Privacy in Blockchain

Murat Osmanoglu

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk'

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- "I desire a society where all may speak freely about whatever topic they will. I desire that all people might be able to choose to whom they wish to speak and to whom they do not wish to speak. I desire a society where all people may have an assurance that their words are directed only at those to whom they wish. Therefore I oppose all efforts by governments to eavesdrop and to become unwanted listeners." (Cyphernomicon, Tim May)

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- "What if we could build a society where the information was never collected? Where you could pay to rent a video without leaving a credit card number or a bank number? Where you could prove you're certified to drive without ever giving your name? Where you could send and receive messages without revealing your physical location, like an electronic post office box? " (Privacy, Technology, and the Open Society, John Gilmore)

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- its roots traced back to the study of David Chaum on anonymous digital cash

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- its roots traced back to the study of David Chaum on anonymous digital cash

  'Security Without Identification: Transaction Systems to Make Big Brother Obsolete', 1985

Cypherpunks

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

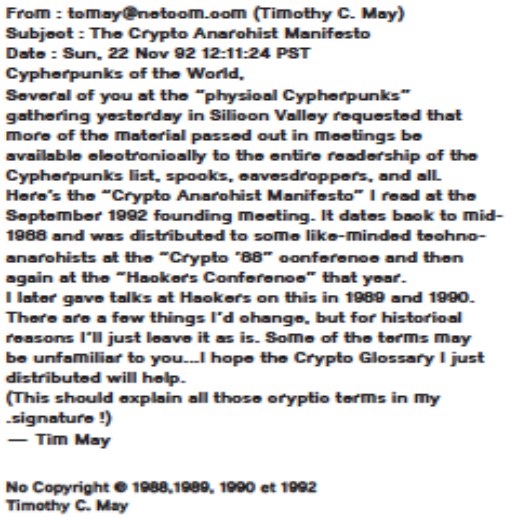
- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- in late 1992, three people: Eric Hughes (mathematicians from Berkeley), Tim May (businissman retired from Intel), and John Gilmore (computer scientist) were gathering to discuss some cryptographic and programing issues

Cypherpunks

- they later initiated a mailing list (the number of subscribers reached 2000 in 1997) to reach out some other cypherpunks outside of Bay Area.

- Timothy May published 'the Crypto Anarchist Manifesto' in 1992



From : tcmay@netcom.com (Timothy C. May)
Subject : The Crypto Anarchist Manifesto
Date : Sun, 22 Nov 92 12:11:24 PST
Cypherpunks of the World,
Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all.
Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year.
I later gave talks at Hackers on this in 1989 and 1990. There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you....I hope the Crypto Glossary I just distributed will help.
(This should explain all those cryptic terms in my .signature !)
— Tim May

No Copyright © 1988,1989, 1990 et 1992
Timothy C. May

THE CRYPTO-ANARCHIST MANIFESTO

Thimothy C.May

MANIFESTE CRYPTO-ANARCHISTE

Cypherpunk Manifesto

- Eric Hughes published *'A Cypherpunk's Manifesto'* in 1993, which can be considered as holy text of this movement.

"Privacy is necessary for an open society in the electronic age"

"Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction.
"

"Privacy in an open society requires anonymous transaction systems."

"We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence"

"We must defend our own privacy if we expect to have any"

Privacy Issues

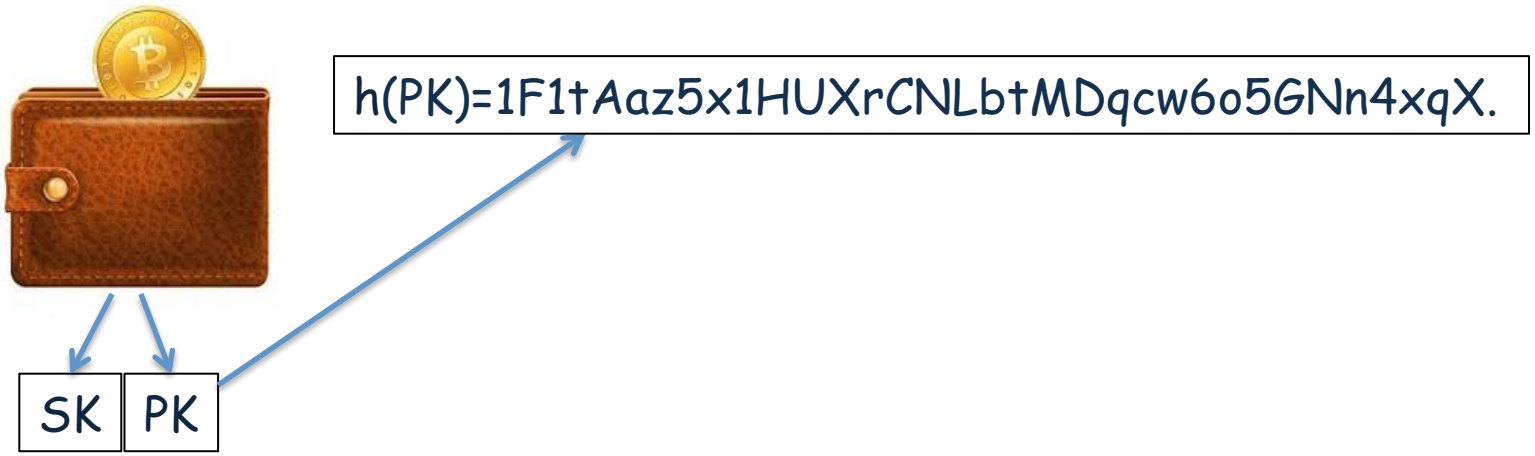
- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone

Privacy Issues

- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone
- Bitcoin uses pseudonymous addresses for users to provide privacy up to a certain degree

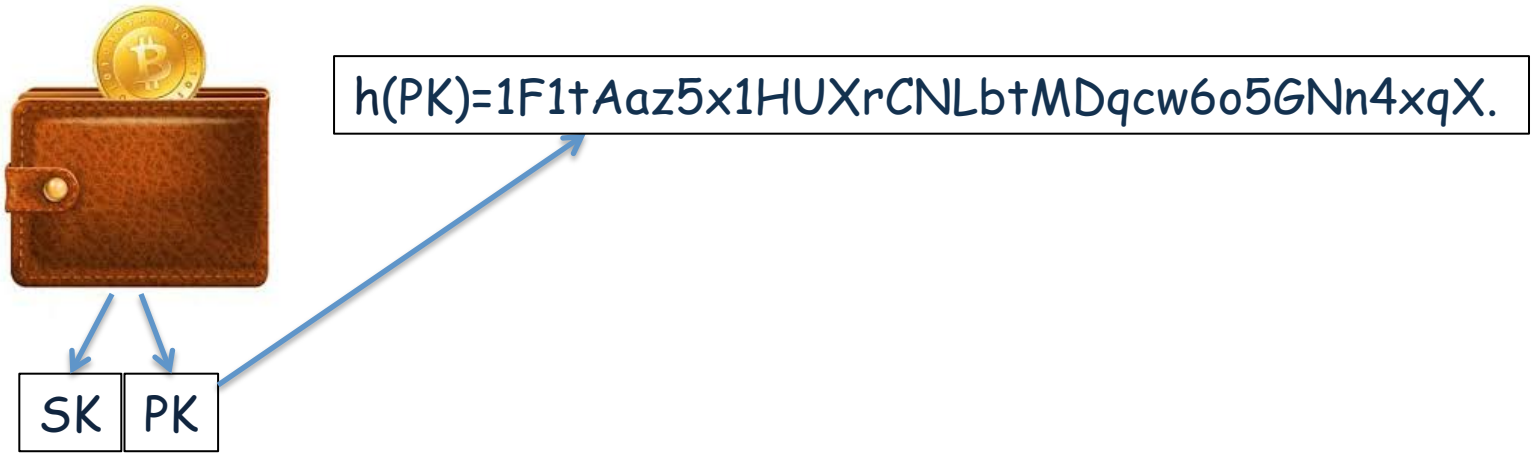
Privacy Issues

- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone
- Bitcoin uses pseudonymous addresses for users to provide privacy up to a certain degree



Privacy Issues

- each user can get all the transactions shared in the network
- it enables each user to validate integrity and authenticity of every transaction
- it also exposes all the transaction associated with an ID to everyone
- Bitcoin uses pseudonymous addresses for users to provide privacy up to a certain degree



- Bitcoin even allows users to have more than one address and to use a new one for each transaction to improve privacy

Privacy Issues

- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.

Privacy Issues

- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.
- since bitcoin enables users to create more than one address, the first goal here is to cluster all addresses belonging to the same user

Privacy Issues

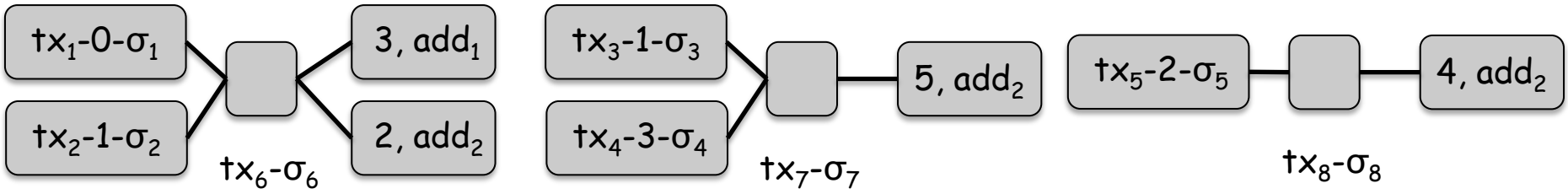
- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.
- since bitcoin enables users to create more than one address, the first goal here is to cluster all addresses belonging to the same user
- analyze the study proposed Reid and Harrigan [1]

Privacy Issues

- it is still possible to link pseudonyms to real identities by utilizing the blockchain data together with the external information obtained from different Internet sources such as twitter posts, forums etc.
- since bitcoin enables users to create more than one address, the first goal here is to cluster all addresses belonging to the same user
- analyze the study proposed Reid and Harrigan [1]
  - they obtained all the transactions recorded in bitcoin from January 2009 to July 2011 (1019486 txs between 1253054 addresses)
  - they built two networks (transaction and user) based on the input-output relationship between transactions and re-use and co-use of the addresses

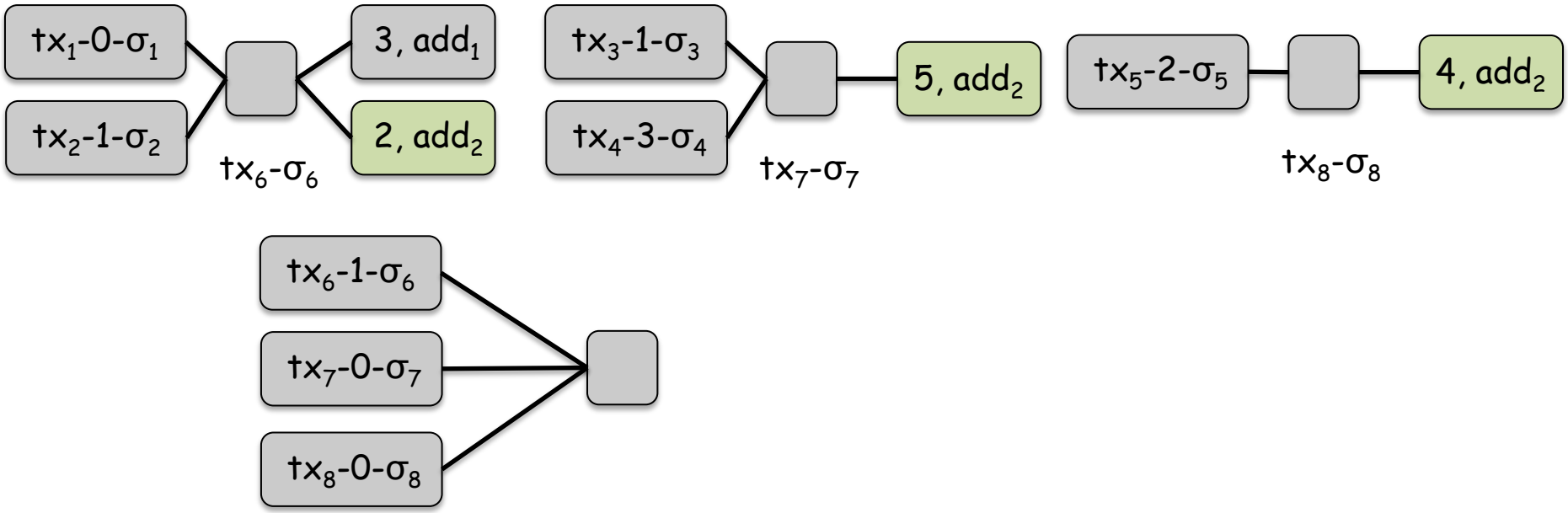
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



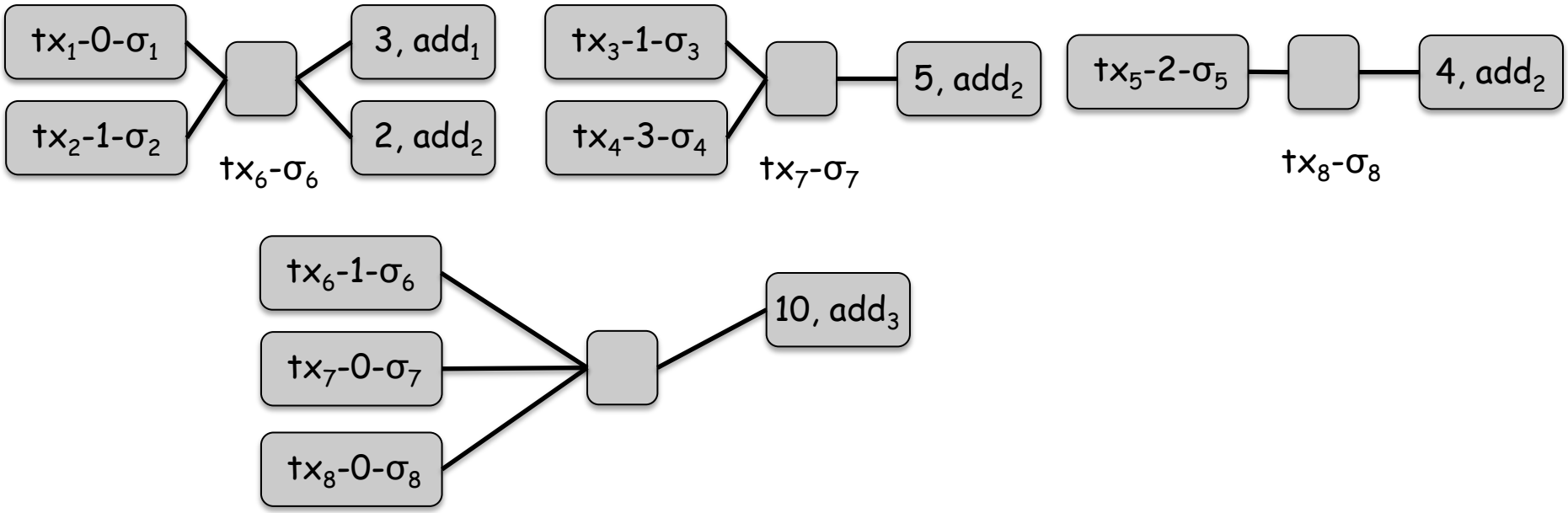
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



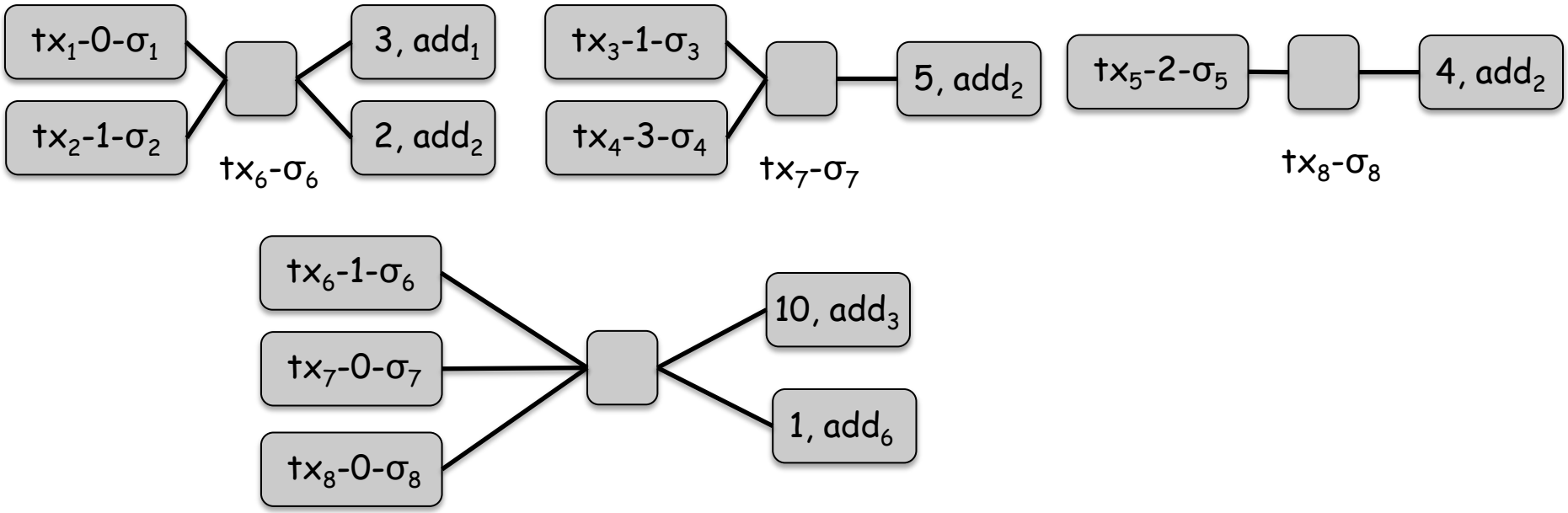
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



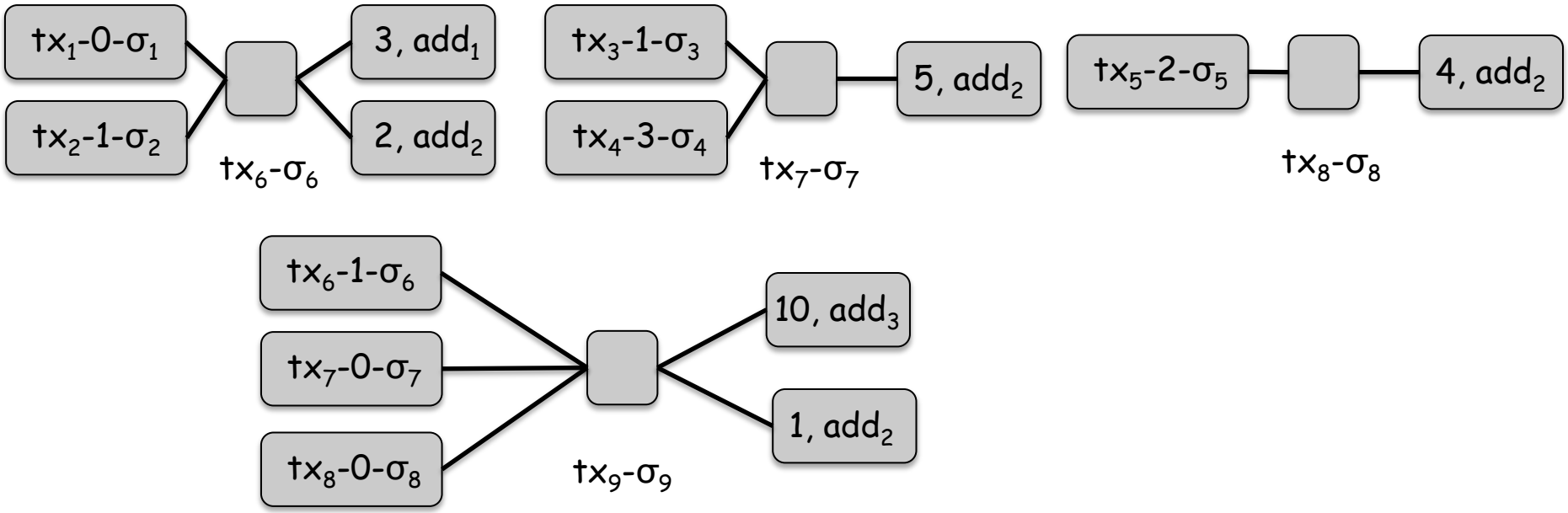
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



