CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

A Holistic Security Analysis of Monero Transactions


Cas Cremers


Julian Loss


Benedikt Wagner

DFG

erc

Monero and RingCT

Monero and RingCT

- Privacy-Focused Currency
- 2.5 Billion USD Market Cap

Monero and RingCT

- Privacy-Focused Currency
- 2.5 Billion USD Market Cap
- Transactions: RingCT

Monero and RingCT

- Privacy-Focused Currency
- 2.5 Billion USD Market Cap
- Transactions: RingCT
  - Linkable Ring Signatures
  - Commitments
  - Range Proofs
  - Stealth Addresses

Monero and RingCT

- Privacy-Focused Currency
- 2.5 Billion USD Market Cap
- Transactions: RingCT

Is RingCT secure?

- Linkable Ring Signatures
- Commitments
- Range Proofs
- Stealth Addresses

Prior Work on RingCT

Prior Work on RingCT

Security for Building Blocks

Prior Work on RingCT

Security for Building Blocks

Composability?

Prior Work on RingCT

Security for Building Blocks

Security for New Schemes

Composability?

Prior Work on RingCT

Security for Building Blocks

Composability?

Security for New Schemes

Implications for RingCT?

Prior Work on RingCT

Security for Building Blocks

Security for New Schemes

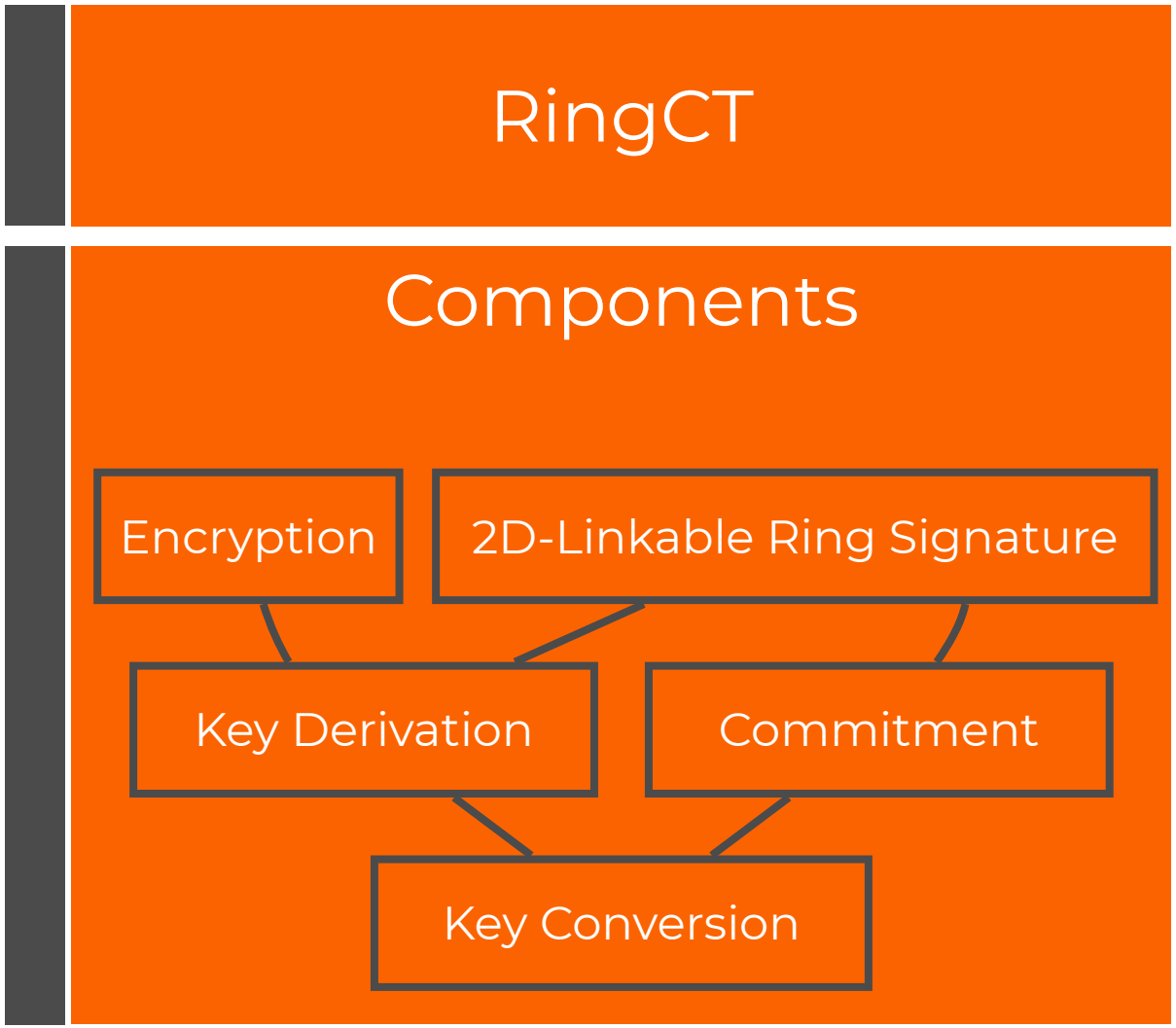
Composability?

Implications for RingCT?

Is RingCT secure?

Our Work: Abstraction and Security Model

Our Work: Abstraction and Security Model



Our Work: Abstraction and Security Model

RingCT

Components

Encryption

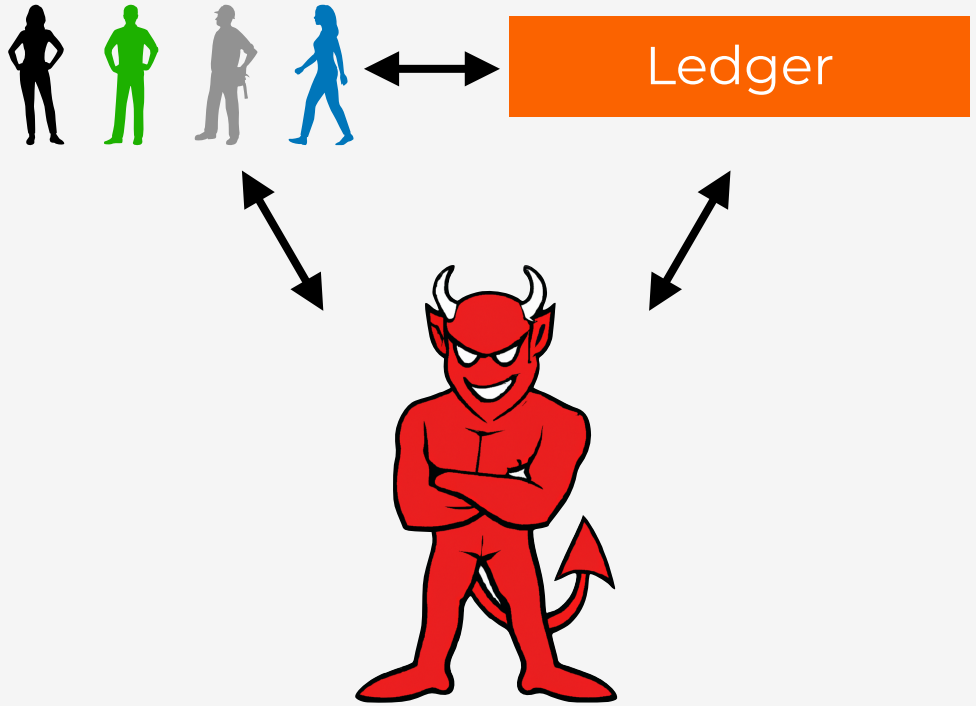
2D-Linkable Ring Signature

Key Derivation

Commitment

Key Conversion

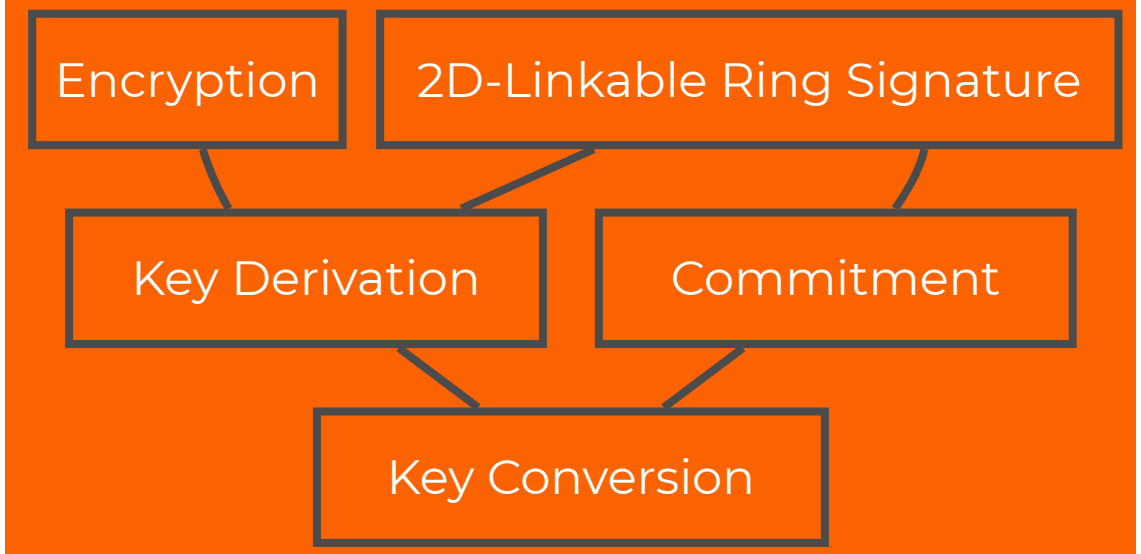
Security Definition



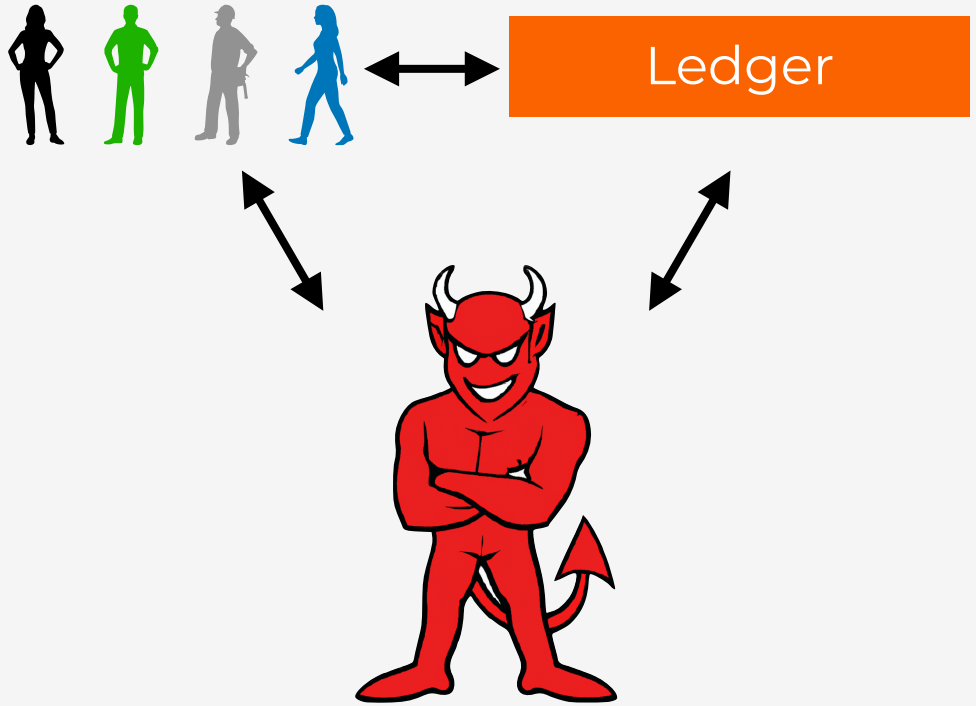
Our Work: Abstraction and Security Model

