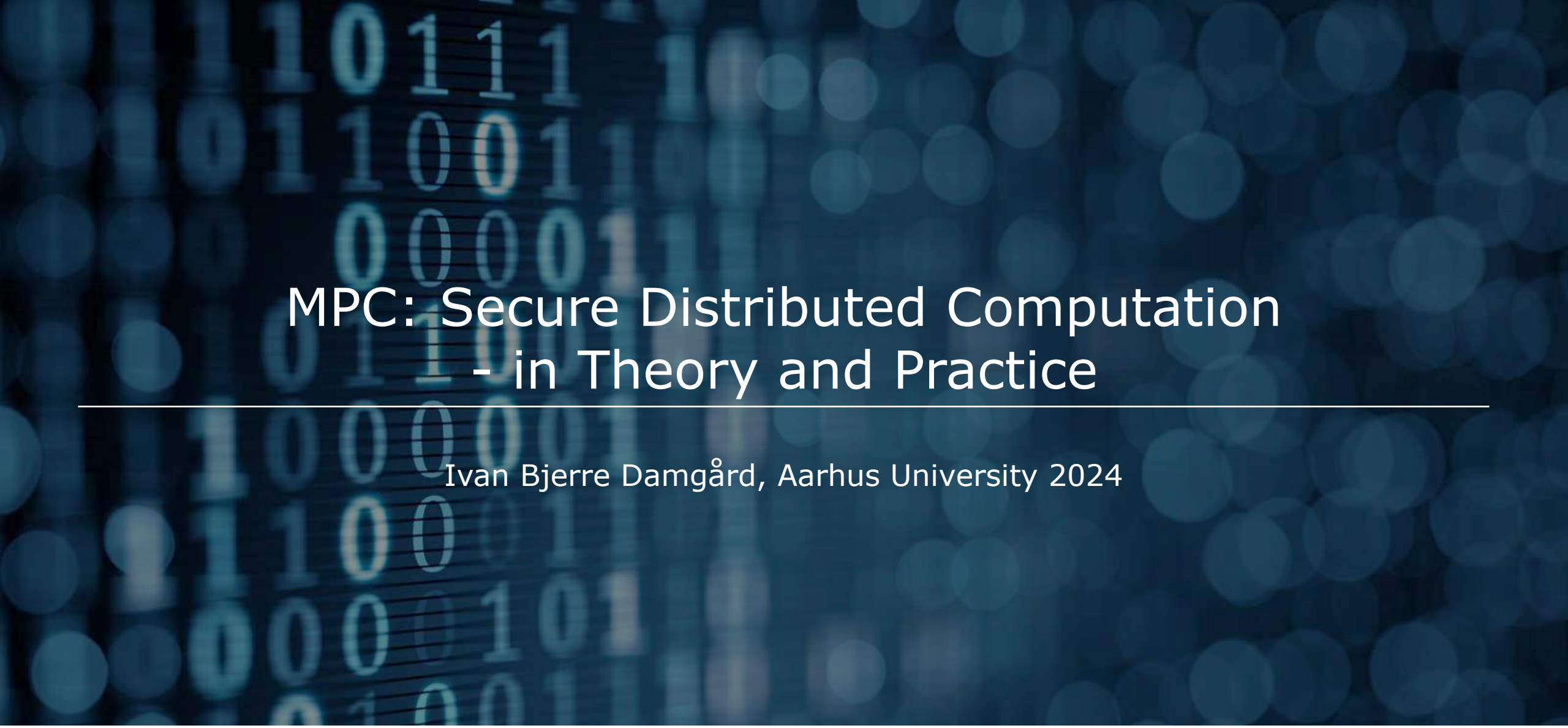
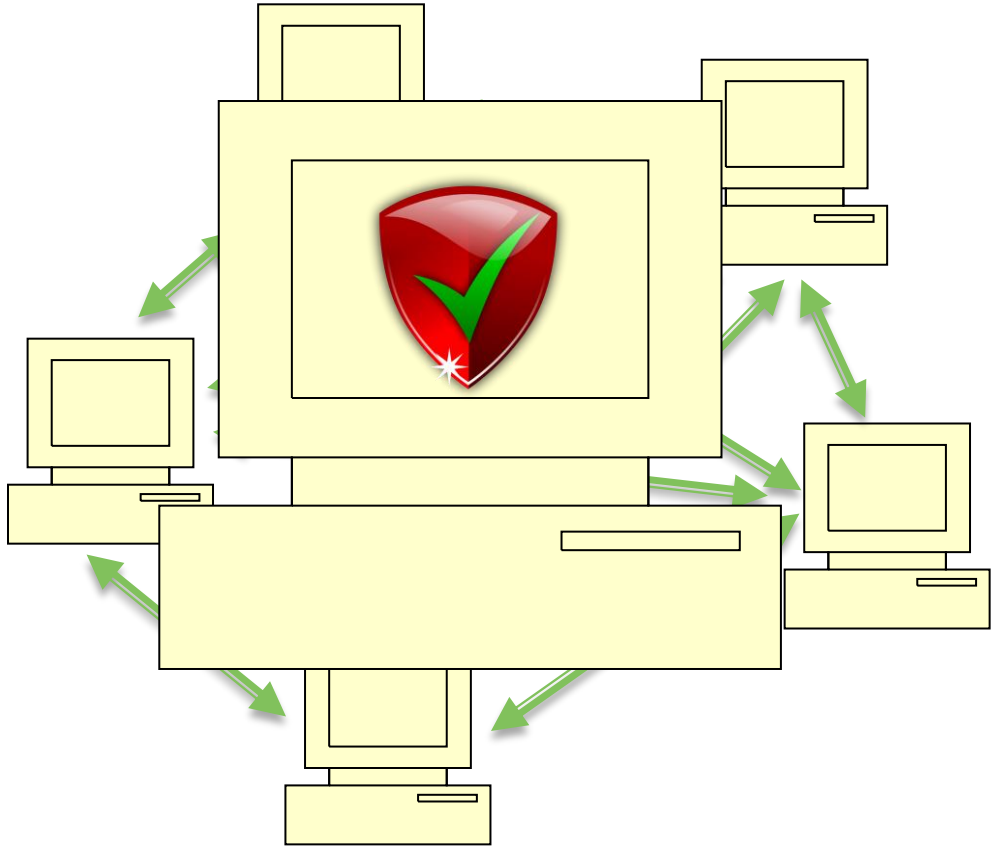


