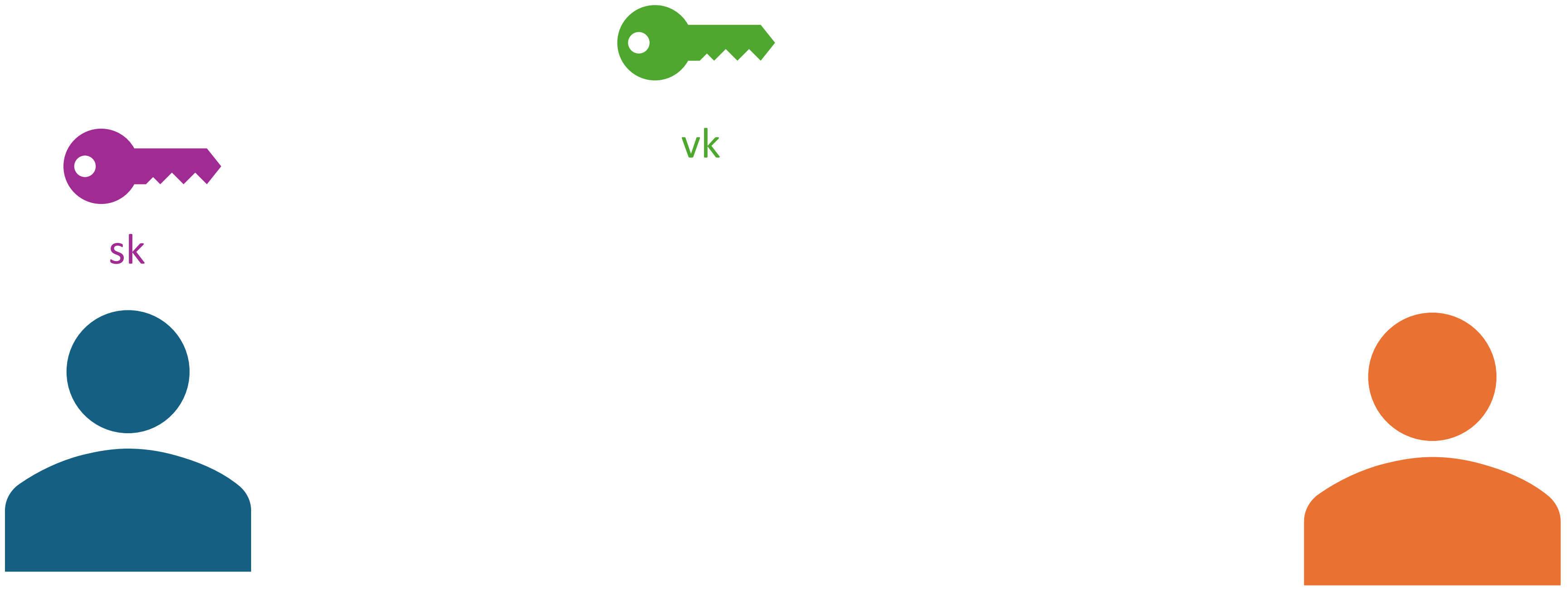
Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption

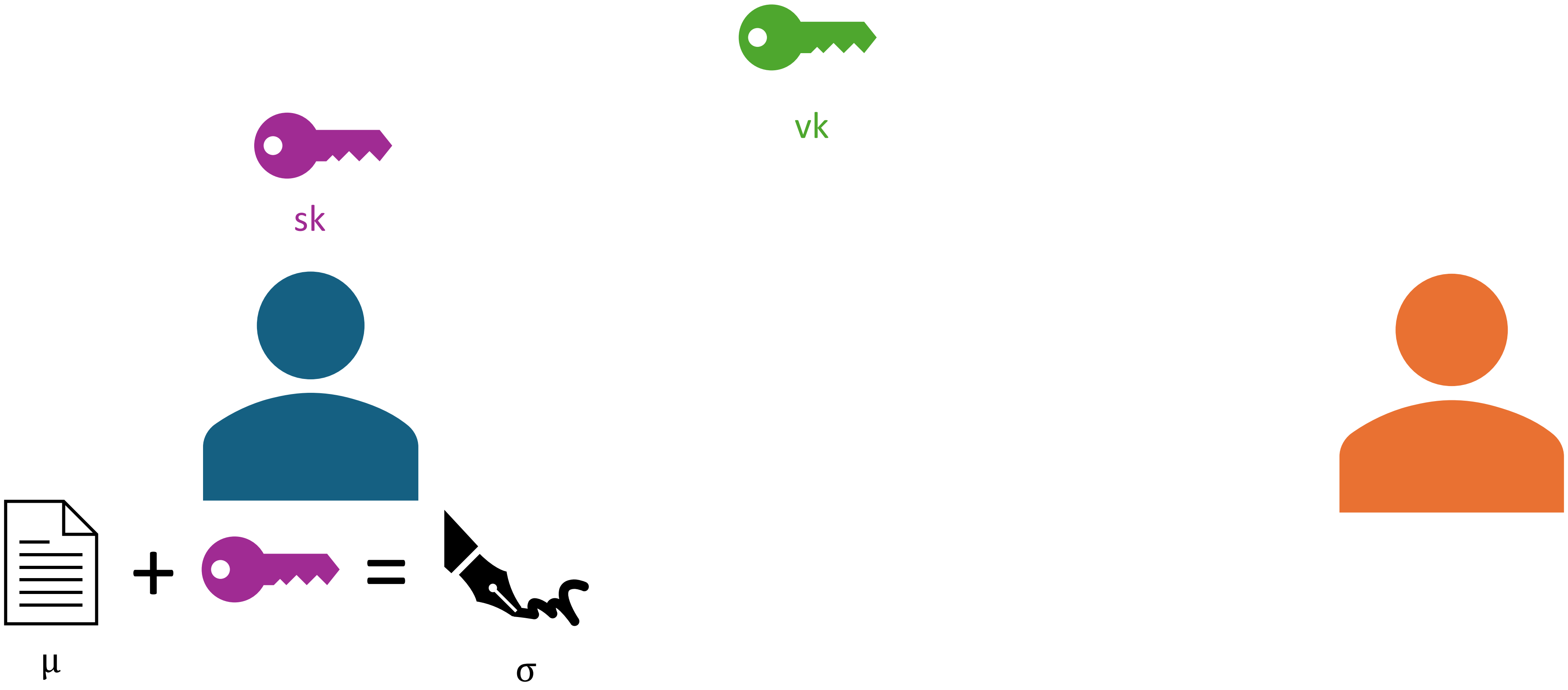
Kamil Doruk Gur (UMD),
Jonathan Katz (Google, UMD),
Tjerand Silde (NTNU)

