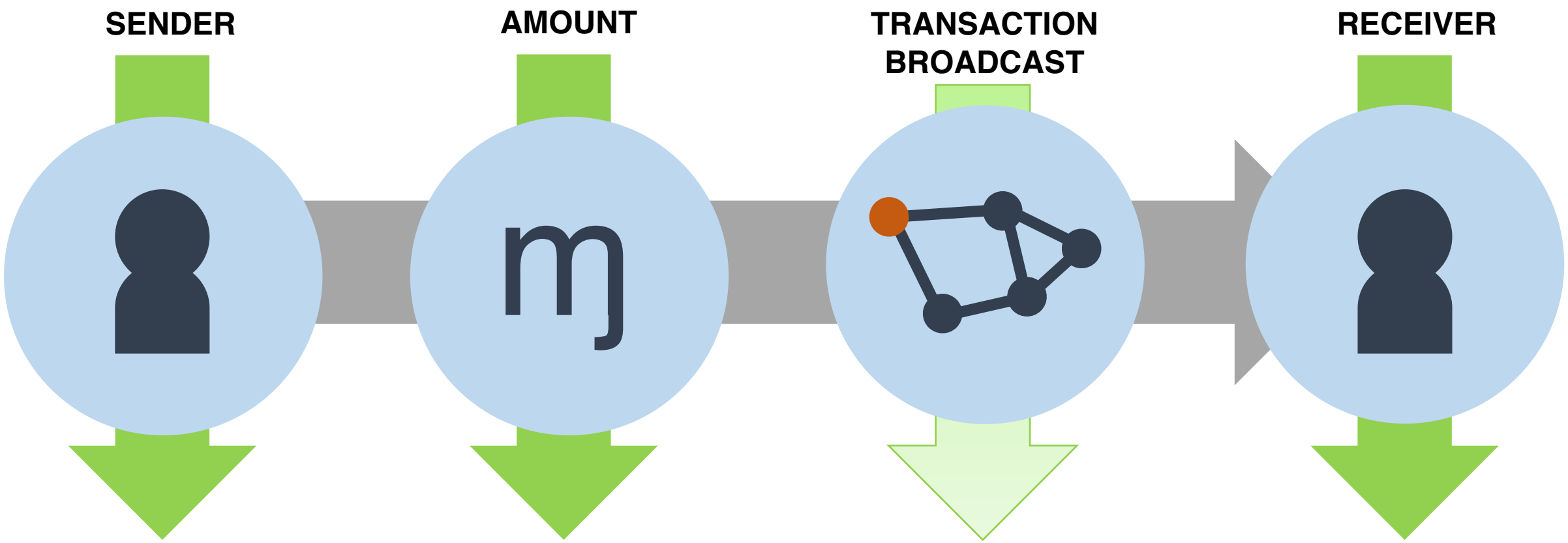
# 门罗币的隐私
# 保护方案原理解析

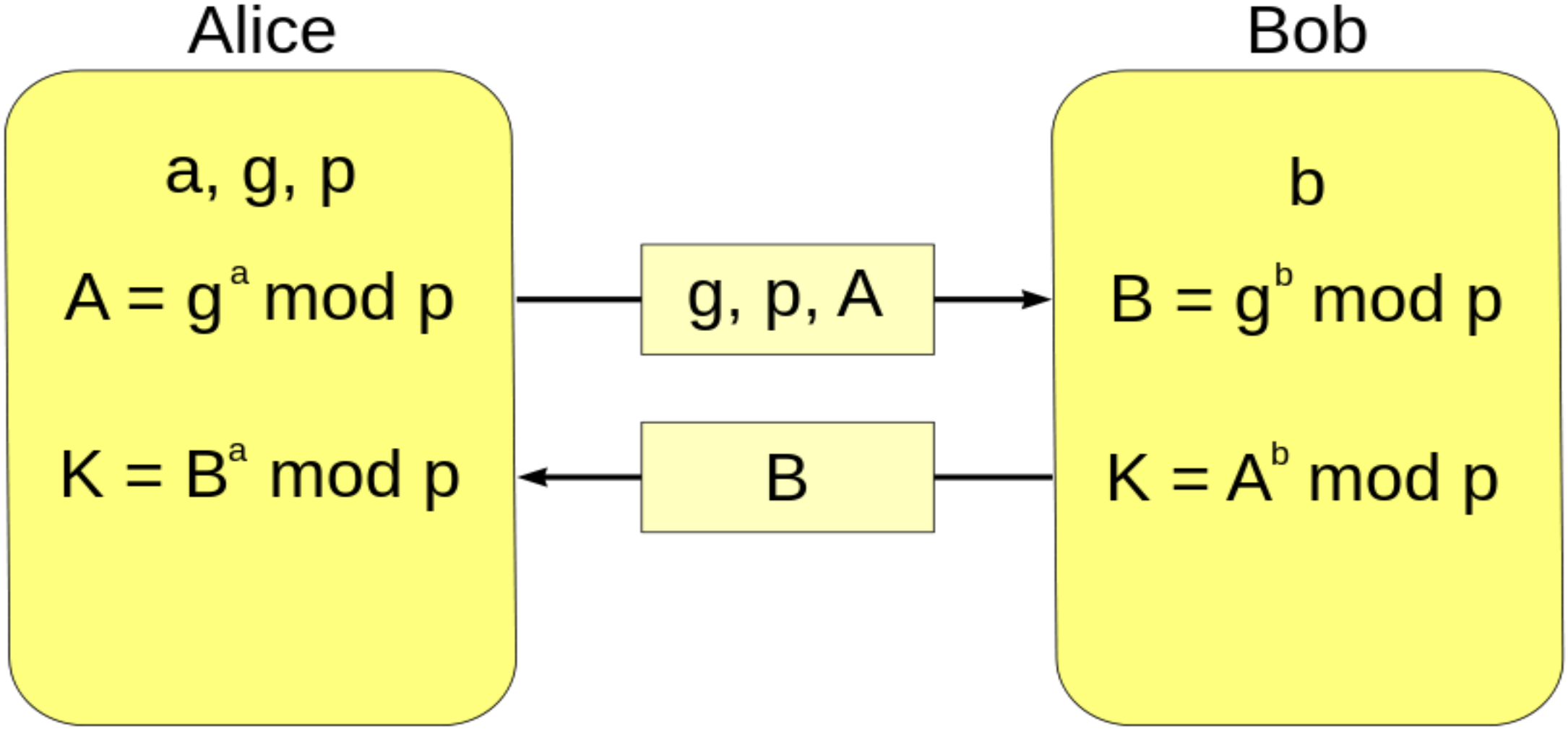
訾晓鹏

2018年9月16日

# The Monero Difference

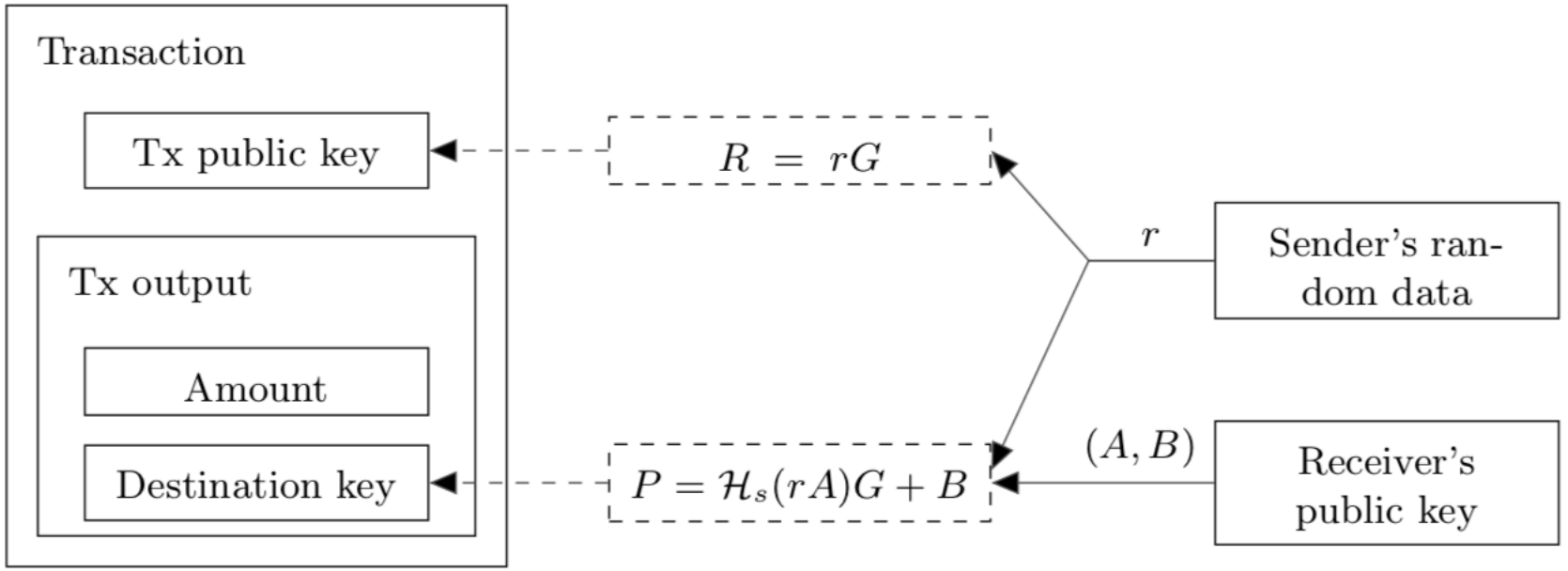


