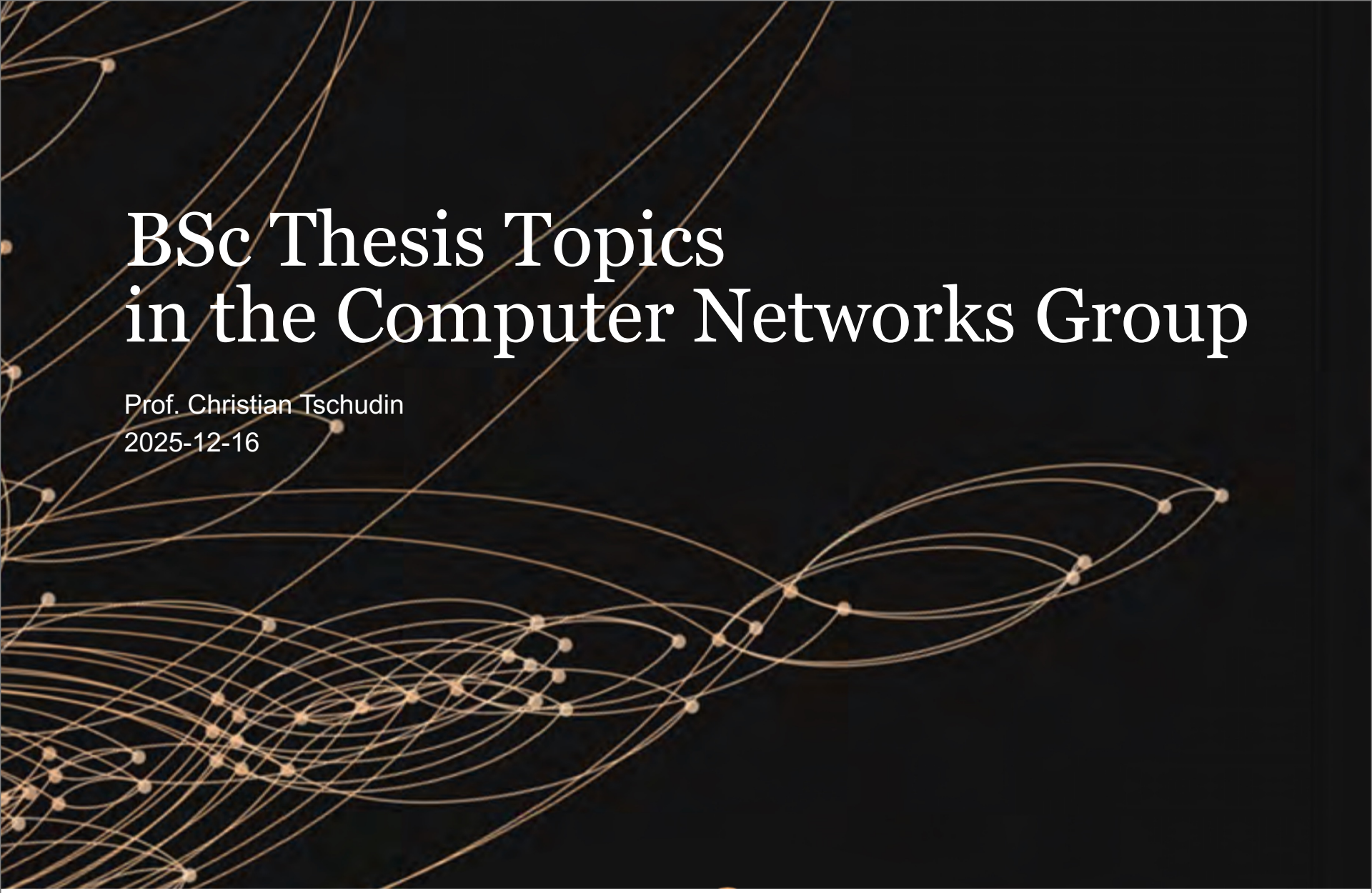


BSc Thesis Topics in the Computer Networks Group

Prof. Christian Tschudin

2025-12-16

University of Basel

Members of the Computer Networks Group

Erick Lavoie	Osman Biçer	Christian Tschudin	Ali Ajorian
peer-to-peer	*cryptography*	*computer networks*	*compilers, crypto*

Teaching

Fall Semester 2025

- Computer Architecture
- Seminar “New Interconnects for P2P applications”
- Foundations of Distributed Systems (MSc, with FC, HS, IW)

