

# Monero Cross-Chain Traceability

## Empirical Analysis of Privacy Implications from Currency Hard-Forks

Abraham Hinteregger

Masterstudium:

Computational Intelligence

Technische Universität Wien

Institut für Informationssysteme

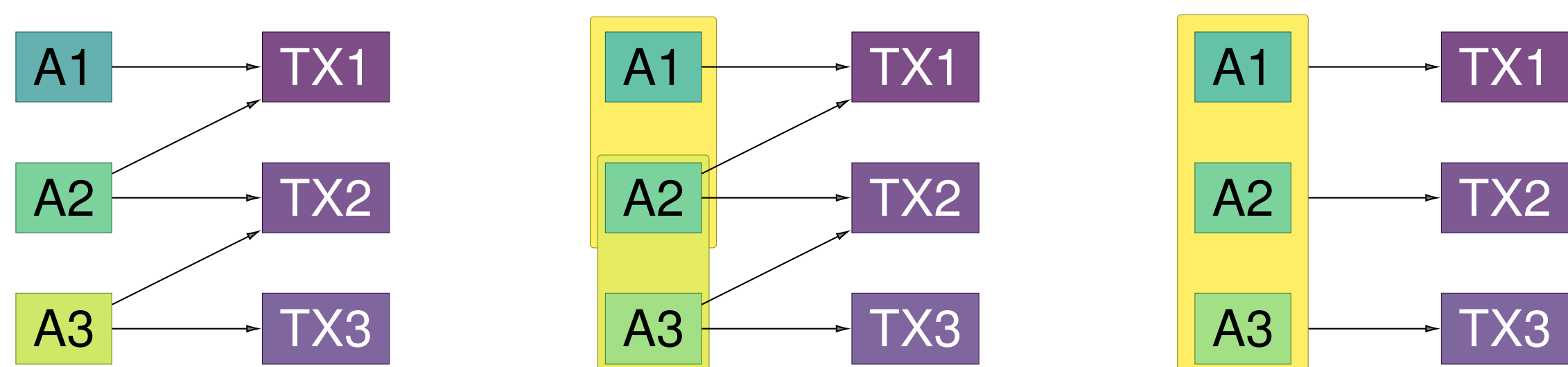
Arbeitsbereich: Algorithms and Complexity Group

Betreuer: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Günther Raidl

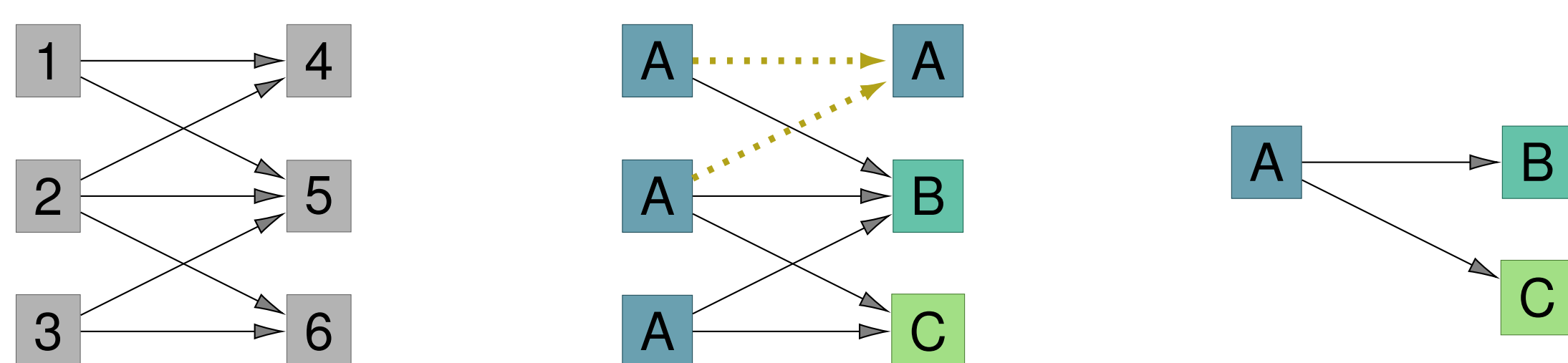
Mitbetreuer: Dr. Bernhard Haslhofer (AIT)

