MINDSHARE

2025 10–11 SEP

CYBERSECURITY LEADERSHIP FORUM

Securing Identity for our Digital Future

MINDSHARE AGENDA

GET APP

All Together

How to make a cat look like guacamole – Attacks on Artificial Intelligence

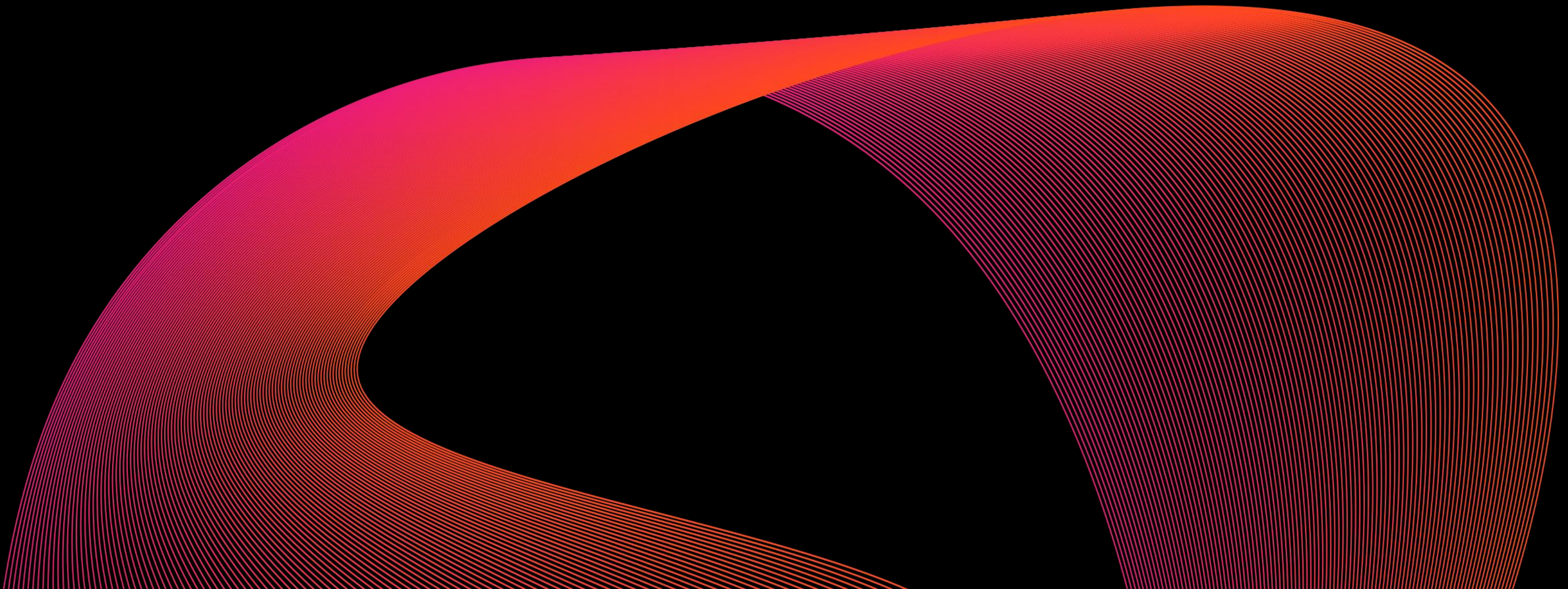
Ground Floor // Konferenzsaal - Pavillo...

Klaus Schmeh

● Speaker ● Host

Artificial Intelligence (AI) tools, such as ChatGPT or Bard, have become important aids for every IT user. However, there are powerful techniques to attack systems of this kind, including AI poisoning, adversarial patterns, AI jailbreaking, and image cloaking. This presentation gives an overview o

