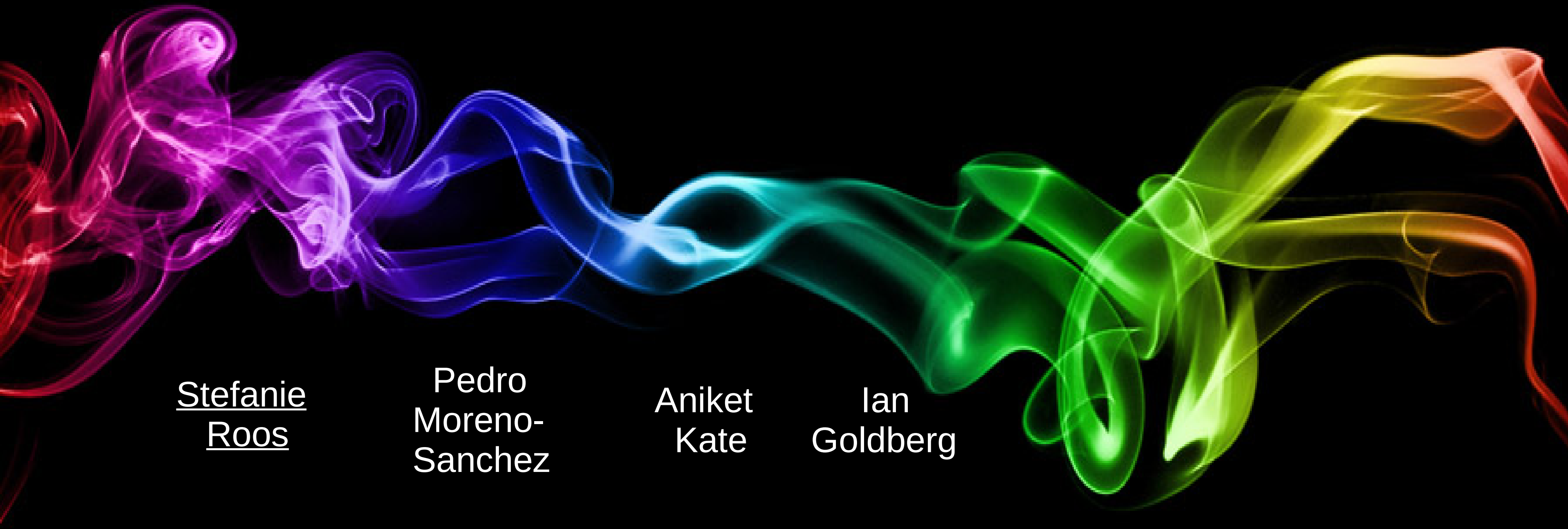
Settling Payments Fast and Private:

Efficient Decentralized Routing for Path-Based Transactions



Stefanie Roos

Pedro Moreno-Sanchez

Aniket Kate

Ian Goldberg

UNIVERSITY OF WATERLOO

PURDUE UNIVERSITY

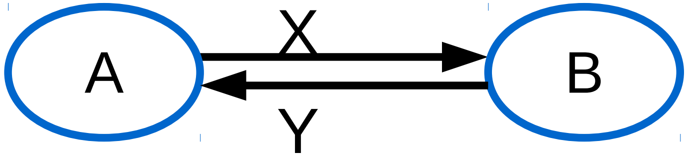
Limitations of Blockchains

Scalability

7 transactions/s

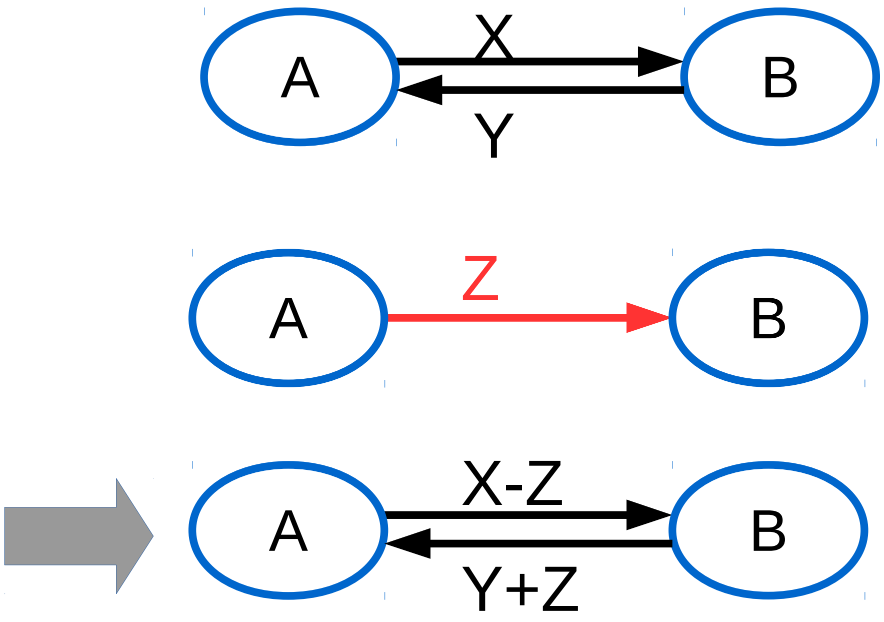
56,000 transactions/s

Payment Channels



Balance between A and B

Payment Channels



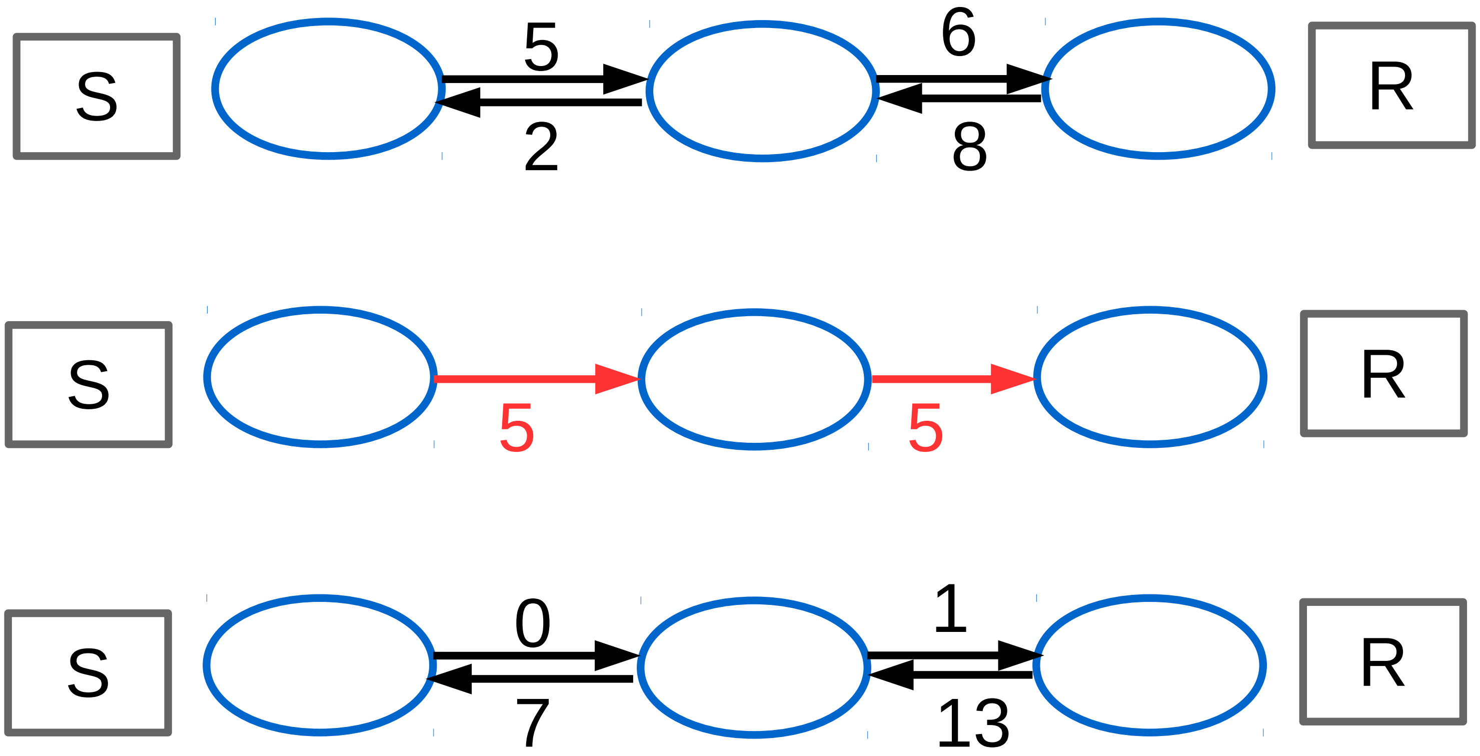
Balance between A and B

A sends Z

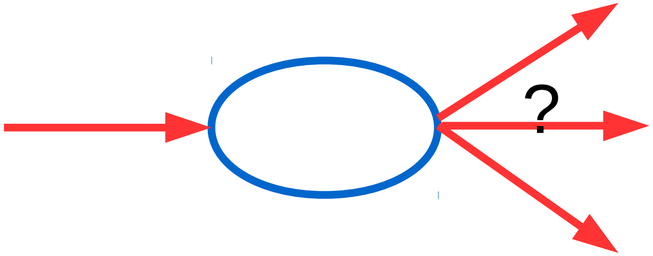
Lightning, Interledger, SilentWhispers

Path-Based Transactions (PBTs)

S wants to send c=5 to R



Contributions



- Privacy goals
- Routing algorithm design
- Privacy evaluation
- Performance evaluation