### Motivation

- Several methods to analyze Bitcoin transactions history
  - Multi-Input heuristic clusters addresses (A1-A3) of inputs occurring in single transaction (TX) as they likely belong to the same user



- Address-graph (left) labelled with address-clusters from multi-input heuristic (center) can be simplified to entity-graph (right)

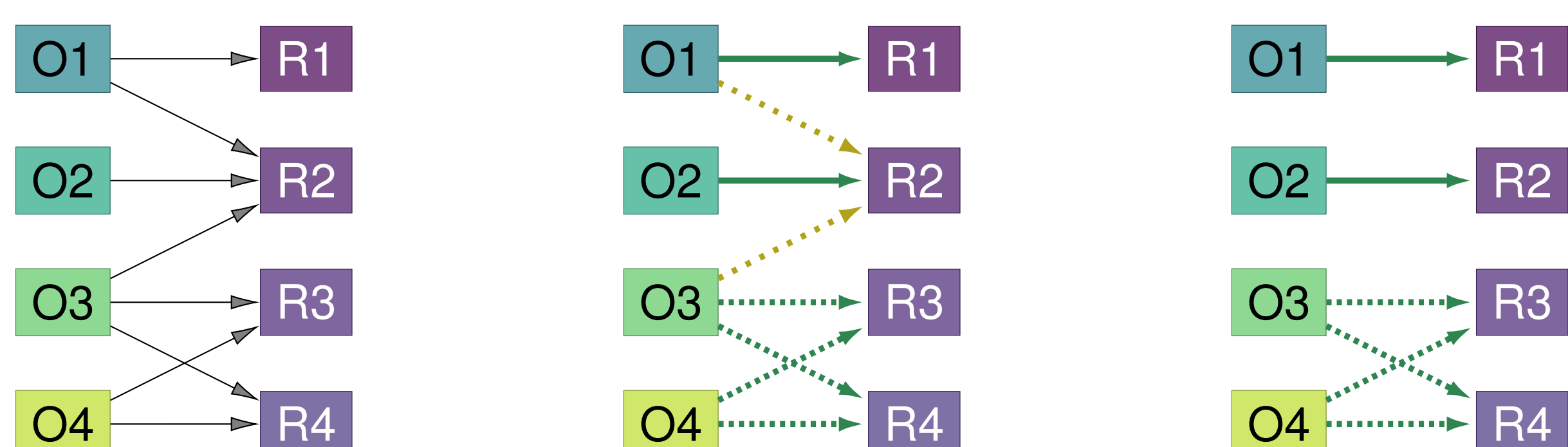


- Increased chance of users being identified via TX-history
- ⇒ privacy-centric coins, e.g. Monero, based on CryptoNote [3]
- Features of Monero, privacy-coin with highest market-cap:
  - Unlinkability:** *Stealth addresses* hide recipients of transactions
  - Untraceability:** Each TX input is a ring instead of a TXO (TX output). A ring is a set of TXOs (with the same denomination), one of which is the real input and the others are decoys (*mixins*). These *ring signatures* obfuscates the path of a given coin.
  - Fungibility:** Values of TXOs are hidden with RingCT (confidential TXs) since 2017, making denomination constraint of rings unnecessary.
- Analysis methods from other currencies do not work for Monero

