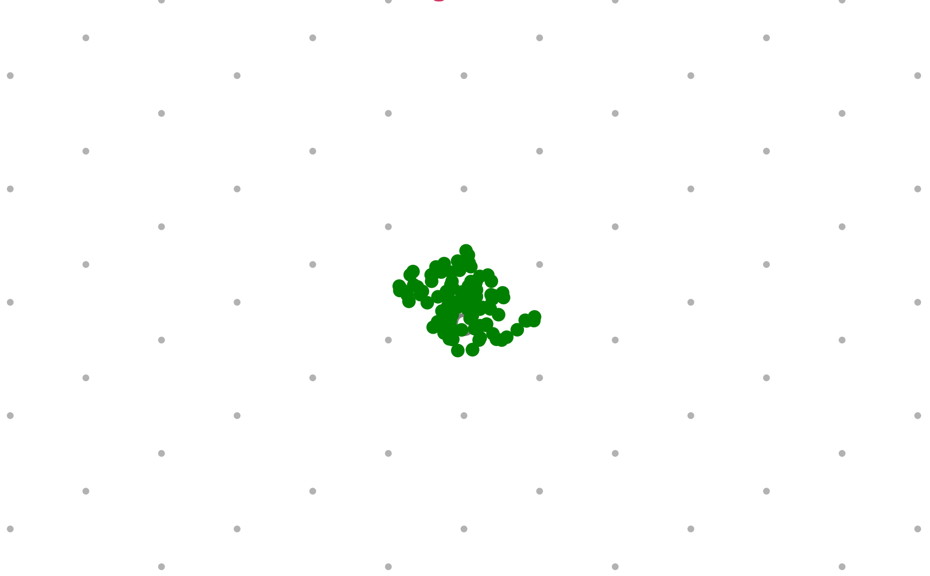


# GGH signatures

## Breaking the scheme

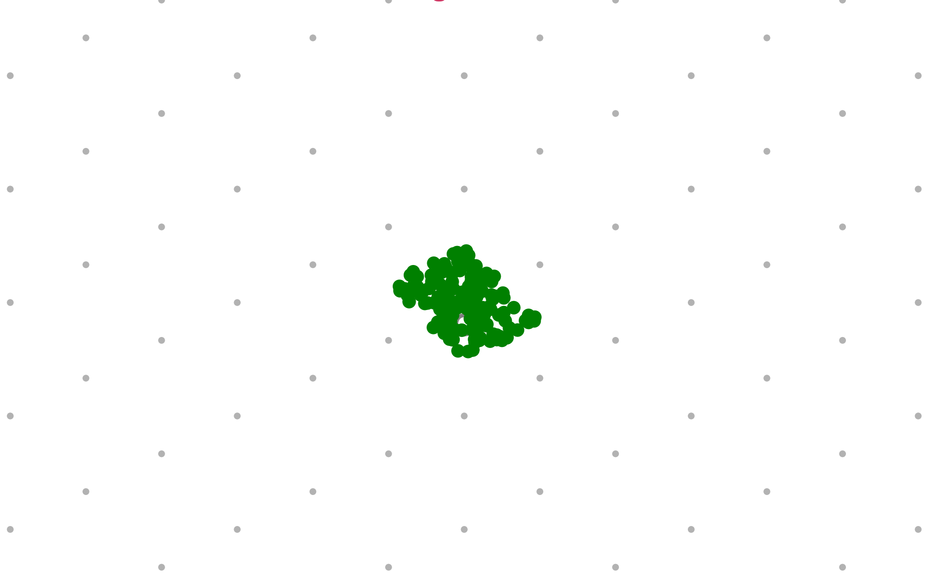
# GGH signatures

## Breaking the scheme



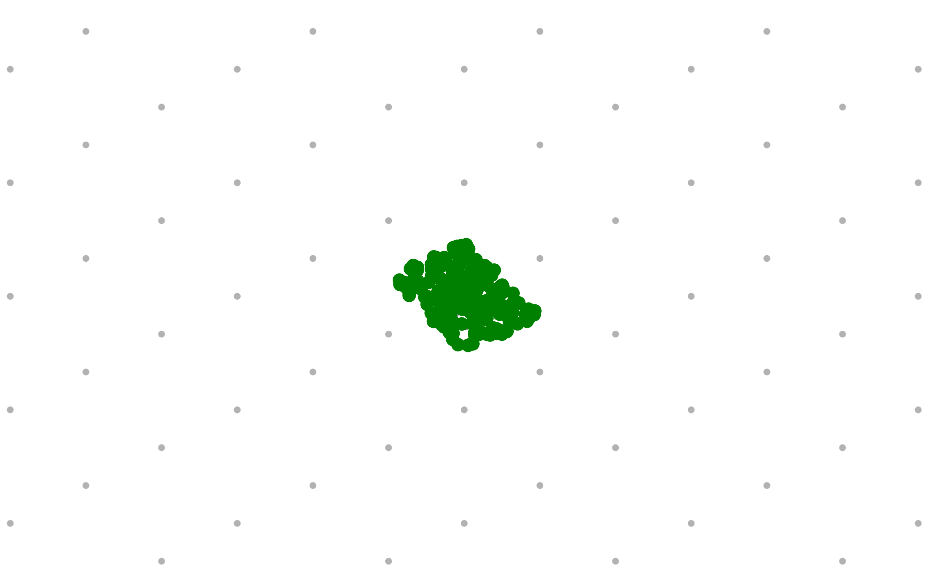