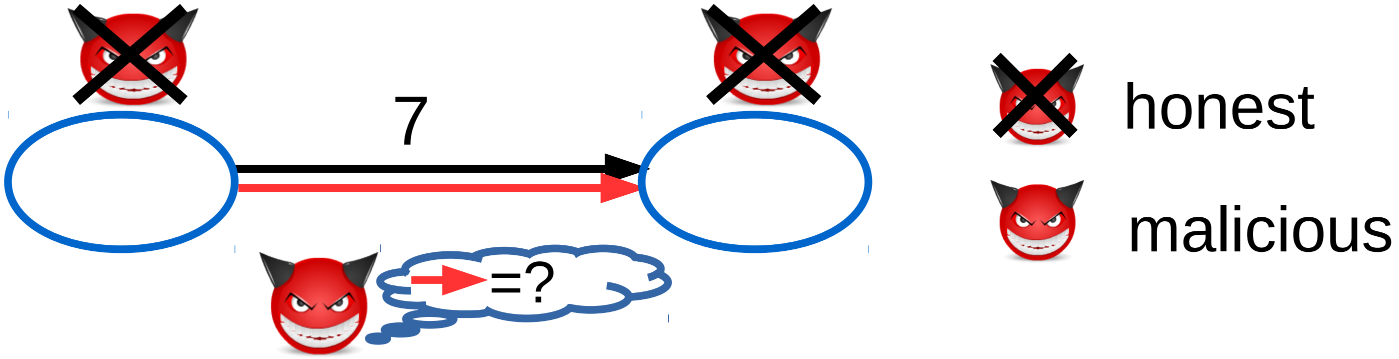
Privacy Goals

Send **?** from **?** to **?**

Privacy Goals

Send **?** from **?** to **?**

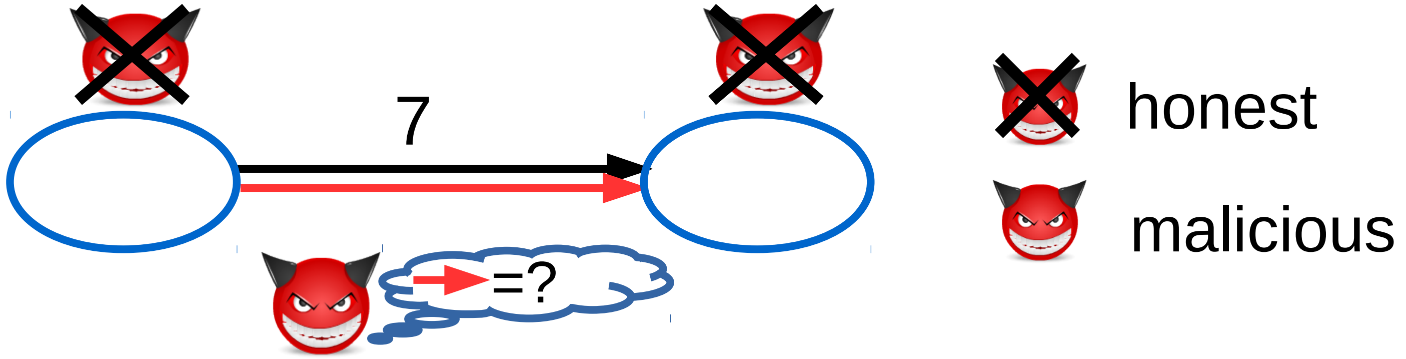
- Value privacy



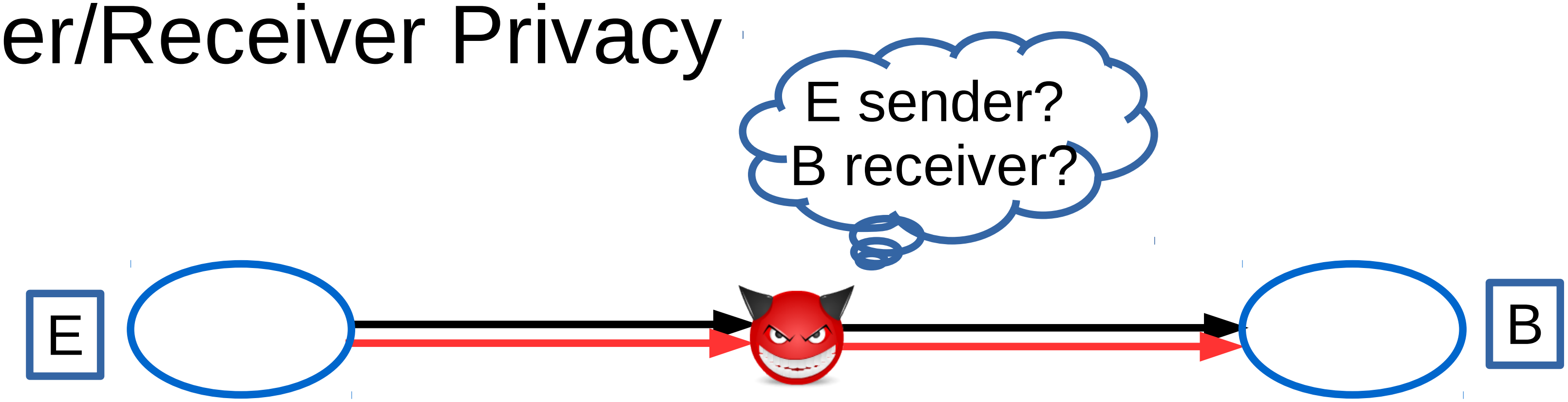
Privacy Goals

Send **?** from **?** to **?**

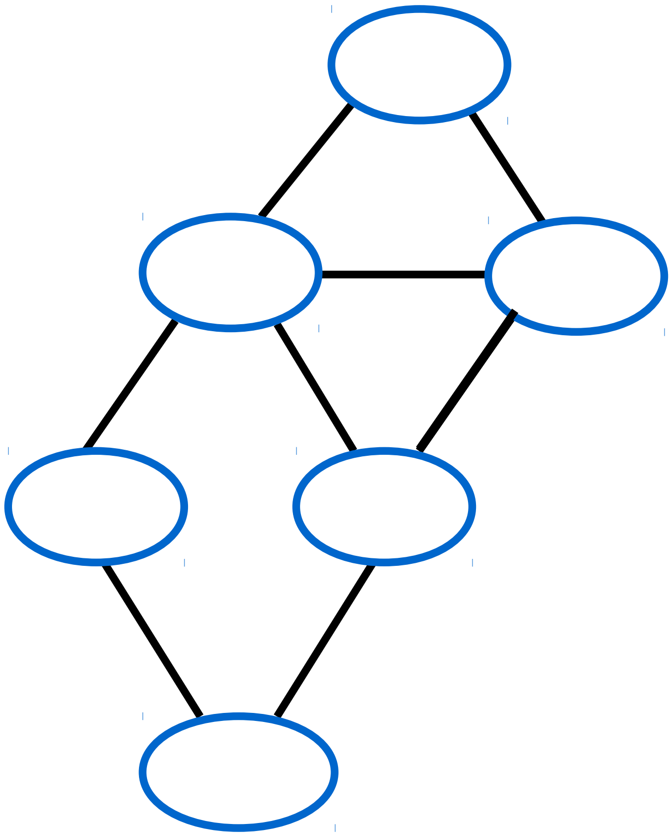
- Value privacy



- Sender/Receiver Privacy

