

DOWNLOAD & USE **THE GOTO GUIDE APP**

DOWNLOAD THE APP
CREATE YOUR SCHEDULE
ASK QUESTIONS
RATE SESSIONS



Encrypted Computation

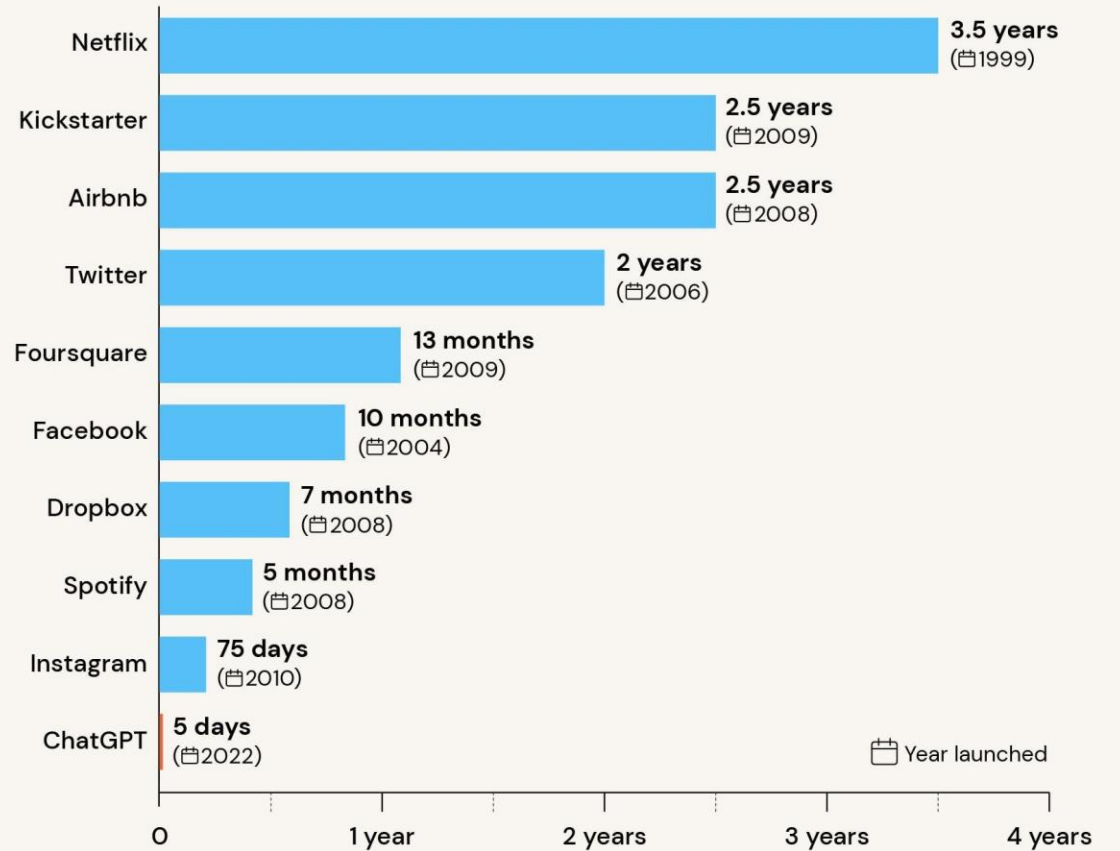
What if decryption wasn't needed?

Katharine Jarmul - Probably Private

AI is really popular!

CHATGPT STATISTICS

Time to reach 1 million users



But it can also be creepy...



r/privacy • vor 1 Jahr



How can I stop my phone from listening to me?