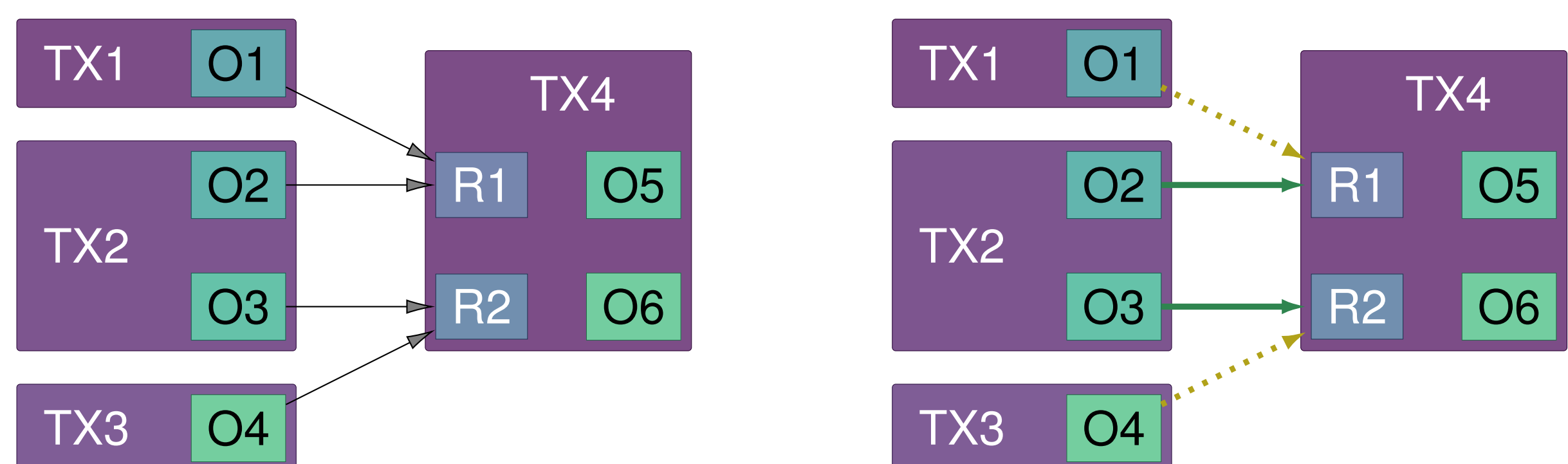
### Traceability Analysis

- Two independent 2017 publications [1, 2] demonstrated that a majority of transactions are traceable. They used the following deductions techniques and heuristics:

- Zero Mixin & Intersection Removal (ZMR & IR): Ring R1 has only one referenced TXO (O1), which is therefore the real input (✓) in that ring and all occurrences in other rings (R2) have to be decoys (✗) and can thus be removed. Intersection removal is a generalization of this technique that marks TXOs occurring in  $n$  rings (R3,R4) with  $n$  identical members (O3,O4) as spent (✓).



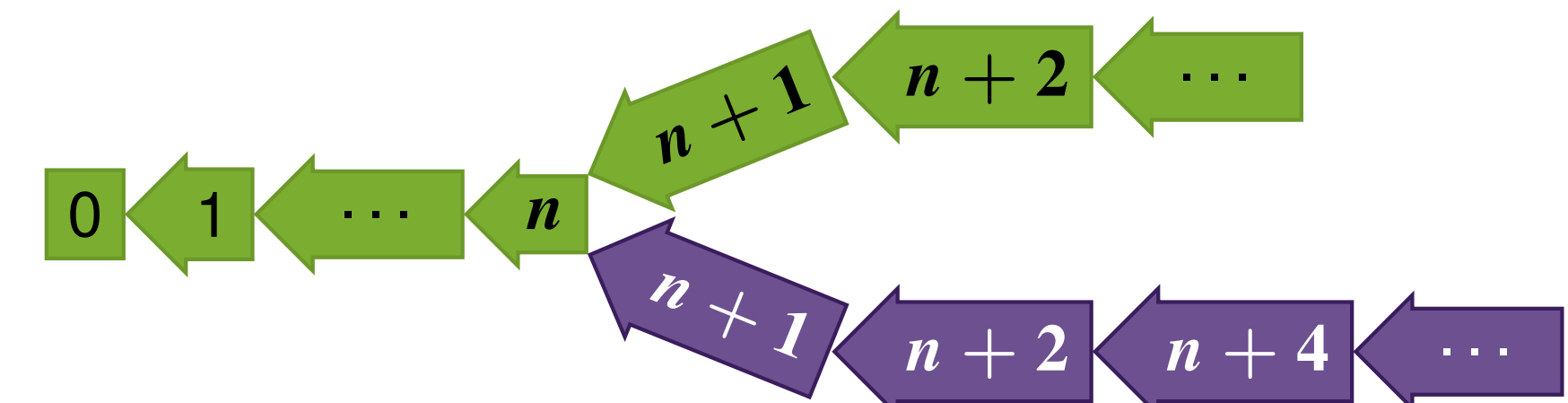
- Guess Newest Heuristic (GNH): Exploits naive decoy sampling. As time distribution of decoys and real outputs differed, most recent TXO was real input in most cases.
- Output Merging Heuristic (OMH): TX4 merges multiple TXOs (O2,O3) from TX2 in distinct rings (R1,R2). OMH assumes that those are the real inputs.