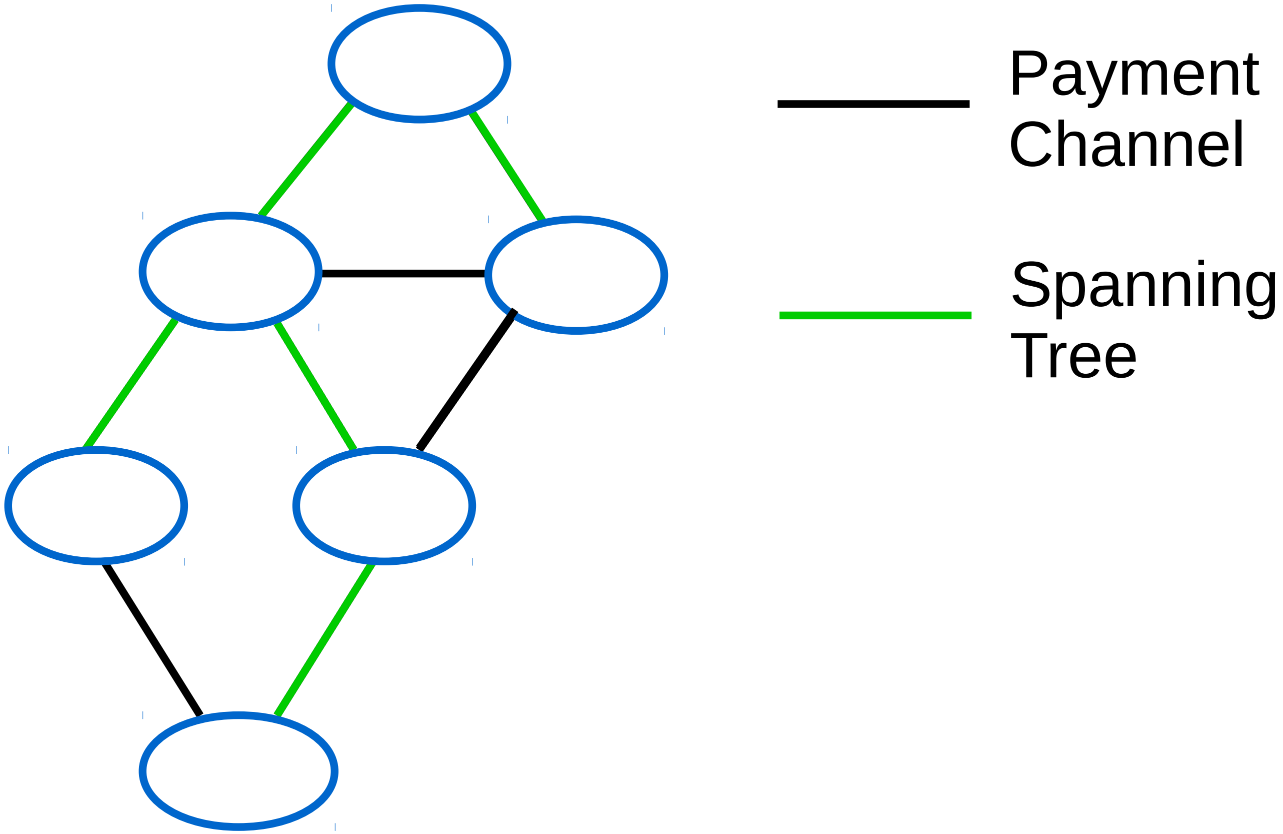


SpeedyMurmurs: Setup



—— Payment Channel

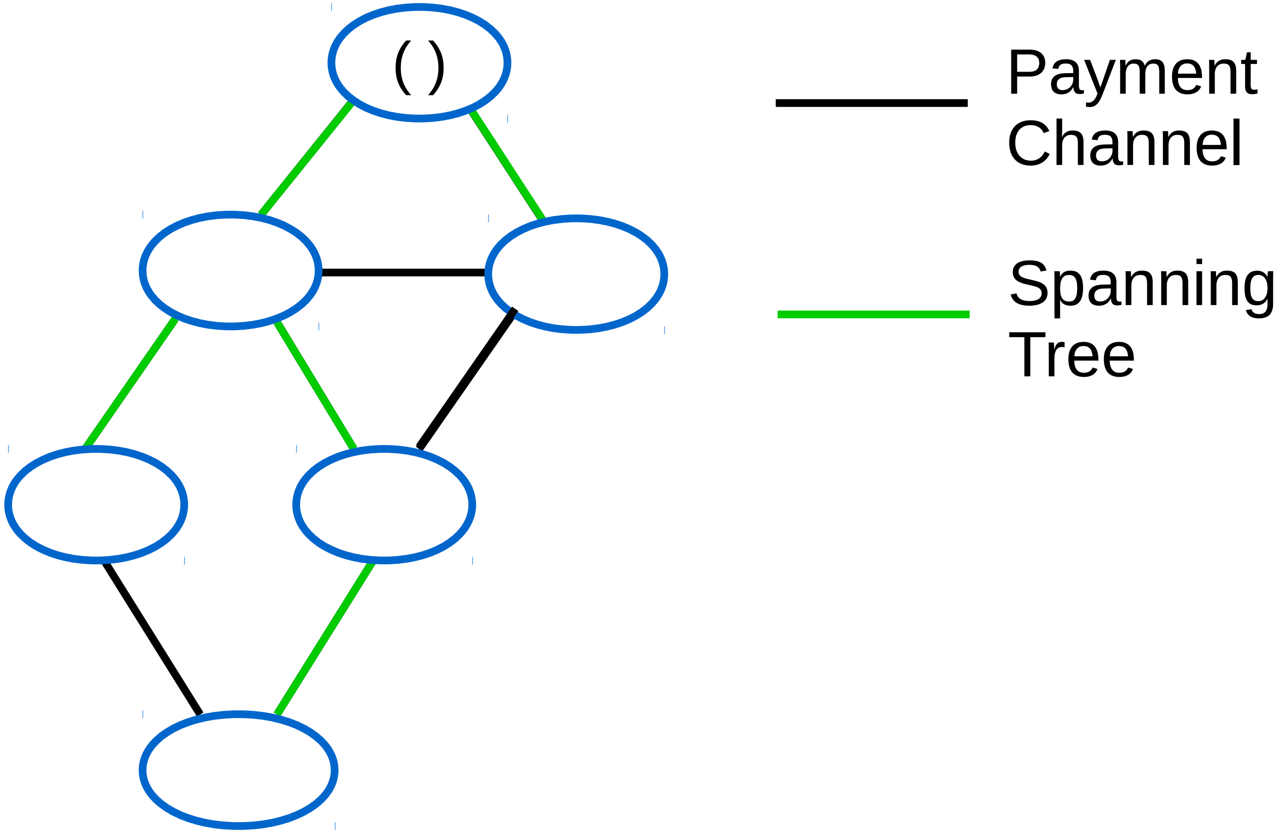
SpeedyMurmurs: Setup



Payment Channel

Spanning Tree

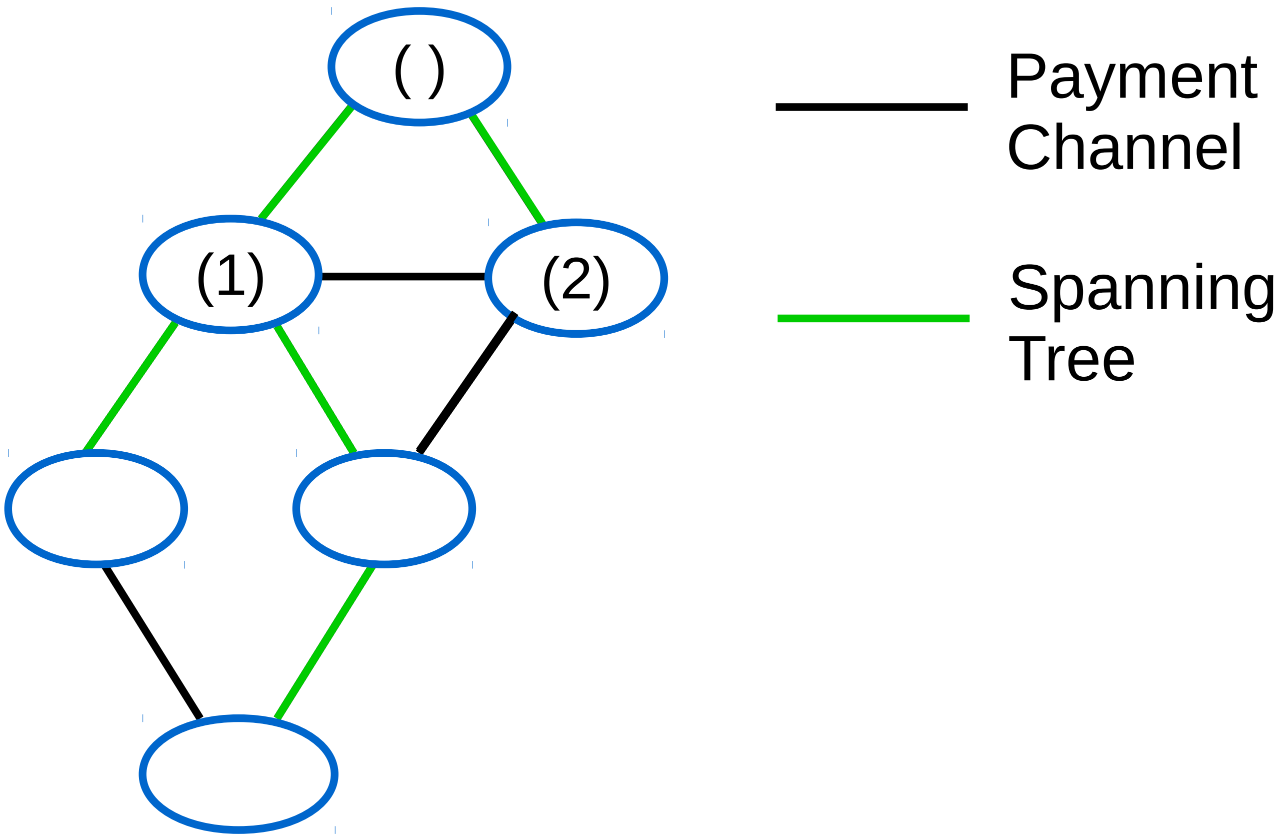
SpeedyMurmurs: Setup



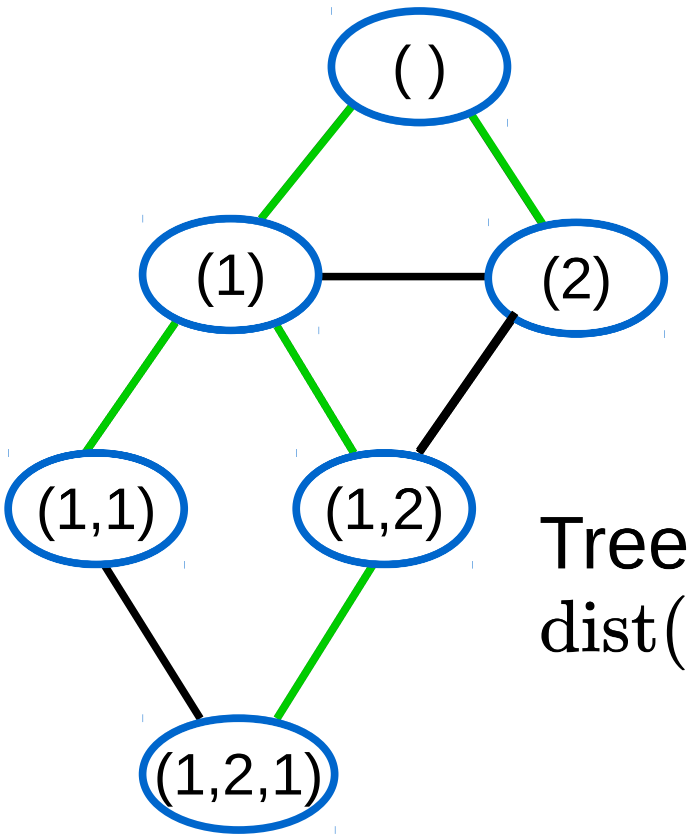
Payment Channel

Spanning Tree

SpeedyMurmurs: Setup



SpeedyMurmurs: Setup



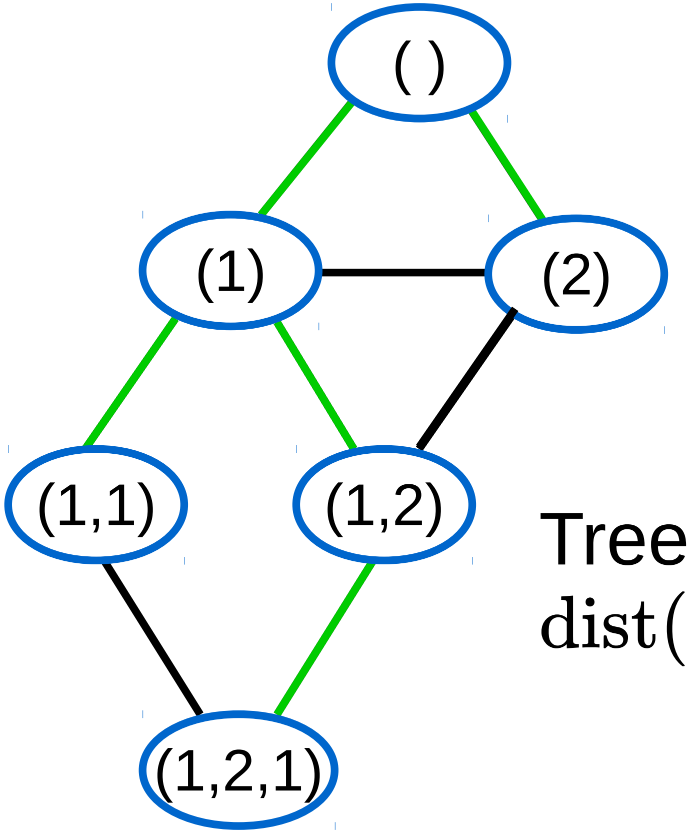