question

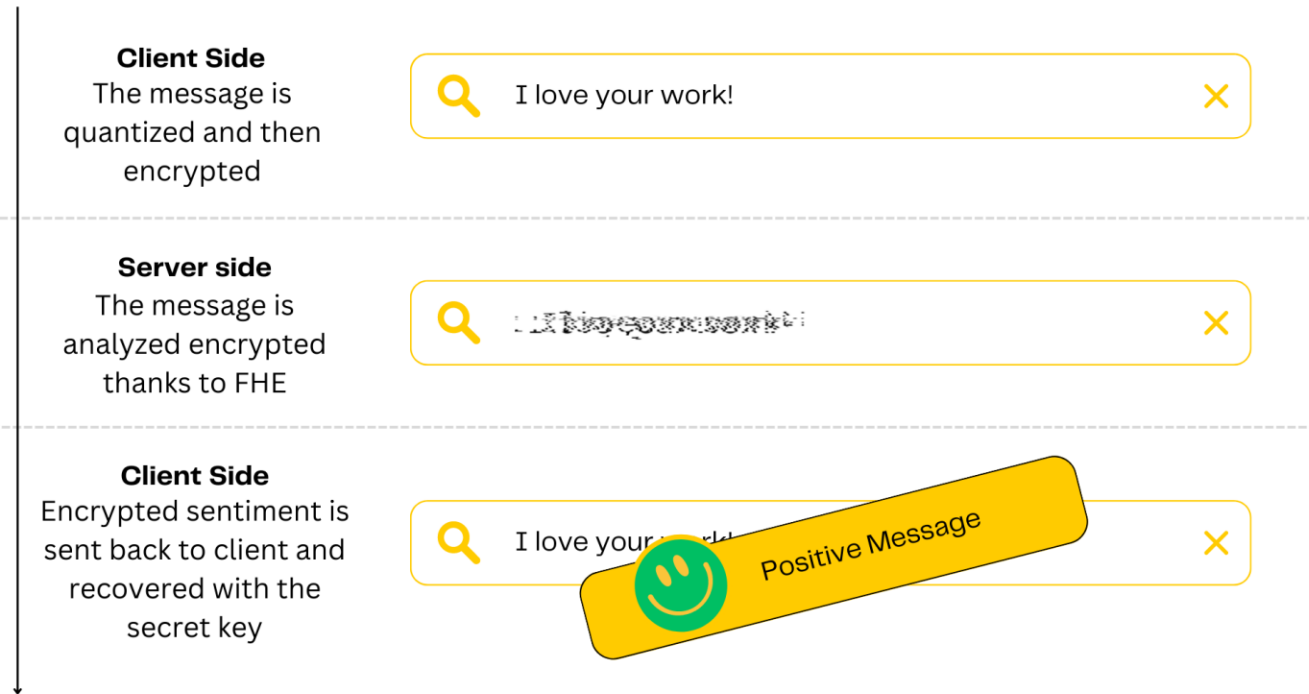
I've been getting targeted ads of things I've been saying. I was talking about Birds with Arms, and then suddenly they appear in my pinterest feed

ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned

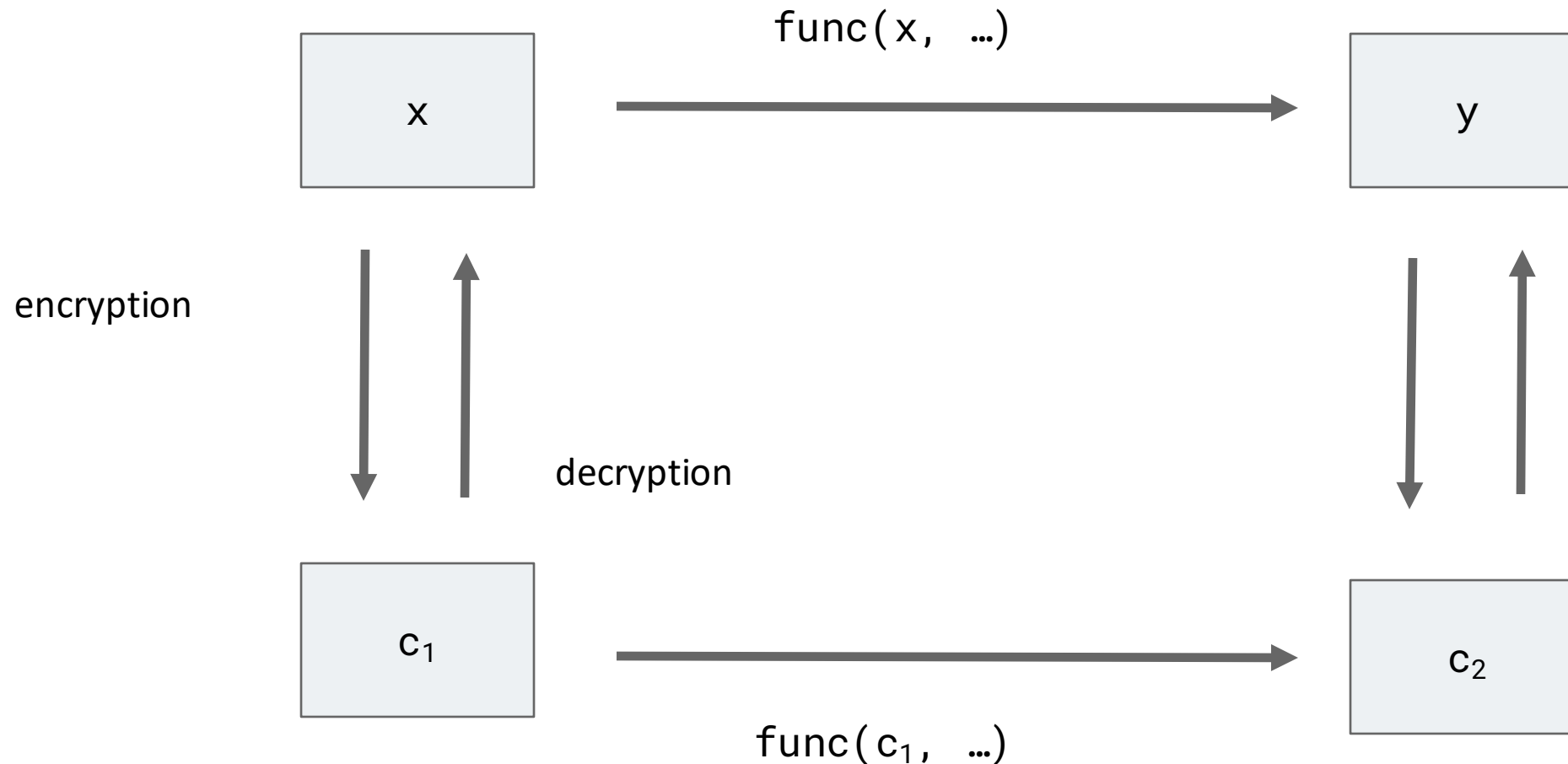
Published: February 8, 2023 2.06am CET Updated: February 10, 2023 5.30am CET