RingCT

Components



Security Definition

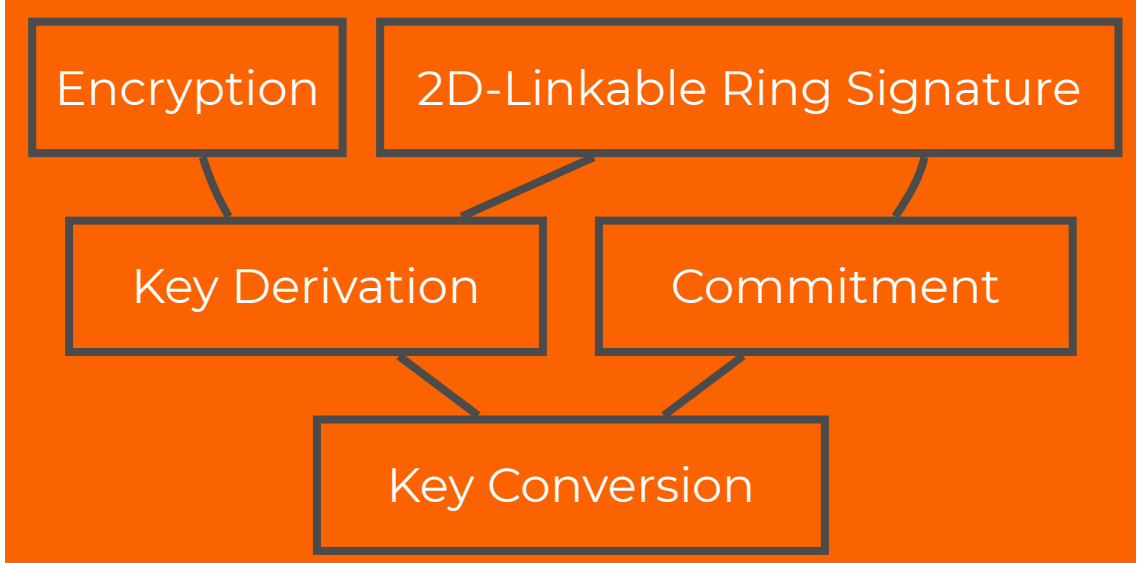


1. *Adversary can not steal coins.*

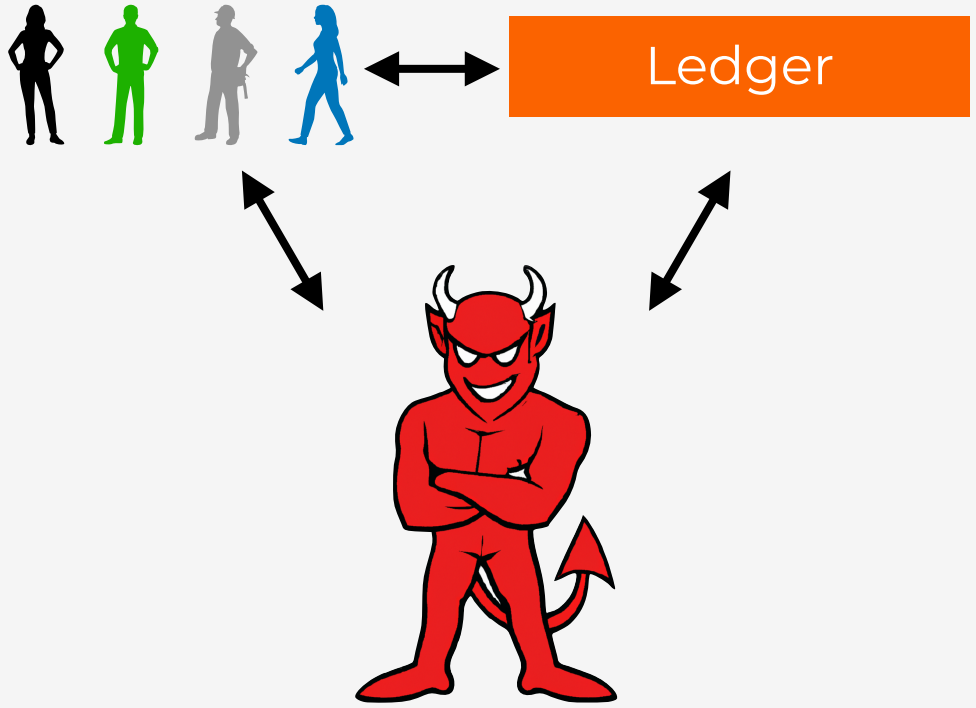
Our Work: Abstraction and Security Model

RingCT

Components



Security Definition



1. *Adversary can not steal coins.*
2. *Adversary can not create coins.*

Our Work: Security Analysis

Our Work: Security Analysis

Security of RingCT

Our Work: Security Analysis

Security of RingCT

Security of Components

Our Work: Security Analysis

Security of RingCT

Security of Components

2D-Linkable Ring Signature

Key Derivation

Knowledge Soundness

Knowledge Linkability

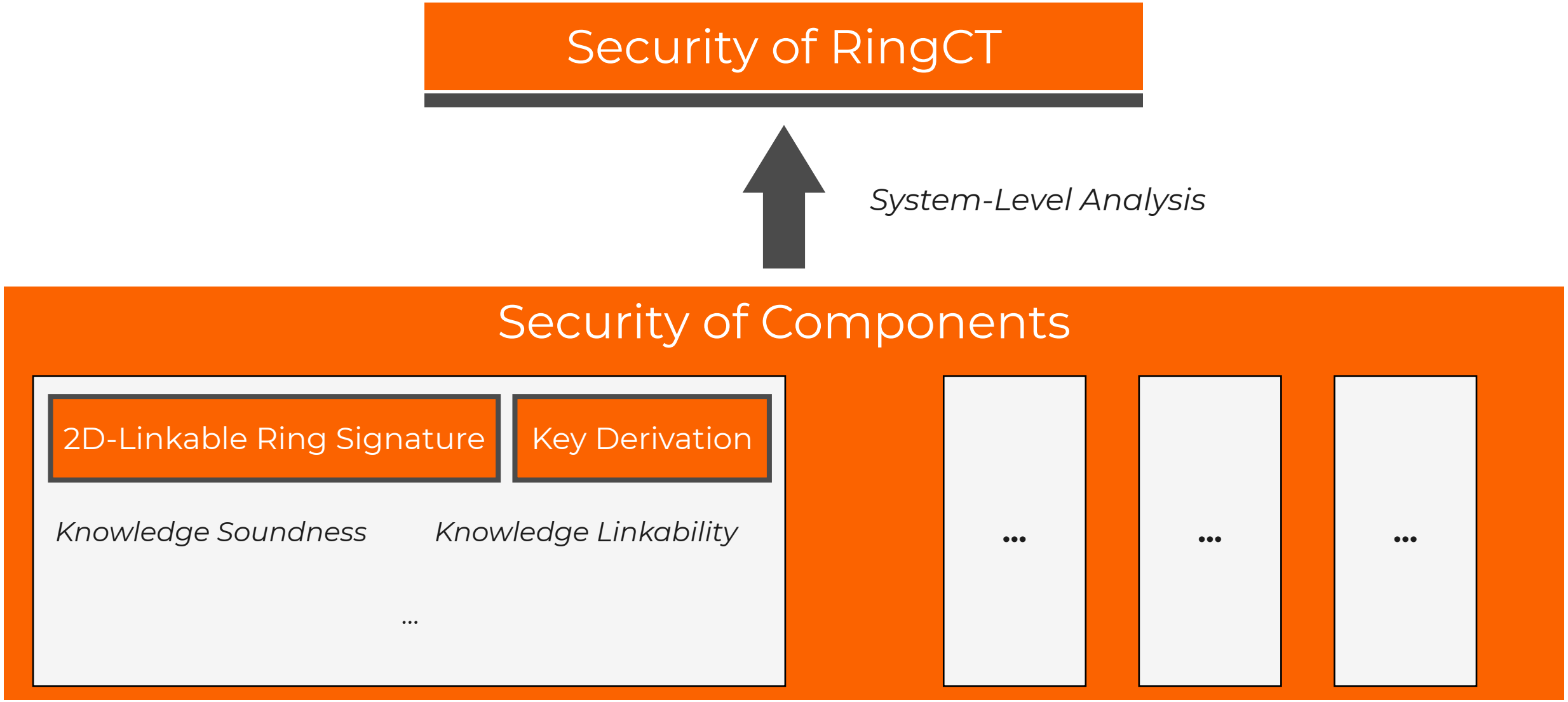
...

...

