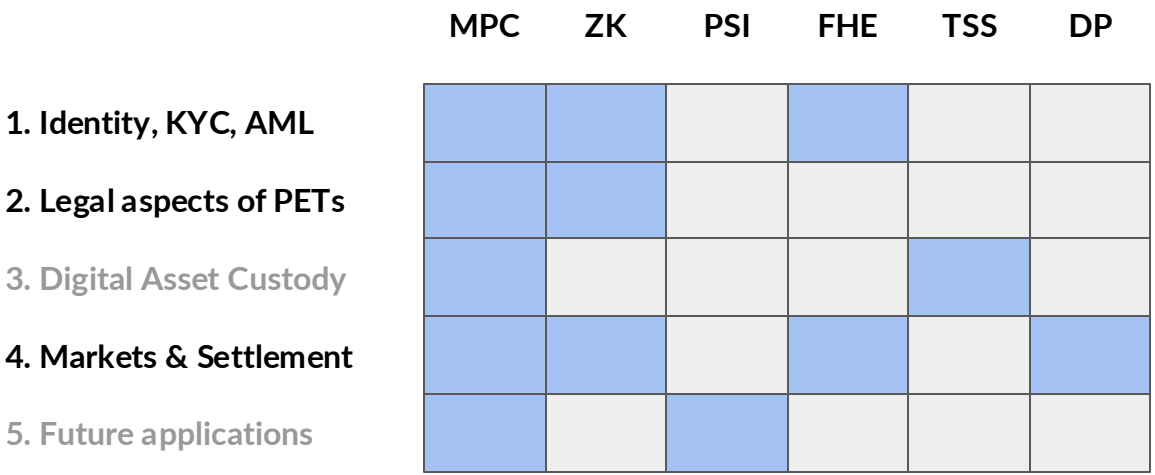
Privacy-Enhancing Technologies in AML

Bernardo David

IT University of Copenhagen

Based on joint work with: Carsten Baum, James Hsin-Yu Chiang, Felix Engelmann, Tore Frederiksen, Mariana da Gama, Markulf Kohlweiss, Christian Lebeda, Elena Pagnin, Misha Volkov

Overview from SoK on PETs for Finance [BCDF23]



eprint.iacr.org/**2023/122**

Introduction to (selected) PETs:

ZK

Interactive / Non-interactive

Prover 🥷 **:**

x: input | **w**: witness

Proves to Verifier $\mathbf{x} \in \mathbf{L_R}$:

$\mathbf{L_R} = \{ \mathbf{x} : \exists \mathbf{w} \text{ s.t. } (\mathbf{x}, \mathbf{w}) \in \mathbf{R} \}$

Verifier 🤷 **:**

Completeness/Soundness

Zero-Knowledge

FHE

sk, pk ← Gen(λ)

With pk: encryption

$enc_{pk}(x) = [x]$

$enc_{pk}(y) = [y]$

$enc_{pk}(z) = [z]$

Anybody: eval operations

$[x \cdot y + z] = [x] \cdot [y] + [z]$

With sk: decrypt

$dec_{sk}([x \cdot y + z]) = x \cdot y + z$

MPC

Private *inputs*:

A: $[x_A]$, B: $[x_B]$, C: $[x_C]$

Jointly: secure evaluation of *F* :

$[(y_A , y_B , y_C)] \leftarrow [\mathbf{F}(x_A , x_B , x_C)]$

Private *outputs*:

A: $[y_A]$, B: $[y_B]$, C: $[y_C]$

What can we do with each of them?

ZK

FHE

MPC

Private Inputs from **ONE** Party or assuming **TRUSTED** prover

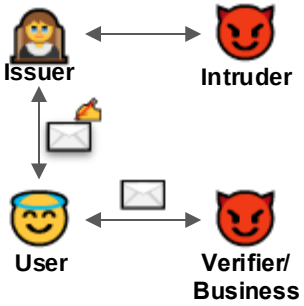
Private Inputs from **MANY** Parties!