# GGH signatures

## Breaking the scheme



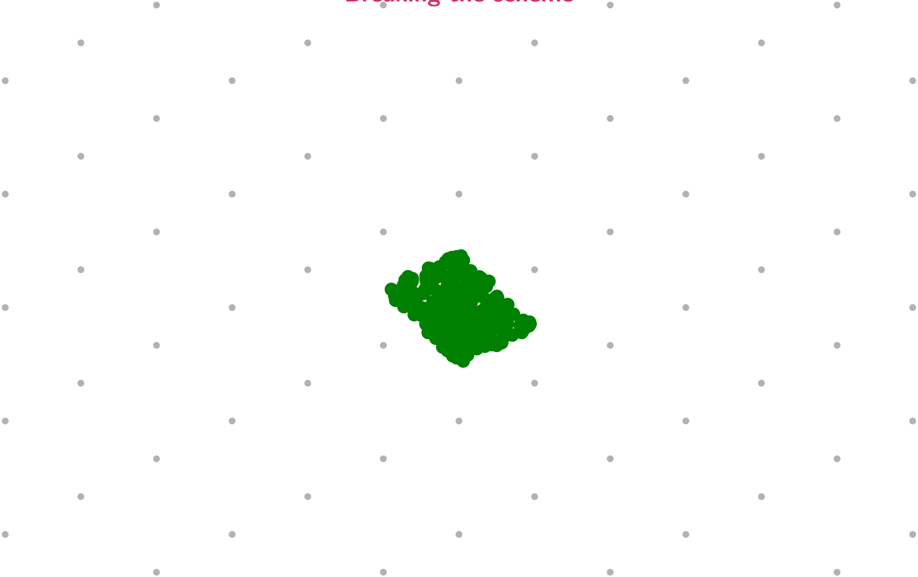
# GGH signatures

## Breaking the scheme



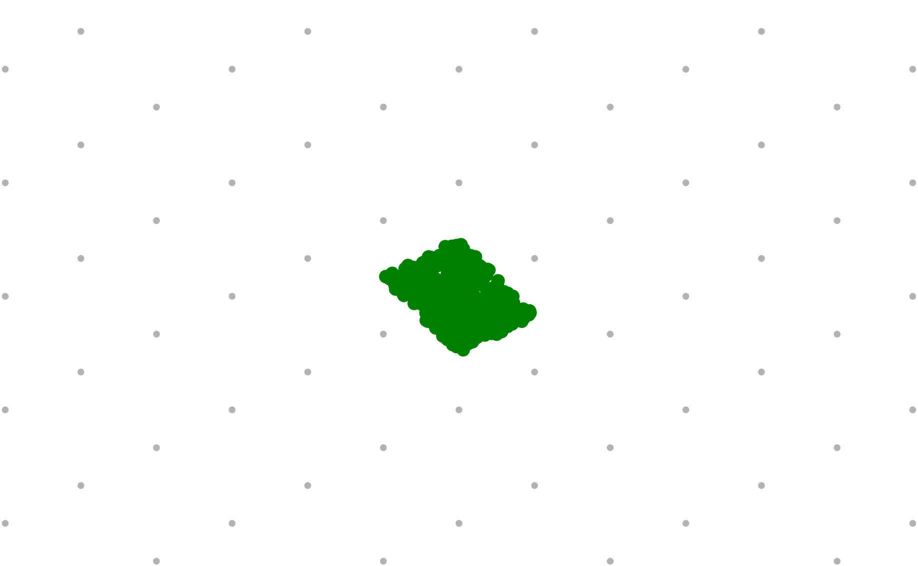
