Privacy II

Murat Osmanoglu

Privacy Enhancing Techniques - Ring Signatures

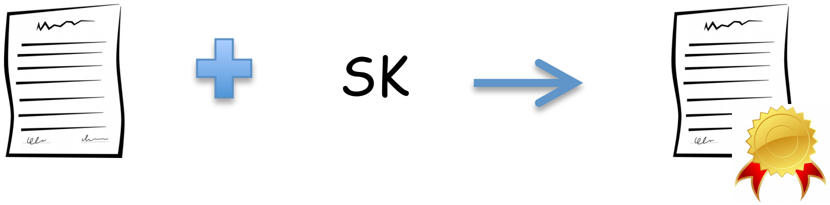
Digital Signatures

PK, SK

Privacy Enhancing Techniques - Ring Signatures

Digital Signatures

PK, SK



SK

Signature

SIGNING ALGORITHM

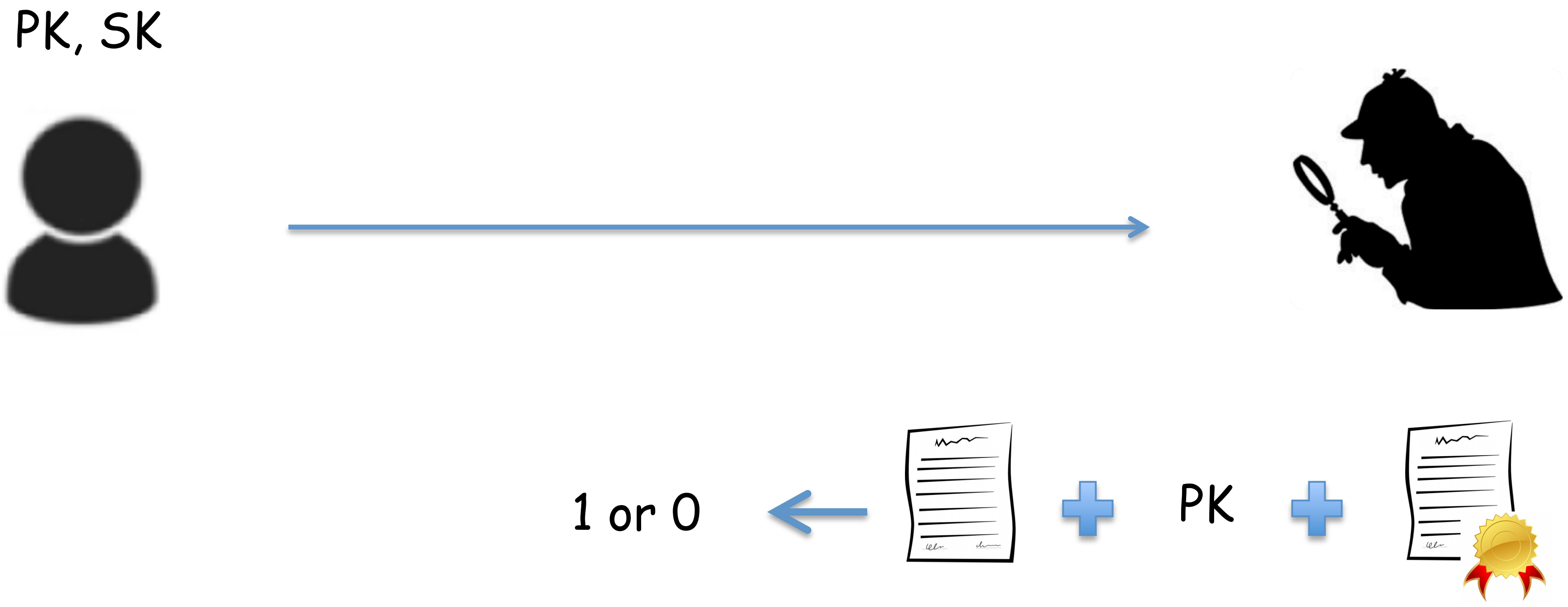
Privacy Enhancing Techniques - Ring Signatures