EVIDEN



MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

UTiLACY

Dr. David Niehues
utilacy GmbH

Secure Multiparty Computation

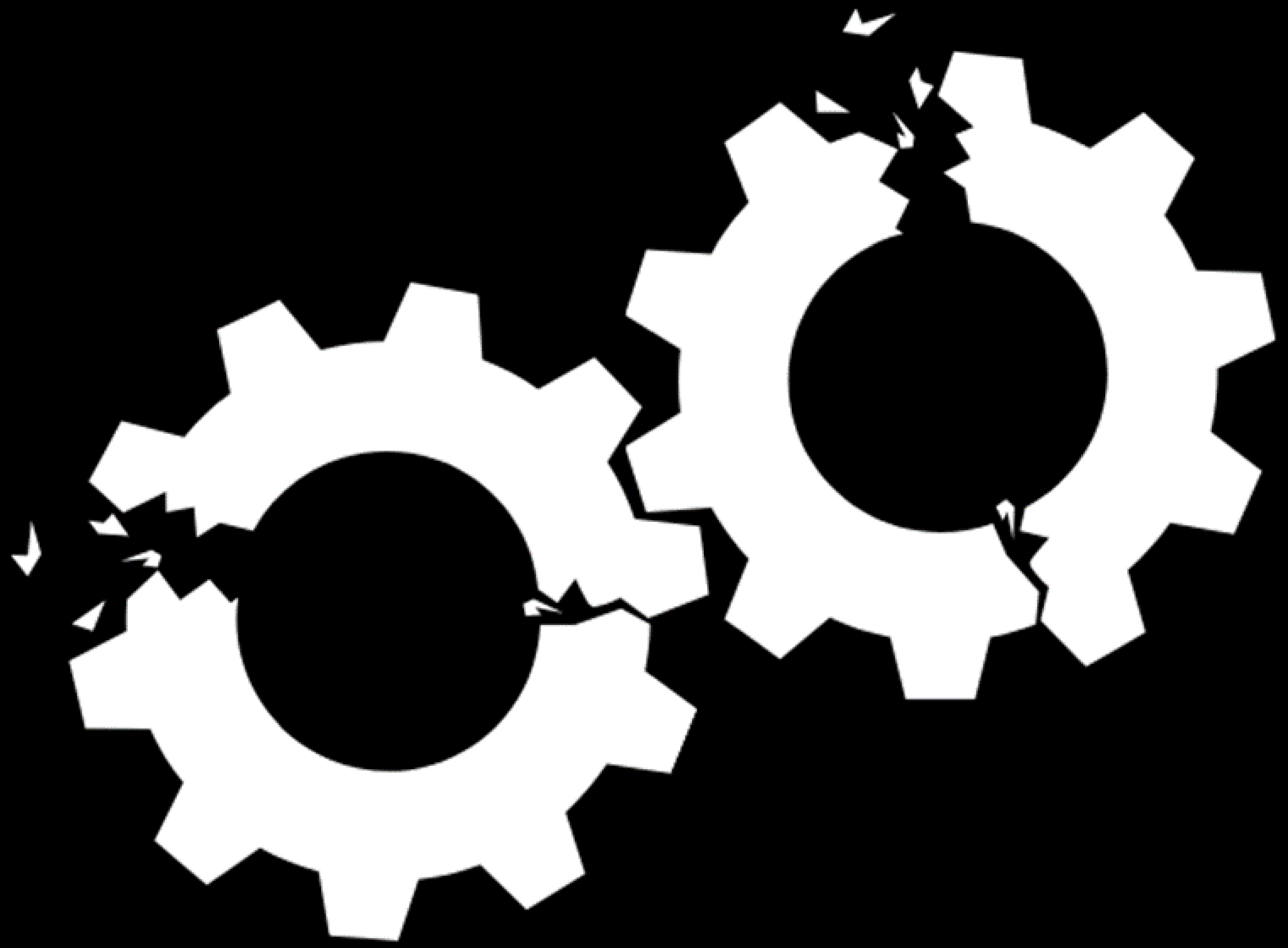
Why you should share your data

- Business Value
  - **Better insights**
  - **Better forecasts**
  - **Industry benchmarks**
- Compliance
- Altruism

Source: Bitkom Research 2024 — „Data Economy – Wo steht die deutsche Wirtschaft?“

Why is it difficult to share data?

- Legal objections
- Fear of misuse
- Competitive risks
- Data compatibility

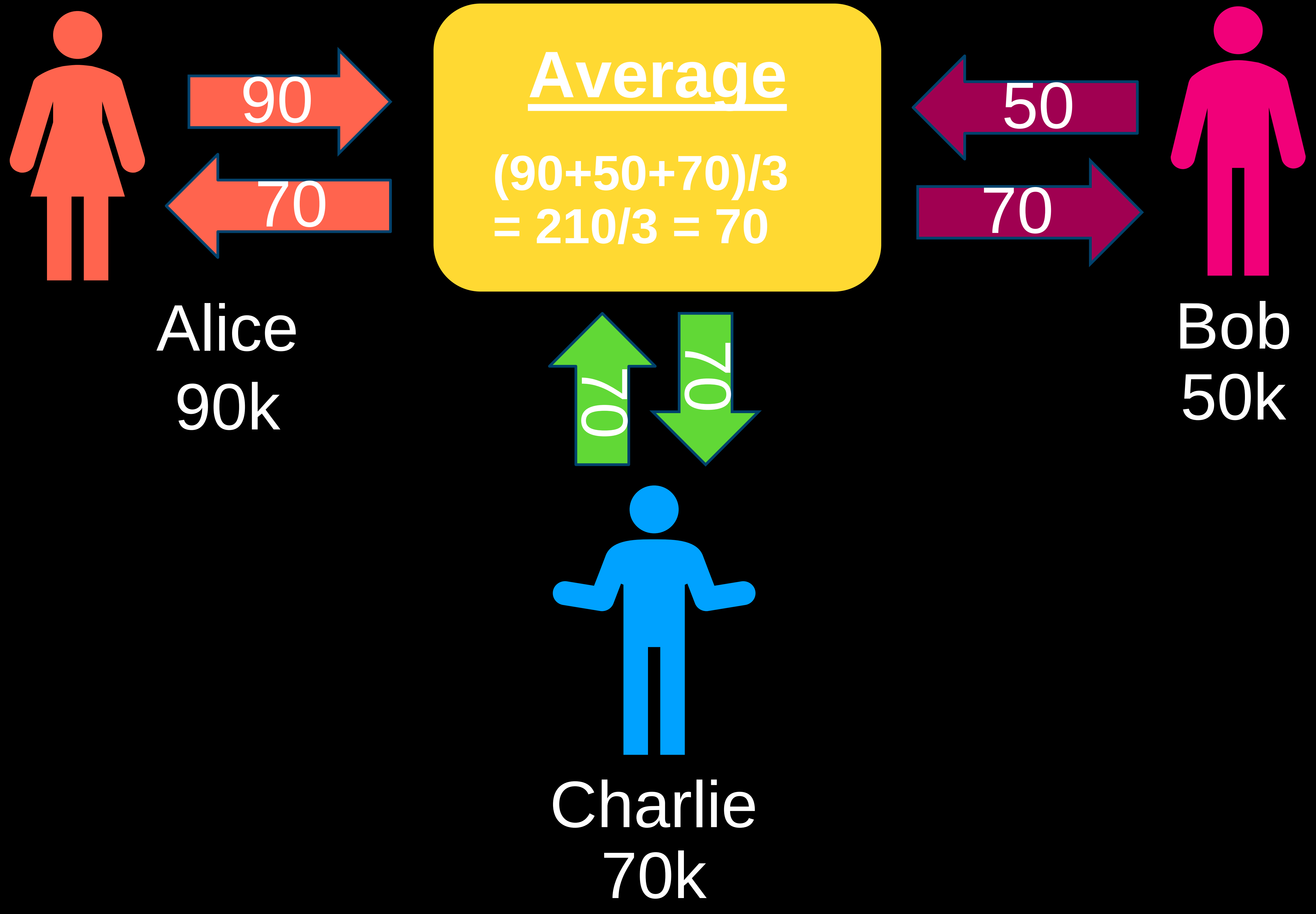


Is my salary adequate?