Overview: Digital Signatures

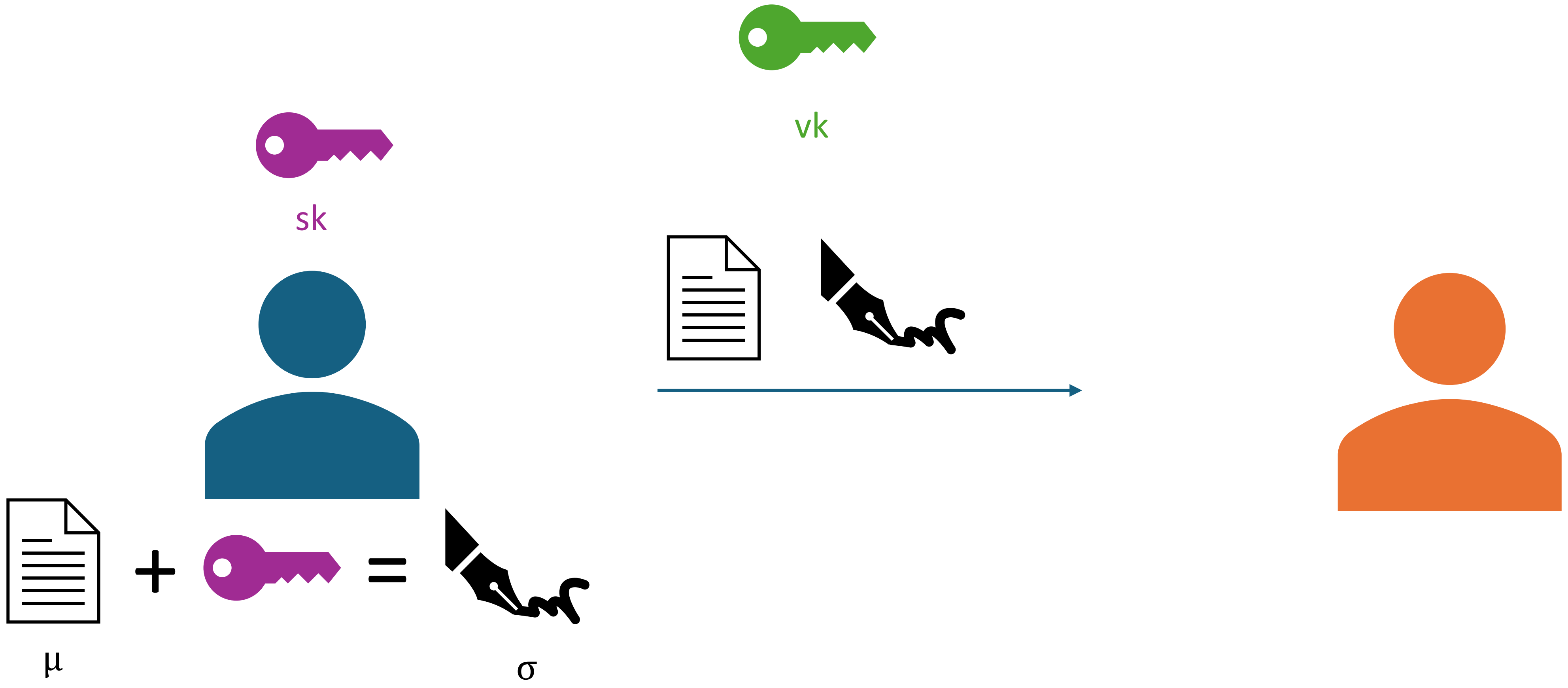
Overview: Digital Signatures



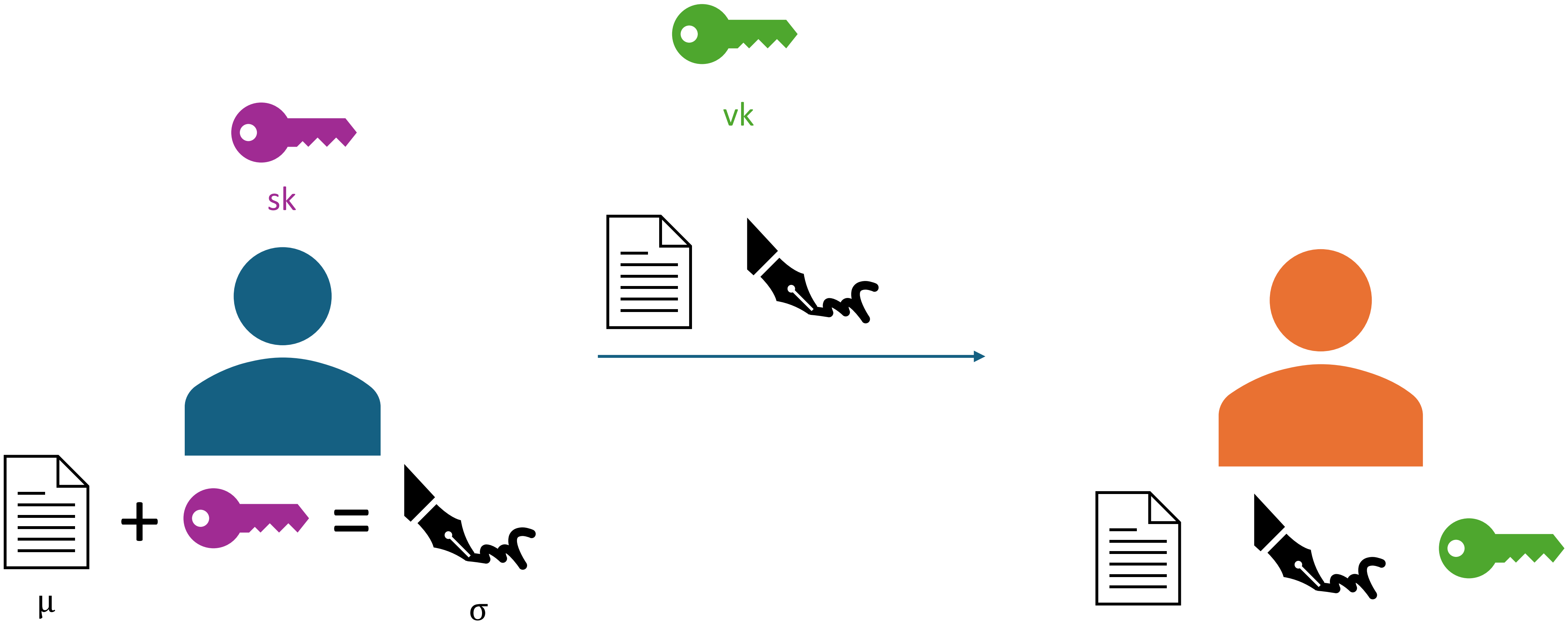
Overview: Digital Signatures



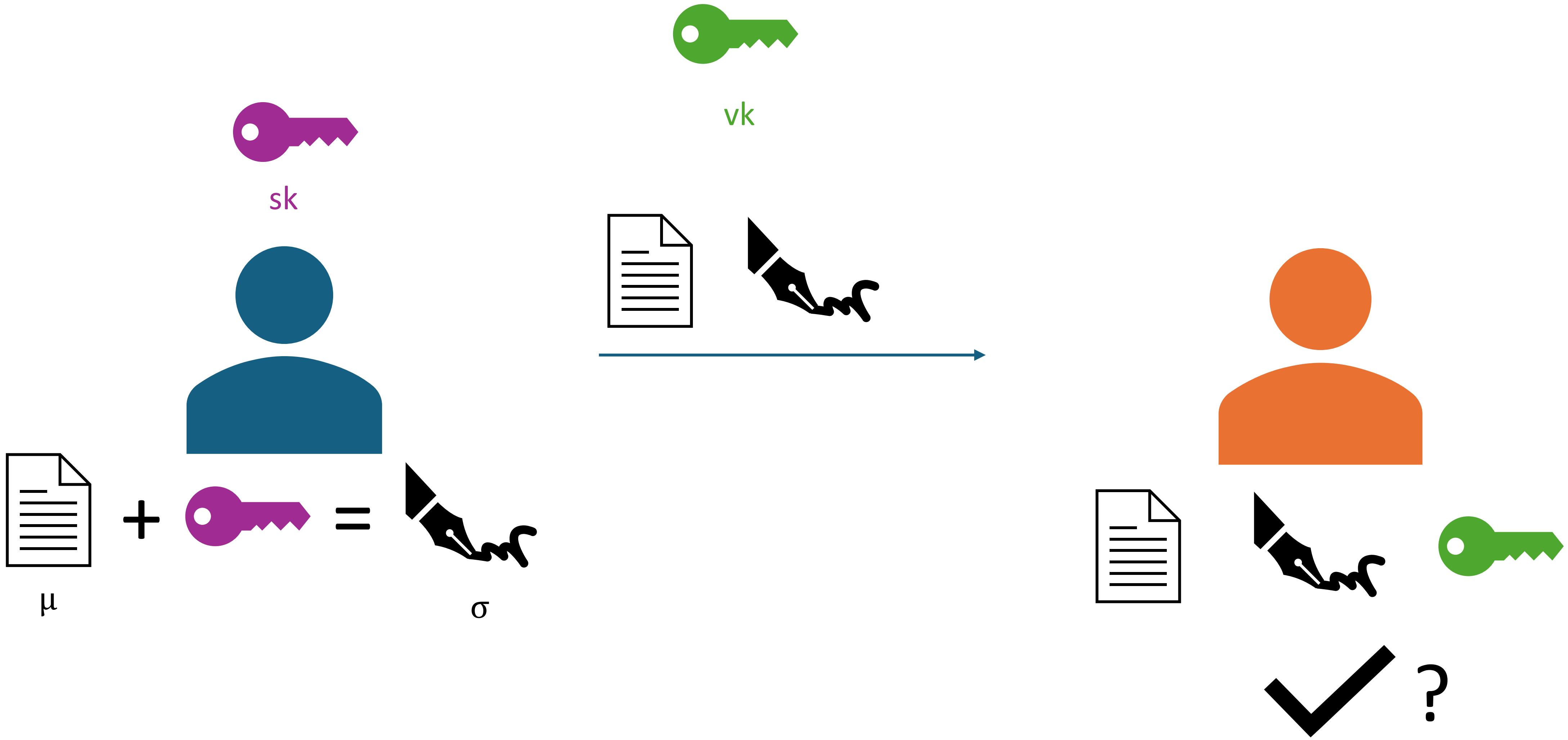
Overview: Digital Signatures



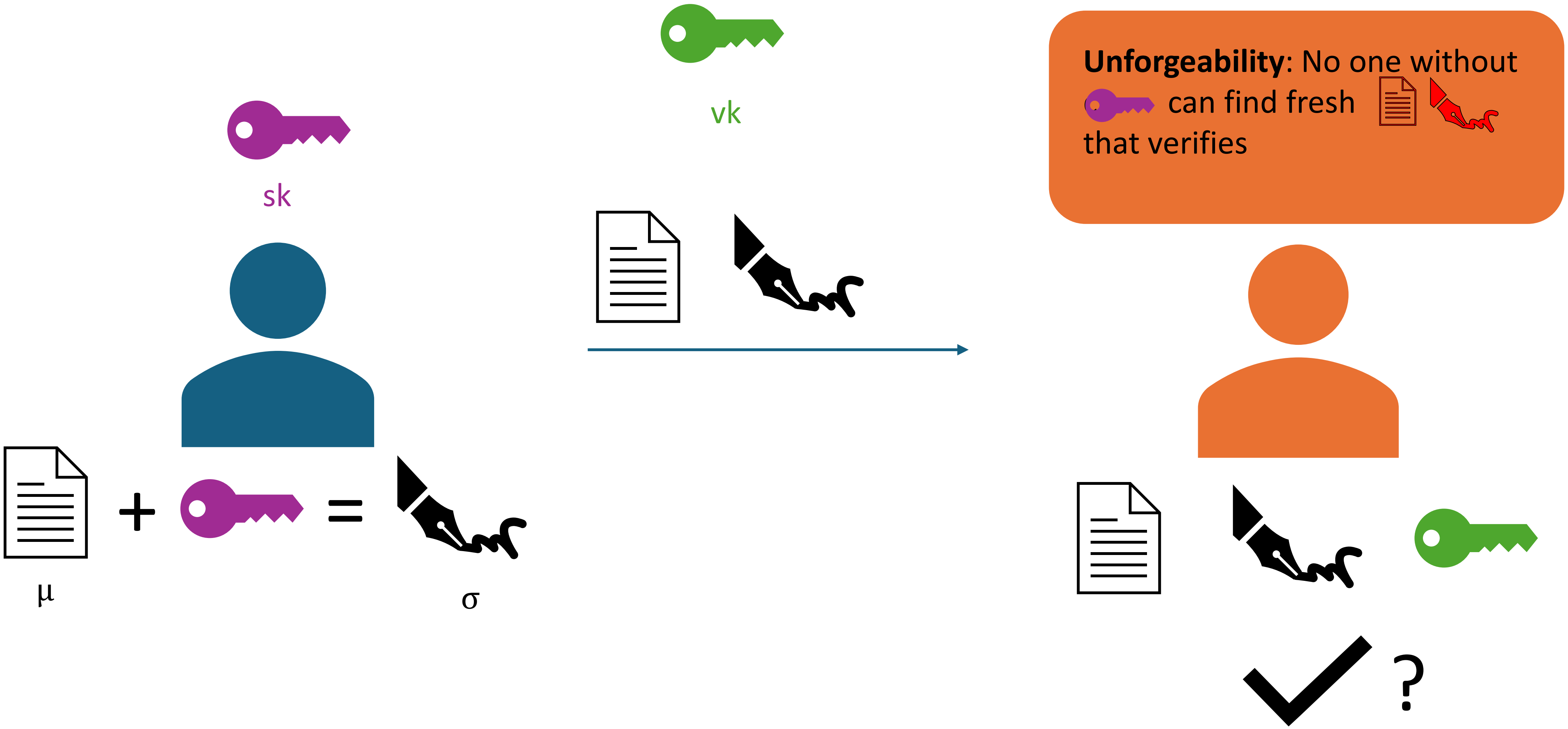
Overview: Digital Signatures



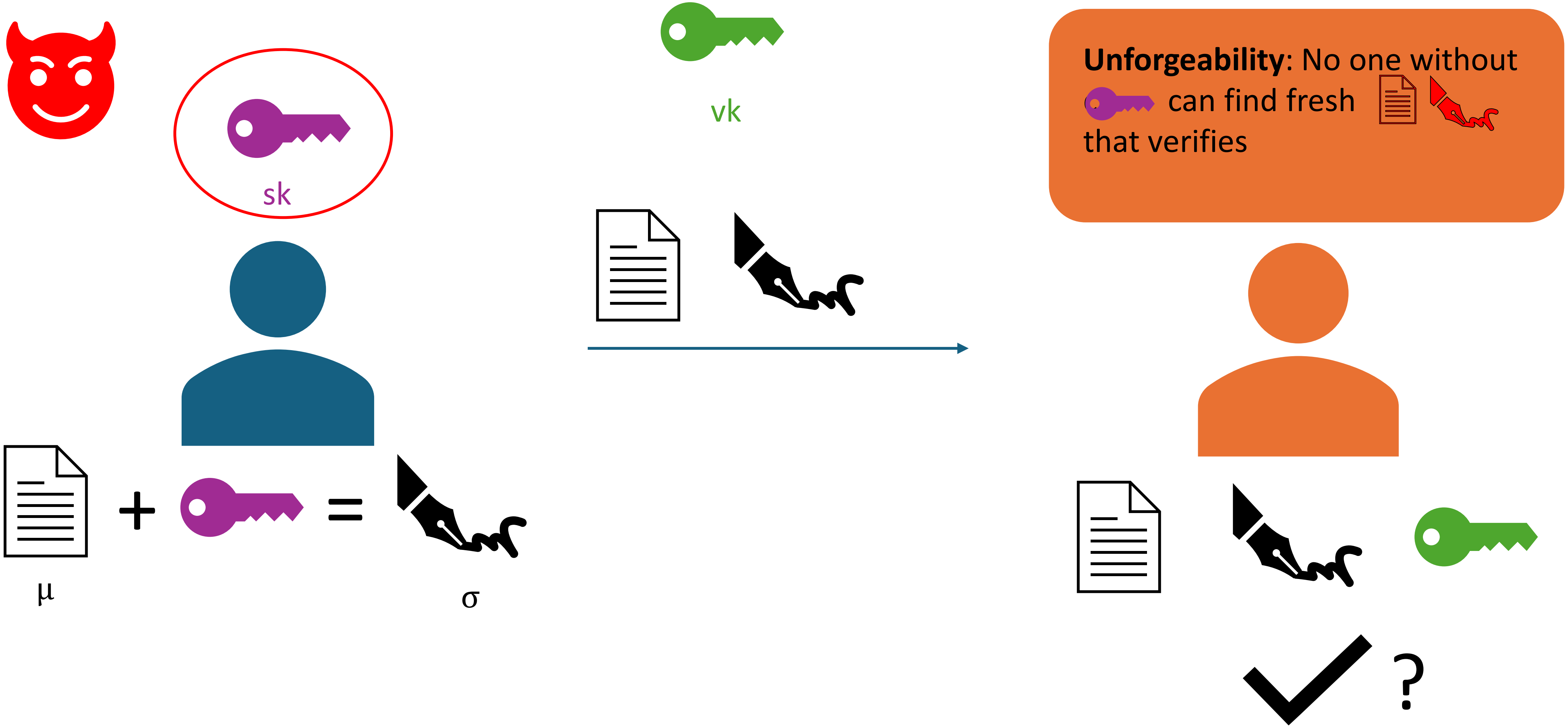
Overview: Digital Signatures



Overview: Digital Signatures

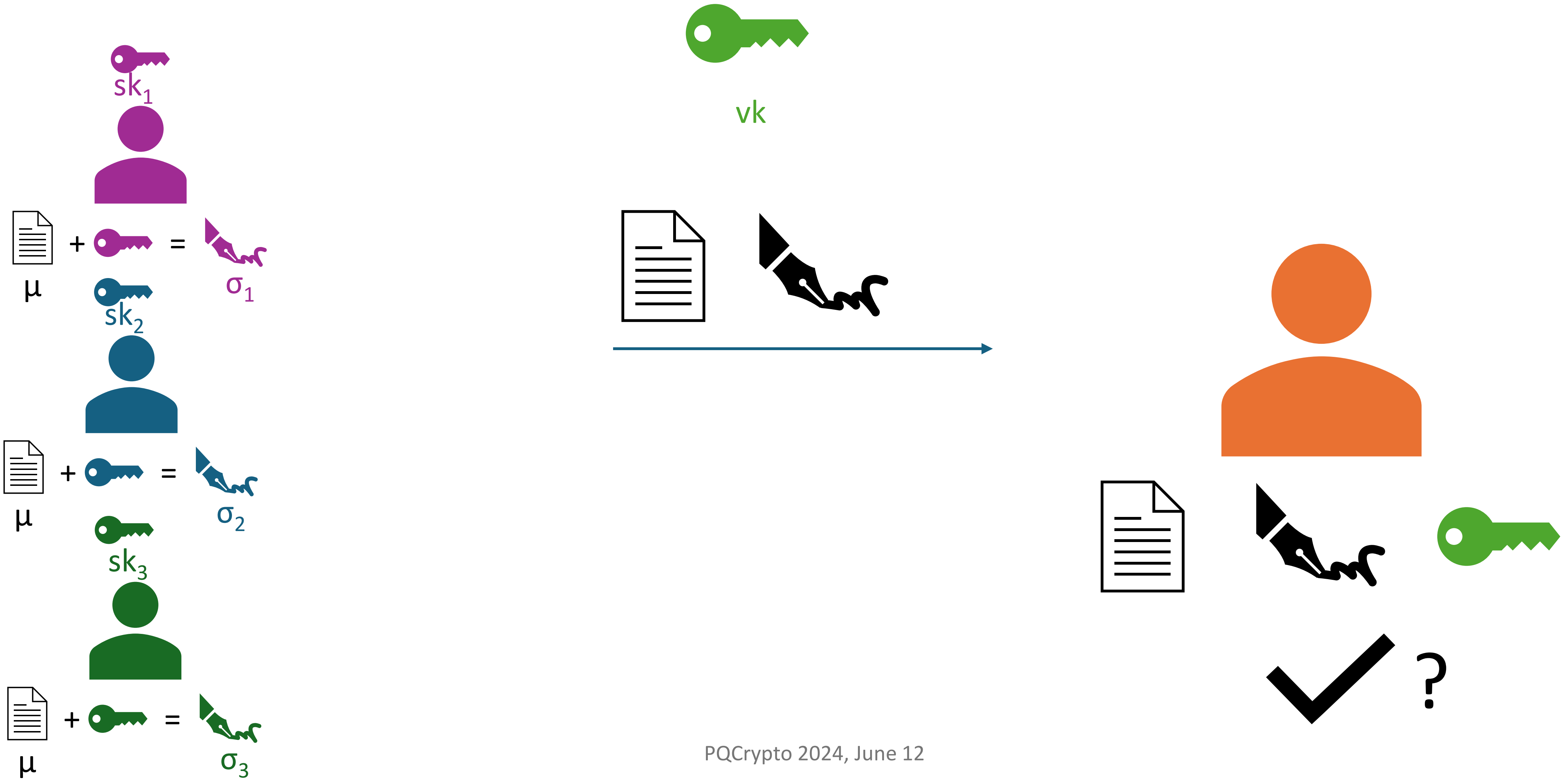


Overview: Digital Signatures

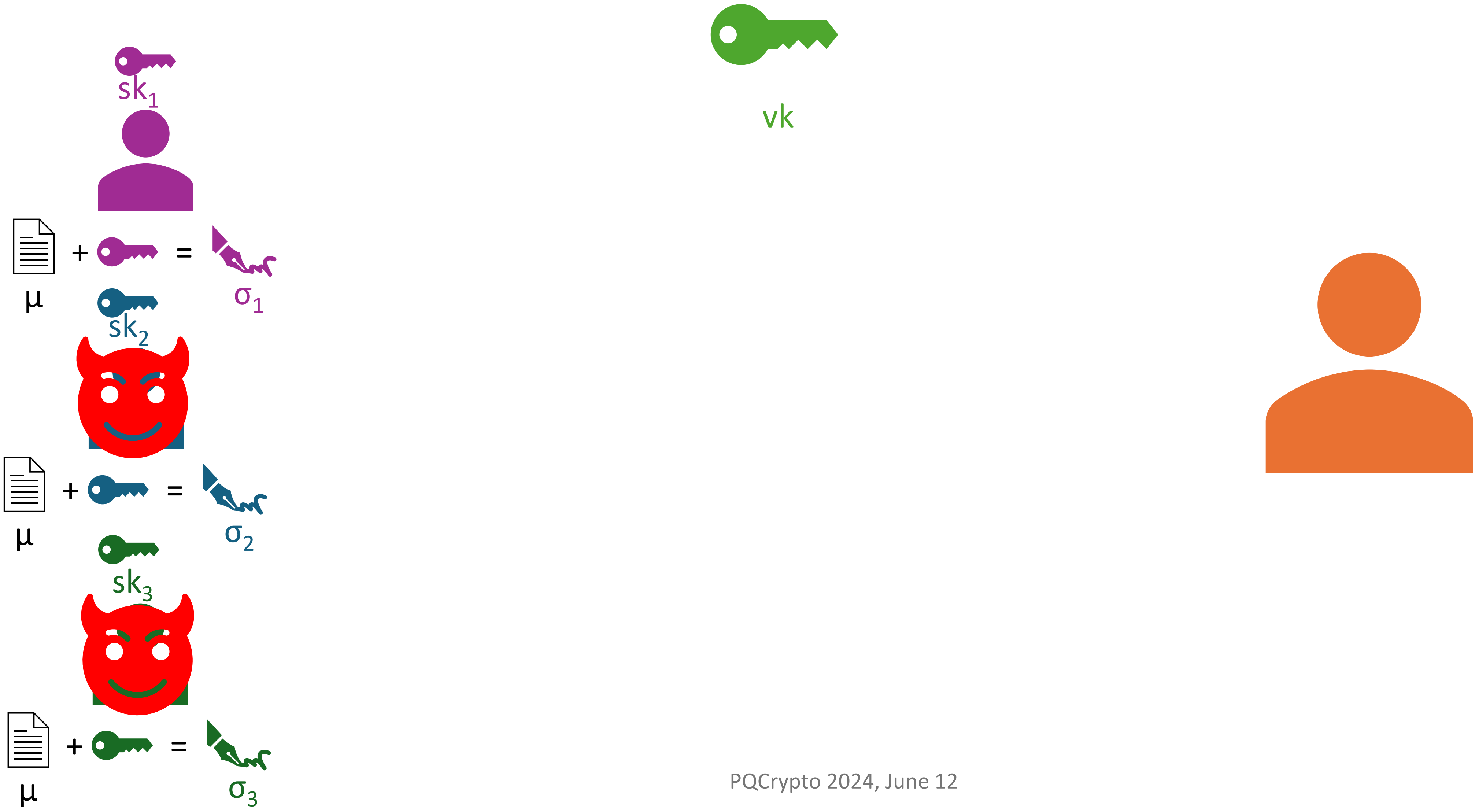


Overview: Digital Signatures

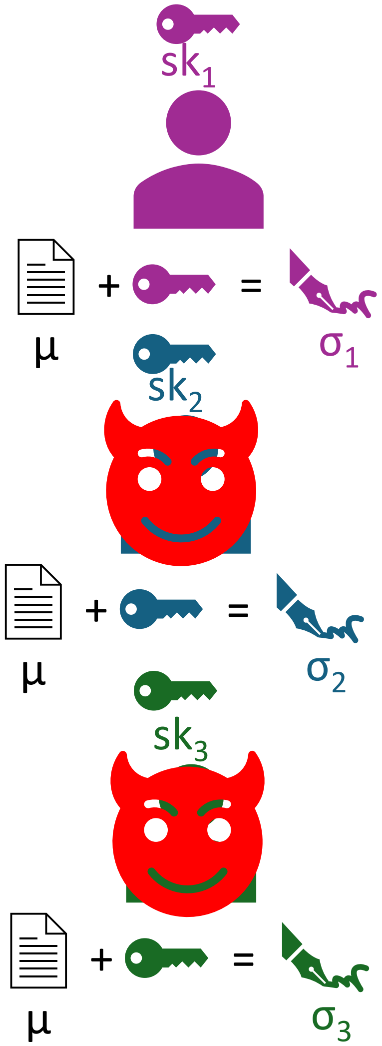
Overview: Threshold Signatures



Overview: Threshold Signatures

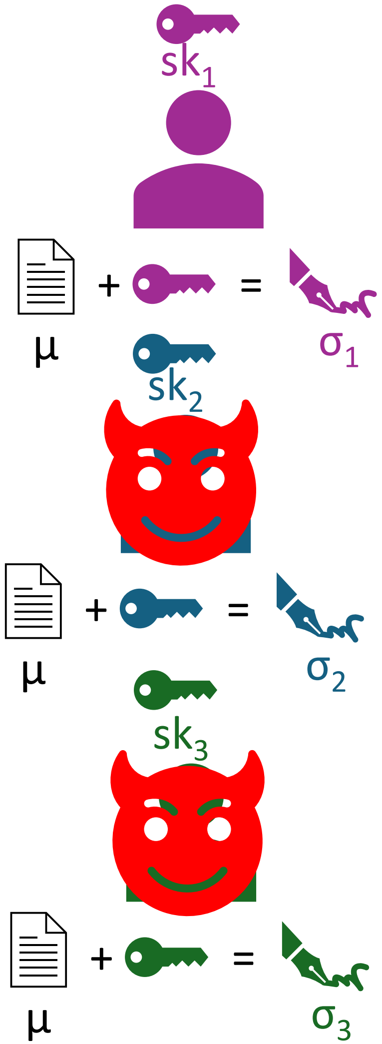


Overview: Threshold Signatures



Threshold Unforgeability: No subset of ≤t-1 corrupted can find fresh that verifies

Overview: Threshold Signatures



Threshold Unforgeability: No subset of ≤t-1 corrupted can find fresh that verifies

Passive or **Active**

Motivation

Motivation

- Allows advanced functionality

Motivation

- Allows advanced functionality
  - Cryptocurrency transactions, contract signing, secure authentication

Motivation

- Allows advanced functionality
  - Cryptocurrency transactions, contract signing, secure authentication
  - NIST standardization intentions

Motivation

- Allows advanced functionality
  - Cryptocurrency transactions, contract signing, secure authentication
  - NIST standardization intentions
- Studied extensively in the classical setting

Motivation

- Allows advanced functionality
  - Cryptocurrency transactions, contract signing, secure authentication
  - NIST standardization intentions
- Studied extensively in the classical setting
  - Schnorr [KG20, Lin24, CGRS23], ECDSA [CGG+20,CCL+20,DJN+20]

Motivation

- Allows advanced functionality
  - Cryptocurrency transactions, contract signing, secure authentication
  - NIST standardization intentions
- Studied extensively in the classical setting
  - Schnorr [KG20, Lin24, CGRS23], ECDSA [CGG+20,CCL+20,DJN+20]
- What about PQ?

Motivation

- Allows advanced functionality
  - Cryptocurrency transactions, contract signing, secure authentication
  - NIST standardization intentions
- Studied extensively in the classical setting
  - Schnorr [KG20, Lin24, CGRS23], ECDSA [CGG+20,CCL+20,DJN+20]
- What about PQ?
  - Non-linear/non-trivial operations

Motivation

- Allows advanced functionality
  - Cryptocurrency transactions, contract signing, secure authentication
  - NIST standardization intentions
- Studied extensively in the classical setting
  - Schnorr [KG20, Lin24, CGRS23], ECDSA [CGG+20,CCL+20,DJN+20]
- What about PQ?
  - Non-linear/non-trivial operations
  - Black-box FHE/MPC based solutions [ASY22,BGG+18,CS19]

Simple Lattice Signature Scheme

Simple Lattice Signature Scheme

$vk = (\bar{\boldsymbol{A}}, \boldsymbol{y})\ (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

Simple Lattice Signature Scheme

$vk \ = \ (\bar{\boldsymbol{A}}, \boldsymbol{y}) \ (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, \left|\left|\boldsymbol{s}\right|\right|_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r} \leftarrow R_{\mathrm{q}}^{\ell}, \left|\left|\boldsymbol{r}\right|\right|_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

Simple Lattice Signature Scheme

$vk \; = \; (\bar{\boldsymbol{A}}, \boldsymbol{y}) \; (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r} \leftarrow R_{\mathrm{q}}^{\ell}, ||\boldsymbol{r}||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$

Simple Lattice Signature Scheme

$vk \; = \; (\bar{\boldsymbol{A}}, \boldsymbol{y}) \; (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r} \leftarrow R_{\mathrm{q}}^{\ell}, ||\boldsymbol{r}||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$

$c = H(\boldsymbol{w}, \mu)$

Simple Lattice Signature Scheme

$vk \;=\; (\bar{\boldsymbol{A}}, \boldsymbol{y})\; (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r} \leftarrow R_{\mathrm{q}}^{\ell}, ||\boldsymbol{r}||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$