MPC: Secure Distributed Computation - in Theory and Practice

Ivan Bjerre Damgård, Aarhus University 2024

A basic research problem

Some computers connected in a network.
Question: Can we make them collaborate, so it seems we have **one single machine**..
.. which, however, is **more secure than** each individual computer on its own?



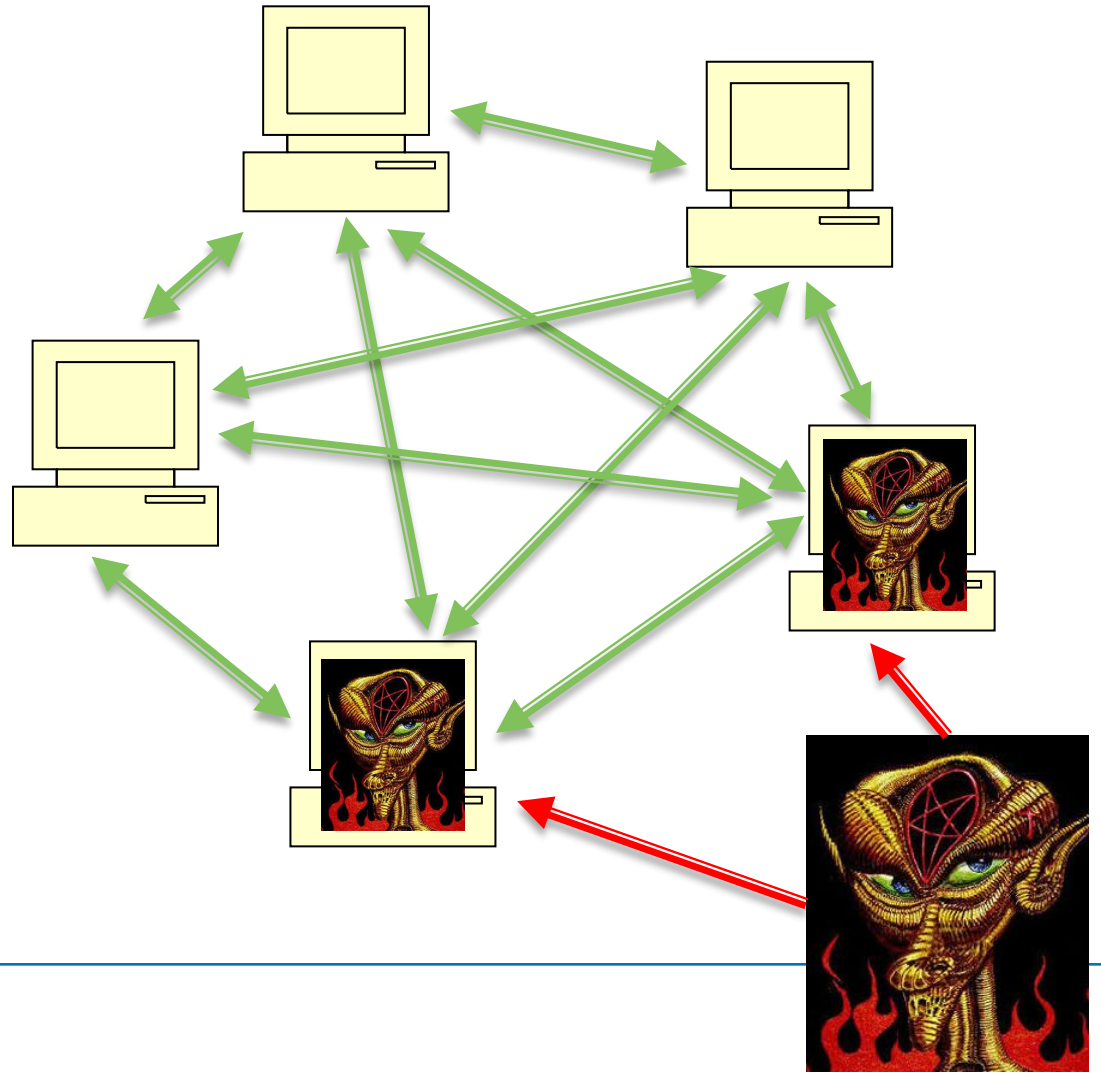
The basic problem, continued

"More secure" means:
Assume a hacker takes control of some of the machines (but not all of them) …

.. The system should still work:

- The attacker cannot steal data
- We get correct results

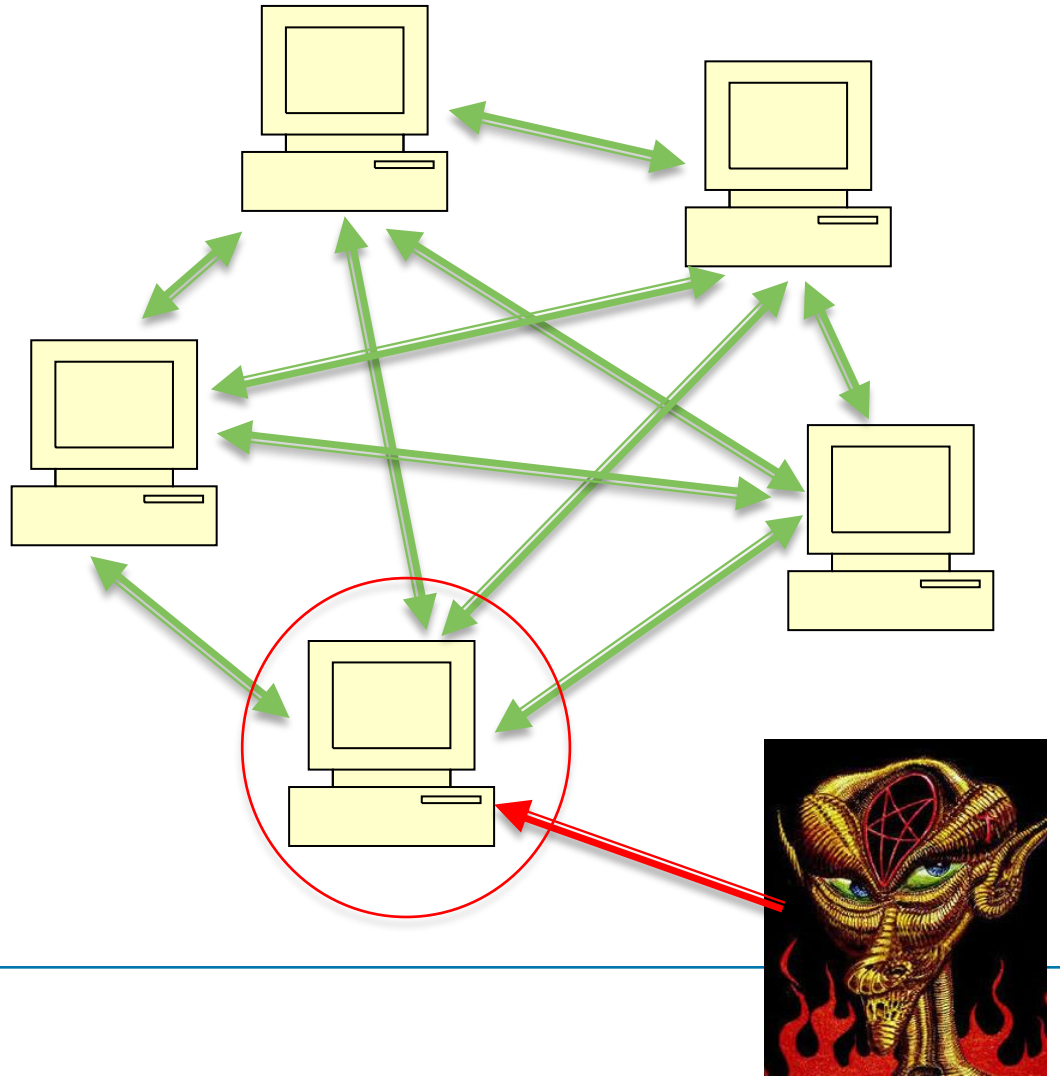
Why is this important? Think of computing the result of an election..



