Technische Universiteit Eindhoven University of Technology

Cryptography, quantum computing, and evolutionary computation

Thijs Laarhoven

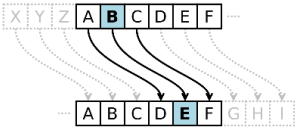
mail@thijs.com
http://www.thijs.com/

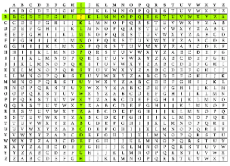
CFMAI 2019, Bangkok, Thailand
(December 13, 2019)

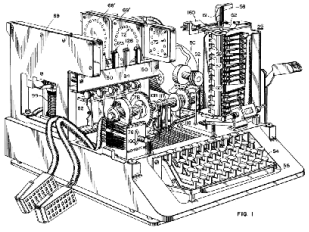
TU/e

Cryptography

History







https://

INTERNET of THINGS

amazon web services

bitcoin

libra

Cryptography

Classical cryptography

Some operations are easy to perform in one direction...

$$7 \times 17 =$$

$$714881 \times 448843 =$$

Cryptography

Classical cryptography

Some operations are easy to perform in one direction...

$$7 \times 17 = 119,$$

$$714881 \times 448843 =$$

Cryptography

Classical cryptography

Some operations are easy to perform in one direction...

$$7 \times 17 = 119,$$

$$714881 \times 448843 = 320869332683,$$

TU/e

Cryptography

Classical cryptography

Some operations are easy to perform in one direction...

$$7 \times 17 = 119,$$

$$714881 \times 448843 = 320869332683,$$

...but are difficult to “invert”, or compute in the reverse direction

$$143 =$$

$$188629334237 =$$

Cryptography

Classical cryptography

Some operations are easy to perform in one direction...

$$7 \times 17 = 119,$$
$$714881 \times 448843 = 320869332683,$$

...but are difficult to “invert”, or compute in the reverse direction

$$143 = 11 \times 13,$$
$$188629334237 =$$

Cryptography

Classical cryptography

Some operations are easy to perform in one direction...

$$7 \times 17 = 119,$$
$$714881 \times 448843 = 320869332683,$$

...but are difficult to “invert”, or compute in the reverse direction

$$143 = 11 \times 13,$$
$$188629334237 = 214729 \times 878453.$$

TU/e

Cryptography

Classical cryptography

Some operations are easy to perform in one direction...

$$7 \times 17 = 119,$$
$$714881 \times 448843 = 320869332683,$$

...but are difficult to “invert”, or compute in the reverse direction

$$143 = 11 \times 13,$$
$$188629334237 = 214729 \times 878453.$$

The security of modern cryptography depends on the hardness of such problems.

Cryptography

Protocols

Example: Suppose Bob wishes to send a private message to Alice across the world.

TU/e

Cryptography

Protocols

Example: Suppose Bob wishes to send a private message to Alice across the world.

Insecure solution:

- Bob sends Alice the message in the clear over the internet.
- Problem: Others can see the contents of the message.

TU/e

Cryptography

Protocols

Example: Suppose Bob wishes to send a private message to Alice across the world.

Insecure solution:

- Bob sends Alice the message in the clear over the internet.
- Problem: Others can see the contents of the message.

More secure solution:

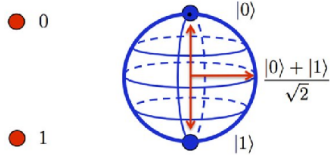
- Alice sends Bob a product (323), for which only she knows the factors $(17, 19)$.
- Bob computes some function of his message modulo 323 and sends it to Alice.
  - This function is easy to compute but hard to invert without the prime factors
- Alice, knowing the prime factors, can invert and recover Bob's message.