$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$
$c = H(\boldsymbol{w}, \mu)$
$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

Simple Lattice Signature Scheme

$vk = (\bar{\boldsymbol{A}}, \boldsymbol{y})\ (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\mu, \sigma = (c, \boldsymbol{z})$

$\boldsymbol{r} \leftarrow R_q^\ell, ||\boldsymbol{r}||_\infty \leq B_{\boldsymbol{r}}$
$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$
$c = H(\boldsymbol{w}, \mu)$
$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

Simple Lattice Signature Scheme

$vk = (\bar{\boldsymbol{A}}, \boldsymbol{y})\ (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\mu, \sigma = (c, \boldsymbol{z})$ →

$\boldsymbol{r} \leftarrow R_q^{\ell}, ||\boldsymbol{r}||_\infty \leq B_{\boldsymbol{r}}$
$\boldsymbol{w} = \bar{A}\boldsymbol{r}$
$c = H(\boldsymbol{w}, \mu)$
$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}}?$

Simple Lattice Signature Scheme

$vk = (\bar{\boldsymbol{A}}, \boldsymbol{y})\ (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\mu, \sigma = (c, \boldsymbol{z})$

$\boldsymbol{r} \leftarrow R_{\mathrm{q}}^{\ell}, ||\boldsymbol{r}||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$

$c = H(\boldsymbol{w}, \mu)$

$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}}?$

$\boldsymbol{w}^* = \bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}$

Simple Lattice Signature Scheme

$vk = (\overline{\boldsymbol{A}}, \boldsymbol{y})\ (\boldsymbol{y} = \overline{\boldsymbol{A}}\boldsymbol{s}, \overline{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\mu, \sigma = (c, \boldsymbol{z})$ →

$\boldsymbol{r} \leftarrow R_q^\ell, ||\boldsymbol{r}||_\infty \leq B_{\boldsymbol{r}}$
$\boldsymbol{w} = \overline{\boldsymbol{A}}\boldsymbol{r}$
$c = H(\boldsymbol{w}, \mu)$
$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}}$?
$\boldsymbol{w}^* = \overline{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}$
$c = H(\boldsymbol{w}^*, \mu)$?

Simple Lattice Signature Scheme

$vk \; = \; (\bar{\boldsymbol{A}}, \boldsymbol{y}) \; (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\mu, \sigma = (c, \boldsymbol{z})$

$\boldsymbol{r} \leftarrow R_q^\ell, ||\boldsymbol{r}||_\infty \leq B_{\boldsymbol{r}}$
$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$
$c = H(\boldsymbol{w}, \mu)$
$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}}?$
$\boldsymbol{w}^* = \bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}$
$c = H(\boldsymbol{w}^*, \mu)?$

Simple Lattice Signature Scheme

$vk = (\bar{\boldsymbol{A}}, \boldsymbol{y})\ (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\mu, \sigma = (c, \boldsymbol{z})$

$\boldsymbol{r} \leftarrow R_q^\ell, ||\boldsymbol{r}||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$

$c = H(\boldsymbol{w}, \mu)$

$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}}?$

$\boldsymbol{w}^* = \bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}$

$c = H(\boldsymbol{w}^*, \mu)?$

Simple Lattice Signature Scheme

$vk = (\bar{\boldsymbol{A}}, \boldsymbol{y})\ (\boldsymbol{y} = \bar{\boldsymbol{A}}\boldsymbol{s}, \bar{\boldsymbol{A}} = [\boldsymbol{A}|\boldsymbol{I}], \boldsymbol{A} \leftarrow R_q^{\ell \times k})$

$sk = \boldsymbol{s} \leftarrow R_q^k, ||\boldsymbol{s}||_\infty \leq B_{\boldsymbol{s}}$

$\mu, \sigma = (c, \boldsymbol{z})$

“rejection sampling”

$\boldsymbol{r} \leftarrow R_q^\ell, ||\boldsymbol{r}||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w} = \bar{\boldsymbol{A}}\boldsymbol{r}$

$c = H(\boldsymbol{w}, \mu)$

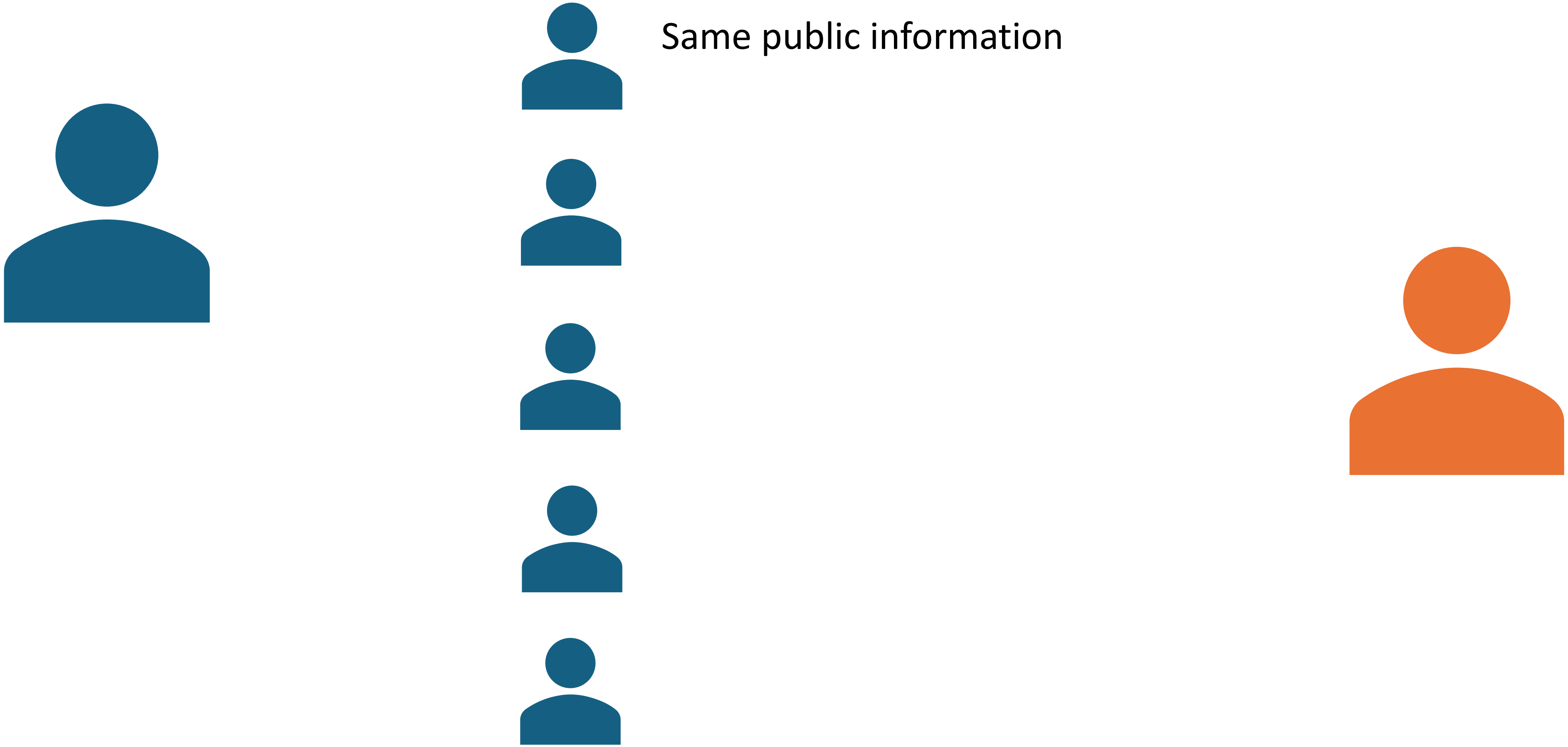
$\boldsymbol{z} = c\boldsymbol{s} + \boldsymbol{r}$

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}}$?

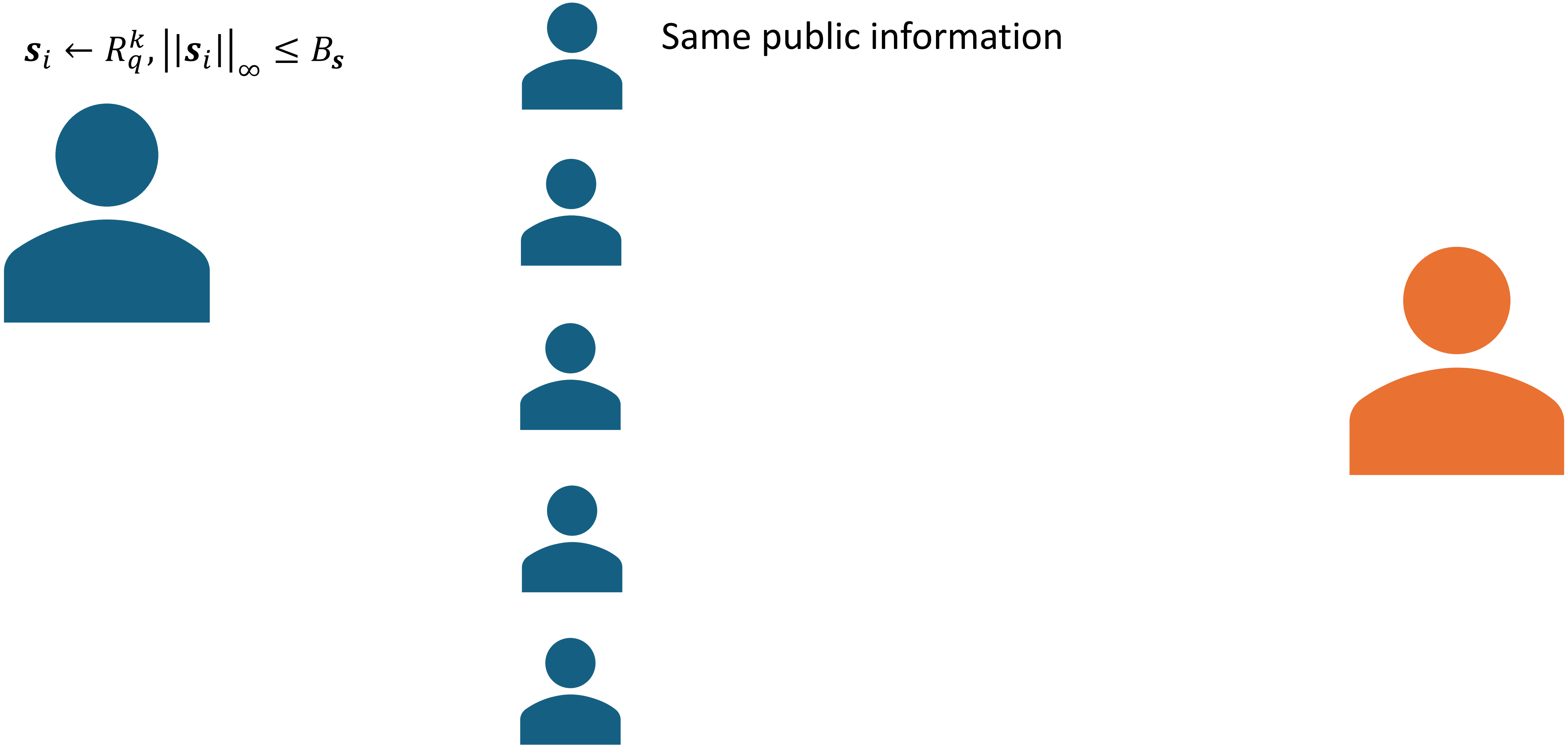
$\boldsymbol{w}^* = \bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}$

$c = H(\boldsymbol{w}^*, \mu)$?

