# Byzantine Fault-Tolerant Aggregate Signatures

AsiaCCS 2024 – Singapore – July 5th 2024

**Quentin Kniep**, Roger Wattenhofer
ETH Zurich – **Dis**tributed **Co**mputing (disco.ethz.ch)

# Motivation

- Shor □ PQ
- Blockchain
  - Verification Time □ Lattices
  - Signature Size □ Aggregation
  - Adversary □ BFT

# Motivation

- Shor □ PQ
- Blockchain
  - Verification Time □ Lattices
  - Signature Size □ Aggregation
  - Adversary □ BFT

# Motivation

- Shor □ PQ
- Blockchain
  - Verification Time □ Lattices
  - Signature Size □ Aggregation
  - Adversary □ BFT

# Motivation

- Shor □ PQ
- Blockchain
  - Verification Time □ Lattices
  - Signature Size □ Aggregation
  - Adversary □ BFT

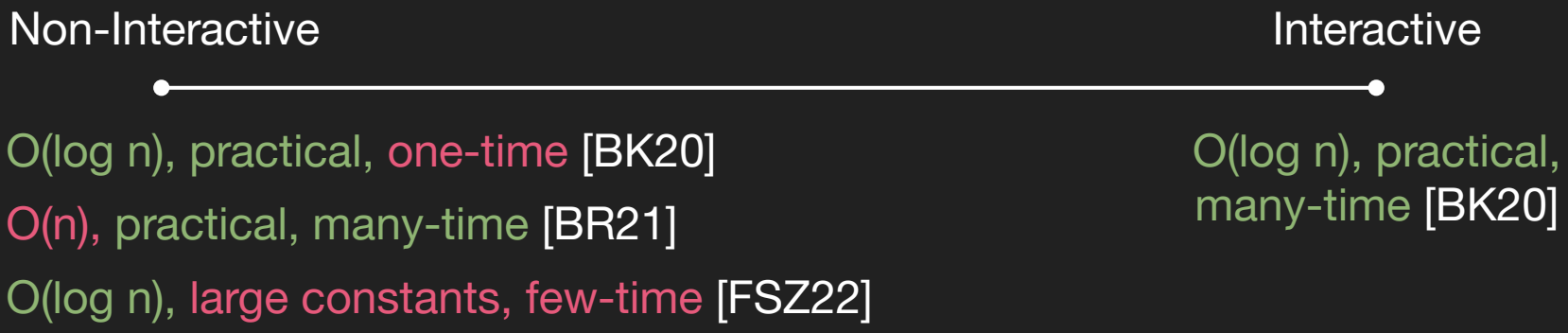
# Motivation

- Shor □ PQ
- Blockchain
  - Verification Time □ Lattices
  - Signature Size □ Aggregation
  - Adversary □ BFT

# Related Work

# Related Work

# Related Work



# Related Work


O(log n), practical, one-time [BK20]

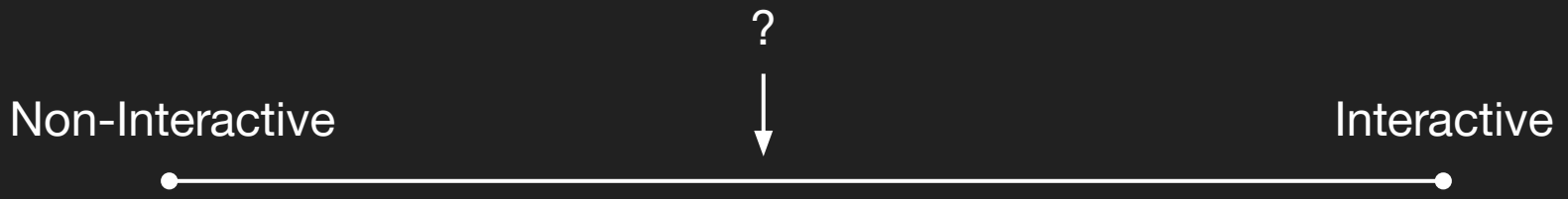
O(n), practical, many-time [BR21]

O(log n), large constants, few-time [FSZ22]

O(log n), practical, many-time [?]

O(log n), practical, many-time [BK20]

# Related Work




O(log n), practical, one-time [BK20]

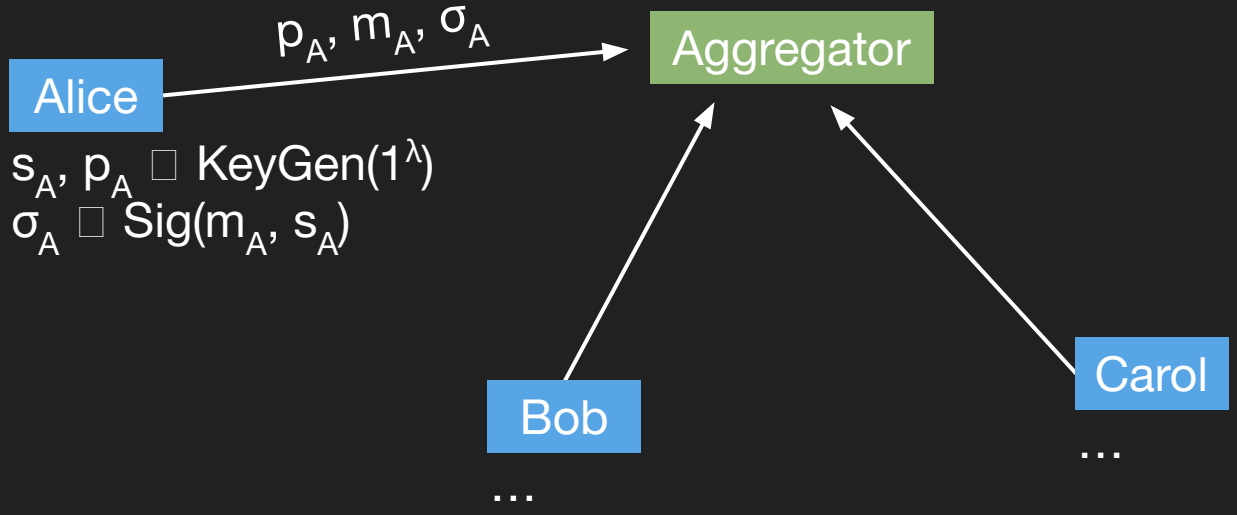
O(n), practical, many-time [BR21]

O(log n), large constants, few-time [FSZ22]

O(log n), practical, many-time [?]

O(log n), practical, many-time [BK20]

# Non-Interactive AS



# Non-Interactive AS

Alice

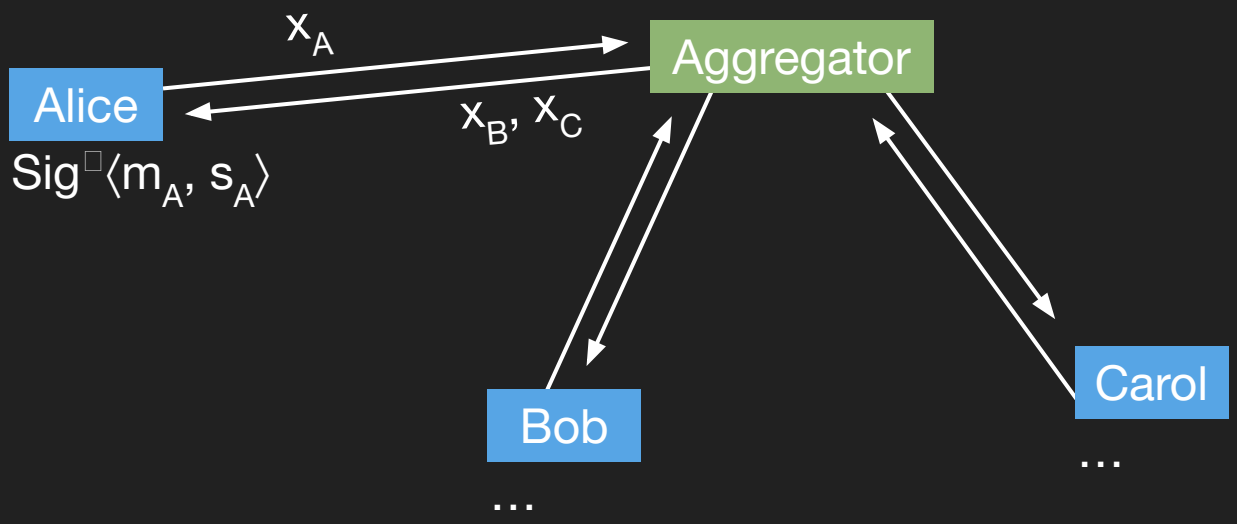
Aggregator

$\sigma_{agg}$ □ SigAgg(Σ, M, P)