Digital Signatures

PK, SK

Privacy Enhancing Techniques - Ring Signatures

Digital Signatures



PK, SK

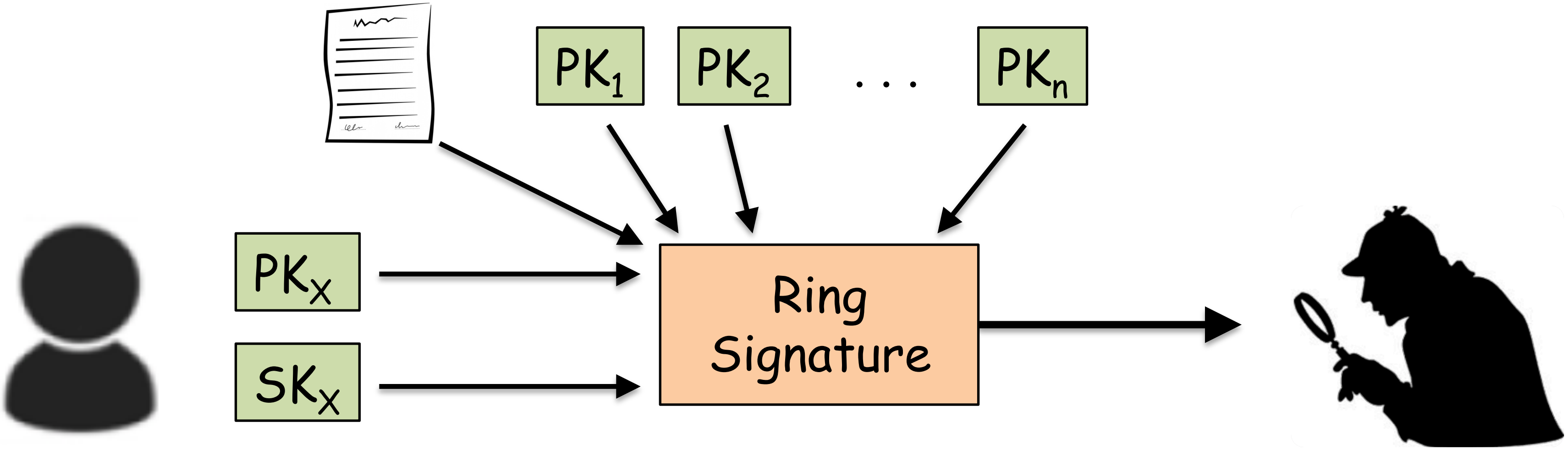
1 or 0

PK

VERIFICATION ALGORITHM

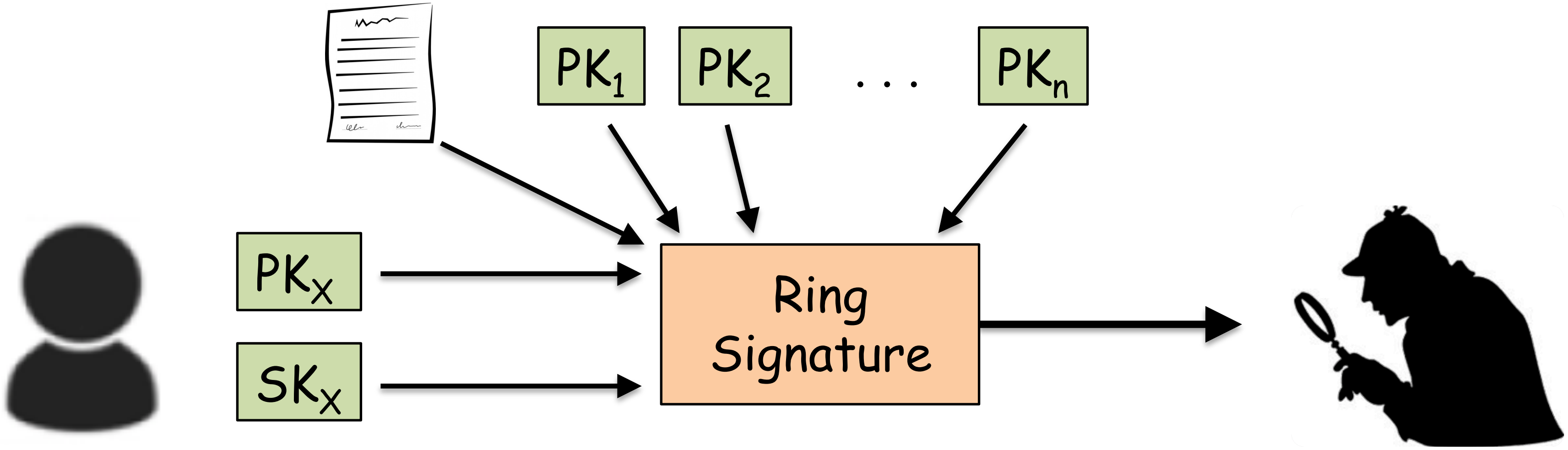
Privacy Enhancing Techniques - Ring Signatures

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



Privacy Enhancing Techniques - Ring Signatures

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



PK_1

PK_2

. . .

PK_n

PK_X

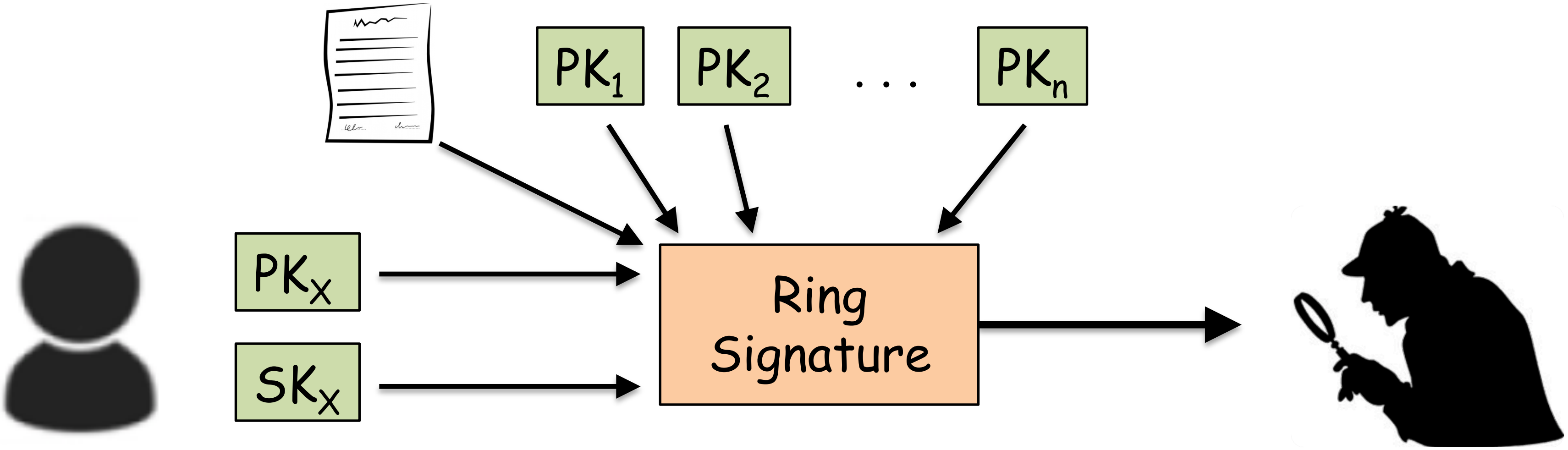
SK_X

Ring Signature

- 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

Privacy Enhancing Techniques - Ring Signatures

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

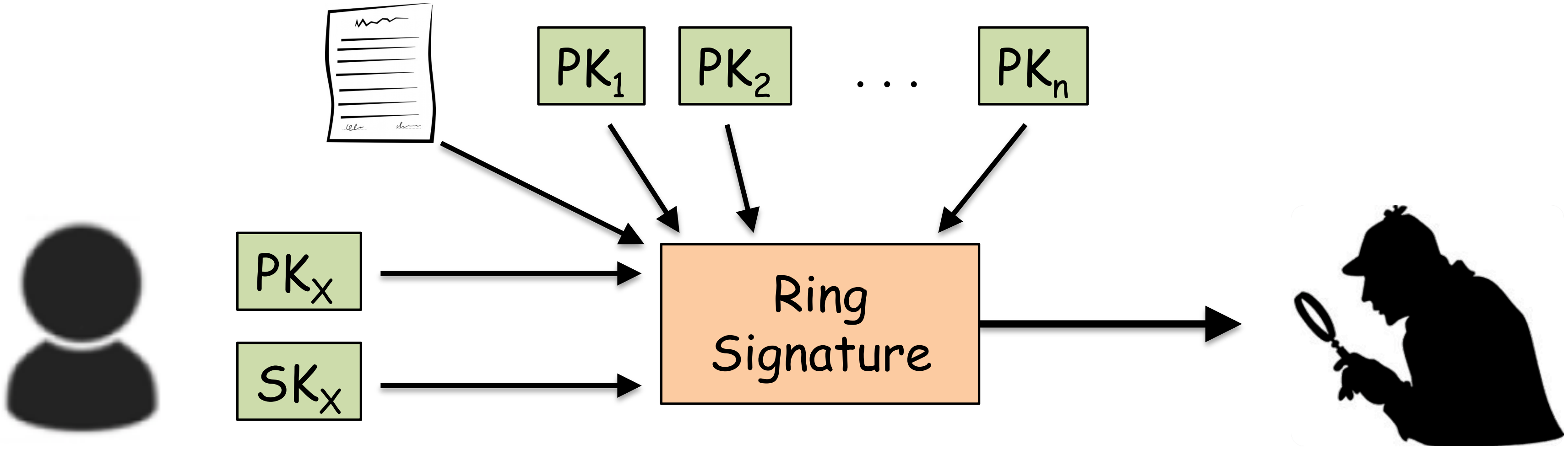


- verifier can tell that one member from the set $\{PK_1, PK_2, \ldots, PK_n, PK_X\}$ signed the message, but cannot tell which one the actual signer

- 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

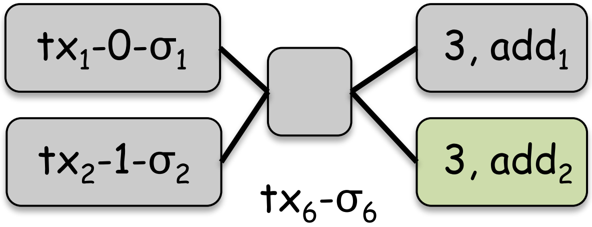


- verifier can tell that one member from the set {PK_1, PK_2, …, PK_n, PK_X} signed the message, but cannot tell which one the actual signer