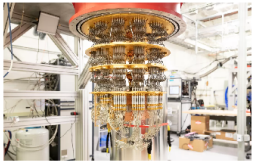
Quantum computing

Overview

IBM Makes Heavy Investments in Quantum Computing

Dec 18, 2017

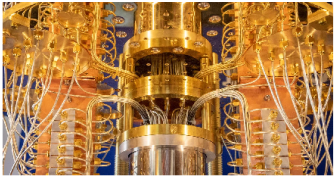




NEWS · 23 OCTOBER 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.



NEWS FEATURE · 02 OCTOBER 2019

Quantum gold rush: the private funding pouring into quantum start-ups

A *Nature* analysis explores the investors betting on quantum technology.

Amazon enters quantum computing race with cloud quantum processors

PHYSICS 3 December 2019

D-Wave partners with NEC to build hybrid HPC and quantum apps

Ron Miller (@ron_miller / 6:31 am +07 • December 11, 2019

Microsoft Is Taking Quantum Computers to the Cloud

The company will allow its cloud customers to tap quantum computers made by Honeywell and two startups.

TU/e

Quantum computing

Applications to cryptography

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Quantum walk algorithm for element distinctness

Andris Ambainis*

ON THE POWER OF QUANTUM COMPUTATION*

DANIEL R. SIMON†

Quantum Amplitude Amplification and Estimation

Gilles Brassard* Peter Høyer†
Michele Mosca‡ Alain Tapp§

A SUBEXPONENTIAL-TIME QUANTUM ALGORITHM FOR THE DIHEDRAL HIDDEN SUBGROUP PROBLEM*

GREG KUPERBERG†

TU/e

Post-quantum cryptography

Ongoing efforts

Organizations Need to be Prepared for Quantum Computing Threats

By: Zeus Kerravala | December 10, 2019

How the United States Is Developing Post-Quantum Cryptography

By **Jeremy Hsu**

Google Tests Post-Quantum Crypto

Quantum Computing Will Shred Current Crypto Systems, Experts Warn

Quantum-Resistant Cryptography: Our Best Defense Against An Impending Quantum Apocalypse

The Quantum Computing Threat to American Security

Google claims supremacy, but the risk remains that U.S. complacency lets China crack all its codes.

Share

The promise and peril of post quantum computing

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

January 30, 2019

Post-quantum cryptography

Candidates

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric-based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

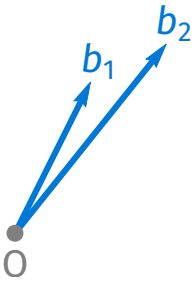
TU/e

Lattices

Basics

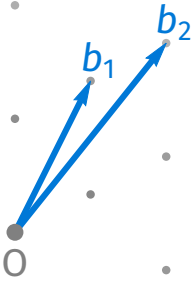
Lattices

Basics



Lattices

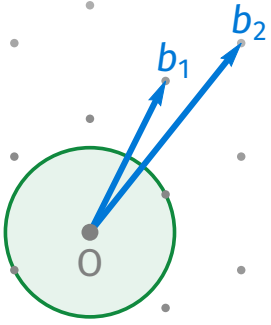
Basics



TU/e

Lattices

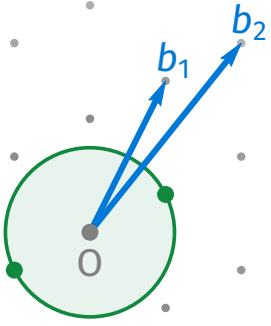
Shortest Vector Problem (SVP)



TU/e

Lattices

Shortest Vector Problem (SVP)



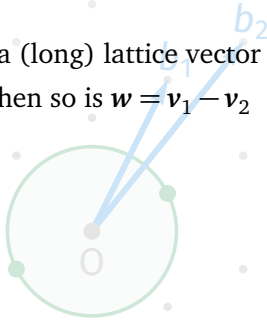
TU/e

Lattices

Evolutionary approach to SVP

Basic lattice tools

- Given a lattice basis, sampling a (long) lattice vector $\boldsymbol{v} \in \mathcal{L}(\boldsymbol{B})$ is easy
- If $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are lattice points, then so is $\boldsymbol{w} = \boldsymbol{v}_1 - \boldsymbol{v}_2$