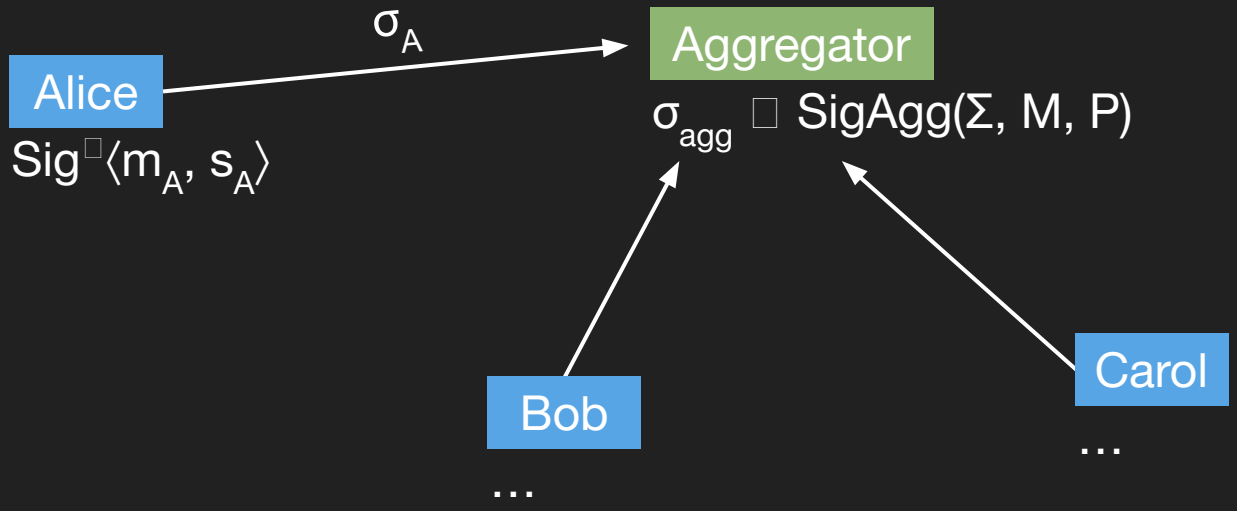
Bob

Carol

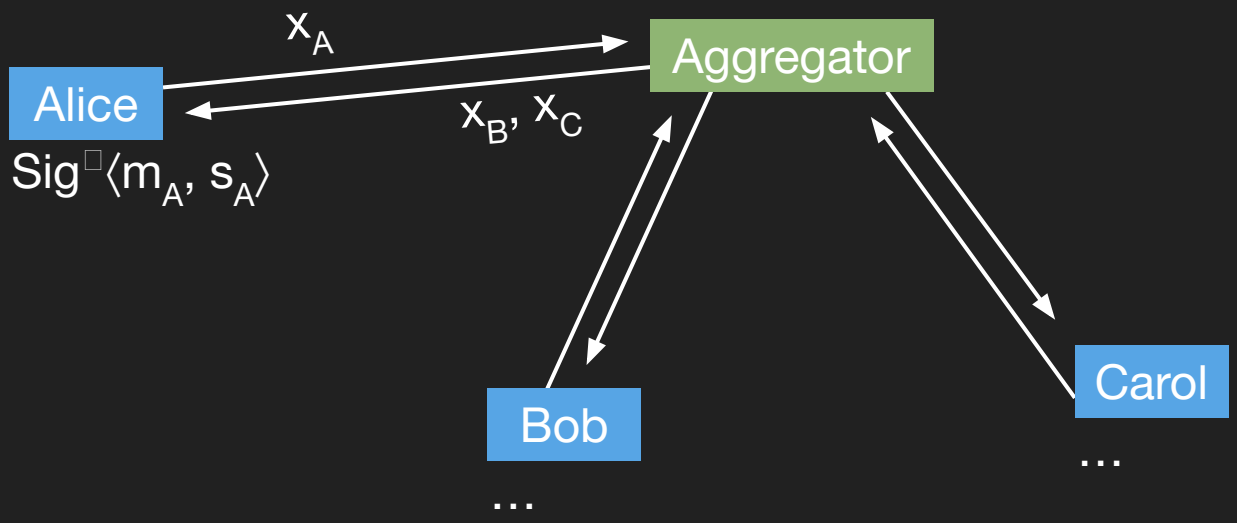
# Interactive AS



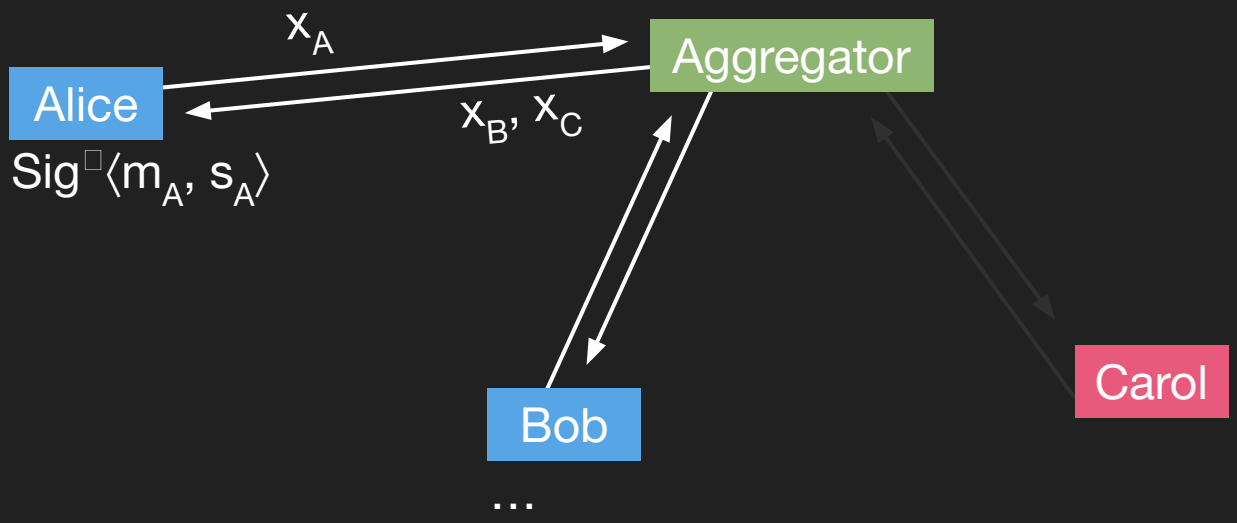
# Interactive AS



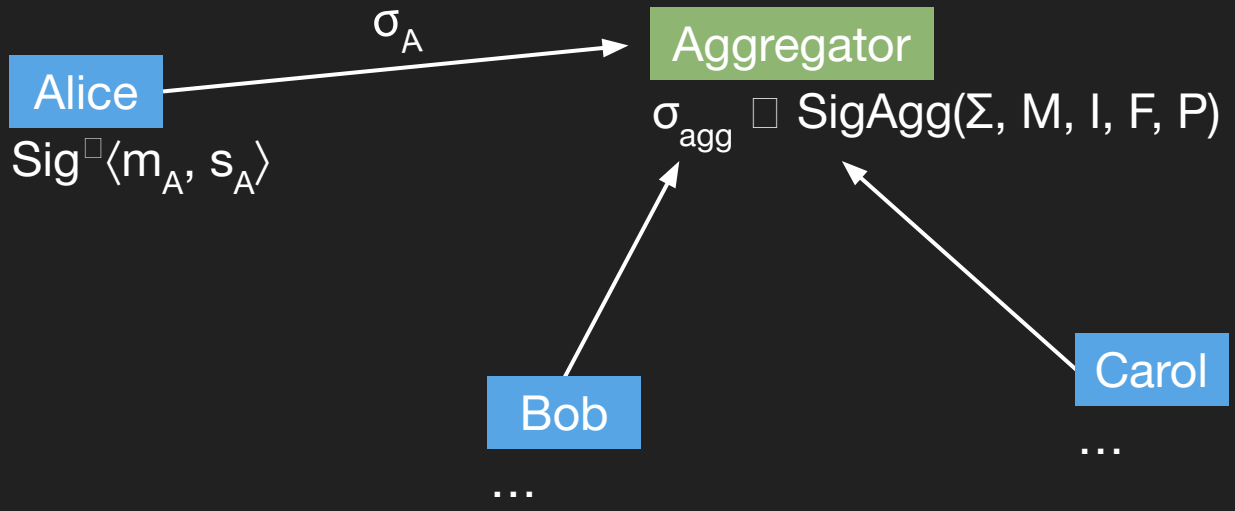
# BFT-Interactive AS



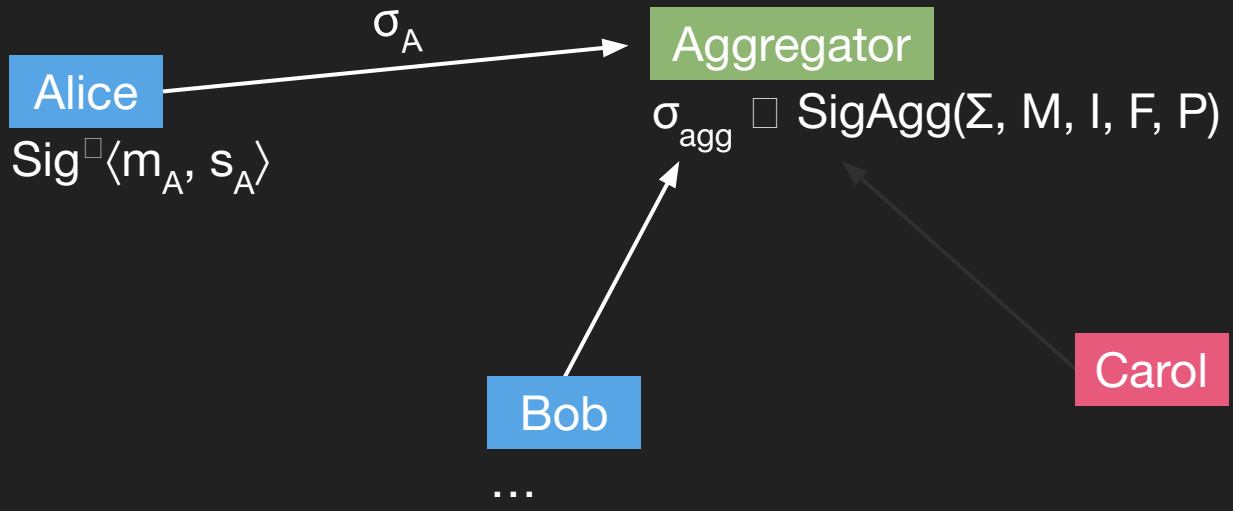
# BFT-Interactive AS



# BFT-Interactive AS

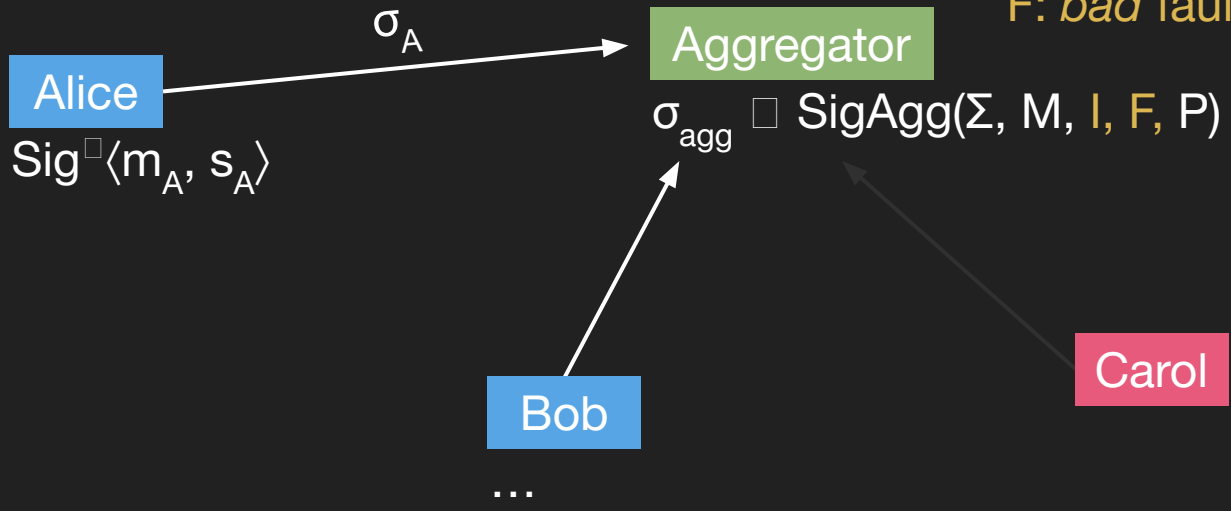


# BFT-Interactive AS



# BFT-Interactive AS

$I \subseteq P,\ F \subseteq P,\ I \cap F = \varnothing$
I: inactive (can be ignored)
F: *bad* faults