Dilemma:

- **Utility**: Many good reasons to ask this question
- **Privacy**: Difficult to answer, because we are reluctant to share the data

Example: Computing the Average Salary

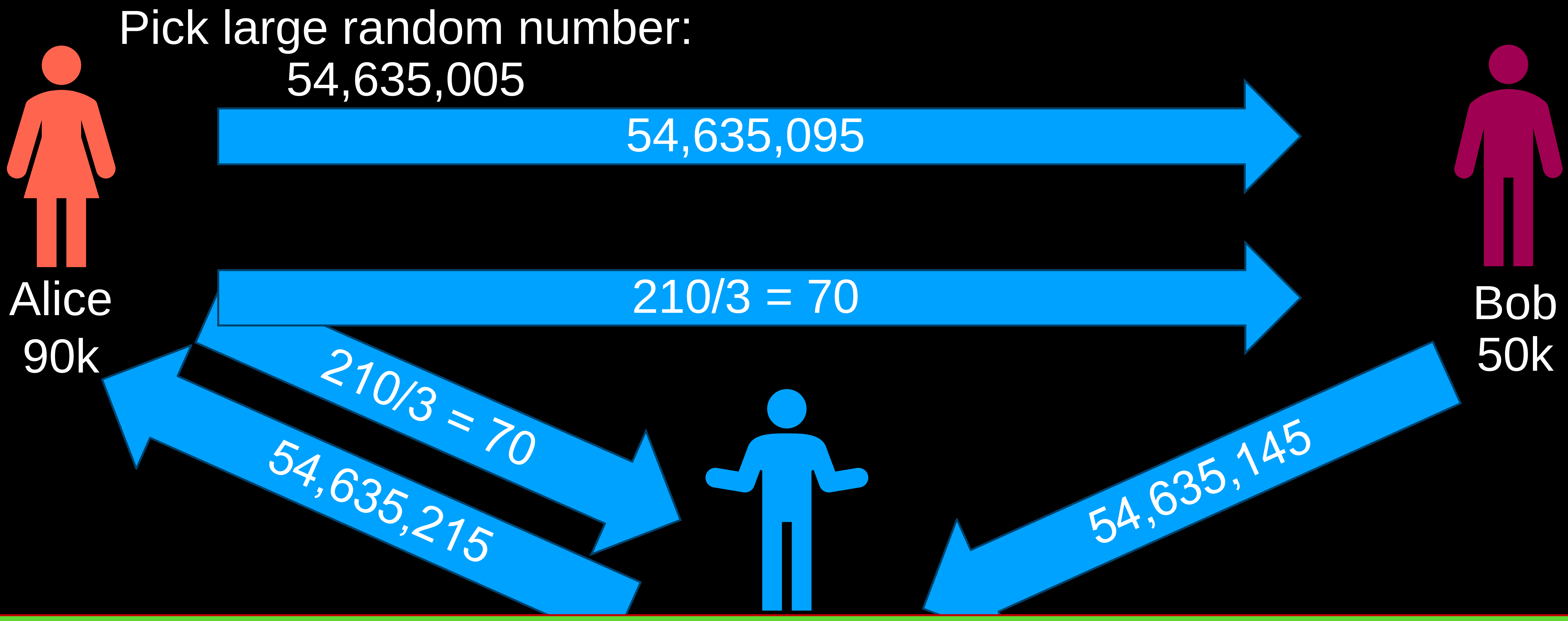


- **Trusted** third party
  (e.g., colleague, notary, …)
- **Trusted** hardware
  (e.g., Intel SGX)
- Use a **magic box**
  (***seems*** not to exist)