Spring Semester

- Distributed Programming and Internet (formerly “Internet and Security”)
- Advanced Computer Networks Topics (MSc)

Topics of some past seminars

. Radio Programming
. Interpretation and Compilation of Programming Languages (Lavoie, Ajorian)
. Conflict-free Replicated Data Types (CRDT, w/ Lavoie)
. Programming with Monads, Haskell (w/ Lüthi)
. Programming with LISP (w/ Lüthi)

General Areas for BSc Projects

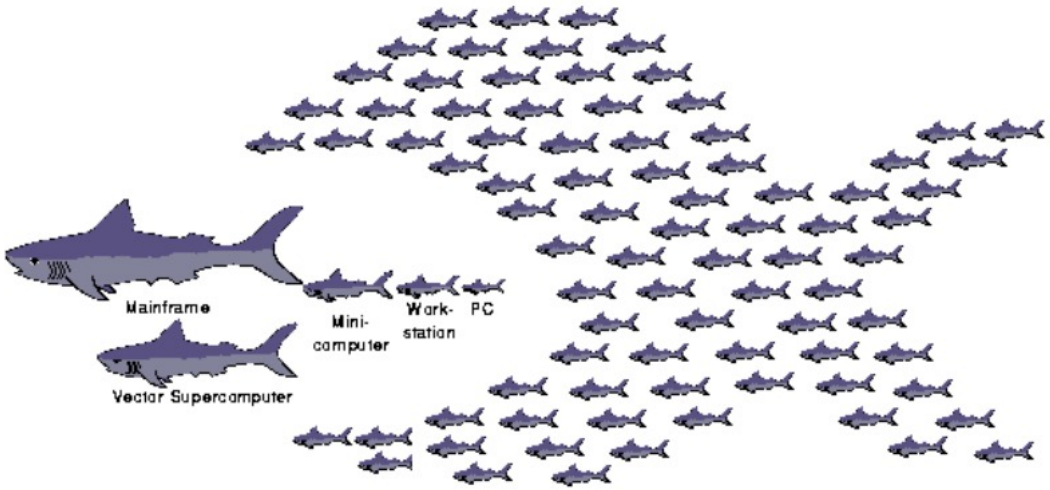
A. Distributed Applications / Peer-to-Peer

B. Hostile Environments
   - like the Internet, or your SmartPhone
   - cloud (homomorphic computing)

C. BYOT

A) Distributed Applications

Aristotle: *«The whole is more than the sum of its parts»*



"scale out" instead of "scale up"

Despite the cloud: statement is not obvious in Computer Science, as server-based solutions dominate, central mgmt

Science question: What «DNA» for successful peer-to-peer applications?

A) Distributed Applications

Aristotle: *«The whole is more than the sum of its parts»*

ut"
ead of
"scale up"

Observation:

we have reached "PEAK CLOUD"
(like "Peak Oil")

It starts to be cheaper again to install and run your own servers, plus the privacy advantage: run LLMs on-prem, not in the cloud

Despite the cl

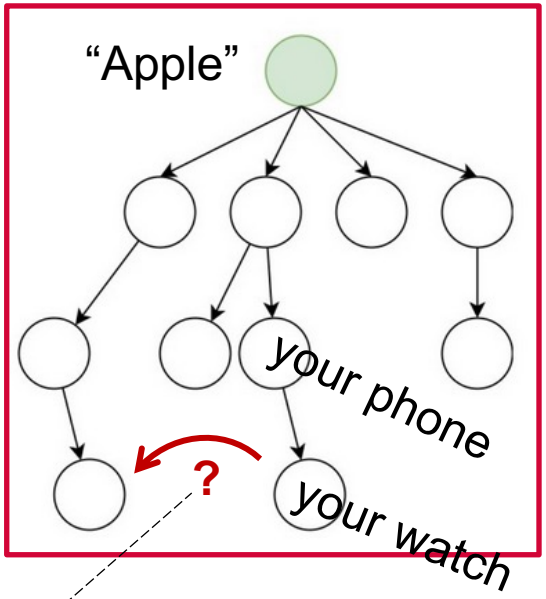
mt

Science questi

peer-to-peer applications?