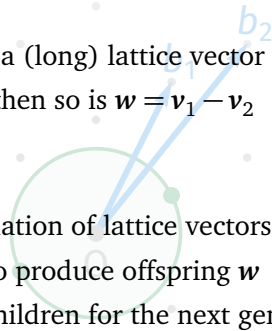
TU/e

Lattices

Evolutionary approach to SVP

Basic lattice tools

- Given a lattice basis, sampling a (long) lattice vector $\boldsymbol{v} \in \mathcal{L}(\boldsymbol{B})$ is easy
- If $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are lattice points, then so is $\boldsymbol{w} = \boldsymbol{v}_1 - \boldsymbol{v}_2$



Evolutionary approach

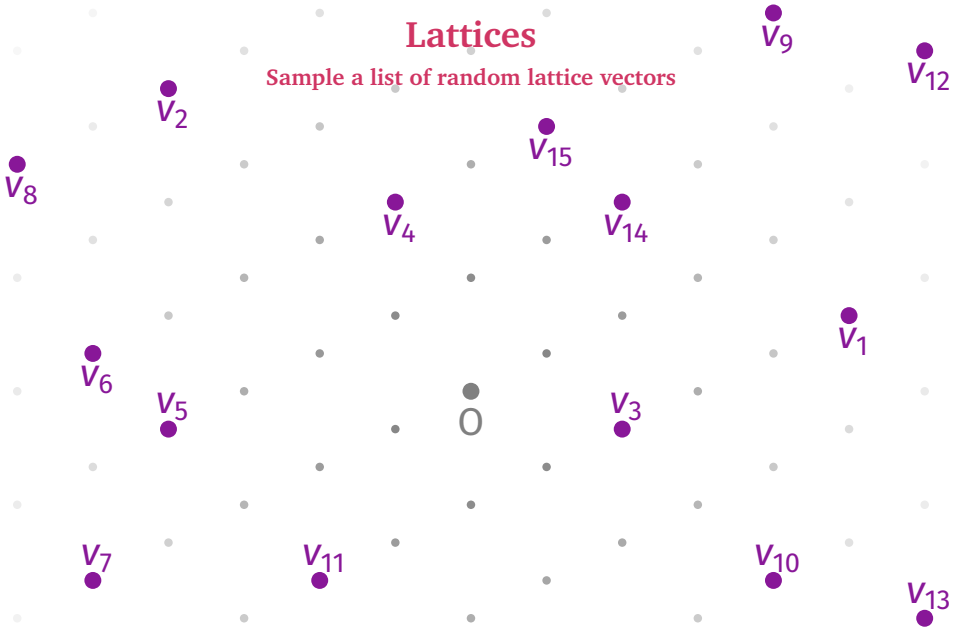
- Construct random initial population of lattice vectors
- Combine parent vectors $\boldsymbol{v}_i, \boldsymbol{v}_j$ to produce offspring $\boldsymbol{w}$
- Select the fittest parents and children for the next generation
- Repeat until the population contains a shortest non-zero lattice vector

