universität
innsbruck

Collaborative Deanonymization

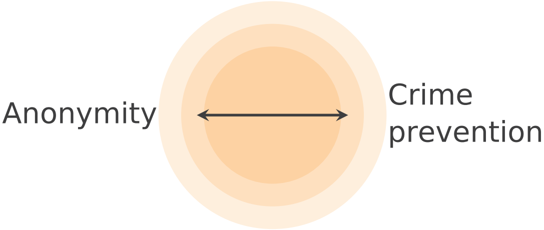
University of Cambridge Security Seminar Series, 26 May 2020

Patrik Keller, Martin Florian, Rainer Böhme

https://arxiv.org/abs/2005.03535

Motivation

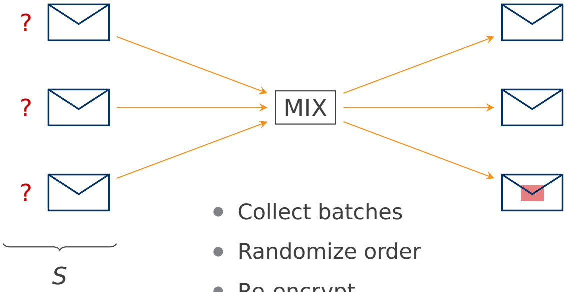
Decentralized systems



Objective: Resolve this tension in a peer-to-peer manner.

Mixing

Establish **unlinkability** of messages in communication systems.



- Collect batches
- Randomize order
- Re-encrypt

The size of the **anonymity set** $|S|$ is a measure of privacy.

Chaum (1981)

Revocable Anonymity

Mixing offers some anonymity ($|S| > 1$) unless all mixes or all other users collude.

Status quo

Place backdoors for privileged parties . . .

- into mixes
- into cryptography

. . . while limiting abuse

- with accountability
- with thresholds

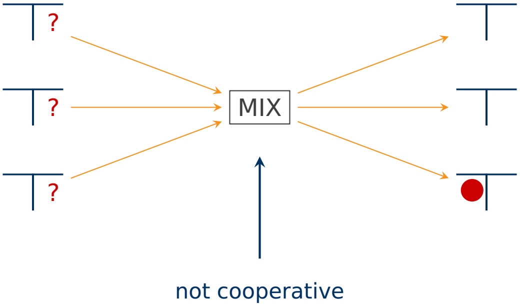
Unexplored problem

How does this transfer to systems that reject the existence of privileged parties ?

Camenisch and Lysyanskaya (2001); Claessens, Díaz, Goemans, Dumortier, Preneel, and Vandewalle (2003)
Köpsell, Wendolsky, and Federrath (2006); Backes, Clark, Kate, Simeonovski, and Druschel (2014)

Mixing in Cryptocurrencies

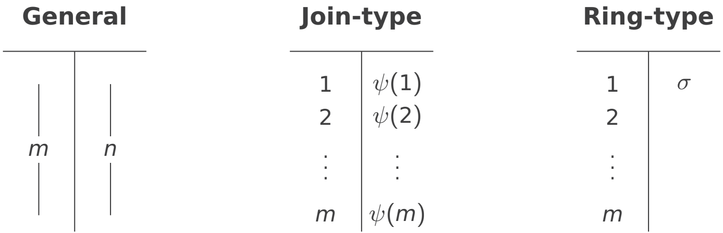
Establish unlinkability of flows in **transaction systems**.



The ledger records all actors: **collaborative deanonymization** as overlay protocols.

