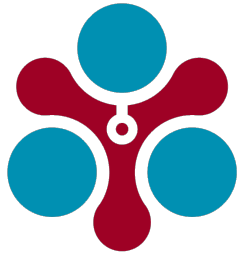
A Personal View of Average-Case Complexity

Russel Impagliazzo
Presented by Bernardo Portela

InfoBlender – 9th of March 2016



HASLab
INESCTEC

Overview

Motivation

Some context

Five worlds

Computational complexity

"There is a large gap between a problem not being easy and the same problem being difficult"

- Russel Impagliazzo, 1995

Preliminaries: P and NP

P: Polynomial time

The solution can be efficiently computed.

- Linear programming, ordering, ...

Preliminaries: P and NP

P: Polynomial time

The solution can be efficiently computed.
- Linear programming, ordering, ...

NP: Non-deterministic polynomial time

The solution cannot be efficiently computed, but can be efficiently verified.
- Hamiltonian path is NP-complete

$$\mathsf{P} \subseteq \mathsf{NP}$$

Preliminaries: One-wayness and PKC

One-way function

A function that is easy to compute for every input, but hard to invert given the image of a random output.

- E.g. Cryptographic hash functions

Preliminaries: One-wayness and PKC

One-way function

A function that is easy to compute for every input, but hard to invert given the image of a random output.
- E.g. Cryptographic hash functions

Public-key cryptography

Simplified as "the task of agreeing on a secret with a stranger over an untrusted channel".

Initial Considerations

What would be the implications of solving the problems of computational complexity?

Initial Considerations

What would be the implications of solving the problems of computational complexity?

- Large scale.

Initial Considerations

What would be the implications of solving the problems of computational complexity?

- Large scale.
- Gauss versus Grouse.

Initial Considerations

What would be the implications of solving the problems of computational complexity?

- Large scale.
- Gauss versus Grouse.

Some assumptions

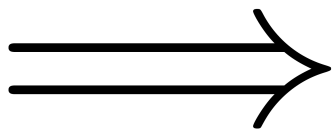
- Undefined computational model.
- Quantitative details ignored.
- Exists implies that everyone knows it.
- If one can run it, everyone can.

Algorithmica

$$P = NP$$

- Grouse fails miserably.
- Computational power allows for extraordinary optimizations.
- Impossible security?

Algorithmica

- Efficient algorithm for an NP-complete problem.  Algorithmica

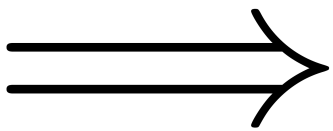
Heuristica

NP hard on worst-case, but feasible on the average-case.

- Grouse fails (less miserably).
- Computational power covers a reduced amount of solutions.
- Impossible security?

Heuristica

- Algorithm for solving NP on average case.
- Lower bound for NP on worst case.



Heuristica

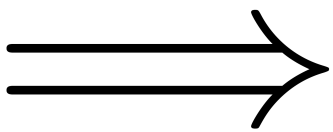
Pessiland

NP hard on average-case. There are no one-way functions.

- "I don't know sir, what's the answer?"
- Optimization via heuristics.
- Problems are useless for cryptography.

Pessiland

- Algorithm for inverting one-way functions.
- Lower bound for NP on average case.



Pessiland

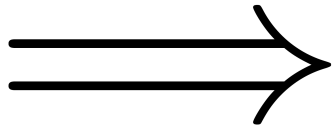
Minicrypt

One-way functions exist. Public-key cryptography impossible.

- The bad guy wins.
- Computation is similar to our world.
- No key agreement, no multiparty computation.

Minicrypt

- No efficient algorithm for inverting one-way functions exists.
- Algorithm for breaking key agreement.



Minicrypt

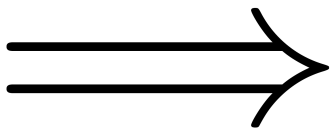
Cryptomania

Public-key cryptography is secure.

- Gauss is utterly defeated.
- Computation is similar to our world.
- Security is similar to our world?

Cryptomania

- Prove a key-agreement as secure.



Cryptomania

Discussion

- The most relevant problems identified in 1995 are still of great relevance in 2016.
- Cryptography and security are always pursuing the middle-ground.
- The worst possibility might not be that bad.

Wrap-up

1. Algorithmica : P = NP
2. Heuristica: NP hard on worst-case, feasible on the average
3. Pessiland: NP hard on average, no one-way functions
4. Minicrypt: One-way functions, no public-key crypto
5. Cryptomania: Public-key crypto

A Personal View of Average-Case Complexity

Russel Impagliazzo
Presented by Bernardo Portela

InfoBlender – 9th of March 2016