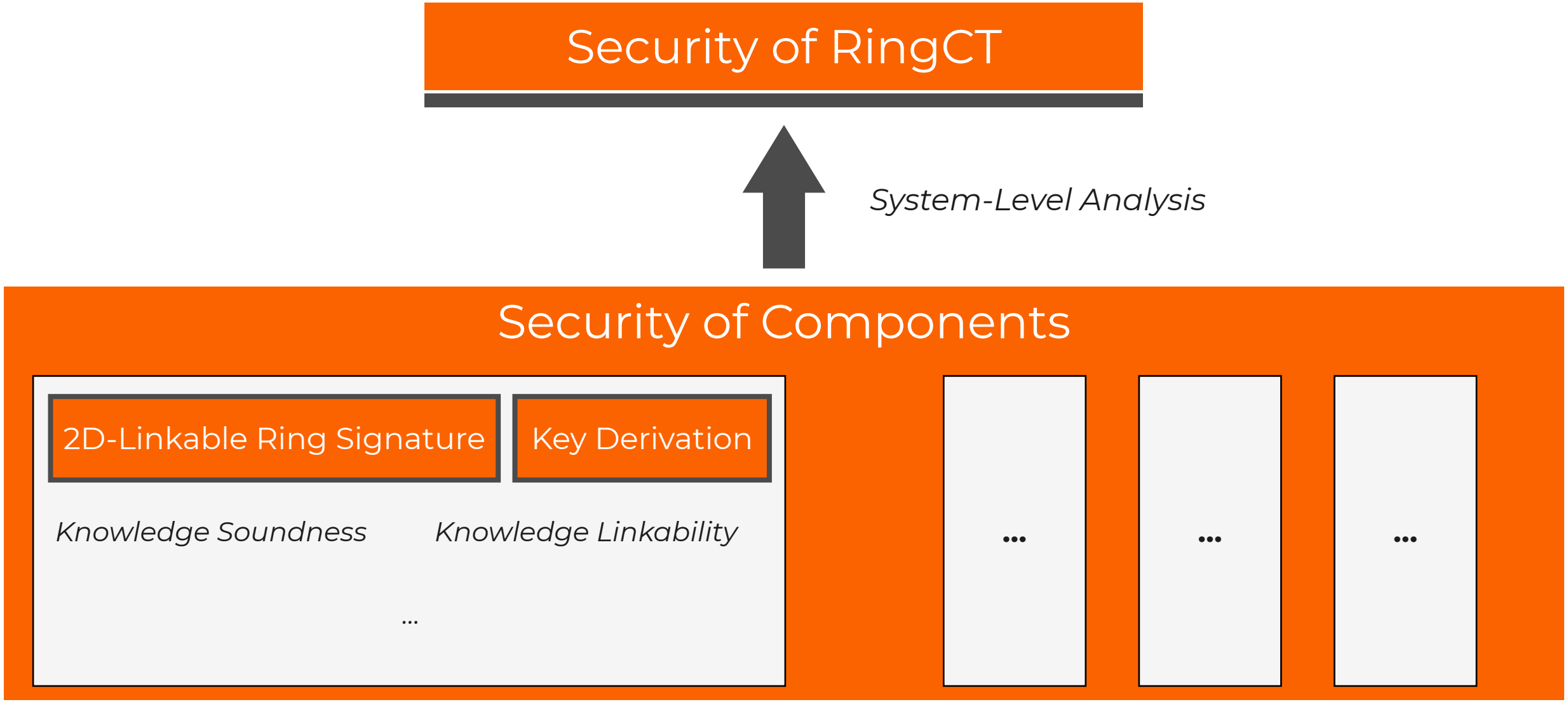
...

...

Our Work: Security Analysis



Our Work: Security Analysis



Outline

Outline

This Talk

Outline

This Talk

Why is security unclear?

Stealth Addresses

Outline

This Talk

Why is security unclear?

Stealth Addresses

What do we prove?

Security Model

Outline

This Talk

Why is security unclear?

Stealth Addresses

What do we prove?

Security Model

Long Talk

YouTube

Details on RingCT

Proof Techniques

Outline

This Talk

- Why is security unclear?
- Stealth Addresses
- What do we prove?
- Security Model

