TU/e Technische Universiteit Eindhoven University of Technology

Thijs Laarhoven

PhD student

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

Department Dialogue, Eindhoven, The Netherlands
(September 17, 2015)

TU/e

Who am I?

- PhD student
- Section: Discrete Mathematics (DM)
- Group: Coding Theory and Cryptology (C&C)
- Promotor: Tanja Lange
- Supervisor: Benne de Weger
- Office: 6.103

TU/e

What do I do?

- Bachelor's project: The Collatz conjecture
- Master's project: Collusion-resistant fingerprinting
- Doctoral project: Lattice algorithms

TU/e

What do I do?

- Bachelor's project: The Collatz conjecture
- Master's project: Collusion-resistant fingerprinting
- Doctoral project: Lattice algorithms

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

Some examples:

- $10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \to \ldots$
  (6 iterations to go from 10 to 1)

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

Some examples:

- $10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \to \ldots$
  (6 iterations to go from 10 to 1)
- $27 \to 82 \to 41 \to \cdots \to 9232 \to \cdots \to 4 \to 2 \to 1 \to \ldots$
  (112 iterations to go from 27 to 1)

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

Some examples:

- $10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \to \ldots$
  (6 iterations to go from 10 to 1)
- $27 \to 82 \to 41 \to \cdots \to 9232 \to \cdots \to 4 \to 2 \to 1 \to \ldots$
  (112 iterations to go from 27 to 1)

1937: Lothar Collatz conjectures that this always leads to 1.

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

Some examples:

- $10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \to \ldots$
  (6 iterations to go from 10 to 1)
- $27 \to 82 \to 41 \to \cdots \to 9232 \to \cdots \to 4 \to 2 \to 1 \to \ldots$
  (112 iterations to go from 27 to 1)

1937: Lothar Collatz conjectures that this always leads to 1.
1970s: Pál Erdős: "Mathematics is not ready for this problem."

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

Some examples:

- $10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \to \ldots$
  (6 iterations to go from 10 to 1)
- $27 \to 82 \to 41 \to \cdots \to 9232 \to \cdots \to 4 \to 2 \to 1 \to \ldots$
  (112 iterations to go from 27 to 1)

1937: Lothar Collatz conjectures that this always leads to 1.
1970s: Pál Erdős: "Mathematics is not ready for this problem."
2009: Thijs Laarhoven starts a Bachelor's project on this problem.

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

Some examples:

- $10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \to \ldots$
  (6 iterations to go from 10 to 1)
- $27 \to 82 \to 41 \to \cdots \to 9232 \to \cdots \to 4 \to 2 \to 1 \to \ldots$
  (112 iterations to go from 27 to 1)

1937: Lothar Collatz conjectures that this always leads to 1.
1970s: Pál Erdős: "Mathematics is not ready for this problem."
2009: Thijs Laarhoven starts a Bachelor's project on this problem.
2014: Problem first posed at the Department Dialogue.

TU/e

The Collatz conjecture

Suppose we iterate the following function:

- If n is even, then $f(n) = n/2$.
- If n is odd, then $f(n) = 3n + 1$.

Some examples:

- $10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to 4 \to \ldots$
  (6 iterations to go from 10 to 1)
- $27 \to 82 \to 41 \to \cdots \to 9232 \to \cdots \to 4 \to 2 \to 1 \to \ldots$
  (112 iterations to go from 27 to 1)

1937: Lothar Collatz conjectures that this always leads to 1.
1970s: Pál Erdős: "Mathematics is not ready for this problem."
2009: Thijs Laarhoven starts a Bachelor's project on this problem.
2014: Problem first posed at the Department Dialogue.
2015: Still no solution!

TU/e

What do I do?

- Bachelor's project: The Collatz conjecture
- Master's project: Collusion-resistant fingerprinting
- Doctoral project: Lattice algorithms

TU/e

What do I do?