# Relationships

Non-Interactive

BFT-Interactive

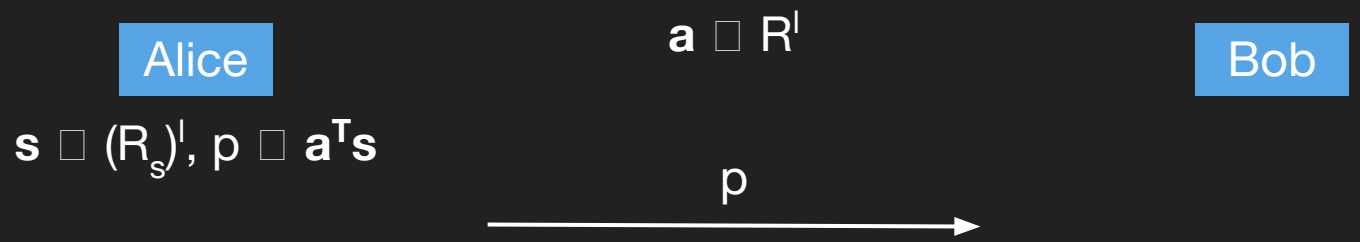
Interactive

# Relationships

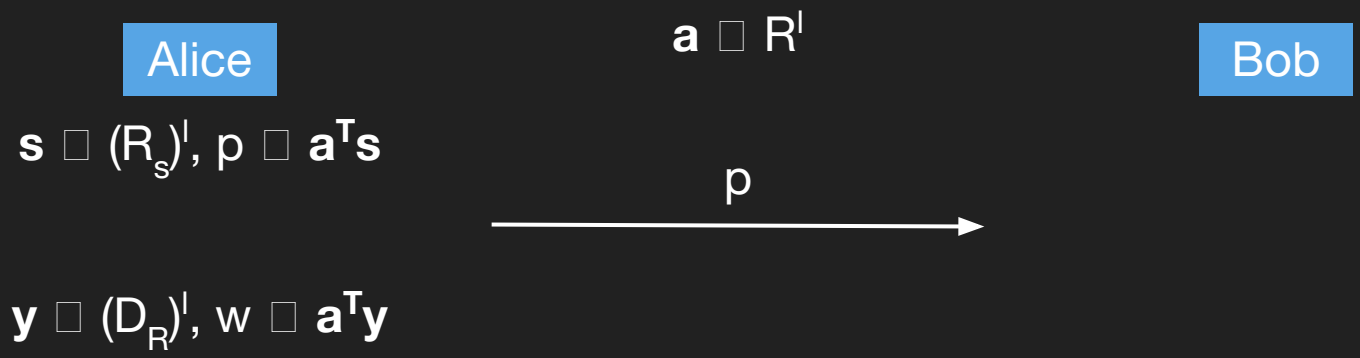
# Relationships

# Relationships

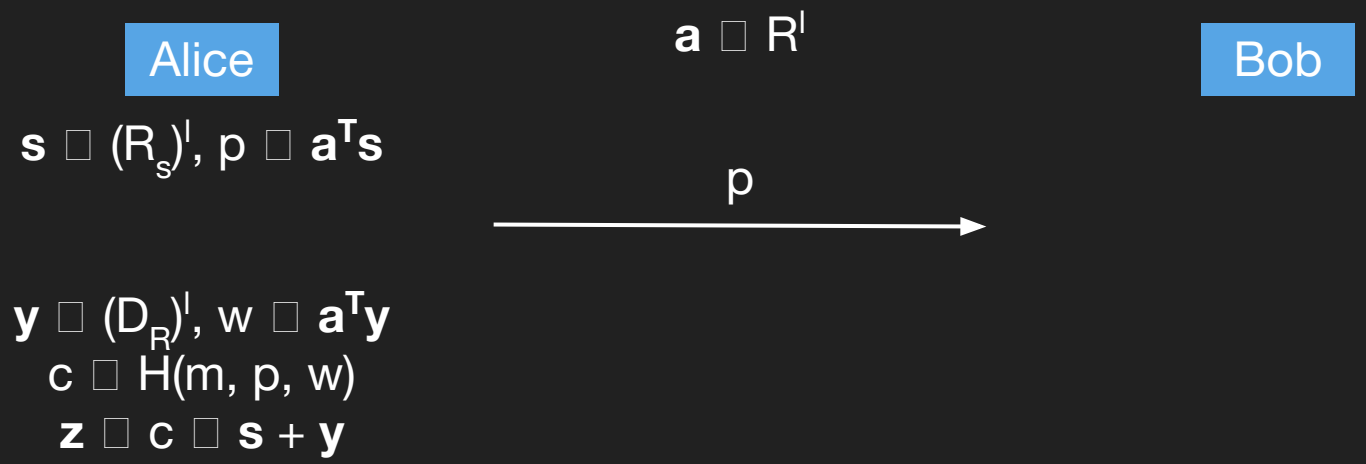
# Fiat-Shamir with Aborts



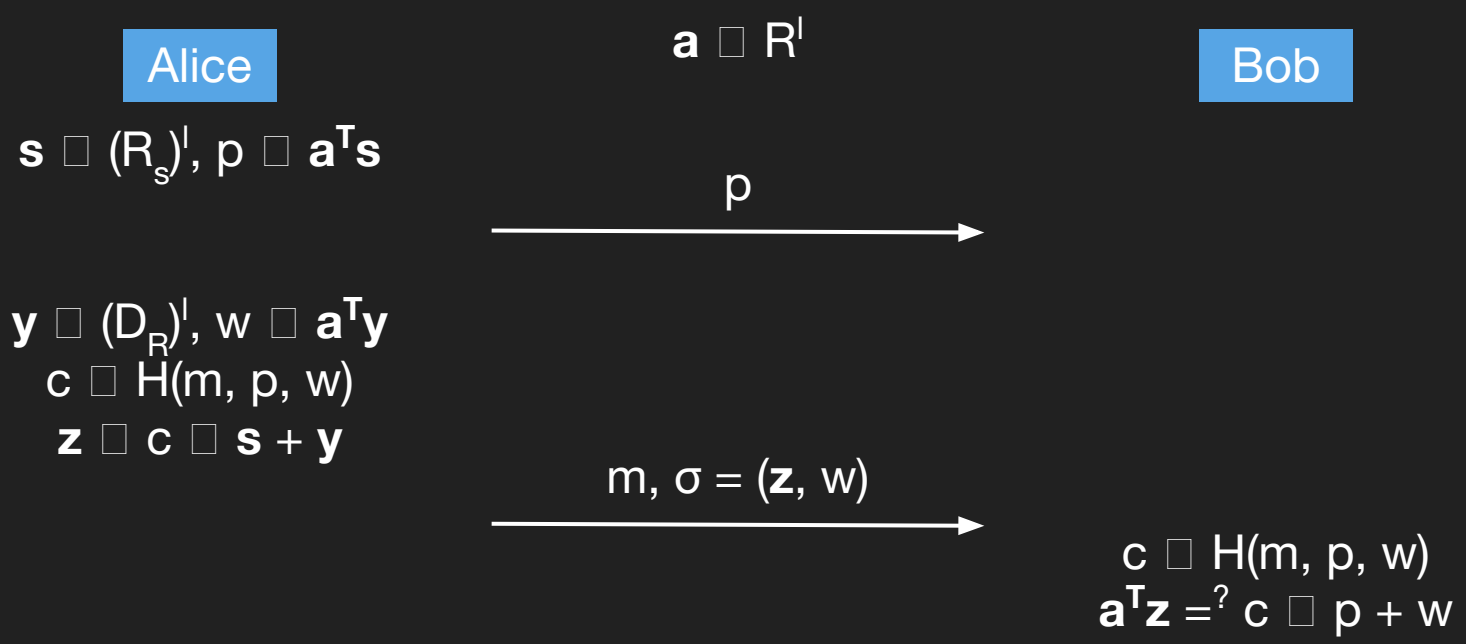
# Fiat-Shamir with Aborts



# Fiat-Shamir with Aborts



# Fiat-Shamir with Aborts



# Fiat-Shamir with Aborts

Alice

$\mathbf{s} \leftarrow (R_s)^l$, $p \leftarrow \mathbf{a}^T\mathbf{s}$

$\mathbf{a} \leftarrow R^l$

Bob

p

$\mathbf{y} \leftarrow (D_R)^l$, $w \leftarrow \mathbf{a}^T\mathbf{y}$

$c \leftarrow H(m, p, w)$

$\mathbf{z} \leftarrow c \cdot \mathbf{s} + \mathbf{y}$

$m, \sigma = (\mathbf{z}, w)$

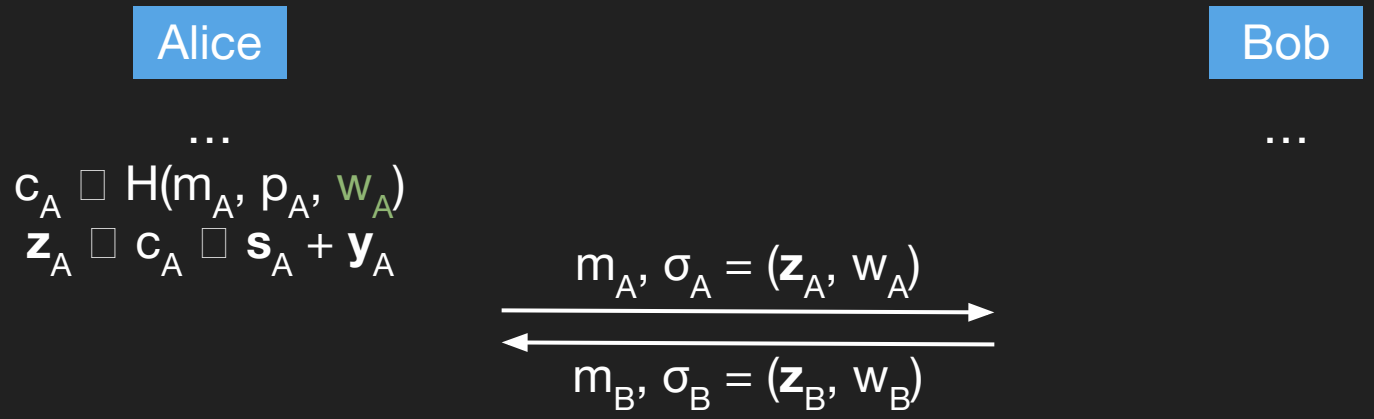
$c \leftarrow H(m, p, w)$

$\mathbf{a}^T\mathbf{z} \stackrel{?}{=} c \cdot p + w$

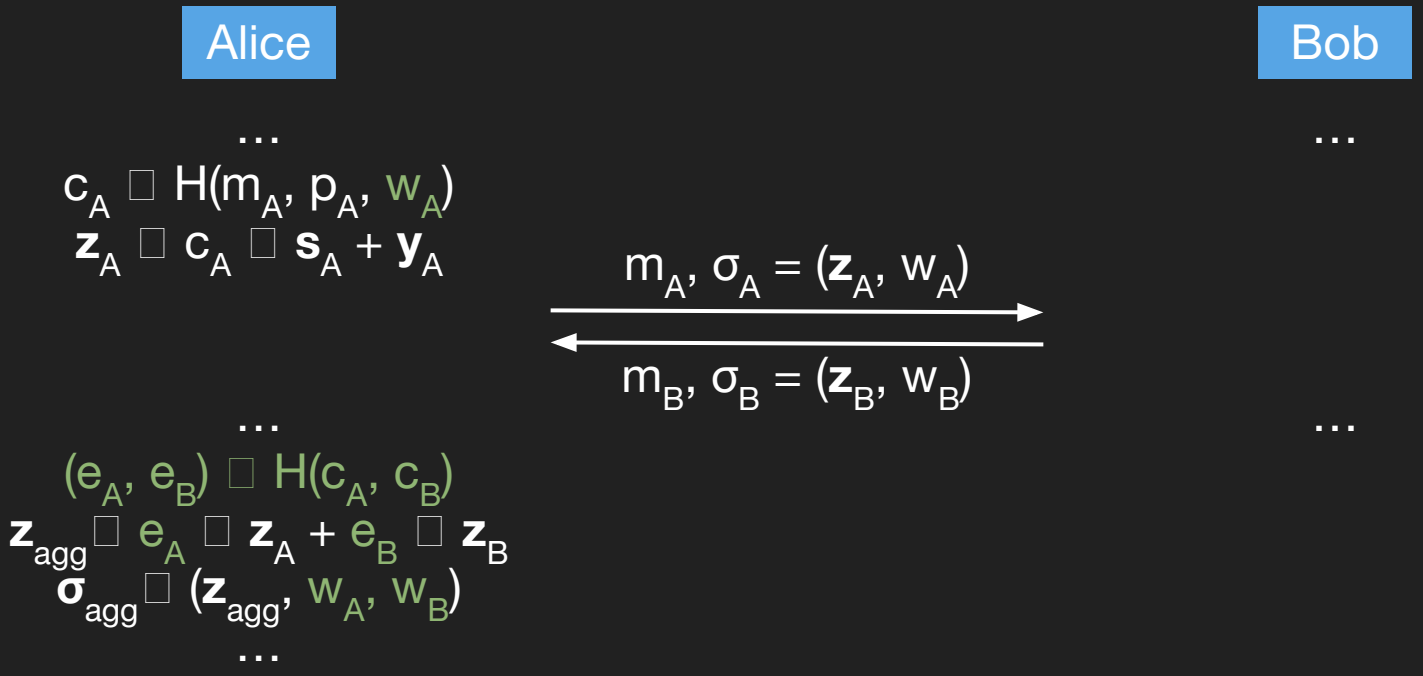
Abort with probability s.t.:

$\mathbf{z} \approx (D_R)^l$

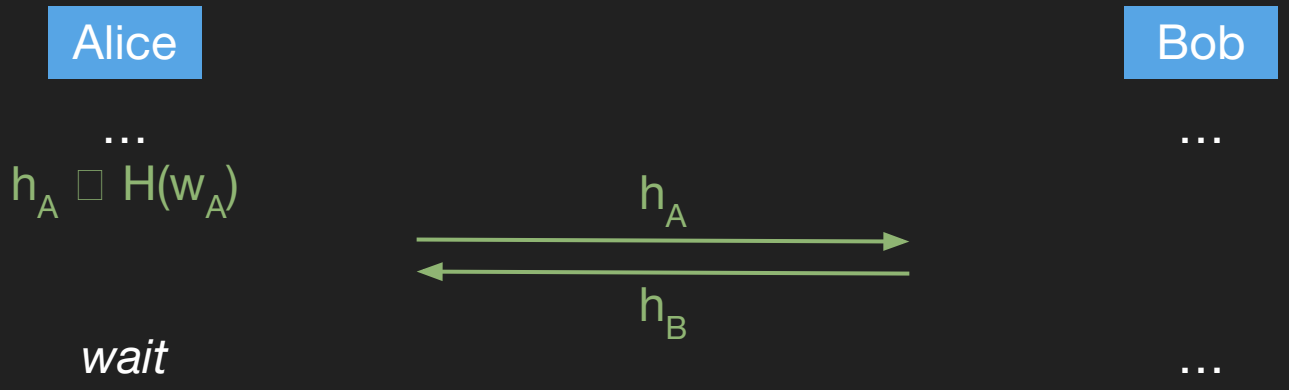
# Non-Interactive Aggregation



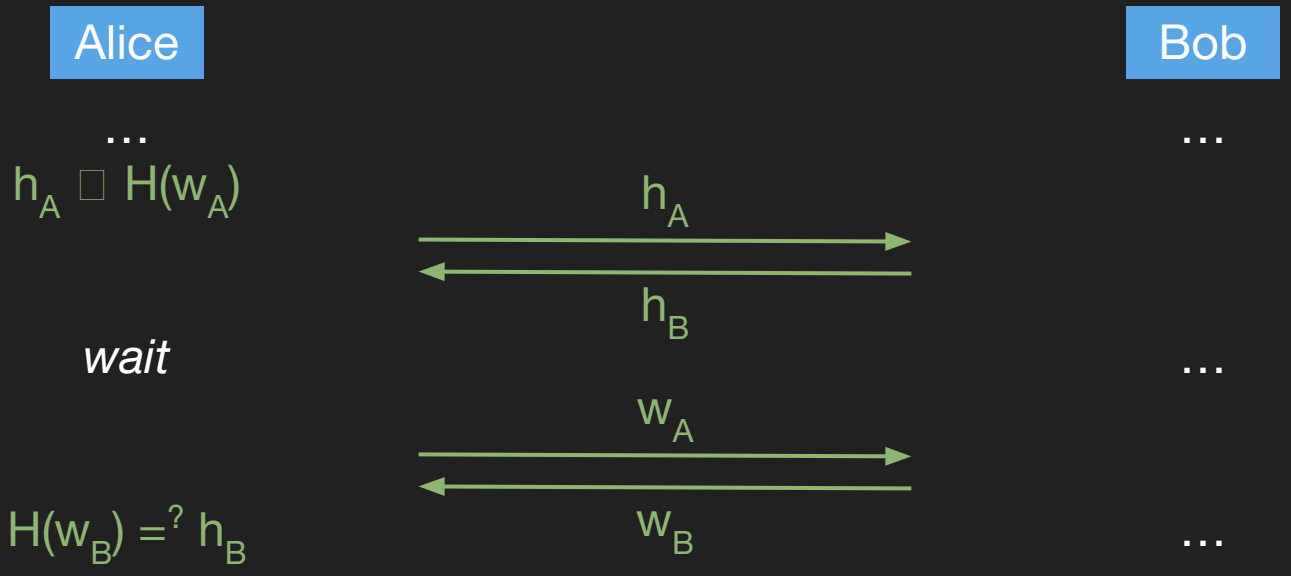
# Non-Interactive Aggregation



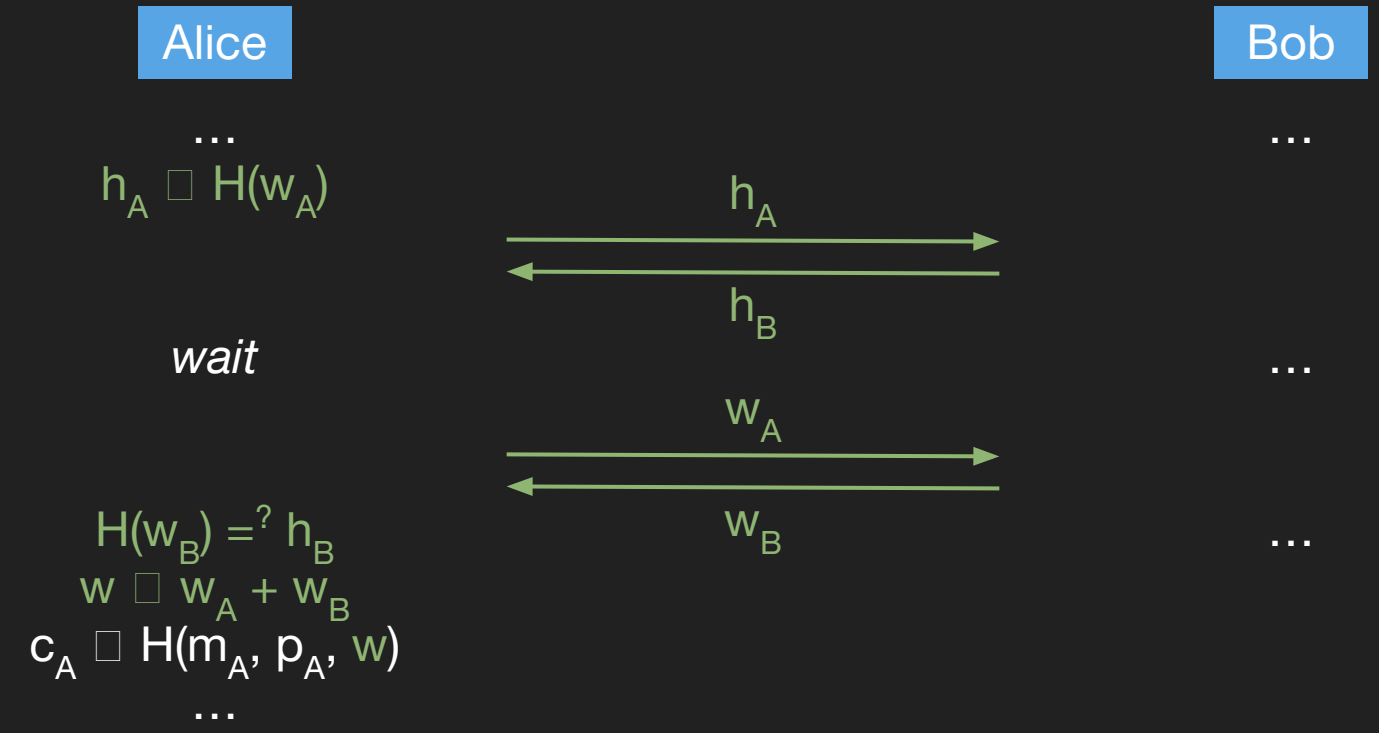
# Interactive Aggregation



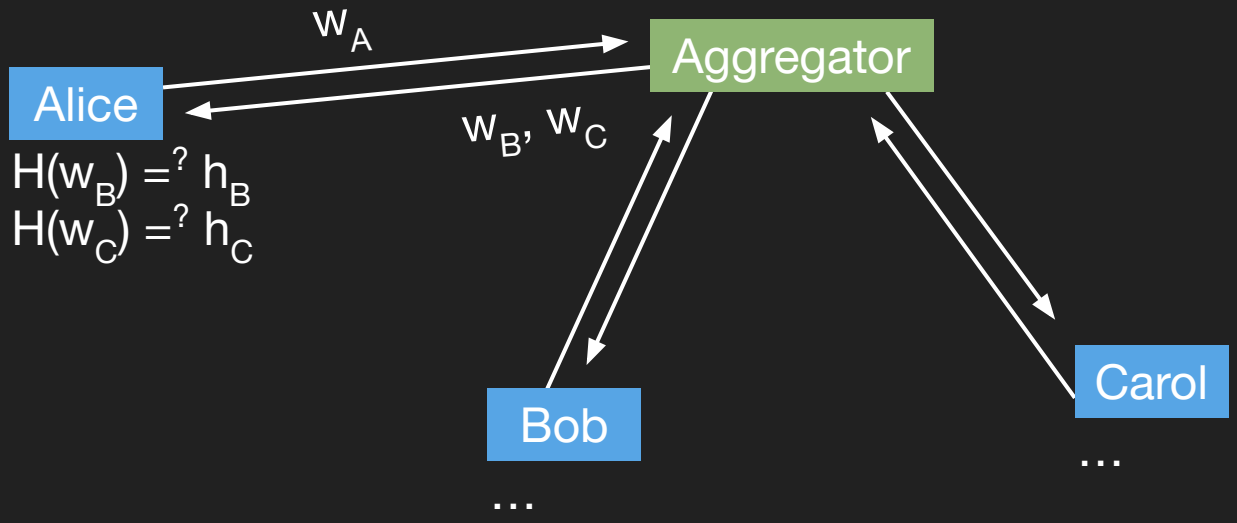
# Interactive Aggregation



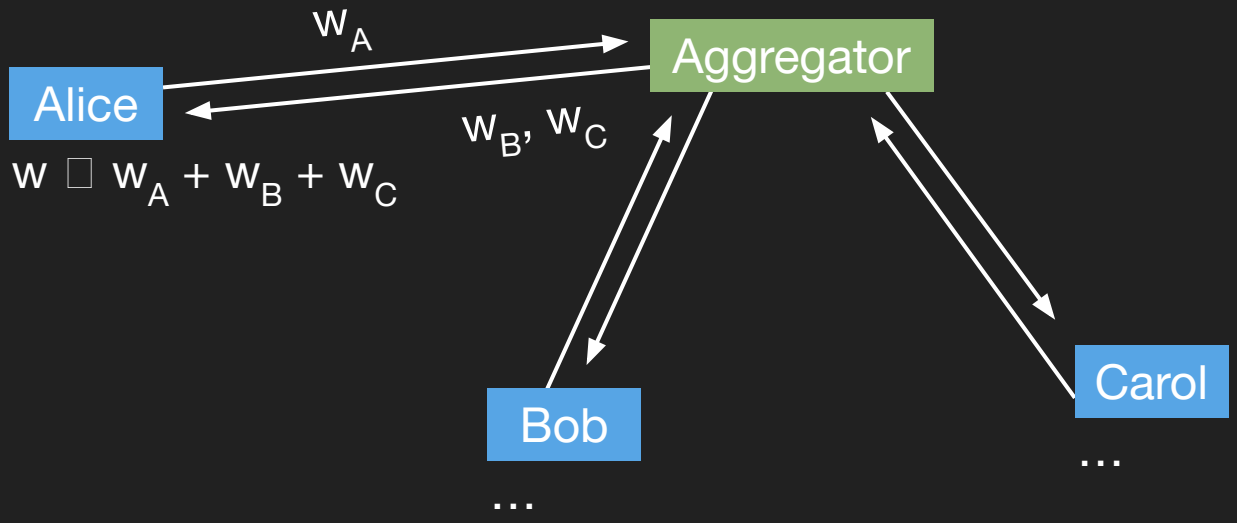
# Interactive Aggregation



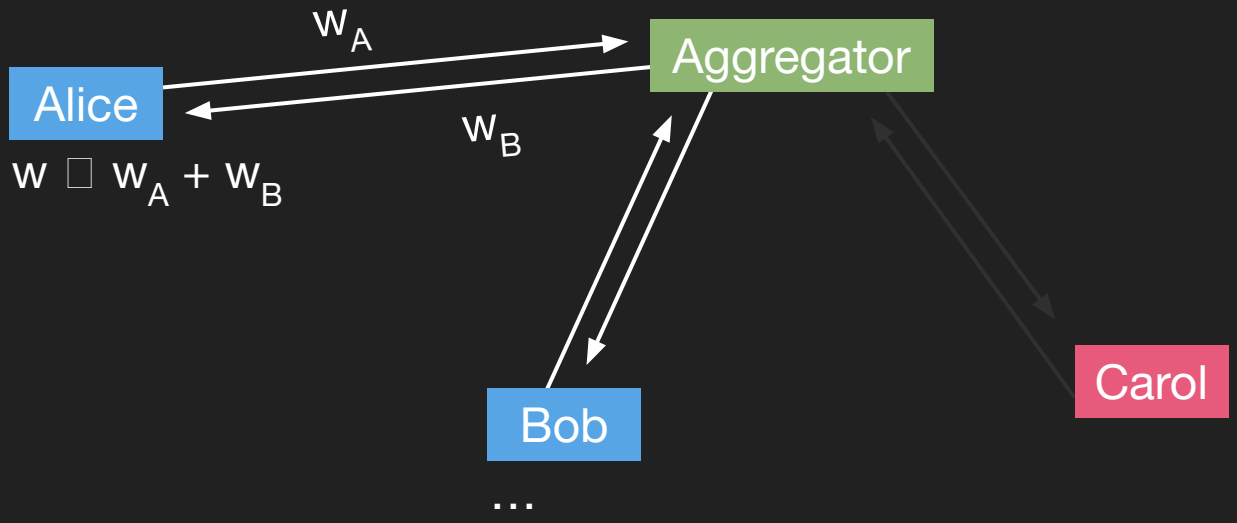
# BFT-Interactive Aggregation



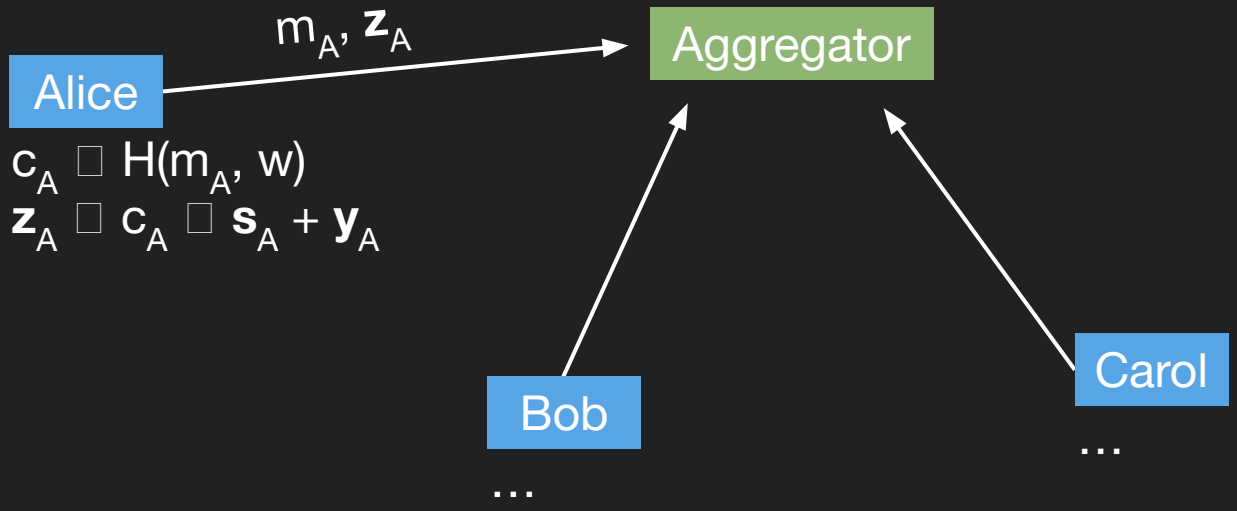
# BFT-Interactive Aggregation



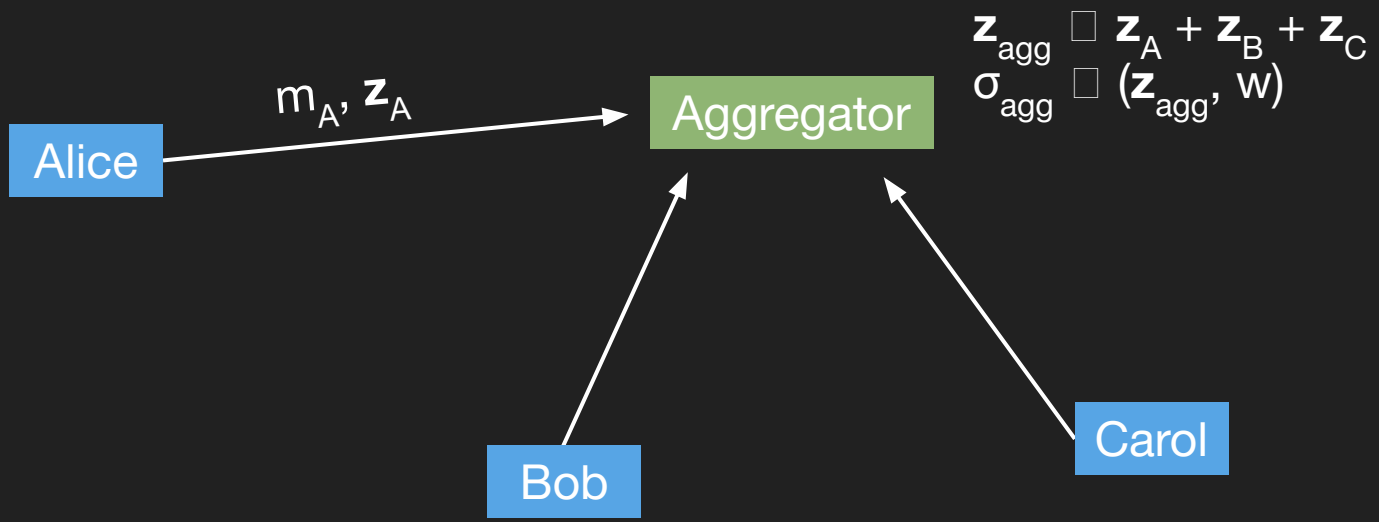
