university of groningen

INFORMATION SYSTEMS GROUP
ENABLING FLEXIBILITY

Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

Funded by the European Union

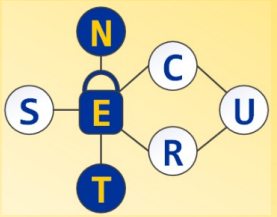
Don't Trust Your PETs, Verify Them

Zero-Knowledge Proofs for Verifiable Privacy-Preserving Computations

Tariq Bontekoe

Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

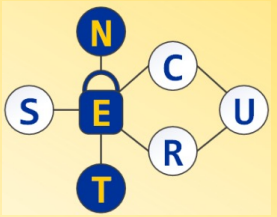
Brief Introduction



- PhD student @ University of Groningen, Information Systems Group
  - Verifiable, Privacy-Preserving Computations
  - 1st Promotor: Dimka Karastoyanova
  - 2nd Promotor/Supervisor: Hassan Jameel Asghar (Macquarie University – Australia)
- Currently @ Secondment
  - 3rd week (out of 3 months)
  - Cybernetica (Tartu, Estonia)
  - Enriching MPC with ZKP

- Email: t.h.bontekoe@rug.nl
- Webpage: https://www.rug.nl/staff/t.h.bontekoe

What are PETs?

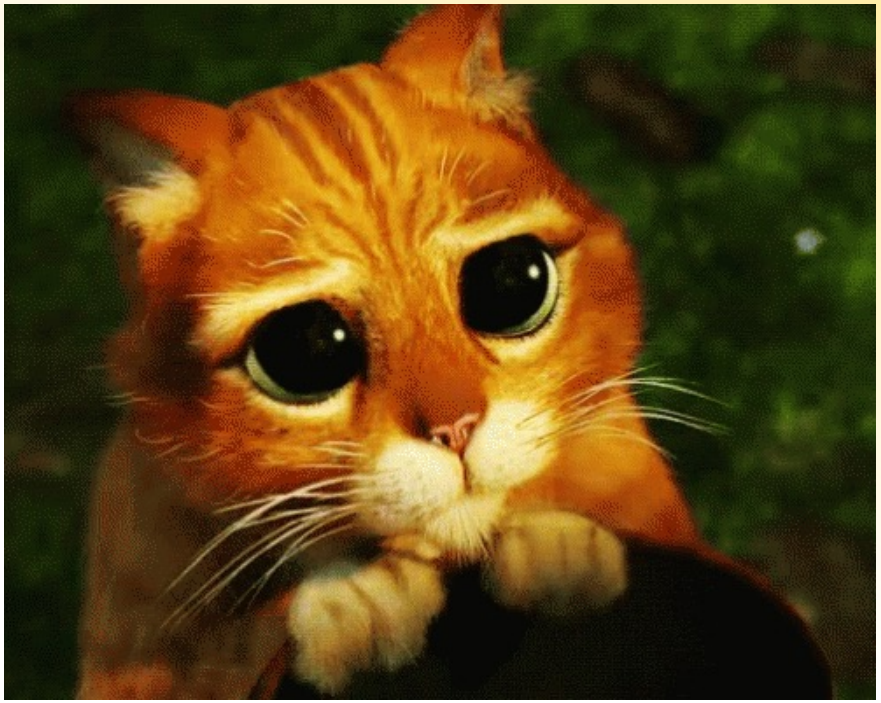


- Computing on Sensitive Data
  - Privacy Regulations
  - Business Sensitive
- Can we…
  - compute on this data, …
  - without revealing it?
- In a distributed setting, …
  - without sharing data?

- Yes, with Privacy-Enhancing Technologies (PETs)
  - One or Multiple Parties
  - Computation
    - *ML/Statistical model*
    - *Mortgage application*
    - *Genomic data*
    - *….*
- In short, PETs are awesome!

But, before diving in…

- So, PETs are great!
- Provable privacy guarantees
- Many kinds
  - Differential Privacy
  - Secure Multi-Party Computation
  - Homomorphic Encryption
  - …
- What's not to like?