# Diffie–Hellman key exchange



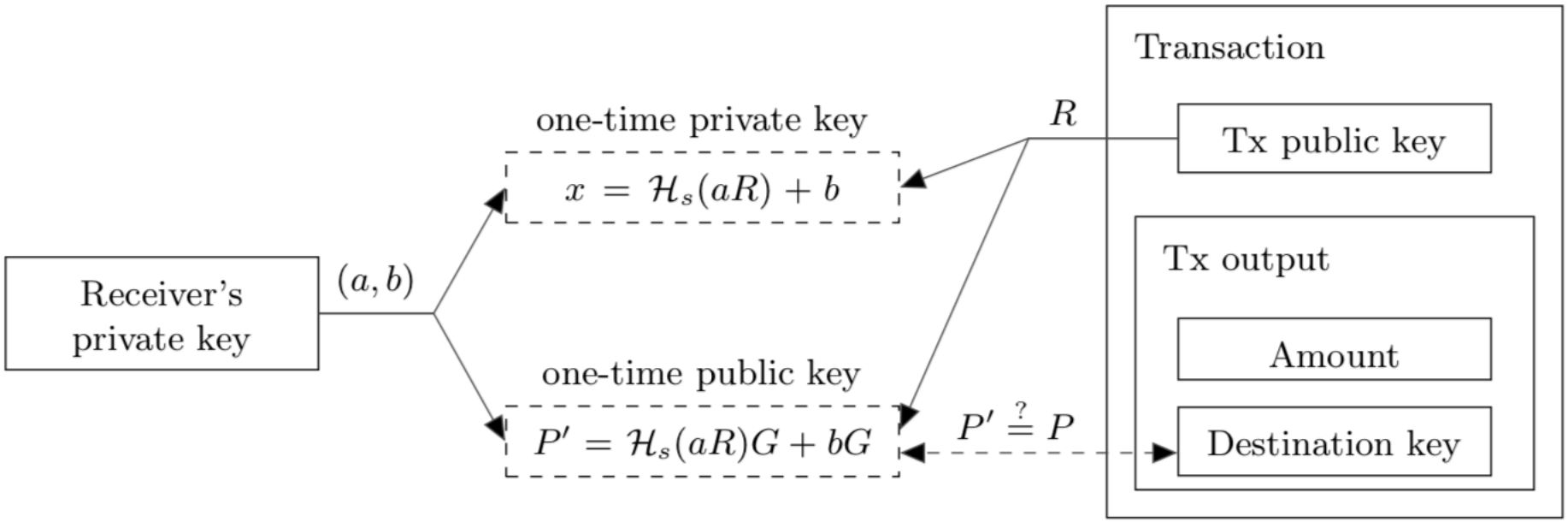

$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

# Stealth Address




Sender

# Stealth Address




Receiver

# Spend Key and View Key

- 1. Bob know the transaction
- 2. Bob can spend
- 3. Alice can not spend
- 4. Carol do not know who receive

- Bob's public key (A, B)
- P = Hs(rA)G+B
- Spend key: Hs(rA)+b

$\mathcal{H}_s$: a cryptographic hash function $\{0,1\}^* \to \mathbb{F}_q$;

