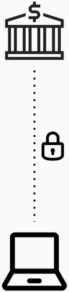
Categories for Cryptographic Composability

Riley Shahar

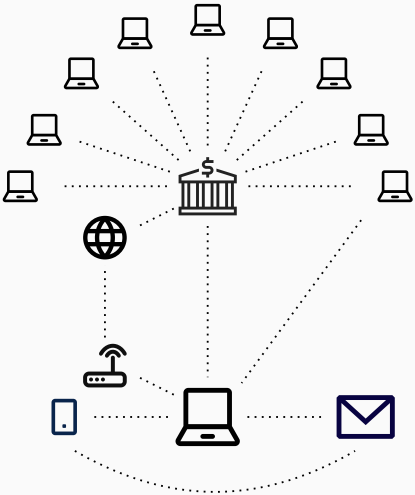
Advised by Angélica and Adam

Motivation

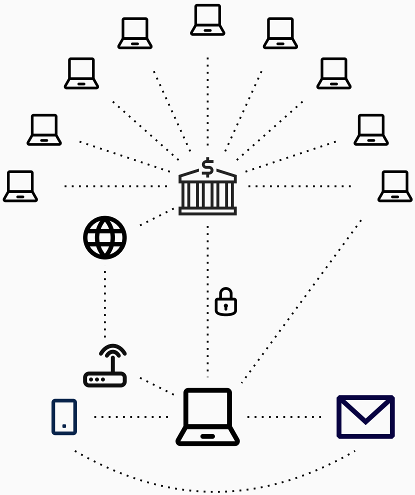
Motivation



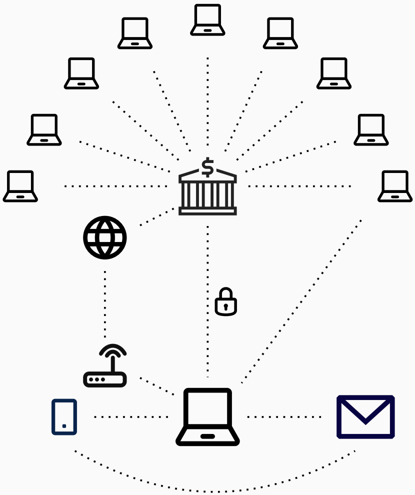
Motivation



Motivation

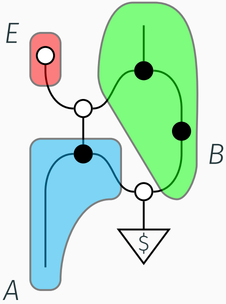


Motivation



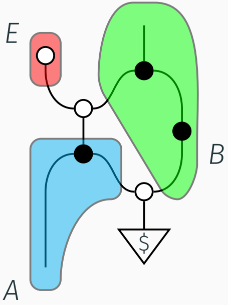
What do we need to prove about a computation in a vacuum so that it's still secure no matter what else is going on?

A Categorical Approach



[Broadbent & Karvonen 2022]

A Categorical Approach



[Broadbent & Karvonen 2022]

Our Contributions:

- Generalizing to enriched bicategories for weak reductions
- Coloring diagrams by party
- Simultaneous reasoning about single- and multi-use resources
- Correlated input
- Novel security proofs
- Heursitic comparison to UC