# GGH signatures

## Breaking the scheme



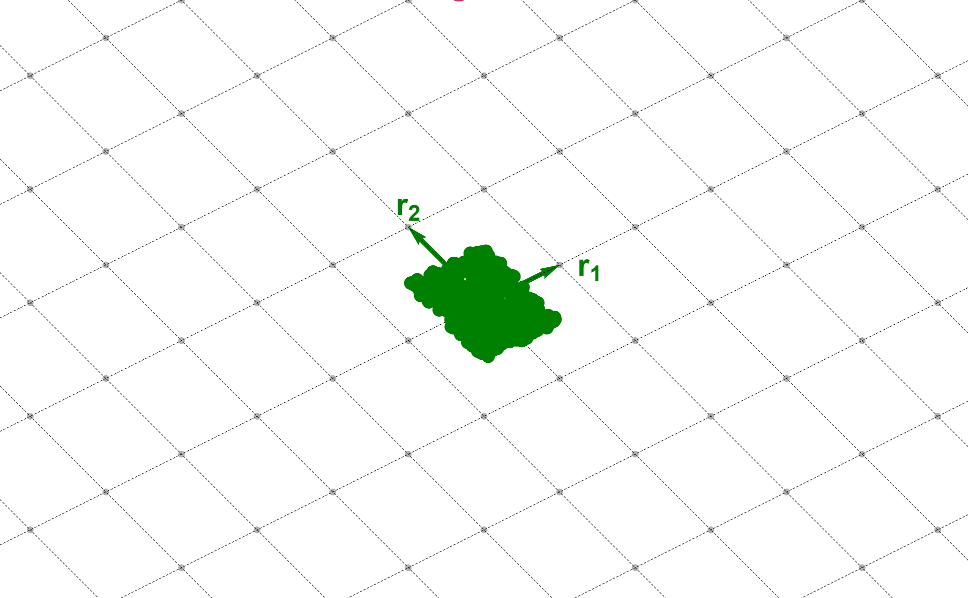
# GGH signatures

## Breaking the scheme

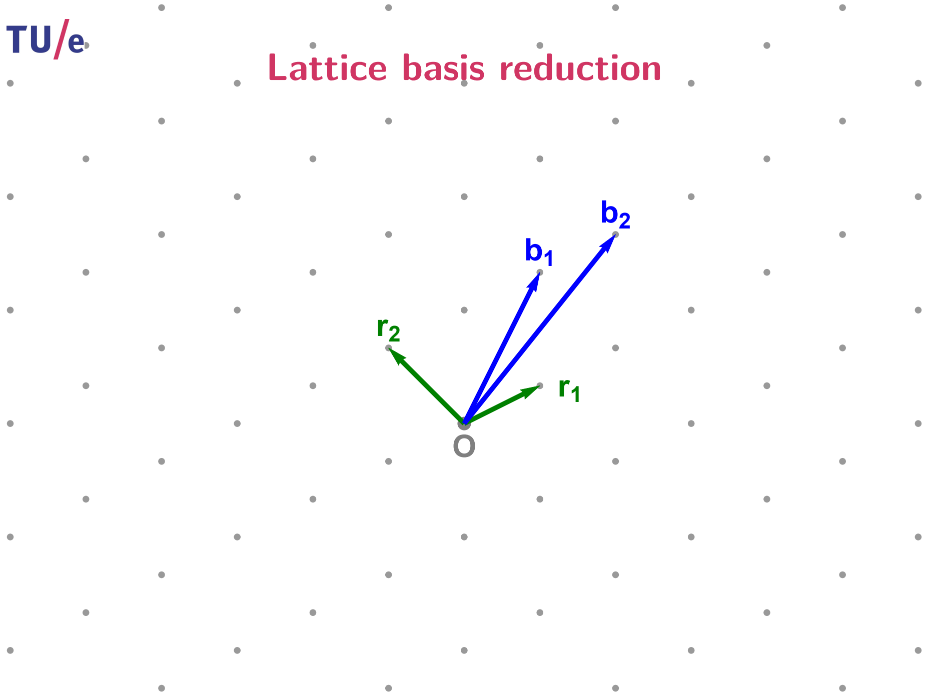