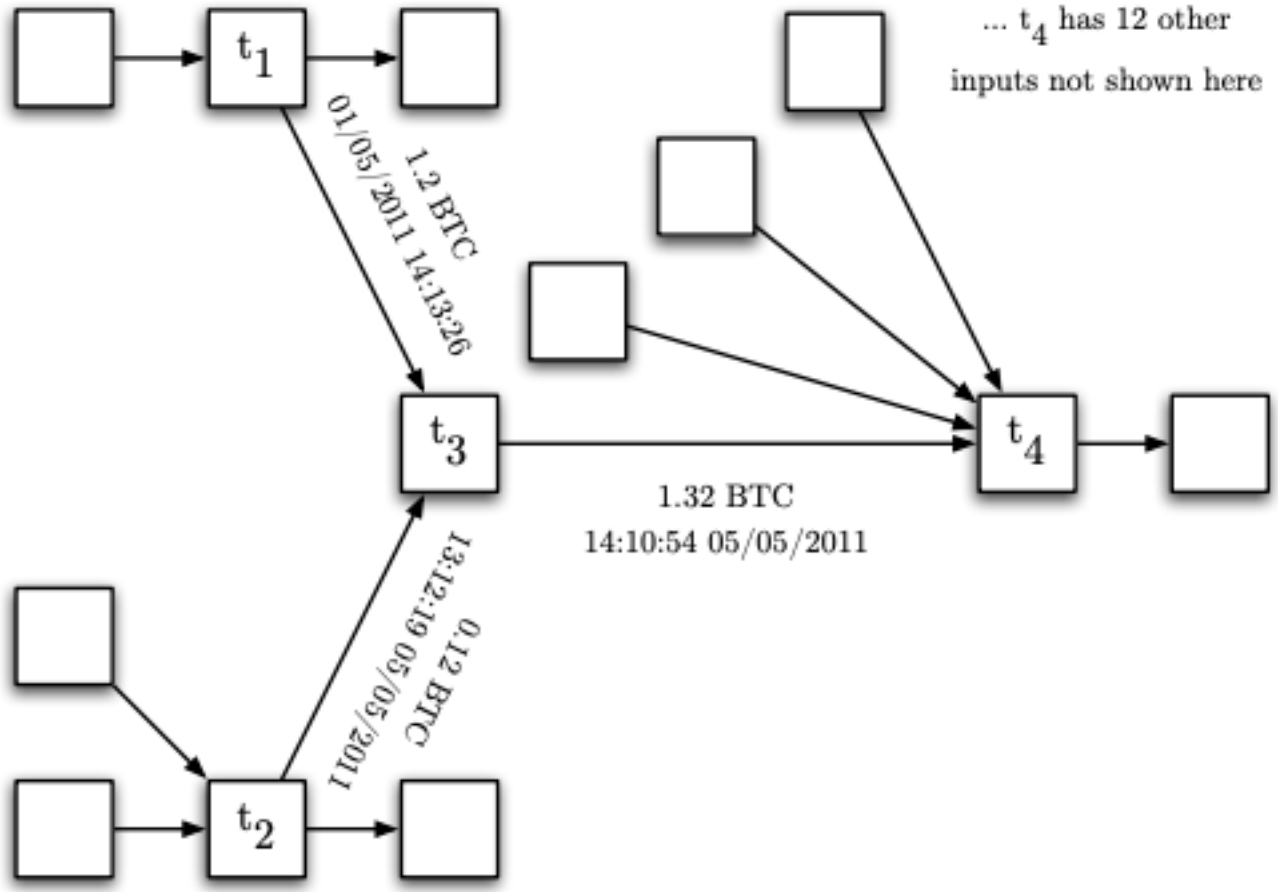
Privacy Issues

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



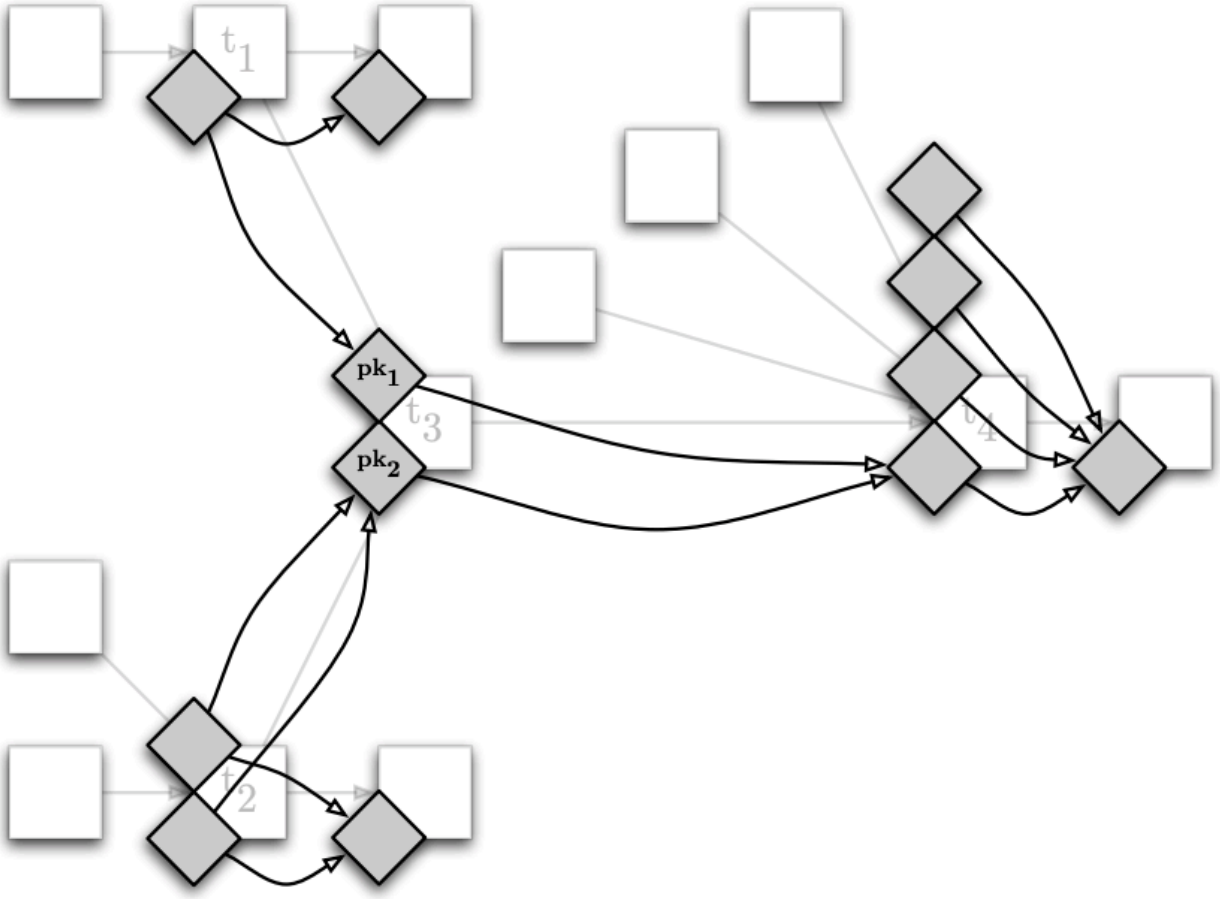
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- a sub-network of transaction network



Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- a sub-network of user network



Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- some findings:
  - user network has cyclic structure (it is expected to just contain Bitcoin flows between one-time addresses keys that were not connected to other addresses)
  - a tx frequently has single input from a larger tx, or multiple inputs from smaller txs
  - a tx frequently has two outputs: one for payment, one directing to user's other address

Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- some findings:
  - user network has cyclic structure (it is expected to just contain Bitcoin flows between one-time addresses keys that were not connected to other addresses)
  - a tx frequently has single input from a larger tx, or multiple inputs from smaller txs
  - a tx frequently has two outputs: one for payment, one directing to user's other address
- data obtained from different Internet sources such as twitter posts, bitcoin forums etc. (they usually post one of their addresses) used to link an address to a real identity
  - utilizing user network, they can even link public addresses to some other address belonging to same users

Privacy Issues

- analyze the study proposed Reid and Harrigan [1]

- they also examined the theft of 25k BTC reported in the bitcoin forums

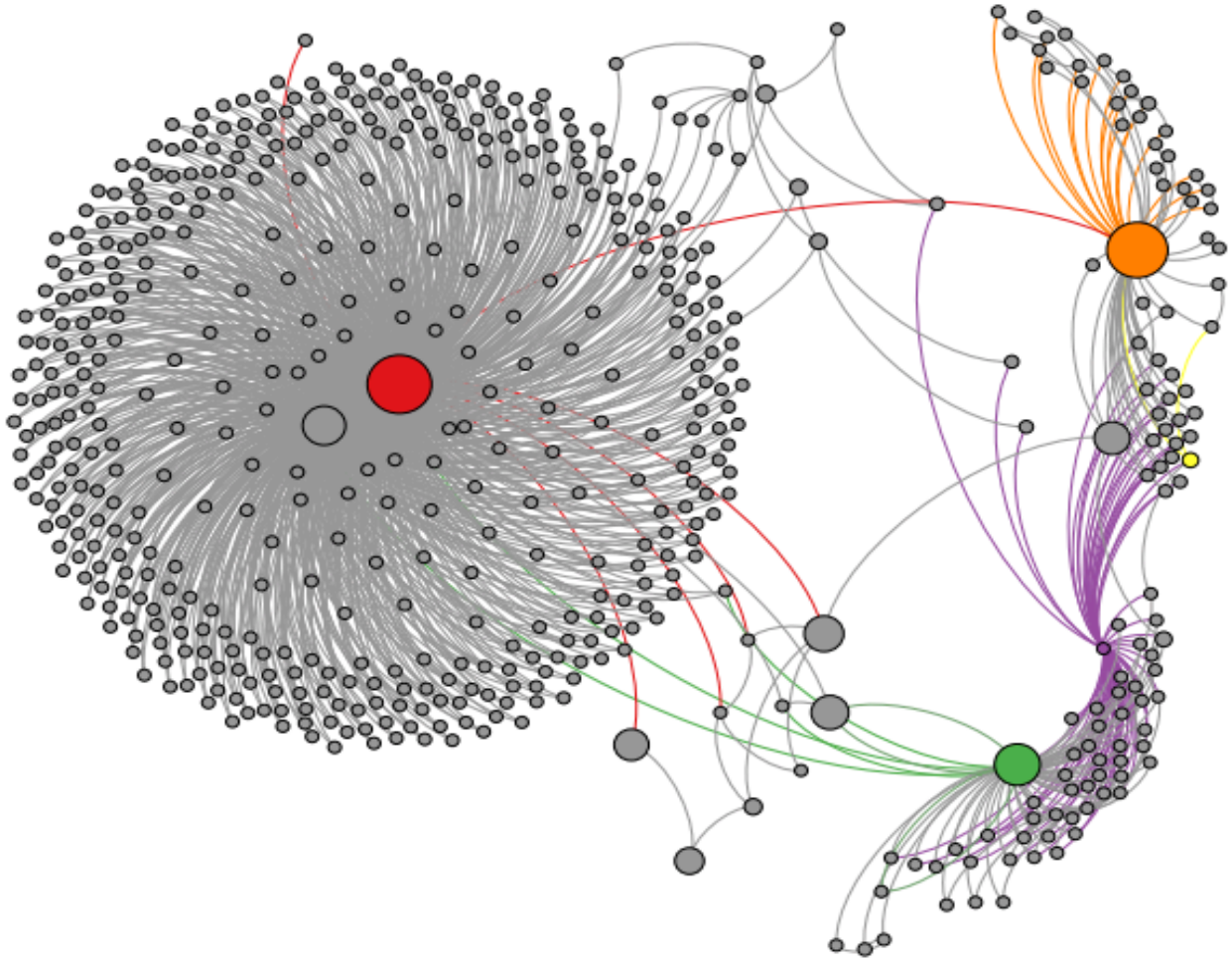
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums

- attacker broke into allinvain's Slush pool account and changed the payout address as his address

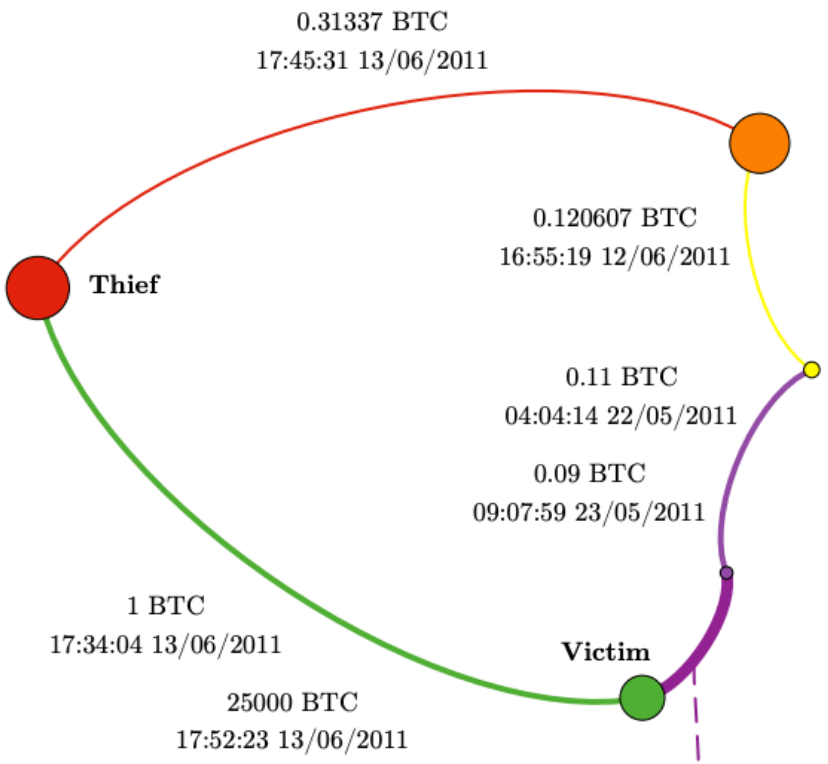
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums



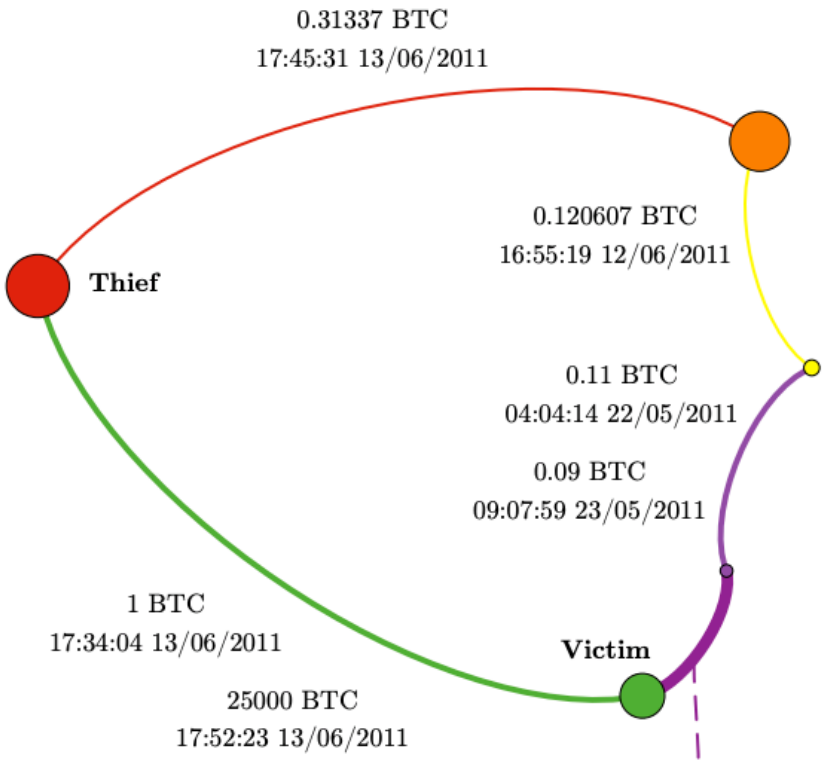
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums
- they deduced that thief address belongs to allinvain



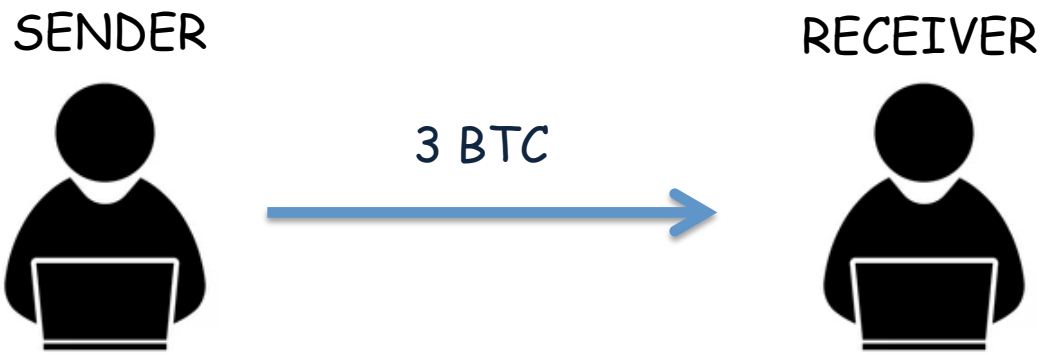
Privacy Issues

- analyze the study proposed Reid and Harrigan [1]
- they also examined the theft of 25k BTC reported in the bitcoin forums
- they deduced that thief address belongs to allinvain



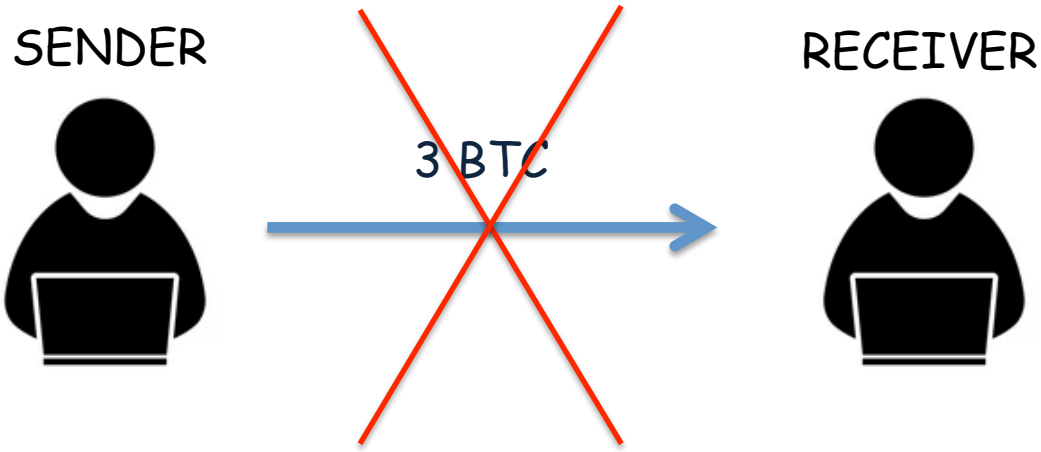
he even tried to associate the thief with the hacker group LulcSec by creating a transaction from hacker to that group

Privacy Enhancing Techniques



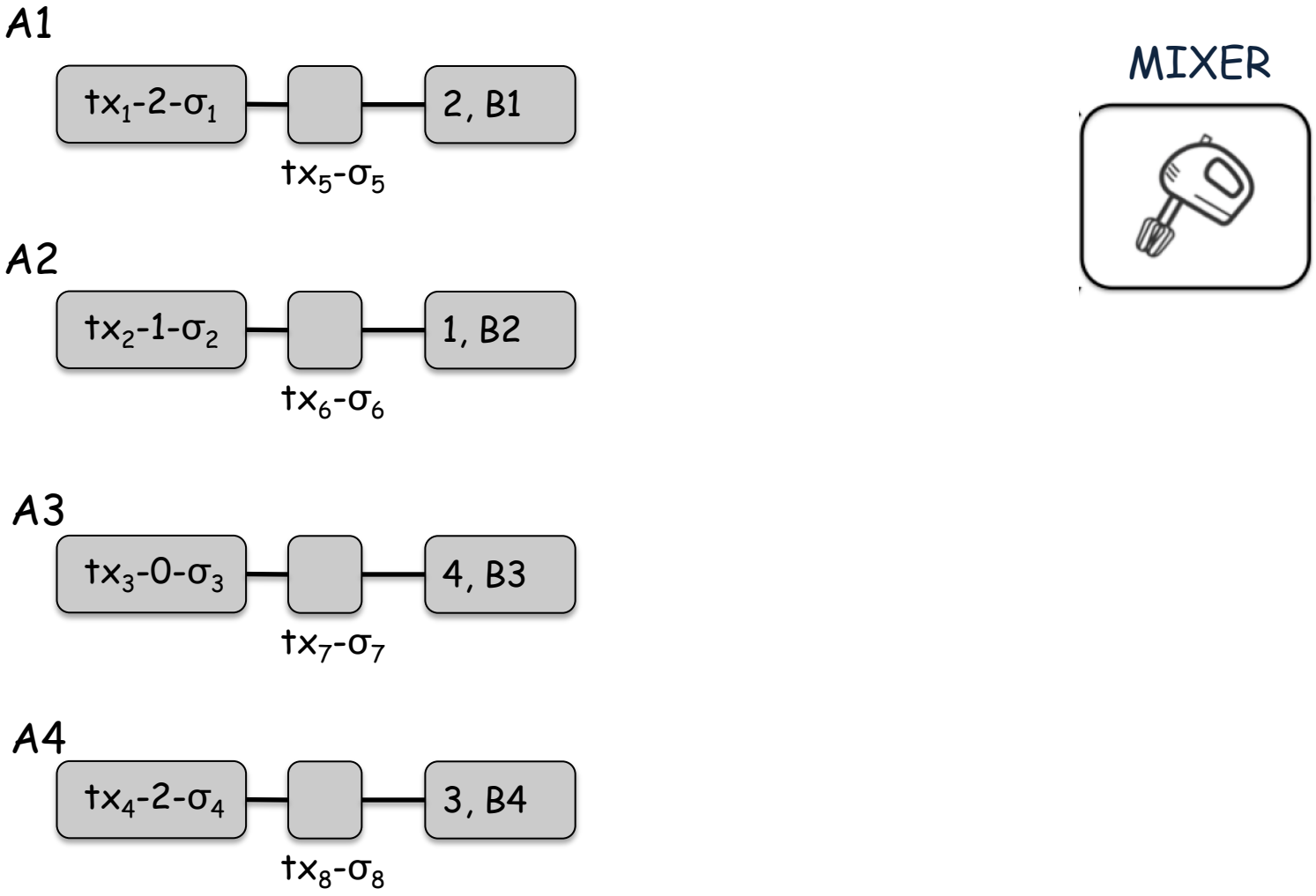
Privacy Enhancing Techniques

- break the link between source and destination address



Privacy Enhancing Techniques - Mixing

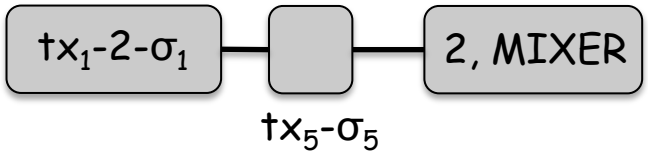
- break the link between source and destination address