━ Payment Channel

🟩 Spanning Tree

Tree distance

$$\mathrm{dist}(u,v) = |u|+|v|-2\underset{\substack{\uparrow\\ \text{Common Prefix Length}}}{\mathrm{cpl}}(u,v)$$

SpeedyMurmurs: Setup



▬ Payment Channel

🟩 Spanning Tree

Tree distance

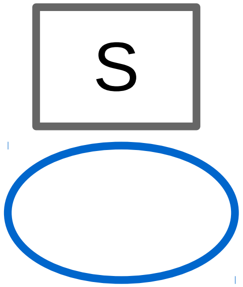
$$\mathrm{dist}(u,v) = |u| + |v| - 2\,\mathrm{cpl}(u,v)$$

Common Prefix Length

t trees (number of paths)

SpeedyMurmurs: Routing

1



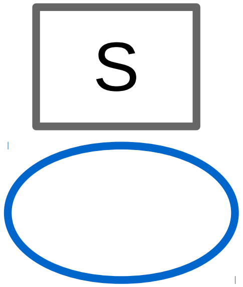
c(1)
c(2)
…
c(t)

$$\sum c(i) = c$$

c(i): value sent using coordinates in i-th tree

SpeedyMurmurs: Routing

1



c(1)
c(2)
...
c(t)

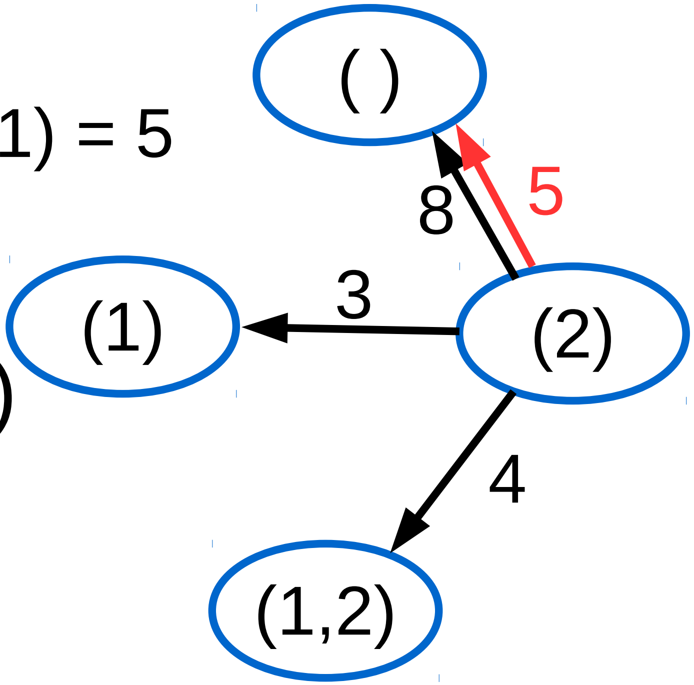
$$\sum c(i) = c$$

c(i): value sent using coordinates in i-th tree

2

Select neighbor
1) closer to receiver
2) has at least balance c(i)