Naïve n-out-of-n Construction



Naïve n-out-of-n Construction



Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

Same public information

Naïve n-out-of-n Construction

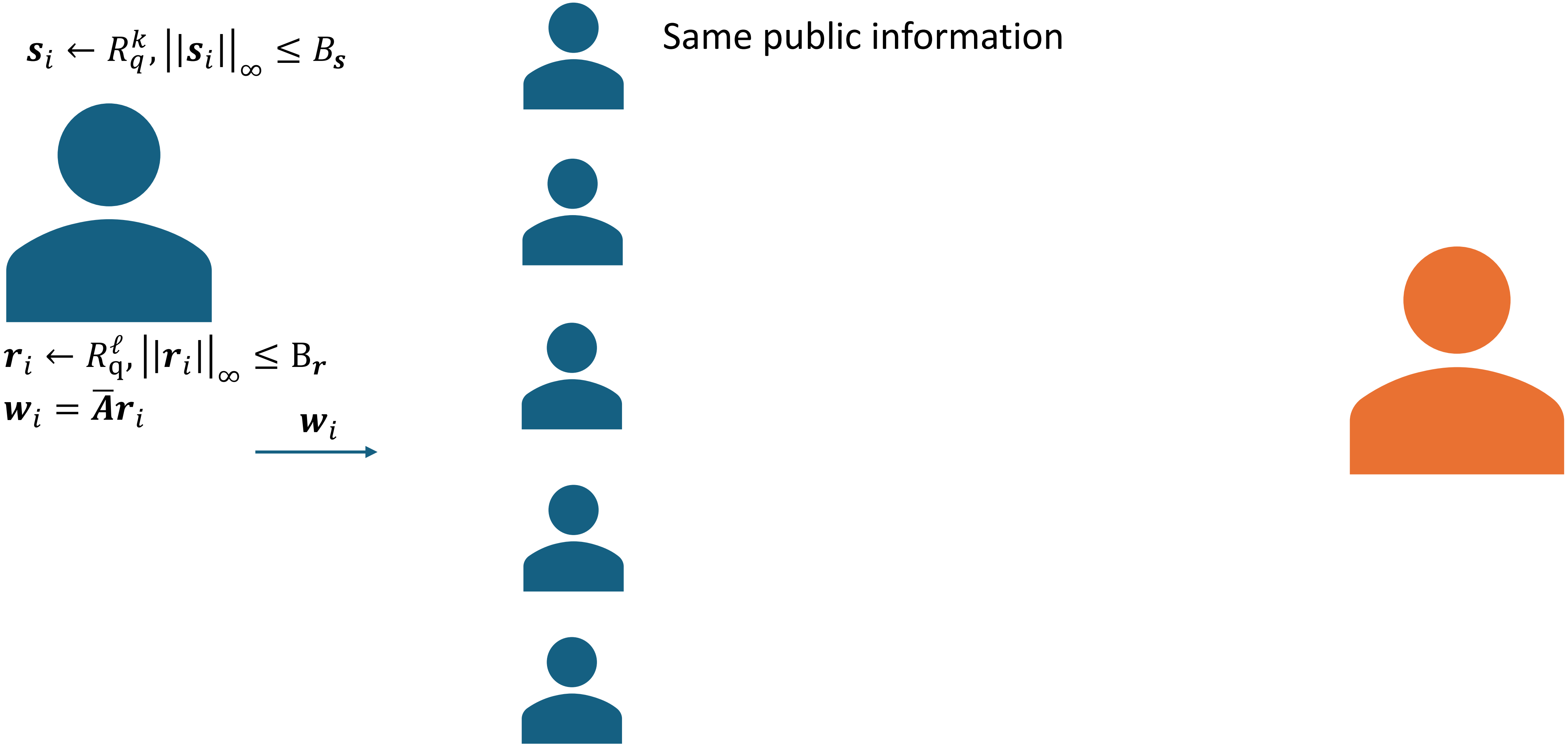
$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

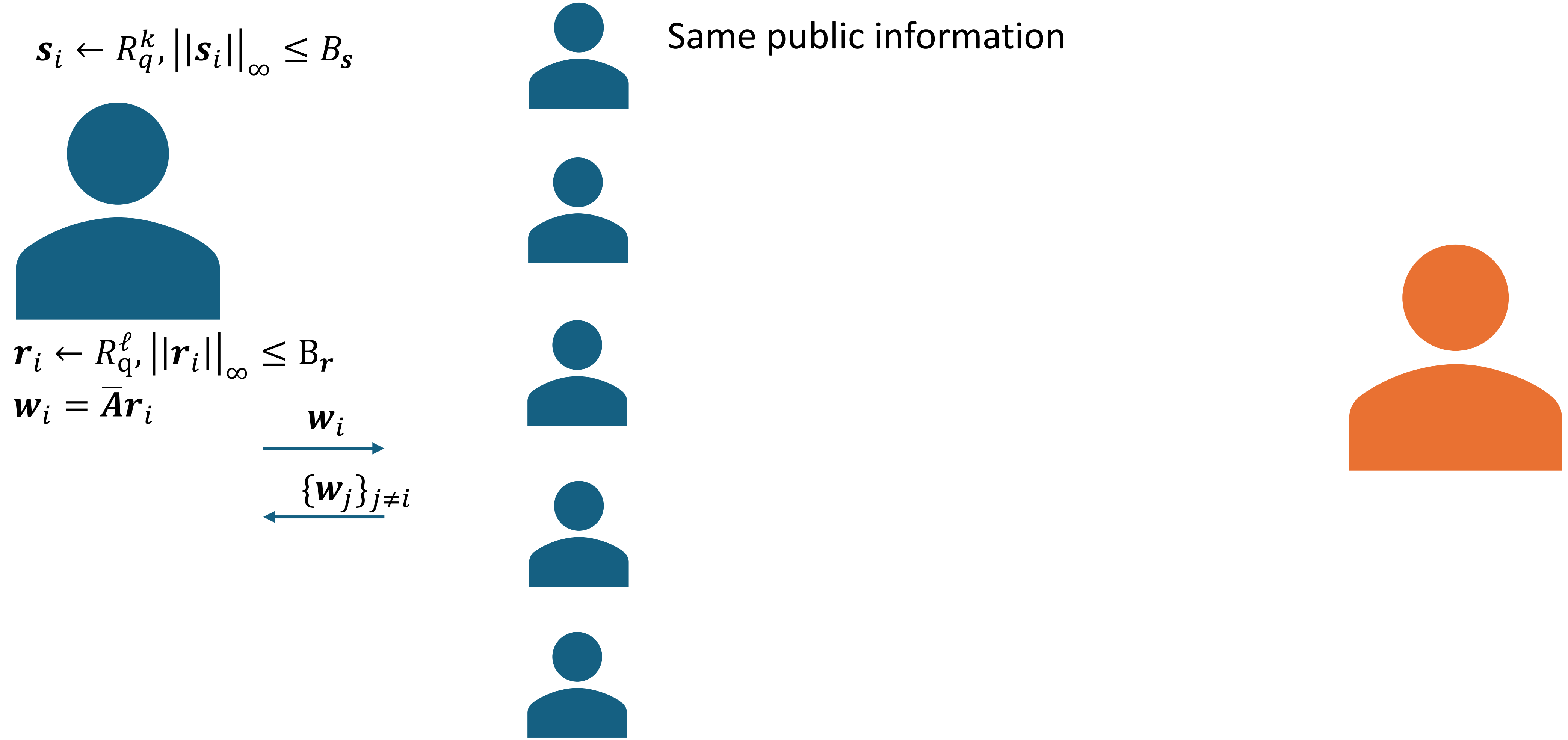
$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

Same public information

Naïve n-out-of-n Construction



Naïve n-out-of-n Construction



Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

$c = H(\sum \boldsymbol{w}_i, \mu)$

Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

$c = H(\sum \boldsymbol{w}_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

Same public information

Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

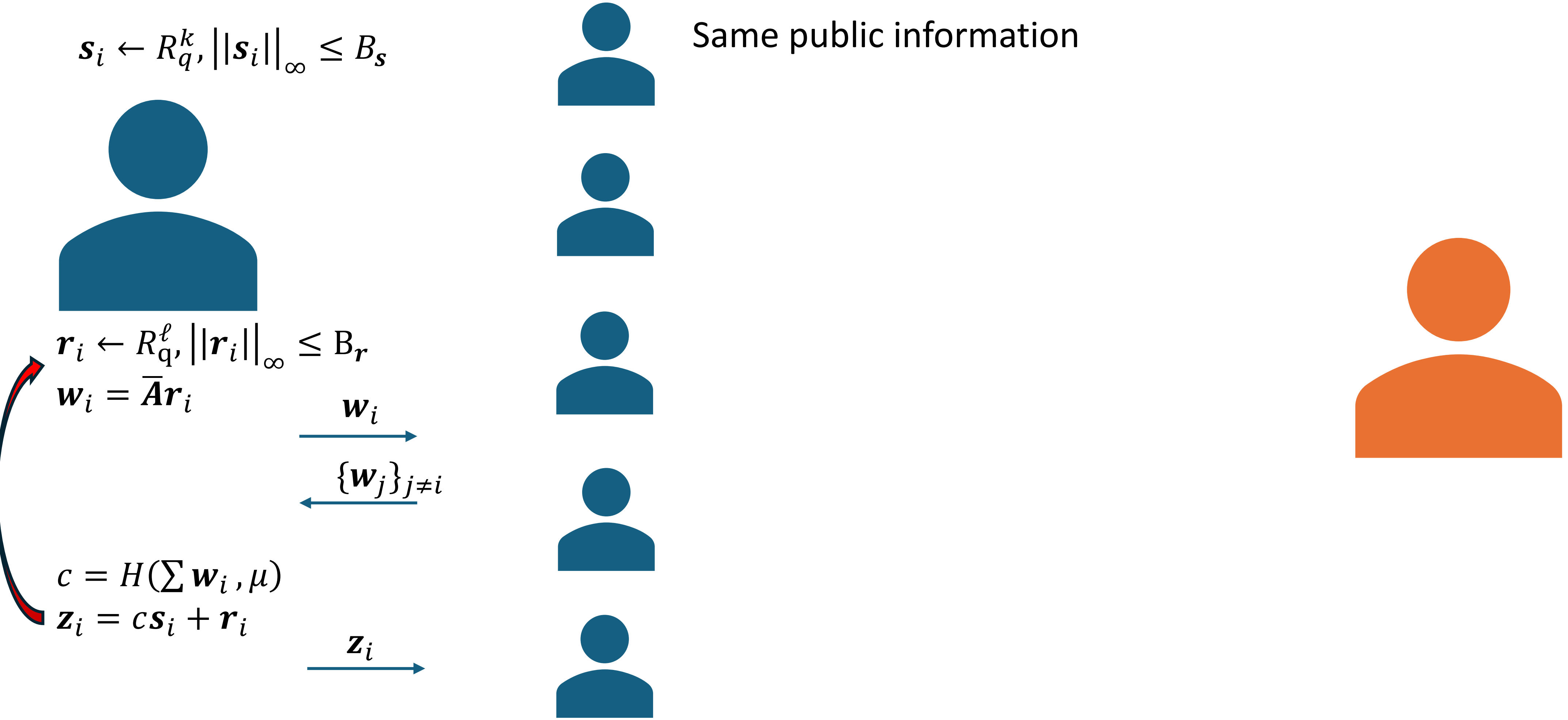
$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

$c = H(\sum \boldsymbol{w}_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

Naïve n-out-of-n Construction



Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

$c = H(\sum \boldsymbol{w}_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i$ →

← $\{\boldsymbol{z}_j\}_{j \neq i}$

Same public information

Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

$c = H(\sum \boldsymbol{w}_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i$ →

← $\{\boldsymbol{z}_j\}_{j \neq i}$

$\boldsymbol{z} = \sum \boldsymbol{z}_i$

Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

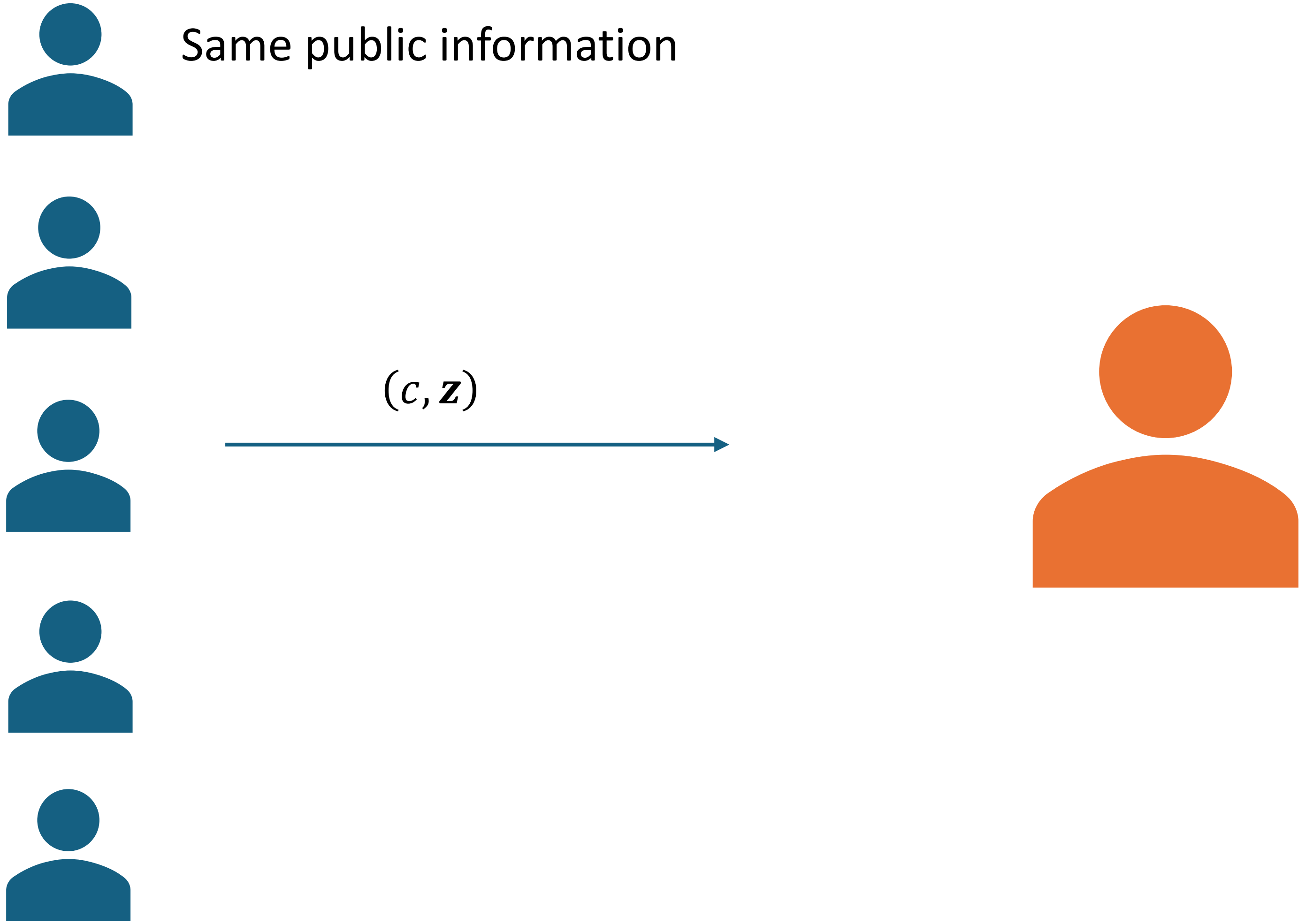
$c = H(\sum \boldsymbol{w}_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i$ →