- Bachelor's project: The Collatz conjecture
- Master's project: Collusion-resistant fingerprinting
- Doctoral project: Lattice algorithms

TU/e

Collusion-resistant fingerprinting

TU/e

Collusion-resistant fingerprinting

TU/e

Collusion-resistant fingerprinting

TU/e

Collusion-resistant fingerprinting

TU/e

Collusion-resistant fingerprinting

TU/e

Collusion-resistant fingerprinting

TU/e

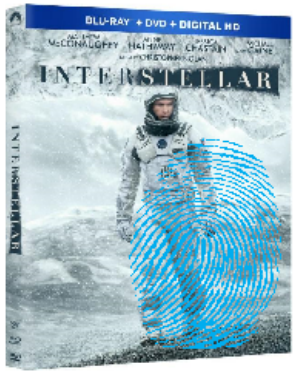
Collusion-resistant fingerprinting

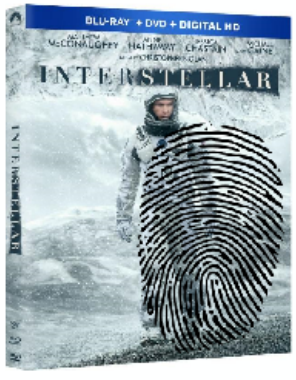
TU/e

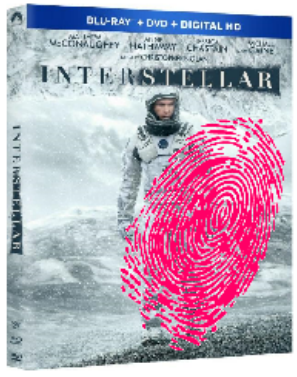
Collusion-resistant fingerprinting

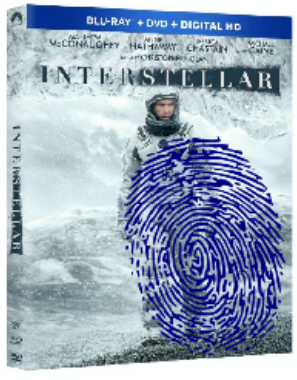
TU/e

Collusion-resistant fingerprinting









TU/e

Collusion-resistant fingerprinting

TU/e

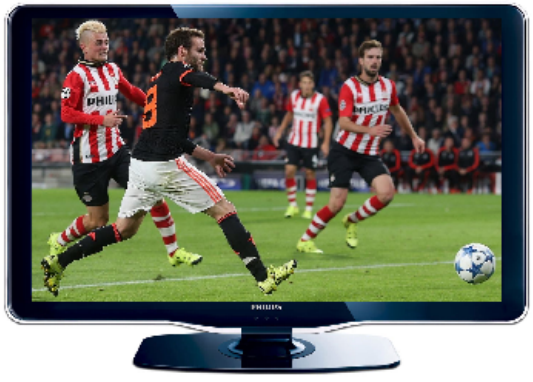
Collusion-resistant fingerprinting

TU/e

Collusion-resistant fingerprinting





TU/e

Collusion-resistant fingerprinting








TU/e

Collusion-resistant fingerprinting








TU/e

Collusion-resistant fingerprinting








TU/e

Collusion-resistant fingerprinting



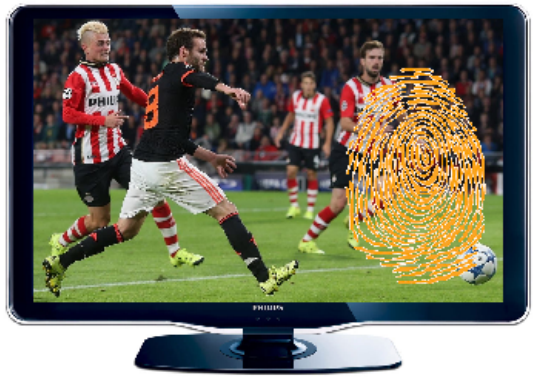





TU/e

Collusion-resistant fingerprinting








TU/e

What do I do?