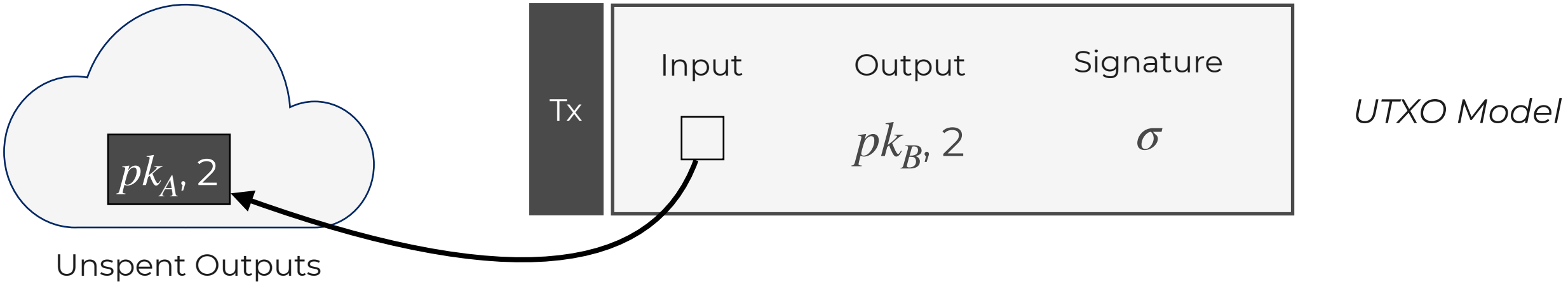
Long Talk

YouTube

- Details on RingCT
- Proof Techniques

Anatomy of Transactions

Anatomy of Transactions



Main Ideas of RingCT

Main Ideas of RingCT

Hiding Senders

Hiding Amounts

Hiding Receivers

Main Ideas of RingCT

Hiding Senders

Hiding Amounts

Hiding Receivers

Ring Signatures

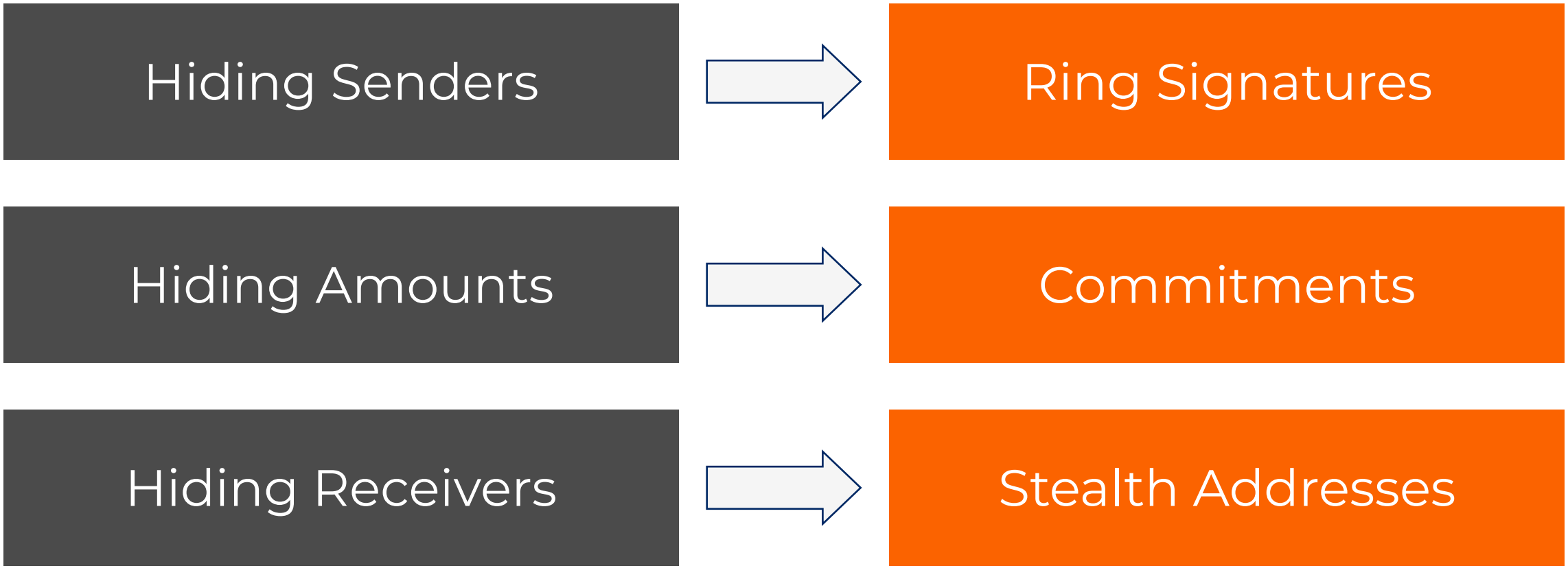
Main Ideas of RingCT

Hiding Senders → Ring Signatures

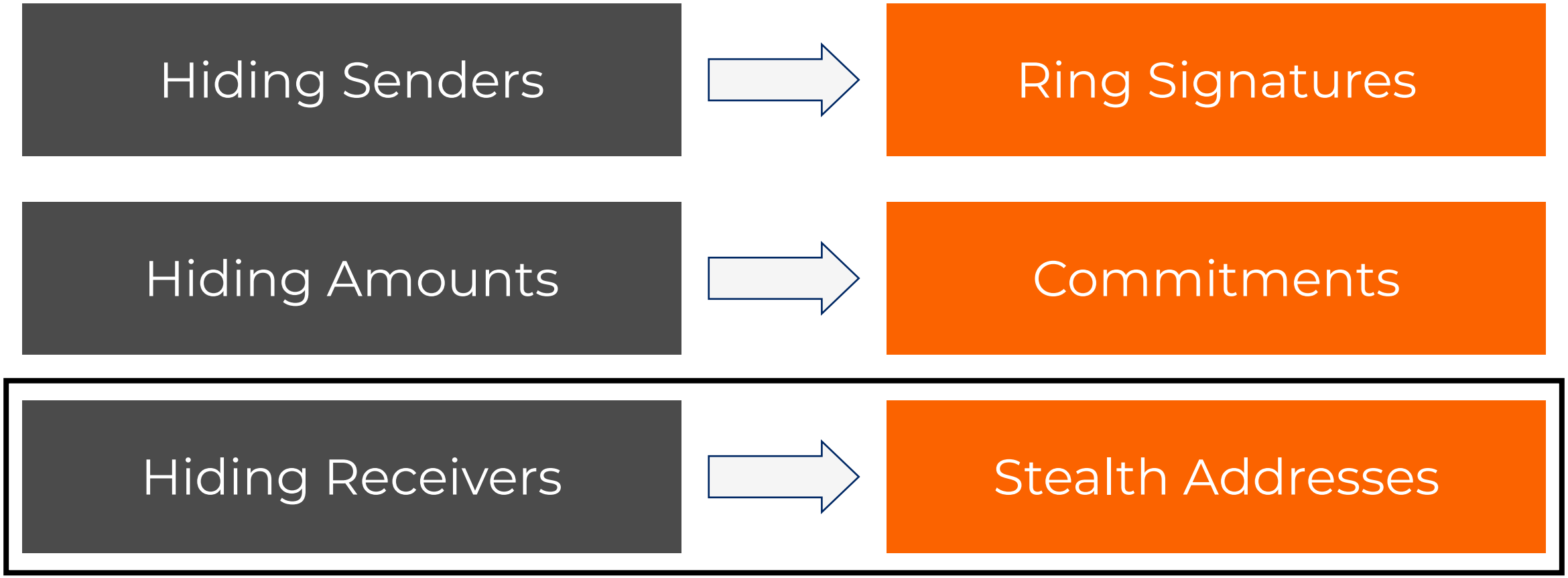
Hiding Amounts → Commitments

Hiding Receivers

Main Ideas of RingCT

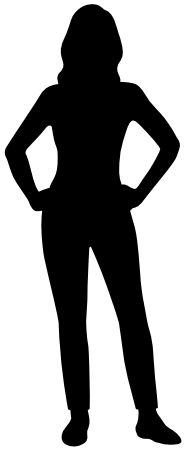


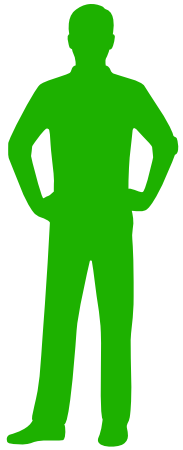
Main Ideas of RingCT



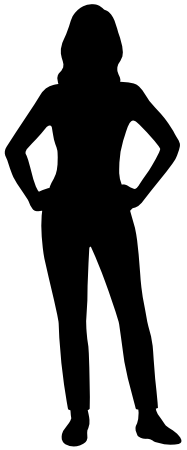
Hiding Receivers with Stealth Addresses

Hiding Receivers with Stealth Addresses

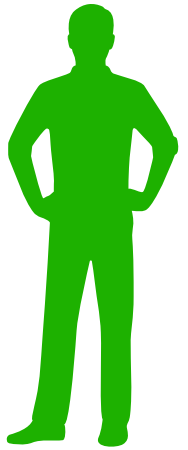




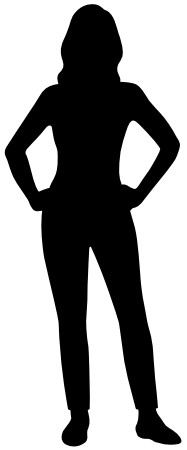
Hiding Receivers with Stealth Addresses



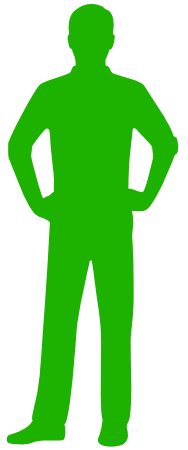
Tx	Inputs	Outputs	Signatures
	$pk_A, 1$		σ_1
	$pk'_A, 1$		σ_2



Hiding Receivers with Stealth Addresses

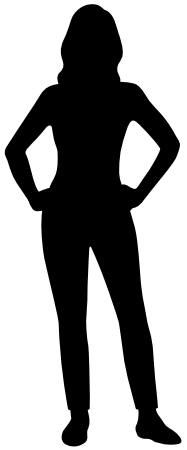


Tx	Inputs	Outputs	Signatures
	$pk_A, 1$		σ_1
	$pk'_A, 1$		σ_2

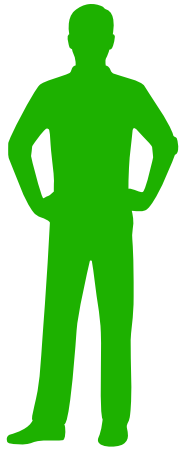


Goal #1: Bob can identify output

Hiding Receivers with Stealth Addresses



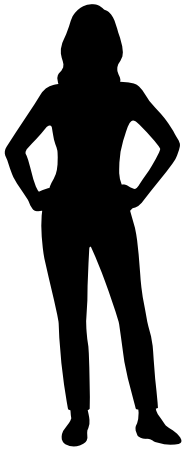
Tx	Inputs	Outputs	Signatures
	$pk_A, 1$		σ_1
	$pk'_A, 1$		σ_2



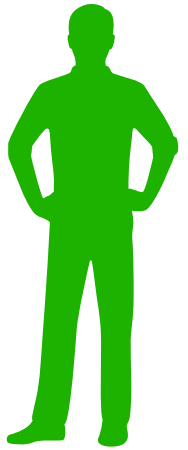
Goal #1: Bob can identify output

Goal #2: No one can link output to Bob

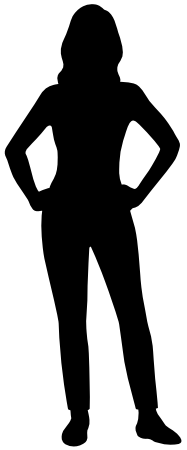
Hiding Receivers with Stealth Addresses

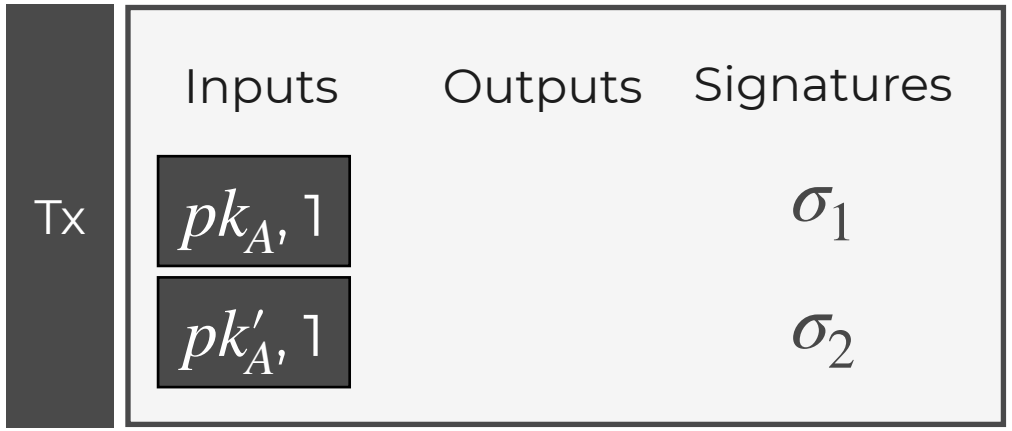


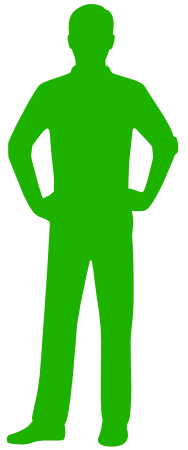
Tx	Inputs	Outputs	Signatures
	$pk_A, 1$		σ_1
	$pk'_A, 1$		σ_2



Hiding Receivers with Stealth Addresses

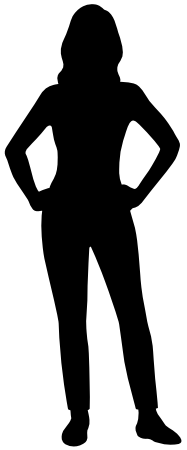




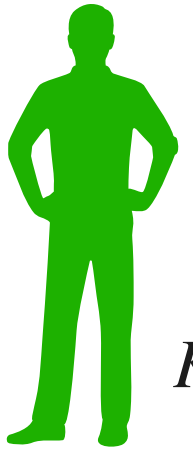


$k_v, k_s \leftarrow \mathbb{Z}_p$

Hiding Receivers with Stealth Addresses



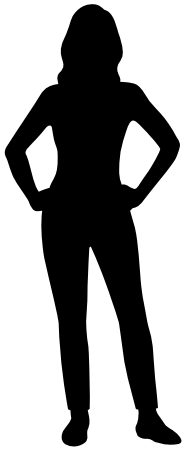
Tx	Inputs	Outputs	Signatures
	$pk_A, 1$		σ_1
	$pk'_A, 1$		σ_2