Types of Mixing Transactions Considered

in the UTXO model adopted in Bitcoin and Monero



General

m n

Join-type

1 $\psi(1)$

2 $\psi(2)$

$\vdots$ $\vdots$

m $\psi(m)$

Ring-type

1 σ

2

$\vdots$

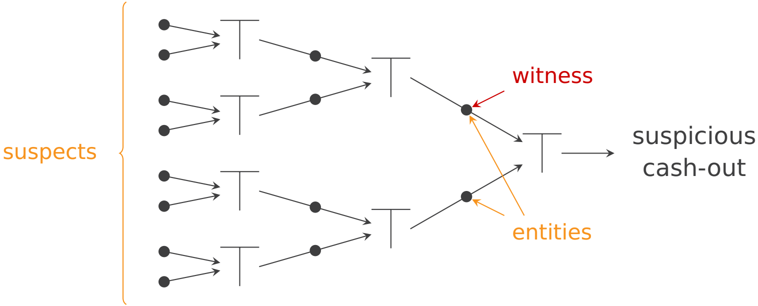
m

A priori, the police does not know:

- Identities behind the key pairs referenced in the m inputs and n outputs
- For join-type transactions: the permutation ψ on $\{1, \ldots, m\}$
- For ring-type transactions: the true input $\sigma \in \{1, \ldots, m\}$

Backtracking Scenario

Example: 7 ring-type transactions with $m = 2$



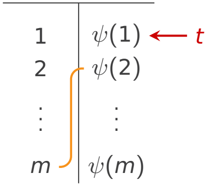
Assumptions: authentic channel from the police to all users, e. g., through wallet software or online wallet / exchange

secure anonymous return channel from witnesses to the police

Individual Testimony

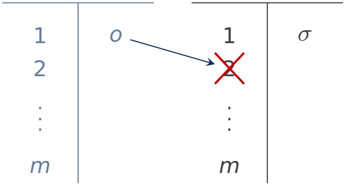
- Let the t-th output be the target.
- Witness controlling the i-th input proves $\psi(t) \neq i$.
- Sing a challenge with the private keys belonging to input i and output $j \neq t$.

Join-type



- Witness controlling the i-th input proves $\sigma \neq i$.
- Prepare phantom transaction T' (not shown) which spends o as single input.
- Traceable ring signatures would indicate double-spending if $\sigma = i$, hence if the key images of T and T' differ, it holds $\sigma \neq i$.

Ring-type



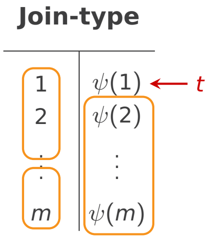
Fujisaki and Suzuki (2007)

Group Testimony

With $m - 1$ individual testimonies, the police learns more than necessary.

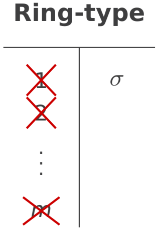
Coordination within groups of witnesses can reduce this privacy loss.

- Multiple witnesses controlling the input set S jointly testify that $\psi(t) \notin S$.
- Sign challenge with all $2 \cdot |S|$ private keys belonging to the witnesses' inputs and outputs.
- The remaining anonymity set size is $|S|$; in the best case $m - 1$.



Group Testimony (cont'd)

- Multiple witnesses controlling the input set S jointly testify that $\sigma \notin S$.
- Provably spent set approach: each phantom T' has $|S|$ inputs, one for each collaborating witnesses' previous output.
- All $|S|$ T' have different key images.
- Remaining anonymity set size $\leq |S|$.
  The inequality is strict if outputs referenced in the phantom transactions have already been spent. They are linkable.
- Group testimonies can span multiple transactions at the same time, enabling to merge anonymity sets and achieve $|S| \geq m$.



Ring-type

$\cancel{1}$ σ

$\cancel{2}$

$\vdots$

$\cancel{m}$

Wijaya, Liu, Steinfeld, and Liu (2018); Yu, Au, Yu, Yang, Xu, and Lau (2019)

Risk of False Testimonies

How much confidence can we place in testimonies ?

Ring-type
Monero stores σ on the blockchain in encrypted form, ruling out false testimonies even if private keys are leaked or stolen.

Join-type
Bitcoin does not commit ψ to the blockchain. A perpetrator with access to private keys of witnesses can produce false testimonies.

With collaborative deanonymization, private keys remain sensitive even if they do not control any funds anymore.