SoK: Overview

1. **Identity, KYC**
   AML
2. Legal aspects of PETs
4. Markets & Settlement

Challenges: Identity, KYC & AML

Identity / Know Your Customer (KYC)



SSO: server breaches

→ *Secure authentication*

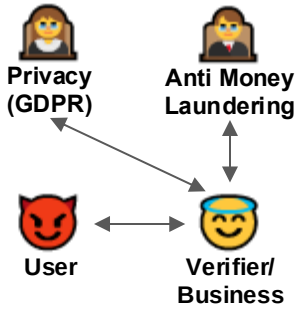
Data leakage from credentials

→ *Anonymous credentials*

Legacy issuance systems

→ *Practical issuance of credentials*

Anti Money Laundering (AML)



Risk profiling exposes private data

→ *Private risk profiling across entities*

TX volume analysis violates privacy

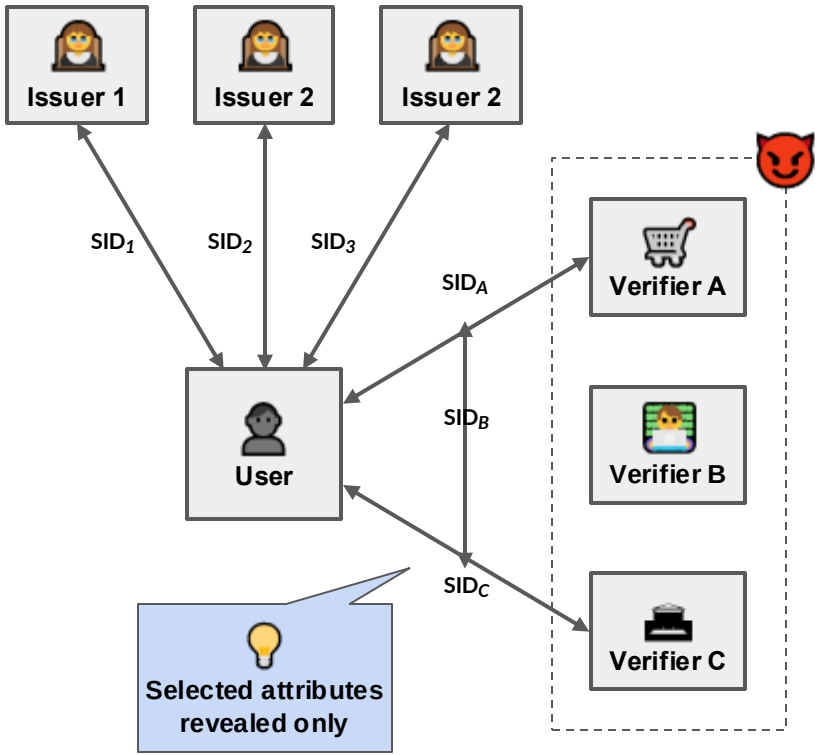
→ *Privacy budget for private transfers*

SoK: Overview

1. **Identity, KYC**
   - Secure SSO
   - **Anonymous credentials**
   - **Practical issuance of credentials**

   AML
2. (Legal aspects of PETs)
4. Markets & Settlement

Anonymous credentials



Privacy goals:

Untraceability/unlinkability

- Rerandomizable “credential”: unlinkable SID’s
- [Chaum82, CL01, CL04, San20]

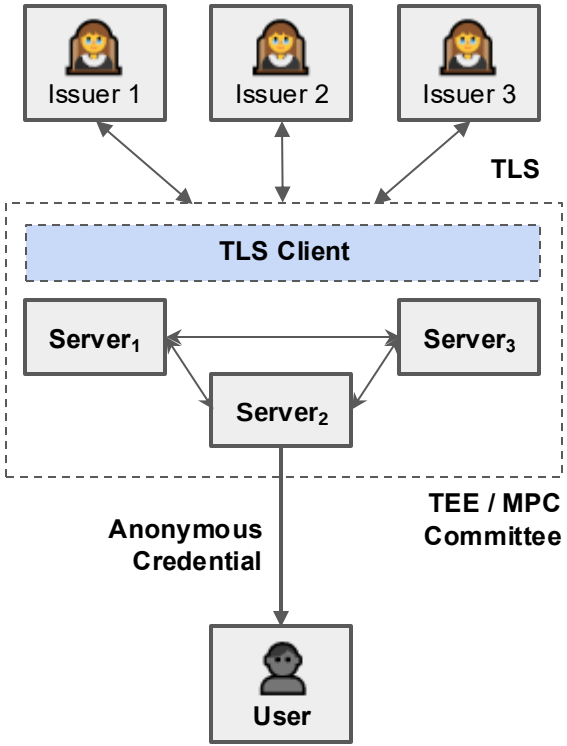
Controlled attribute release

- Selected attributes (age, scores, …)
- Selected, arbitrary attribute *relations*