What if...?

Hugging Face + Zama's Concrete Library



Homomorphic Encryption - Commutativity



Pallier Cryptosystem

$$\mathcal{E}(m) = g^m r^n \bmod n^2$$

Encrypt

Message (plaintext)

Finite group base

Randomness

Modulus (large prime, divides the order of g)

Pallier Homomorphisms

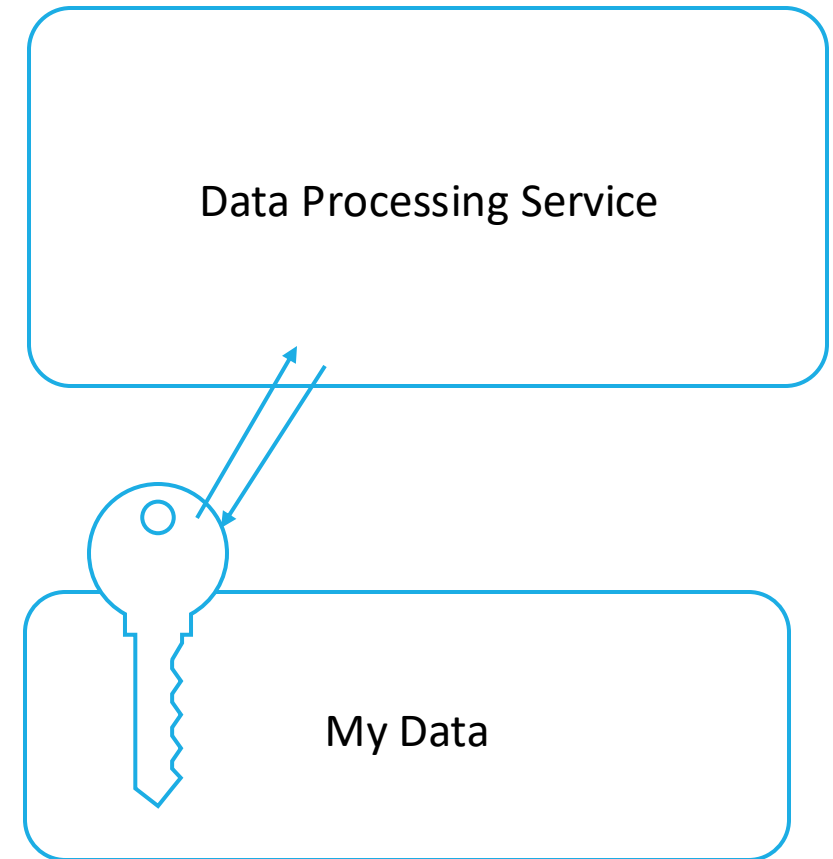
$$\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) = (g^{m_1} r_1^n)(g^{m_2} r_2^n) \bmod n^2$$

Let's try it out!!