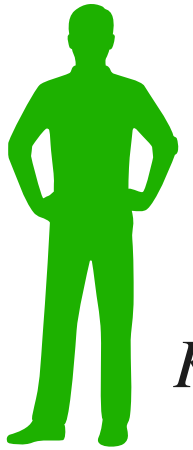
$$k_v, k_s \leftarrow \mathbb{Z}_p$$

$$K_v = g^{k_v},\ K_s = g^{k_s}$$

Hiding Receivers with Stealth Addresses



Tx	Inputs	Outputs	Signatures
	$pk_A, 1$		σ_1
	$pk'_A, 1$		σ_2

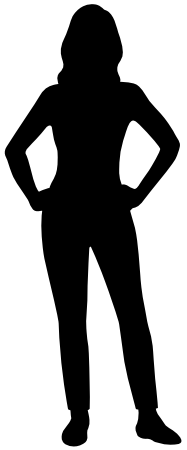


$$k_v, k_s \leftarrow \mathbb{Z}_p$$

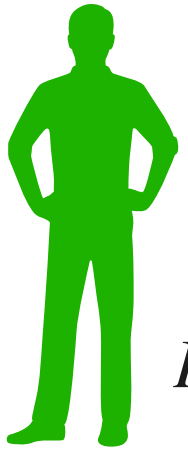
$$K_v = g^{k_v},\ K_s = g^{k_s}$$

Public Long-Term Key

Hiding Receivers with Stealth Addresses



Tx	Inputs	Outputs	Signatures
	$pk_A, 1$		σ_1
	$pk'_A, 1$		σ_2



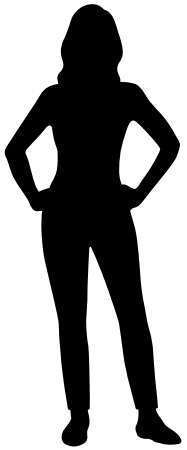
$k_v, k_s \leftarrow \mathbb{Z}_p$

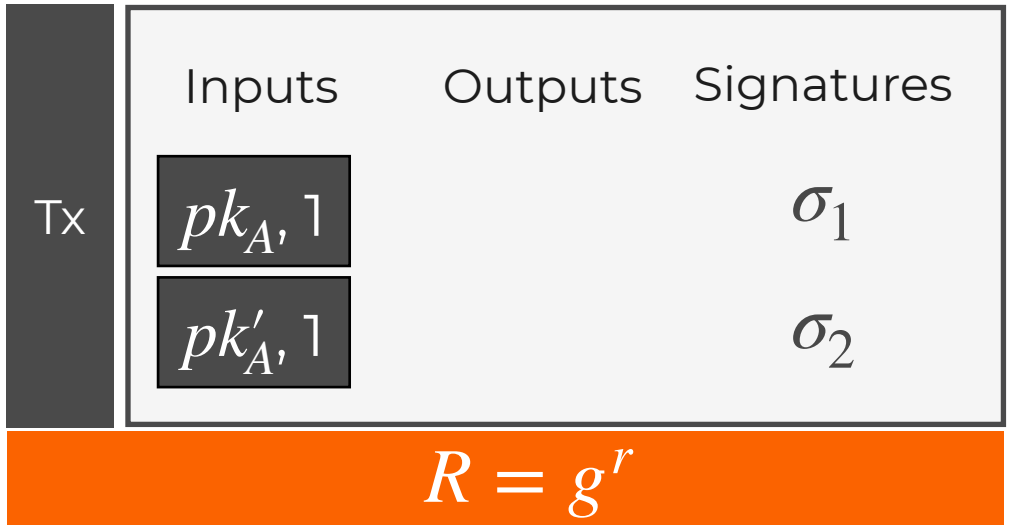
$K_v = g^{k_v}, K_s = g^{k_s}$

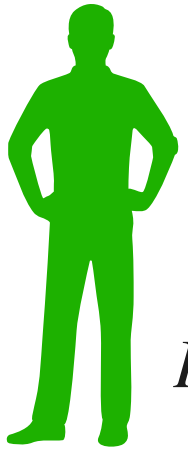
Public Long-Term Key

$r \leftarrow \mathbb{Z}_p$

Hiding Receivers with Stealth Addresses







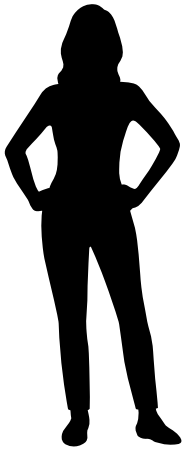
$r \leftarrow \mathbb{Z}_p$

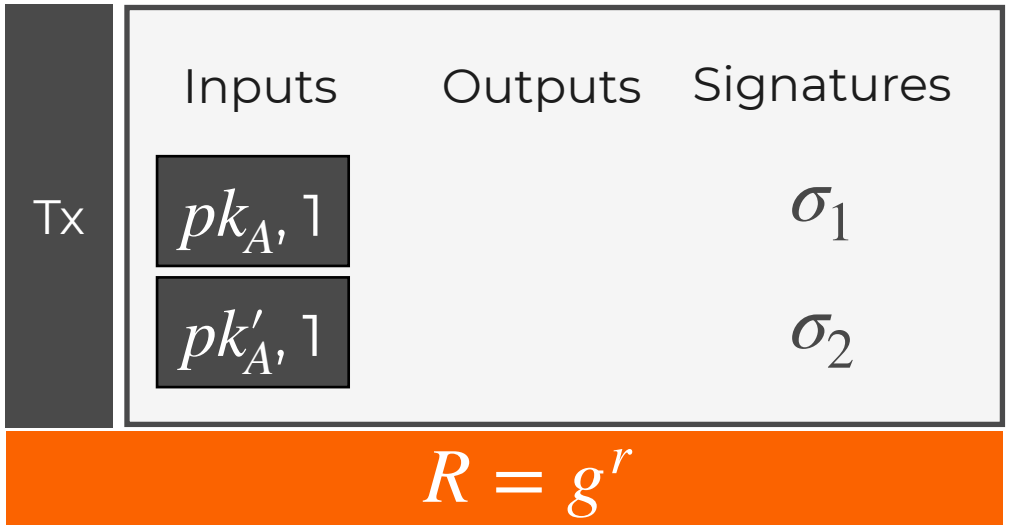
$k_v, k_s \leftarrow \mathbb{Z}_p$

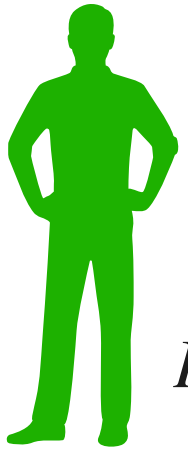
$K_v = g^{k_v}, K_s = g^{k_s}$

Public Long-Term Key

Hiding Receivers with Stealth Addresses







$k_v, k_s \leftarrow \mathbb{Z}_p$

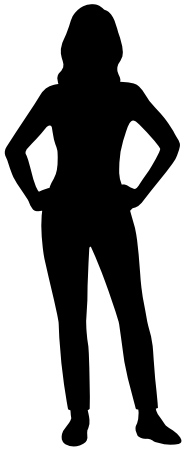
$K_v = g^{k_v}, K_s = g^{k_s}$

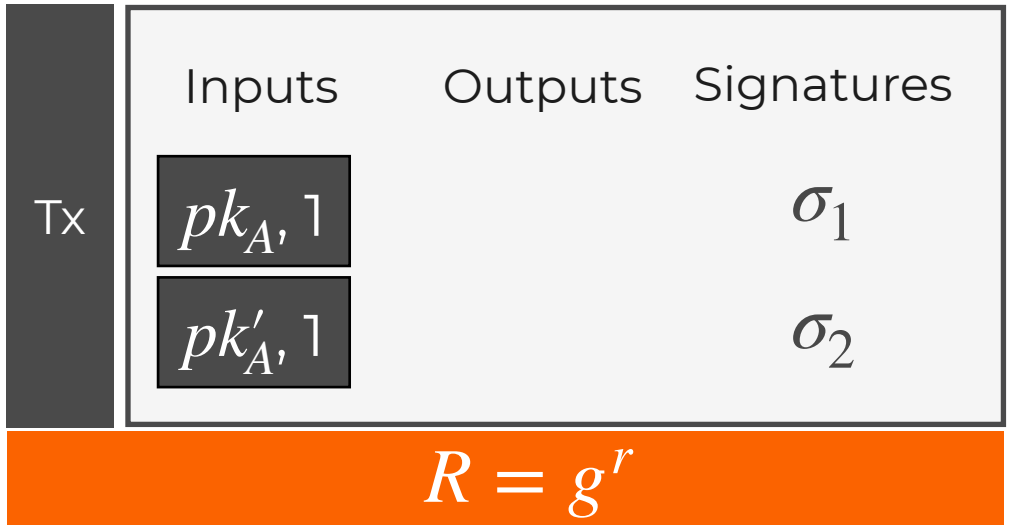
Public Long-Term Key

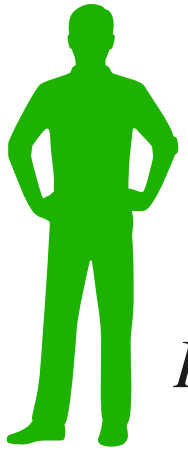
$r \leftarrow \mathbb{Z}_p$

$ok := K_v^r$

Hiding Receivers with Stealth Addresses







$k_v, k_s \leftarrow \mathbb{Z}_p$

$K_v = g^{k_v}, K_s = g^{k_s}$

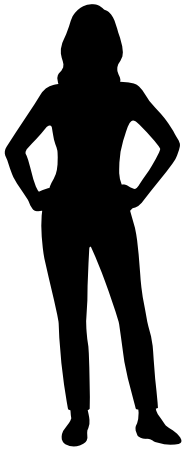
Public Long-Term Key

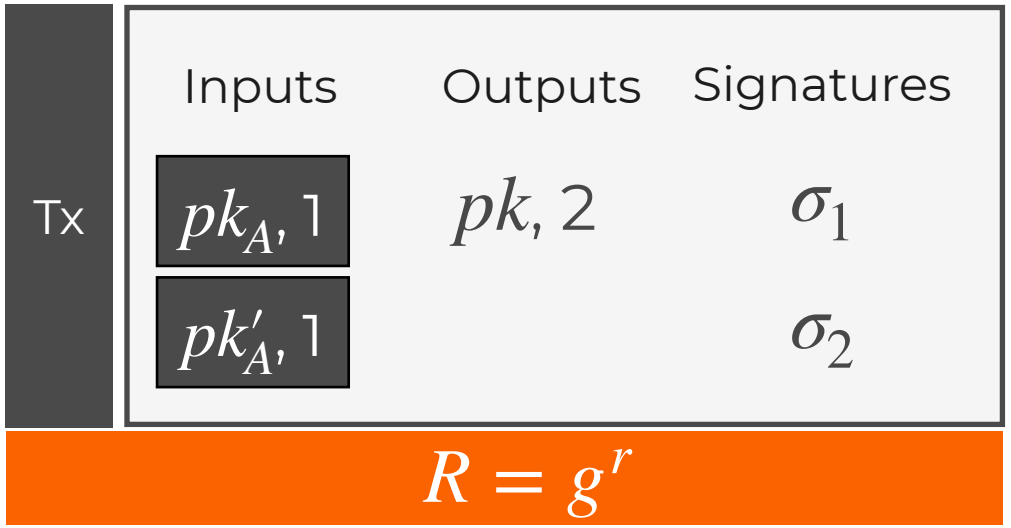
$r \leftarrow \mathbb{Z}_p$

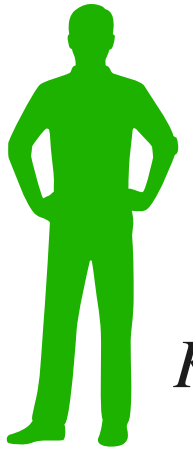
$ok := K_v^r$

$pk := g^{H(ok)} \cdot K_s$

Hiding Receivers with Stealth Addresses







$k_v, k_s \leftarrow \mathbb{Z}_p$

$K_v = g^{k_v}, K_s = g^{k_s}$

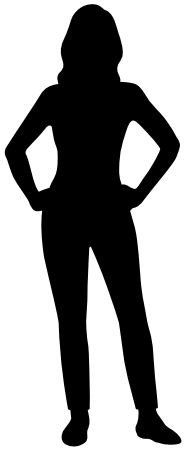
Public Long-Term Key

$r \leftarrow \mathbb{Z}_p$

$ok := K_v^r$

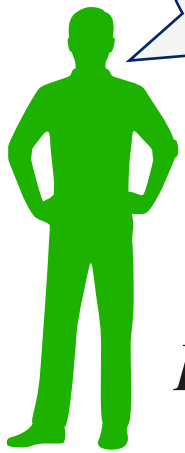
$pk := g^{H(ok)} \cdot K_s$

Hiding Receivers with Stealth Addresses



Tx	Inputs	Outputs	Signatures
	$pk_A, 1$	$pk, 2$	σ_1
	$pk'_A, 1$		σ_2

$R = g^r$



$k_v, k_s \leftarrow \mathbb{Z}_p$

$K_v = g^{k_v}, K_s = g^{k_s}$

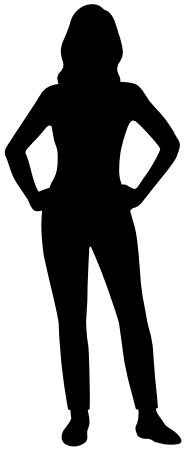
Public Long-Term Key

$r \leftarrow \mathbb{Z}_p$

$ok := K_v^r$

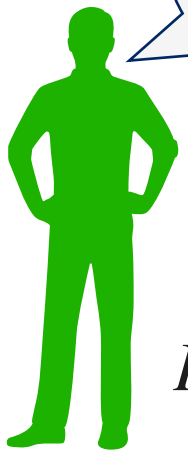
$pk := g^{H(ok)} \cdot K_s$

Hiding Receivers with Stealth Addresses



Tx	Inputs	Outputs	Signatures
	$pk_A, 1$	$pk, 2$	σ_1
	$pk'_A, 1$		σ_2

$R = g^r$



Is this output mine?