Revocation

- *Certificate revocation:* nullifiers/accumulators [CL02]
- *Privacy revocation* triggered by auditor policy [KLN22]
- *Publicly auditable revocation* [BDGPW23]

Credential issuance from legacy services



Challenge: Legacy issuers slow to adopt state-of-the-art crypto

Solution(s): Bridge legacy issuer and anonymous credentialing

Verifiable responses from TLS sessions

- TLS provides authenticated response from issuer
- Move TLS client inside TTP
  - TEE: Town Crier [ZCC+16]
  - MPC: DECO [ZMM+20]

Credential bootstrapping from legacy services

- MPC issues credentials w/ legacy web service: CANDID [MMZ+21]

SoK: Overview

1. Identity, KYC

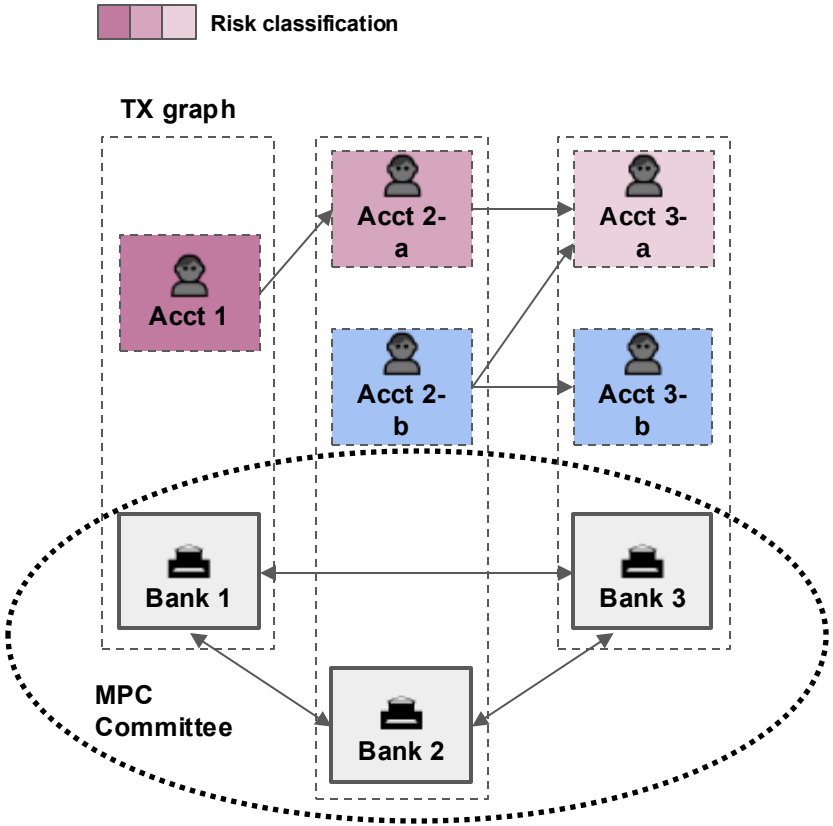
   AML

   - **Private risk score mgmt**
   - **Privacy budgets**

2. (Legal aspects of PETs)