Lattices

Sample a list of random lattice vectors

Lattices

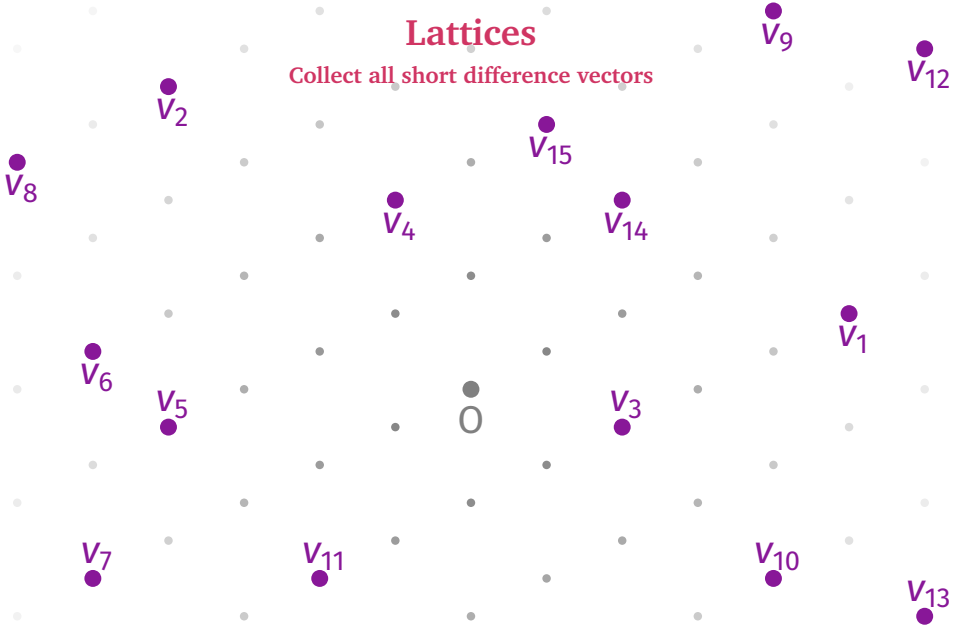
Sample a list of random lattice vectors



TU/e

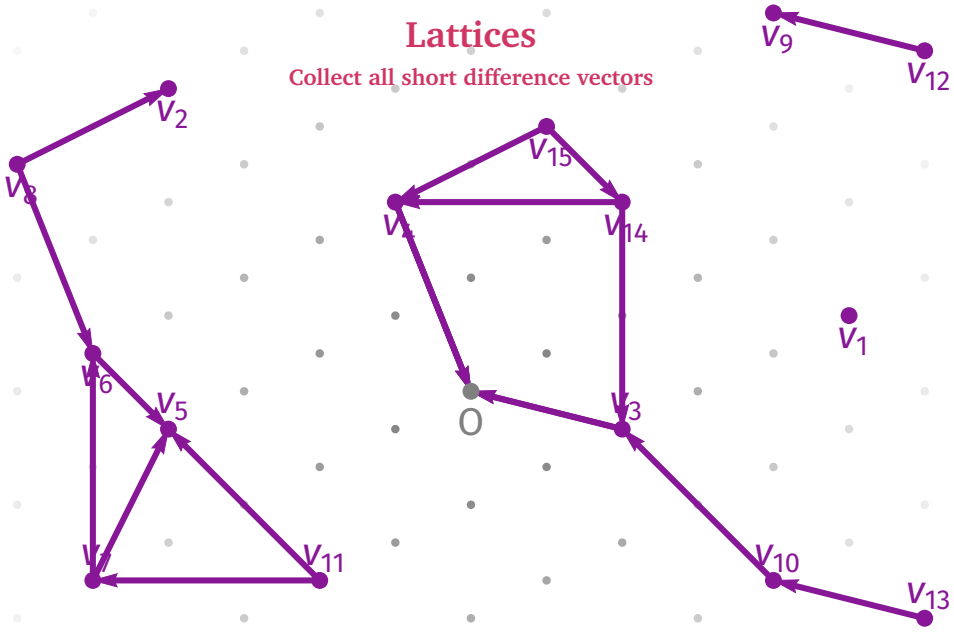
Lattices

Collect all short difference vectors



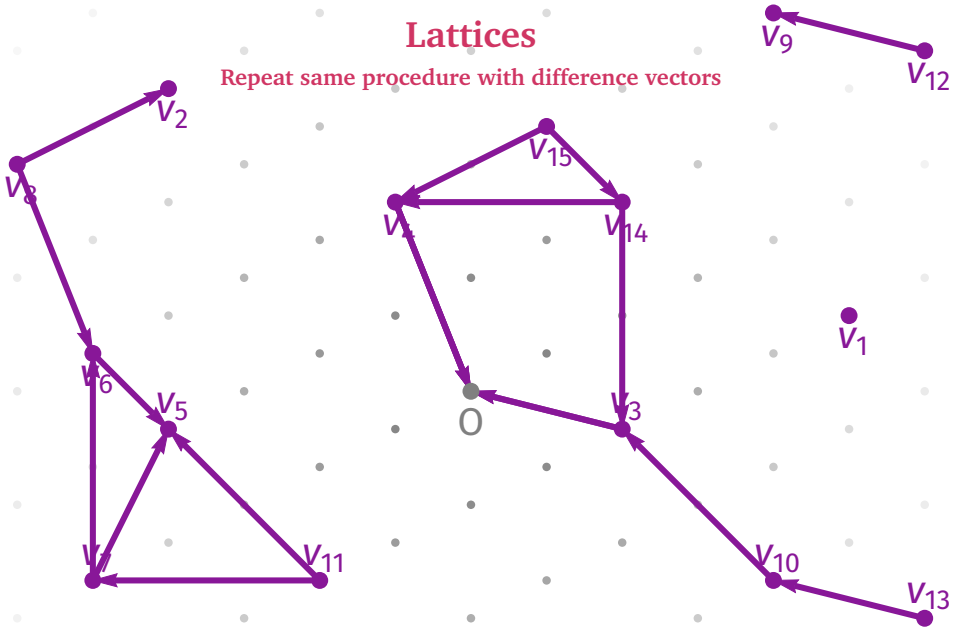
Lattices

Collect all short difference vectors



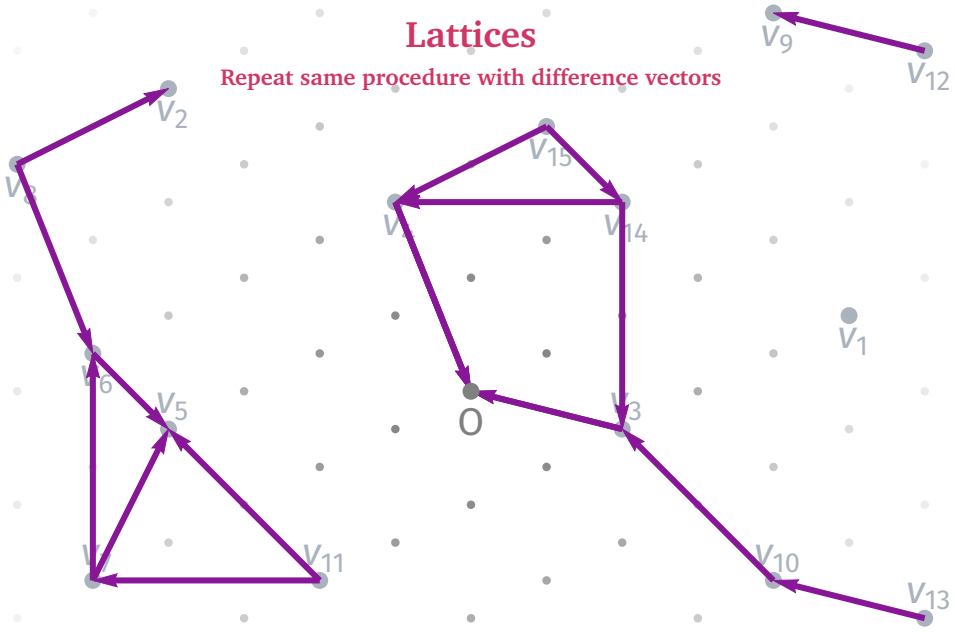
Lattices

Repeat same procedure with difference vectors



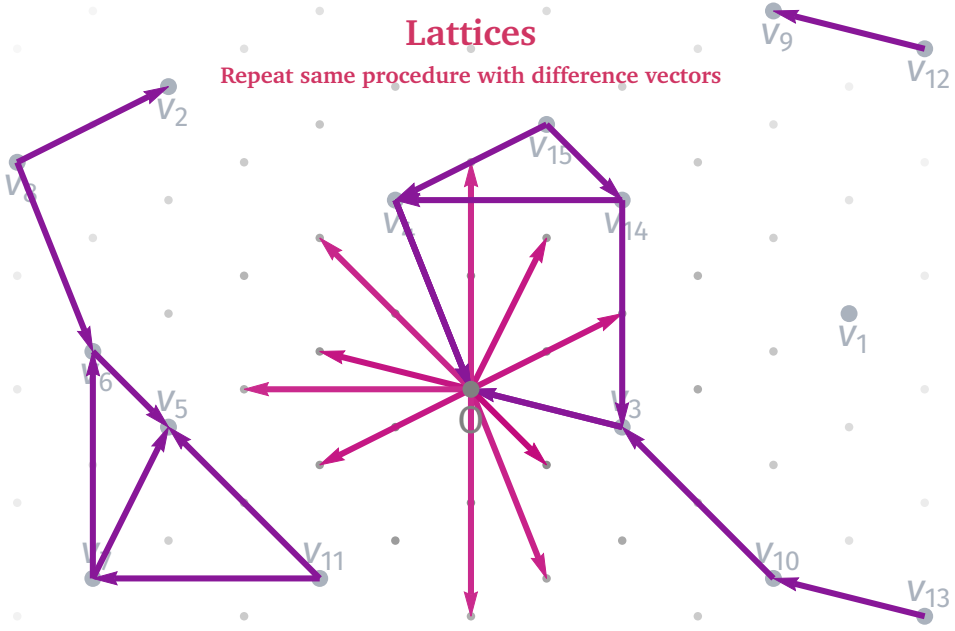
Lattices

Repeat same procedure with difference vectors



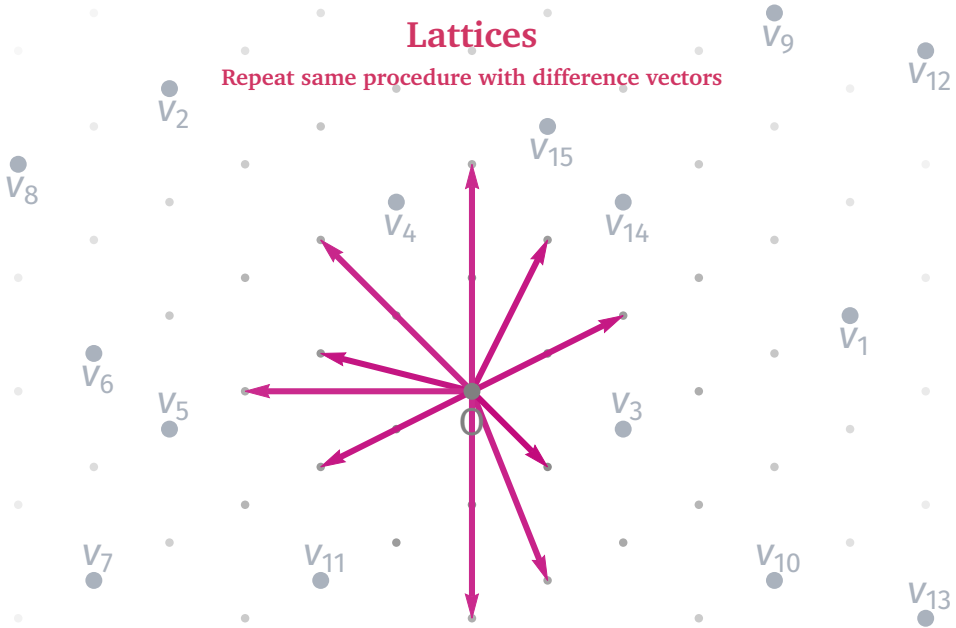
Lattices

Repeat same procedure with difference vectors



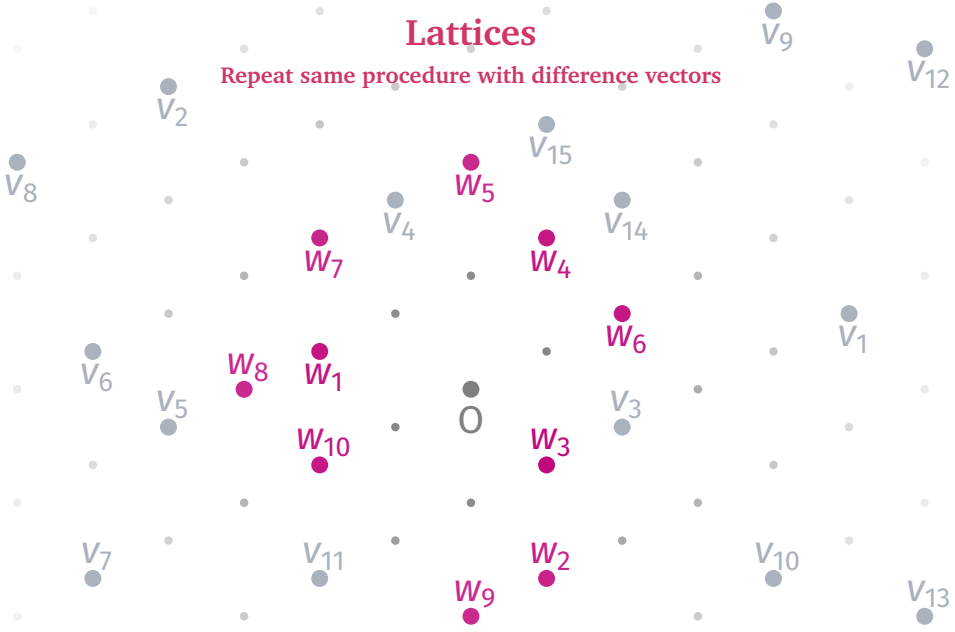
Lattices