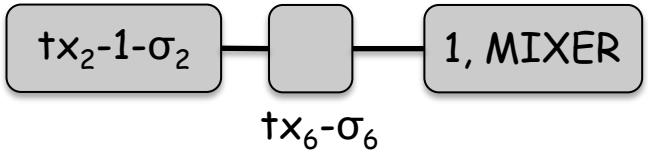
Privacy Enhancing Techniques - Mixing

- break the link between source and destination address

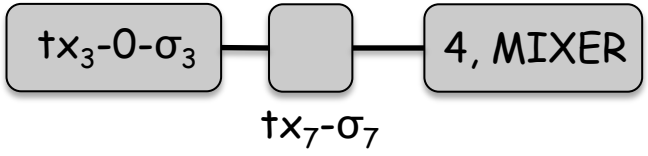
A1



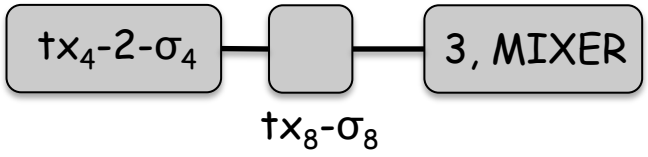
A2



A3



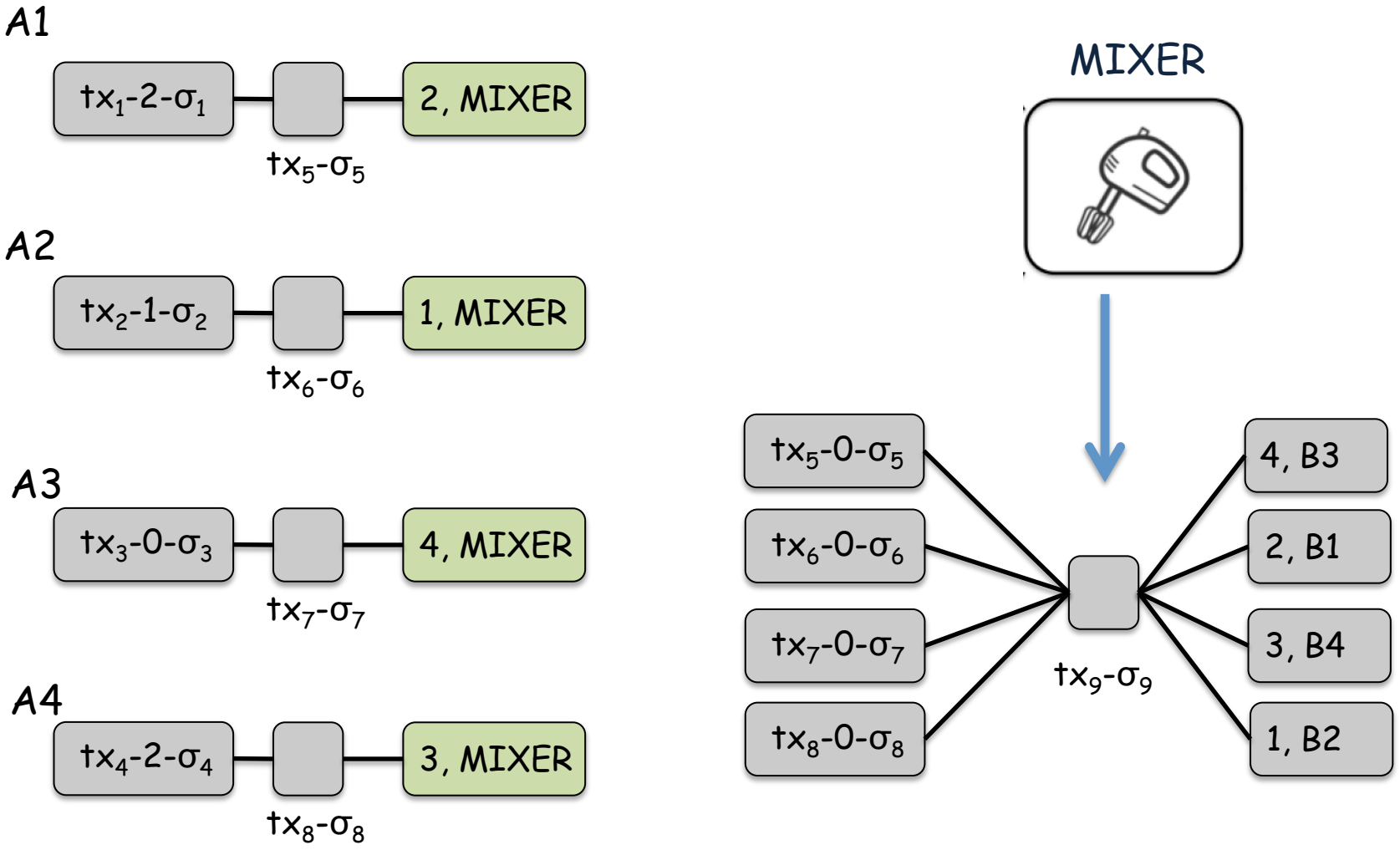
A4



MIXER

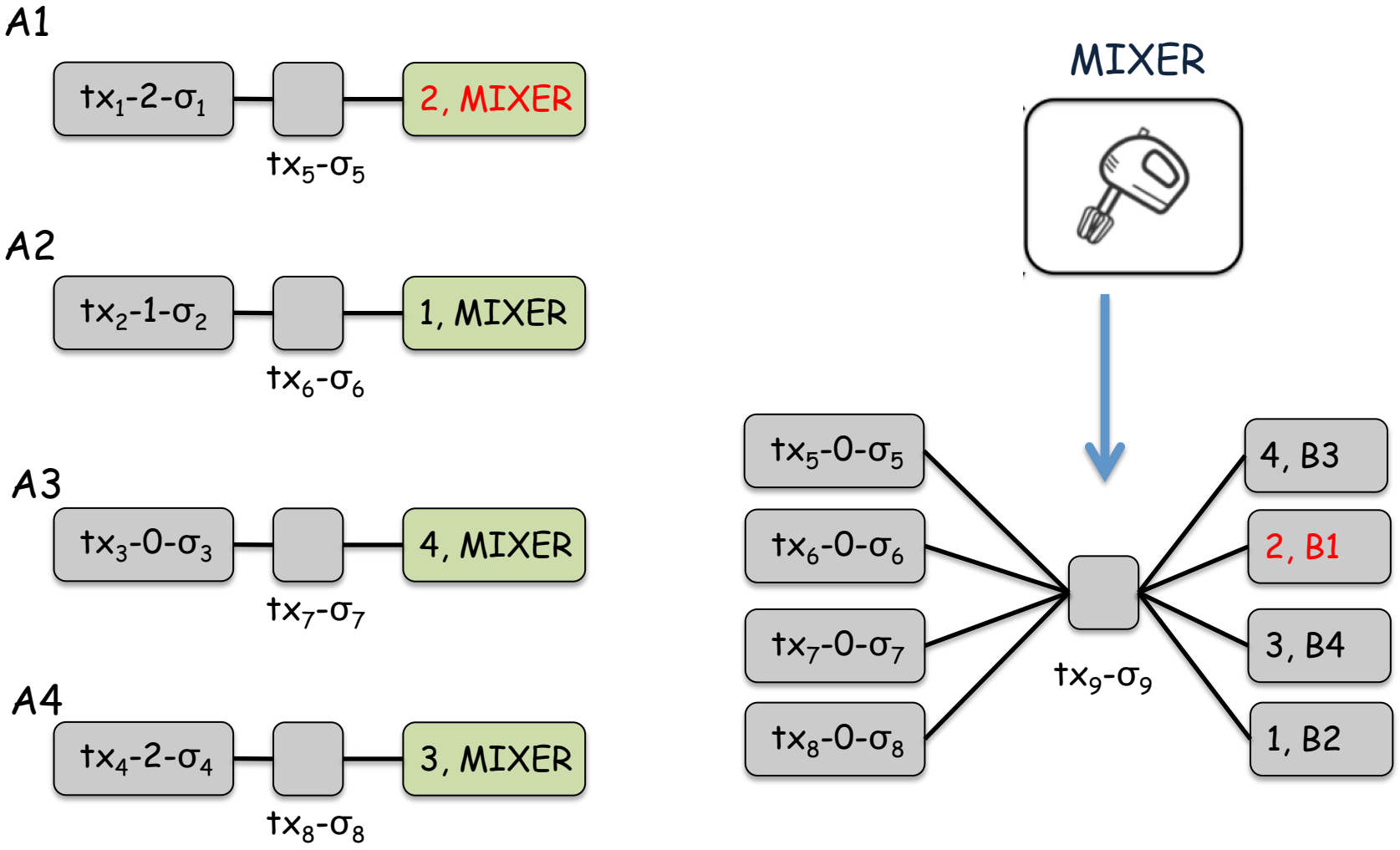
Privacy Enhancing Techniques - Mixing

- break the link between source and destination address



Privacy Enhancing Techniques - Mixing

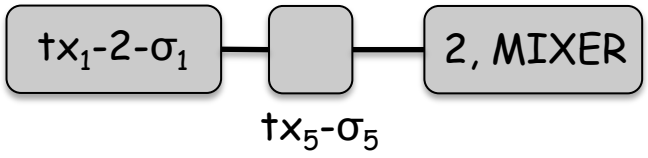
- break the link between source and destination address



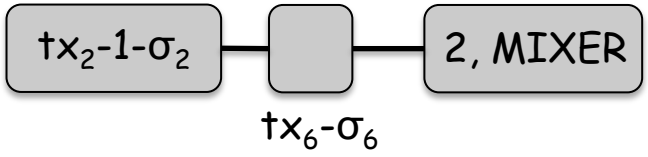
Privacy Enhancing Techniques - Mixing

- break the link between source and destination address

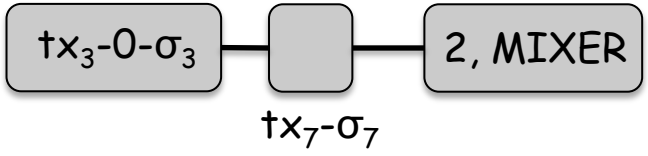
A1



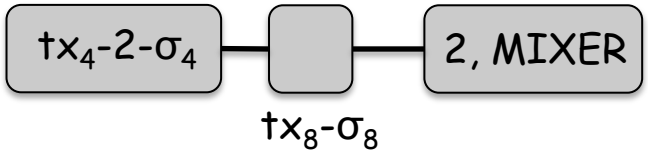
A2



A3



A4

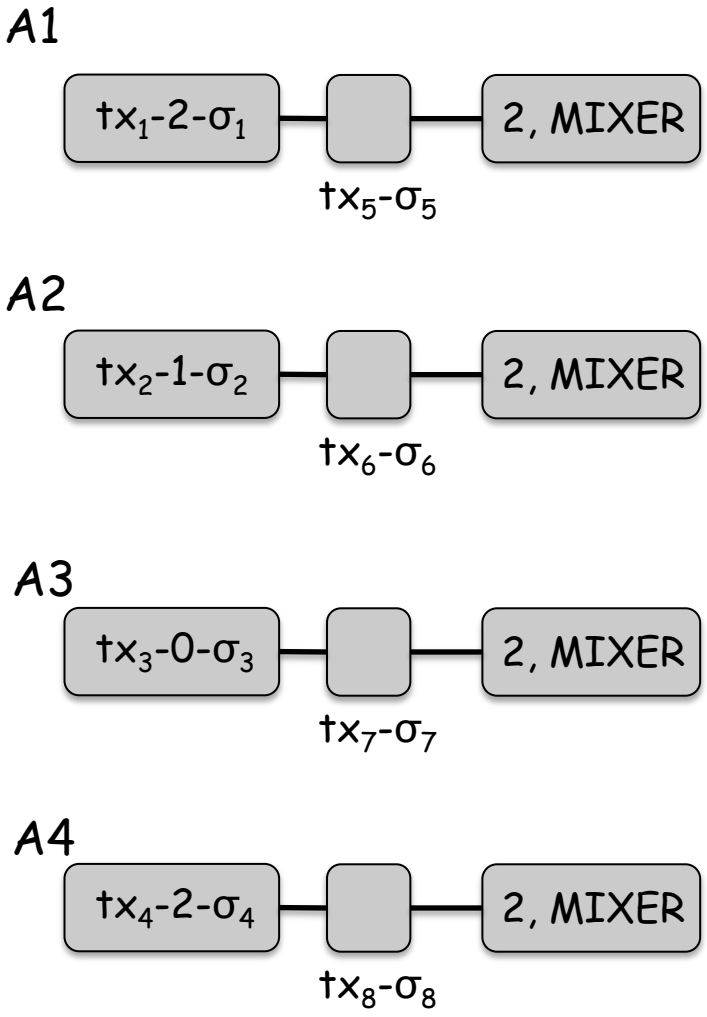


MIXER

- transaction amount should be same to be indistinguishable

Privacy Enhancing Techniques - Mixing

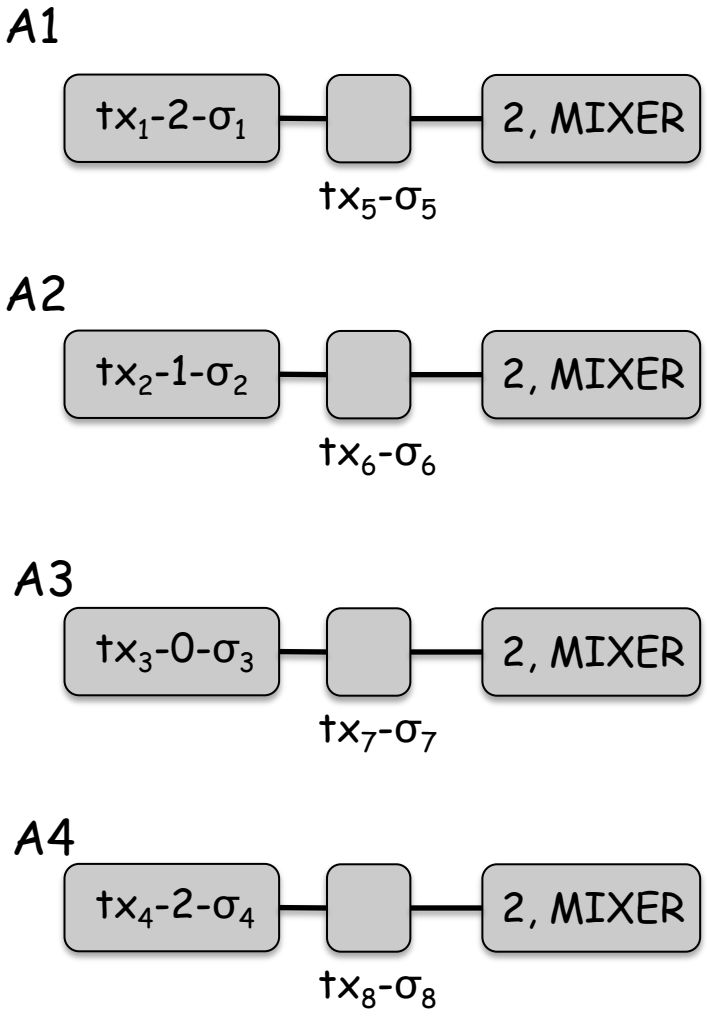
- break the link between source and destination address



- transaction amount should be same to be indistinguishable
- mixer should be trusted

Privacy Enhancing Techniques - Mixing

- break the link between source and destination address



- transaction amount should be same to be indistinguishable
- mixer should be trusted
  - it can steal the money
  - it knows all the senders and receivers addresses, it can reveal that information

Privacy Enhancing Techniques - Mixing

Mixcoin

- introduced by Bonneau et al. [2] in 2014

Mixcoin

- introduced by Bonneau et al. [2] in 2014

- before sending bitcoin, sender takes a signed warrant from the mixer stating that

  if the mixer gets x bitcoin from A by time t, it will send x' bitcoin to B by time t'

Mixcoin

- introduced by Bonneau et al. [2] in 2014

- before sending bitcoin, sender takes a signed warrant from the mixer stating that

  if the mixer gets x bitcoin from A by time t, it will send x' bitcoin to B by time t'

- if mixer steals the money, A publishes the warrant to ruin mixer's reputation

Mixcoin

- introduced by Bonneau et al. [2] in 2014
- before sending bitcoin, sender takes a signed warrant from the mixer stating that

  if the mixer gets x bitcoin from A by time t, it will send x' bitcoin to B by time t'

- if mixer steals the money, A publishes the warrant to ruin mixer's reputation
- mixer may reveal the sender's and receiver's address