MINDSHARE

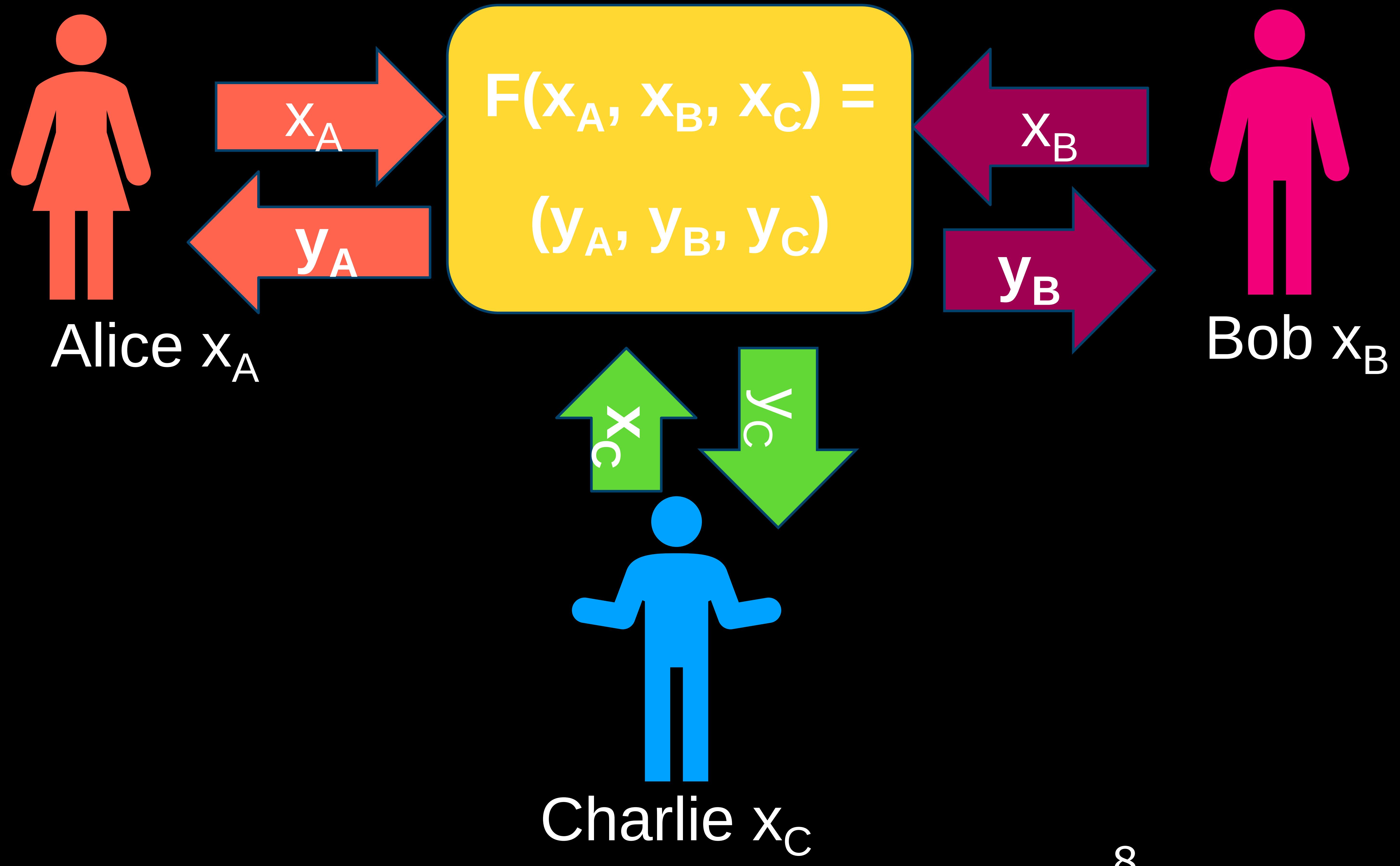
UTILACY

Computing the average salary, securely



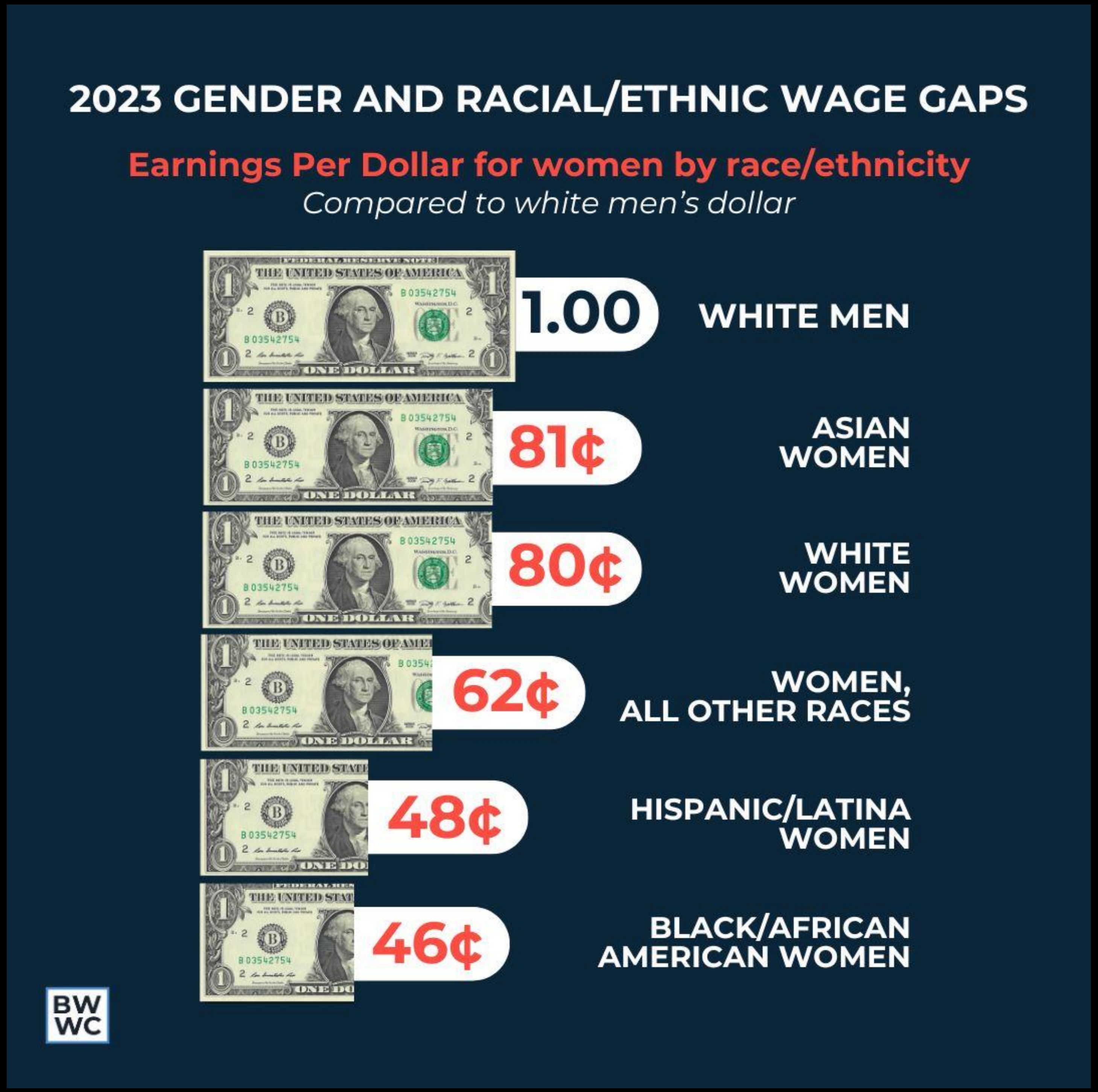
Possible to perform joint calculations with secret data, without disclosing it