# Ring signature

- no managers
- no prearranged groups
- anonymity

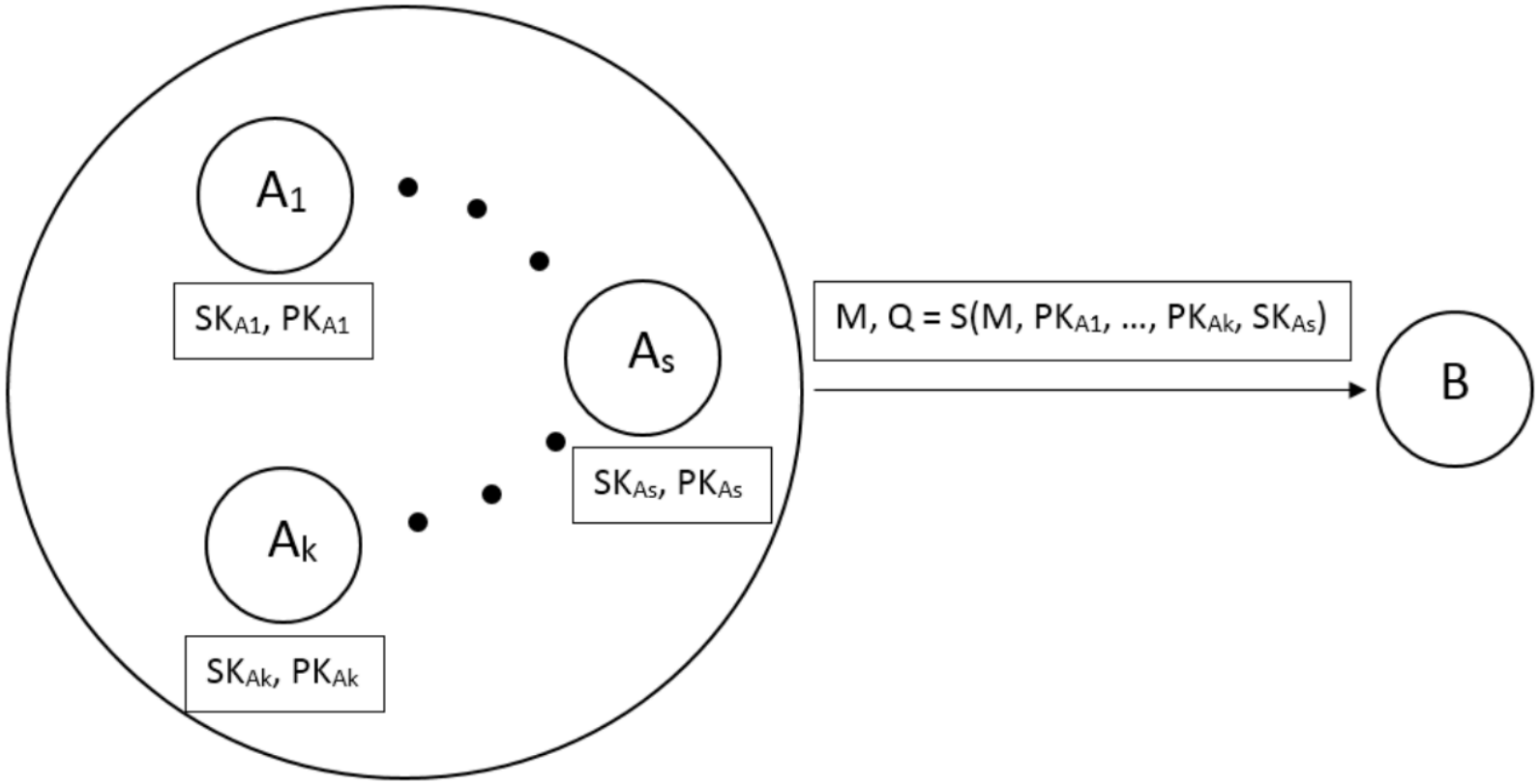
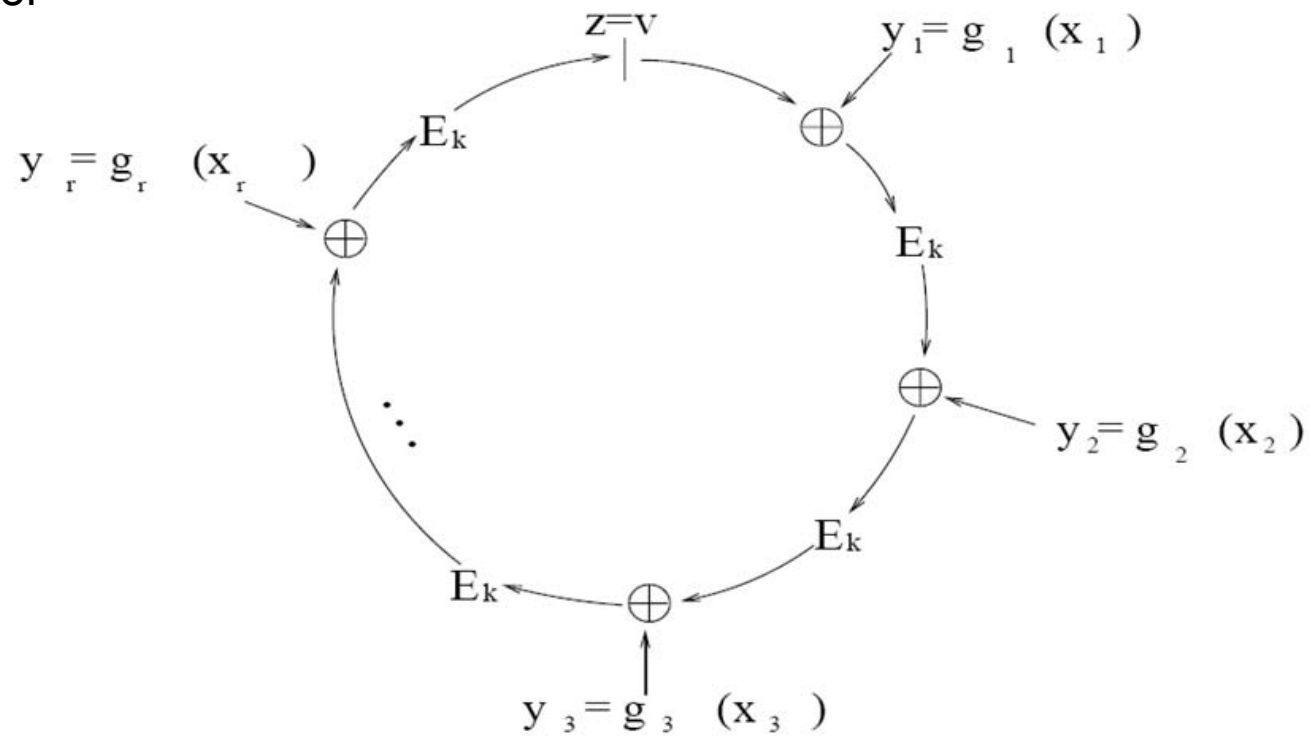