A) Distributed Applications:

a decentralized scenario



Today's distribution economics:
- buy a smart watch
- buy a smartphone
  (to connect your smart watch)
- buy a mobile plan
  (to connect your smartphone to the cloud)
- buy a cloud subscription
  (to access Apple's services)

An alternate economic model:
- buy some device
- let the device talk to its peers, directly

There is a market for P2P knowhow, startups

A) Distributed Applications (contd):

re-structuring «the stack»

A post-Internet architecture for distributed applications:

distributed applications based on CRDTs *)

data replication via trustable append-only logs

peer-to-peer connectivity

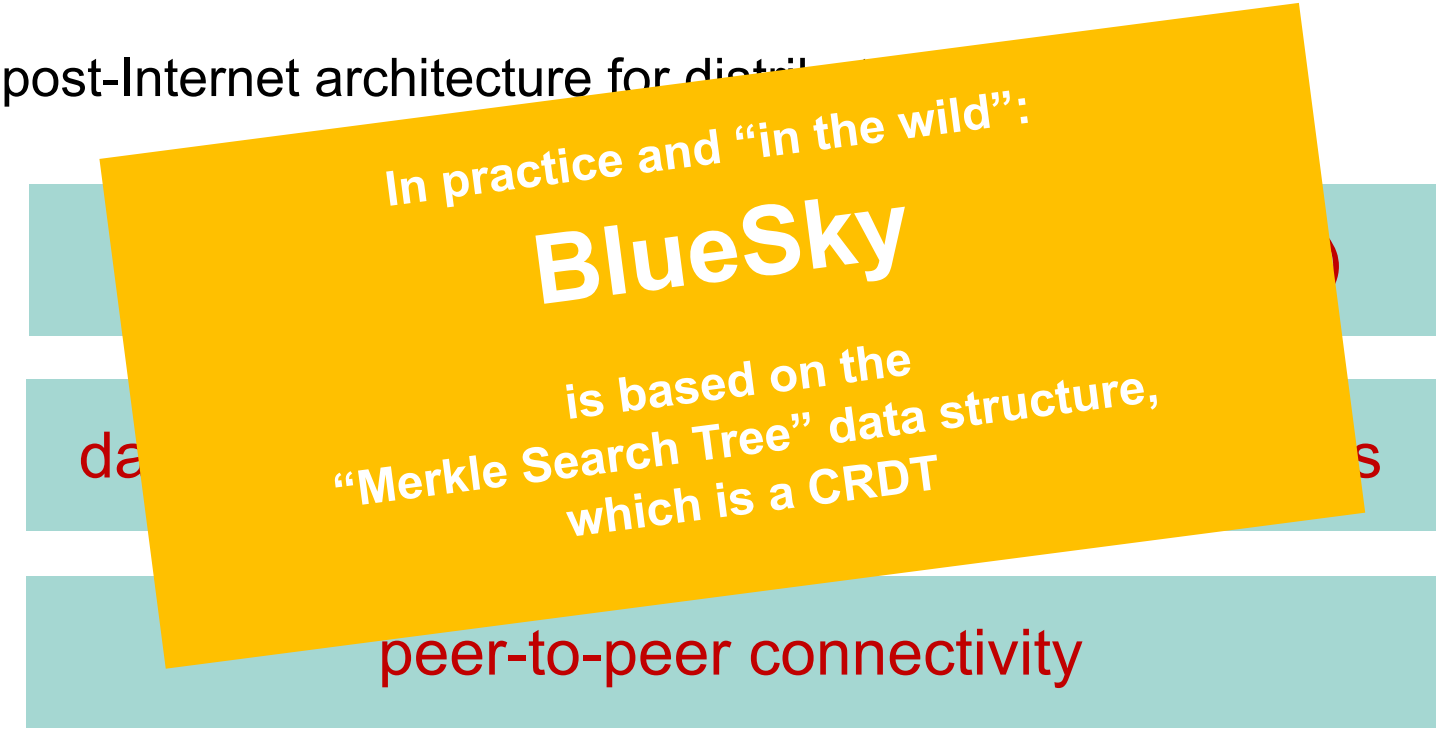
CRDT=«Conflict-free Replicated Data Types», discovered 2011

Theme: Cut out the middle men, build your own network → go radio

A) Distributed Applications (contd):

re-structuring «the stack»

A post-Internet architecture for distri



CRDT=«Conflict-free Replicated Data Types», discovered 2011

Theme: Cut out the middle men, build your own network → go radio

A) Distributed Applications (contd) – as a BSc thesis topic

Useful CRDTs:

- productivity (Kanban, shopping list, «lokens»)
- games (combining CRDT with state machines, «secure dice rolling»)
- decentralized app-store
- «personal tech» (does not have to be P2P, replication is value, already):

  replicated password store, contacts list

  that is independent of Google, Apple and Dropbox

Theme: Cut out the middle men

B) Hostile Computing Environments

How to safely use a computer, post-compromise?

yes, this is about your SmartPhone and your Laptop
(forced updates of OS and apps, not blockable
scanning of your content)

Cryptographic solutions exist in the client/server model.
But what about peer-to-peer?