- 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

- 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



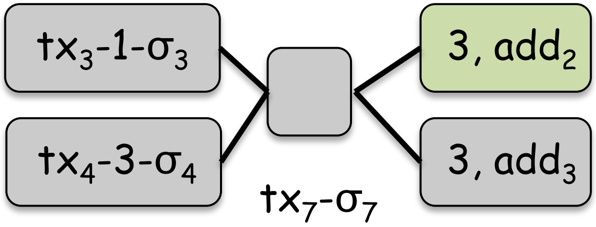
tx_1-0-σ_1

tx_2-1-σ_2

3, add_1

3, add_2

tx_6-σ_6



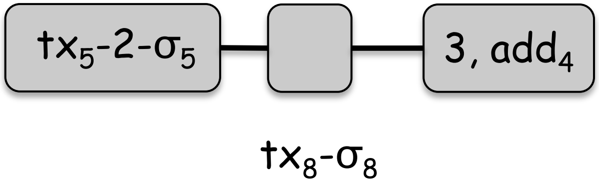
tx_3-1-σ_3

tx_4-3-σ_4

3, add_2

3, add_3

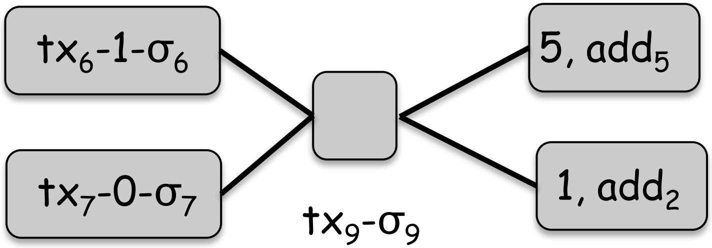
tx_7-σ_7



tx_5-2-σ_5

3, add_4

tx_8-σ_8



tx_6-1-σ_6

tx_7-0-σ_7

5, add_5

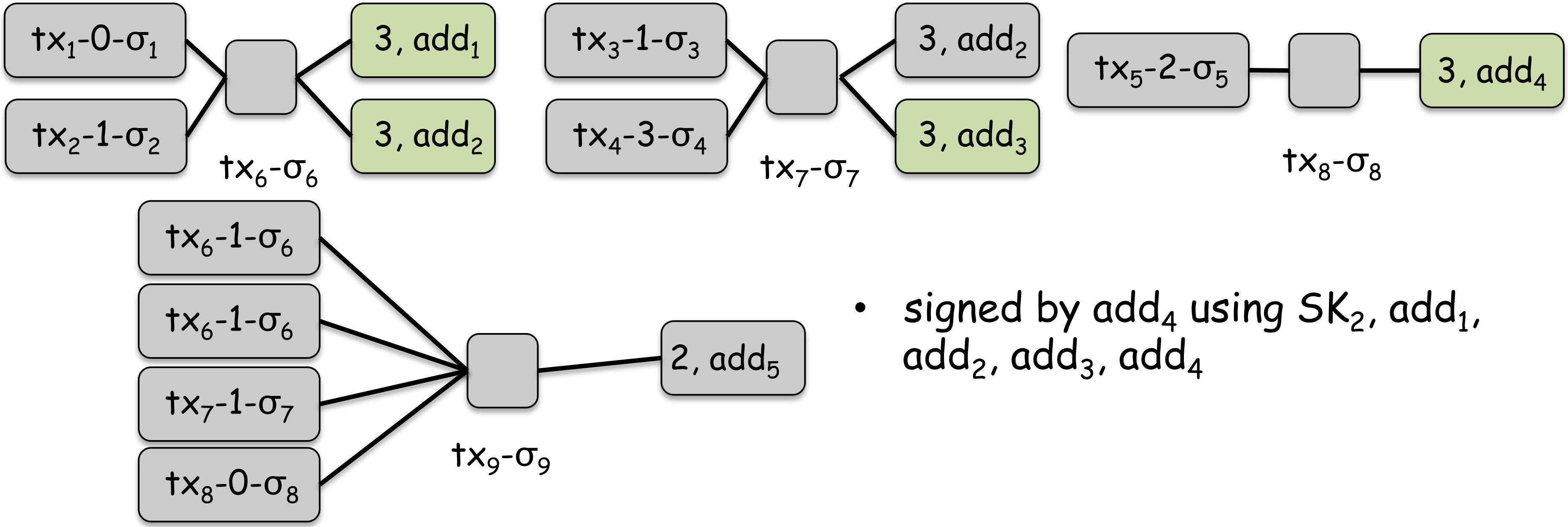
1, add_2

tx_9-σ_9

- signed by add_2 using SK_2

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