# BFT-Interactive Aggregation



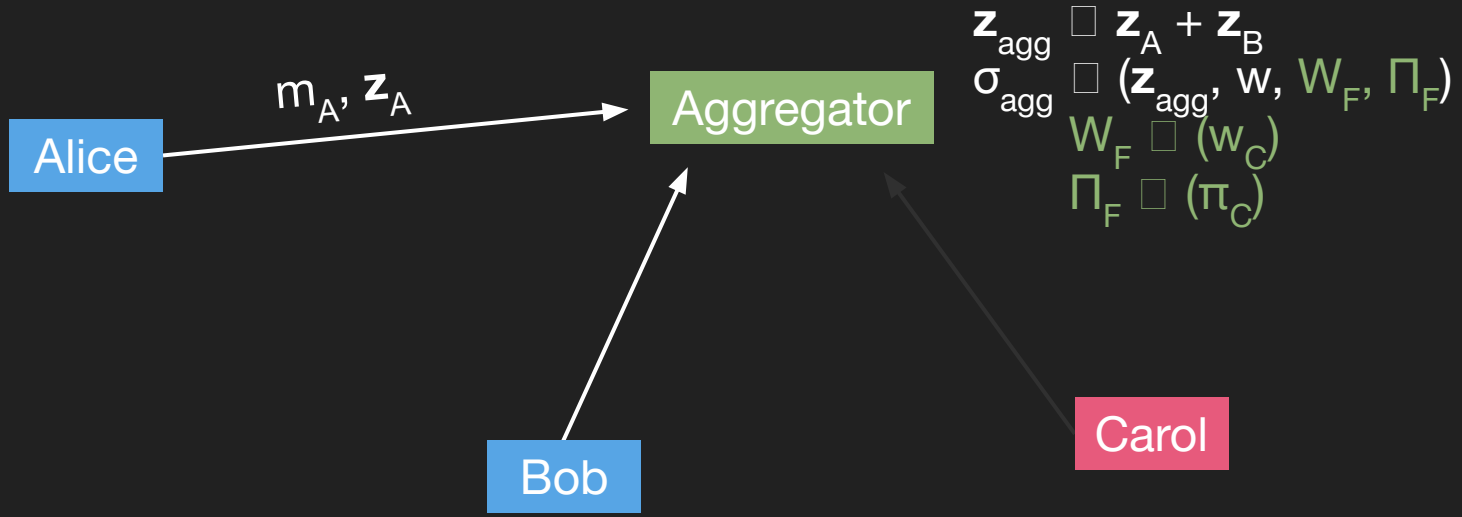
# BFT-Interactive Aggregation



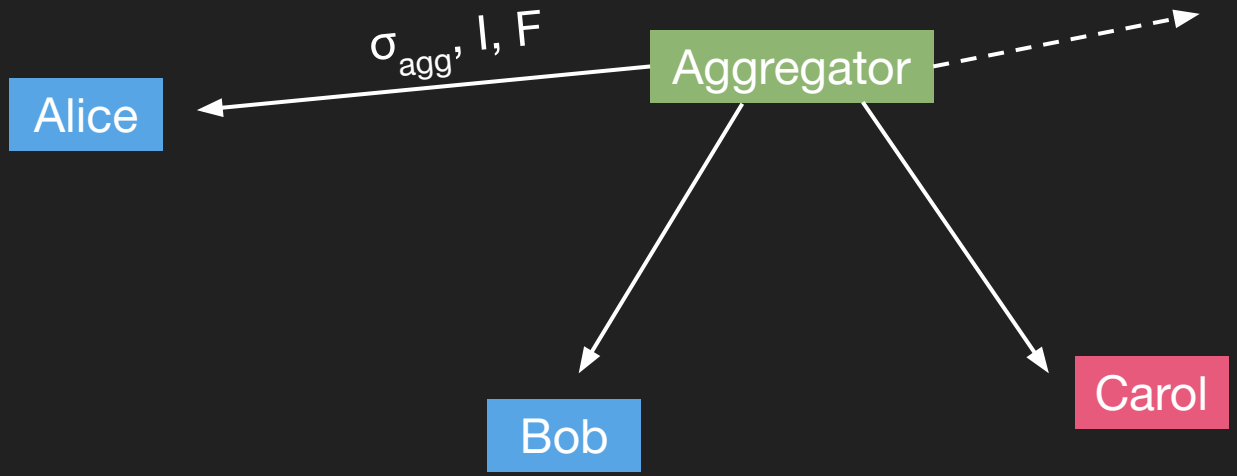
# BFT-Interactive Aggregation



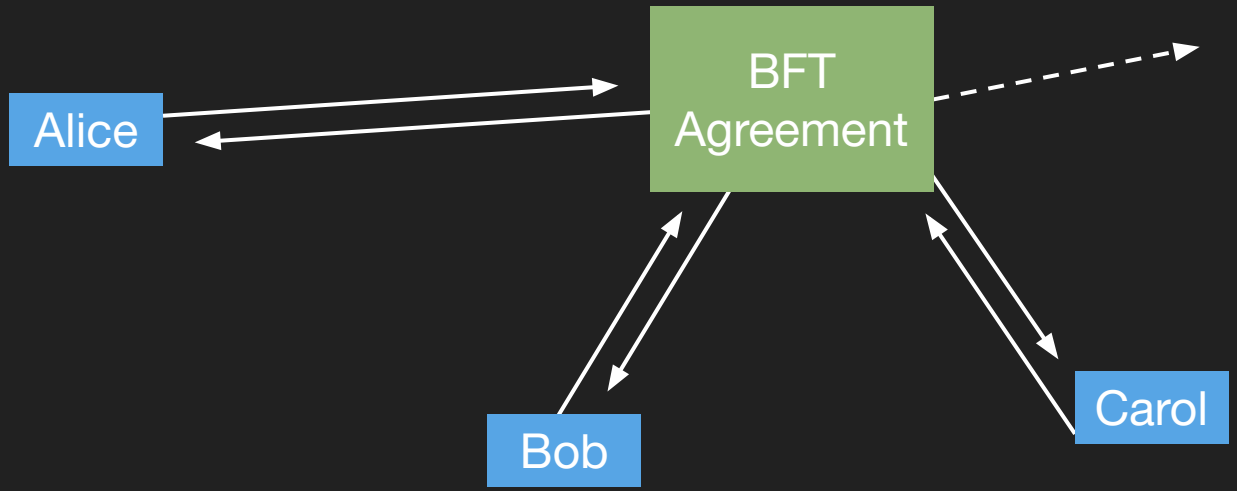
# BFT-Interactive Aggregation



# BFT-Interactive Aggregation



# BFT-Interactive Aggregation



# Signature Size (N=1024)

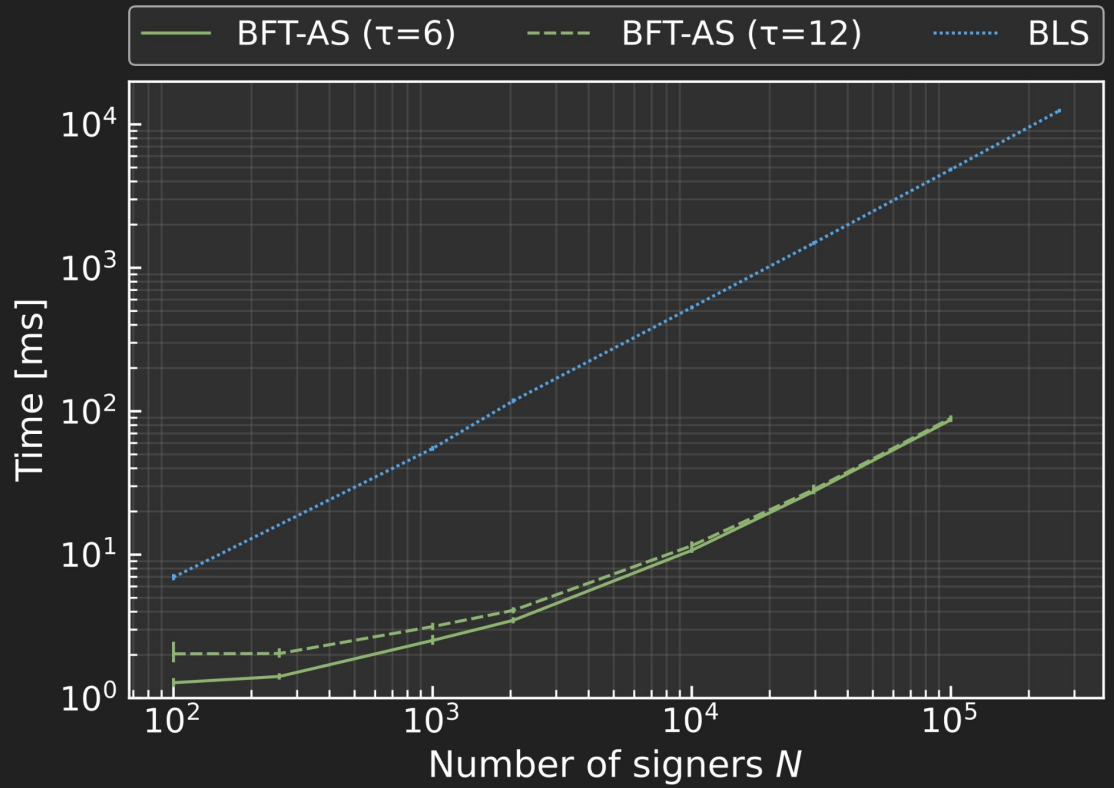
| | PQ | PK | Sig. | Agg. Sig. (Best) | Agg. Sig. (Worst) |
|---|---|---|---|---|---|
| BLS [BGLS03] | ✗ | 48 B | 96 B | 96 B | 96 B |
| Half-Agg. [BR21] | ✔ | ~ 10 KiB | ~ 15 KiB | > 20 MiB | |
| Squirrel [FSZ22] | ✔ | 0.9 KiB | 45 KiB | 572 KiB | |
| Naive (Falcon) | ✔ | 897 B | 666 B | 666 KiB | |
| **Ours (HAB)** | ✔ | **2.1 KiB** | **74 KiB** | **41 KiB** | **156 KiB** |

# Signature Size (N=1024)

| | PQ | PK | Sig. | Agg. Sig. (Best) | Agg. Sig. (Worst) |
|---|---|---|---|---|---|
| BLS [BGLS03] | ✗ | 48 B | 96 B | 96 B | 96 B |
| Half-Agg. [BR21] | ✔ | ~ 10 KiB | ~ 15 KiB | > 20 MiB | |
| Squirrel [FSZ22] | ✔ | 0.9 KiB | 45 KiB | 572 KiB | |
| Naive (Falcon) | ✔ | 897 B | 666 B | 666 KiB | |
| **Ours (HAB)** | ✔ | **2.1 KiB** | **74 KiB** | **41 KiB** | **156 KiB** |