# GGH signatures

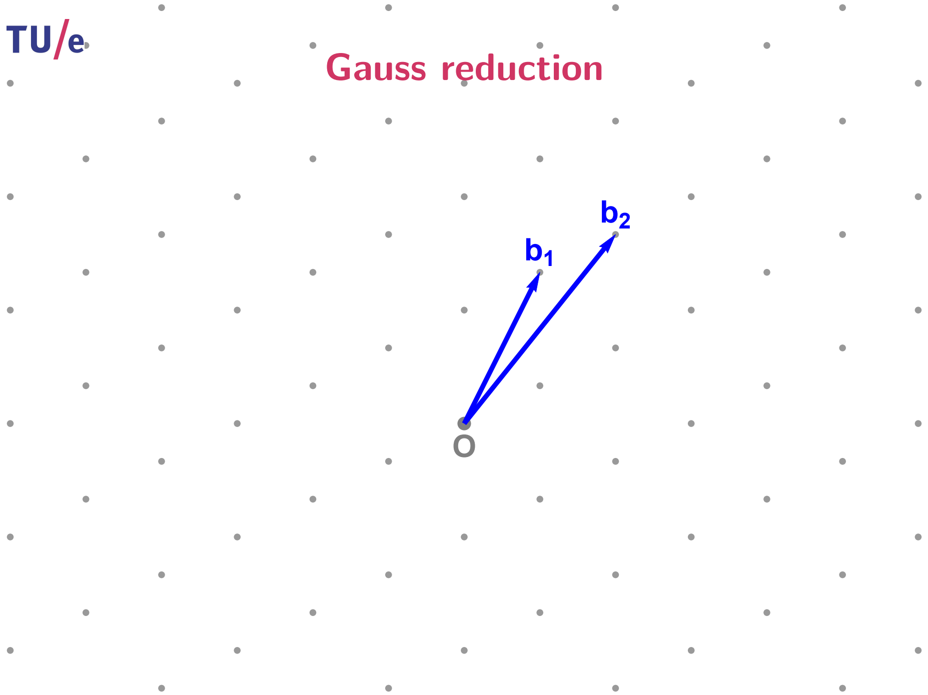
## Breaking the scheme



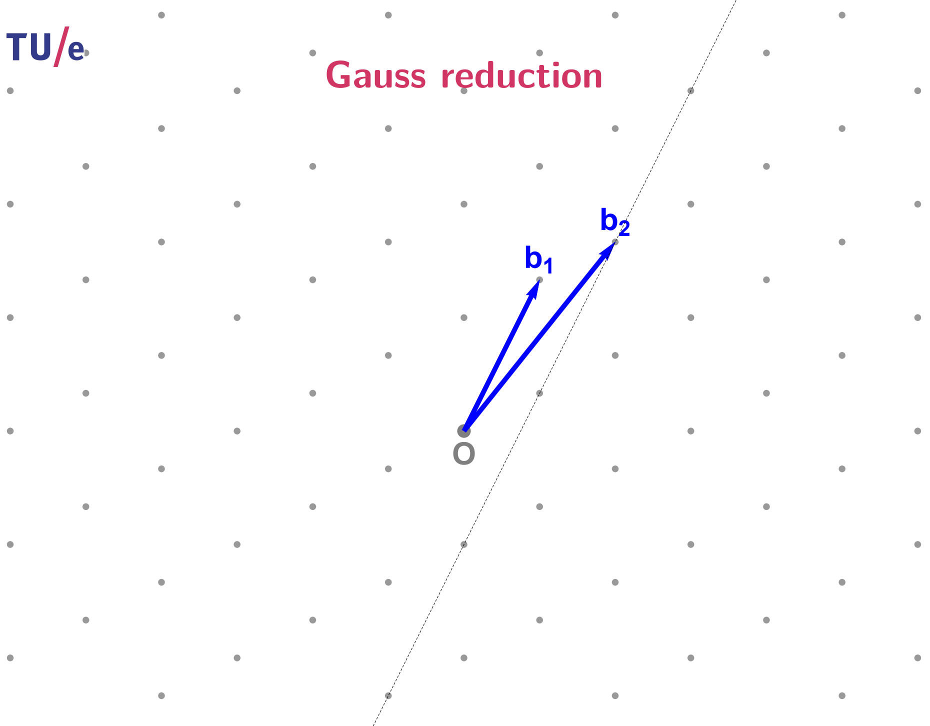
# Lattice basis reduction



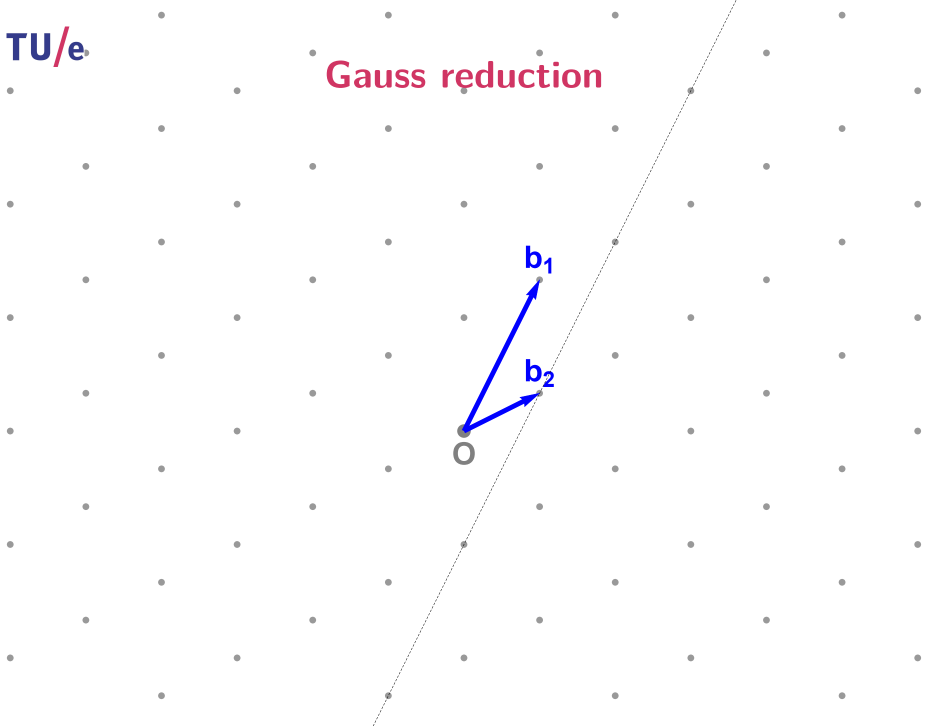