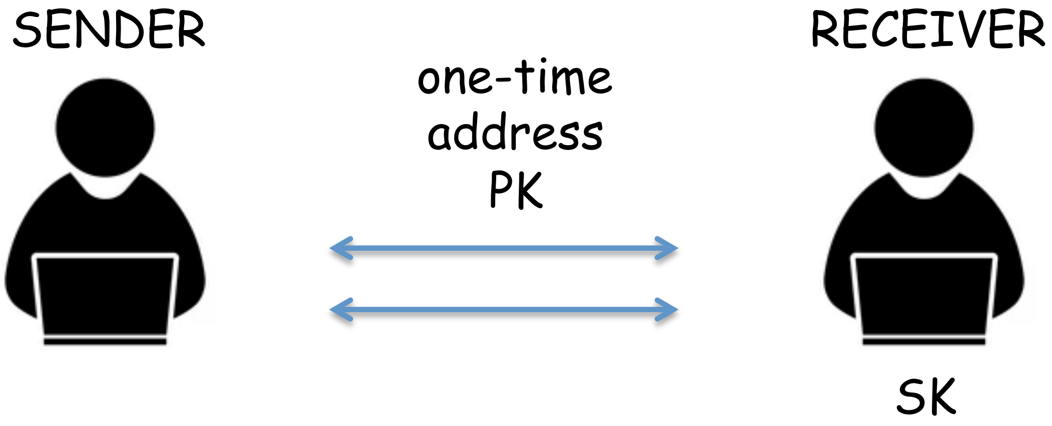
CryptoNote

- introduced by van Saberhagen [7] in 2013

Privacy Enhancing Techniques - Ring Signatures

CryptoNote

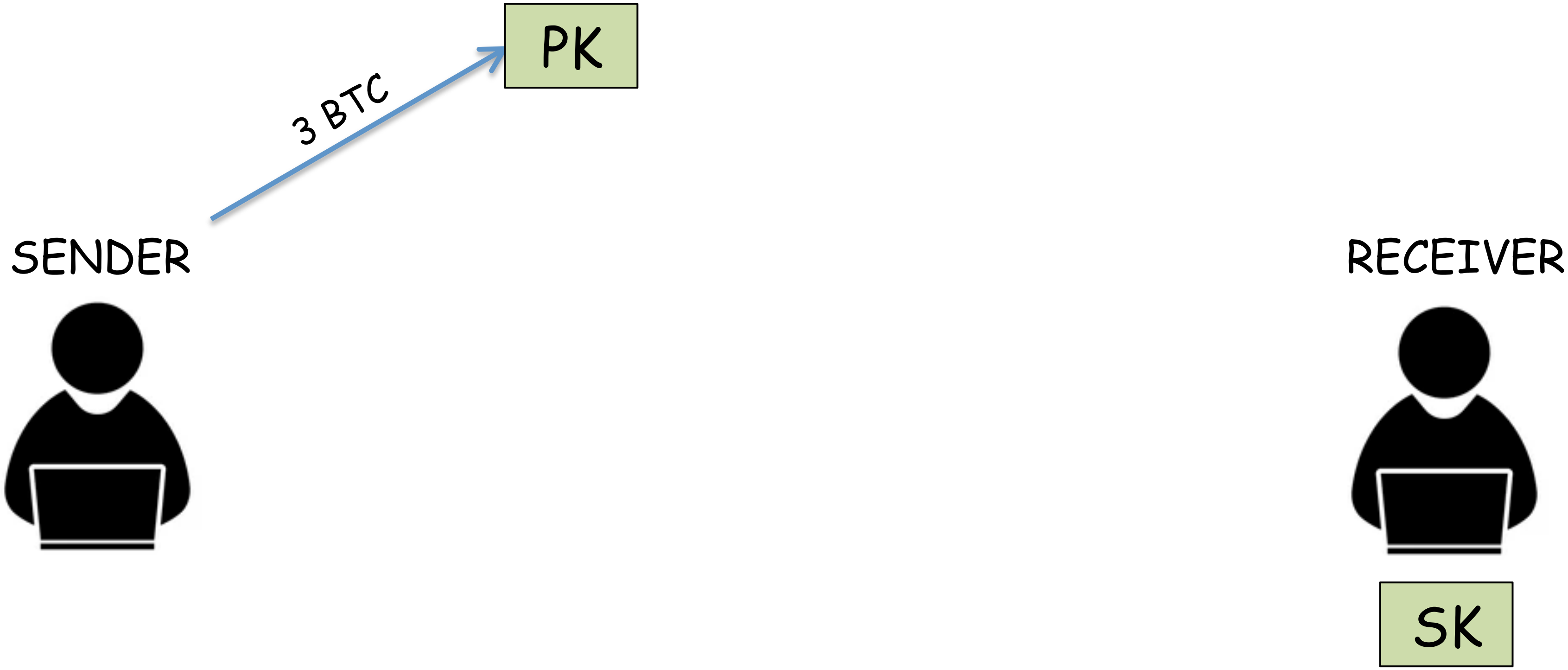
- introduced by van Saberhagen [7] in 2013



Privacy Enhancing Techniques - Ring Signatures

CryptoNote

- introduced by van Saberhagen [7] in 2013



PK

3 BTC

SENDER

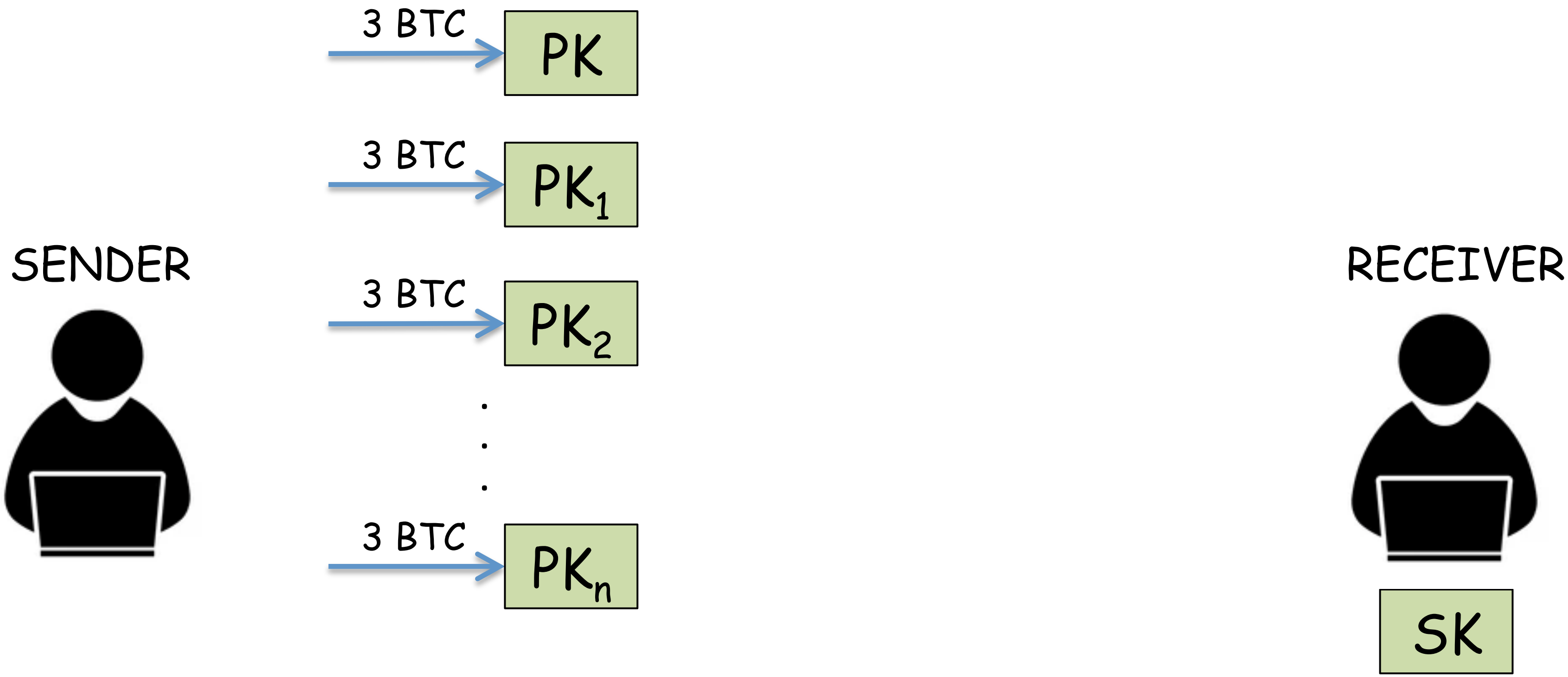
RECEIVER

SK

Privacy Enhancing Techniques - Ring Signatures

CryptoNote

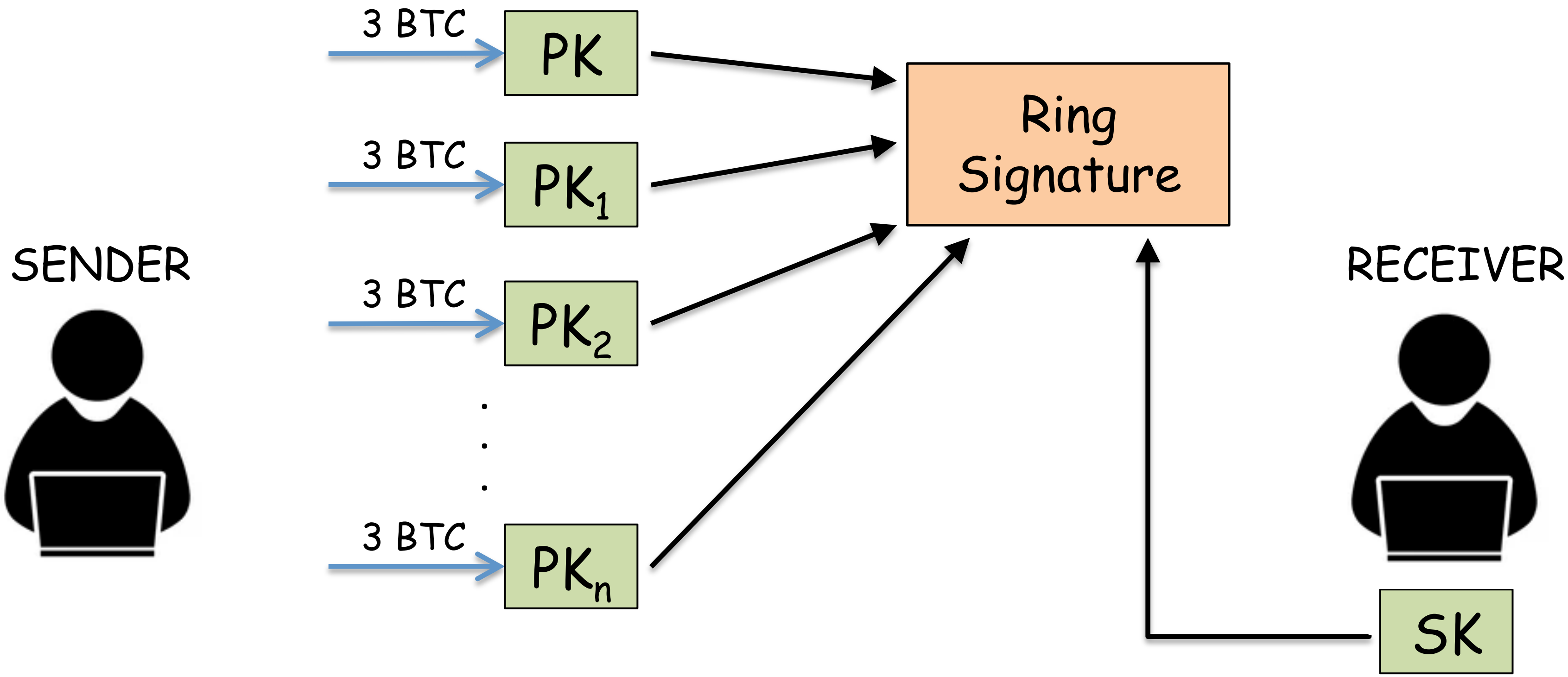
- introduced by van Saberhagen [7] in 2013