First theory result in our group, «oblivious homomorphic encryption»
awaits exploration with implementations, and obfuscation approaches

B) Hostile Computing Environments (continued)

How to safely use a computer, post-compromise?

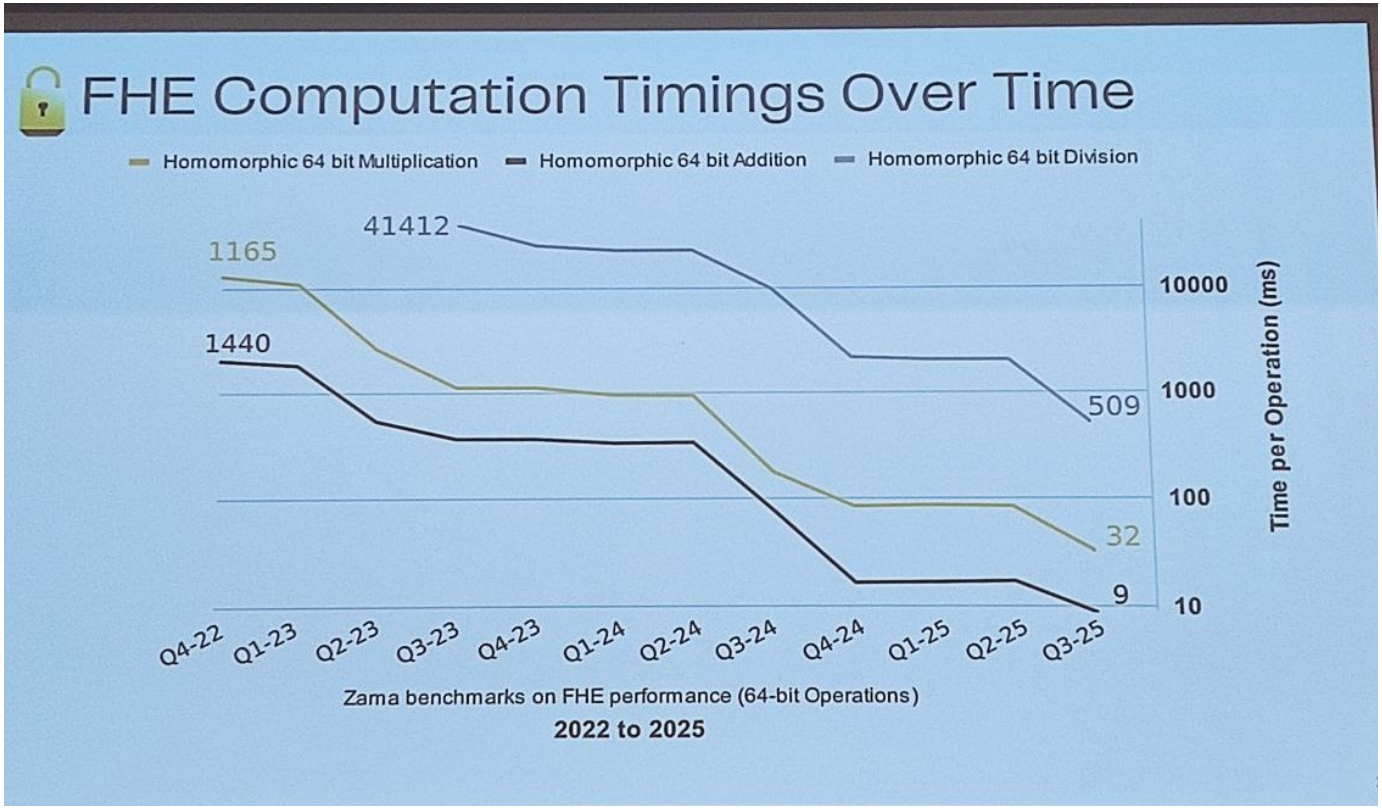
Crypto meets Computer Architecture (circuits!):

Yao's millionaire problem: how can two millionaires find out who owns more, without revealing how much they own? → «secure multiparty computation»

MPC can be solved with «garbled circuits»:
- let your adversary compute the output of a digital circuit (XOR, AND gates)

Similar techniques used today for zero-knowledge proofs,
with applications in crypto-coins and online-voting

(from past Friday, Crypto workshop at Bocconi University, Milan, Italy)



100-fold or more speedup progress for FHE in the past years ..