Repeat same procedure with difference vectors



Lattices

Repeat same procedure with difference vectors



TU/e

Summary

- **Cryptography**:
  - Methods for secure communication over insecure (public) channels
  - More applications every day with an interconnected world
  - Security currently relies on number-theoretic problems, like factoring

TU/e

Summary

- **Cryptography**:
  - Methods for secure communication over insecure (public) channels
  - More applications every day with an interconnected world
  - Security currently relies on number-theoretic problems, like factoring
- **Quantum computing**:
  - Offers new opportunities in many areas, to solve harder problems
  - Poses threat to currently-deployed cryptographic schemes

TU/e

Summary

- **Cryptography**:
  - Methods for secure communication over insecure (public) channels
  - More applications every day with an interconnected world
  - Security currently relies on number-theoretic problems, like factoring
- **Quantum computing**:
  - Offers new opportunities in many areas, to solve harder problems
  - Poses threat to currently-deployed cryptographic schemes
- **Post-quantum cryptography**:
  - Relies on different hard problems, such as lattice problems
  - Transitions are gradually happening, standardization in progress

TU/e

Summary

- **Cryptography**:
  - Methods for secure communication over insecure (public) channels
  - More applications every day with an interconnected world
  - Security currently relies on number-theoretic problems, like factoring
- **Quantum computing**:
  - Offers new opportunities in many areas, to solve harder problems
  - Poses threat to currently-deployed cryptographic schemes
- **Post-quantum cryptography**:
  - Relies on different hard problems, such as lattice problems
  - Transitions are gradually happening, standardization in progress
- **Artificial intelligence**:
  - Offers new powerful algorithmic tools and capabilities
  - Evolutionary techniques improve state-of-the-art for lattice problems
  - Only scratching the surface – more applications possible?