← $\{\boldsymbol{z}_j\}_{j \neq i}$

$\boldsymbol{z} = \sum \boldsymbol{z}_i$



Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information

$\boldsymbol{r}_i \leftarrow R_{\mathrm{q}}^{\ell}, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

$(c, \boldsymbol{z})$ →

$c = H(\sum \boldsymbol{w}_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

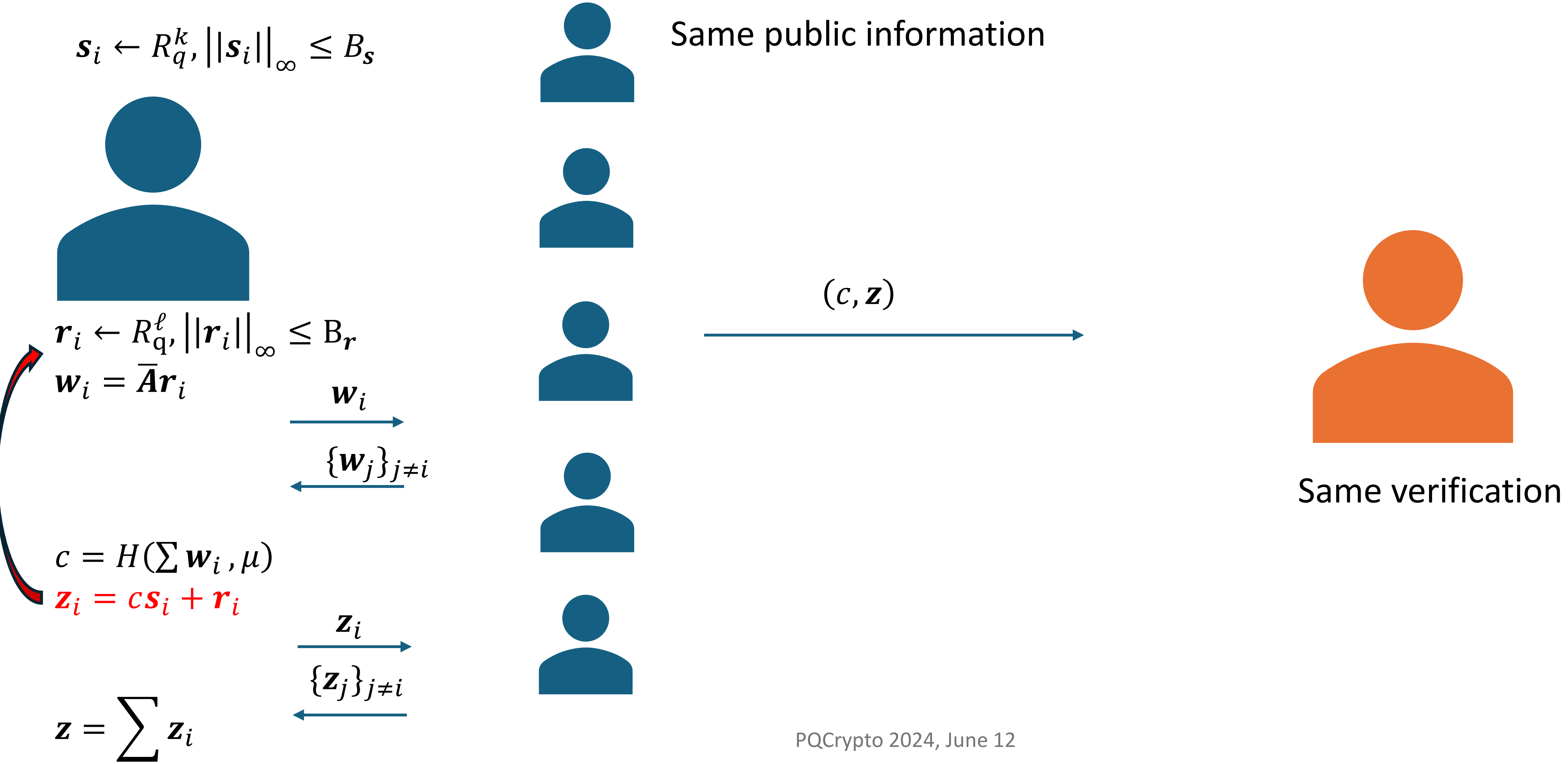
$\boldsymbol{z}_i$ →

← $\{\boldsymbol{z}_j\}_{j \neq i}$

$\boldsymbol{z} = \sum \boldsymbol{z}_i$

Same verification

Naïve n-out-of-n Construction



Naïve n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \le B_{\boldsymbol{s}}$

Same public information

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \le B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$

$\boldsymbol{w}_i$ →

← $\{\boldsymbol{w}_j\}_{j \neq i}$

$(c, \boldsymbol{z})$ →

$c = H(\sum \boldsymbol{w}_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

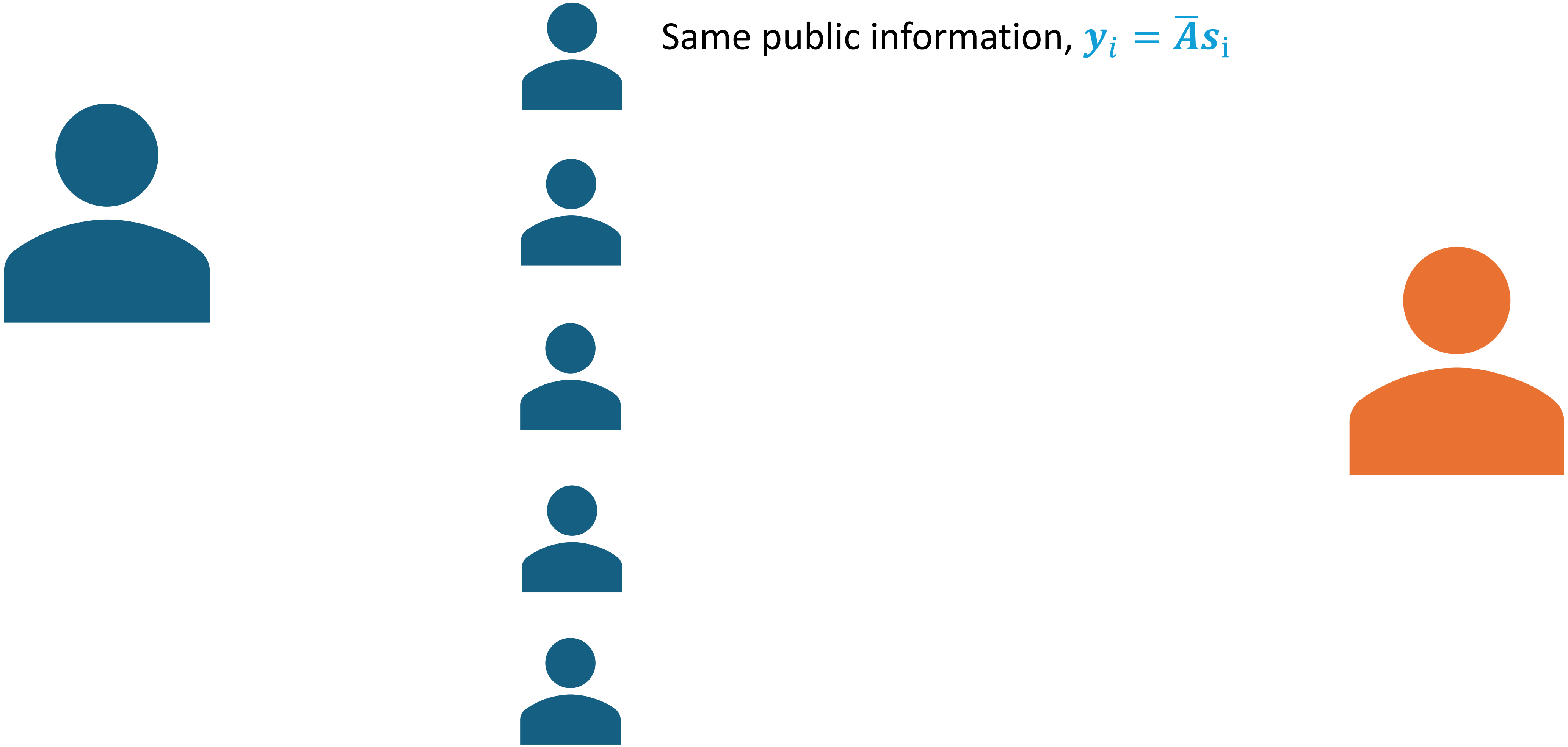
$\boldsymbol{z}_i$ →

← $\{\boldsymbol{z}_j\}_{j \neq i}$

$\boldsymbol{z} = \sum \boldsymbol{z}_i$

Same verification

[DOTT21] n-out-of-n Construction

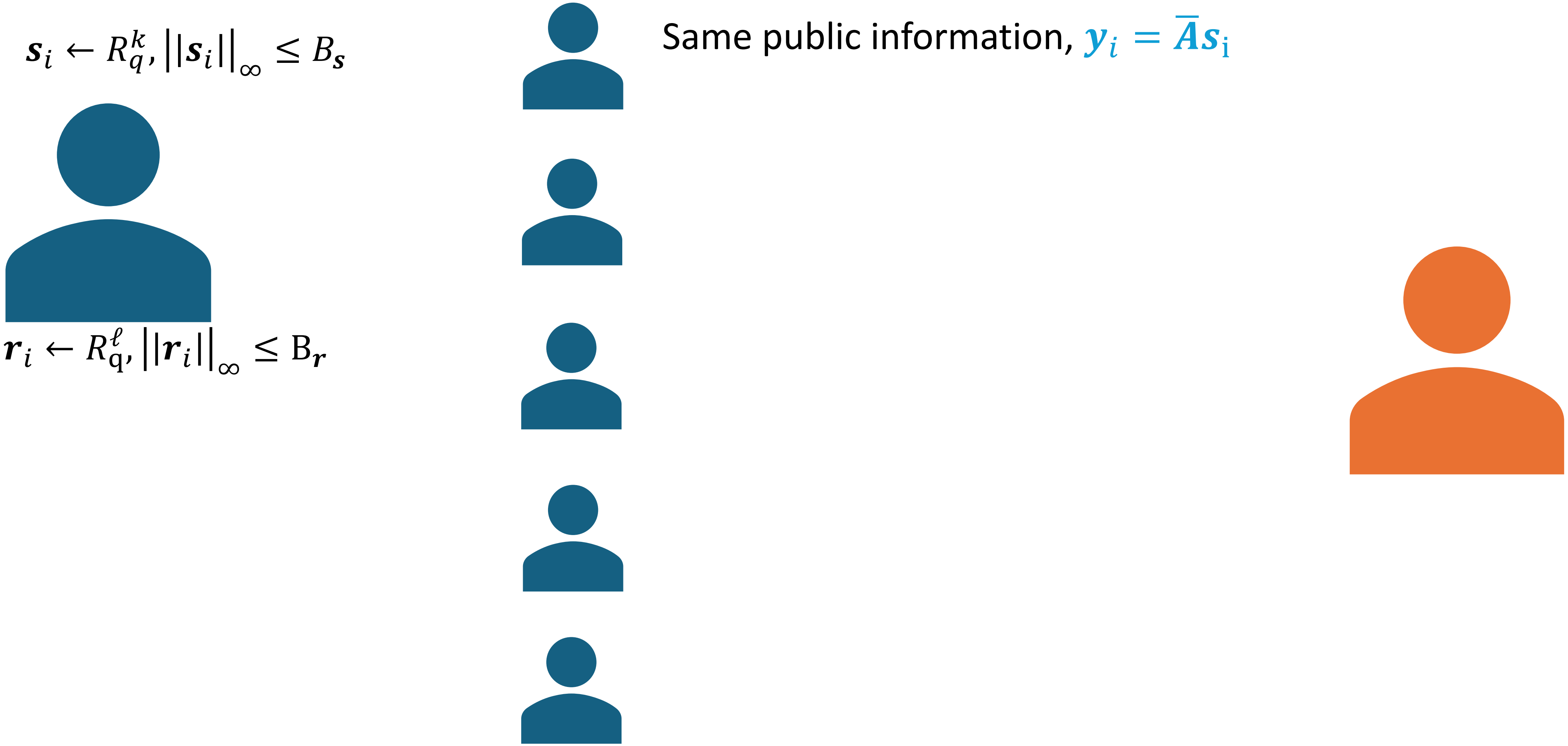


[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

[DOTT21] n-out-of-n Construction



[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_{\mathrm{i}}$

$\boldsymbol{r}_i \leftarrow R_{\mathrm{q}}^{\ell}, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

$\boldsymbol{r}_i \leftarrow R_\mathrm{q}^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_{\mathrm{i}}$

$\boldsymbol{r}_i \leftarrow R_{\mathrm{q}}^{\ell}, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_i$

[DOTT21] n-out-of-n Construction

$s_i \leftarrow R_q^k, ||s_i||_\infty \le B_s$

Same public information, $y_i = \bar{A}s_i$

$r_i \leftarrow R_q^\ell, ||r_i||_\infty \le B_r$

$w_i = \bar{A}r_i$, $ck = H(y, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(w_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

[DOTT21] n-out-of-n Construction

$s_i \leftarrow R_q^k, ||s_i||_\infty \leq B_s$

Same public information, $y_i = \bar{A}s_i$

$r_i \leftarrow R_q^\ell, ||r_i||_\infty \leq B_r$

$w_i = \bar{A}r_i$, $ck = H(y, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(w_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$z_i = cs_i + r_i$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_i$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i

$\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

$\boldsymbol{r}_i \leftarrow R_\mathrm{q}^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i, ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_i$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

$\{com_j\}_{j \neq i}$ ←

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

$\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$ ←

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_i$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

$\{com_j\}_{j \neq i}$ ←

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

$\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$ ←

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j ; \rho_j)$?

[DOTT21] n-out-of-n Construction

$s_i \leftarrow R_q^k, ||s_i||_\infty \leq B_s$

Same public information, $y_i = \bar{A}s_i$

$r_i \leftarrow R_q^\ell, ||r_i||_\infty \leq B_r$

$w_i = \bar{A}r_i$, $ck = H(y, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(w_i; \rho_i)$

com_i

$\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$z_i = cs_i + r_i$

z_i, ρ_i

$\{z_j, \rho_j\}_{j \neq i}$

$com_j = Com_{ck}(\bar{A}z_j - cy_j; \rho_j)$?

$z = \sum z_i$, $\rho = \sum \rho_i$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

$(c, \boldsymbol{z}, \rho)$

$\boldsymbol{r}_i \leftarrow R_\mathrm{q}^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i

$\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$

$\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j ; \rho_j)$?