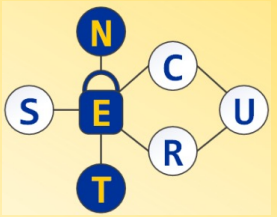


Use PETs responsibly

- Security Model
  - Honest-but-curious vs. active
- Assumptions
  - Input correctness
- External validation
  - Public verifiability

- PETs are still great! Just don’t use them blindly ☺
  - *Actually: Trust PETs, verify the people using them!*

Verifiable Privacy-Preserving Computations

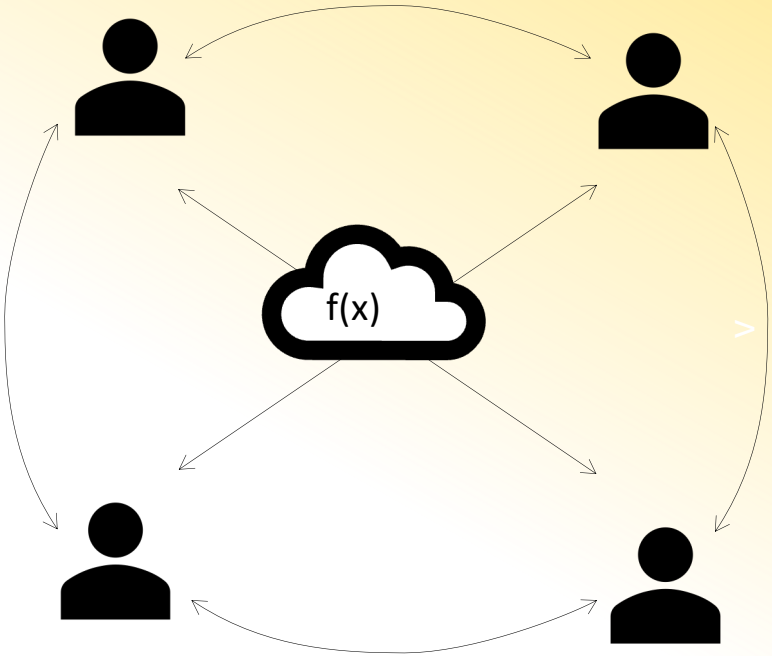


- My PhD so far…
- …PET + ZKP (privacy-enhancing technology + zero-knowledge proof)
  - Survey Verifiable, Privacy-Preserving Computation on Distributed Data
  - ZKPs for Differential Privacy (DP) Differential Verifiable Differential Privacy in the Shuffle Model
  - ZKPs for Federated Learning (FL) Modular Zero-Knowledge Proofs of Training in the Federated Setting
  - Multi-Party Computation (MPC) for ZKPs Collaborative, Commit-and-Prove NIZKs
  - ZKPs with MPC Proving the Value of Additional Data

- Currently @ Secondment
  - Enriching MPC with ZKPs

Multi-Party Computation

- Interactive
  - n parties
- Arithmetic secret sharing (boolean sharing, garbled circuits)
  - $x = x_1 + \cdots + x_n \pmod{p}$
  - 'Free': addition, addition/multiplication with public value
  - Interactive protocol for multiplication
- Semi-honest security
  - E.g., Cybernetica's Sharemind
  - Clients follow protocol
  - Efficient
- Active security
  - Clients may deviate arbitrarily from protocol
  - Costly



Zero-Knowledge proofs

- ZKP
- Prove correctness of statement and nothing more
- Example

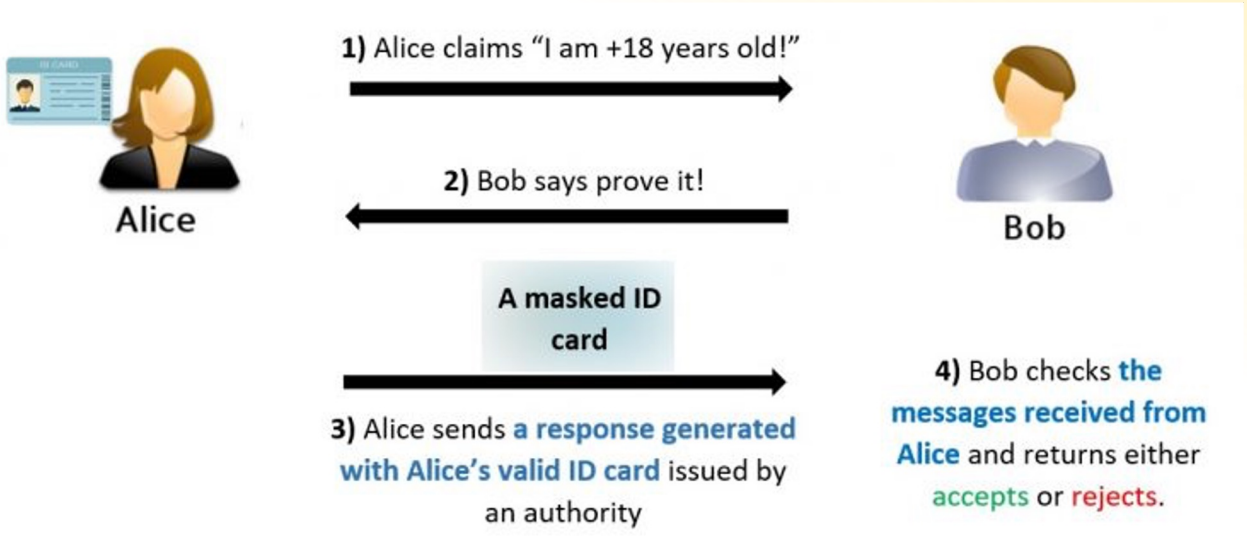
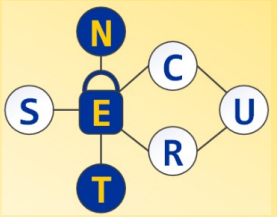