Wait! Is this even possible??

If the system stores data and can compute on them, then the data must be on one of more of the computers?
So, if the attacker “hits” a machine that “knows something”, he can steal at least part of our data.

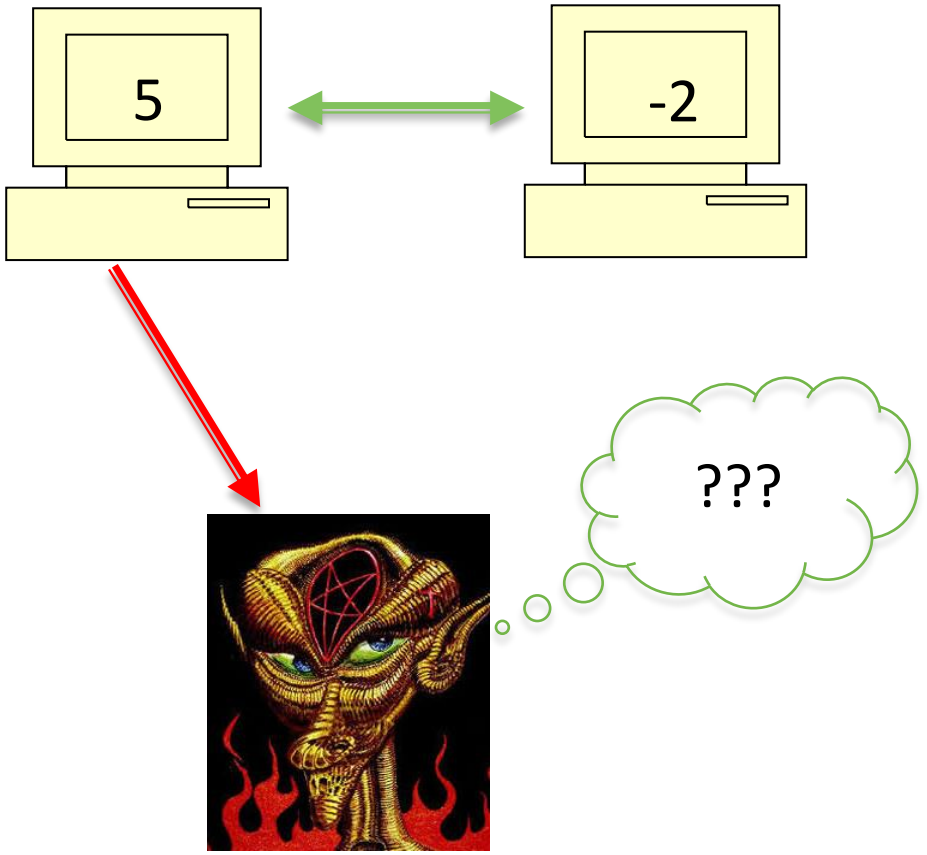
..note that we don’t know in advance where the attack will hit.



There are solutions!

Assume our secret information is a number: 3
We choose two random numbers that sum to the secret, say 5 and -2
Store one number in each of two machines.
Even if one machine is broken into, the attacker has no idea what the secret is.

