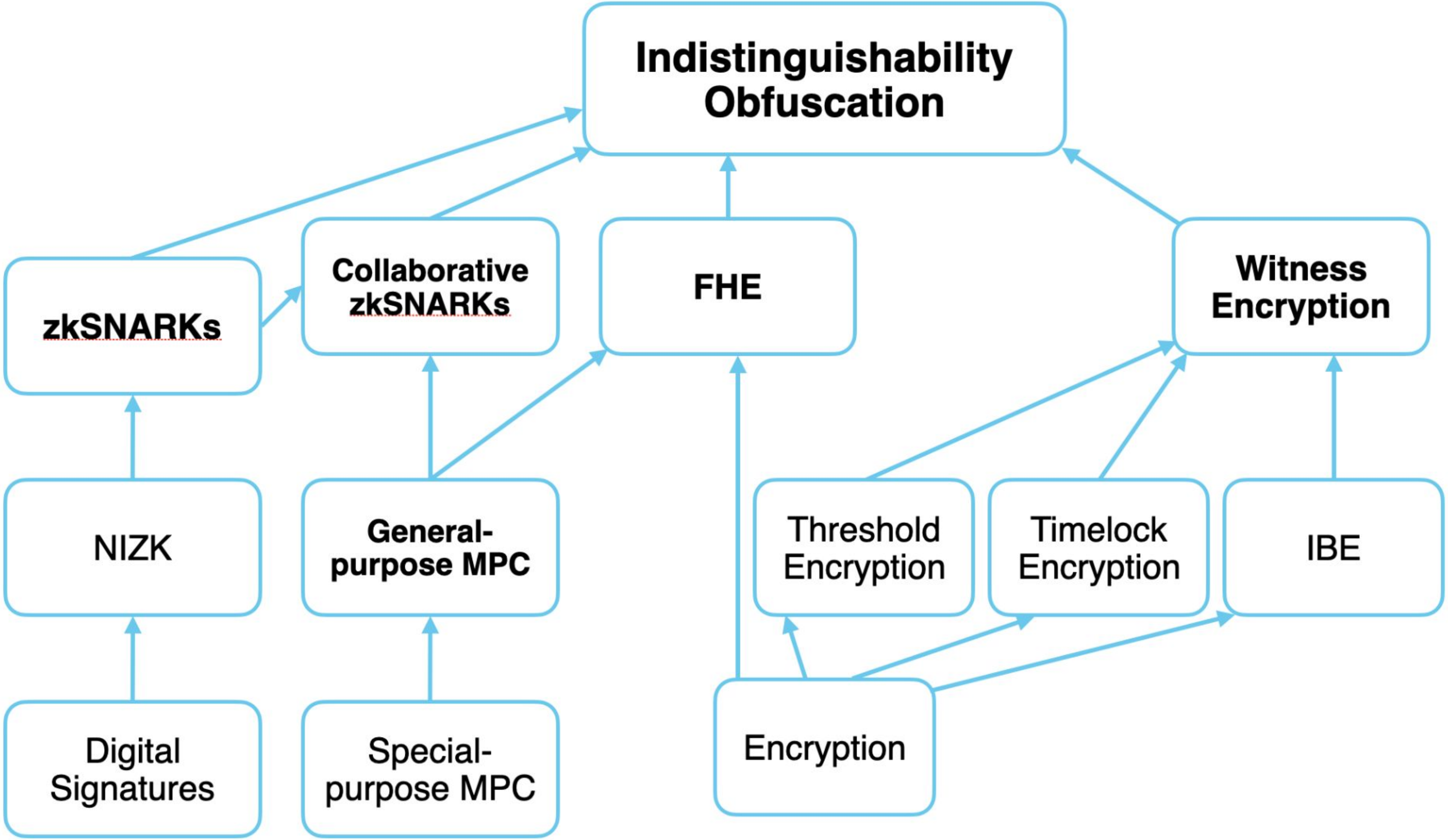
Hallucinated Servers

An introduction to Programmable Cryptography

0xPARC

0xPARC


Indistinguishability Obfuscation
zkSNARKs
Collaborative zkSNARKs
FHE
Witness Encryption
NIZK
General-purpose MPC
Threshold Encryption
Timelock Encryption
IBE
Digital Signatures
Special-purpose MPC
Encryption

Four primitives

- Succinct zero-knowledge proofs
- Multiparty computation
- Fully homomorphic encryption
- Indistinguishability obfuscation

Four primitives

- Succinct zero-knowledge proofs
  - Data integrity, verifiable computation
  - Cryptographic adapter
- Multiparty computation and fully homomorphic encryption
  - Collaboration with privacy
  - Hallucinated server
- Indistinguishability obfuscation
  - Arbitrary programmable functionality
  - Autonomous cryptographic agent

Four primitives

- **Succinct zero-knowledge proofs**
    - Data integrity, verifiable computation
    - Cryptographic adapter
- Multiparty computation and fully homomorphic encryption
    - Collaboration with privacy
    - Hallucinated server
- Indistinguishability obfuscation
    - Arbitrary programmable functionality
    - Autonomous cryptographic agent

Succinct zero-knowledge proofs

- I know a secret input *x* such that *f(x)* = 0.
    - I don’t reveal *x*
    - Or, I reveal only a part of *x*
- I know the private key corresponding to this public key.
- I possess a message…
    - with a valid digital signature from [authority]’s known public key…
    - and here are the first 50 characters of the message

Succinct zero-knowledge proofs

- Applicable and widely used in practice
- Cost overhead: Thousands

Four primitives

- Succinct zero-knowledge proofs
  - Data integrity, verifiable computation
  - Cryptographic adapter
- **Multiparty computation** and fully homomorphic encryption
  - Collaboration with privacy
  - Hallucinated server
- Indistinguishability obfuscation
  - Arbitrary programmable functionality
  - Autonomous cryptographic agent

Multi-party computation

- Each of us has some secret number *x_i*
- We want to know some function of all our secrets
  - How many are bigger than 100?
- Application: Danish beet auction

Multi-party computation

- Applicable in practice
  - At least for small groups
- Cost overhead: Thousands

Four primitives

- Succinct zero-knowledge proofs
  - Data integrity, verifiable computation
  - Cryptographic adapter
- Multiparty computation and **fully homomorphic encryption**
  - Collaboration with privacy
  - Hallucinated server
- Indistinguishability obfuscation
  - Arbitrary programmable functionality
  - Autonomous cryptographic agent

Fully homomorphic encryption

- I encrypt my secret data
- You can operate on the data, but you can’t access it
- I decrypt and learn the results of your operation

Fully homomorphic encryption

- Overhead: Millions

Four primitives

- Succinct zero-knowledge proofs
  - Data integrity, verifiable computation
  - Cryptographic adapter
- Multiparty computation and fully homomorphic encryption
  - Collaboration with privacy
  - Hallucinated server
- **Indistinguishability obfuscation**
  - Arbitrary programmable functionality
  - Autonomous cryptographic agent

Program obfuscation

- I can “obfuscate” any program *f* (a function)
- I give you the obfuscated source code
- You can run it and learn the output… but you can’t learn anything more about how *f* works

Program obfuscation

- Several protocols proposed
  - Some secure but impractical
  - Some fast(ish) but might be insecure
  - Further research needed

Four primitives

- Succinct zero-knowledge proofs
    - Data integrity, verifiable computation
    - Cryptographic adapter
- Multiparty computation and fully homomorphic encryption
    - Collaboration with privacy
    - Hallucinated server
- Indistinguishability obfuscation
    - Arbitrary programmable functionality
    - Autonomous cryptographic agent