$k_v, k_s \leftarrow \mathbb{Z}_p$

$K_v = g^{k_v}, K_s = g^{k_s}$

Public Long-Term Key

$r \leftarrow \mathbb{Z}_p$

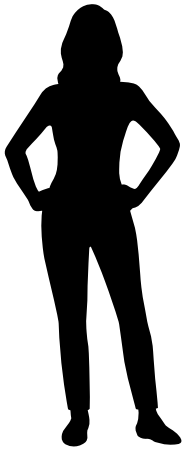
$ok := K_v^r$

$pk := g^{H(ok)} \cdot K_s$

$ok := R^{k_v}$

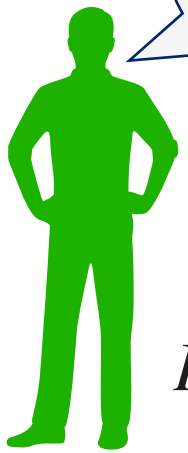
$pk = g^{H(ok)} \cdot K_s$??

Hiding Receivers with Stealth Addresses



Tx	Inputs	Outputs	Signatures
	$pk_A, 1$	$pk, 2$	σ_1
	$pk'_A, 1$		σ_2

$R = g^r$



Is this output mine?

$k_v, k_s \leftarrow \mathbb{Z}_p$

$K_v = g^{k_v}, K_s = g^{k_s}$

Public Long-Term Key

$r \leftarrow \mathbb{Z}_p$

$ok := K_v^r$

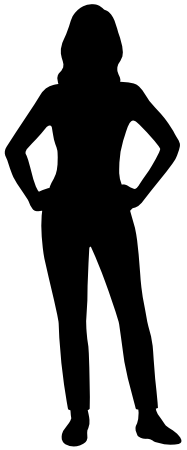
$pk := g^{H(ok)} \cdot K_s$

$ok := R^{k_v}$

$pk = g^{H(ok)} \cdot K_s$??

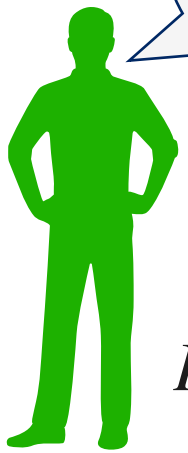
$sk := H(ok) + k_s$

Hiding Receivers with Stealth Addresses



Tx	Inputs	Outputs	Signatures
	$pk_A, 1$	$pk, 2$	σ_1
	$pk'_A, 1$		σ_2

$R = g^r$



Is this output mine?

$k_v, k_s \leftarrow \mathbb{Z}_p$

$K_v = g^{k_v}, K_s = g^{k_s}$

Public Long-Term Key

$r \leftarrow \mathbb{Z}_p$

$ok := K_v^r$

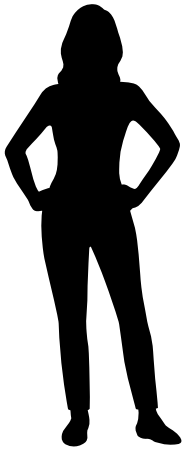
$pk := g^{H(ok)} \cdot K_s$

$ok := R^{k_v}$

$pk = g^{H(ok)} \cdot K_s$??

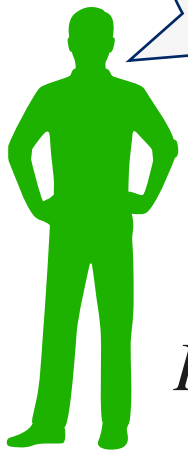
$sk := H(ok) + k_s$

Hiding Receivers with Stealth Addresses



Tx	Inputs	Outputs	Signatures
	$pk_A, 1$	$pk, 2$	σ_1
	$pk'_A, 1$		σ_2

$R = g^r$



Is this output mine?

$k_v, k_s \leftarrow \mathbb{Z}_p$

$K_v = g^{k_v}, K_s = g^{k_s}$

Public Long-Term Key

$r \leftarrow \mathbb{Z}_p$

$ok := K_v^r$

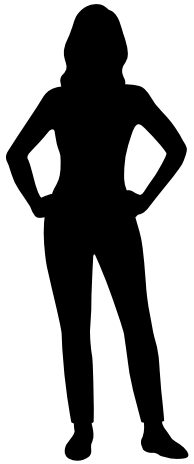
$pk := g^{H(ok)} \cdot K_s$

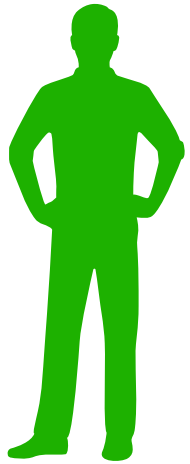
$ok := R^{k_v}$

$pk = g^{H(ok)} \cdot K_s$??