$\boldsymbol{z} = \sum \boldsymbol{z}_i$, $\rho = \sum \rho_i$

[DOTT21] n-out-of-n Construction

$s_i \leftarrow R_q^k, ||s_i||_\infty \leq B_s$

Same public information, $y_i = \bar{A}s_i$

$r_i \leftarrow R_q^\ell, ||r_i||_\infty \leq B_r$

$w_i = \bar{A}r_i$, $ck = H(y, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(w_i; \rho_i)$

com_i →

$\{com_j\}_{j \neq i}$ ←

$c = H(\sum com_i, \mu)$

$z_i = cs_i + r_i$

z_i, ρ_i →

$\{z_j, \rho_j\}_{j \neq i}$ ←

$com_j = Com_{ck}(\bar{A}z_j - cy_j ; \rho_j)?$

$z = \sum z_i$, $\rho = \sum \rho_i$

(c, z, ρ) →

$||z||_\infty \leq B_{z'}?$

[DOTT21] n-out-of-n Construction

$s_i \leftarrow R_q^k, ||s_i||_\infty \leq B_s$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

$\boldsymbol{r}_i \leftarrow R_\mathrm{q}^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

$(c, \boldsymbol{z}, \rho)$

com_i

$\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$

$\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$

$||\boldsymbol{z}||_\infty \leq B_{z'}$?

$ck = H(\boldsymbol{y}, \mu)$

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j ; \rho_j)$?

$\boldsymbol{z} = \sum \boldsymbol{z}_i$, $\rho = \sum \rho_i$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

$\boldsymbol{r}_i \leftarrow R_\mathrm{q}^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

$c = H(\sum com_i , \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

← $\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j ; \rho_j)$?

$\boldsymbol{z} = \sum \boldsymbol{z}_i$, $\rho = \sum \rho_i$

$(c, \boldsymbol{z}, \rho)$ →

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}'}$?

$ck = H(\boldsymbol{y}, \mu)$

$com^* = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}; \rho)$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_i$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

$\{com_j\}_{j \neq i}$ ←

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

$\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$ ←

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j ; \rho_j)$?

$\boldsymbol{z} = \sum \boldsymbol{z}_i$, $\rho = \sum \rho_i$

$(c, \boldsymbol{z}, \rho)$ →

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}'}$?

$ck = H(\boldsymbol{y}, \mu)$

$com^* = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}; \rho)$

$c = H(com^*, \mu)$?

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

$\boldsymbol{r}_i \leftarrow R_\mathrm{q}^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i, ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

← $\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j; \rho_j)$?

$\boldsymbol{z} = \sum \boldsymbol{z}_i, \rho = \sum \rho_i$

$(c, \boldsymbol{z}, \rho)$ →

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}'}$?

$ck = H(\boldsymbol{y}, \mu)$

$com^* = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}; \rho)$

$c = H(com^*, \mu)$?

What happens when you have an arbitrary threshold?

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_i$

$\boldsymbol{r}_i \leftarrow R_q^\ell, ||\boldsymbol{r}_i||_\infty \leq B_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i, ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

← $\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j; \rho_j)$?

$\boldsymbol{z} = \sum \boldsymbol{z}_i, \rho = \sum \rho_i$

$(c, \boldsymbol{z}, \rho)$ →

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}'}$?

$ck = H(\boldsymbol{y}, \mu)$

$com^* = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}; \rho)$

$c = H(com^*, \mu)$?

What happens when you have an arbitrary threshold?

[DOTT21] n-out-of-n Construction

$s_i \leftarrow R_q^k, ||s_i||_\infty \leq B_s$

Same public information, $y_i = \bar{A}s_i$

$r_i \leftarrow R_q^\ell, ||r_i||_\infty \leq B_r$

$w_i = \bar{A}r_i$, $ck = H(y, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(w_i; \rho_i)$

com_i

$\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$z_i = cs_i + r_i$

z_i, ρ_i

$\{z_j, \rho_j\}_{j \neq i}$

$com_j = Com_{ck}(\bar{A}z_j - cy_j;\ \rho_j)?$

$z = \sum z_i$, $\rho = \sum \rho_i$

(c, z, ρ)

What happens when you have an arbitrary threshold?

$||z||_\infty \leq B_{z'}?$

$ck = H(y, \mu)$

$com^* = Com_{ck}(\bar{A}z - cy; \rho)$

$c = H(com^*, \mu)?$

[DOTT21] n-out-of-n Construction

$\boldsymbol{s}_i \leftarrow R_q^k, ||\boldsymbol{s}_i||_\infty \leq B_{\boldsymbol{s}}$

Same public information, $\boldsymbol{y}_i = \bar{\boldsymbol{A}}\boldsymbol{s}_\mathrm{i}$

$\boldsymbol{r}_i \leftarrow R_\mathrm{q}^\ell, ||\boldsymbol{r}_i||_\infty \leq \mathrm{B}_{\boldsymbol{r}}$

$\boldsymbol{w}_i = \bar{\boldsymbol{A}}\boldsymbol{r}_i$, $ck = H(\boldsymbol{y}, \mu)$

$\rho_i \leftarrow \{0,1\}^*, com_i = Com_{ck}(\boldsymbol{w}_i; \rho_i)$

com_i →

← $\{com_j\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$\boldsymbol{z}_i = c\boldsymbol{s}_i + \boldsymbol{r}_i$

$\boldsymbol{z}_i, \rho_i$ →

← $\{\boldsymbol{z}_j, \rho_j\}_{j \neq i}$

$com_j = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z}_j - c\boldsymbol{y}_j \,;\, \rho_j)$?

$\boldsymbol{z} = \sum \boldsymbol{z}_i$, $\rho = \sum \rho_i$

$(c, \boldsymbol{z}, \rho)$ →

What happens when you have an arbitrary threshold?

$||\boldsymbol{z}||_\infty \leq B_{\boldsymbol{z}'}$?

$ck = H(\boldsymbol{y}, \mu)$

$com^* = Com_{ck}(\bar{\boldsymbol{A}}\boldsymbol{z} - c\boldsymbol{y}; \rho)$

$c = H(com^*, \mu)$?

Is there an efficient lattice-based threshold signature scheme for arbitrary thresholds?

Starting Point: FHE as a Subprotocol

Starting Point: FHE as a Subprotocol

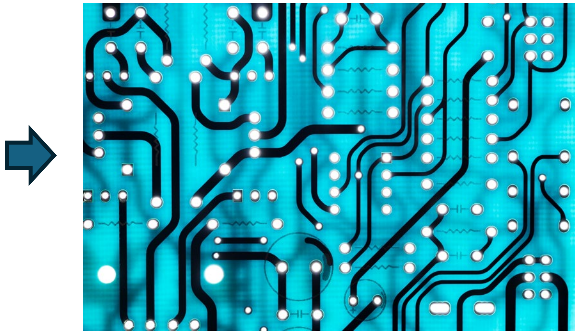
- [BGG+18] and the “universal thresholdizer”

Starting Point: FHE as a Subprotocol

- [BGG+18] and the “universal thresholdizer”

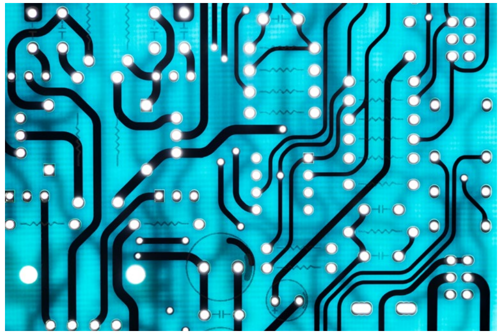
Starting Point: FHE as a Subprotocol

- [BGG+18] and the “universal thresholdizer”



Starting Point: FHE as a Subprotocol

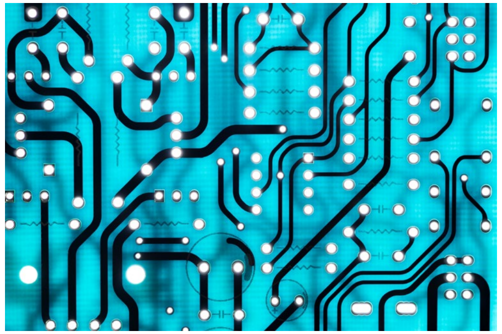
- [BGG+18] and the "universal thresholdizer"



"UT" :
Threshold FHE +
NIZK/Homomorphic
signatures

Starting Point: FHE as a Subprotocol

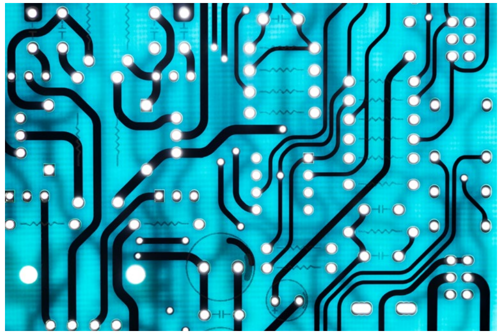
- [BGG+18] and the "universal thresholdizer"



"UT" :
Threshold FHE +
NIZK/Homomorphic
signatures

Starting Point: FHE as a Subprotocol

- [BGG+18] and the “universal thresholdizer”

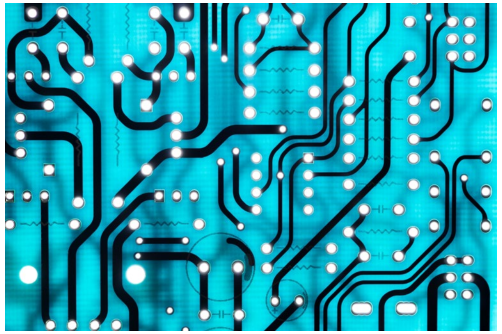


“UT” :
Threshold FHE +
NIZK/Homomorphic
signatures

- Can use the signature scheme as the circuit
    - Have to run challenge & rejection over ciphertexts!

Starting Point: FHE as a Subprotocol

- [BGG+18] and the “universal thresholdizer”



“UT” :
Threshold FHE +
NIZK/Homomorphic
signatures

- Can use the signature scheme as the circuit
  - Have to run challenge & rejection over ciphertexts!
- Can we salvage these ideas?

Our Idea: Threshold decryption of a signature

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an <u>encrypted</u> “signing key” like [DOTT21]

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an <u>encrypted</u> “signing key” like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an <u>encrypted</u> "signing key" like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys
- Signing:

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an <u>encrypted</u> “signing key” like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys
- Signing:
  - Start signature randomness like [DOTT21]

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an encrypted "signing key" like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys
- Signing:
  - Start signature randomness like [DOTT21]
  - Encrypted signature randomness, linearly computed encrypted signature

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an <u>encrypted</u> "signing key" like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys
- Signing:
  - Start signature randomness like [DOTT21]
  - <u>Encrypted</u> signature randomness, linearly computed <u>encrypted</u> signature
  - t-out-of-n decryptions for signature shares

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an encrypted "signing key" like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys
- Signing:
  - Start signature randomness like [DOTT21]
  - Encrypted signature randomness, linearly computed encrypted signature
  - t-out-of-n decryptions for signature shares
  - Final signature remains the same

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an encrypted “signing key” like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys
- Signing:
  - Start signature randomness like [DOTT21]
  - Encrypted signature randomness, linearly computed encrypted signature
  - t-out-of-n decryptions for signature shares
  - Final signature remains the same

No reason to run TFHE over the entire signature!

Our Idea: Threshold decryption of a signature

- Combine [BGG+18] and [DOTT21]
- Key Generation:
  - Generate an encrypted "signing key" like [DOTT21]
  - t-out-of-n shared decryption keys as signing keys
- Signing:
  - Start signature randomness like [DOTT21]
  - Encrypted signature randomness, linearly computed encrypted signature
  - t-out-of-n decryptions for signature shares
  - Final signature remains the same

No reason to run TFHE over the entire signature!

We can use the TFHE in [BGG+18] and be done right?

Problem: Threshold (F)HE is not trivial

Problem: Threshold (F)HE is not trivial

- Out-of-box TFHE does not have distributed key generation

Problem: Threshold (F)HE is not trivial

- Out-of-box TFHE does not have distributed key generation
- The security notion is not standard for our setting

Problem: Threshold (F)HE is not trivial

- Out-of-box TFHE does not have distributed key generation
- The security notion is not standard for our setting
- Shamir secret sharing impact norm bounds

Problem: Threshold (F)HE is not trivial

- Out-of-box TFHE does not have distributed key generation
- The security notion is not standard for our setting
- Shamir secret sharing impact norm bounds

Also overlooked rejection!

Organization

Organization

- Build a suitable threshold linearly HE

Organization

- Build a suitable threshold linearly HE
- Avoid rejection sampling

Organization

- Build a suitable threshold linearly HE
- Avoid rejection sampling
- Combine HE with rejection-free signature

Building Threshold HE

Building Threshold HE

- New notion of security: “indistinguishability”

Building Thresh

- New notion of secu

- Weaker than standard
- Adversary allowed to be in keygen, query for partial decryptions
- **Not allowed to query on challenge ciphertext!**

Building Threshold HE

- New notion of security: “indistinguishability”
- Use [BGV12] (F)HE as the base scheme

Building Threshold HE

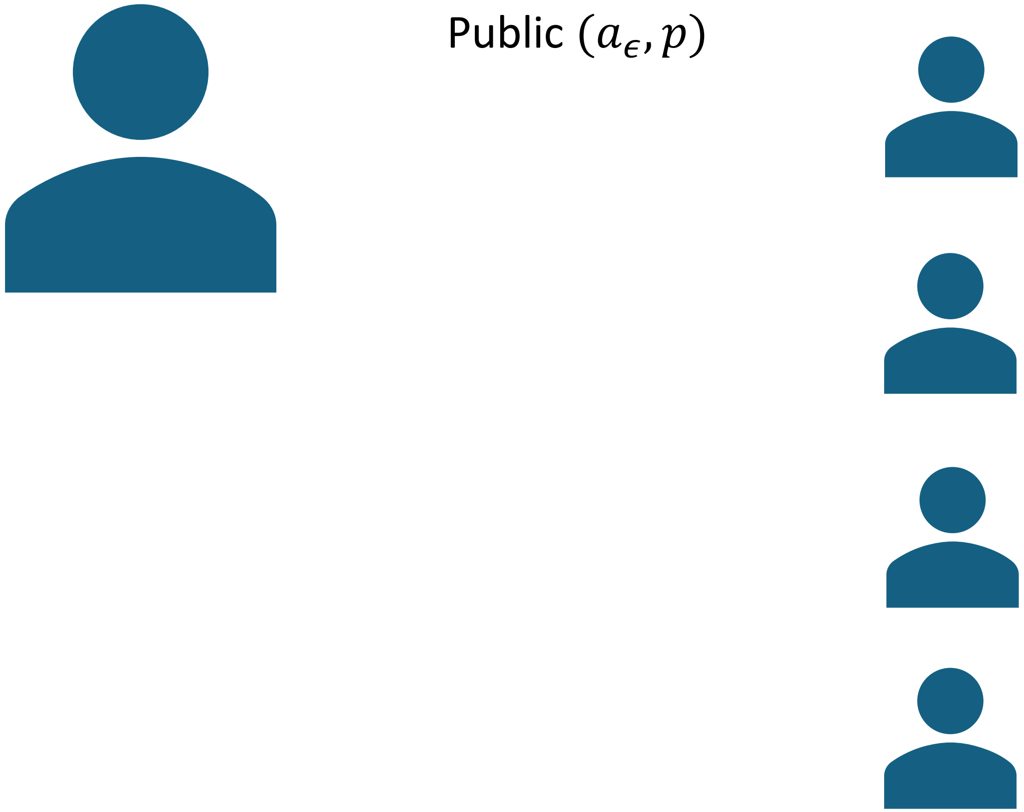
- New notion of security: “indistinguishability”
- Use [BGV12] (F)HE as the base scheme
- Do simple sharing based distributed key generation