Building “Magic Boxes” with Cryptography



- Protocol leaks **no information** beyond the desired result
- Mathematically guaranteed: **Cryptographic Zero Trust**

Application 1: Boston Women's Workforce Council



From: https://thebwwc.org

Goal: Eliminate gender and racial wage gaps in Greater Boston

- Employers are often unwilling to share payroll data due to **privacy concerns**
- Traditional analysis methods rely on **self-reported, incomplete, or biased data**
- **MPC** enables comparison without disclosing individual or company-level details

Application 2: Mozilla's Privacy-Preserving Attribution (PPA)

Ethical Ad Attribution Without Surveillance

- **Organizations:**
  Mozilla (Firefox),
  ISRG (DAP operator),
  Meta (collaborator)

> *"Digital advertising is not going away,*
>
> *but the surveillance parts could [..]"*
> — Mozilla CTO

From: https://www.reddit.com/r/firefox/comments/1e43w7v

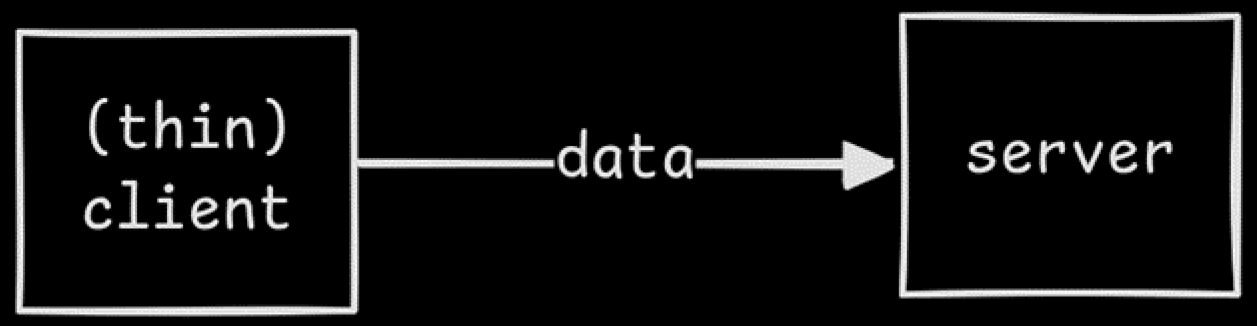
- **Motivation:** Replace **invasive cross-site tracking** with **default-private mechanisms**

- **Prototype:** Enabled experimentally in **Firefox 128** for a limited number of test sites