Figure 1 - Ring signature scheme with As member as actual signer

# Ring Signature

RST01(Ronald Rivest, Adi Shamir and Yael Tauman)

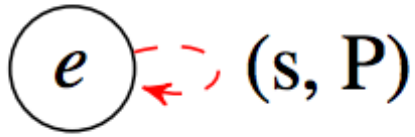
$$\sigma = (v, x_1, \ldots, x_r)$$




$$C_{k,v}(y_1, y_2, \ldots, y_r) = E_k(y_r \oplus E_k(y_{r-1} \oplus E_k(y_{r-2} \oplus E_k(\ldots \oplus E_k(y_1 \oplus v)\ldots))))$$

# Ring Signature

- Time travel and chameleon hashes
- Construct hash function, e = H(m,e,s)

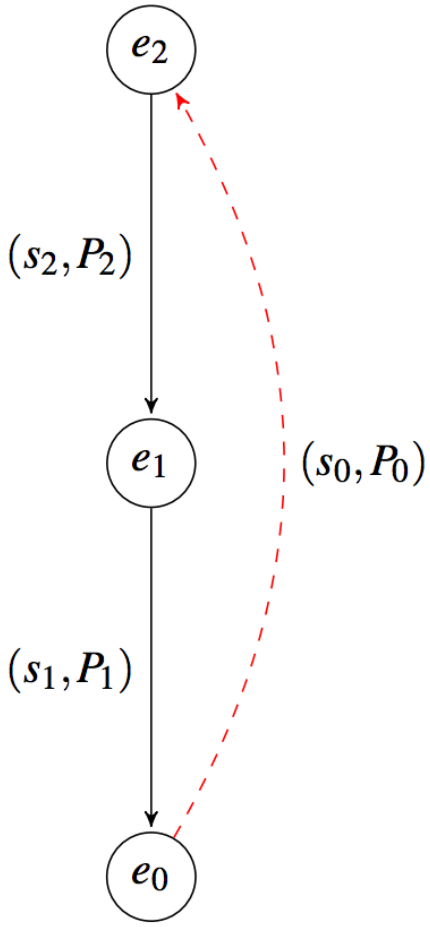



1. P = xG
2. e = H(m ll kG)
3. s = k+xe
4. Let H(m,e,s) = H(m ll sG–eP)

# AOS signature

- PK：P0,P1,P2

- σ = {e0,s0,s1,s2}
- kiG = siG + eiPi
- ei = H(kiG), if i!=0
- σ is true, if e0==H(k2G)