# Gauss reduction



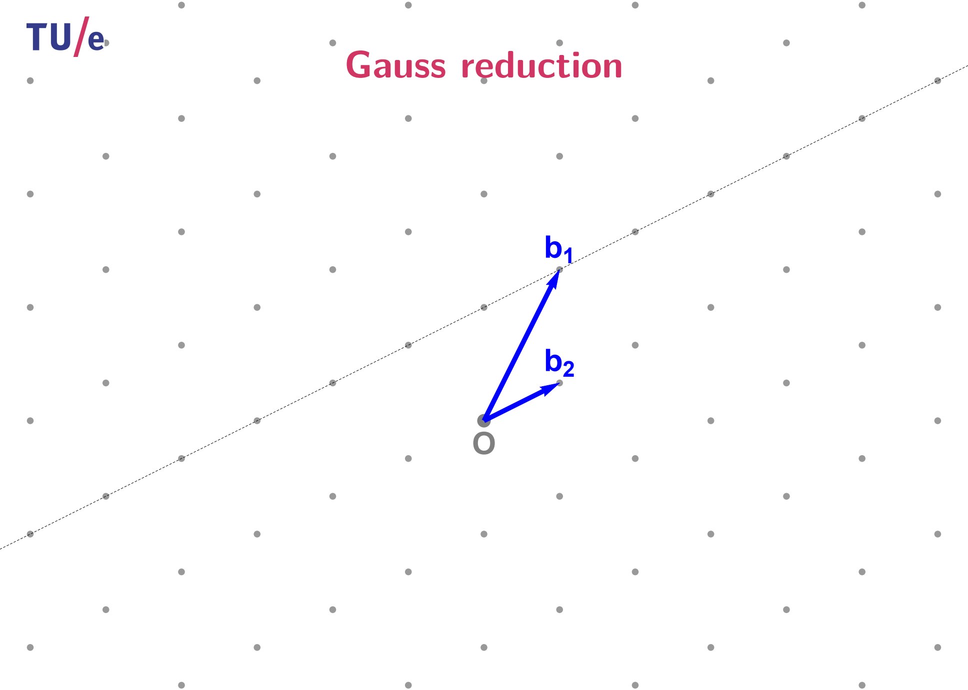
# Gauss reduction



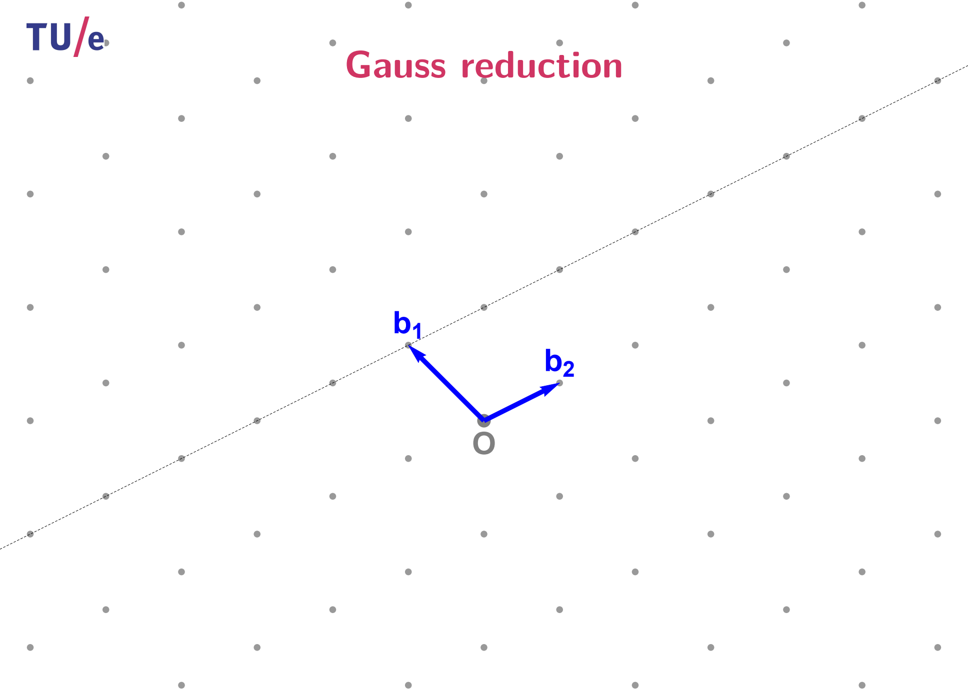
# Gauss reduction



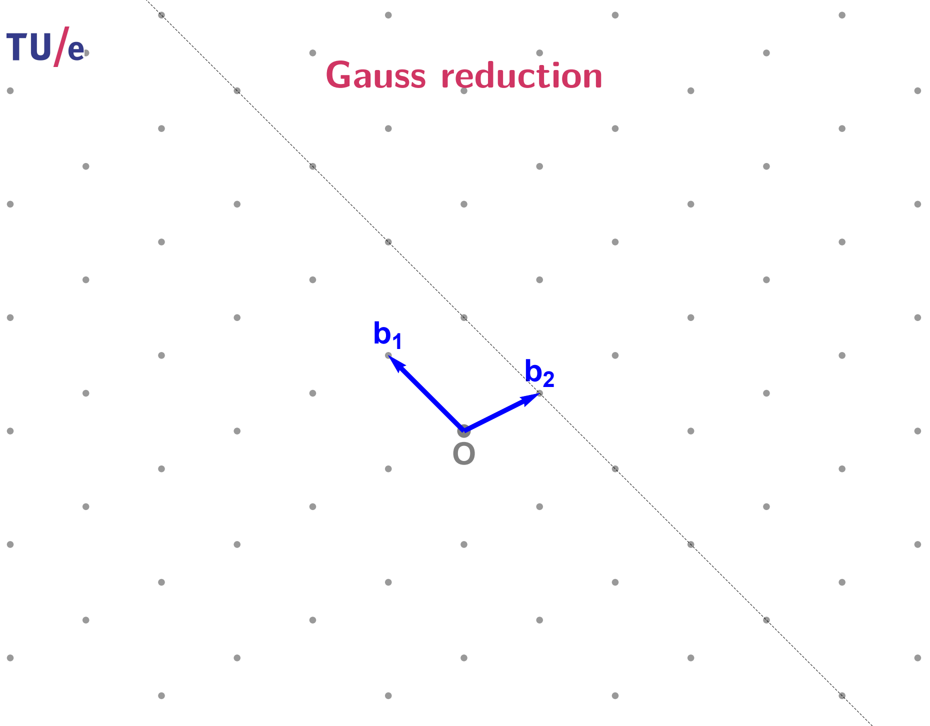