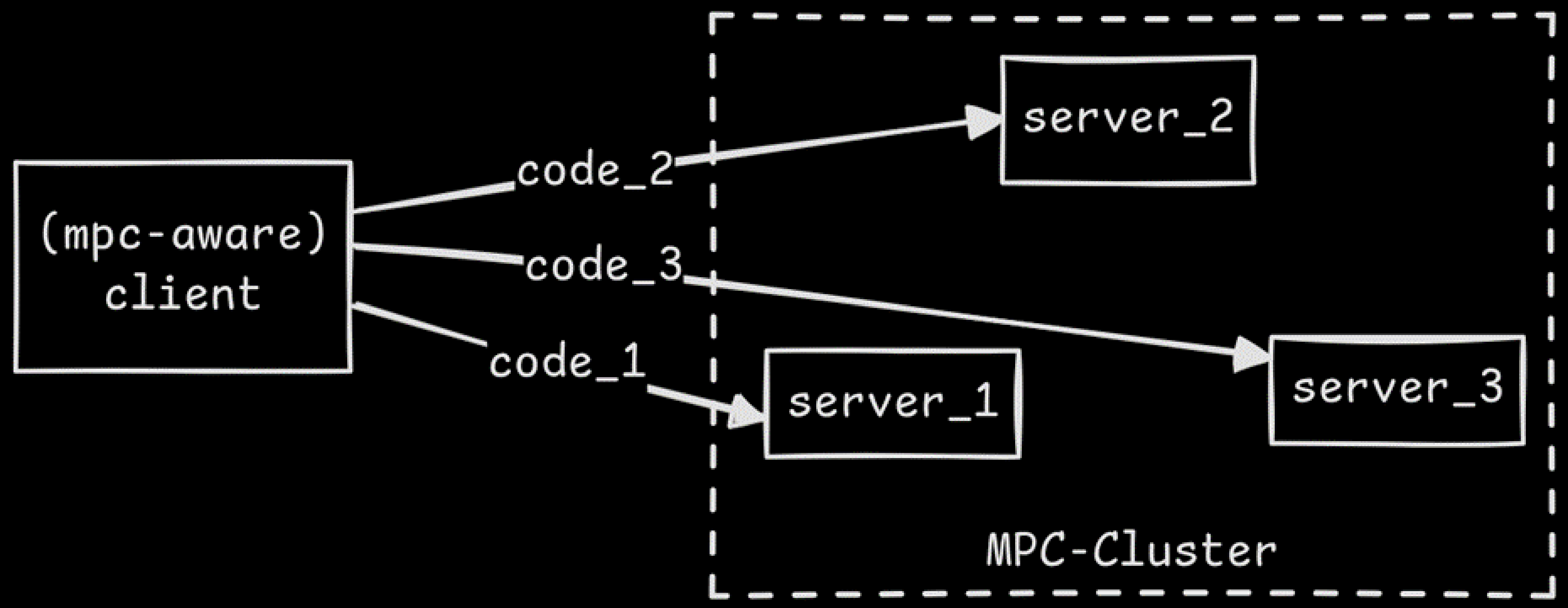
The Catch: MPC Is a Leaky Abstraction

Why adoption is hard in practice

- Data must be transformed **before** it enters the protocol
- Every data source (and data sink) **must be MPC-aware**
- **Not backwards-compatible** with existing systems
- Changes must happen at the edges