Privacy Enhancing Techniques - Mixing

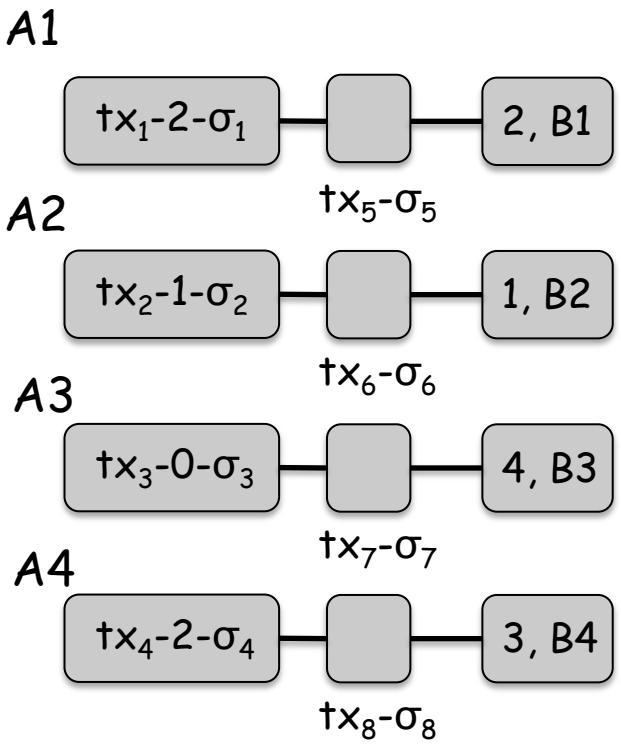
CoinJoin

- introduced by Maxwell [3] in 2013

Privacy Enhancing Techniques - Mixing

CoinJoin

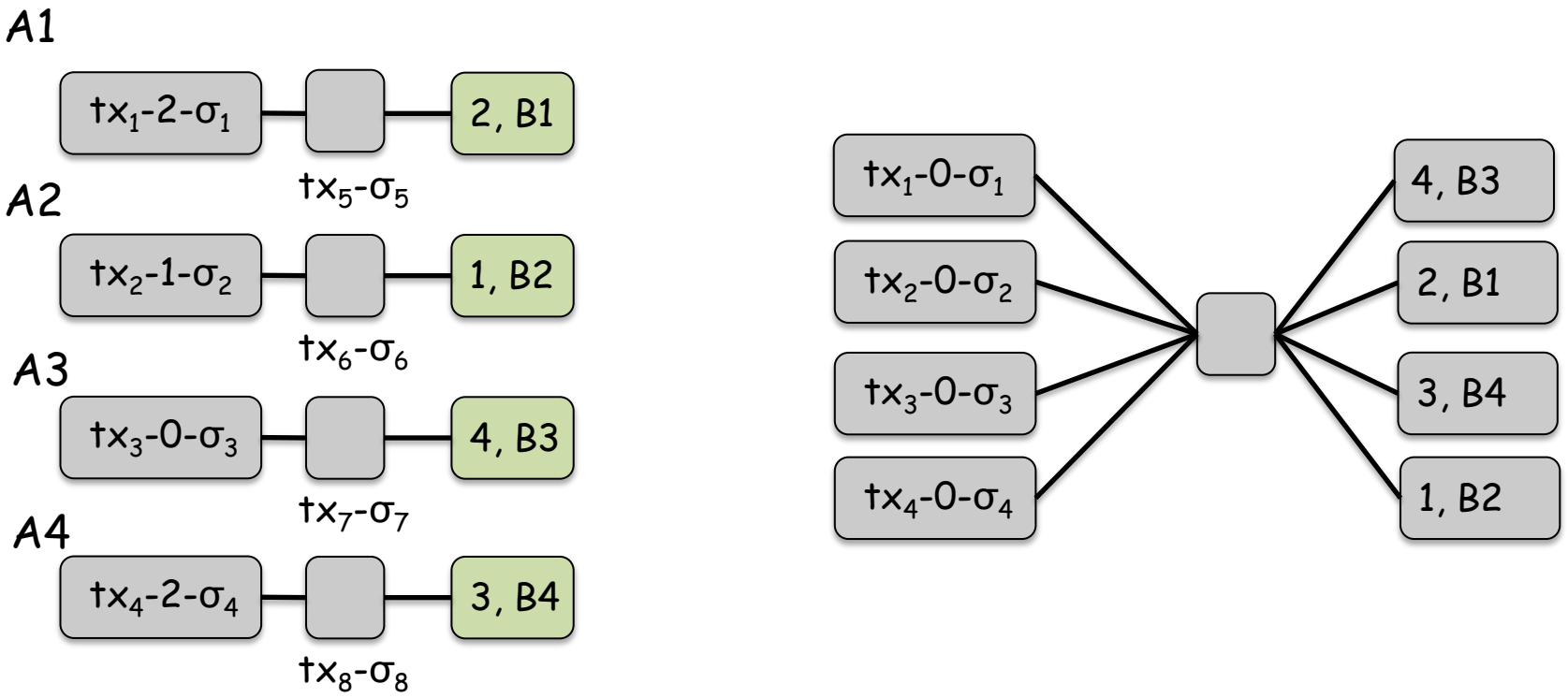
- introduced by Maxwell [3] in 2013



Privacy Enhancing Techniques - Mixing

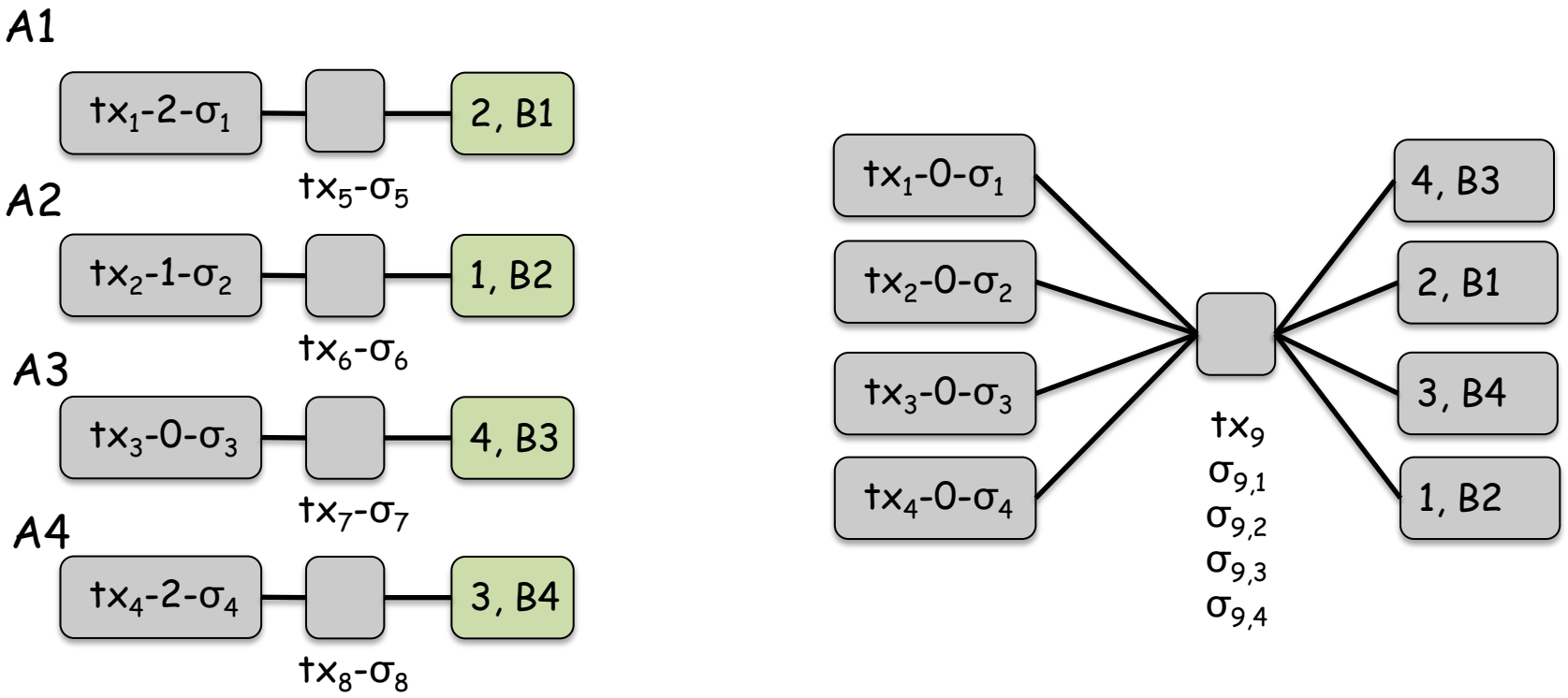
CoinJoin

- introduced by Maxwell [3] in 2013



CoinJoin

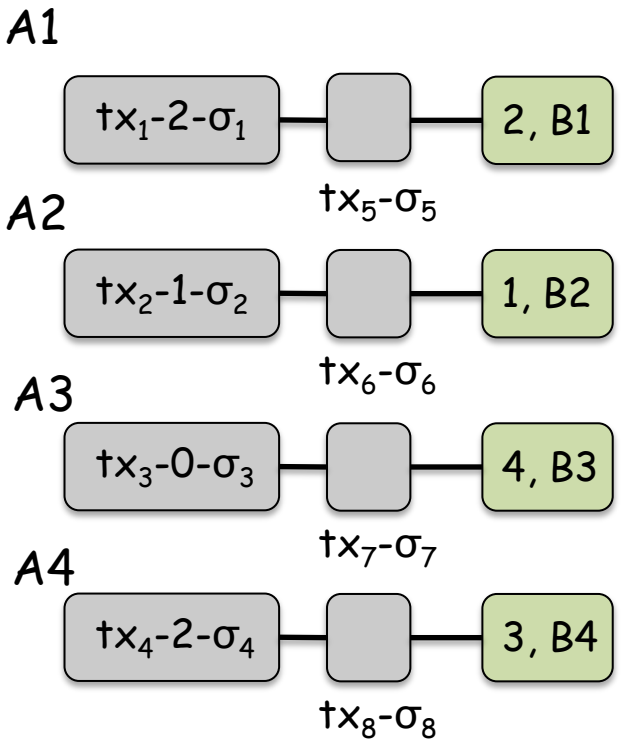
- introduced by Maxwell [3] in 2013



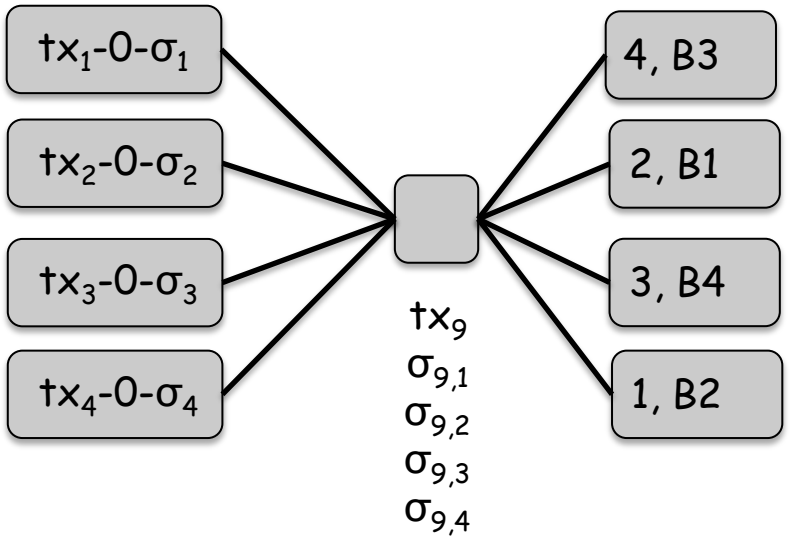
Privacy Enhancing Techniques - Mixing

CoinJoin

- introduced by Maxwell [3] in 2013



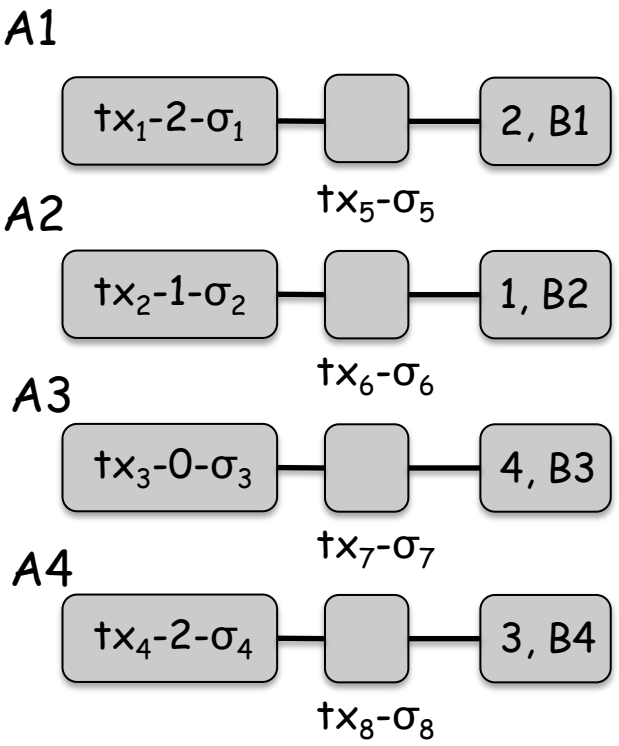
- insiders can reveal the link of each transaction



Privacy Enhancing Techniques - Mixing

CoinShuffle

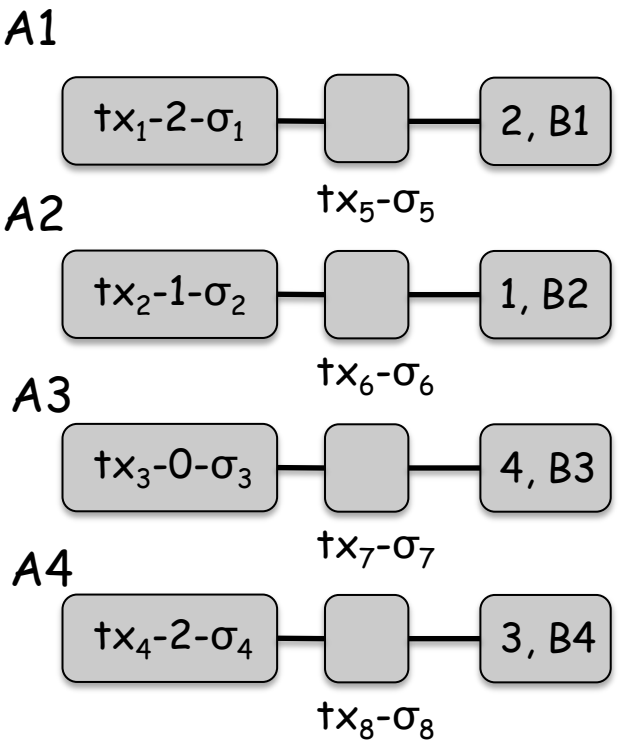
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

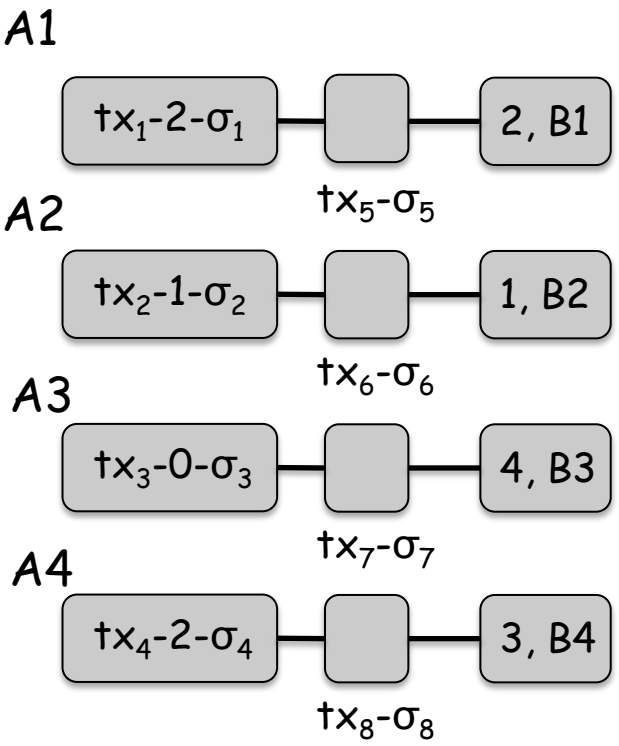
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

- introduced by Ruffing et al. [4] in 2014

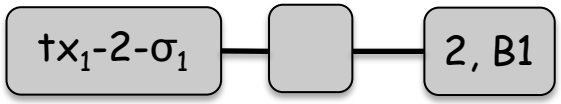


Privacy Enhancing Techniques - Mixing

CoinShuffle

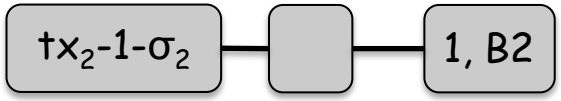
- introduced by Ruffing et al. [4] in 2014

A1



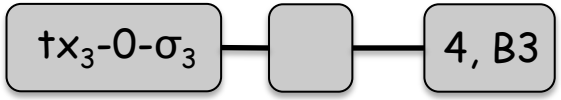
tx_5-σ_5

A2



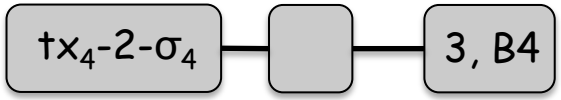
tx_6-σ_6

A3



tx_7-σ_7

A4



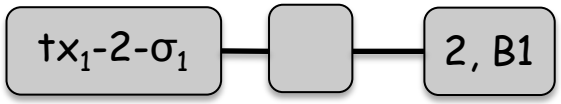
tx_8-σ_8

Privacy Enhancing Techniques - Mixing

CoinShuffle

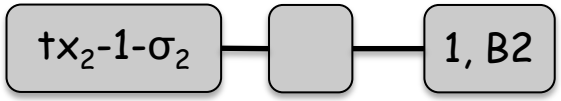
- introduced by Ruffing et al. [4] in 2014