- Bachelor's project: The Collatz conjecture
- Master's project: Collusion-resistant fingerprinting
- Doctoral project: Lattice algorithms

TU/e

What do I do?

- Bachelor's project: The Collatz conjecture
- Master's project: Collusion-resistant fingerprinting
- Doctoral project: Lattice algorithms

TU/e

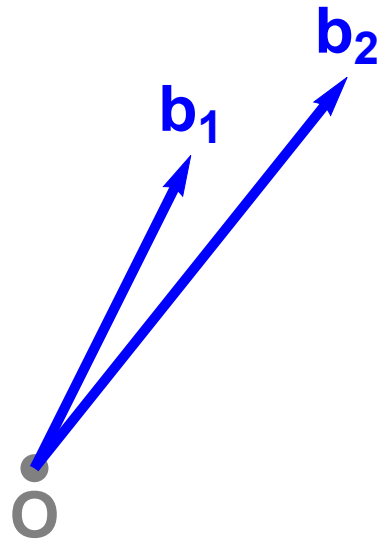
Lattices

What is a lattice?

TU/e

Lattices

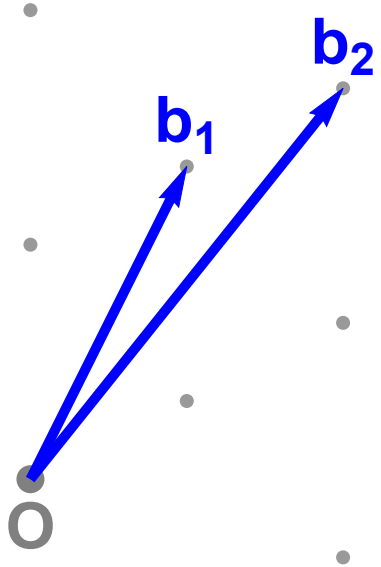
What is a lattice?



TU/e

Lattices

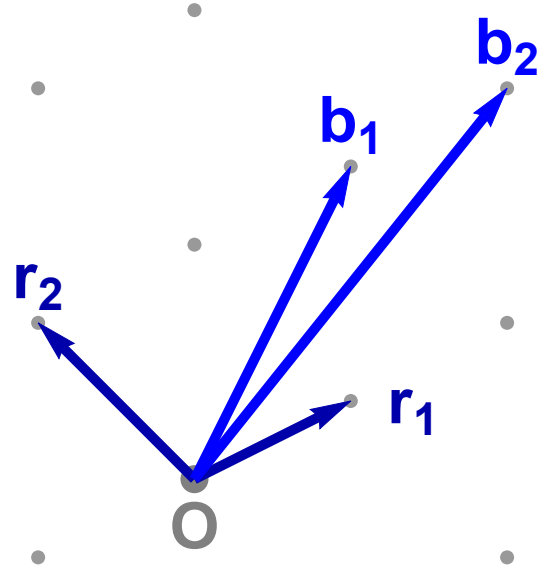
What is a lattice?



TU/e

Lattices

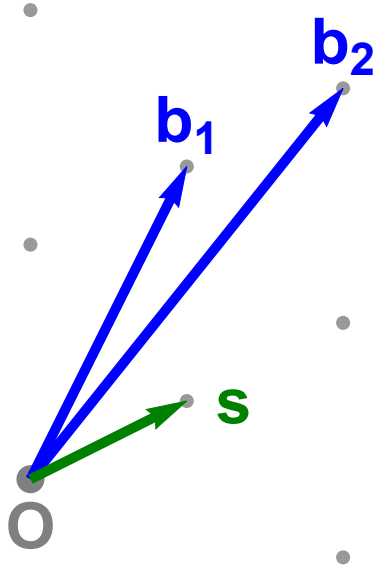
Lattice basis reduction



TU/e

Lattices

Shortest Vector Problem (SVP)



TU/e

Questions?