41–156 B/Signer

# Verification Time



# Thank You!

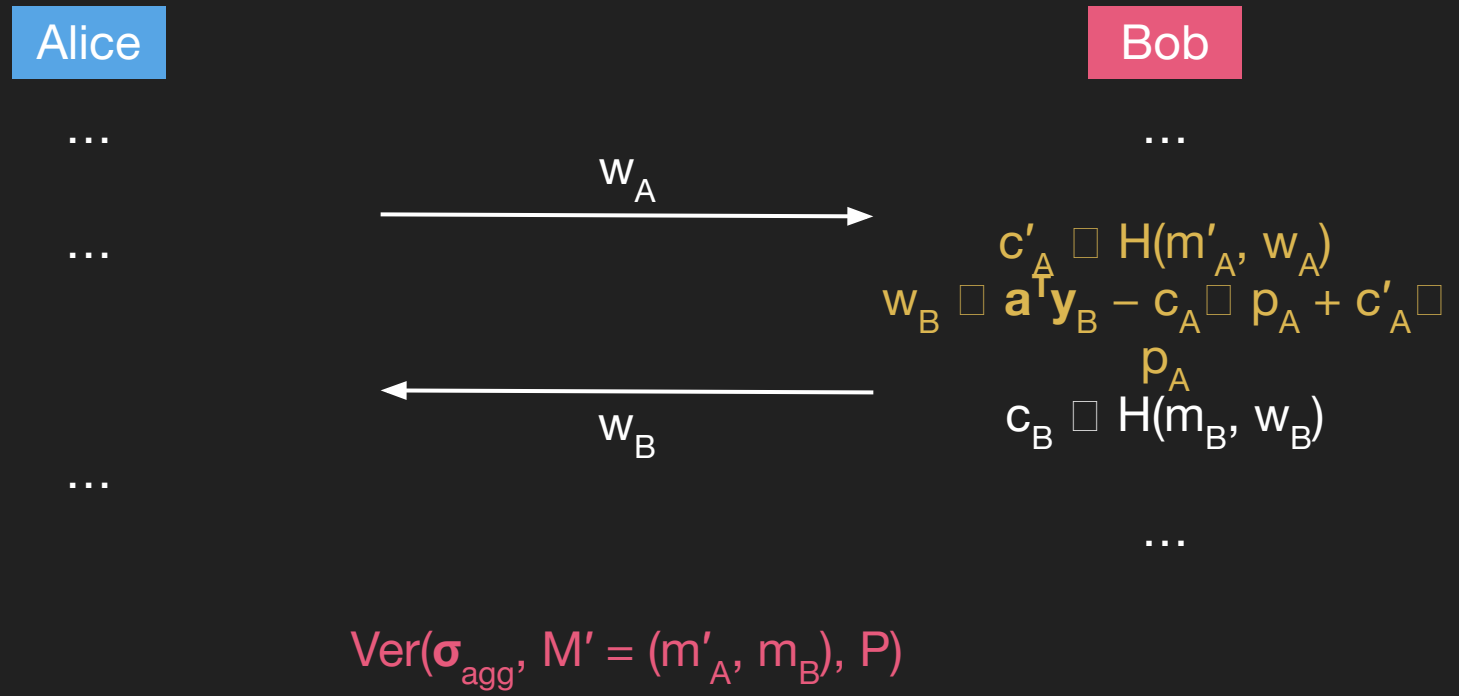
Quentin Kniep
qkniep@ethz.ch

https://disco.ethz.ch

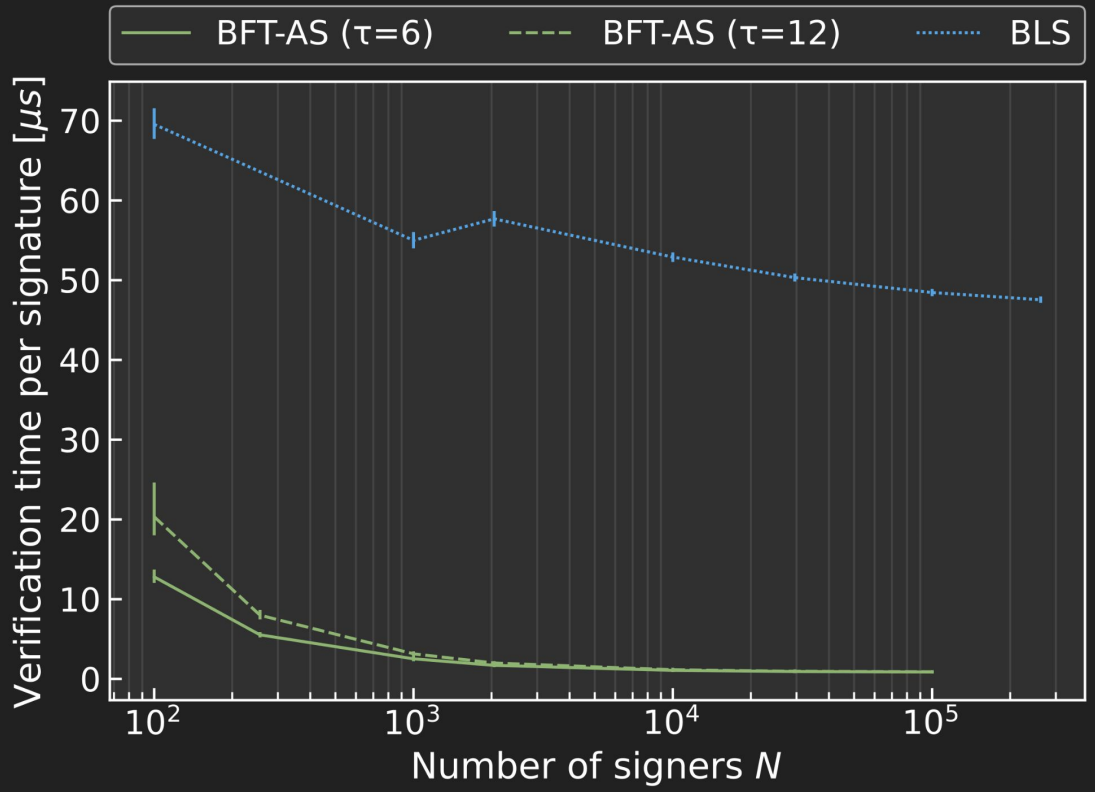
# Related Work

- FSwA One-Time Signatures [LM08]
- Interactive Many-Time Aggregate Signatures [BK20]
- Non-Interactive One-Time Aggregate Signatures [BK20]
- Non-Interactive Half-Aggregate Signatures [BR21]
- Few-Time Synchronized Multi-Signatures [FSZ22]

