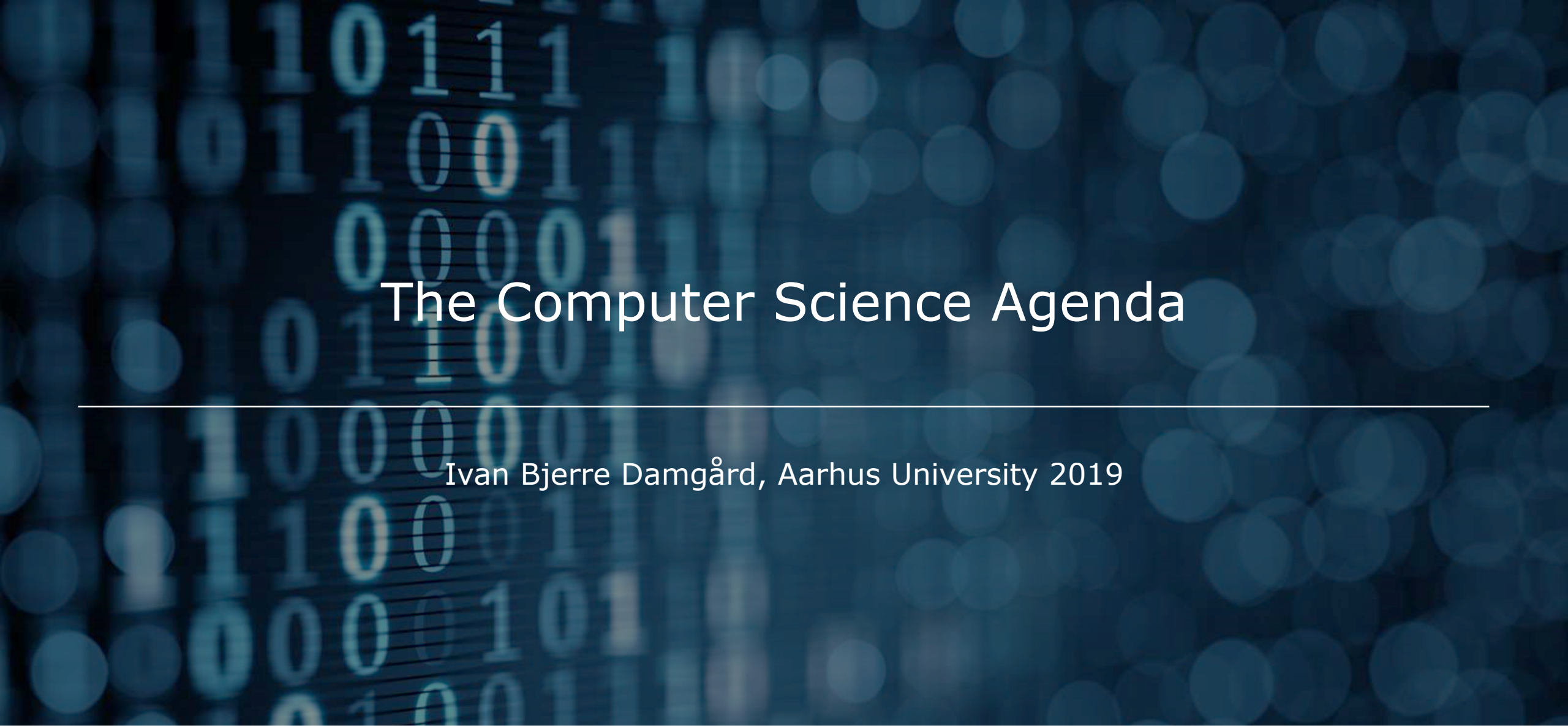


The Computer Science Agenda

Ivan Bjerre Damgård, Aarhus University 2019

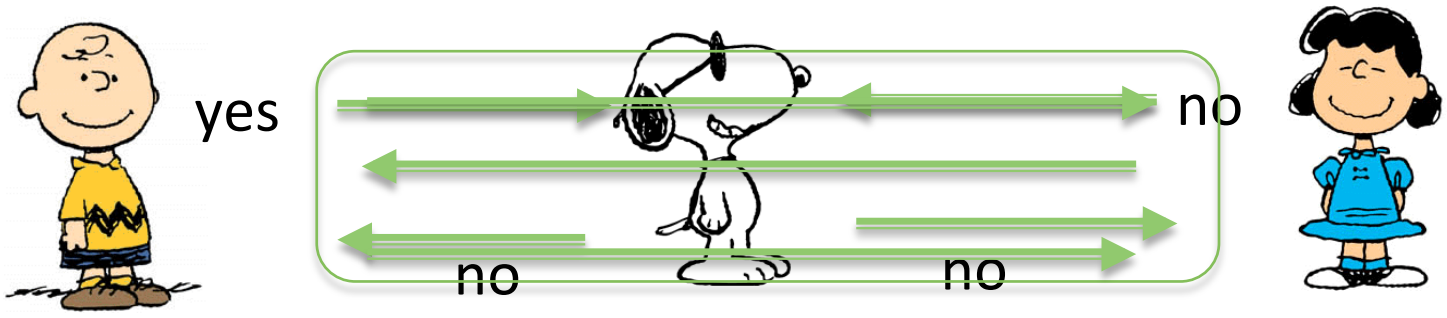
Secure Computation

- A number of parties each hold some private data. Want to compute some output they are all interested in.
- But such that the intended result is the **only** new data that is leaked.
- Means that inputs are kept as private as possible.

- Tons of applications: secure benchmarking, privacy preserving machine learning, secure statistics, etc..
- CS Research: explore what we can and cannot do, more efficient solutions. Stay at the forefront of the development. But also some completely new issues..

An Example

- Charlie wonders if Lucie wants to go out with him. Lucie considers the same question
- Question: How to find out if there is mutual interest without risk of embarassment?
- Easy with a trusted third party.
- But with secure computation we can do without trusted parties!



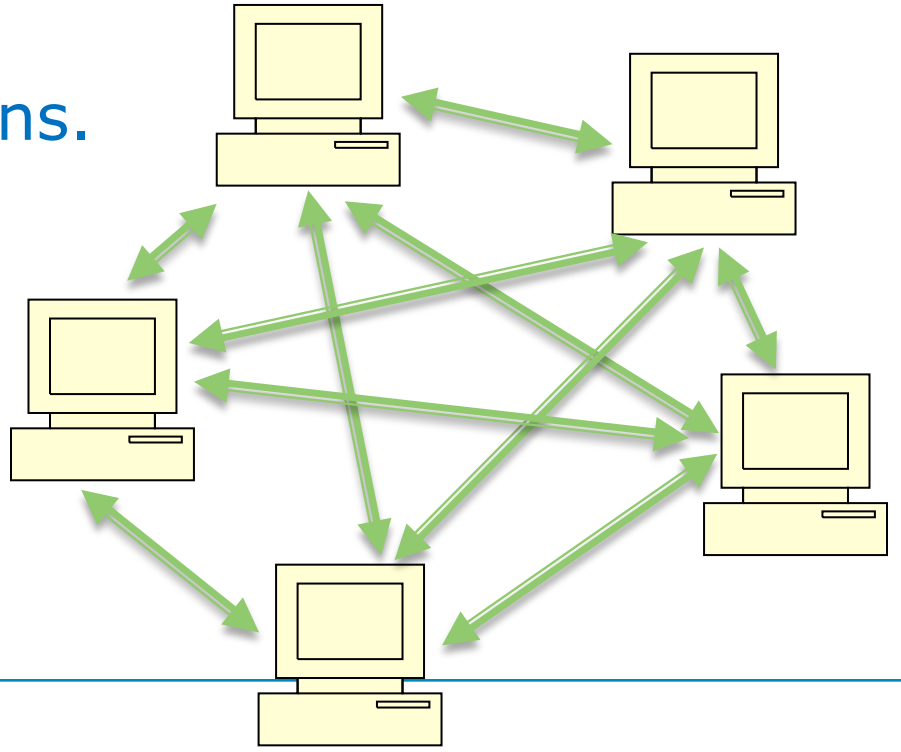
Secure Computation Protocol

A problem

- What if Lucy is malicious? She could pretend to be interested, and then would find out what Charlie's input is.
- Cryptography cannot help here: you can always run a system with whatever input you want.
- Concepts from Economy relevant here: make sure parties have **incentive** to provide their true input.
- Much more research neded to understand such issues: not just the inputs, why would you want to play the game in the first place?

Distributed Systems and Blockchains

- Consider a bunch of computers, connected by a network
- When events happen in the system, want that all nodes learn what happened, and agree on the order in which events took place.
- Totally ordered broadcast.
- Important for, e.g., financial transactions.



Blockchain is a way to achieve totally ordered broadcast, even if parties come and go and network is imperfect.

CS Research and More

- Design even more efficient protocols for reaching consensus, e.g., in blockchain scenarios
- Prove that they work making as few assumptions as possible, on the network quality and the number of players who follow protocol.
- Problem: even if we can guarantee that everything works if half the players are honest, how do we know this is true in practice?
- Typical answer in cryptocurrency setting: because we pay players when they do the right thing.
- But these games are poorly understood – currently we have to hope for the best. Research badly needed.

Thanks!