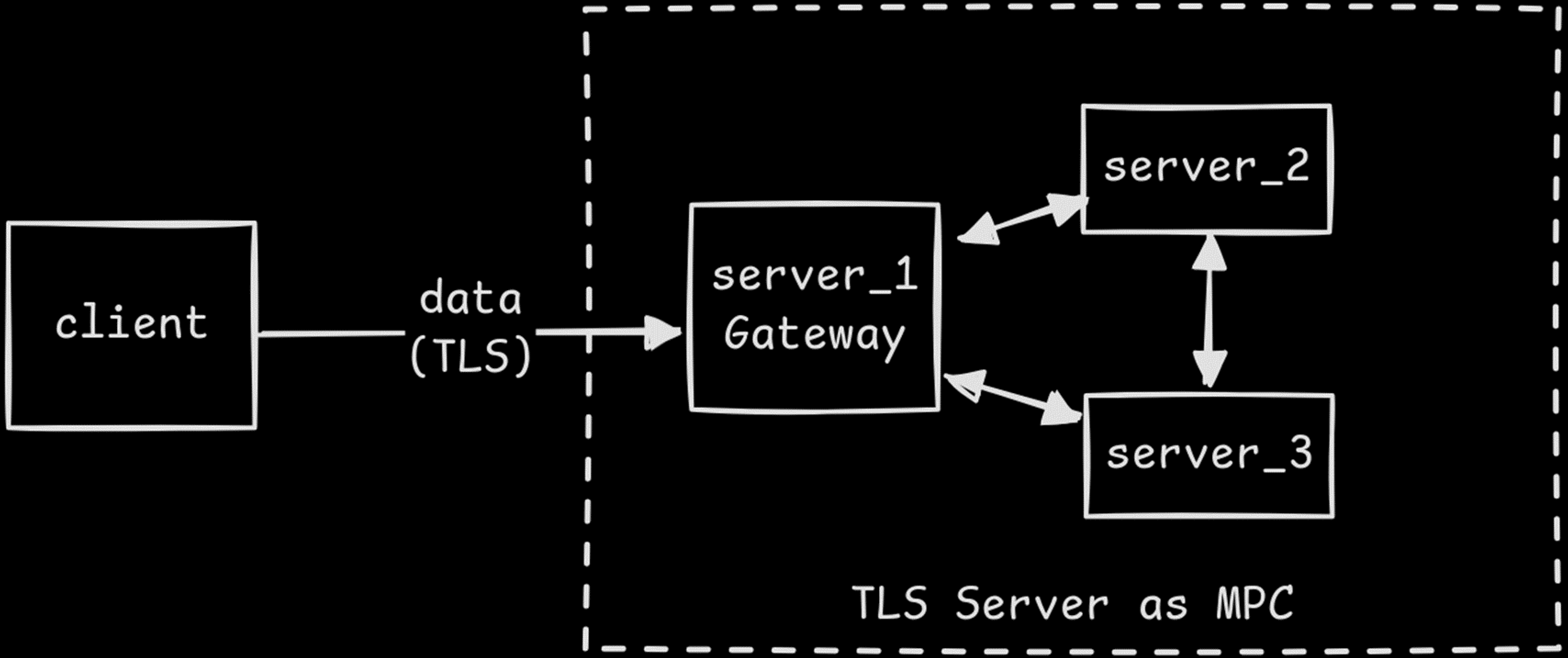


Traditional Systems



System with MPC

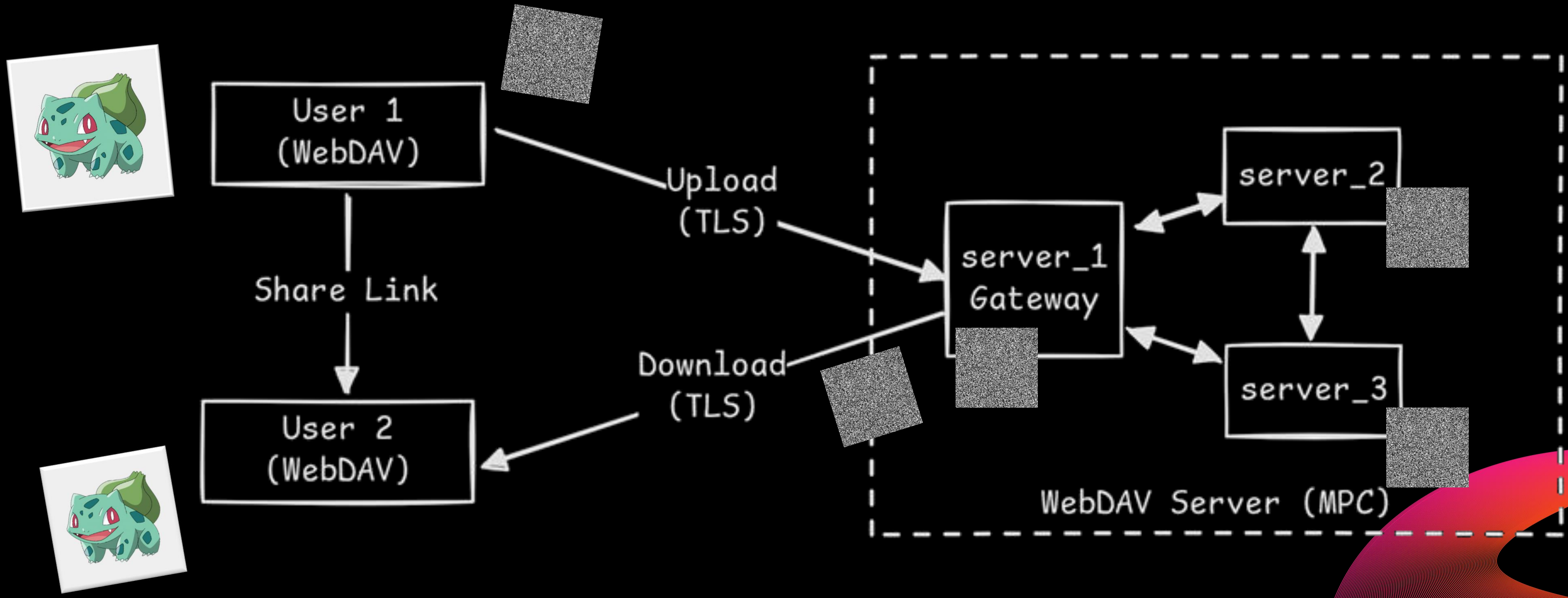
Oblivious TLS*: Smuggling MPC into the Internet



* https://eprint.iacr.org/2021/318.pdf,
Work by: Damiano Abram, Ivan Damgård, Peter Scholl, and Sven Trieflinger

UTiLACY

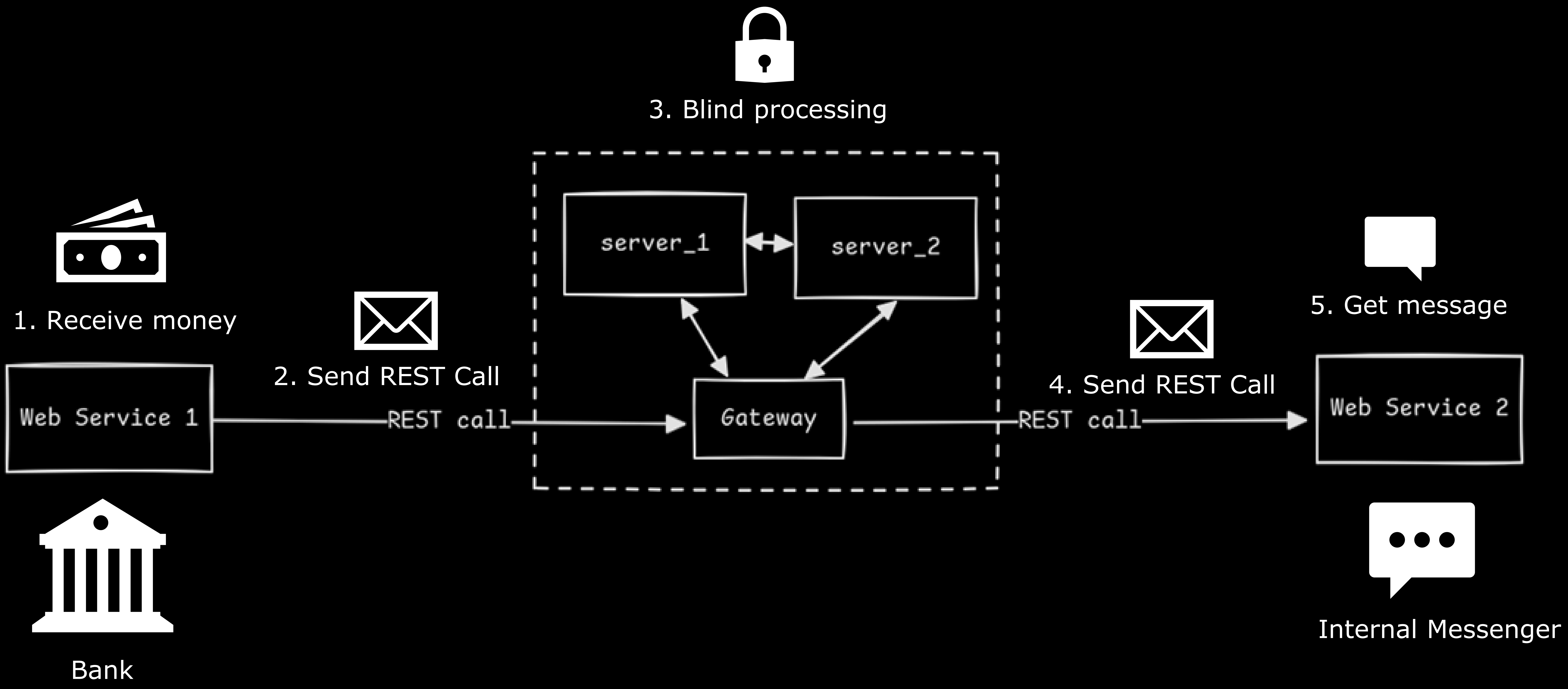
Application 3: Secure Cloud Storage, With No Trusted Server