Privacy Enhancing Techniques - Ring Signatures

CryptoNote

- introduced by van Saberhagen [7] in 2013



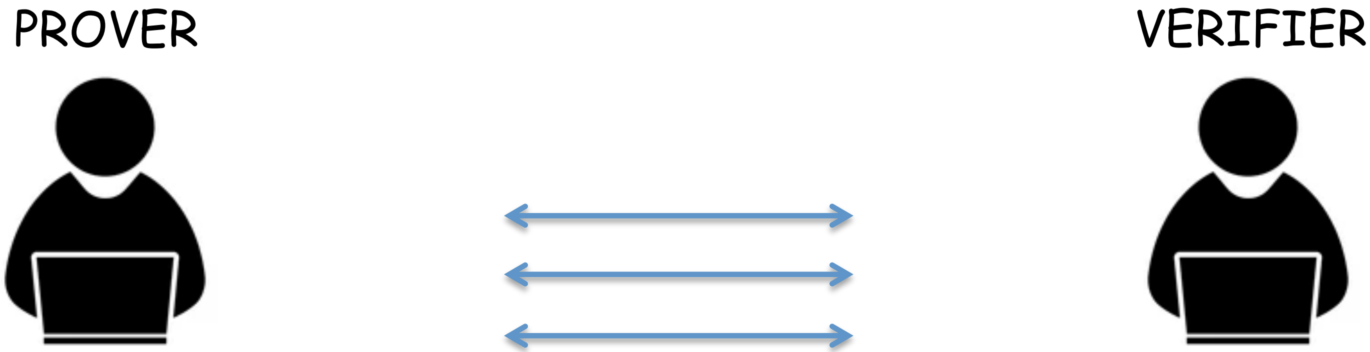
Privacy Enhancing Techniques - Ring Signatures

CryptoNote

- introduced by van Saberhagen [7] in 2013
- 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