A1



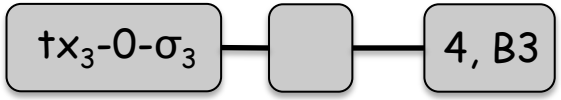
tx_5-σ_5

A2



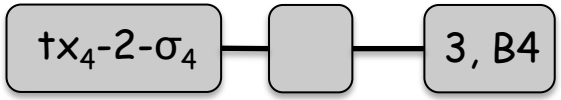
tx_6-σ_6

A3



tx_7-σ_7

A4

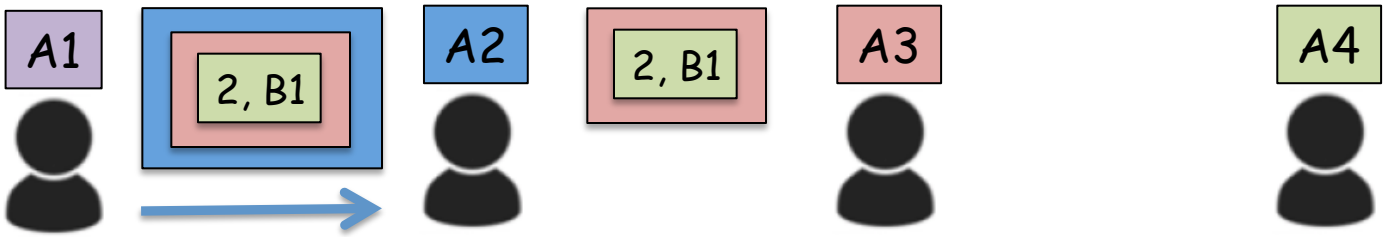


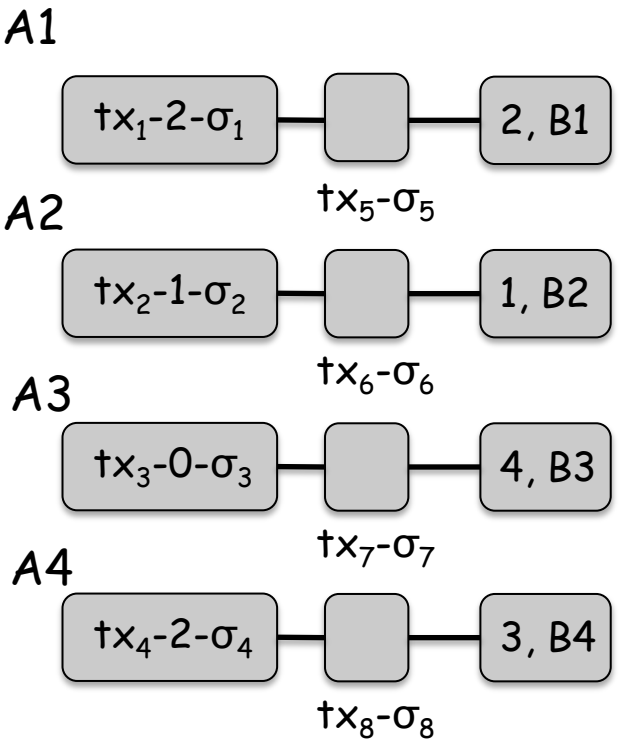
tx_8-σ_8

Privacy Enhancing Techniques - Mixing

CoinShuffle

- introduced by Ruffing et al. [4] in 2014

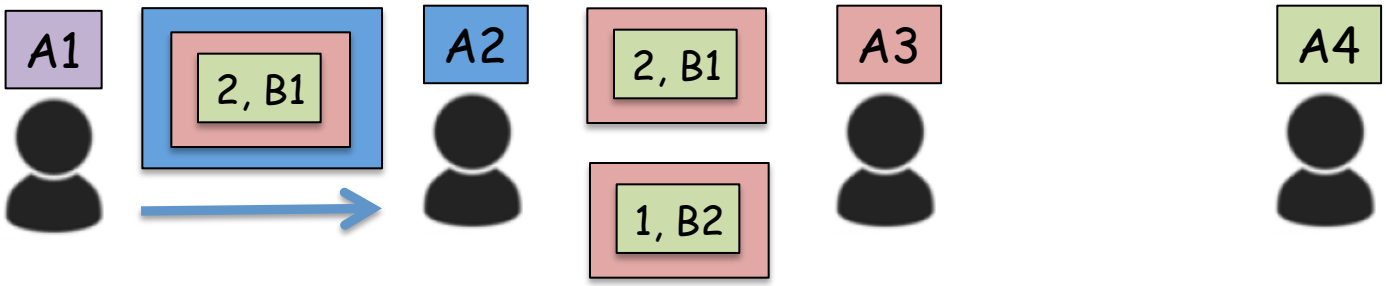




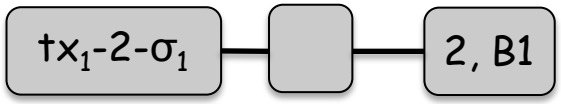
Privacy Enhancing Techniques - Mixing

CoinShuffle

- introduced by Ruffing et al. [4] in 2014

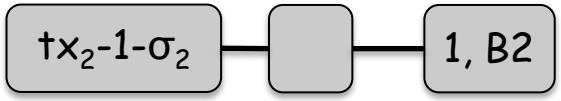


A1



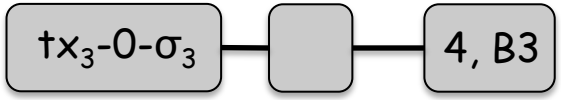
tx_5-σ_5

A2



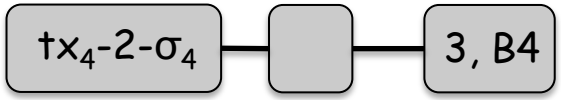
tx_6-σ_6

A3



tx_7-σ_7

A4

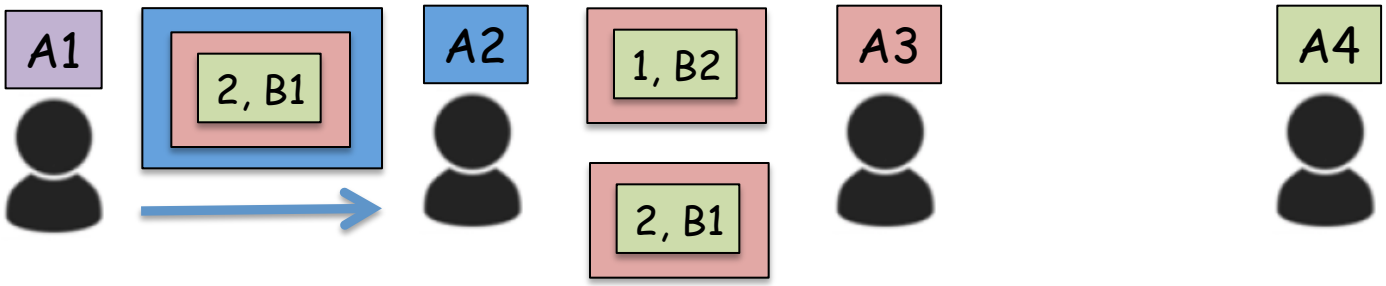


tx_8-σ_8

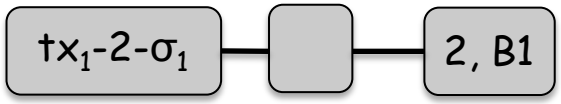
Privacy Enhancing Techniques - Mixing

CoinShuffle

- introduced by Ruffing et al. [4] in 2014

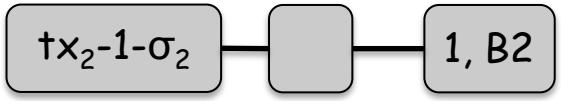


A1



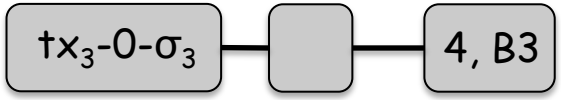
tx_5-σ_5

A2



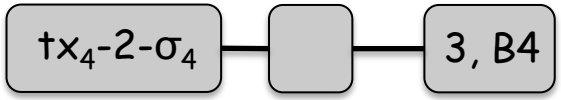
tx_6-σ_6

A3



tx_7-σ_7

A4

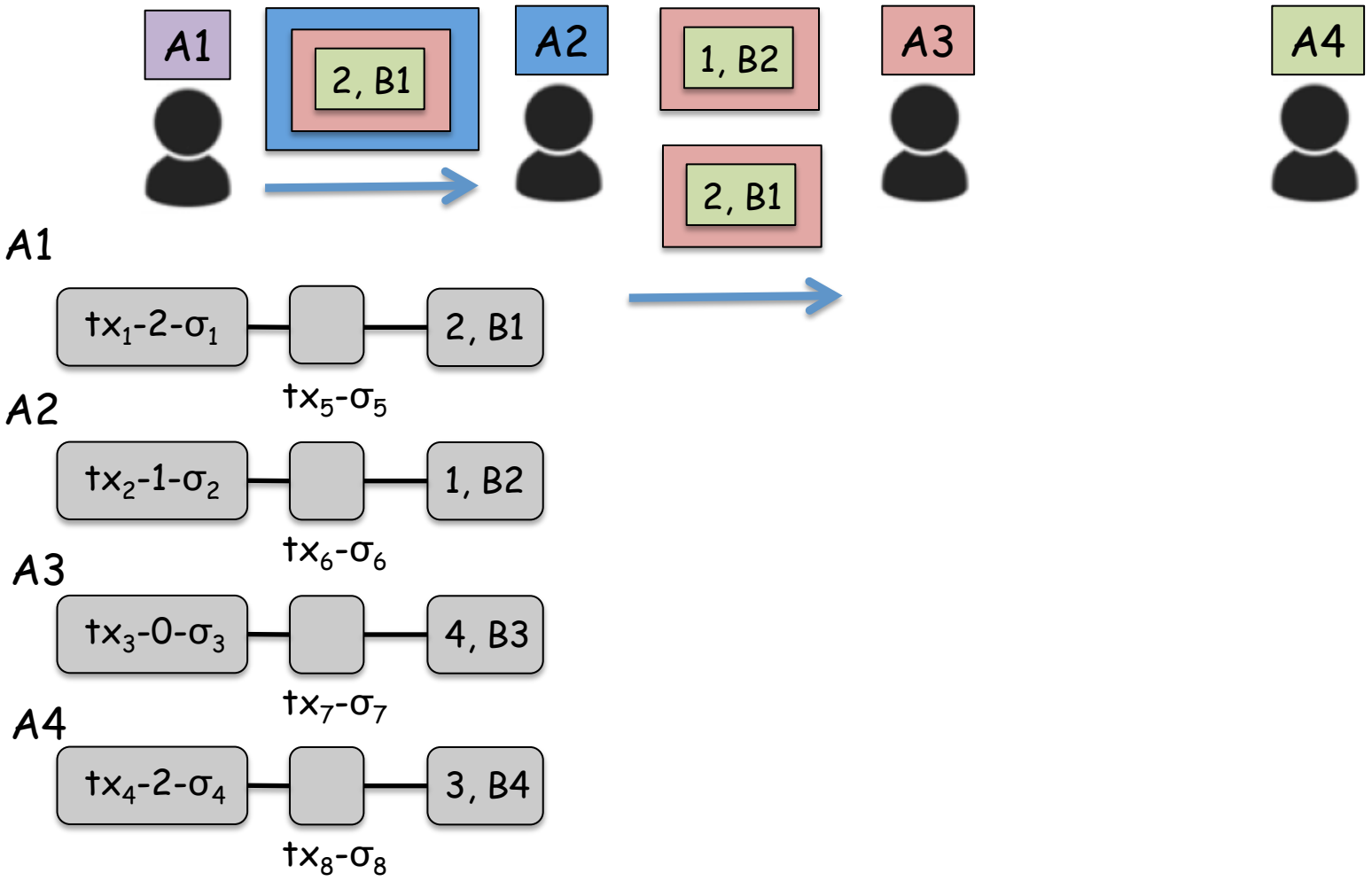


tx_8-σ_8

Privacy Enhancing Techniques - Mixing

CoinShuffle

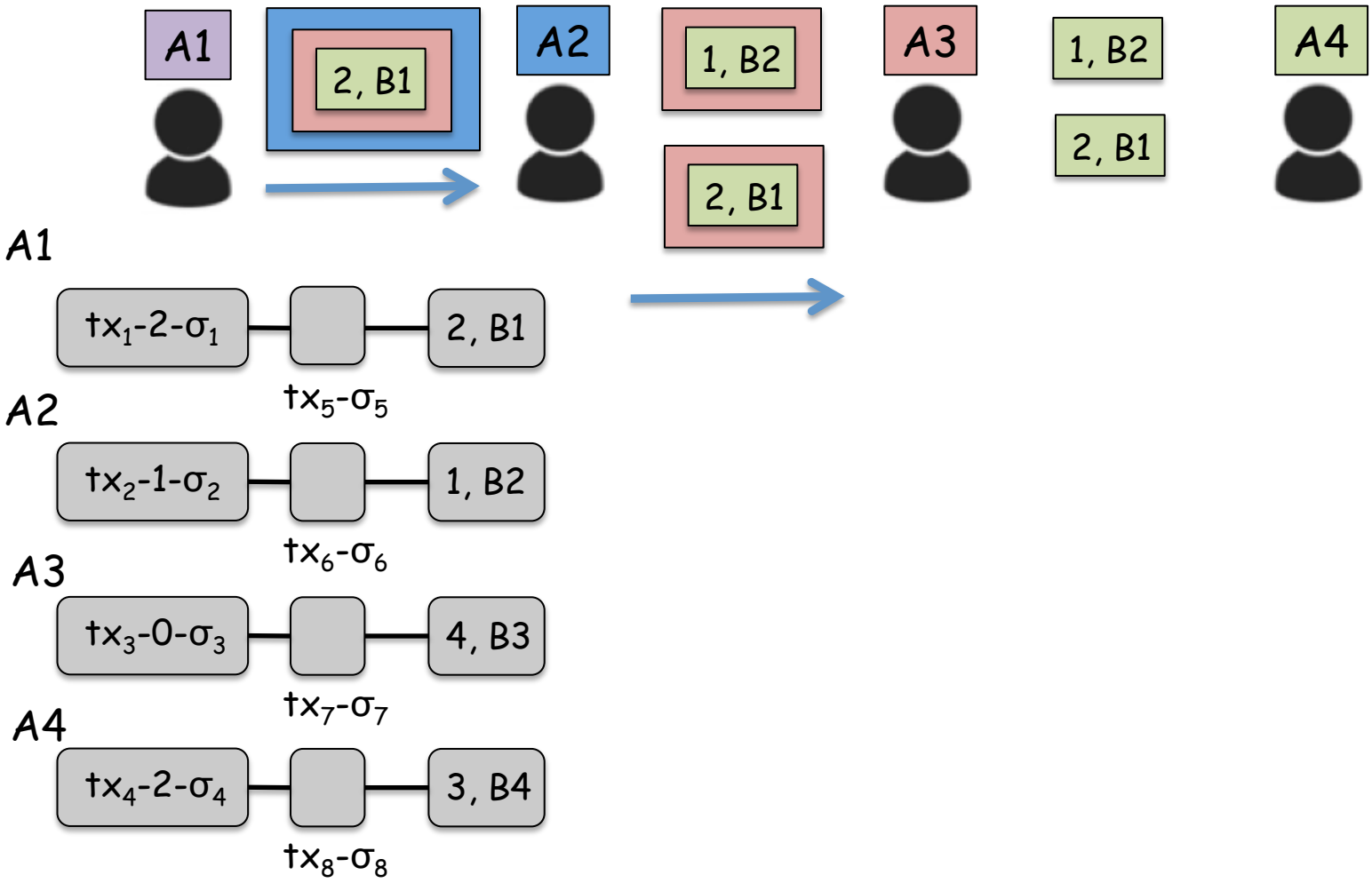
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

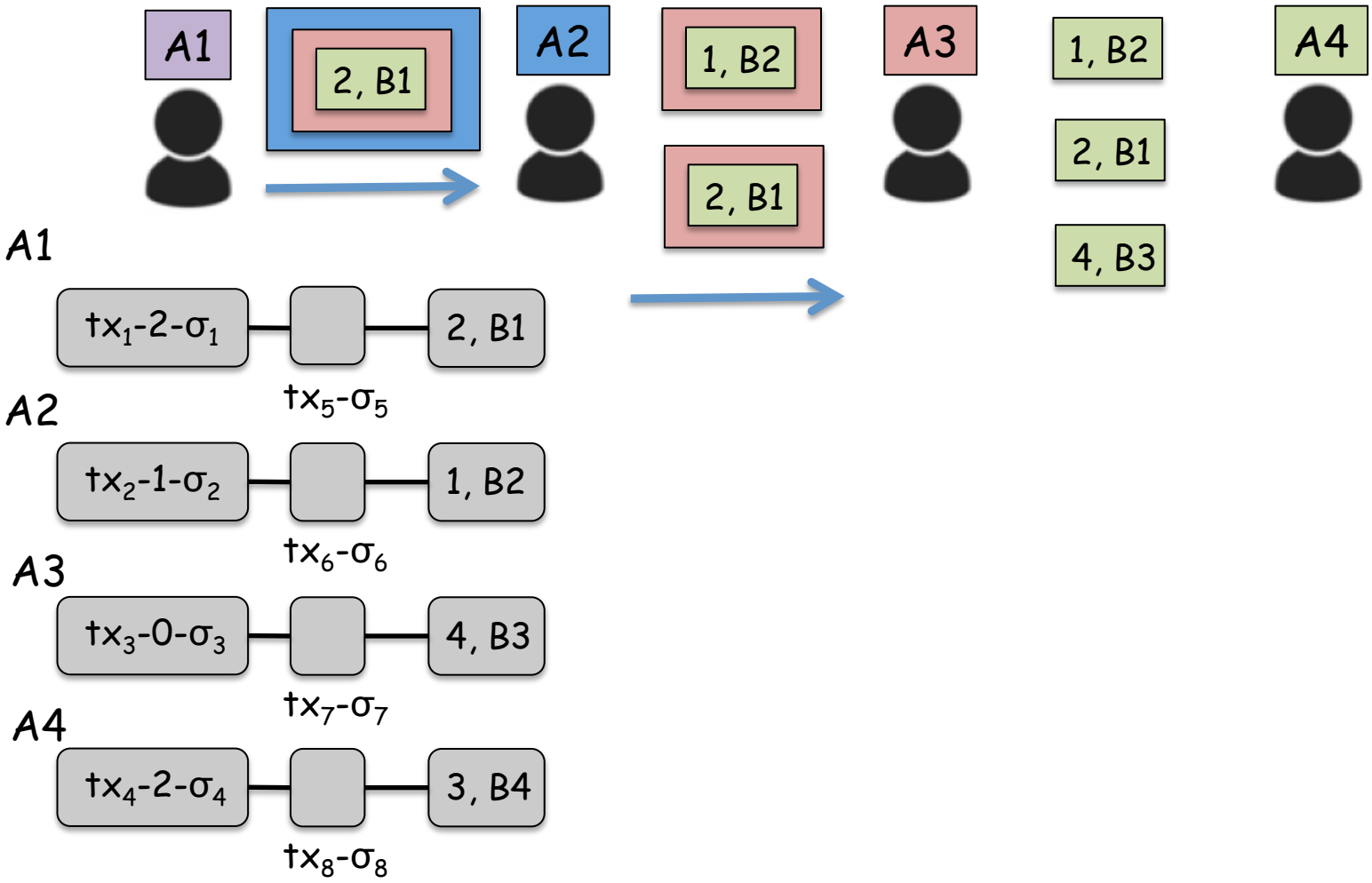
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

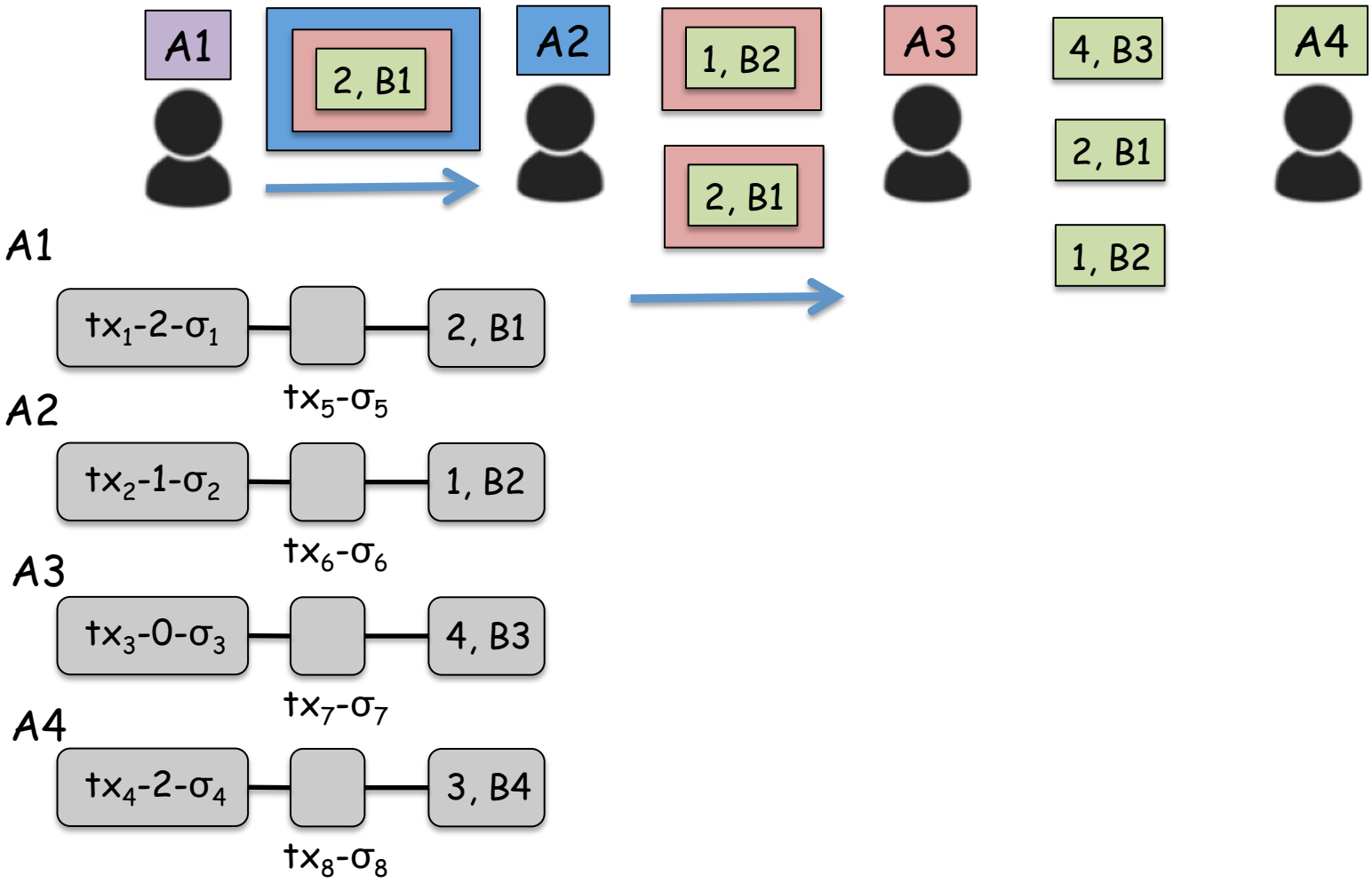
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

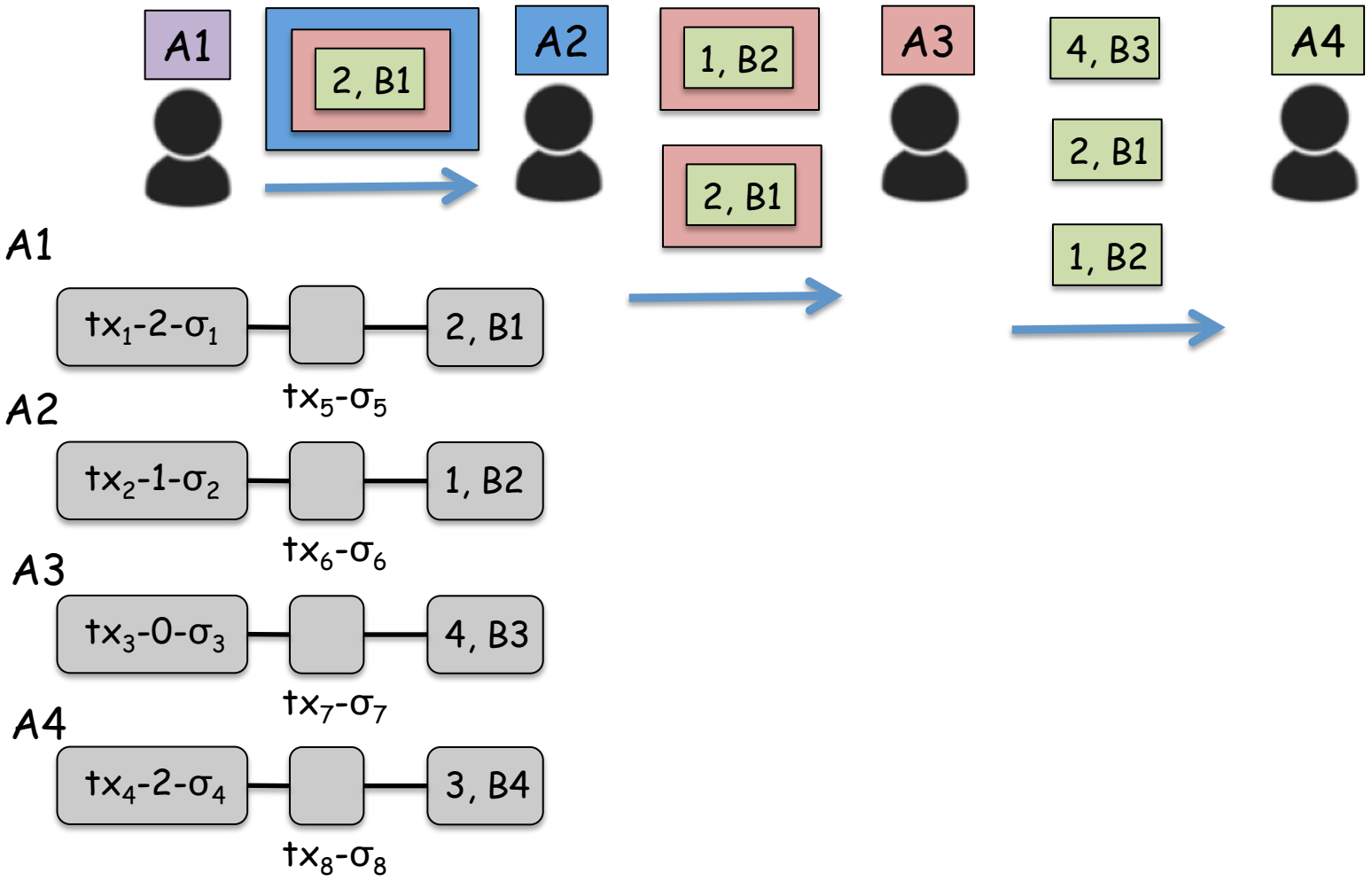
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

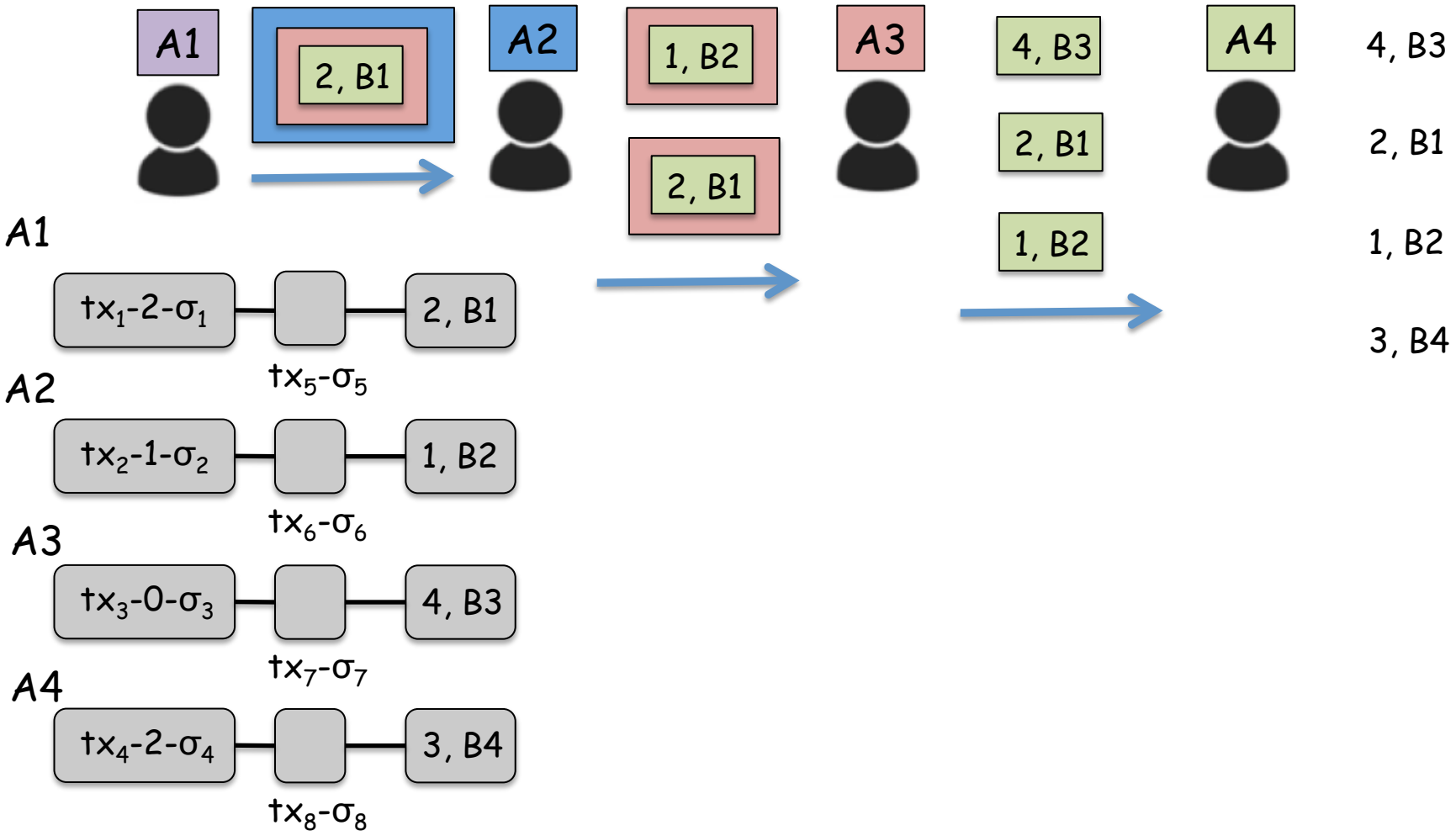
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