4. Markets & Settlement

AML: Compliant AML analysis



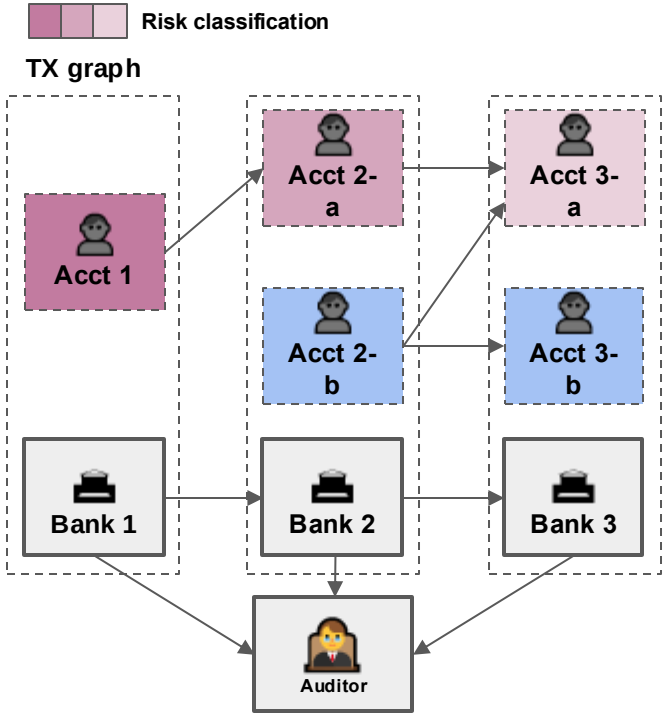
Compliance

- Privacy: user consent (GDPR)
- AML:
  - Explainability: suspicious “flag” requires evidence/data
    Auditability: MPC committee with “auditing” member

Compliant AML risk management across financial institutions

- Transactions, Entities, Risk factors
- Obliviously propagate suspicious sources [vERS21]
- Dedicated ML auditor [ZOP20]
- **Specific-purpose** transaction graph analysis [vEDBRSPV24]

AML: Non-interactive Collaborative Risk Analysis with Updatable Privacy Preserving Blueprints [DEFKPV24]



Compliance

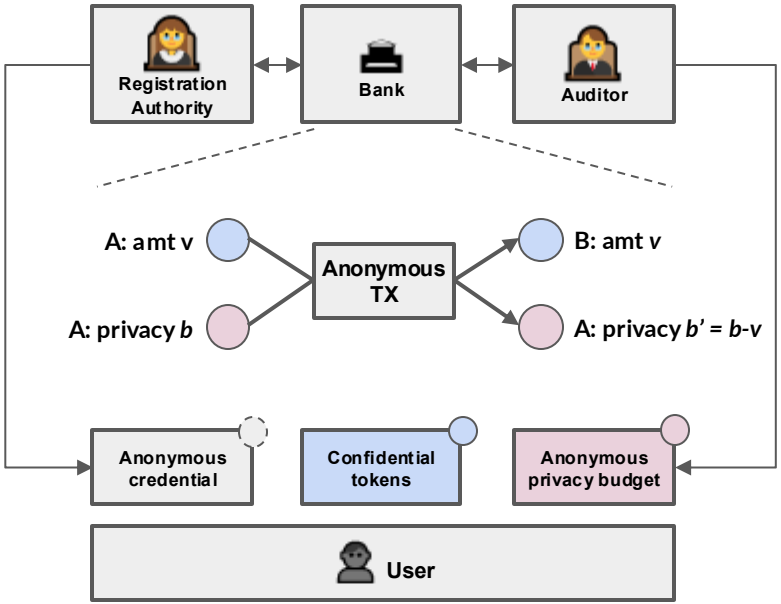
- Privacy: user consent (GDPR)
- AML:
  - Explainability: suspicious “flag” is accompanied by blueprint containing exceeded risk score, which can be verified
  - Auditability: Each bank (or an auditor) learns if risk threshold is exceeded, but nothing else

Collaborative but Non-interactive AML across financial institutions

- Transactions, Entities, Risk factors
- Banks updates local receiver risk scores w.r.t. sender’s risk score
- Risk scores maintained by each bank remain private
- Audit trail shows exactly at which point risk exceeded a threshold

Banks locally update blueprints containing risk scores accompanied by proofs of validity,
if risk is above threshold, banks (or auditor) learn **only** that threshold is exceeded.