Application 3: Secure Cloud Storage, With No Trusted Server

- Leverages existing **WebDAV protocol** and **TLS infrastructure**
- Client uses standard tools: **no changes required**
- Data is stored encrypted: **no server ever sees the original**
- Enables **private sharing** with others via standard clients
- Backwards compatible **end-to-end encryption**

Application 4: Privately combining REST-APIs



Takeaways

UTiLACY

- **MPC** lets us compute without revealing our data
- **Oblivious TLS** bridges modern cryptography with existing infrastructure
- We can upgrade privacy without changing clients or **breaking compatibility**
- **What utilacy does:**
  - we build MPC applications and interfaces
  - we see huge potentials with OTLS and are building implementations
  - we can do it better than state-of-the-art: Ready for real world usage

Thank you

Dr. David Niehues

niehues@utilacy.de

www.utilacy.de

UTILACY

utilize secret data

Keep Your Data Sovereignty!

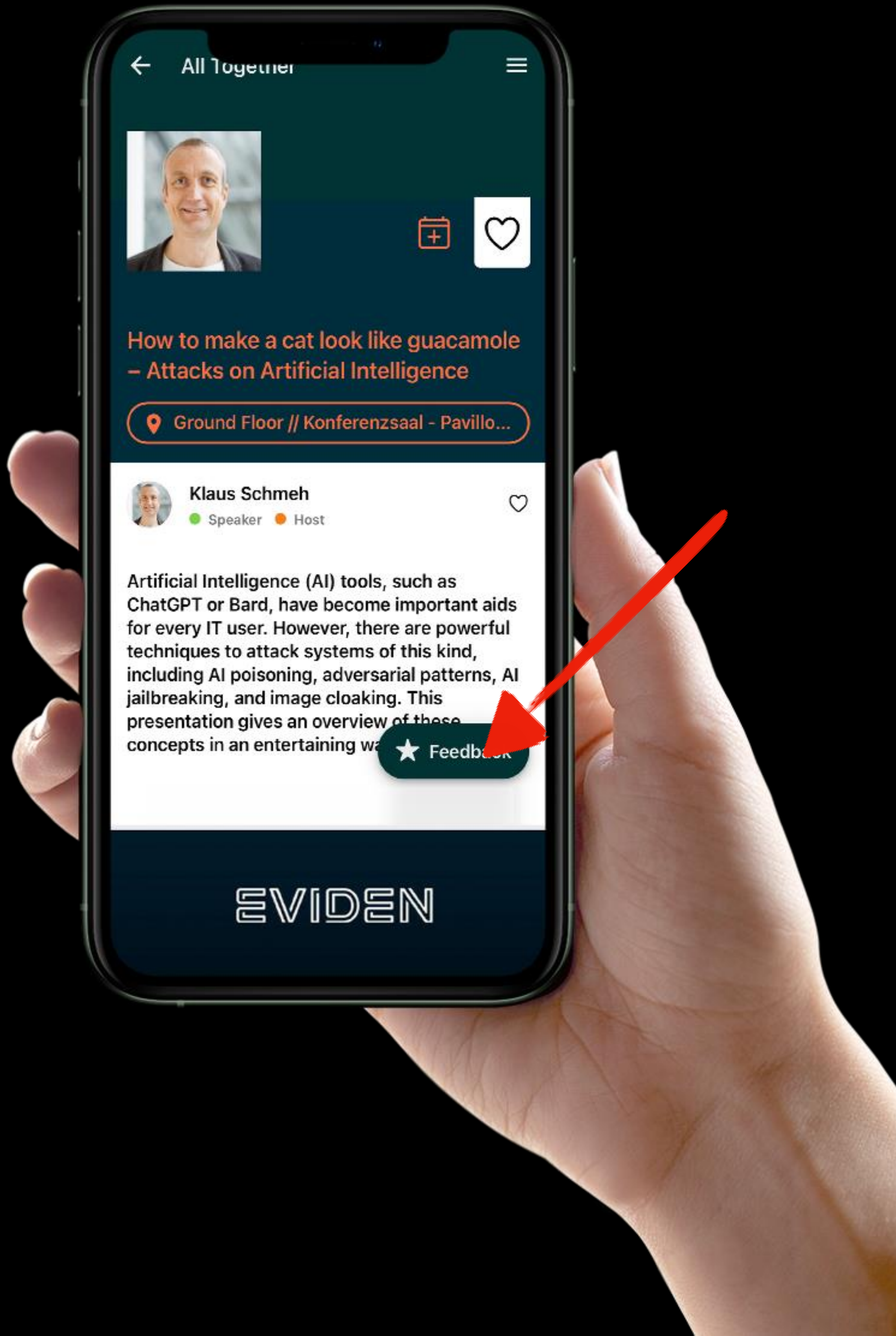
MINDSHARE

2025 10–11 SEP

CYBERSECURITY
LEADERSHIP FORUM

Securing
Identity for
our Digital
Future

TAKE A MINUTE AND GIVE US FEEDBACK



How to make a cat look like guacamole – Attacks on Artificial Intelligence

Ground Floor // Konferenzsaal - Pavillo...

Klaus Schmeh

● Speaker ● Host

Artificial Intelligence (AI) tools, such as ChatGPT or Bard, have become important aids for every IT user. However, there are powerful techniques to attack systems of this kind, including AI poisoning, adversarial patterns, AI jailbreaking, and image cloaking. This presentation gives an overview of these concepts in an entertaining wa