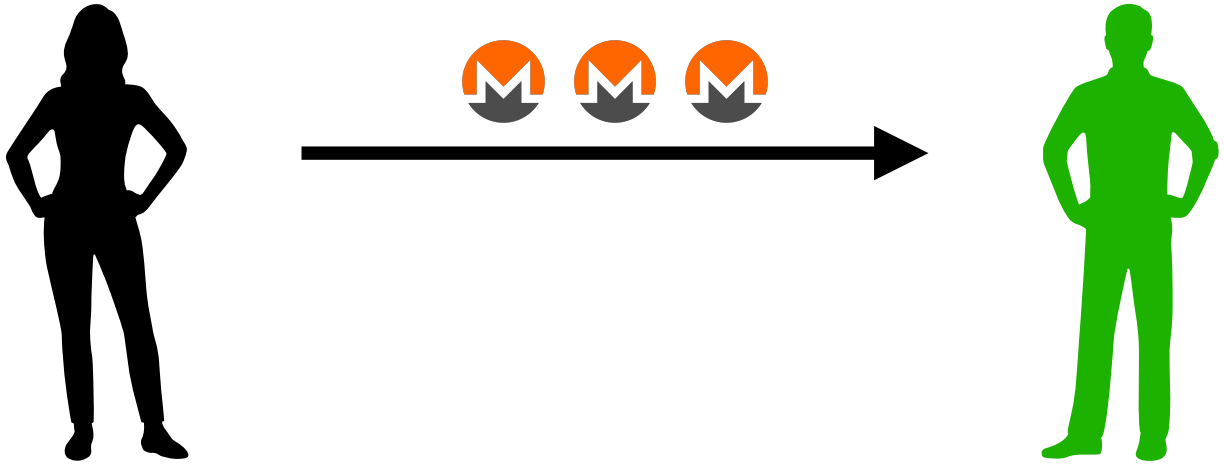
$sk := H(ok) + k_s$

Hiding Receivers with Stealth Addresses

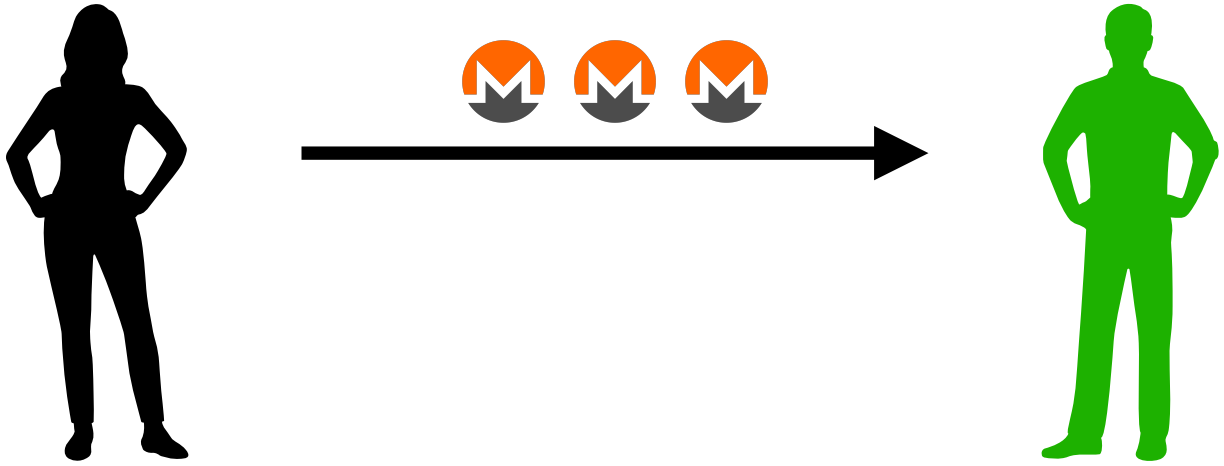




Hiding Receivers with Stealth Addresses

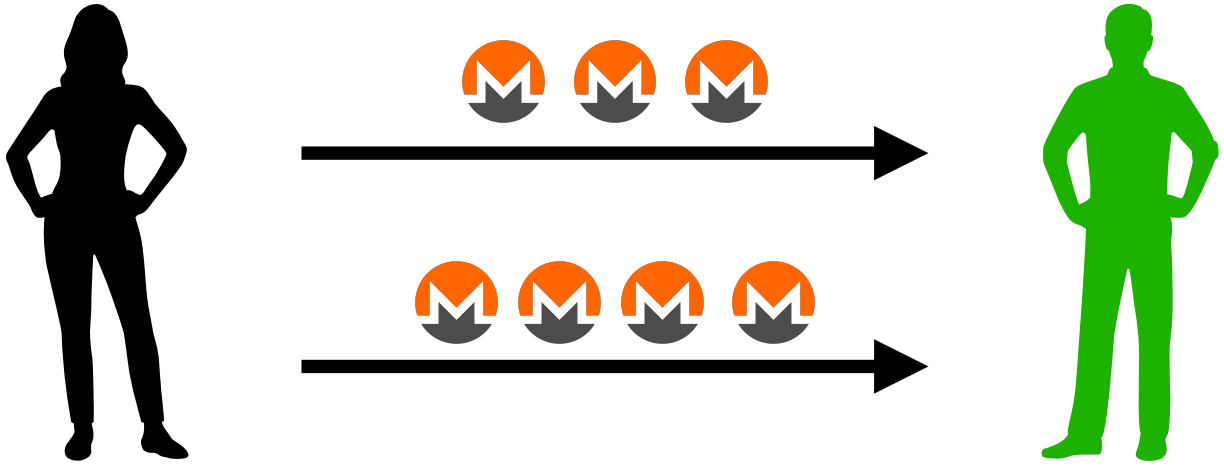


Hiding Receivers with Stealth Addresses



$$pk_1 = g^{H(ok_1)} \cdot K_s$$

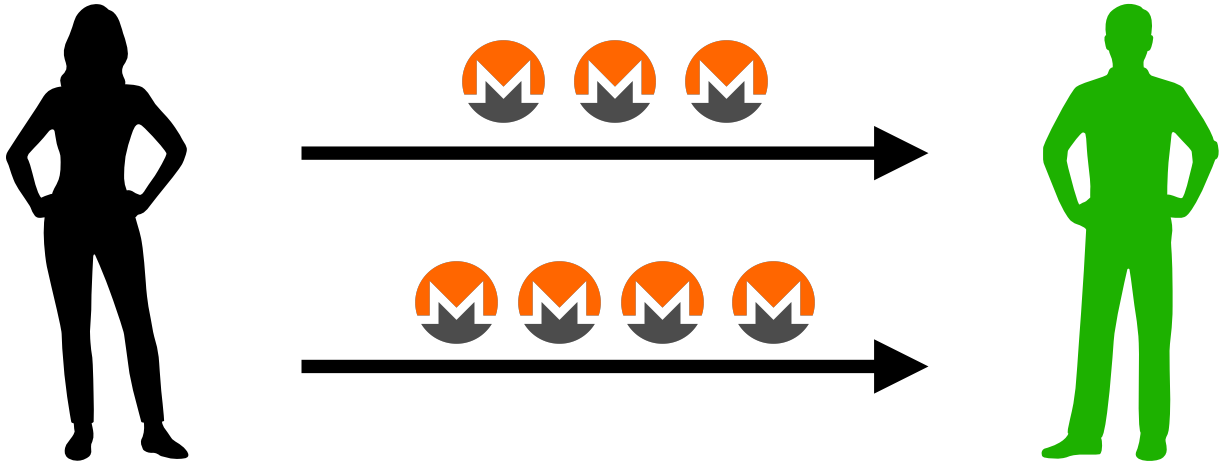
Hiding Receivers with Stealth Addresses



$$pk_1 = g^{H(ok_1)} \cdot K_s$$

$$pk_2 = g^{H(ok_2)} \cdot K_s$$

Hiding Receivers with Stealth Addresses

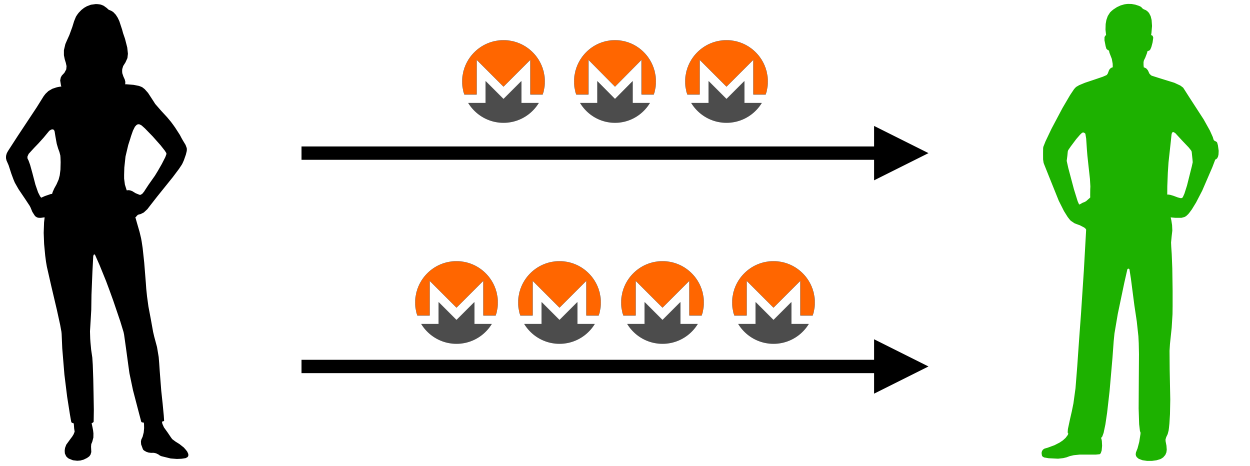


$$pk_1 = g^{H(ok_1)} \cdot K_s$$

$$pk_2 = g^{H(ok_2)} \cdot K_s$$

$$sk_1 - sk_2 = H(ok_1) - H(ok_2)$$

Hiding Receivers with Stealth Addresses



$$pk_1 = g^{H(ok_1)} \cdot K_s$$

$$pk_2 = g^{H(ok_2)} \cdot K_s$$

$$sk_1 - sk_2 = H(ok_1) - H(ok_2)$$

Related Key Attacks?

Outline

This Talk

Why is security unclear?

Stealth Addresses

What do we prove?

Security Model

Long Talk

YouTube

Details on RingCT

Proof Techniques

Outline

This Talk

Why is security unclear?

Stealth Addresses

What do we prove?

Security Model

Long Talk

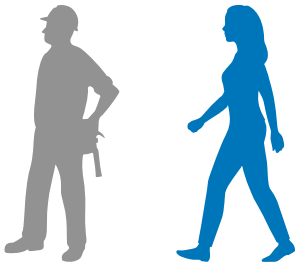
YouTube

Details on RingCT

Proof Techniques

Security Model: Adversarial Capabilities

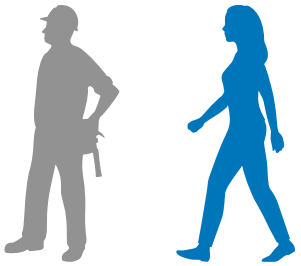
Ledger



Security Model: Adversarial Capabilities

Adversary can …

Ledger

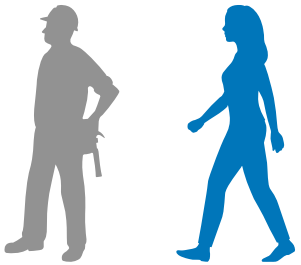


Security Model: Adversarial Capabilities

Adversary can …

- Create new honest users

Ledger



Security Model: Adversarial Capabilities

Adversary can …

- Create new honest users

K_s, k_v

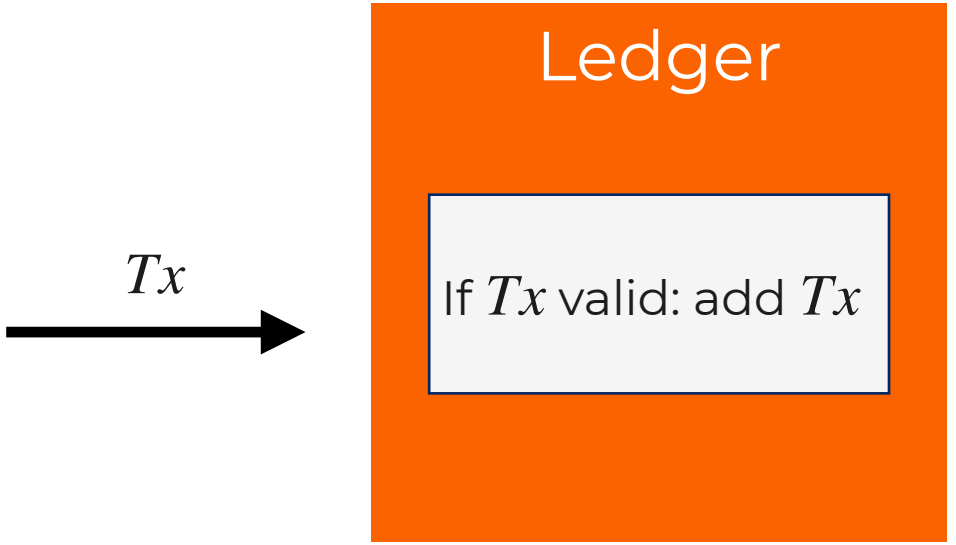
Ledger

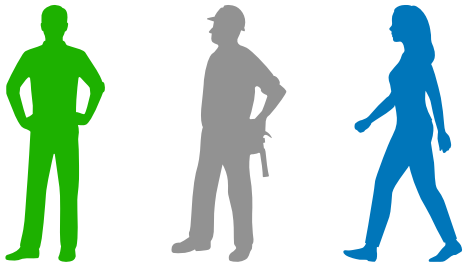
Security Model: Adversarial Capabilities