# MLSAG

- Multilayered Linkable Spontaneous Anonymous Group signatures
- Signature is (I1, ..., Im, c1, s1, ..., sm1 , s12, ..., sm2 , ..., s1n, ..., smn ),

$$L_\pi^j = \alpha_j G$$

$$R_\pi^j = \alpha_j H\left(P_\pi^j\right)$$

for random scalars $\alpha_j$ and $j = 1, ..., m$. Now, again analogously to section 2.1, set:

$$c_{\pi+1} = H\left(\mathfrak{m}, L_\pi^1, R_\pi^1, ..., L_\pi^m, R_\pi^m\right).$$

$$L_{\pi+1}^j = s_{\pi+1}^j G + c_{\pi+1} P_{\pi+1}^j$$

$$R_{\pi+1}^j = s_{\pi+1}^j H\left(P_{\pi+1}^j\right) + c_{\pi+1} I_j$$

and repeat this, incrementing $i$ modulo $n$ until we arrive at

$$L_{\pi-1}^j = s_{i-1}^j G + c_{i-1} P_{i-1}^j$$

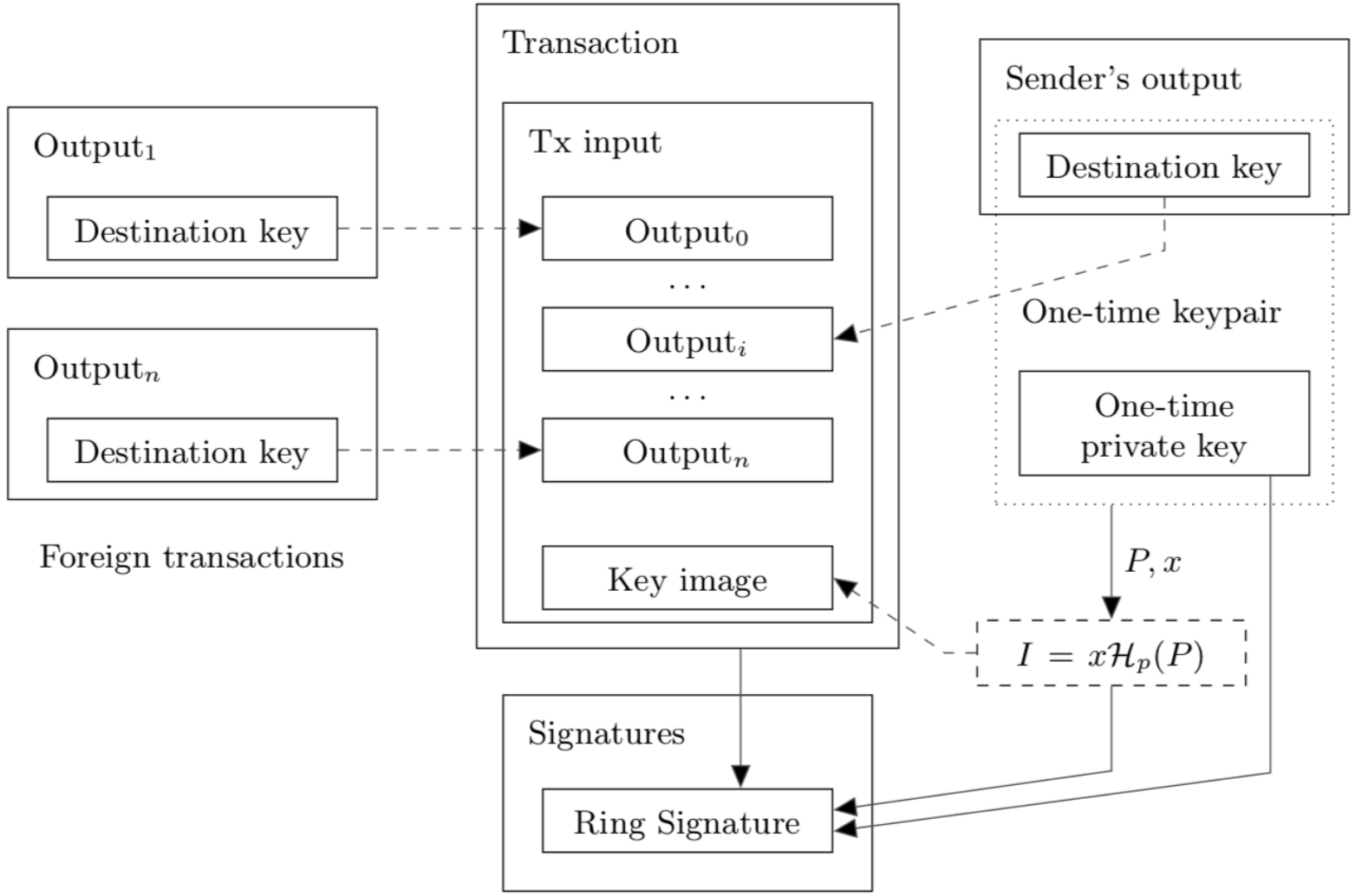
$$R_{\pi-1}^j = s_{i-1}^j H\left(P_{i-1}^j\right) + c_{i-1} \cdot I_j$$