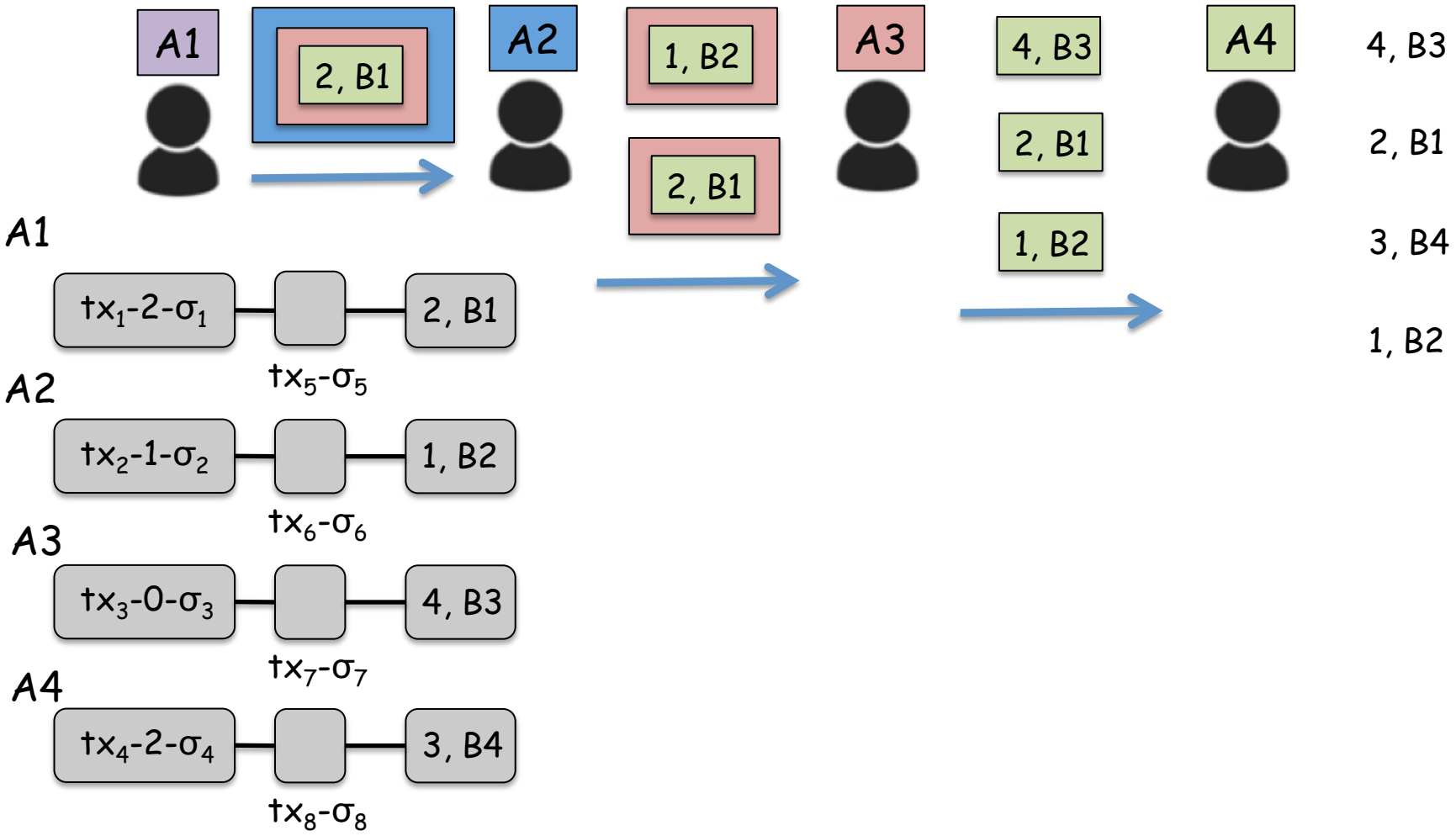
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

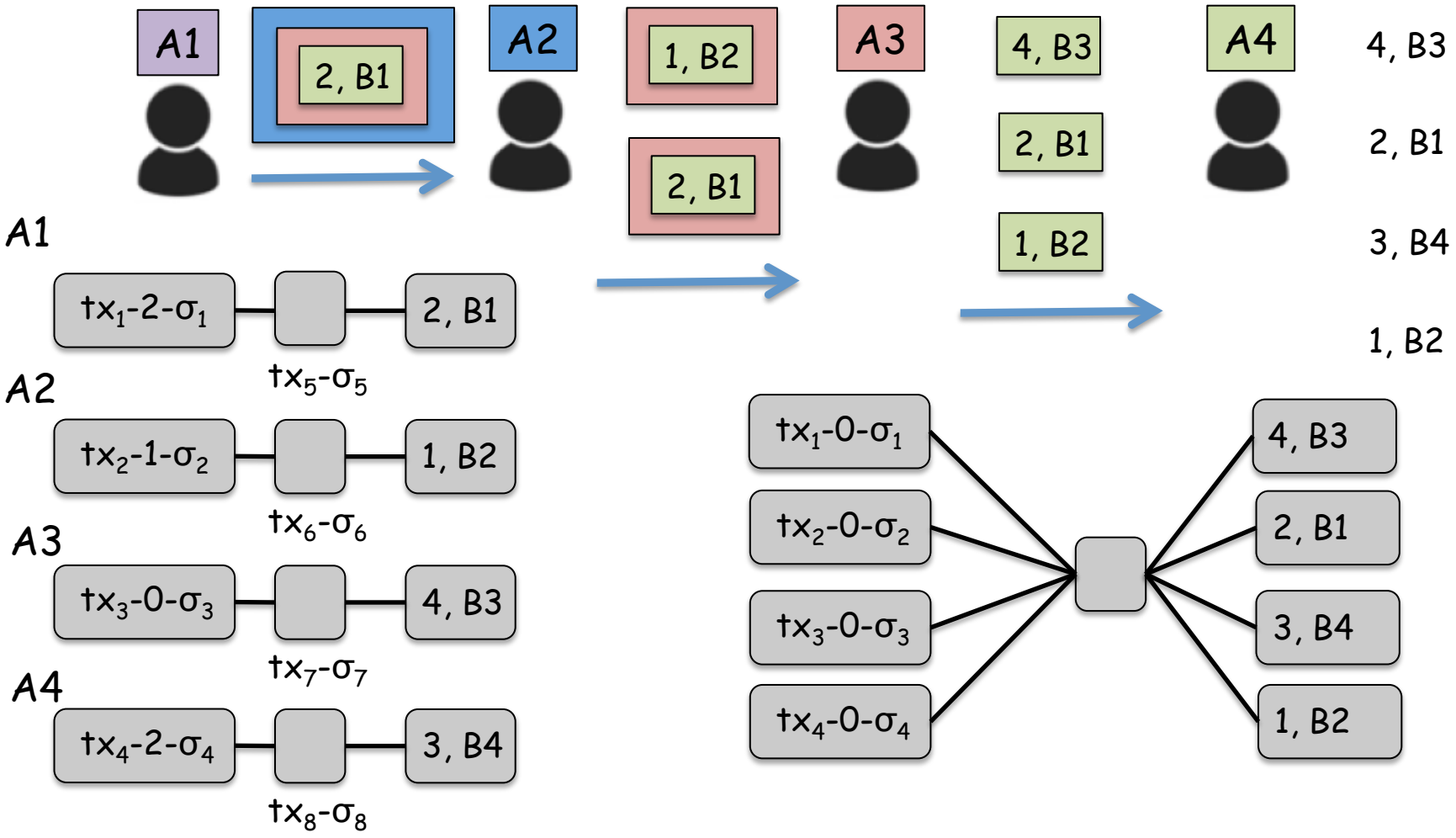
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

CoinShuffle

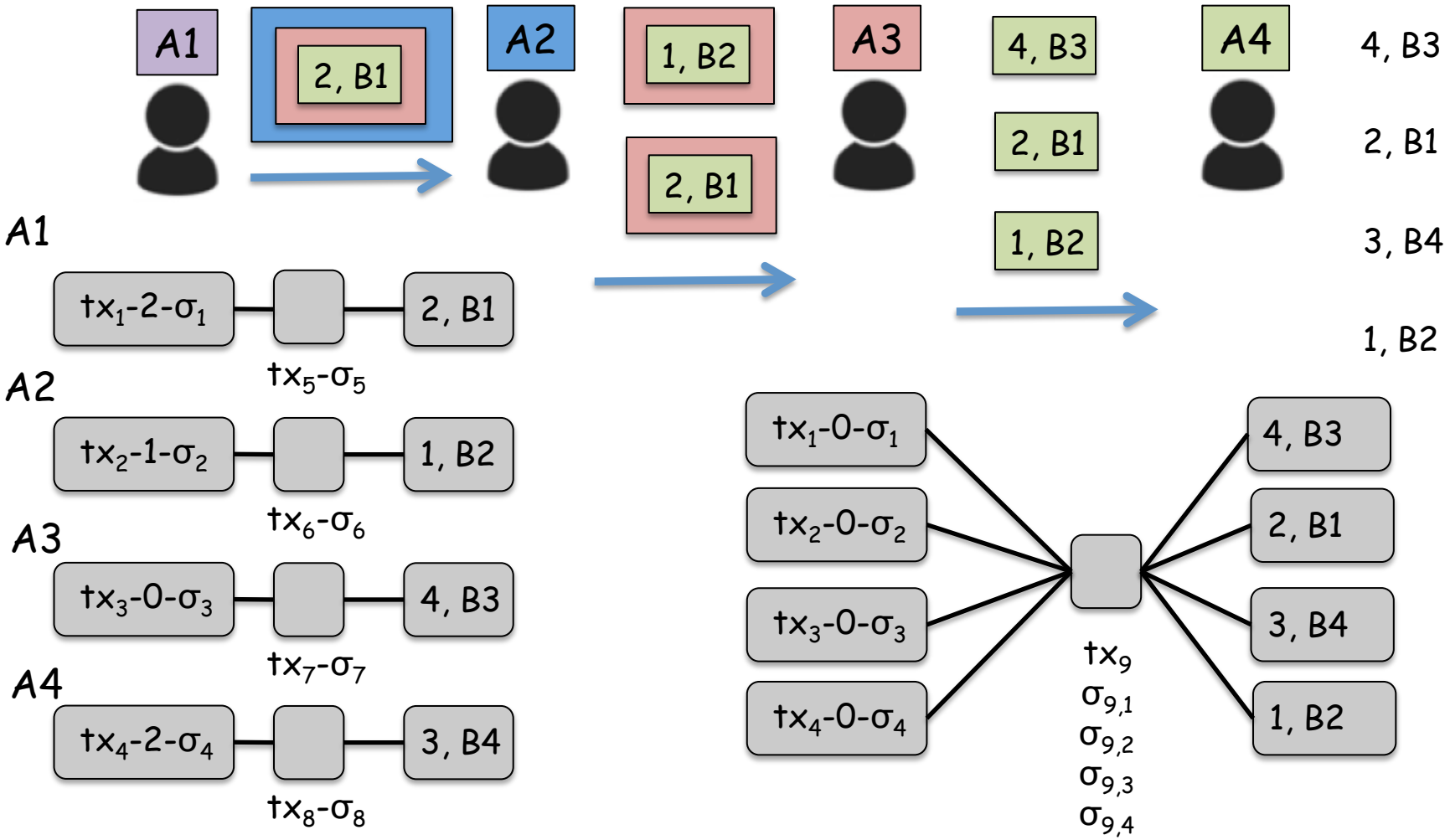
- introduced by Ruffing et al. [4] in 2014



Privacy Enhancing Techniques - Mixing

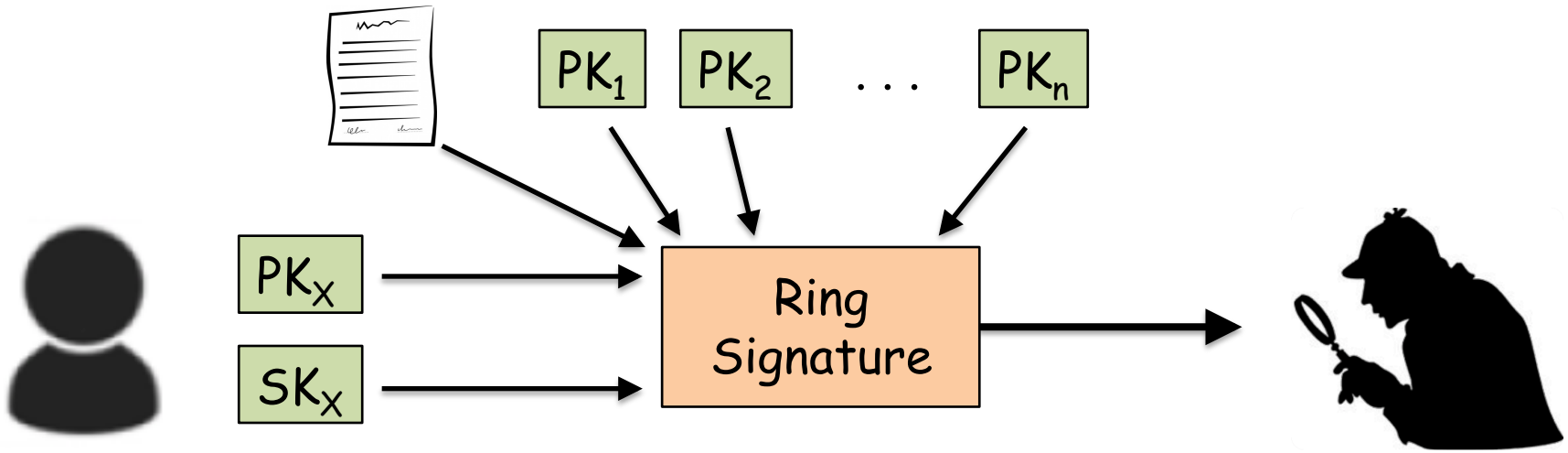
CoinShuffle

- introduced by Ruffing et al. [4] in 2014



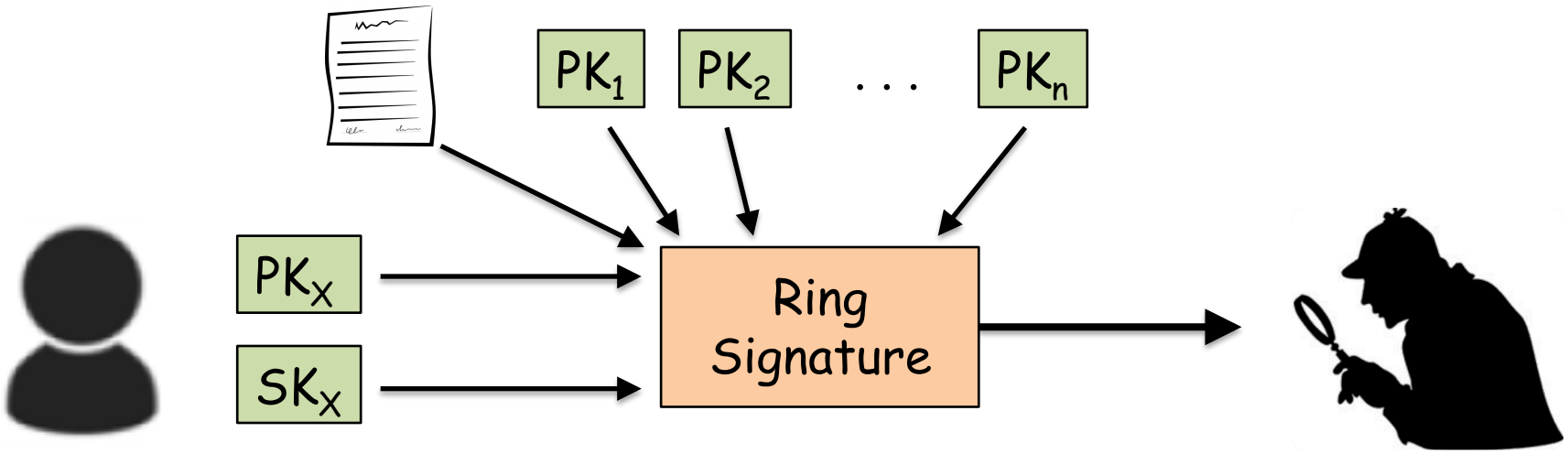
Privacy Enhancing Techniques - Ring Signatures

- introduced by Rivest et al. [5] in 2001



Privacy Enhancing Techniques - Ring Signatures

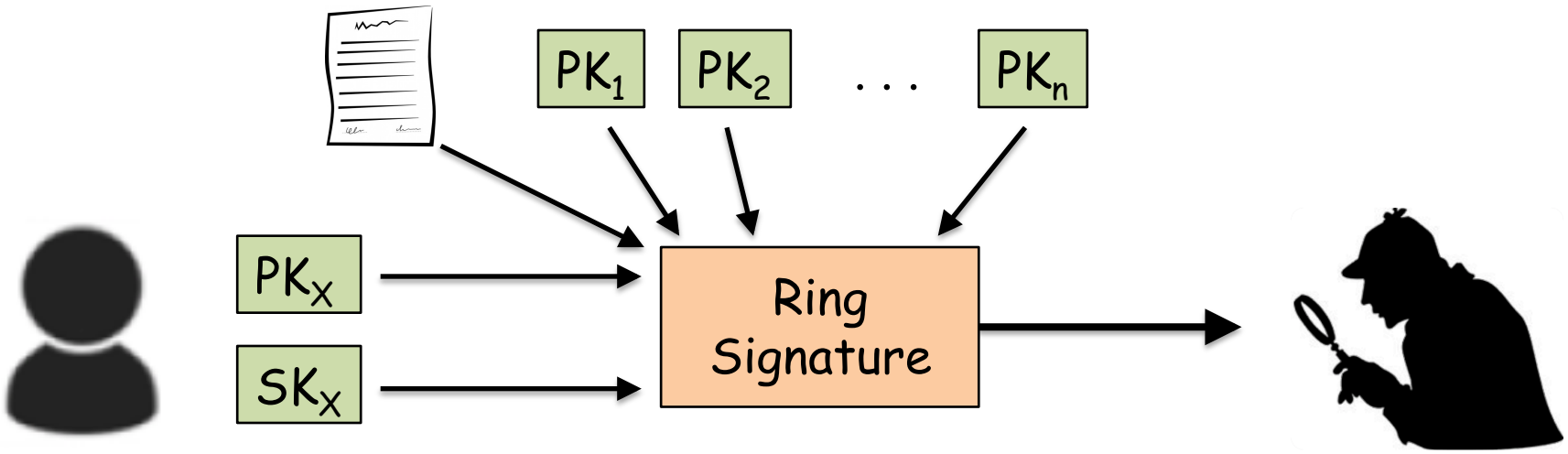
- introduced by Rivest et al. [5] in 2001



- verifier can tell that one member from the set {PK_1, PK_2, …, PK_n, PK_X} signed the message, but cannot tell which one the actual signer

Privacy Enhancing Techniques - Ring Signatures

- introduced by Rivest et al. [5] in 2001

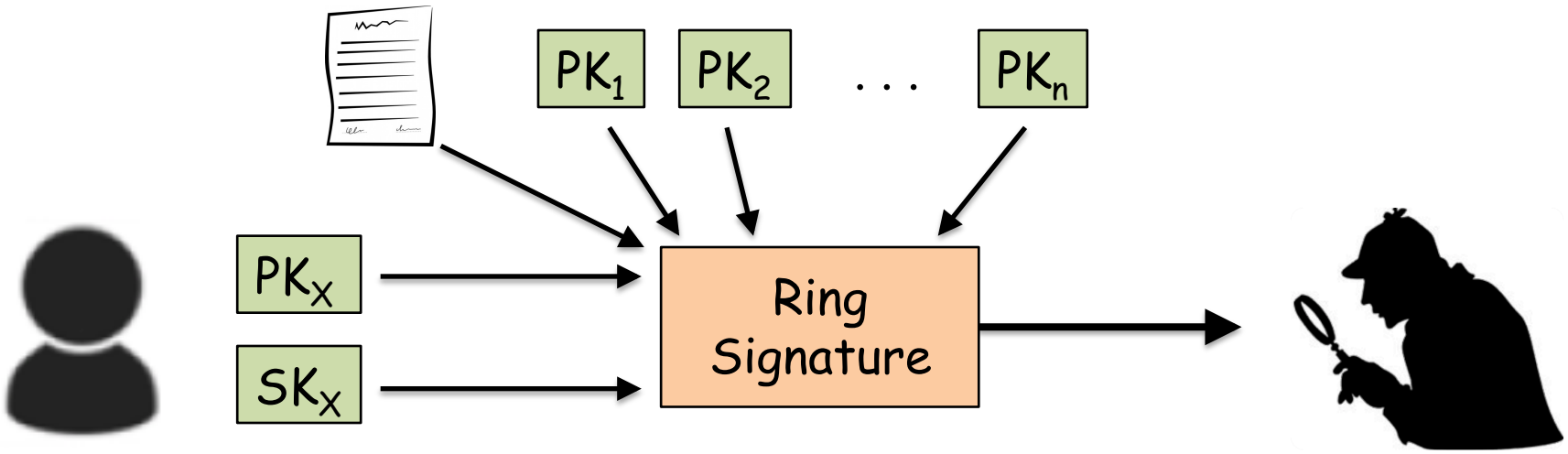


- verifier can tell that one member from the set $\{PK_1, PK_2, \ldots, PK_n, PK_X\}$ signed the message, but cannot tell which one the actual signer