Adversary can …

- Create new honest users
- Submit txs

Tx



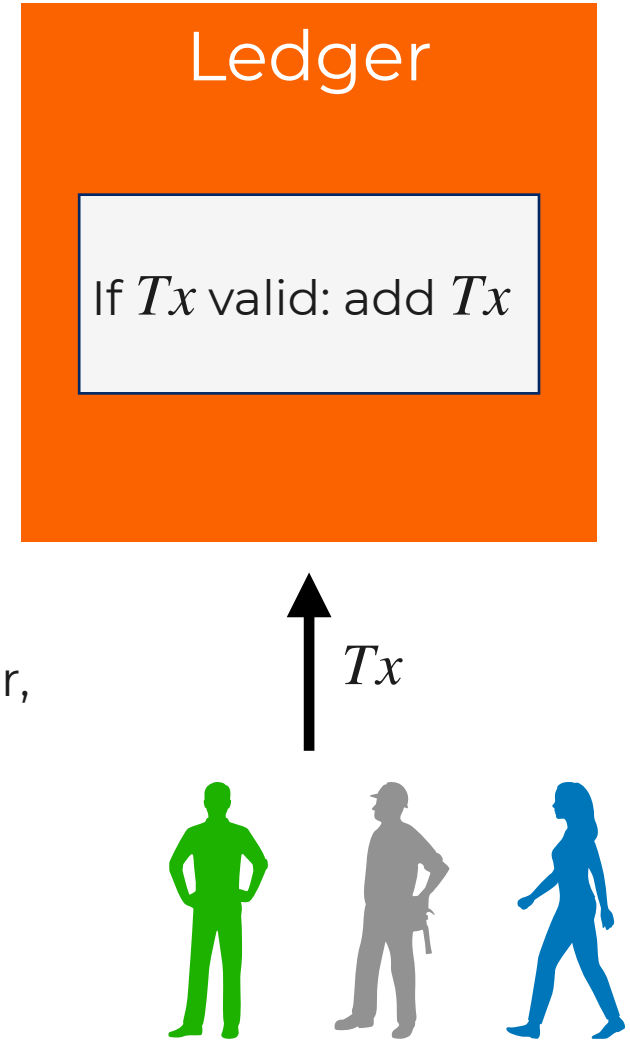


Security Model: Adversarial Capabilities

Adversary can …

- Create new honest users
- Submit txs
- Make users submit txs

Sender, Receiver, Amount



Security Model: Adversarial Capabilities

Adversary can …

- Create new honest users
- Submit txs
- Make users submit txs

Ledger

Security Model: Adversarial Capabilities

Adversary can …

- Create new honest users
- Submit txs
- Make users submit txs
- Corrupt users

k_s

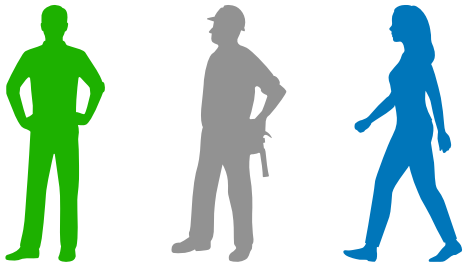
Ledger

Security Model: Adversarial Capabilities

Adversary can …

- Create new honest users
- Submit txs
- Make users submit txs
- Corrupt users
- Create new “source“ coins

Ledger



Security Model: Winning Conditions

Security Model: Winning Conditions

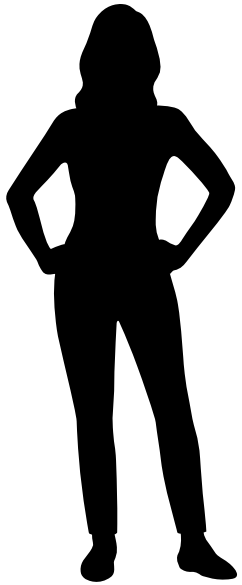
1. Winning Condition: Adversary steals coins

2. Winning Condition: Adversary creates coins

Security Model: Stealing

Security Model: Stealing

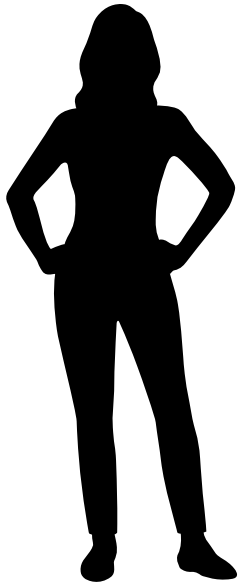
Ledger



Security Model: Stealing

Ledger

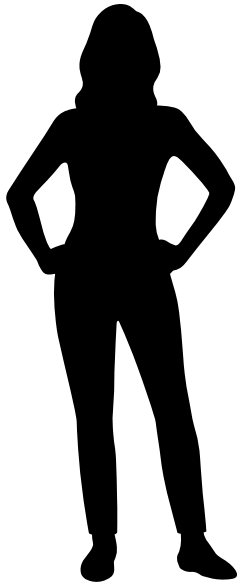
Send 10 coins to Bob



Security Model: Stealing

Ledger

Send 10 coins to Bob

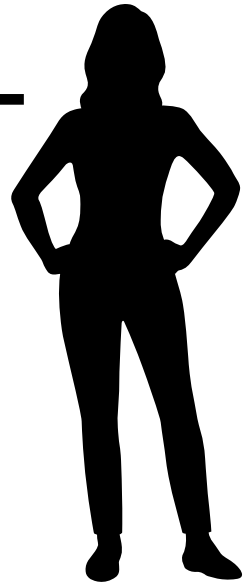


I have 10
unspent coins!

Security Model: Stealing

Ledger

Tx



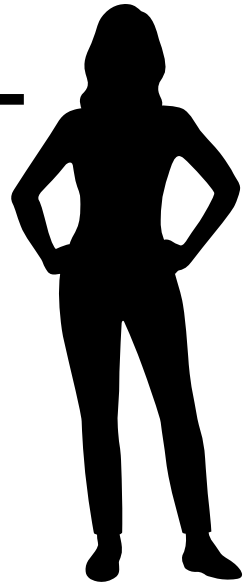
I have 10 unspent coins!

Send 10 coins to Bob

Security Model: Stealing

Ledger

Tx



I have 10 unspent coins!

Send 10 coins to Bob

1. Winning Condition: Tx is rejected $\Longrightarrow$ Adversary wins

Security Model: Creating Coins

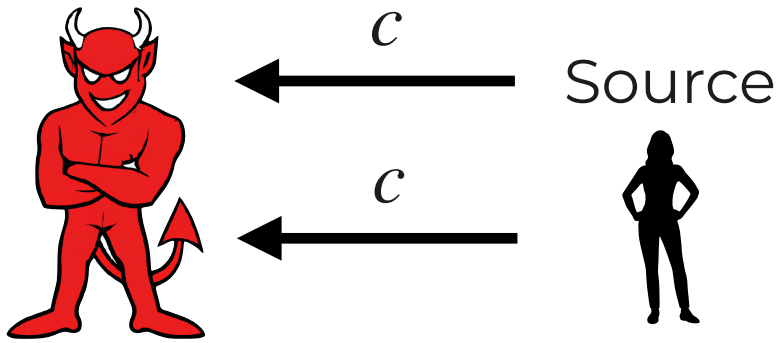
Security Model: Creating Coins

$\text{received} \in \mathbb{N}_0$

$\text{spent} \in \mathbb{N}_0$

Security Model: Creating Coins

received $\in \mathbb{N}_0$

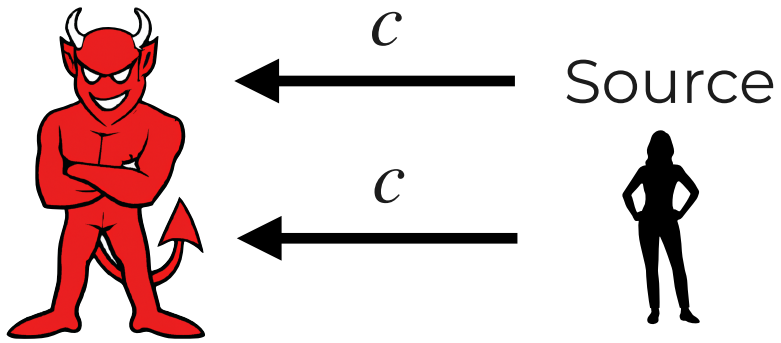


Adversary gets c coins
$\Longrightarrow$ received := received + c

spent $\in \mathbb{N}_0$

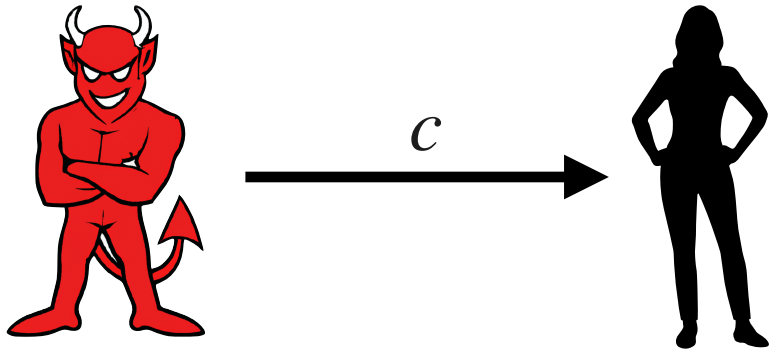
Security Model: Creating Coins

received $\in \mathbb{N}_0$



Adversary gets c coins
$\Longrightarrow$ received := received + c

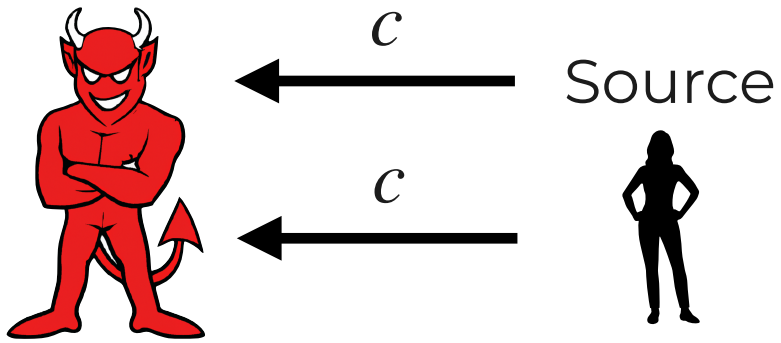
spent $\in \mathbb{N}_0$



Adversary submits Tx and
honest user receives c coins
$\Longrightarrow$ spent := spent + c

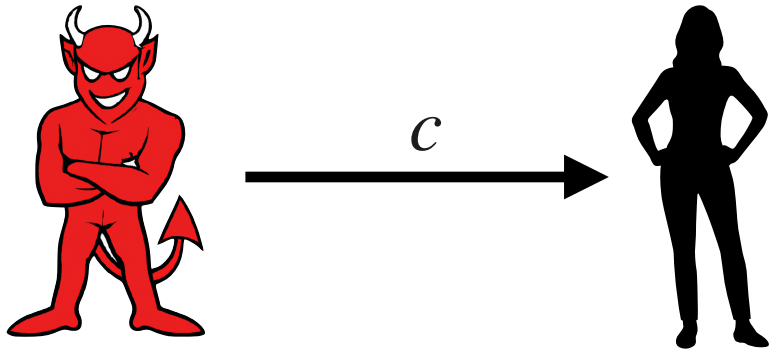
Security Model: Creating Coins

received $\in \mathbb{N}_0$



Adversary gets c coins
$\Longrightarrow$ received := received + c

spent $\in \mathbb{N}_0$



Adversary submits Tx and
honest user receives c coins
$\Longrightarrow$ spent := spent + c

2. Winning Condition: spent > received $\Longrightarrow$ Adversary wins

Summary

Summary

RingCT and Its Unclear Security

Summary

RingCT and Its Unclear Security

Our Security Model

Summary

- RingCT and Its Unclear Security
- Our Security Model
- Proof Techniques using Network Flow

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

A Holistic Security Analysis of Monero Transactions



Paper

Long Talk