$$c_\pi = H\left(\mathfrak{m}, L_{\pi-1}^1, R_{\pi-1}^1, ..., L_{\pi-1}^m, R_{\pi-1}^m\right).$$

# Key Image

- Prevent double-spend

$I = xH_p(P_j)$



# RingCT

- Pedersen Commitment
- Range Proof

# Pedersen Commitment

- commitment = xG + aH
- Addtion and commutative property
  - C(BF1, data1) + C(BF2, data2) == C(BF1 + BF2, data1 + data2)
  - C(BF1, data1) - C(BF1, data1) == 0
- verify the transaction
  - (In1 + In2 + In3 + plaintext_input_amount*H...) - (Out1 + Out2 + Out3 + ... fees*H) == 0.

# Modification for Anonymity

$$C_{in} = x_c G + aH$$

$$C_{out-1} = y_1 G + b_1 H$$

$$C_{out-2} = y_2 G + b_2 H$$

$$C_{in} - \sum_{i=1}^{2} C_{out-i}$$

$$= x_c G + aH - y_1 G - b_1 H - y_2 G - b_2 H$$

$$= zG.$$

xc =y1+y2+z
yi are mask values, z>0
a = b1 +b2

$$\left\{ P_1 + C_{1,in} - \sum_j C_{j,out}, ..., P_s + C_{s,in} - \sum_j C_{j,out}, ..., P_n + C_{n,in} - \sum_j C_{j,out} \right\}.$$

# Range proof

- addition of large values can 'overflow'
- (1 + 1) – (-5+7) == 0
- "someone spends two bitcoins, gets a '-5' bitcoin out that they discard out, and a 7 bitcoin output"

# Range Proof

1. $b = b_0 2^0 + b_1 2^1 + b_2 2^2 + \cdots + b_n 2^n$
2. computes commitments Cj to bj · 2j

$$C^1_{out,i} + C^2_{out,i} + \cdots + C^n_{out,i} = C_{out,i}$$

3. computes a ring signature on ($C_j$ ,$C_j$ –$2_j$H)

$$(C^j_{out,i}, C^j_{out,i} - 2^j H)$$

# Bullet Proof

- reduce transactions sizes by greater than 80%
- in turn lower fees which are calculated on a XMR/byte basis

# Roadmap

2014 | 2015 | 2016 | 2017 | **2018** | Future

- 2018-04-06: New Proof of Work CryptoNoteV7
- 2018-04-06: Network upgrade to increase minimal ringsize to 7, integrate multisig, subaddresses, and change PoW algo
- 2018-04-24: Getmonero.org Localization in French and Polish
- 2018-06-04: Ledger Hardware Wallets Support
- 2018-08-01: Kovri alpha release
- Forum Funding System redesign
- Implementation of BulletProofs instead of RingCT to reduce transaction sizes
- Kovri beta release

# References


- CryptoNote v 2.0
- http://cryptowiki.net/index.php?title=Ring_signatures_and_their_applications
- RING CONFIDENTIAL TRANSACTIONS
- Confidential Transactions