Outlook

Our working paper discusses:

- Coercion risk for witnesses
- Forward tracking
- Relation to blacklisting
- Cover transactions

New directions:

- Legal framework for law enforcement
- Economic incentives
- Knock-on effects on participation in mixing
- Deniable anonymity techniques

Möser, Böhme, and Breuker (2014); Abramova, Schöttle, and Böhme (2017); Arce and Böhme (2018)

Summary

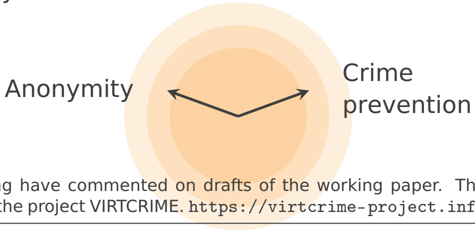
Revoking anonymity by collaboration of users has been overlooked.

It might have a place in solving and preventing crime with cryptocurrencies.

Our protocols leave witnesses autonomy in deciding whether they testify.

Unlike traffic and blockchain analysis, collaborative deanonymization does not scale.

This limits the risk of abuse for mass surveillance and upholds the peer-to-peer spirit in transaction systems with revokable anonymity.



Acknowledgements: Michael Fröwis, Malte Möser and Tim Ruffing have commented on drafts of the working paper. The research was supported by the Austrian FFG's KIRAS program under the project VIRTCRIME. `https://virtcrime-project.info`

universität
innsbruck

Thank you for listening.

Collaborative Deanonymization

Patrik Keller, Martin Florian, Rainer Böhme

https://arxiv.org/abs/2005.03535

S. Abramova, P. Schöttle, and R. Böhme. Mixing coins of different quality: A game-theoretic approach. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, editors, *Financial Cryptography and Data Security Workshops*, volume 10323 of *Lecture Notes in Computer Science*, pages 280–297. Springer, 2017.

D. G. Arce and R. Böhme. Pricing anonymity. In S. Meiklejohn and K. Sako, editors, *Financial Cryptography and Data Security*, volume 10957 of *Lecture Notes in Computer Science*, pages 349–368. Springer, 2018.

M. Backes, J. Clark, A. Kate, M. Simeonovski, and P. Druschel. BackRef: Accountability in anonymous communication networks. In I. Boureanu, P. Owesarski, and S. Vaudenay, editors, *Applied Cryptography and Network Security*, volume 8479 of *Lecture Notes in Computer Science*, pages 380–400. Springer, 2014.

J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In B. Pfitzmann, editor, *Advances in Cryptology (Proceedings of EUROCRYPT)*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

D. Chaum. Untracable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2), 1981.

J. Claessens, C. Díaz, C. Goemans, J. Dumortier, B. Preneel, and J. Vandewalle. Revocable anonymous access to the Internet? *Internet Research*, 13(4):242–258, 2003.

E. Fujisaki and K. Suzuki. Traceable ring signature. In T. Okamoto and X. Wang, editors, *Public Key Cryptography*, volume 4450 of *Lecture Notes in Computer Science*, pages 181–200. Springer, 2007.

S. Köpsell, R. Wendolsky, and H. Federrath. Revocable anonymity. In G. Müller, editor, *Emerging Trends in Information and Communication Security*, volume 3995 of *Lecture Notes in Computer Science*, pages 206–220. Springer, 2006.

M. Möser, R. Böhme, and D. Breuker. Towards risk scoring of Bitcoin transactions. In R. Böhme, M. Brenner, T. Moore, and M. Smith, editors, *Financial Cryptography and Data Security Workshops*, volume 8438 of *Lecture Notes in Computer Science*, pages 16–32. Springer, 2014.

D. A. Wijaya, J. Liu, R. Steinfeld, and D. Liu. Monero ring attack: Recreating zero mixin transaction effect. In *Trust, Security And Privacy In Computing And Communications*, pages 1196–1201. IEEE, 2018.

Z. Yu, M. H. Au, J. Yu, R. Yang, Q. Xu, and W. F. Lau. New empirical traceability analysis of CryptoNote-style blockchains. In I. Goldberg and T. Moore, editors, *Financial Cryptography and Data Security*, volume 11598 of *Lecture Notes in Computer Science*, pages 133–149. Springer, 2019.