AML: CBDC with privacy budgets



UTT: Decentralized Ecash with Accountable Privacy [TBAAGPY22]

Registration authority

- Issues anonymous registration credentials
- Prevents sybil attacks on privacy budget

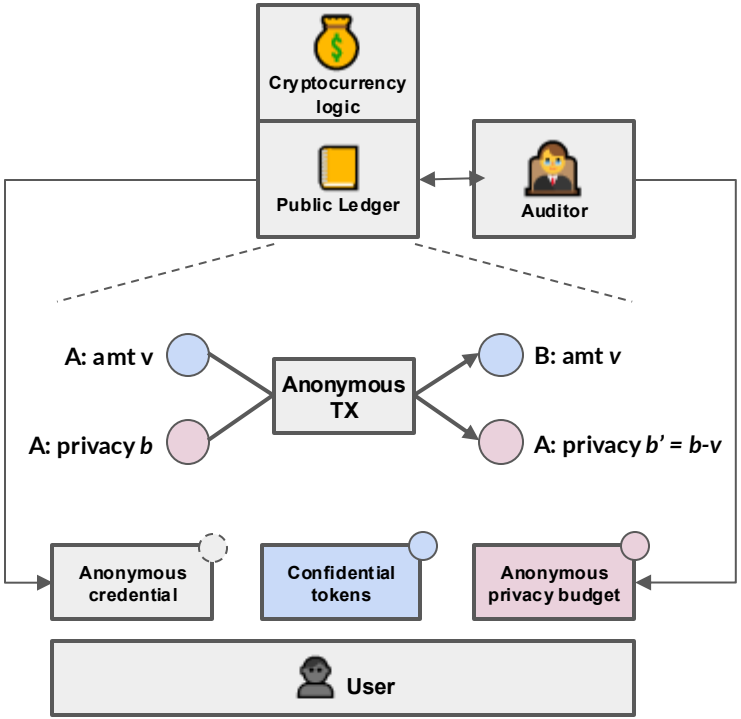
Auditor

- Issues privacy budget for each registered entity
- Privacy budget is proven to bank during transfers

Bank

- Issues confidential, spendable tokens
- Privacy-preserving payments consume privacy budget

AML: Cryptocurrencies (centrally banked or not) with privacy budgets via Updatable Privacy Preserving Blueprints [DEFKPV24]



Implementing Privacy Budgets with uBlu

Auditor

- Issues privacy budget for each registered entity
- Audits transaction to detect exceeded budgets

User

- At every transaction update a blueprint keeping track of their own privacy budget (which can be verified)

Cryptocurrency

- Only transactions accompanied by a valid privacy budget blueprint update are processed.

SoK: Overview

1. Identity, KYC, AML
2. **Legal aspects of PETs**
   - GDPR & PETs
   - PETs in Law & Business
4. Markets & Settlement

PETs in Law & Business

ZK	MPC
	Law enforcement
Court evidence [BCGW22] *Proof that proprietary algorithms, models do not violate law*	**Collaboration between enforcement agencies** *Over potentially classified information*
Secret laws [GP18] *Satisfaction of secret laws proven (in publicly verifiable manner)*	
	Business
Due diligence *Proof that proprietary knowledge, models, or data satisfy claims.*	**Credit score computation [DDN+16]** *Over sensitive private information*

SoK: Overview

1. Identity, KYC, AML
2. (Legal aspects of PETs)

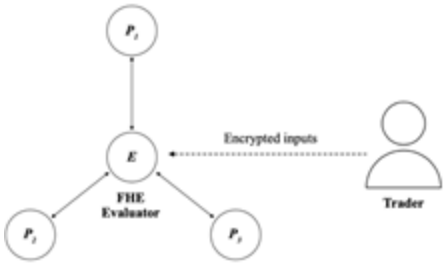
4. Markets & Settlement

- **PETs & markets in traditional markets**
- PETs & markets with public ledgers
- PETs & demand-response markets
- PETs & interbank netting

Dark Pools with MPC/FHE

[CSTA21]

[BDP20]



Continuous double auctions w/ MPC [CSTA19]

- Expensive scanning of secret limit order book (LOB)
- Expensive insertion into LOB
- 35-40 orders/second (on expected LOB size of 30)

Periodic double auctions w/ MPC [CSTA21]

- Clearing at single price for all limit orders in round
- 2000 orders every 5s across 4000 assets
- Gateway MPC assigns assets across 280 MPC instances
- Volume matching only improves throughput [dGCP+22]
- Large committee sizes [dGCSA22]

Periodic double auctions w/ FHE [BDP20]

- FHE key is jointly computed and stored by “institutions”
- FHE evaluator performs matching of orders