- assume you designing a voting scheme using ring signatures
  - one can vote for two different candidate without being detected

Privacy Enhancing Techniques - Ring Signatures

- introduced by Rivest et al. [5] in 2001



- verifier can tell that one member from the set $\{PK_1, PK_2, \ldots, PK_n, PK_X\}$ signed the message, but cannot tell which one the actual signer

- assume you designing a voting scheme using ring signatures
  - one can vote for two different candidate without being detected
  - traceable ring signatures, introduced by Fujisaka and Suzuki [6] in 2007, enabling us to detect if two signatures produced by same user

Privacy Enhancing Techniques - Ring Signatures

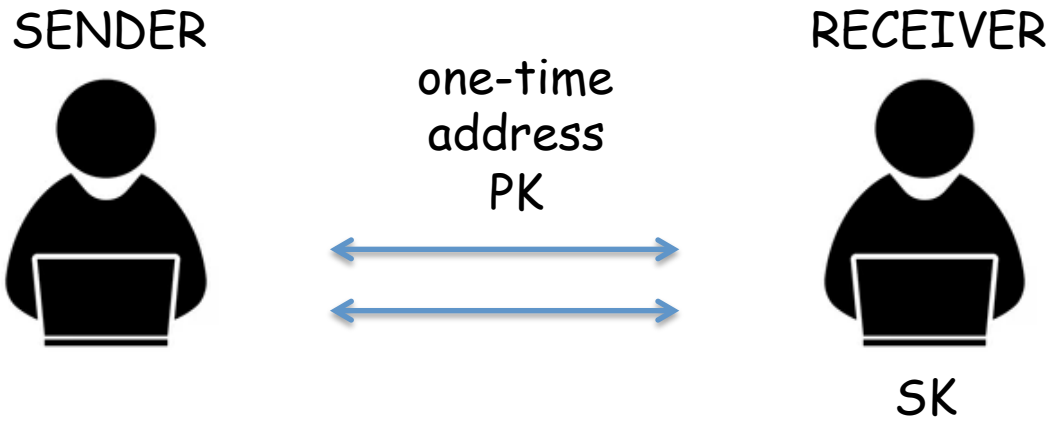
CryptoNote

- introduced by van Saberhagen [7] in 2013

Privacy Enhancing Techniques - Ring Signatures

CryptoNote

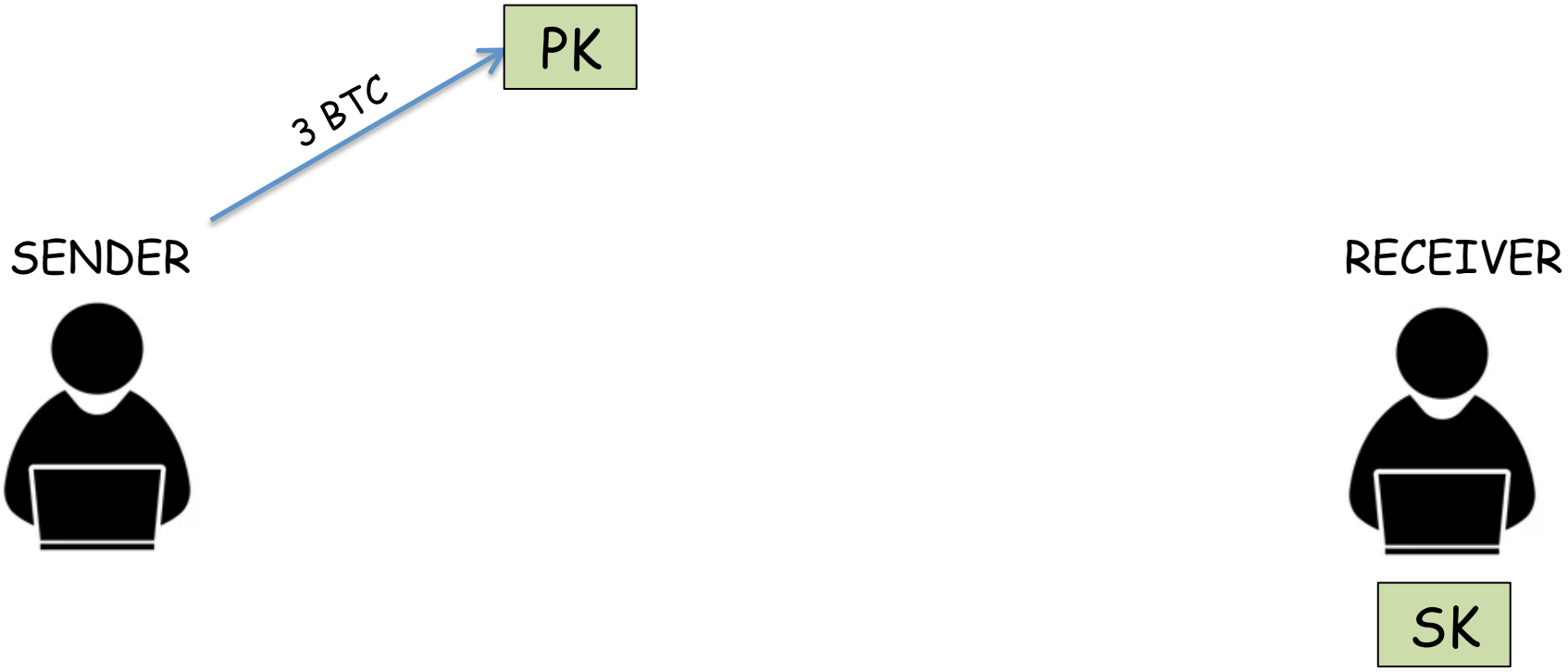
- introduced by van Saberhagen [7] in 2013



Privacy Enhancing Techniques - Ring Signatures

CryptoNote

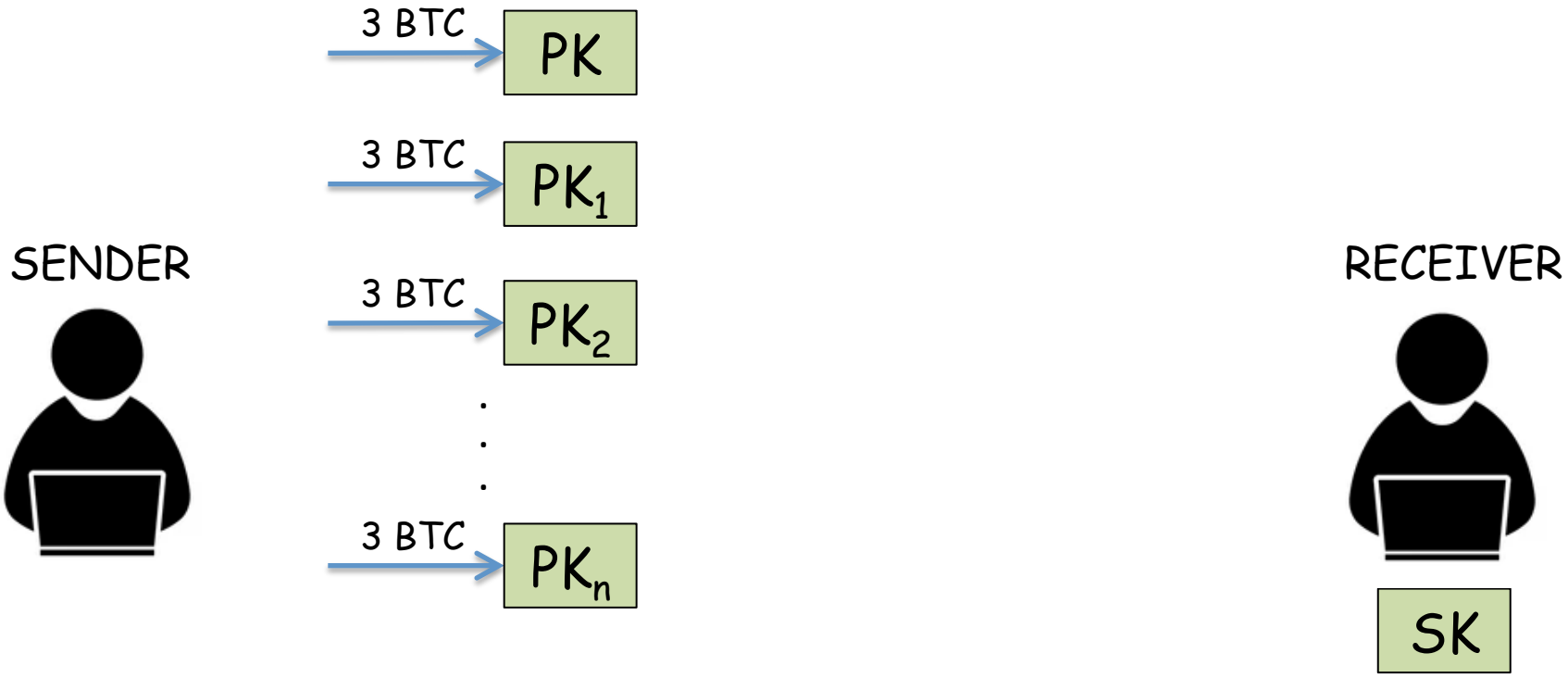
- introduced by van Saberhagen [7] in 2013



Privacy Enhancing Techniques - Ring Signatures

CryptoNote

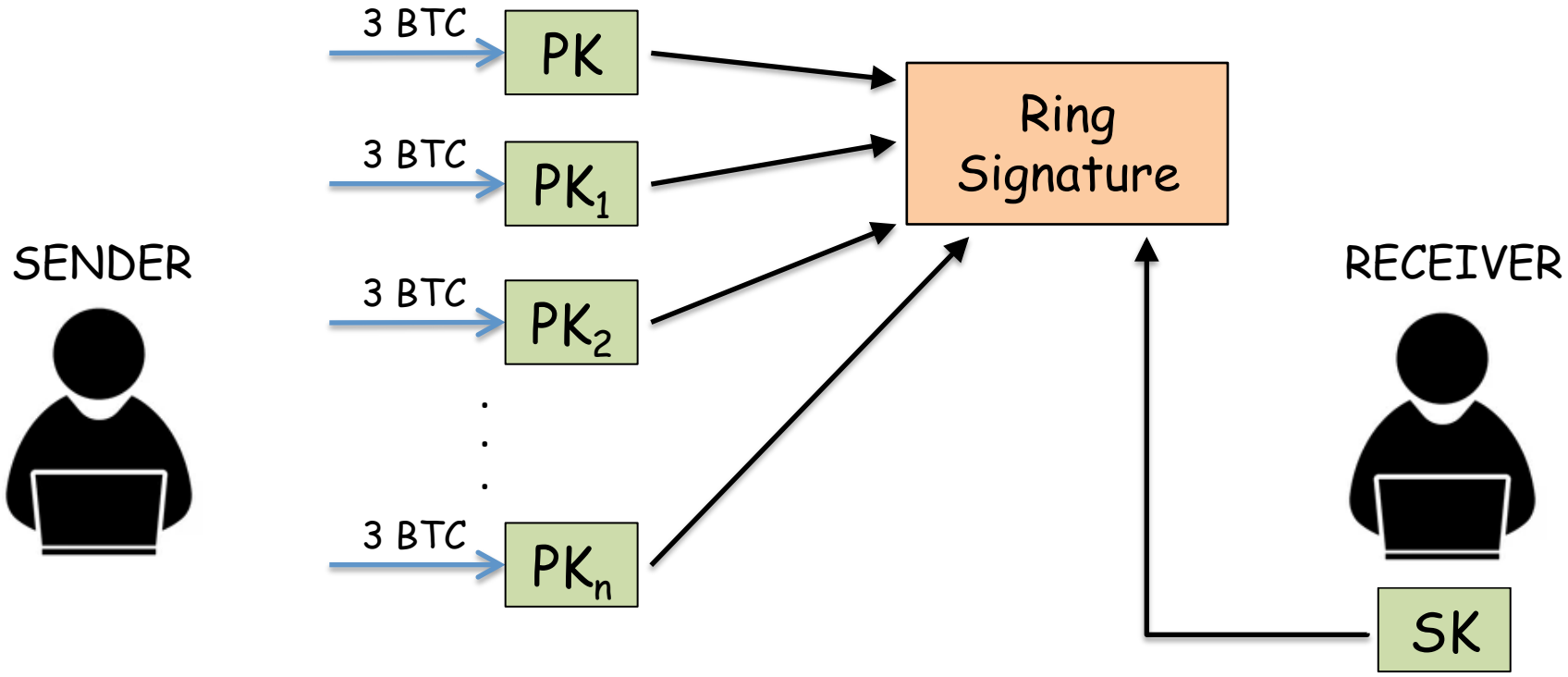
- introduced by van Saberhagen [7] in 2013



Privacy Enhancing Techniques - Ring Signatures

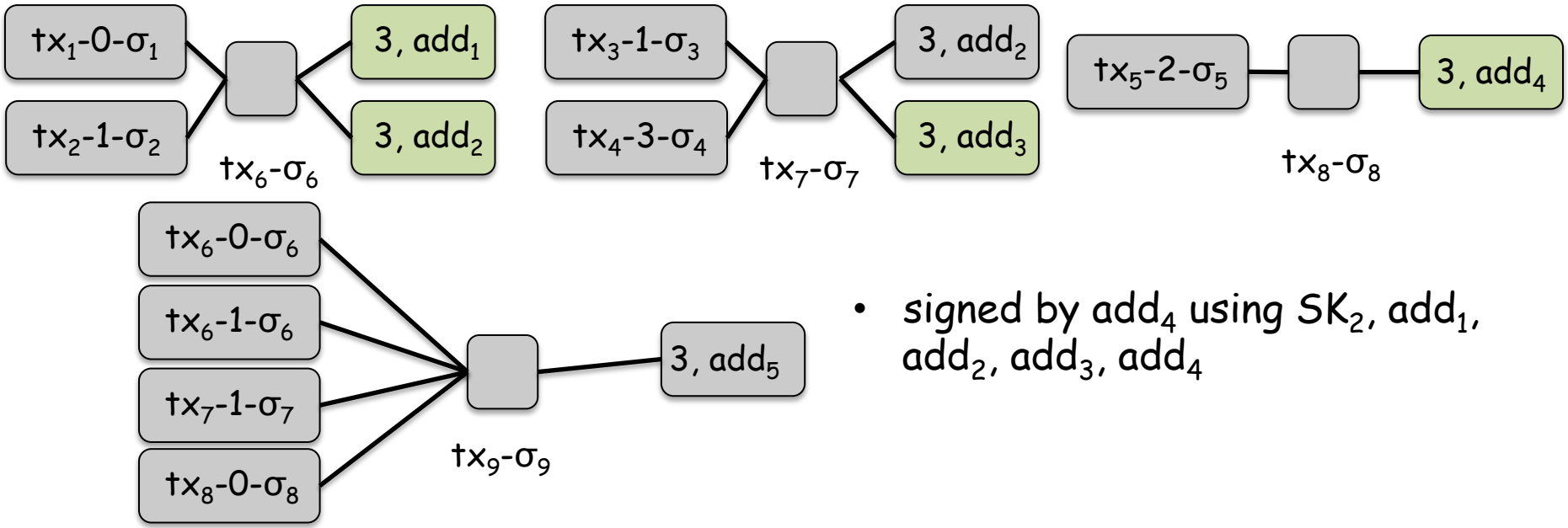
CryptoNote

- introduced by van Saberhagen [7] in 2013



Privacy Enhancing Techniques - Ring Signatures

- the transfer of an amount bitcoin ownership rights from one address to another one
- each tx consists of two main fields :
  - input : unspent transaction outputs claimed by the sender from previous transactions (previous transaction id, index, scriptsign)
  - output : instructions for claiming the sent bitcoins (value, scriptpublickey)
- if the transaction output not spent before, and the signature is valid, the transaction considered as valid



- signed by add_4 using SK_2, add_1, add_2, add_3, add_4

Privacy Enhancing Techniques - Ring Signatures

CryptoNote

- introduced by van Saberhagen [7] in 2013

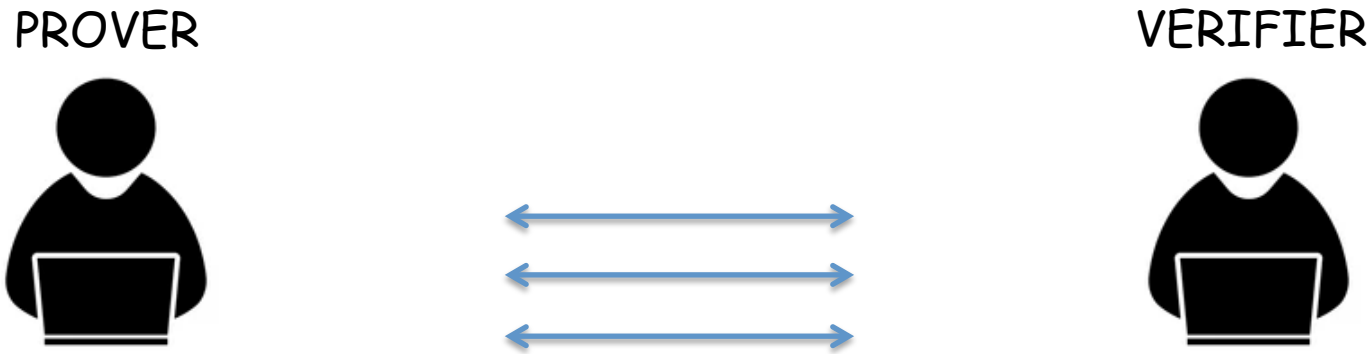
- Kumar et al. [8] analized Monero network to examine the untreacibility characteristics of CryptoNote

  - 93% of all transaction output amounts appear only once in the network
    (cannot be combined with others to form ring signatures)

  - users mostly use small number of transaction outputs to avoid high fees

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985



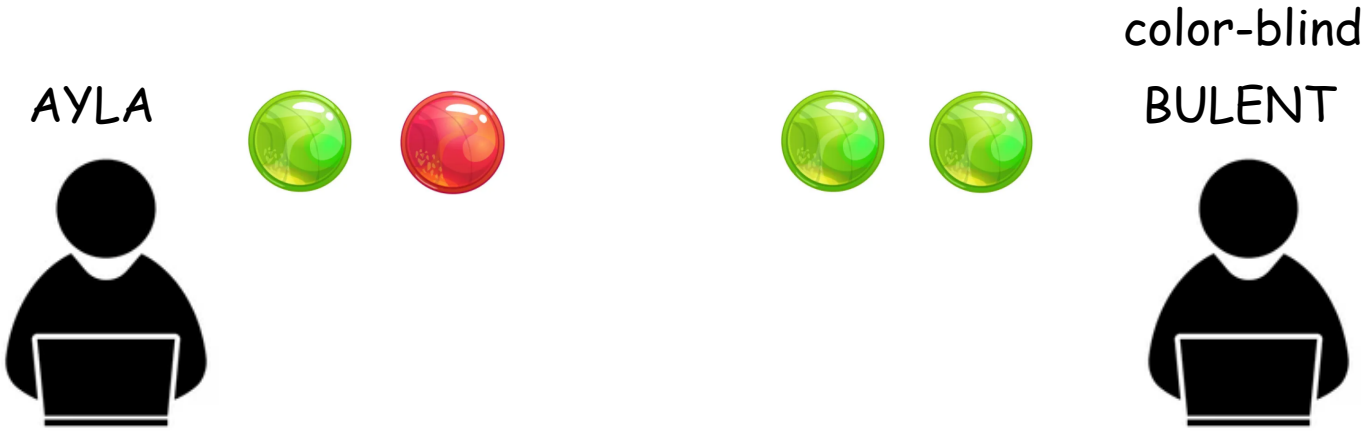
- allows one party (prover) to convince another party (verifier) that a statement is true without revealing any information other than this fact