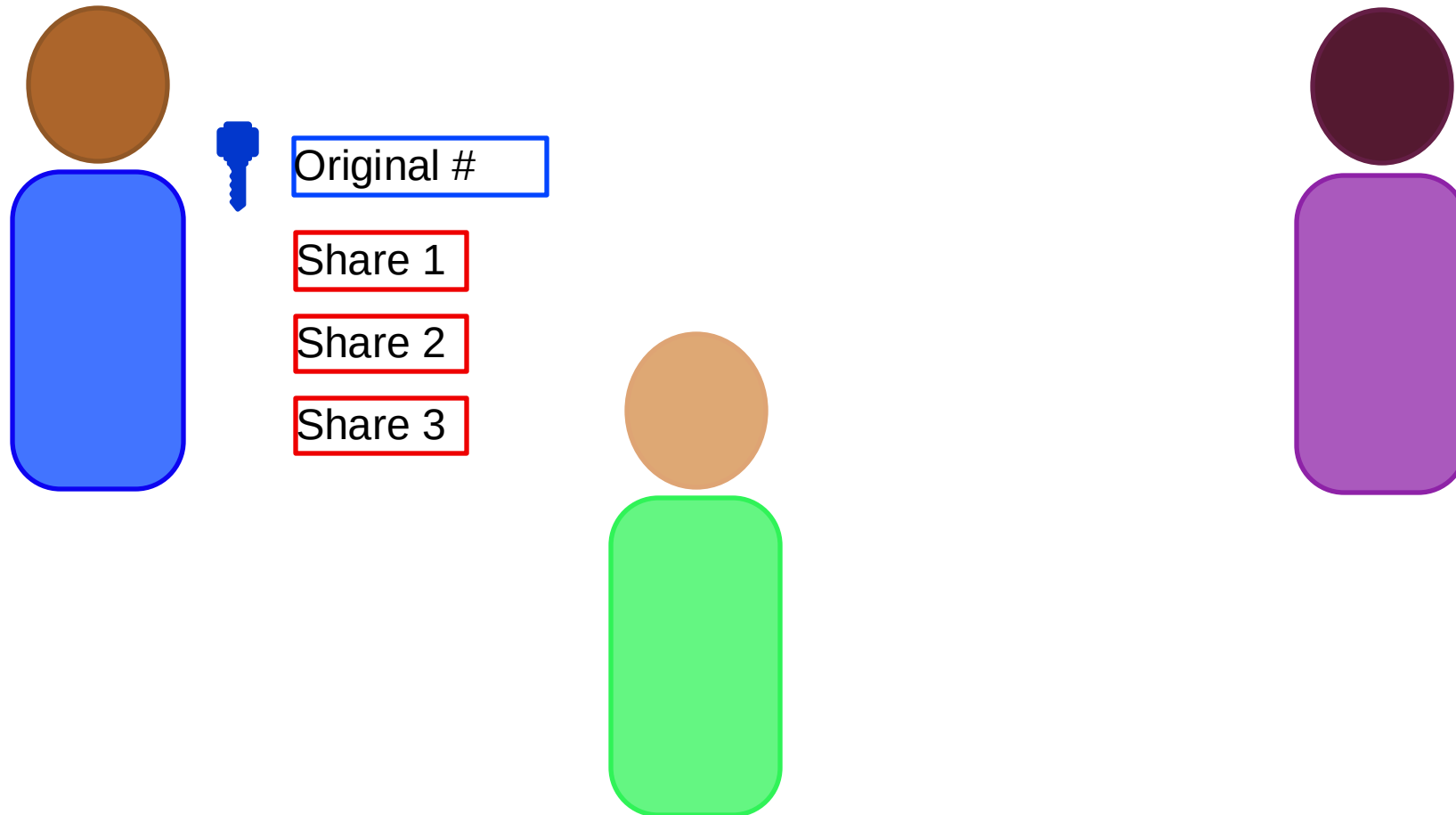
$$\bmod n^2$$
$$= \mathcal{E}(m_1 + m_2).$$