Combining MPC and Differential Privacy [CDdGL23]

- Compute order matching in MPC and add noise
- Seeing outcome of own orders does not allow a party to learn about another party’s strategy

SoK: Overview

1. Identity, KYC, AML
2. (Legal aspects of PETs)
4. **Markets & Settlement**
   - PETs & markets in traditional markets
   - **PETs & markets with public ledgers**
   - PETs & demand-response markets
   - PETs & Interbank Netting

Presentation: short overview

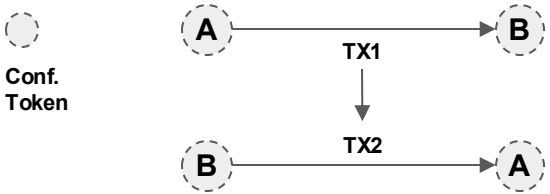
SoK: PETs in Finance

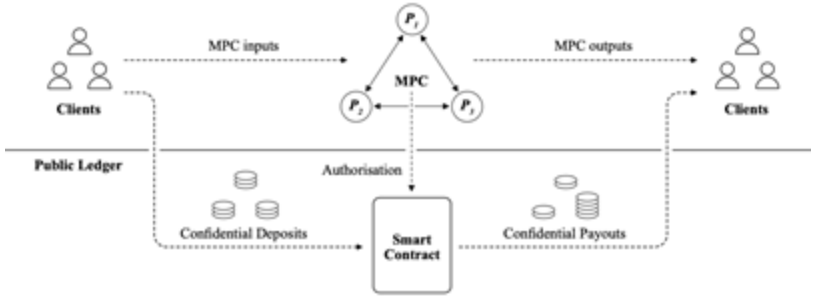
eprint.iacr.org/**2023/122**

SoK: front-running mitigation in DeFi [DeFi'22]

eprint.iacr.org/**2021/1628**

Privacy-preserving decentralized exchanges and AMMs





Intent-based, private DEX

- No “matching” by algorithm; self-discovery of peers
- Atomic swap with counterparty [BCG+20] [NMKW21]

Private DEX/AMM

- P2DEX: Cross-ledger DEX with MPC order matching [B**D**F21]
- Eagle: private smart contracts with MPC [BC**D**F23]
- Many more in “SoK: front-running mitigation” [BC**D**FG22]

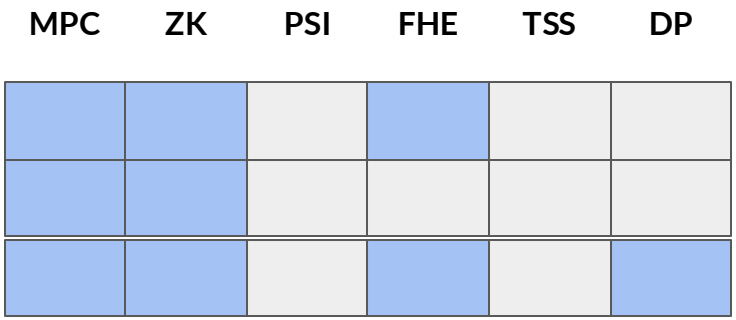
Private DEX for futures

- Future obligation to buy/sell are traded
- Net position: liquidity and future obligations
- Price manipulation can force liquidation if net position leaked
- Net position privacy with zero-knowledge [NMKW21]

Private DEX/AMM via MPC (e.g. Eagle)+Differential Privacy
[C**D**dGL23]

- Compute order matching in MPC and add noise
- Seeing outcome of own orders does not allow a party to learn about another party’s strategy

Summary



- Integrate KYC+AML in transactions systems
- Use PETs in investigations/law enforcement
- Integrate KYC+AML in markets

- General purpose MPC allows for any kind of collaboration (plus automating private financial transactions)
- Specific purpose protocols may perform better for certain AML mechanisms (e.g. privacy budgets, graphs)

MPC+Differential Privacy for Market Making :
eprint.iacr.org/**2023/943**

SoK on PETs for Finance:
eprint.iacr.org/**2023/122**

Non-interactive AML via PETs:
eprint.iacr.org/**2023/1787**

Privacy Preserving Smart Contracts:
eprint.iacr.org/**2022/1435**