Building Threshold HE

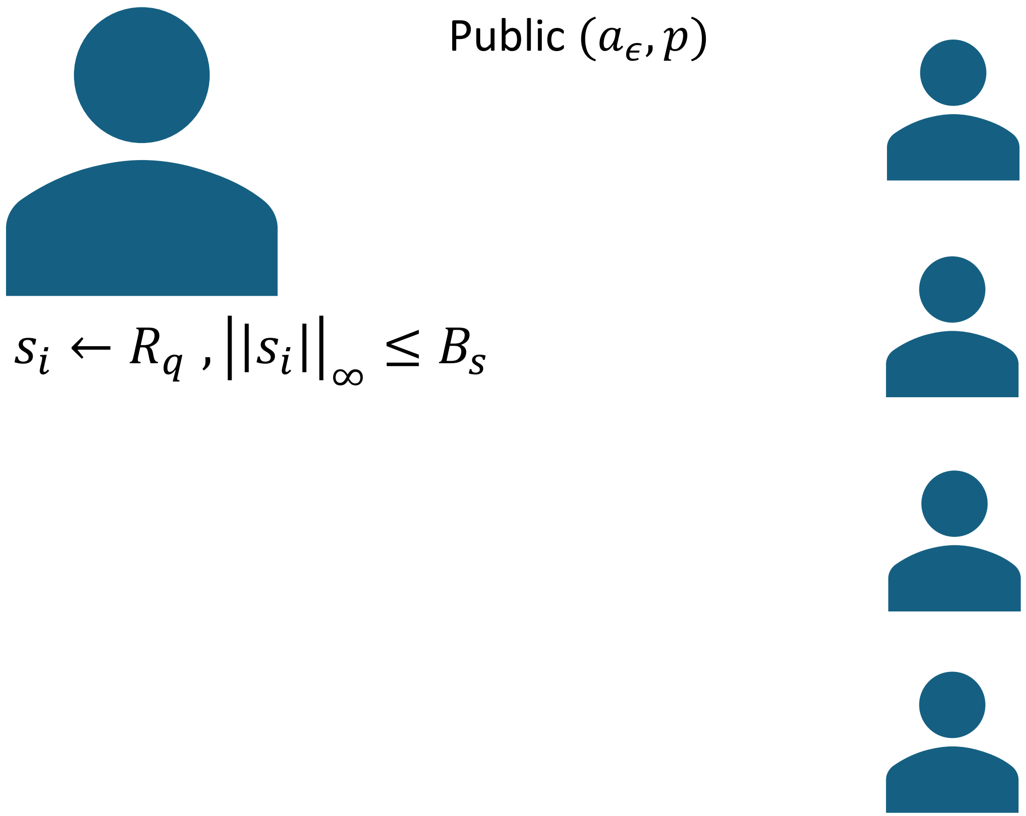
- New notion of security: “indistinguishability”
- Use [BGV12] (F)HE as the base scheme
- Do simple sharing based distributed key generation
- Use <u>noise flooding</u> for decryption/signature shares

Building Threshold HE: Key Generation

Building Threshold HE: Key Generation



Building Threshold HE: Key Generation

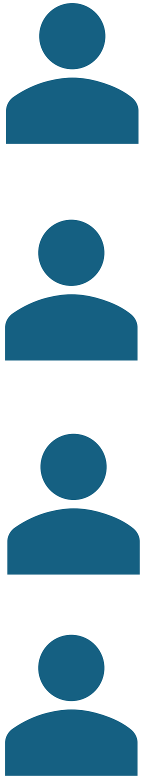


Building Threshold HE: Key Generation

Public (a_ϵ, p)

$s_i \leftarrow R_q\ , \left|\left|s_i\right|\right|_\infty \leq B_s$

$e_i \leftarrow D_e, b_i = a\ s_i + p\ e_i$



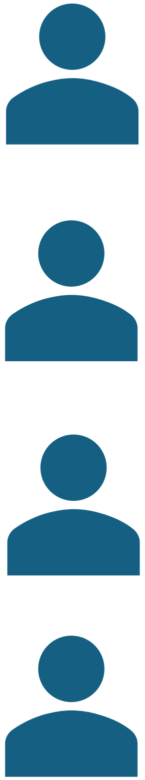
Building Threshold HE: Key Generation

$s_i \leftarrow R_q$, $||s_i||_\infty \leq B_s$

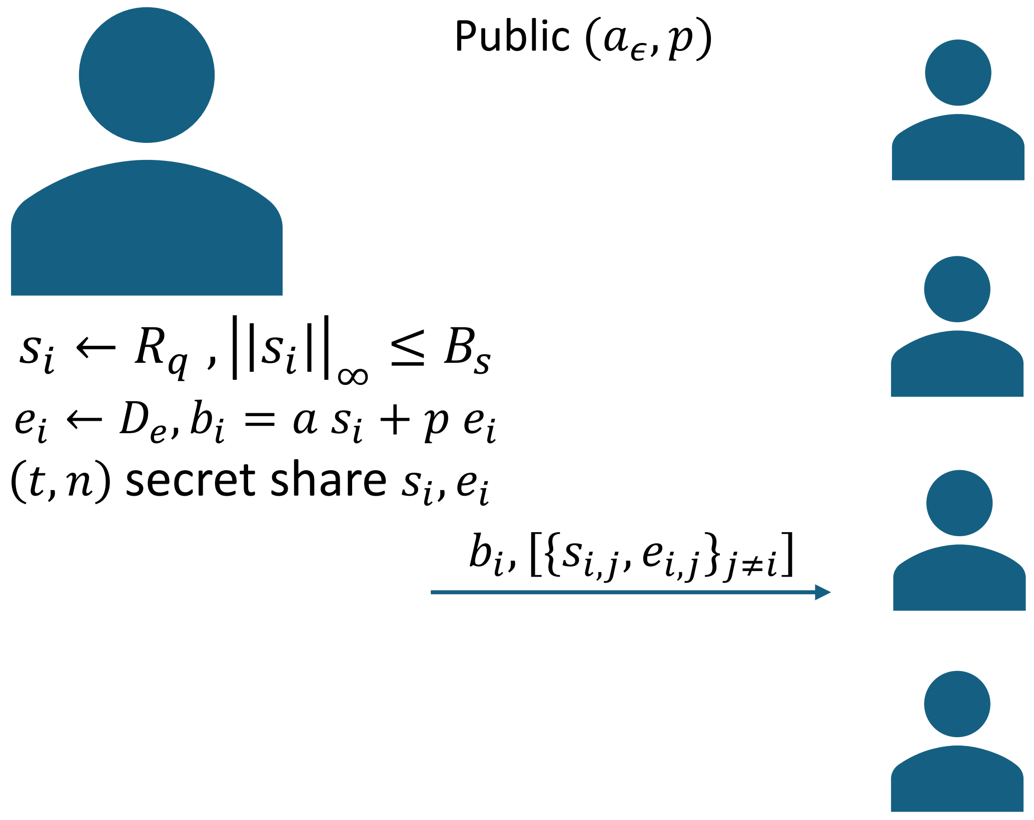
$e_i \leftarrow D_e, b_i = a\ s_i + p\ e_i$

(t, n) secret share s_i, e_i

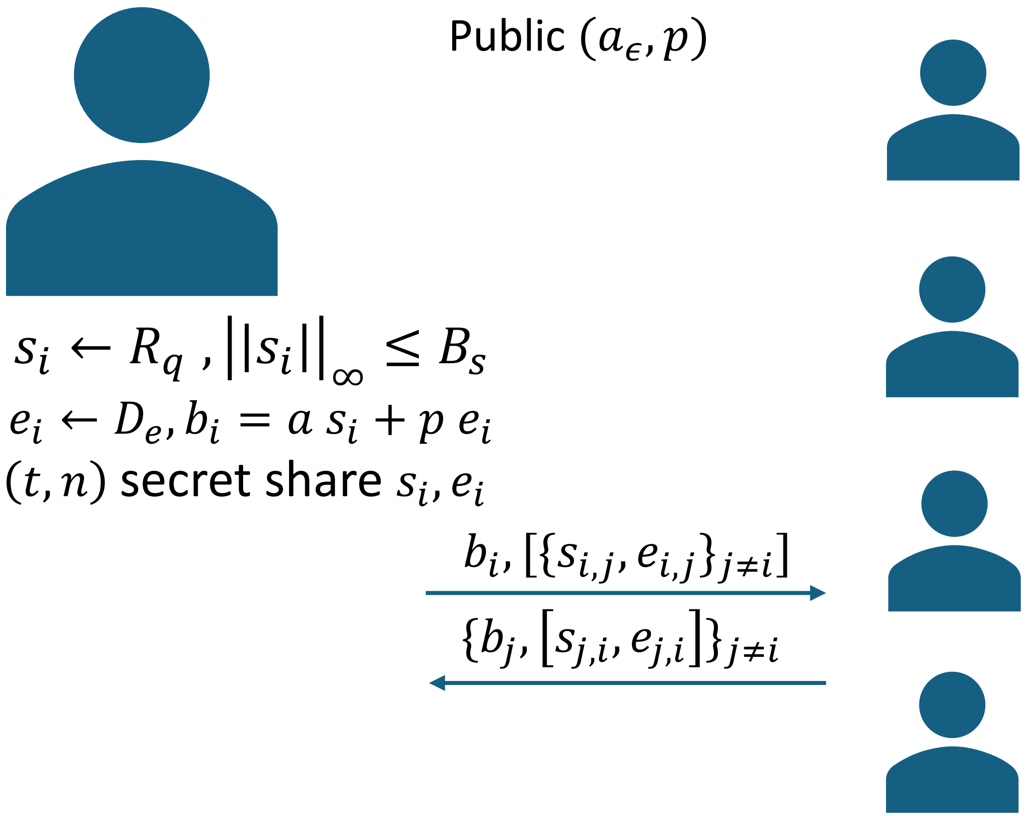
Public (a_ϵ, p)



Building Threshold HE: Key Generation



Building Threshold HE: Key Generation



Building Threshold HE: Key Generation

Public (a_ϵ, p)

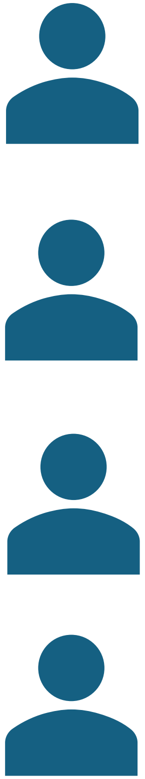
$s_i \leftarrow R_q \,, \left|\left|s_i\right|\right|_\infty \leq B_s$

$e_i \leftarrow D_e, b_i = a\, s_i + p\, e_i$

(t, n) secret share s_i, e_i

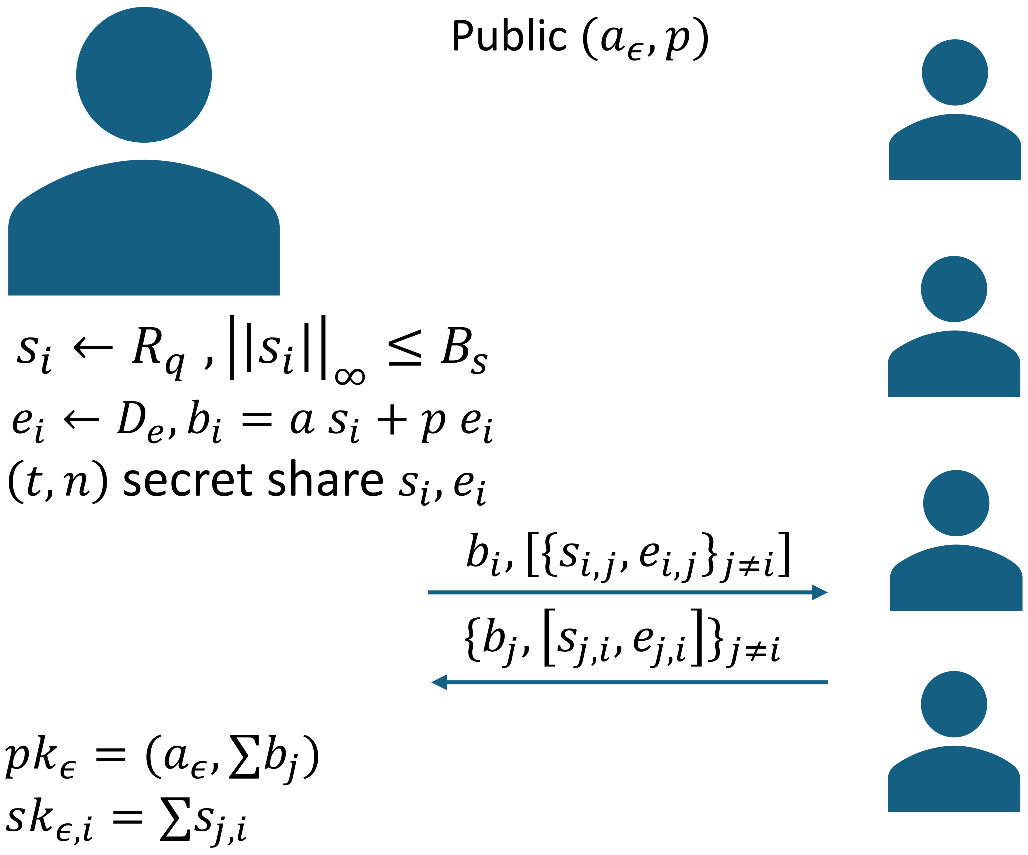
$b_i, [\{s_{i,j}, e_{i,j}\}_{j \neq i}]$ →