# Gauss reduction



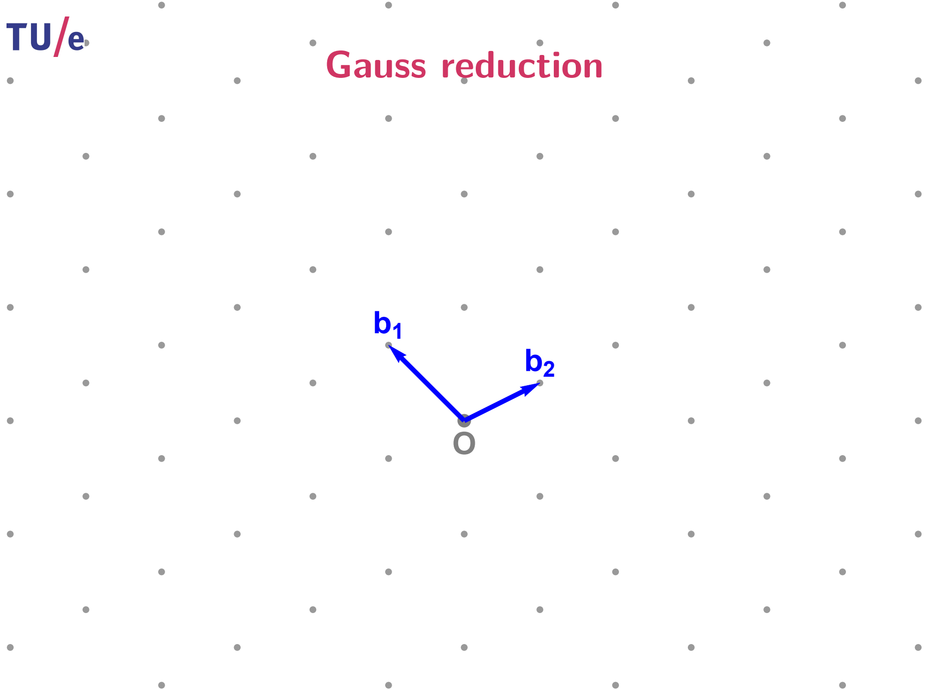
# Gauss reduction



# Gauss reduction



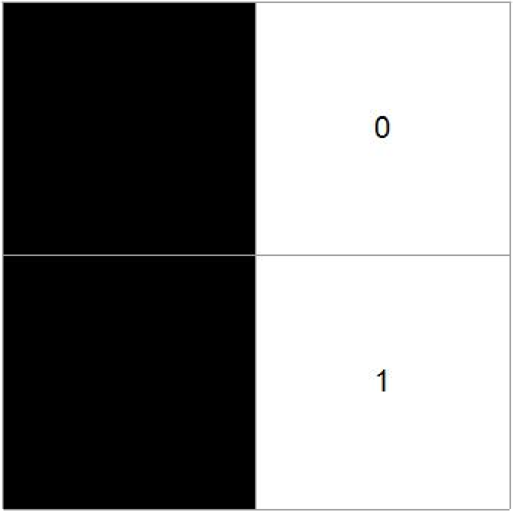
# Gauss reduction



# Gauss reduction

| | |