PROVER

VERIFIER

- 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

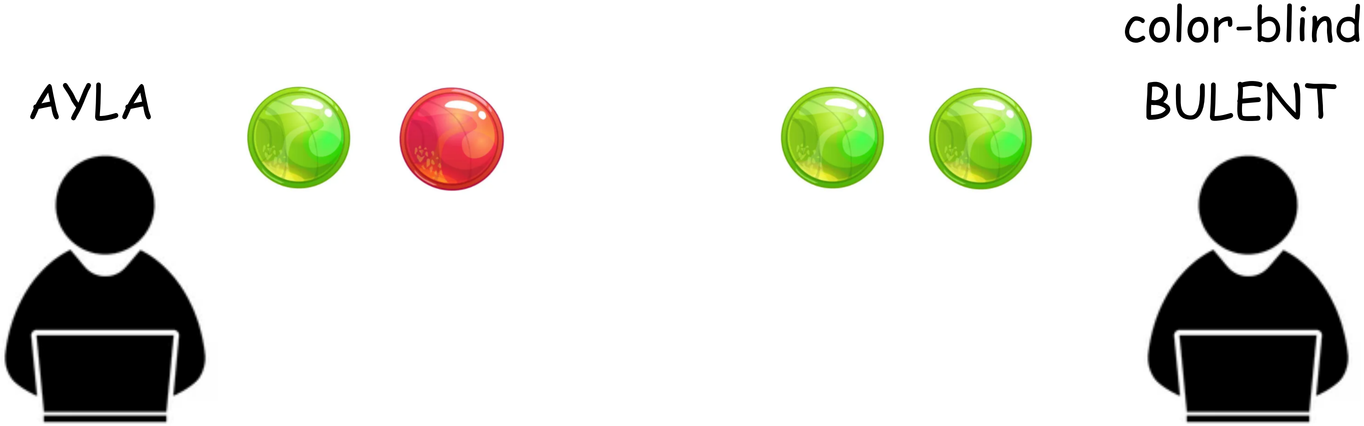
AYLA

color-blind

BULENT

Privacy Enhancing Techniques - Zero Knowledge

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



color-blind

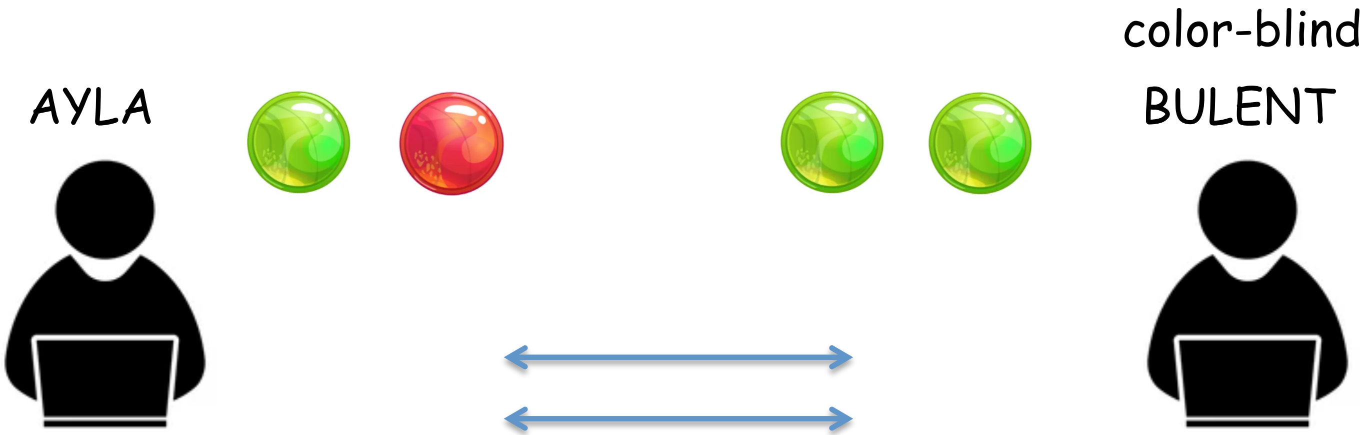
AYLA

BULENT

they seem completely identical to Bulent

Privacy Enhancing Techniques - Zero Knowledge

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

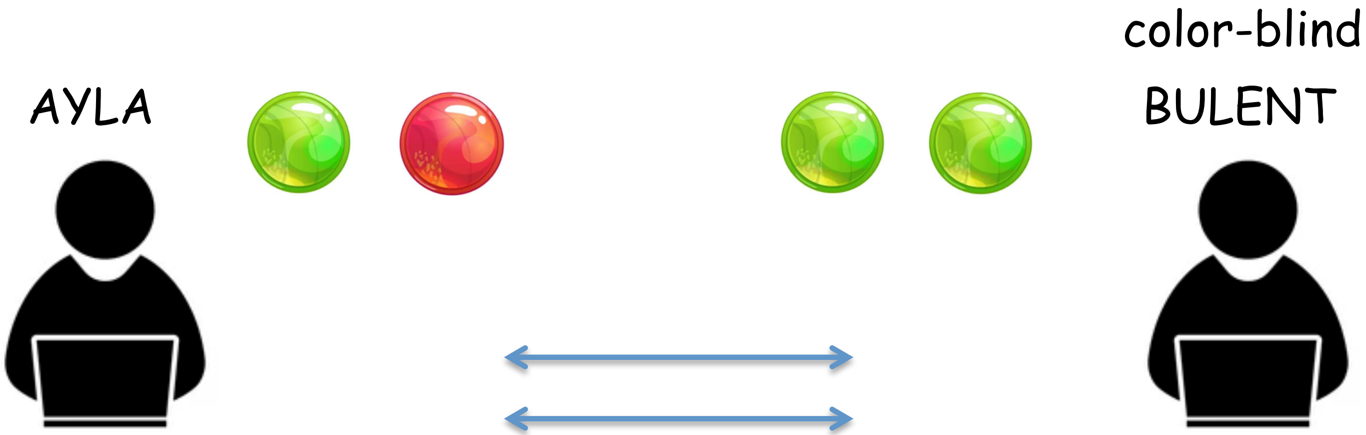


Ayla wants to convince Bulent they are in diffferent colors without revealing which one is red and which one is green

they seem completely identical to Bulent

Privacy Enhancing Techniques - Zero Knowledge

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



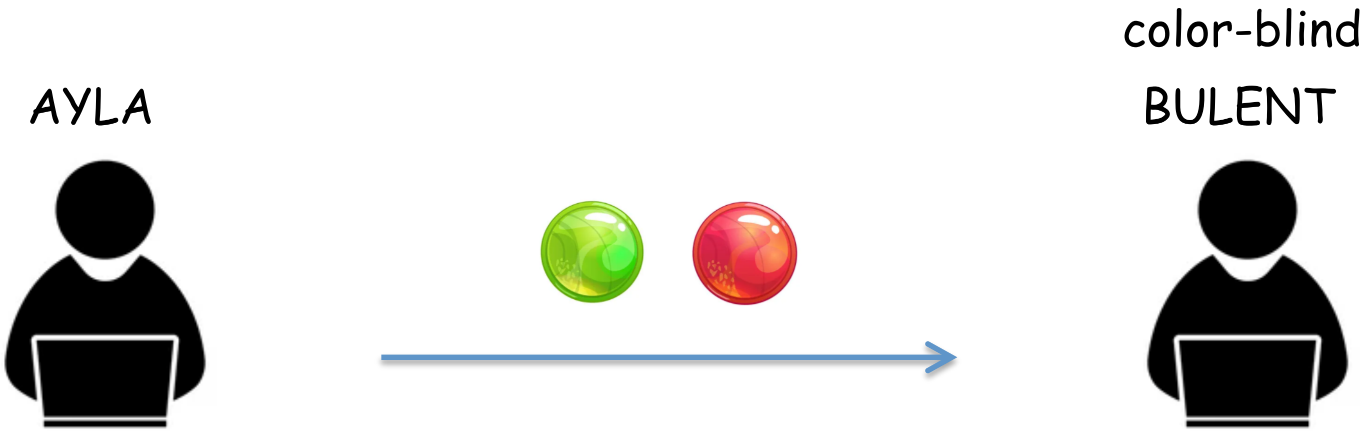
Ayla wants to convince Bulent they are in diffferent colors without revealing which one is red and which one is green

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



color-blind

AYLA

BULENT

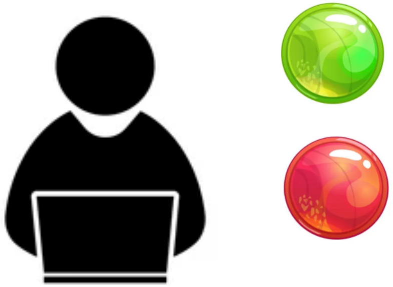
Privacy Enhancing Techniques - Zero Knowledge