c(1) = 5



Privacy

- Value c hidden from nodes not on paths
- Nodes on paths can estimate c

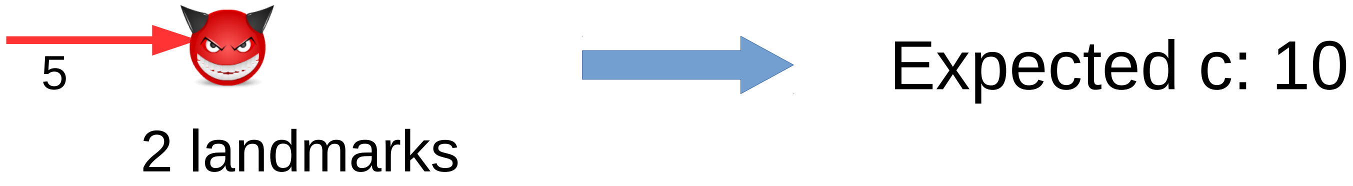
5

2 trees

Expected c: 10

Privacy Analysis

- Value c hidden from nodes not on paths
- Nodes on paths can estimate c



5

2 landmarks

Expected c: 10

- Sender/Receiver Privacy : obfuscated coordinates (Roos et al., Infocom 2016)

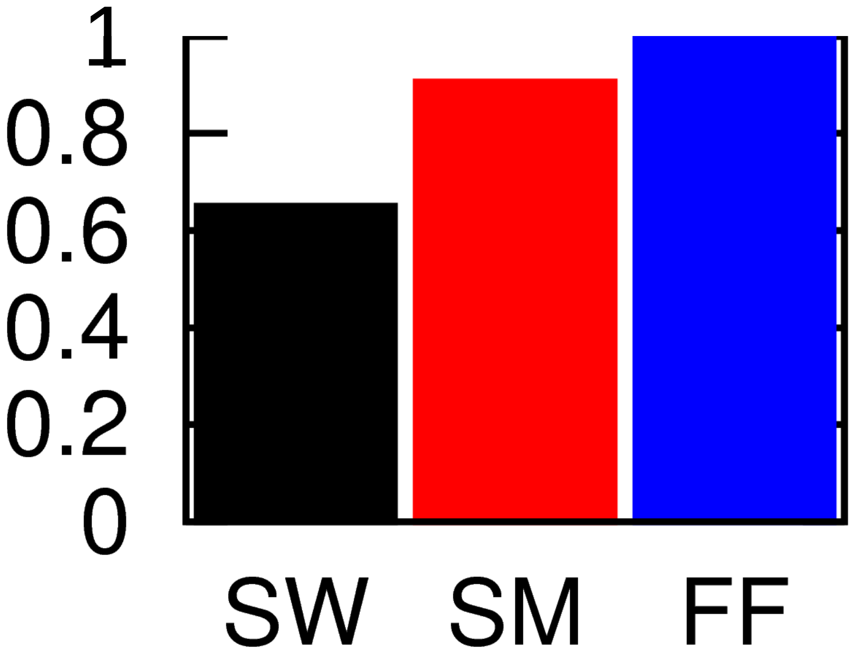
Performance: Success Ratio

Real-world data set: Ripple
(~60,000 nodes, 300,000 transactions)

SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson

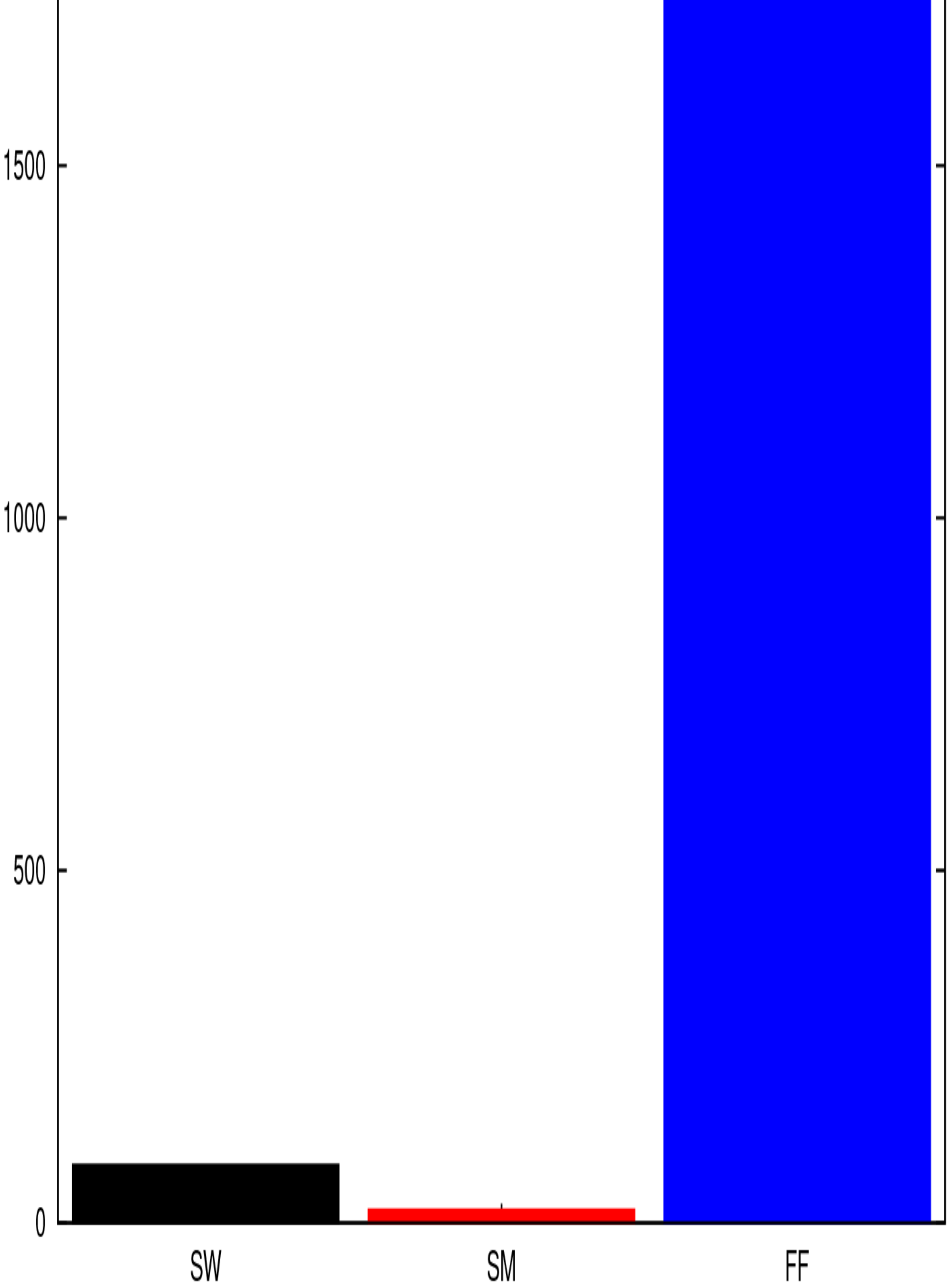
Performance: Success Ratio

Real-world data set: Ripple
(~60,000 nodes, 300,000 transactions)



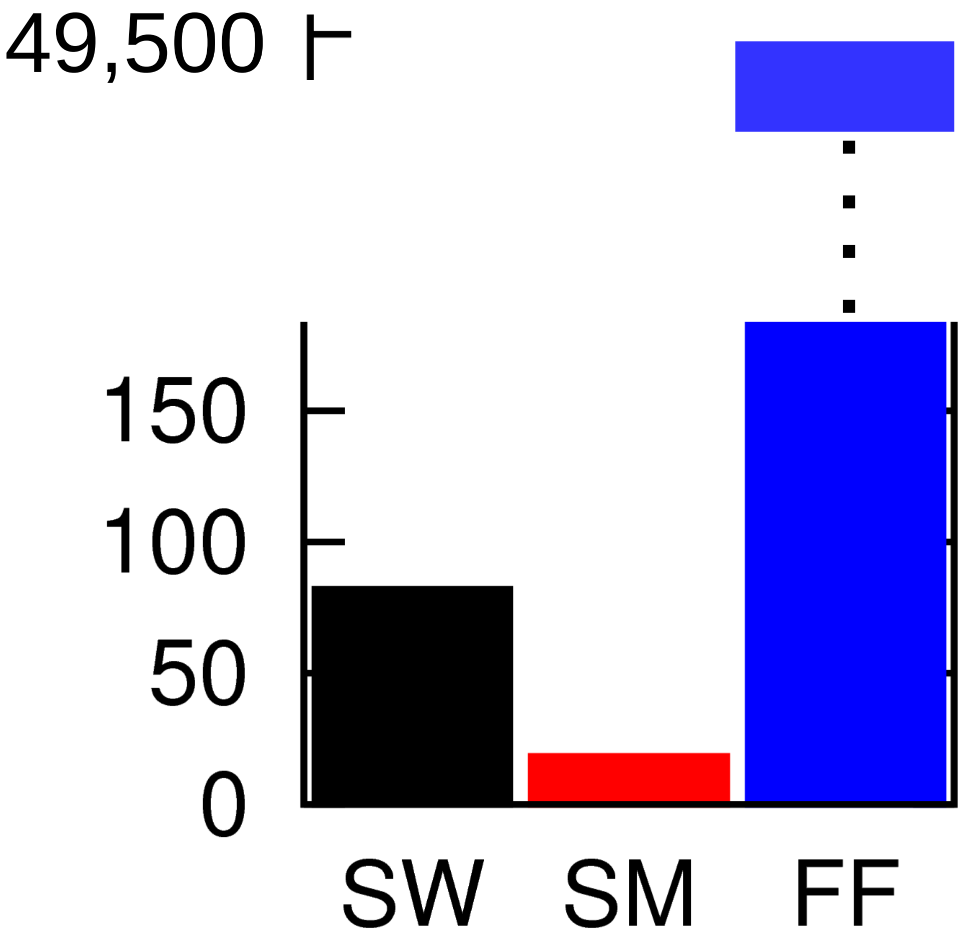
SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson

Messages



SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson

Evaluation: Messages



SW – SilentWhispers
SM – SpeedyMurmurs
FF – Ford-Fulkerson

Summary

- SpeedyMurmurs
  - Embedding-based routing
  - (Dynamic maintenance)
  - (Concurrency-aware routing)
- Effective, efficient, scalable, privacy-preserving
- Applicable to Lightning, Interledger, SilentWhispers
- Data sets and simulation framework:

  https://crysp.uwaterloo.ca/software/speedymurmurs/