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

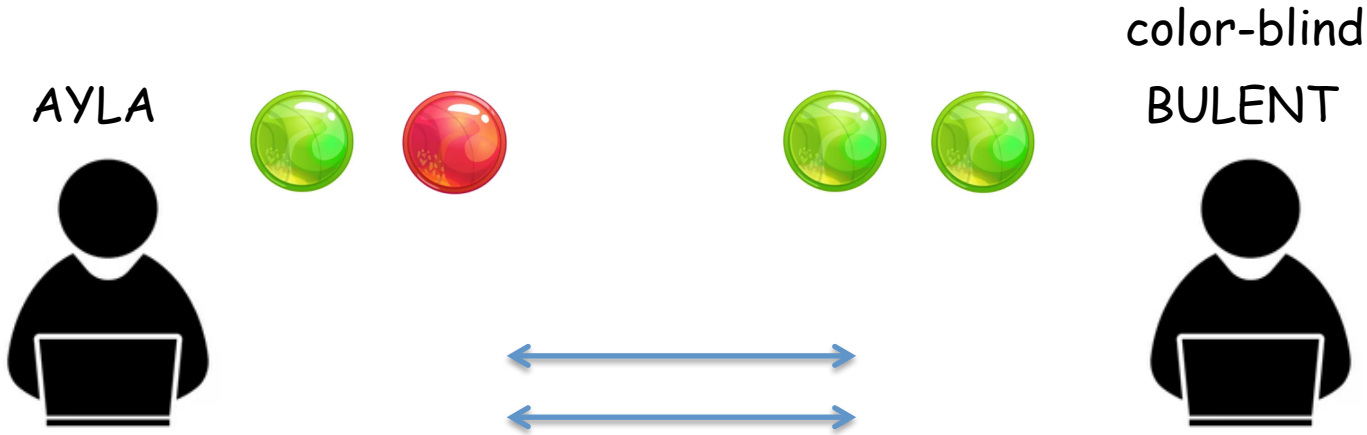
Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985



Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

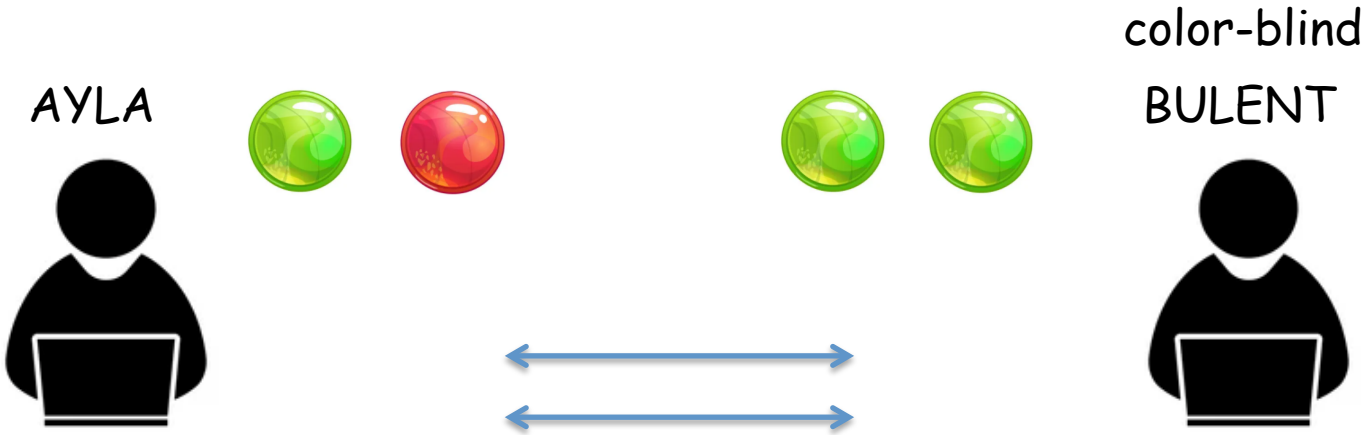


Ayla wants to convince Bulent they are in diffferent colors without revealing which one is red and which one is green

they seem completely identical to Bulent

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985



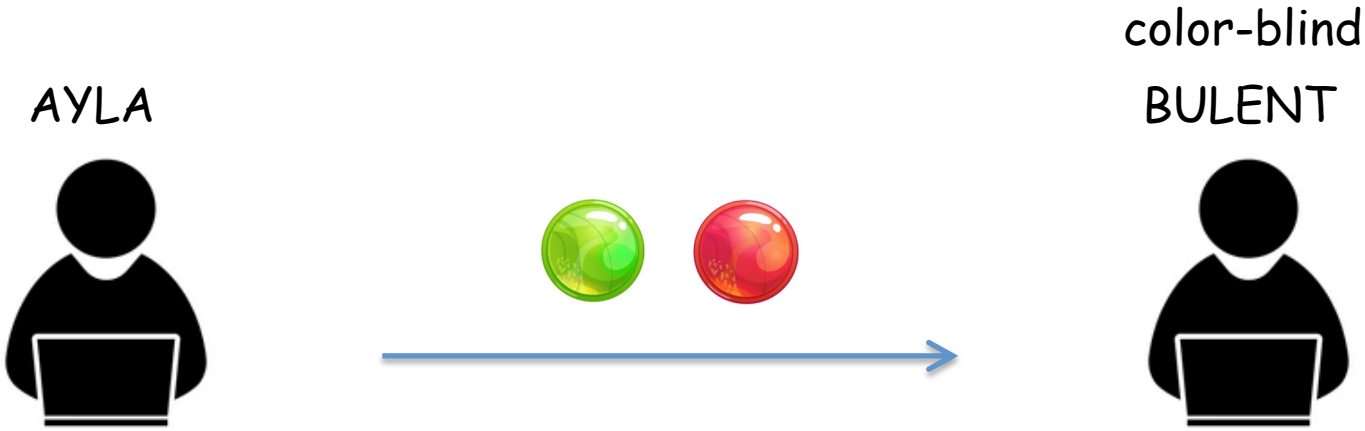
Ayla wants to convince Bulent they are in diffferent colors without revealing which one is red and which one is green

they seem completely identical to Bulent

he thinks they are actually distinguishable

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985



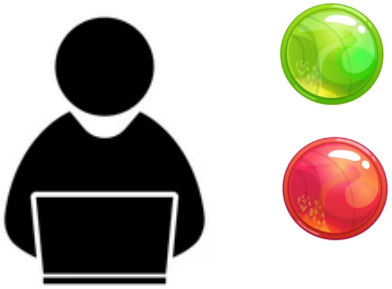
Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

AYLA

color-blind

BULENT



he either switching the balls, or keeping them in same hands

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

color-blind

AYLA

BULENT

"Did I swtich the balls ?"

he either switching the balls, or keeping them in same hands

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

color-blind

AYLA

BULENT

"Did I swtich the balls ?"

he either switching the balls, or keeping them in same hands

- assume Ayla doesn't know which one green and which one is red
- what would be the probability that Ayla correctly guess whether he switched or not ?

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

color-blind

AYLA

BULENT

"Did I swtich the balls ?"

he either switching the balls, or keeping them in same hands

- assume Ayla doesn't know which one green and which one is red
- what would be the probability that Ayla correctly guess whether he switched or not ?

1 / 2 = 0.5

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

"Did I swtich the balls ?"

he either switching the balls, or keeping them in same hands

- assume Ayla doesn't know which one green and which one is red
- what would be the probability that Ayla correctly guess whether he switched or not ?

$1 / 2 = 0.5$

$1 / 2^2 = 0.25$

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

AYLA

color-blind

BULENT

"Did I swtich the balls ?"

he either switching the balls, or keeping them in same hands

- assume Ayla doesn't know which one green and which one is red
- what would be the probability that Ayla correctly guess whether he switched or not ?

$1 / 2 = 0.5$

$1 / 2^5 = 0.03125$

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985

AYLA

color-blind

BULENT

"Did I swtich the balls ?"

he either switching the balls, or keeping them in same hands

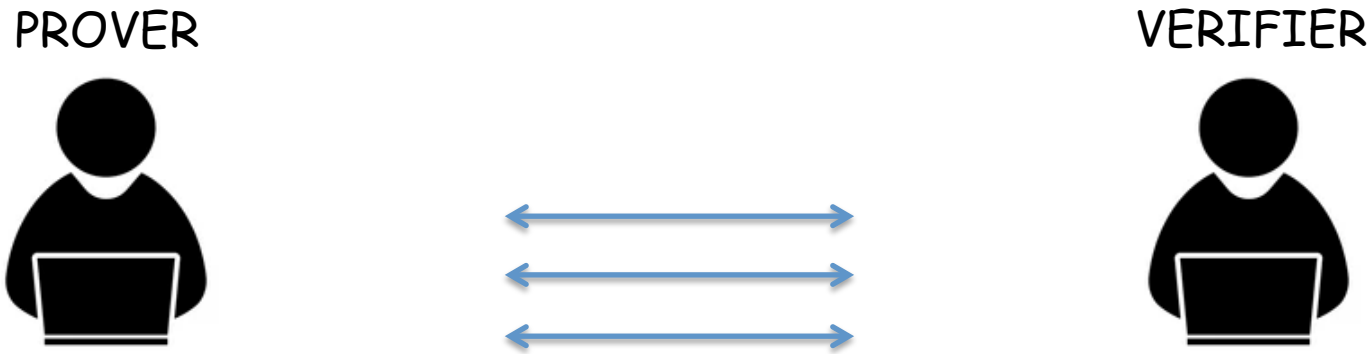
- assume Ayla doesn't know which one green and which one is red
- what would be the probability that Ayla correctly guess whether he switched or not ?

$1 / 2 = 0.5$

$1 / 2^{10} = 0.00097$

Privacy Enhancing Techniques - Zero Knowledge

- introduced by Goldwasser et al. [9] in 1985



- allows one party (prover) to convince another party (verifier) that a statement is true without revealing any information other than this fact
- Completeness : if the statement is true, the honest verifier will be convinced by the honest prover
- Soundness : if the statement is false, no cheating prover can convince the honest verifier that it is true
- Zero-Knowledge : the verifier learns anything other than the statement is true

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

- introduced by Miers et al. [10] in 2013

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

- introduced by Miers et al. [10] in 2013

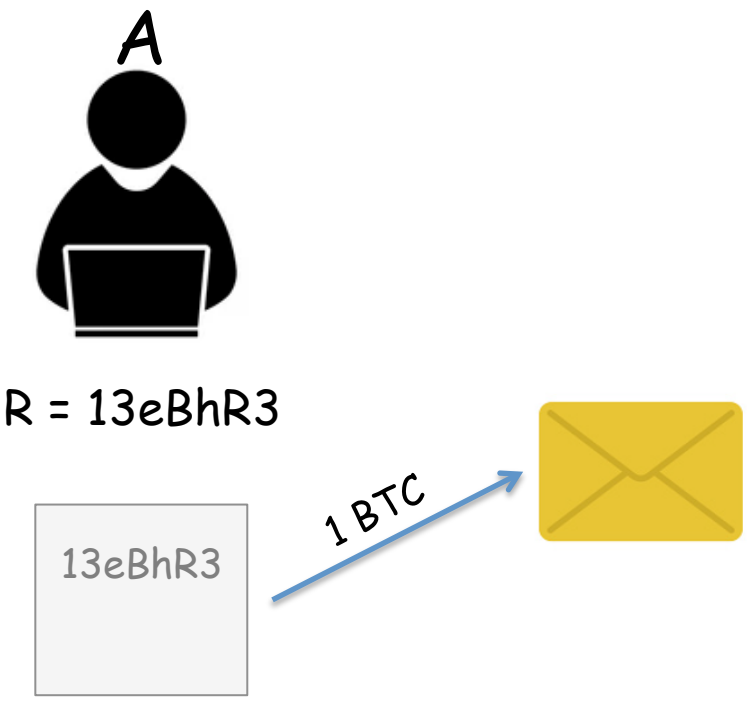
R = 13eBhR3

13eBhR3

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

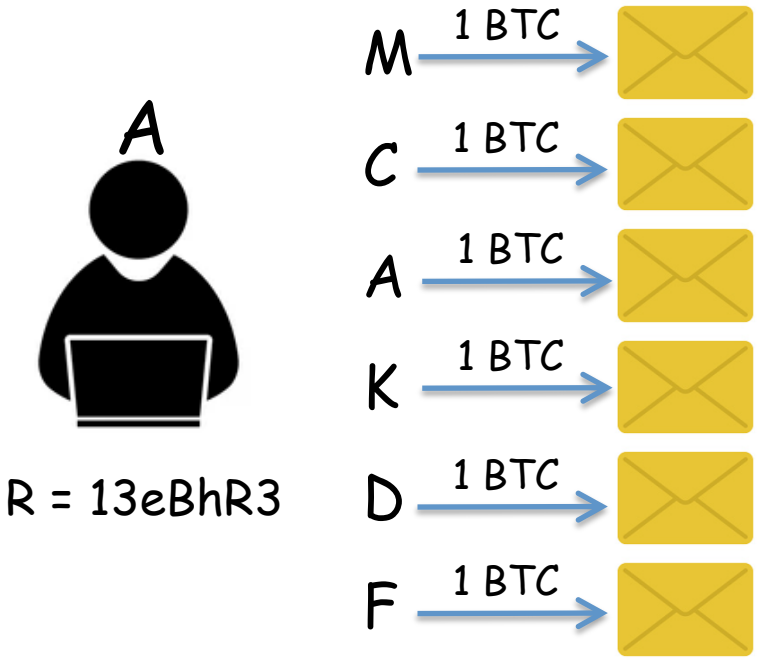
- introduced by Miers et al. [10] in 2013



Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

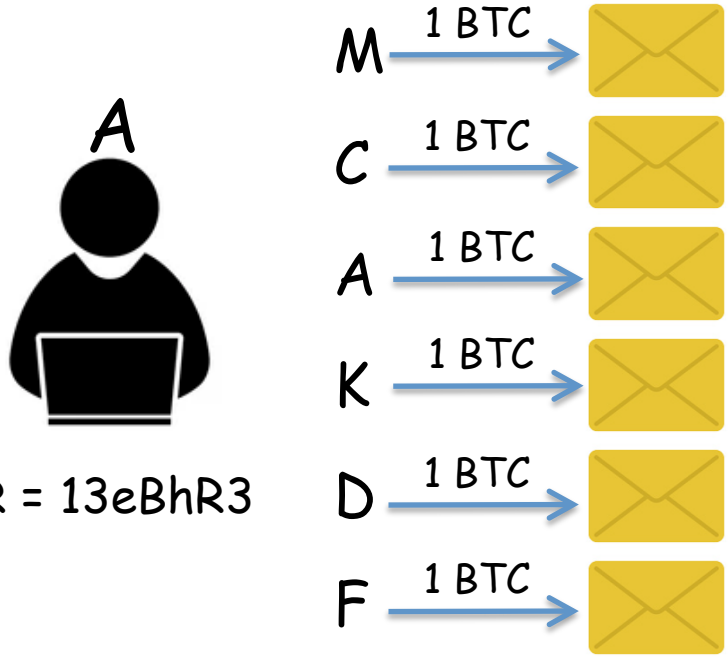
- introduced by Miers et al. [10] in 2013



Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

- introduced by Miers et al. [10] in 2013



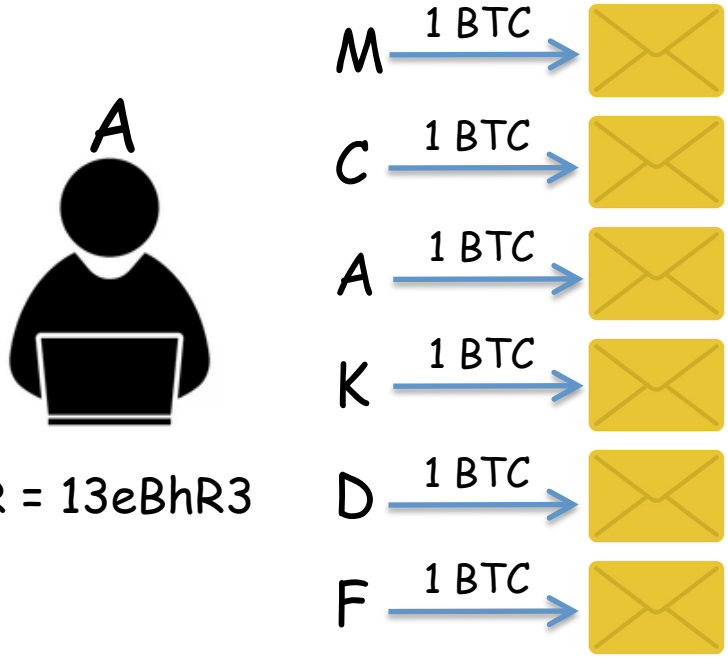
- R, proof

proof shows that on of the unclaimed zerocoins contains the serial number R

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

- introduced by Miers et al. [10] in 2013



- R, proof

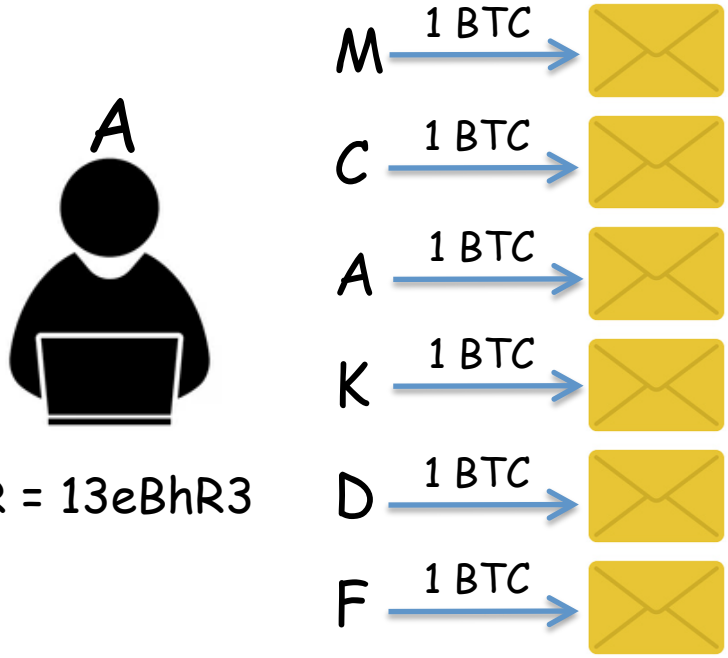
proof shows that on of the unclaimed zerocoins contains the serial number R

- prover A tries to convince verifier (whole network) that one of the commitments contains R without revealing which one exactly containing R

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

- introduced by Miers et al. [10] in 2013



- R, proof

proof shows that on of the unclaimed zerocoins contains the serial number R

- prover A tries to convince verifier (whole network) that one of the commitments contains R without revealing which one exactly containing R
  - 'zero knowledge' prevents one to link this transaction to a specific address

Privacy vs Accountability

- attractive tools for criminals to perform illegal activities

Privacy vs Accountability

- attractive tools for criminals to perform illegal activities

Cryptocurrencies + Add to myFT

Monero emerges as crypto of choice for cybercriminals

Untraceable 'privacy coin' is rising in popularity among ransomware gangs, posing problems for law enforcement

"Justin Ehrenhofer, member of the monero developer, estimates that about 10 or 20% of ransoms are paid in monero, and that figure will probably rise to 50% by the end of the year"

Privacy vs Accountability

- attractive tools for criminals to perform illegal activities
- Singapore exchange Bittrue hacked in June 2019, over $4 million stolen

  "Bittrue working with Houbi, Bittrex to freeze stolen cryptocurrencies and accounts associated with the hack"

Privacy vs Accountability

- attractive tools for criminals to perform illegal activities
- Singapore exchange Bittrue hacked in June 2019, over $4 million stolen

  "Bittrue working with Houbi, Bittrex to freeze stolen cryptocurrencies and accounts associated with the hack"

- Japan exchange Liquid hacked in August 2021, over $97 million stolen

  " stolen funds converted to Ether using Uniswap and Sushiswap, then Ether laundered through Tornado Cash"

Privacy vs Accountability

- attractive tools for criminals to perform illegal activities

Tornado Cash

"Tornado Cash has been used to launder more than $7 billion worth of virtual currency since its creation in 2019. This includes over $455 million stolen by the Lazarus Group"

"Tornado Cash was subsequently used to launder more than $96 million of malicious cyber actors' funds derived from the June 24, 2022 Harmony Bridge Heist"

THANK YOU

- for details

Murat Osmanoglu, and Ali Aydın Selcuk. "Privacy in blockchain systems", Turkish Journal of Electrical Engineering & Computer Sciences (2022)

References

1. Reid, F., Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. In: Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A. (Eds.), Security and Privacy in Social Networks. Springer, New York, pp. 197–223.

2. Bonneau J, Narayanan A, Miller A, Clark J, Kroll JA et al. Mixcoin: Anonymity for bitcoin with accountable mixes. In: Financial Cryptography and Data Security; Christ Church, Barbados; 2014. pp. 486-504.

3. Maxwell G. (2013). Coinjoin: Bitcoin privacy for the real world [online]. Website https://bitcointalk.org/index.php?topic=279249.0 [accessed 11 April 2021].

4. Rufing T, Moreno-Sanchez P, Kate A. Coinshuffle: Practical decentralized coin mixing for bitcoin. In: European Symposium on Research in Computer Security; Wroclaw, Poland; 2014. pp. 345-364.

5. Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT); Gold Coast, Australia; 2001. pp. 552-565.

References

6. Fujisaki E, Suzuki K. Traceable ring signature. In: International Conference on Practice and Theory in Public-Key Cryptography; Beijing, China; 2007. pp. 181-200.

7. van Saberhagen N. (2013). Cryptonote v 2.0 [online]. Website https://bytecoin.org/old/whitepaper.pdf [accessed 13 May 2021].

8. Kumar A, Fischer C, Tople S, Saxena P. A traceability analysis of monero's blockchain. In: European Symposium on Research in Computer Security; Oslo, Norway; 2017. pp. 153-173.

9. Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems (extended abstract). In: ACM Symposium on Theory of Computing; Providence, Rhode Island, USA; 1985. pp. 291-304.

10. Miers I, Garman C, Green M, Rubin AD. Zerocoin: Anonymous distributed e-cash from bitcoin. In: IEEE Symposium on Security and Privacy; Berkeley, CA, USA; 2013. pp. 397–411.