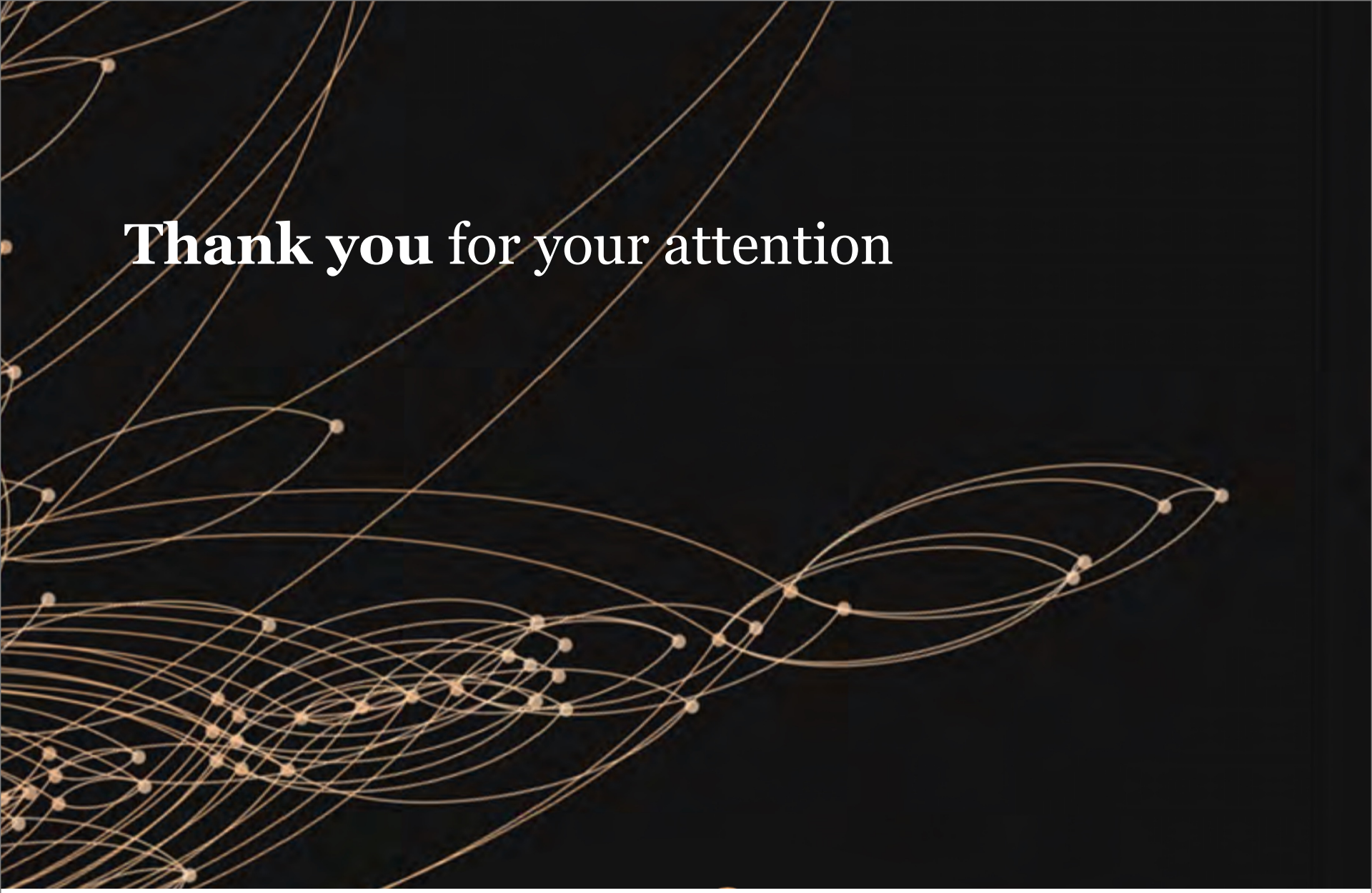
C) BYOT (bring your own topic)

Many ways «to do distribution» and a BSc thesis on this question.

If you have an idea or use case:

come and talk to us!

See more BSc topics on the Web Site



University of Basel