- 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

AYLA

color-blind

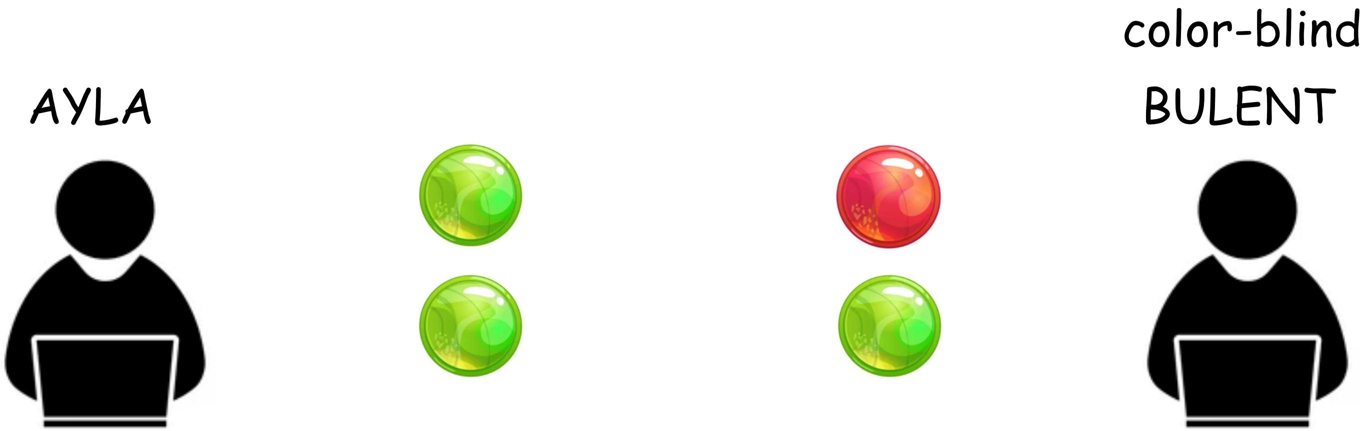
BULENT

“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



"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

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

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

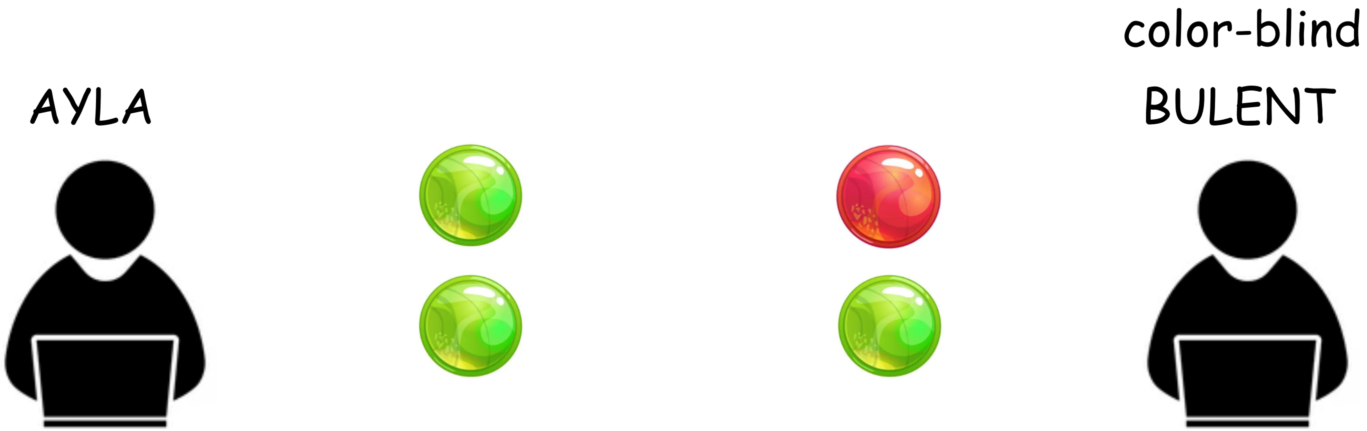
- assume Ayla doesn't know which one green and which one is red
- what would be the probability that Ayla correctly guess whether he switched or not ?

$1 / 2 = 0.5$

$1 / 2^2 = 0.25$

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

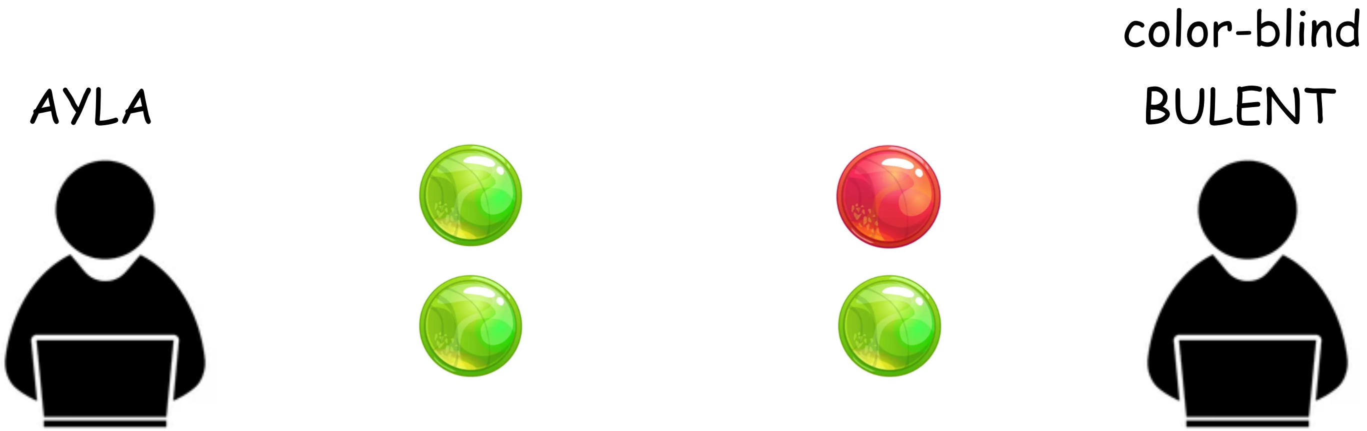
- what would be the probability that Ayla correctly guess whether he switched or not ?

$1 / 2 = 0.5$

$1 / 2^5 = 0.03125$

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

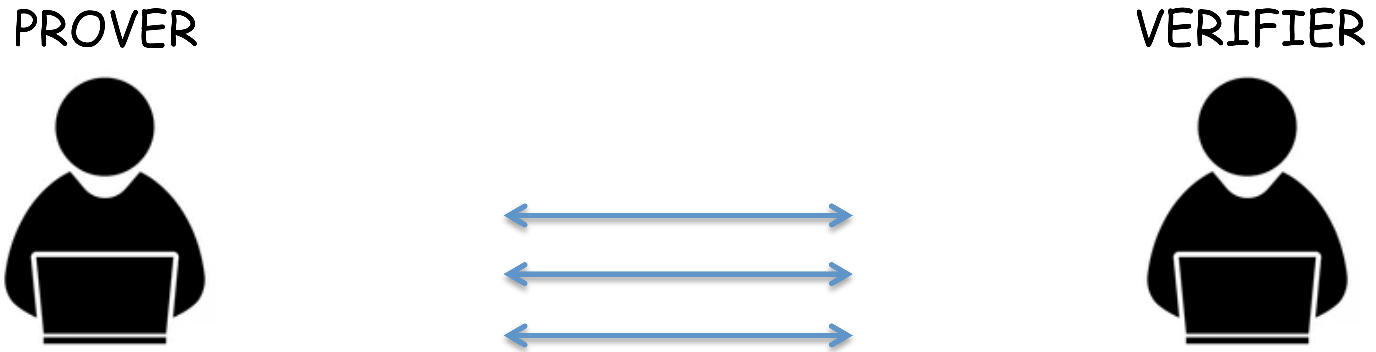
- what would be the probability that Ayla correctly guess whether he switched or not ?