Conklusion: **Even if data is in the system, it does not have to be in any single place!**



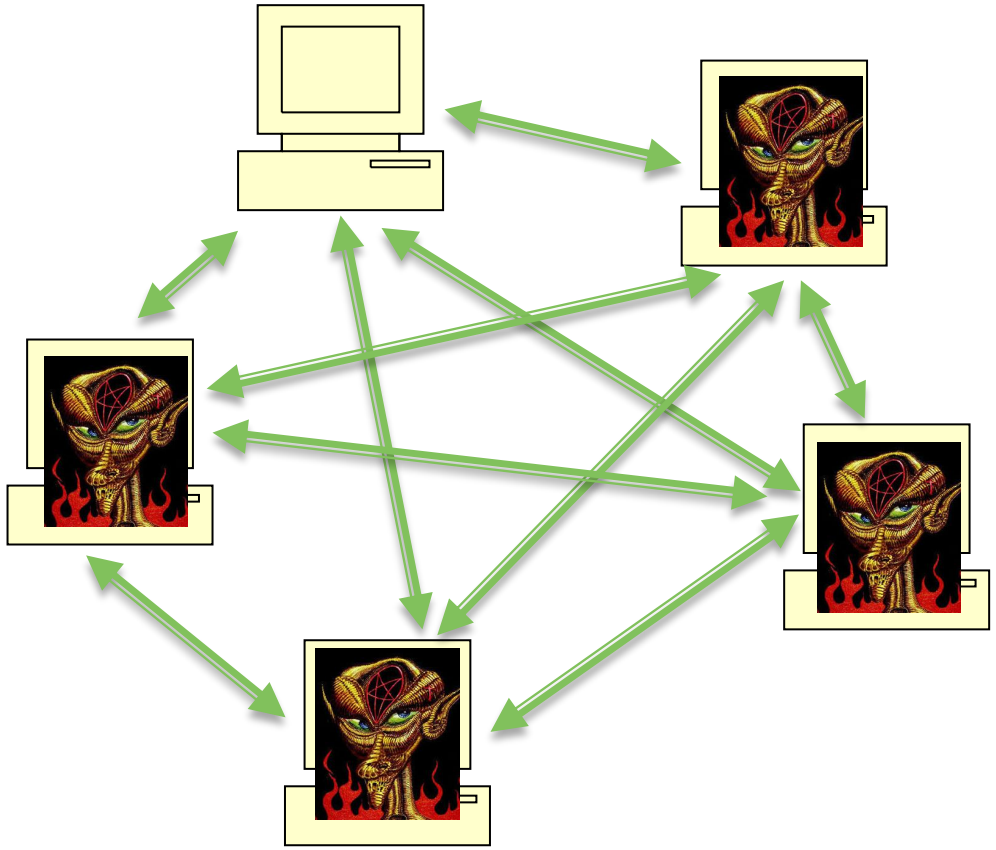
Multiparty Computation (MPC)

Question: can we build one secure computer from several less secure ones?

Answer:

Yes! If *less than half the machines* are taken over by an attacker.

Even if *all but one machine* are attacked, we can still do it – almost: worst case, the system stops. No data can be stolen, no incorrect output.



Applying MPC

- It’s not just about building a more secure system: the computers in the system can be operated by several different parties/companies.
- This way, MPC offers a way to collaborate on doing a computation on private data, without giving away the data.

An example: persons A,B,C,D and E want to know what the average of their salaries is.

But without revealing how much they each make.

Note: it will be enough to compute the sum of the salaries.

Computing the sum using MPC

The salary of A is a number a, for B a number b, etc.

A chooses 5 random numbers a1, a2, a3, a4, a5 such that
a = a1+a2+a3+a4+a5

A keeps a1 and sends privately a2 to B, a3 to C, a4 to D and a5 to E.

The others do something similar, as a result we have…

Computing the sum using MPC

Received by:		A	B	C	D	E	Sum to:
Sent by:	A	a1	a2	a3	a4	a5	a
	B	b1	b2	b3	b4	b5	b
	C	c1	c2	c3	c4	c5	c
	D	d1	d2	d3	d4	d5	d
	E	e1	e2	e3	e4	e5	e
		s1 +	s2 +	s3 +	s4 +	s5 =	Result

Everyone just gets random numbers: learns nothing new.

Everyone adds their columns and publishes the sum.

We can all compute the result!

Conclusion and the Future

- MPC can be used to do tasks that could not be done before, either because data protection regulations were in the way, or because of lack of trust.
- In the future, we can imagine a whole new data economy where people never need to give up control of their data.

  Instead, you consent to your data being used for a certain purpose.

  You can trust that the data is used only as intended.

  Not because you have to trust a single party (a public authority, Google, Facebook…).

  But because the MPC system keeps your data hidden and only reveals the results we agreed on.

Thanks!

Questions?