|---|---|
| 3141592653 | 0 |
| 5897932384 | 1 |

# Gauss reduction



TU/e

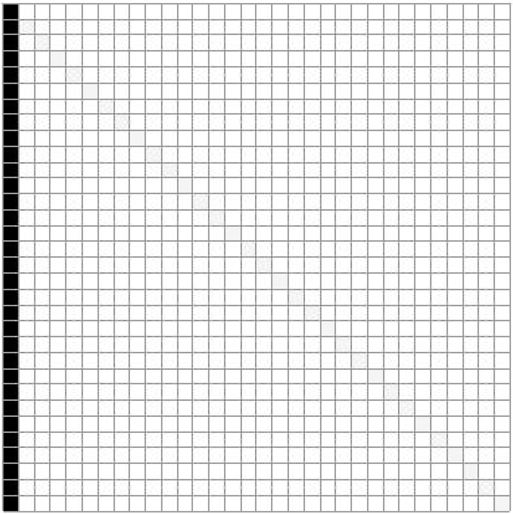
# LLL algorithm

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

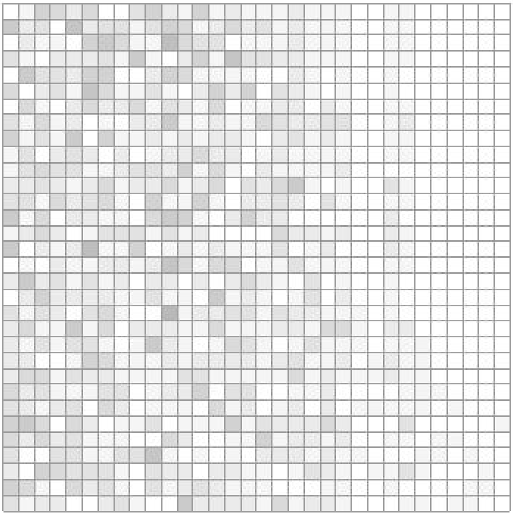
# LLL algorithm

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

# LLL algorithm



# LLL algorithm



# BKZ algorithm