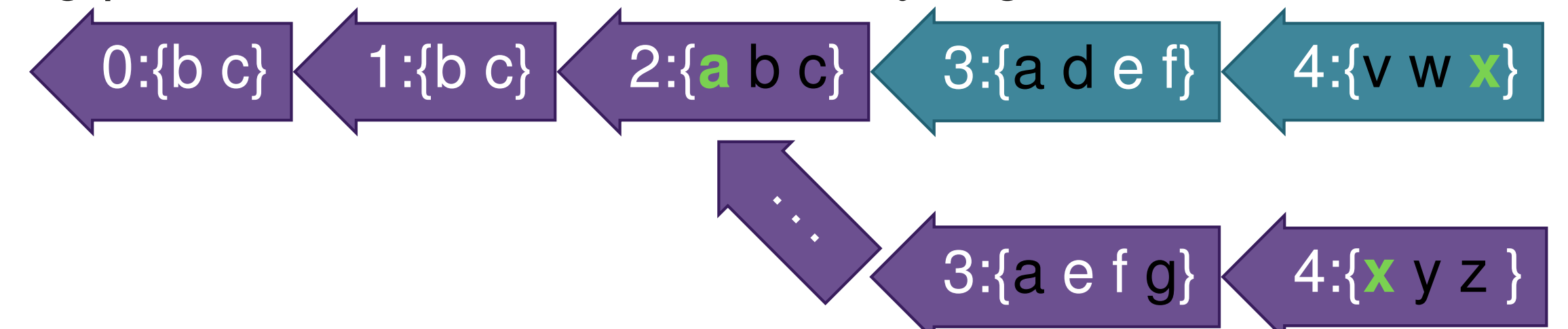
- Monero developers reacted by implementing countermeasures:
  - Higher mandatory minimum ringsize against ZMR (from 3 to 7)
  - Improved decoy sampling against GNH (sampling multiple  $\leq 1.8$  day old inputs and soon from a  $\gamma$ -distribution)
- This work contributes to the state of the art in two ways:
  - We propose a new tracing method, which exploits information leaked on currency-forks. We measure the privacy-impact from two recent forks (Monero Original & MoneroV)
  - We evaluate the accuracy of GNH & OMH based on results from our traceability analysis (using ZMR, IR and our new method).