Homomorphic Encryption: Recap

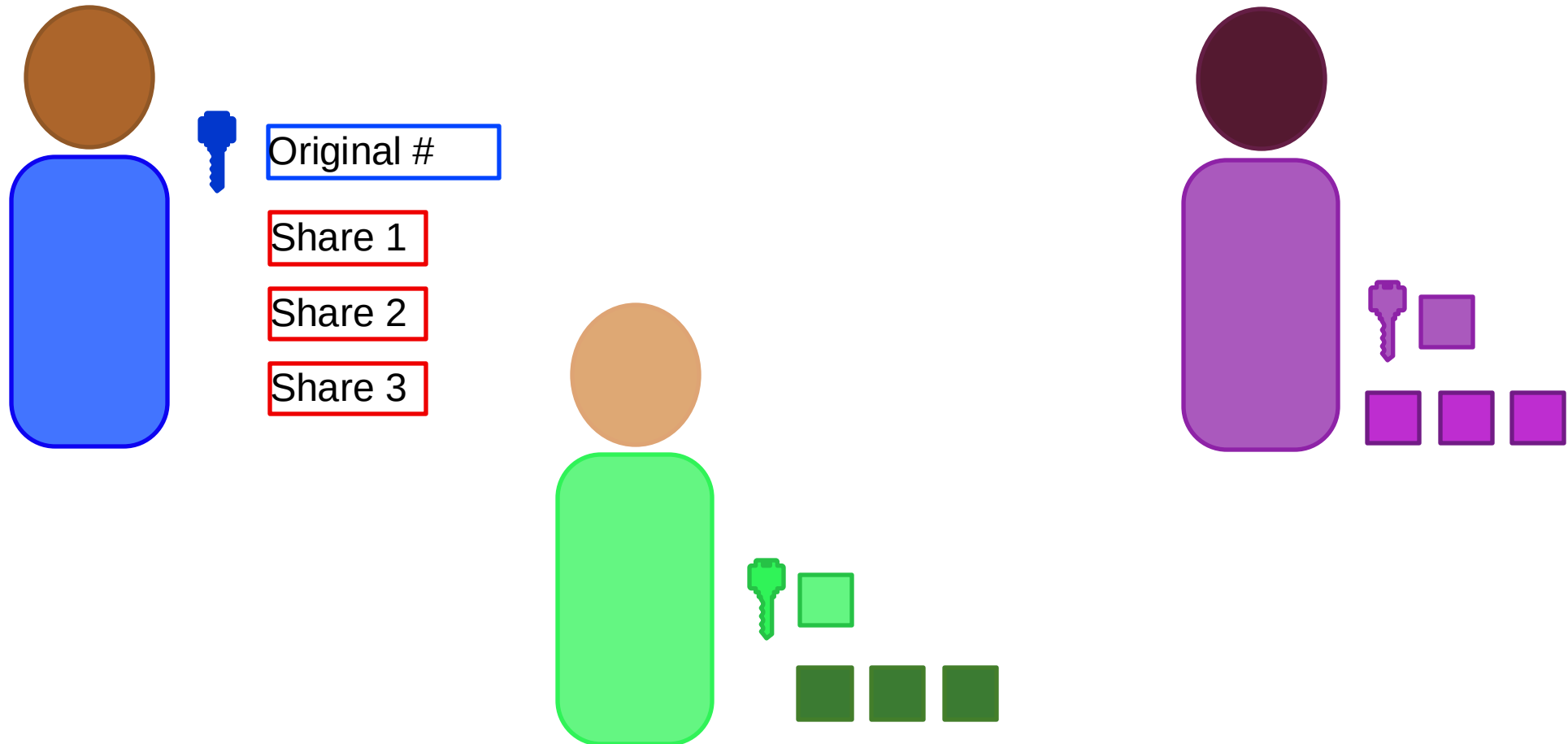
- Based on cryptoscheme/-system with homomorphisms
- Great for use cases where data owner and data processor are different
- Large computations are expensive and may require specialized hardware
- Acceleration possible with accuracy tradeoffs for some protocols