$$1 / 2 = 0.5$$

$$1 / 2^{10} = 0.00097$$

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

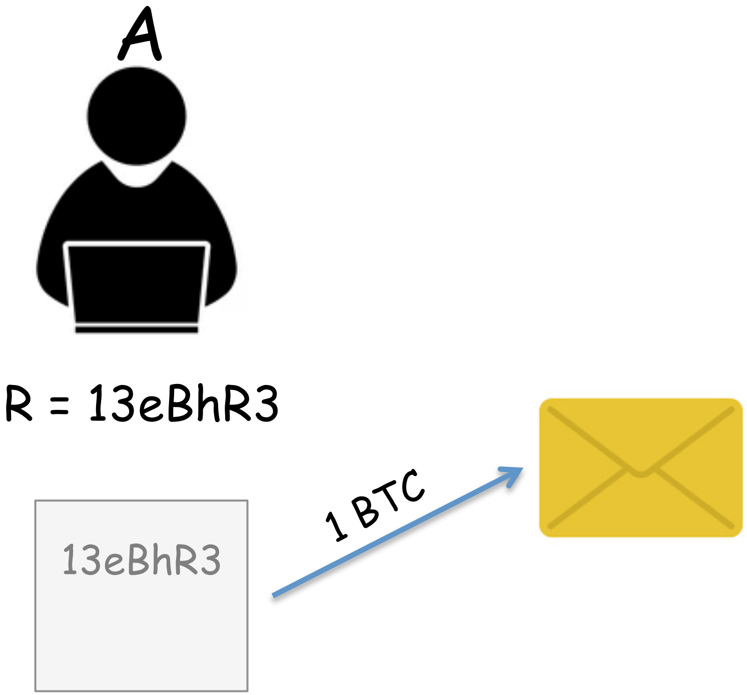
R = 13eBhR3

13eBhR3

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

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



A

R = 13eBhR3

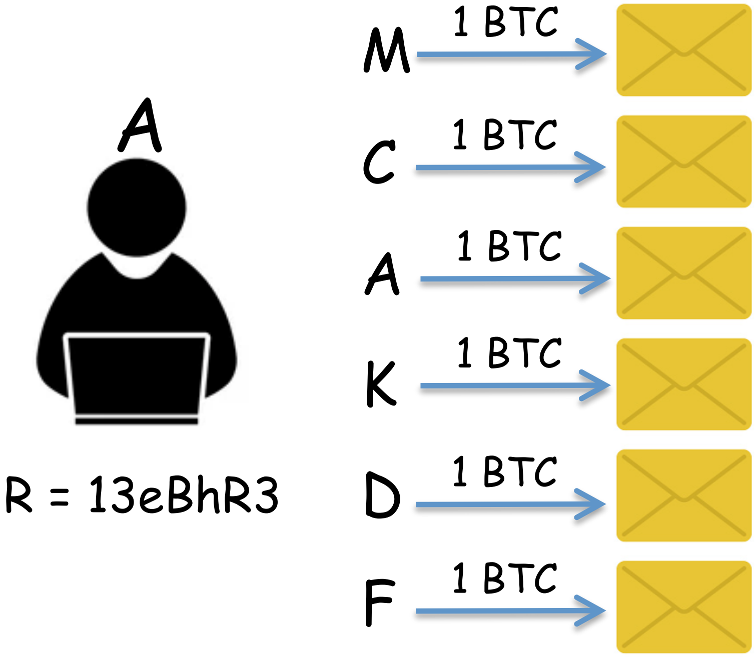
13eBhR3

1 BTC

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

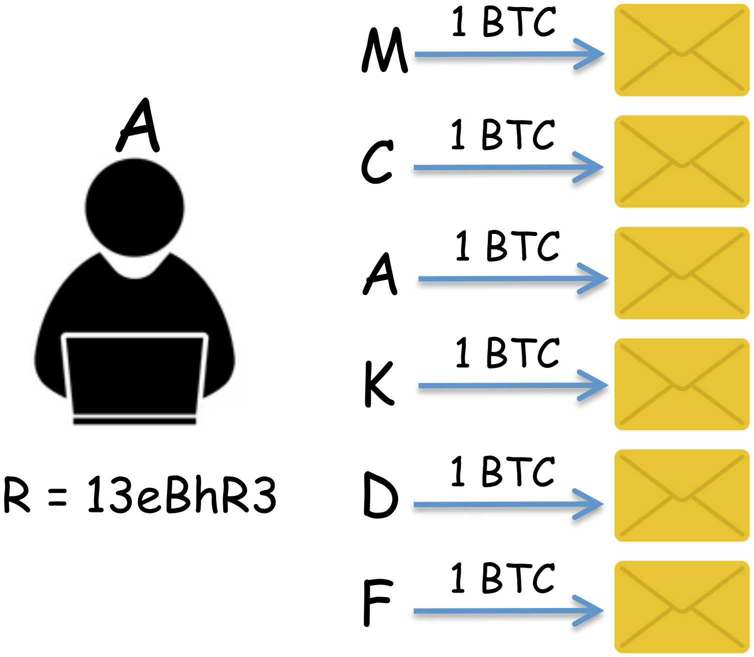
- introduced by Miers et al. [10] in 2013



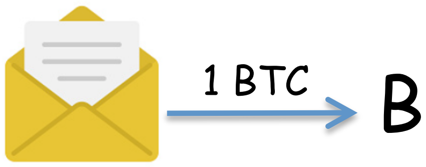
Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

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



R = 13eBhR3



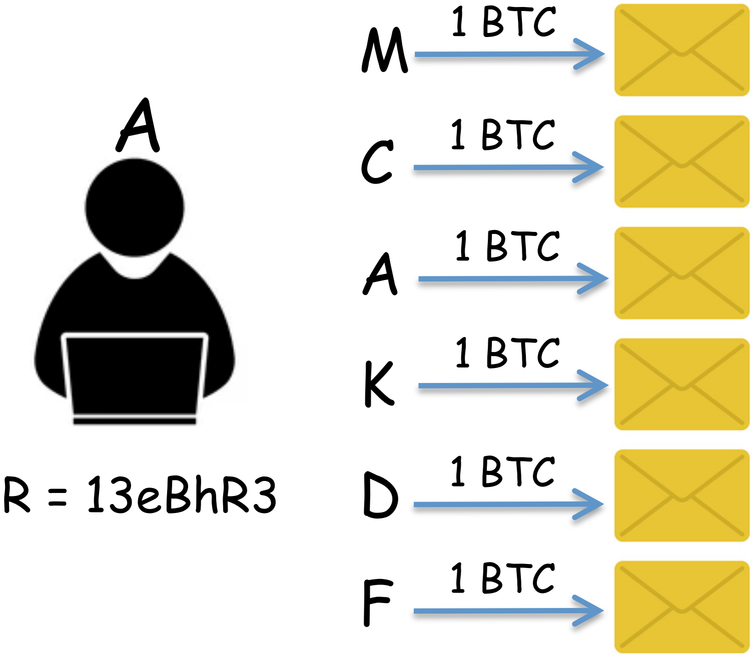
- R, proof

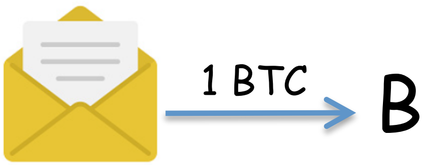
proof shows that on of the unclaimed zerocoins contains the serial number R

Privacy Enhancing Techniques - Zero-Knowledge

ZeroCoin

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





- R, proof

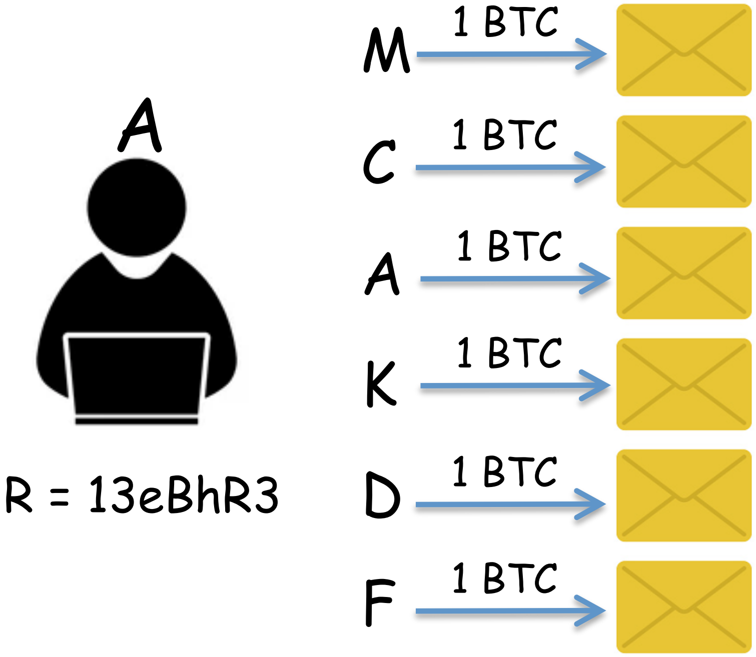
proof shows that on of the unclaimed zerocoins contains the serial number R

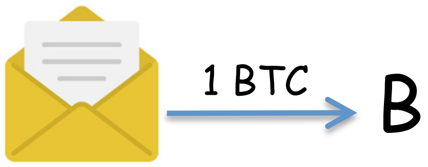
- prover A tries to convince verifier (whole network) that one of the commitments contains R without revealing which one exactly containing R

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 Enhancing Techniques

Privacy vs Accountability

Privacy Enhancing Techniques

Privacy vs Accountability

- attractive tools for criminals to perform illegal activities
- introducing serious concerns for regulatory authorities
- 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 Enhancing Techniques

Privacy vs Accountability

- attractive tools for criminals to perform illegal activities
- introducing serious concerns for regulatory authorities
- 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"

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. Ruffing 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.