### Forks & Cross Chain Analysis (CCA)

- Cryptocurrencies forks result in two coins with a common history



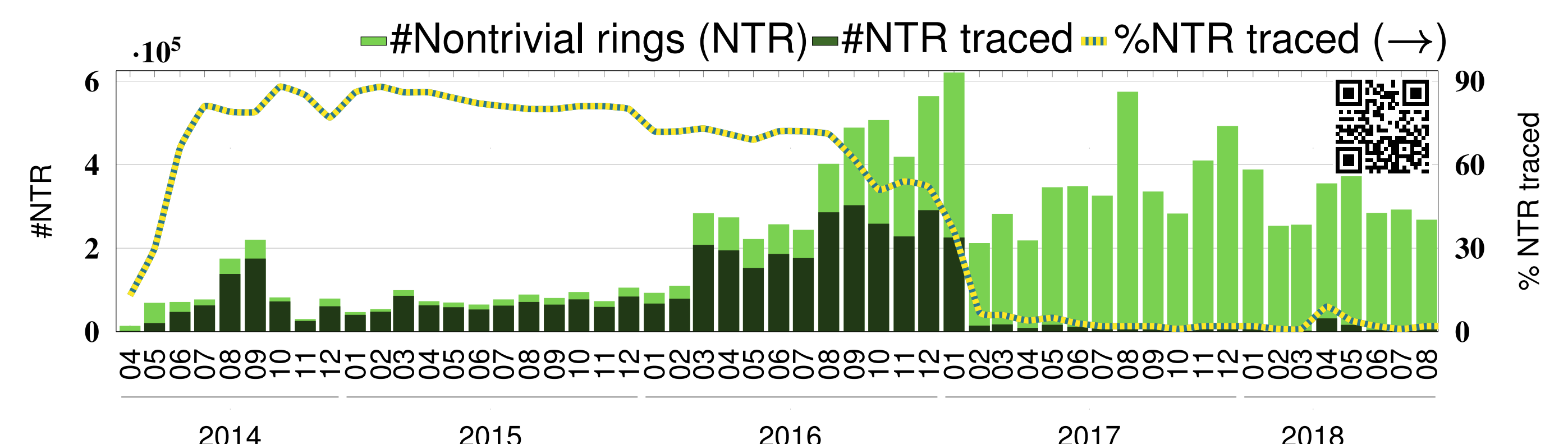
- Unspent pre-fork coins can be spent on both branches
- A *key image* (uniquely determined by real input) used to prevent double spending
- If multiple rings (one per branch) have the same KeyImg, the same pre-fork TXO is spent in them
- Real input is in intersection of the rings
- TXOs in the symmetric difference must be decoys
- Monero blockchain ( $\leftarrow$  XMR) two blocks before and after a fork ( $\leftarrow$  XMO)
- One ring per block, numbers refer to KeyImg, letters are TXOs



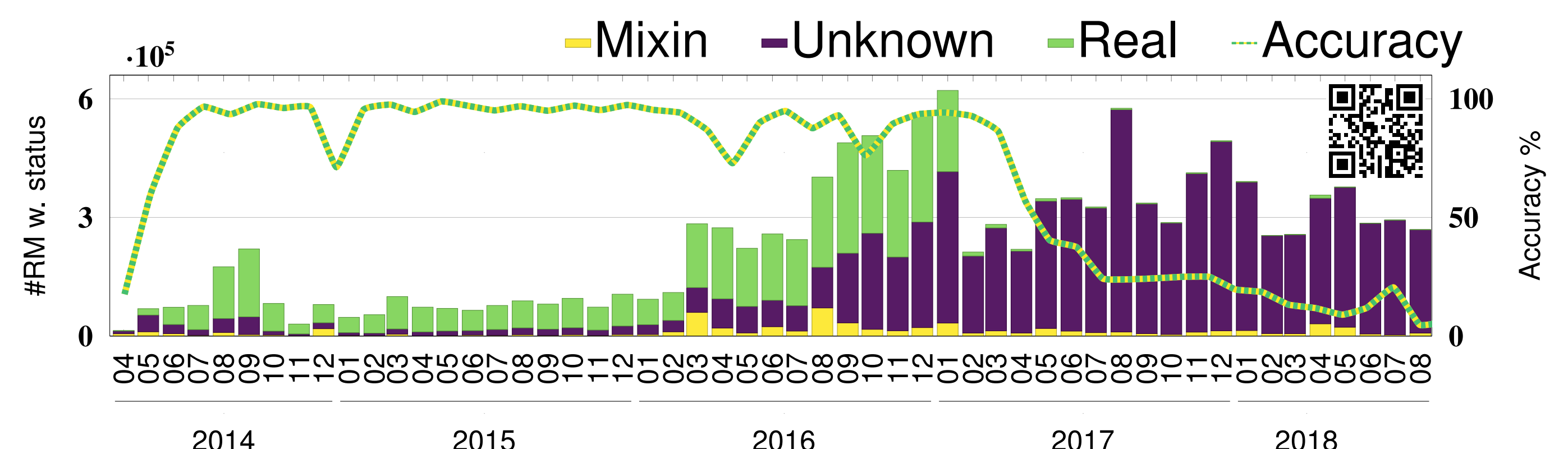
- IR can be applied to ring 0 and 1,  $b, c$  therefore decoys in ring 2.
- ZMR sets  $a$  as *real input* in ring 2 and decoy in both rings 3.
- CCA sets  $d, g$  as decoys because  $\notin \{a, d, e, f\} \cap \{a, e, f, g\}$
- CCA sets  $x$  as real input because  $|\{v, w, x\} \cap \{x, y, z\}| = 1$