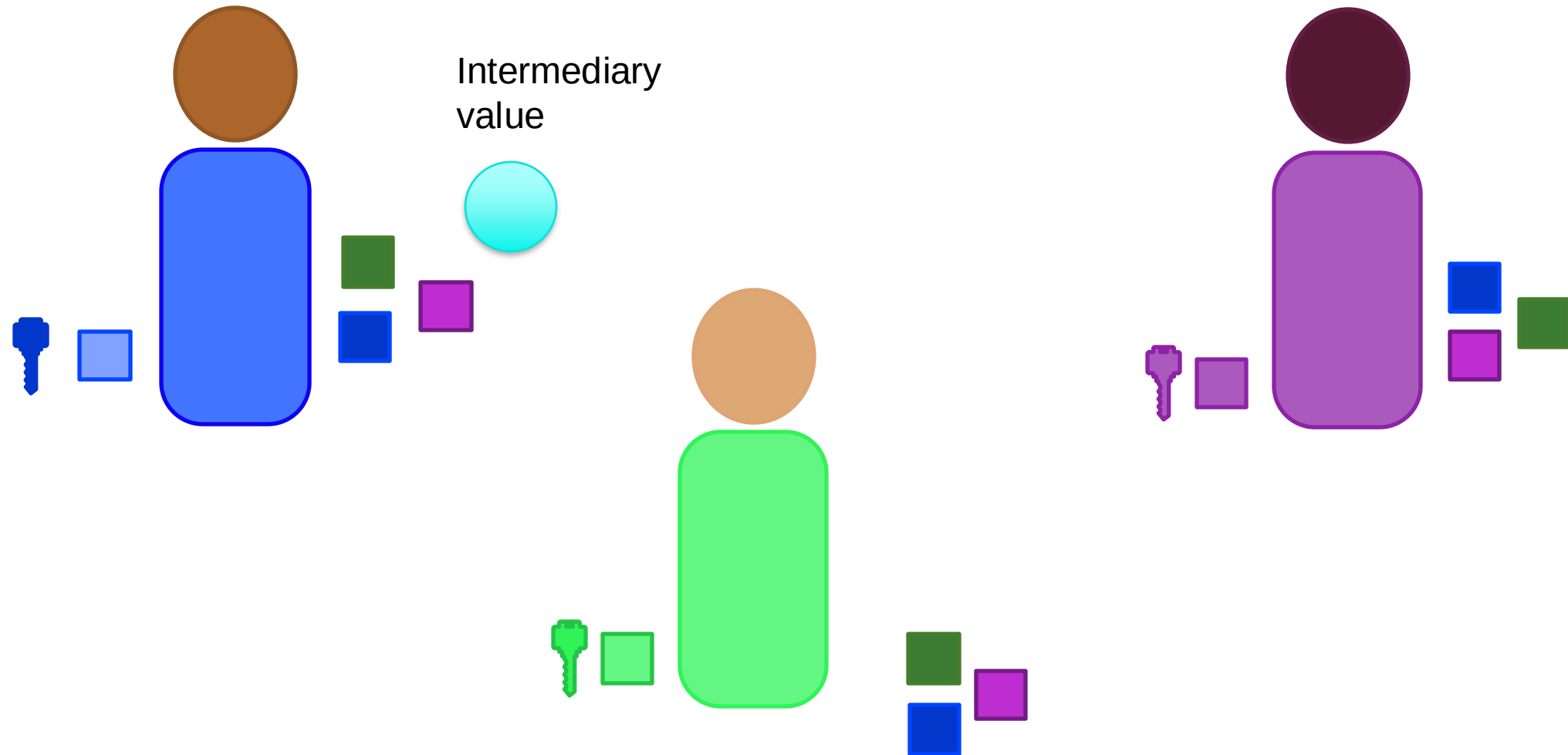
Multi-Party Computation (MPC)