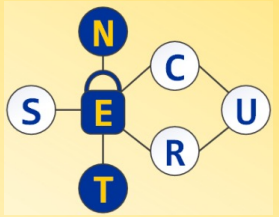
Image source: https://www.esat.kuleuven.be/cosic/blog/co6gc-introduction-to-zero-knowledge-proc

ZKP + actively secure MPC: A perfect match?



- Advantages
  - Move local computations to ZKP
    - *Improved efficiency/communication*
    - *Compute offline*
    - *Re-usable*
  - Input validation/authentication
  - Combining MPC over different fields?
- Main difficulty
  - ZKPs and MPC expect data in different fields/rings

Constructing a Match-Maker

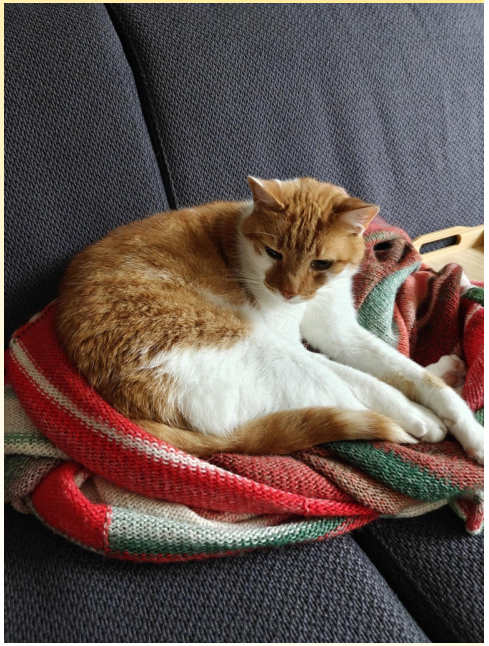


- Given
  - ZKP based on Pedersen Commitments
    - (Elliptic curve) group $\mathbb{G}$ of prime order p; 2 generators $G, H \in \mathbb{G}$
    - Data $x_p \in \mathbb{F}_p$, randomness $r \in \mathbb{F}_p$
    - Commitment $x_p G + rH$
  - Arithmetic secret sharing based MPC
    - *Prime field $\mathbb{F}_q$, q is not secure for Pedersen Commitments*
    - *Data $x_q \in \mathbb{F}_q$, Secret shares $x_1 \in \mathbb{F}_q$, $x_2 \in \mathbb{F}_q$, such that $x_1 + x_2 \equiv_q x_q$*
- So far: ZKP to show $x_p = x_q$ in $\mathbb{Z}$
- To be done
  - Vector commitments
  - More than 2 parties
  - MPC over rings i/o fields
  - (combining MPC over different fields, ZKPs with different commitments, …)

$\mathbb{Z}$:= all integers: $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{G}$:= 'Set' of values of size (order) p
Generator $G \in \mathbb{G}$: $\mathbb{G} = \{0G, 1G, 2G, \dots, (p-1)G\}$
$\mathbb{F}_p$:= integers modulo p: $\{0, \dots, p-1\}$

PETs are great!

- Verification makes them even better!
- More than just verifying the computation
  - Correctness of Input Data
  - External/Public Verifiability
- Comes at a cost
  - General solutions are great, but …
  - … costly for real-world problems
  - Think before you apply:
    - *Modularity*
    - *Different technologies, different trade-offs*



My cat (looks cute, not to be trusted…)

Thank you for listening!

Questions?!