### Results

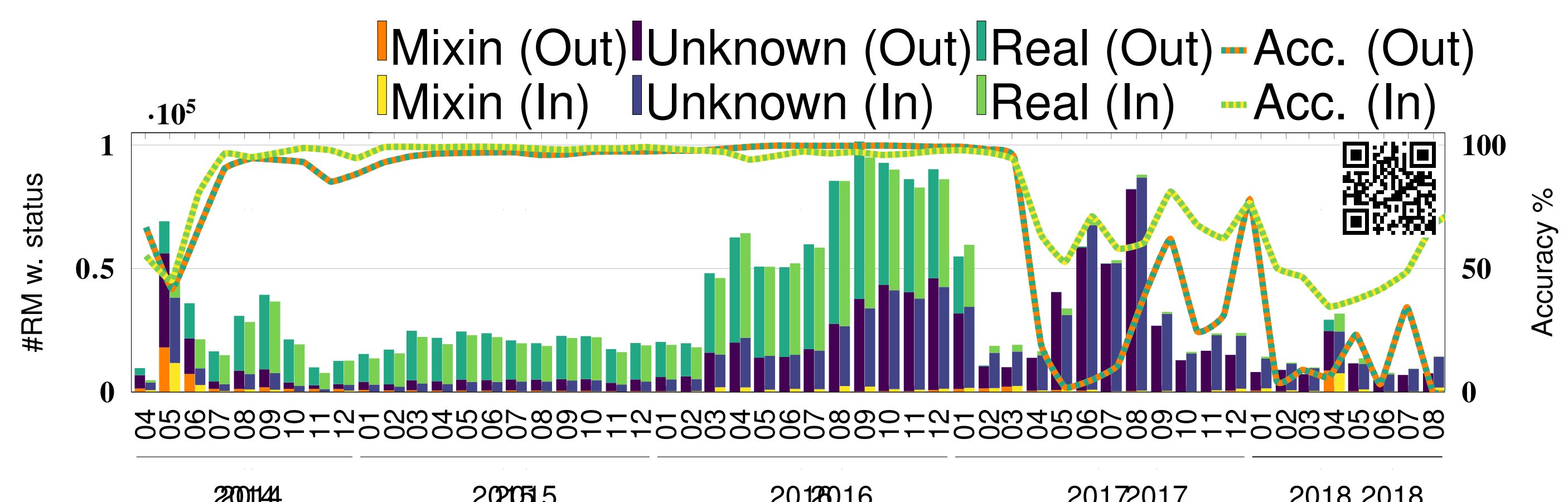
- Number of nontrivial rings (NTR,  $> 1$  RM)) and traced NTRs.
  - Accuracy low since 2017/RingCT. Small peak in April 2018 due to CCA.



- Status of RM identified as 'real' with GNH and OMH.
  - Improved decoy sampling routines resulted in low accuracy.



- Aggregation by output-creation (out) or spend time (in).
- Lower # of applications due to less outputs/inputs since RingCT.



- Results suggest that amount of traceable rings with current transaction protocol is low enough to not jeopardize privacy of Monero's users.
- Forks with more traction than XMO/XMV could have higher impact.