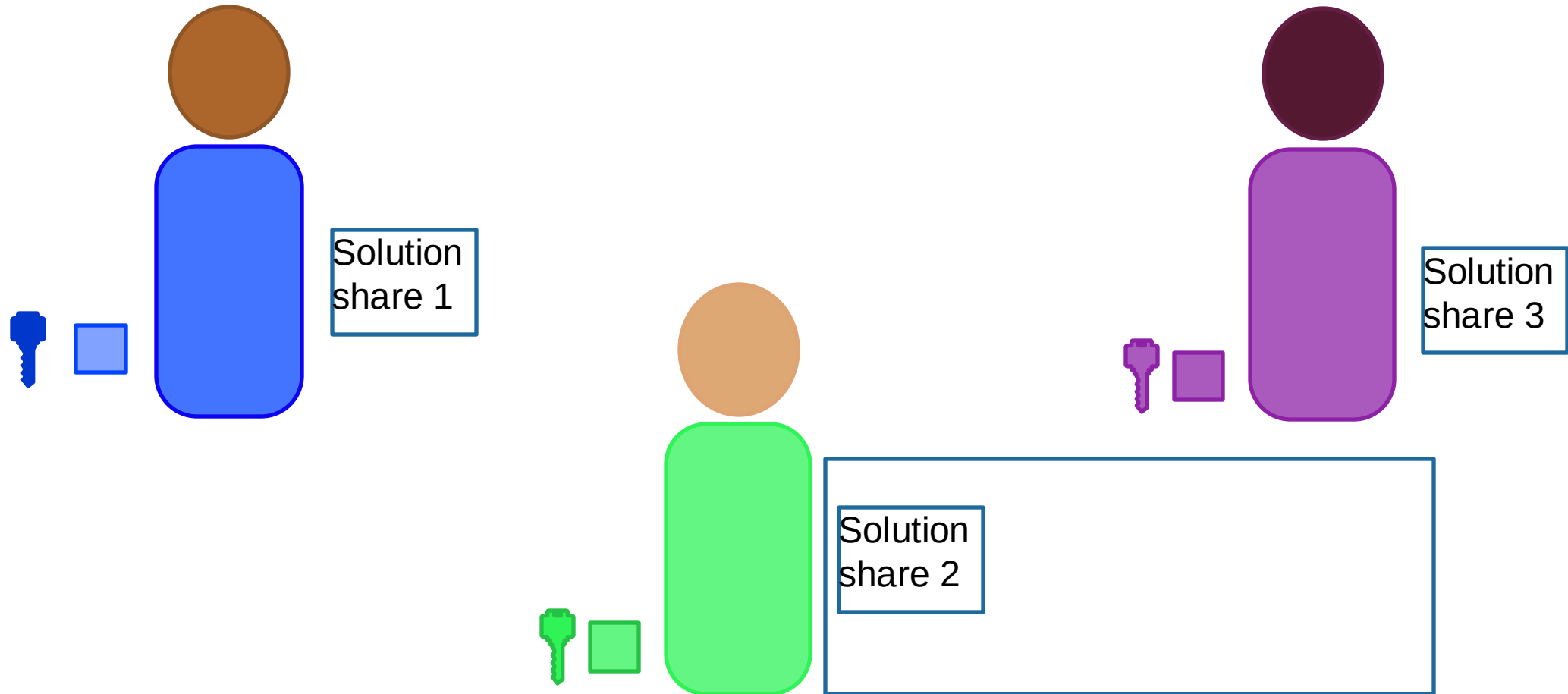
Multi-Party Computation (MPC)



Multi-Party Computation (MPC)



Multi-Party Computation (MPC)



Example Machine Learning Use Case

E-Commerce
Operator

Brick and
Mortar Store

Combined Model for Seasonality
and Popularity



tensorflow-encrypted
moose

Use Cases for Encrypted Computation

Example	Encryption Protocol and/or System
Private and secret auction	Multi-party computation with participation threshold
Private inference (prediction on encrypted data)	Homomorphic Encryption and encrypted machine learning
Private query or lookup	Private Information Retrieval (usually HE based)
Customer Comparisons / Analytics	Private Set Intersection (PSI) and Multi-Party Computation

Getting Started with Encrypted Computation



swift-homomorphic-encryption Public

Supported iOS functionality



zama-ai / concrete

numpy / matrix operations with FHE



kjam / practical-data-privacy

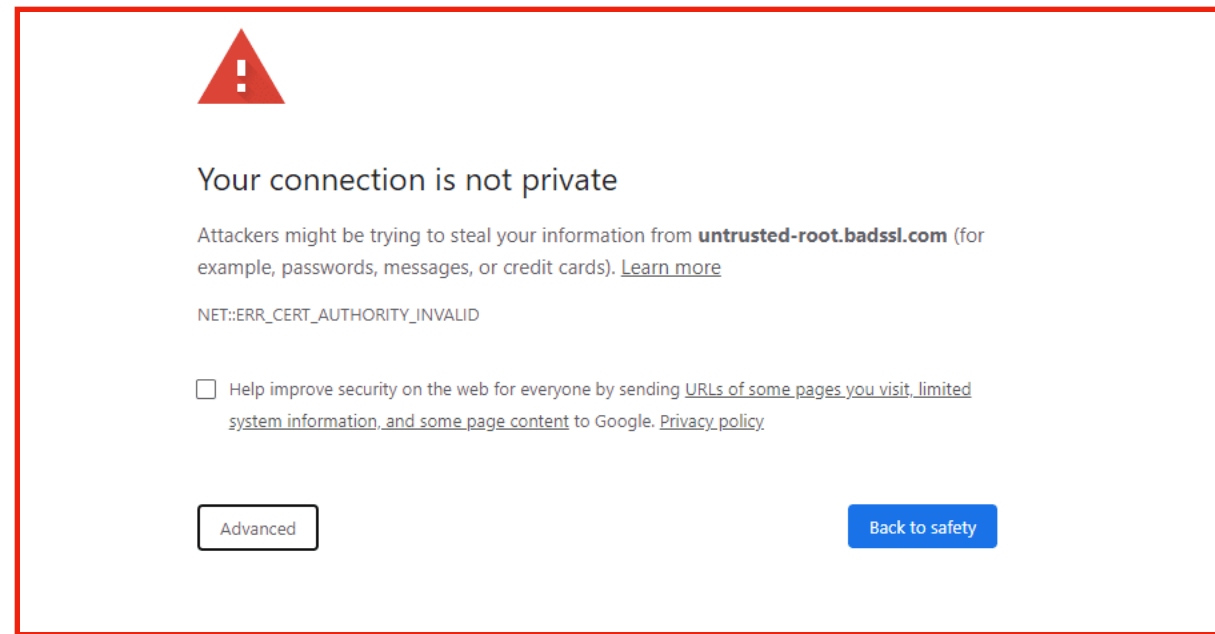
introductory notebooks (also on other privacy technology)