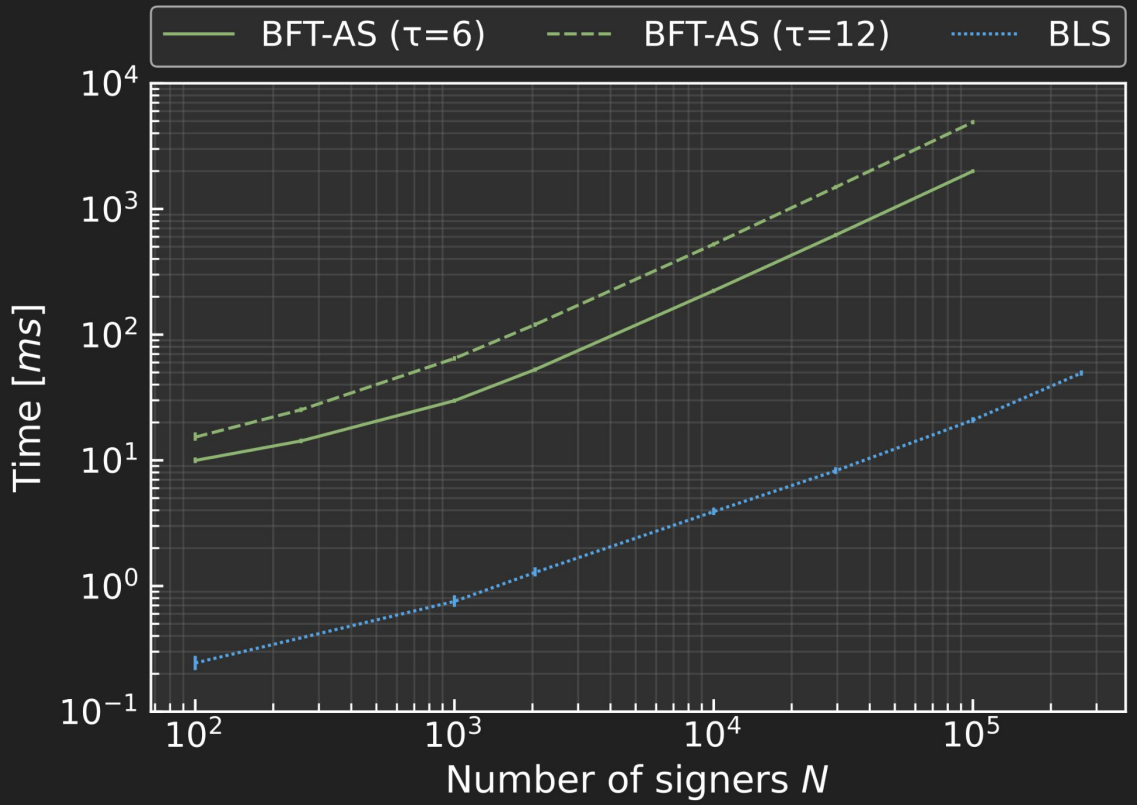
# Rogue-Key Attack



# Verification Time (per Signer)



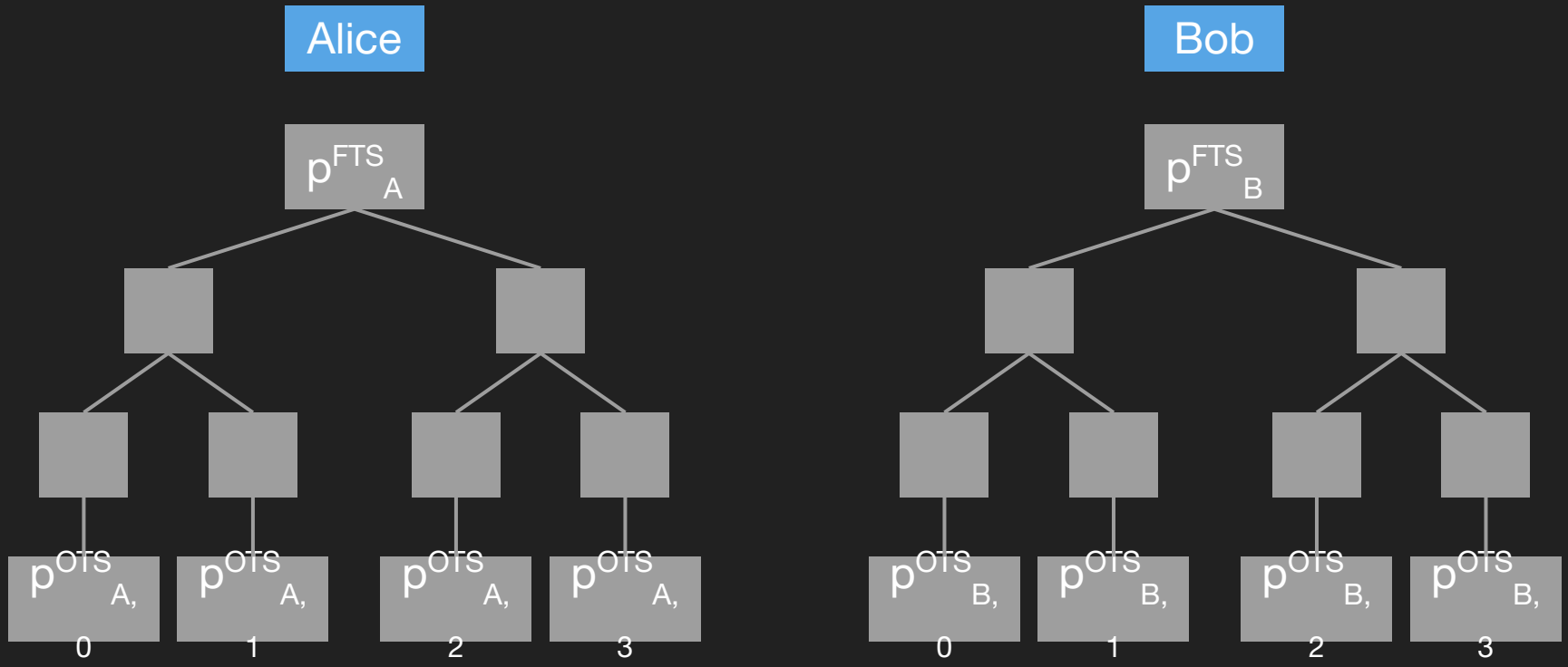
# Aggregation Time



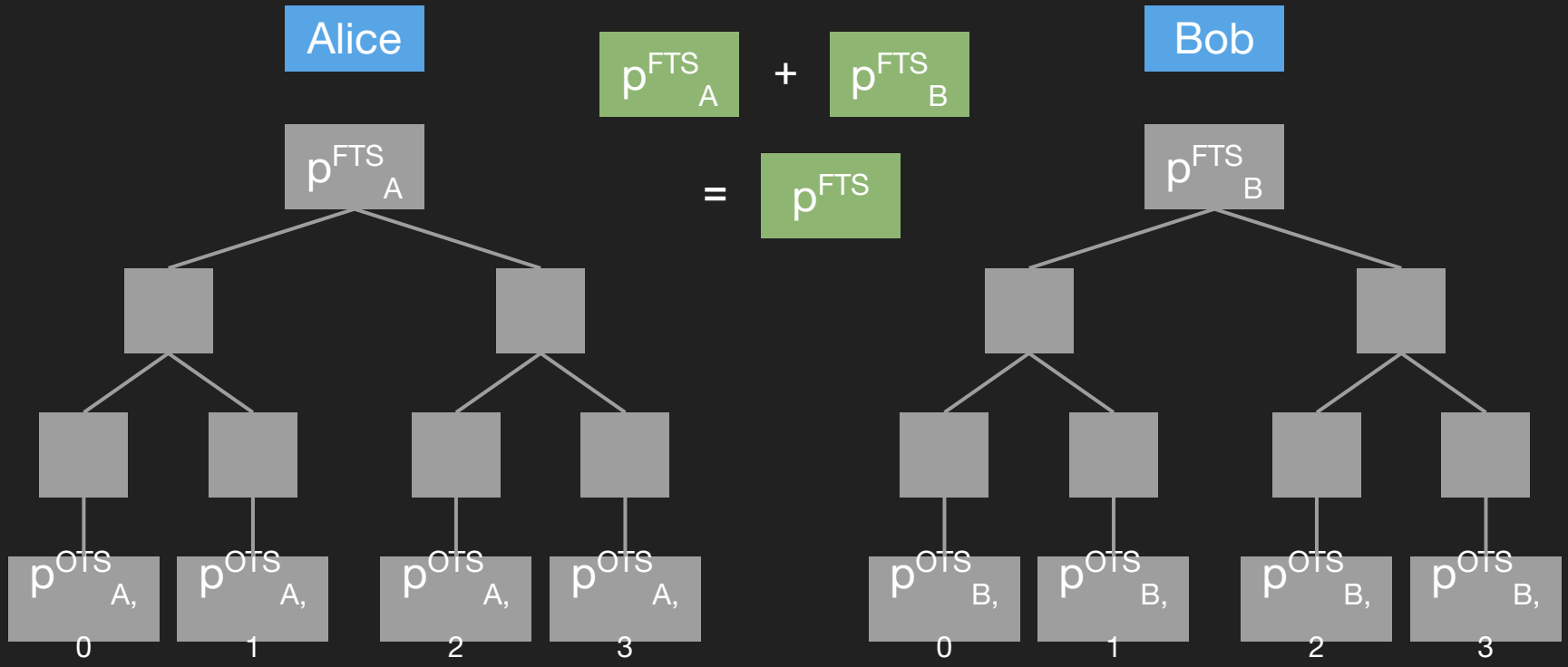
# Signature Size (N=1024)

| | PQ | Interactivity | PK | Sig. | Agg. Sig. (Best) | Agg. Sig. (Worst) |
|---|---|---|---|---|---|---|
| BLS [BGLS03] | ✗ | None | 48 B | 96 B | 96 B | 96 B |
| Half-Agg. [BR21] | ✔ | None | ~ 10 KiB | ~ 15 KiB | > 20 MiB | |
| Squirrel [FSZ22] | ✔ | Sync. | 0.9 KiB | 45 KiB | 572 KiB | |
| Naive (Falcon) | ✔ | None | 897 B | 666 B | 666 KiB | |
| Ours (SSB) | ✔ | BFT | 1.2 KiB | 15 KiB | 41 KiB | 931 KiB |
| Ours (BAS) | ✔ | Sync. | 2.1 KiB | 74 KiB | 156 KiB | |
| **Ours (HAB)** | ✔ | **BFT** | **2.1 KiB** | **74 KiB** | **41 KiB** | **156 KiB** |

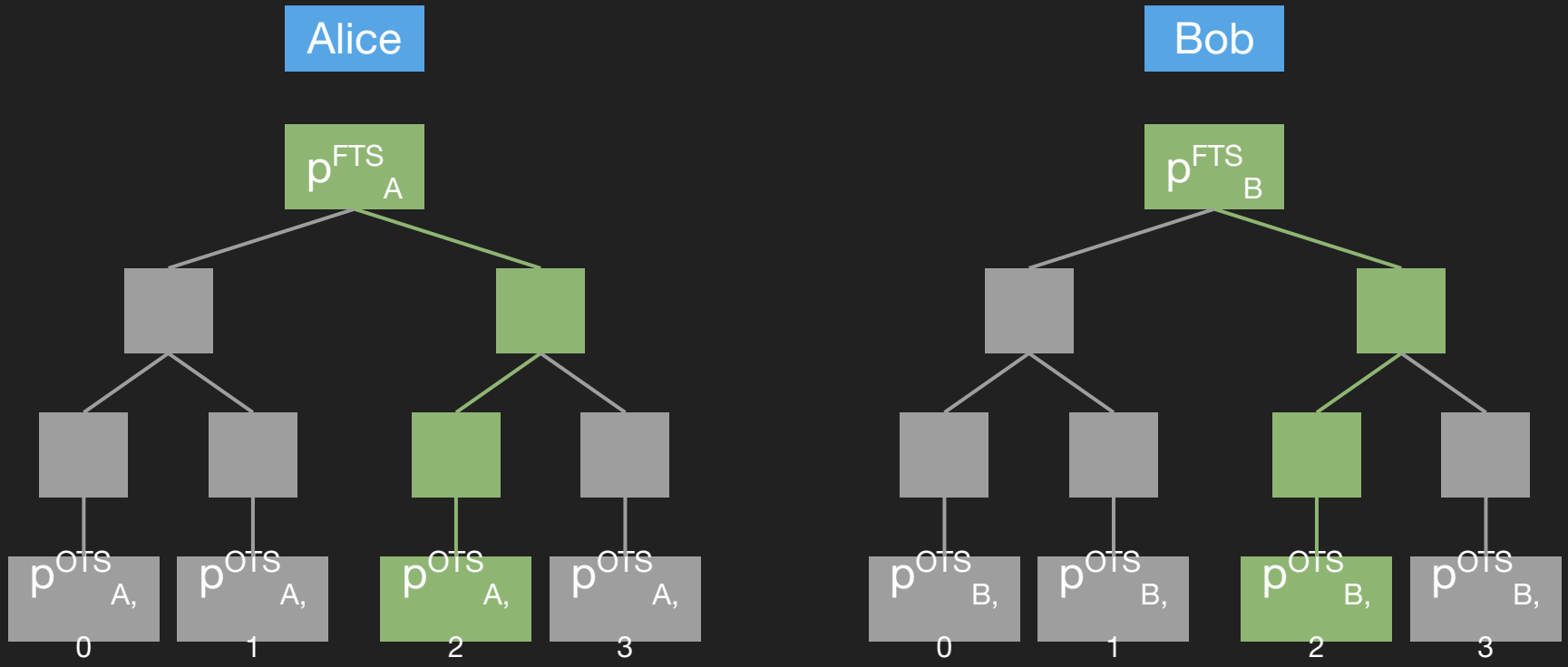
# Squirrel: Synchronized Aggregate FTS



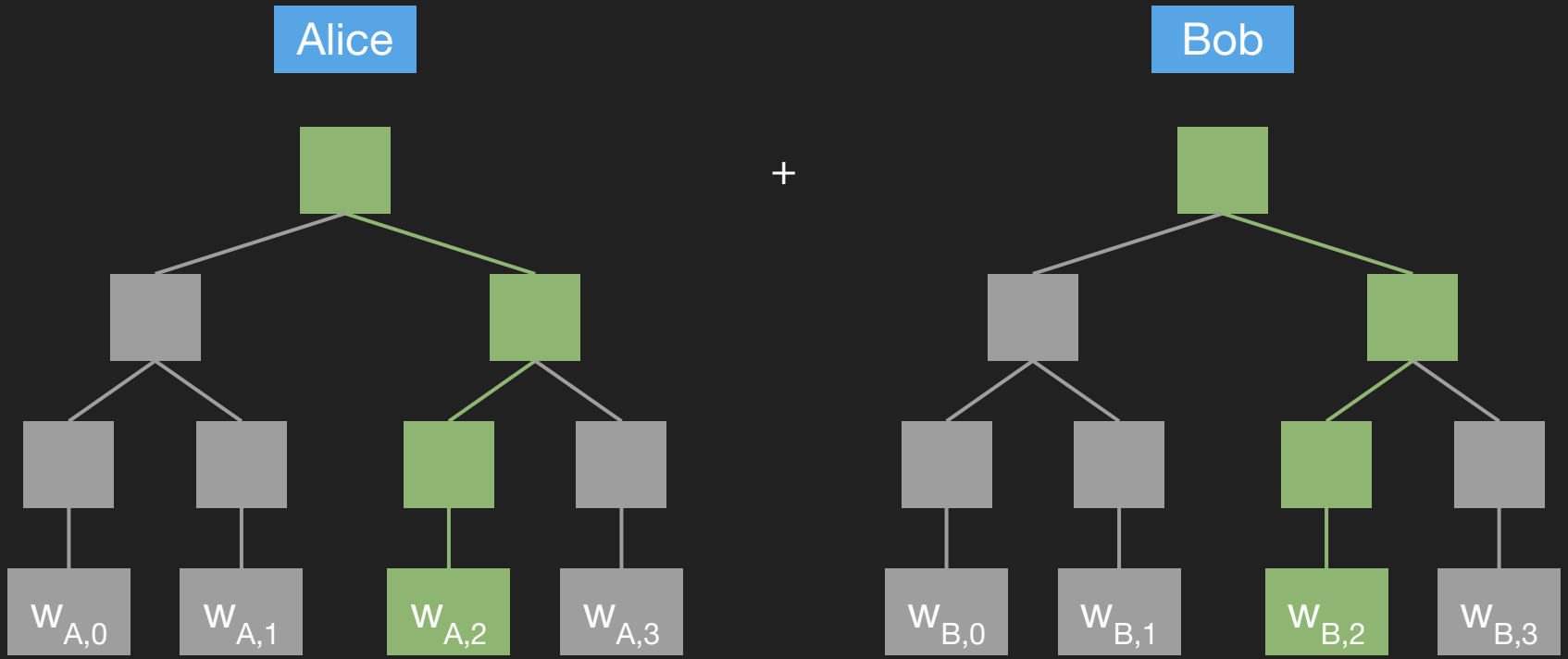
# Squirrel: Synchronized Aggregate FTS



# Squirrel: Synchronized Aggregate FTS



# Worst Case Fallback



# Key Generation