carbynestack Public

platform for MPC by Bosch

User control and understanding builds trust

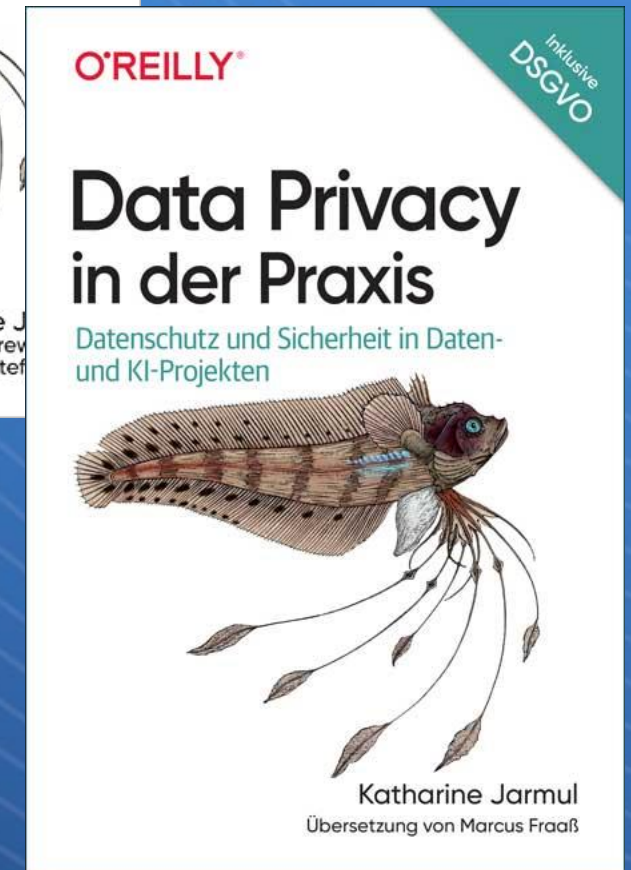
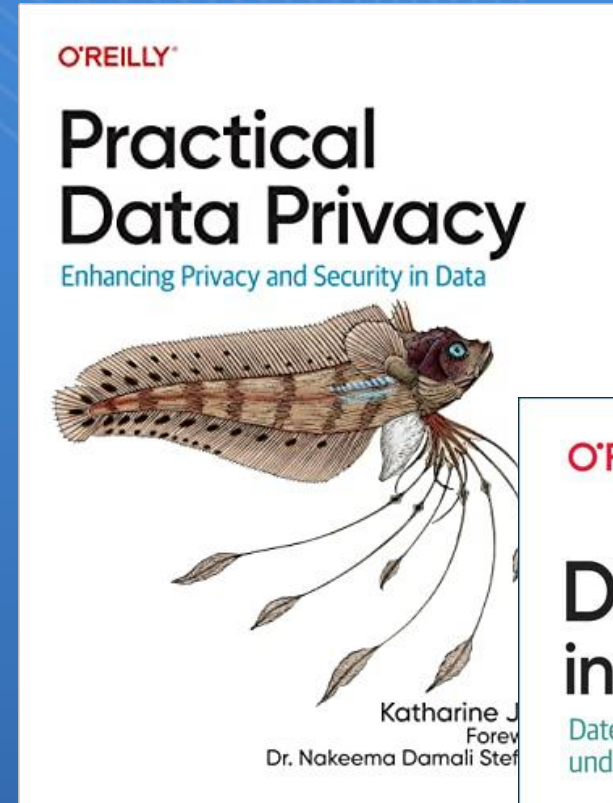


Thank you!

Questions or comments?

Later: katharine @
probablyprivate.com

Newsletter there too :)



**Rate this session
in the GOTO Guide app**
and claim your reward