← $\{b_j, [s_{j,i}, e_{j,i}]\}_{j \neq i}$

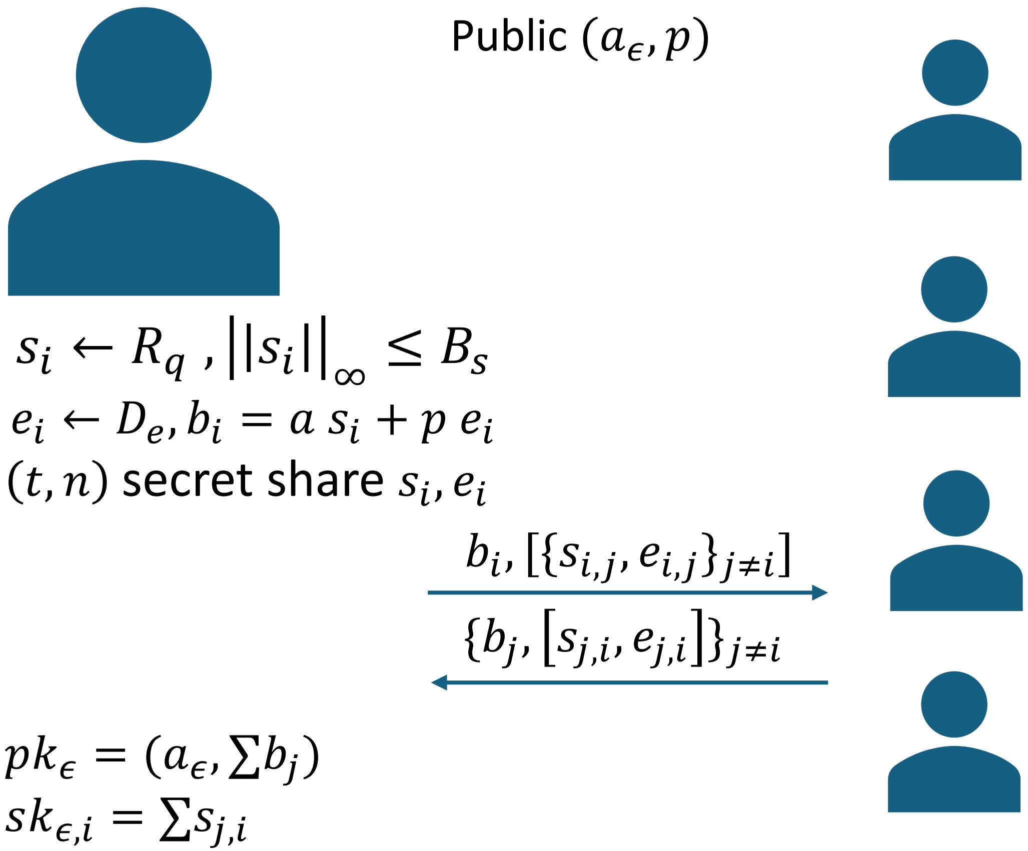


$pk_\epsilon = (a_\epsilon, \sum b_j)$

Building Threshold HE: Key Generation

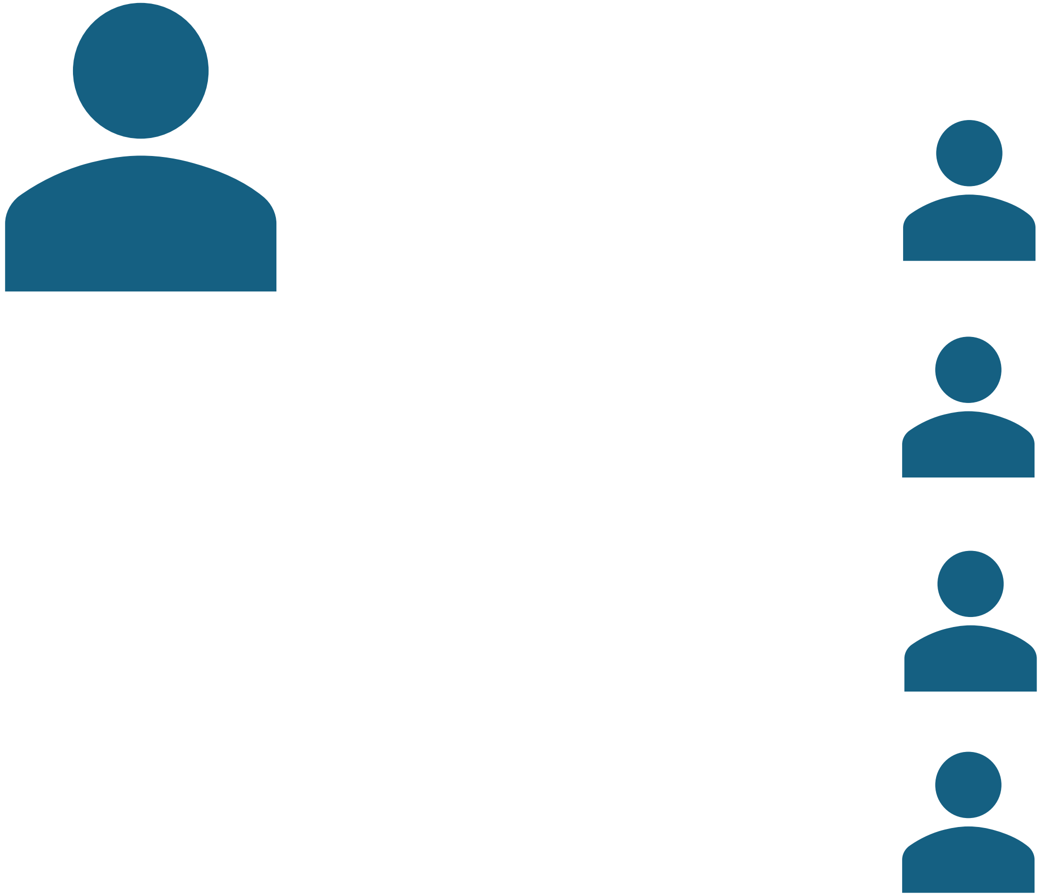


Building Threshold HE: Key Generation



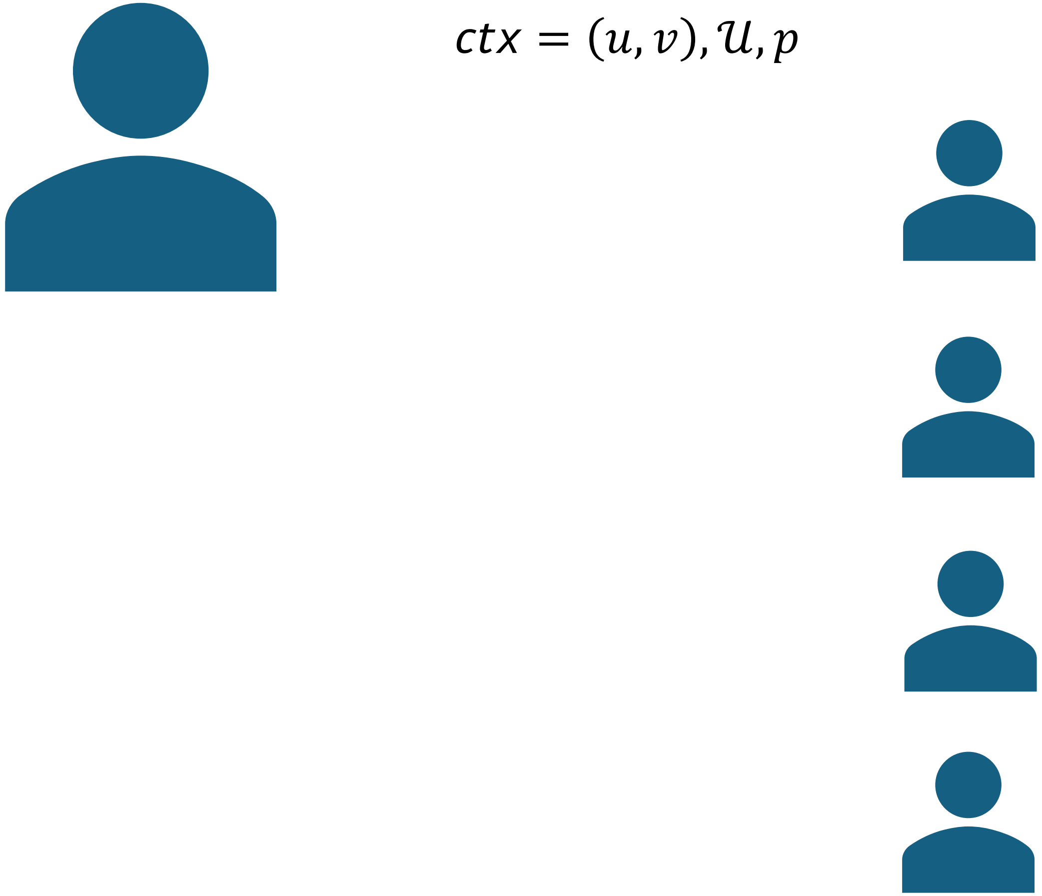
Commitments and ZKPs for active security

Building Threshold HE: Threshold Decryption

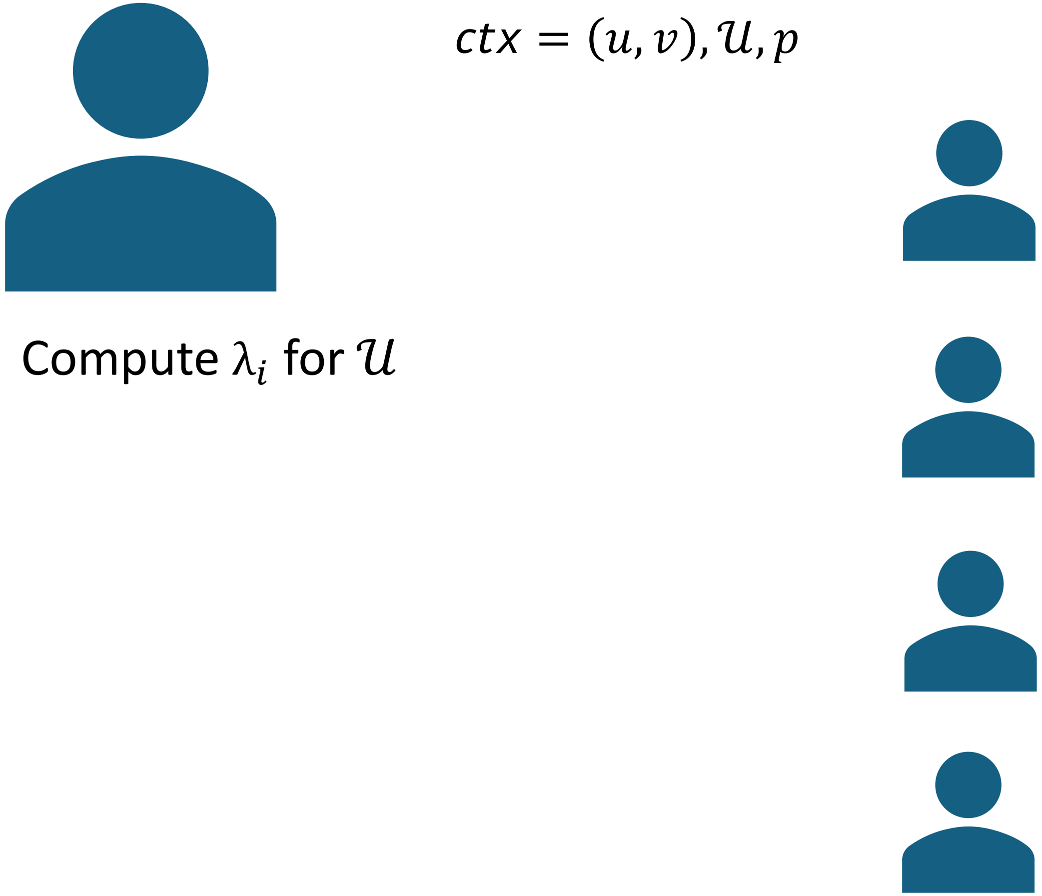


Building Threshold HE: Threshold Decryption

$ctx = (u, v), \mathcal{U}, p$



Building Threshold HE: Threshold Decryption

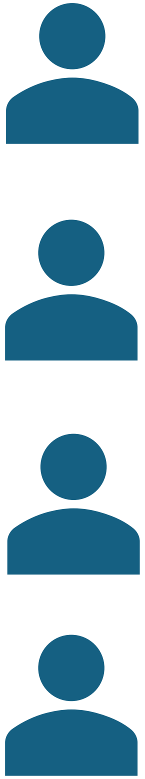


Building Threshold HE: Threshold Decryption

$ctx = (u, v), \mathcal{U}, p$

Compute λ_i for $\mathcal{U}$

$E_i \leftarrow D_{TDec}$



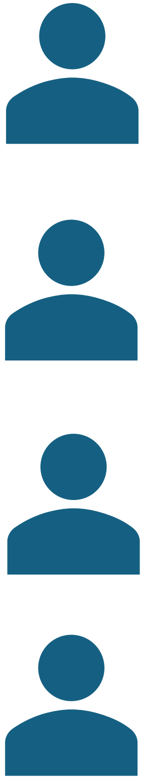
Building Threshold HE: Threshold Decryption

$ctx = (u, v), \mathcal{U}, p$

Compute λ_i for $\mathcal{U}$

$E_i \leftarrow D_{TDec}$

$d_i = \lambda_i sk_{\epsilon,i} u + pE_i$



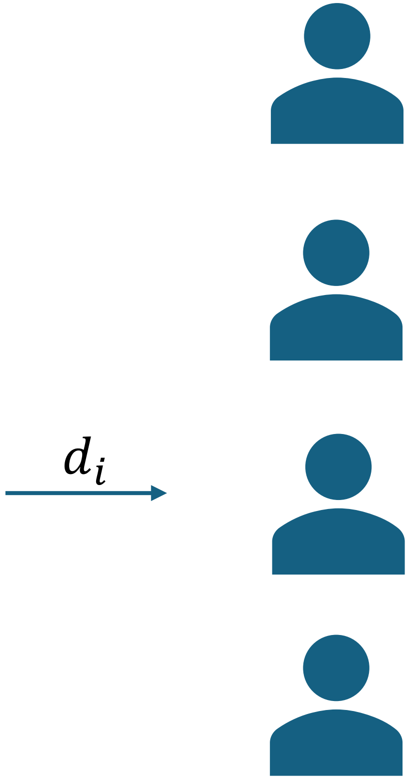
Building Threshold HE: Threshold Decryption

$ctx = (u, v), \mathcal{U}, p$

Compute λ_i for $\mathcal{U}$

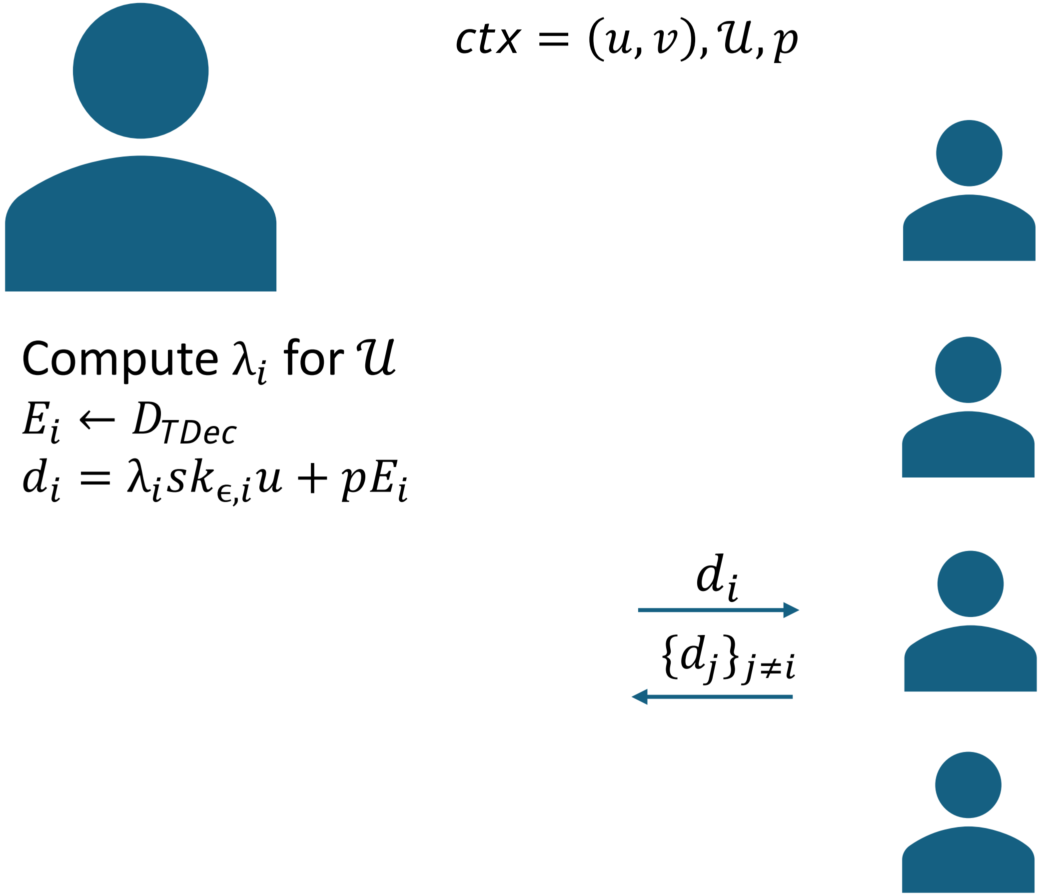
$E_i \leftarrow D_{TDec}$

$d_i = \lambda_i sk_{\epsilon,i} u + pE_i$



Building Threshold HE: Threshold Decryption

$ctx = (u, v), \mathcal{U}, p$



Compute λ_i for $\mathcal{U}$

$E_i \leftarrow D_{TDec}$

$d_i = \lambda_i sk_{\epsilon,i} u + pE_i$

d_i

$\{d_j\}_{j \neq i}$

Building Threshold HE: Threshold Decryption

$ctx = (u, v), \mathcal{U}, p$

Compute λ_i for $\mathcal{U}$

$E_i \leftarrow D_{TDec}$

$d_i = \lambda_i sk_{\epsilon,i} u + pE_i$

d_i →

← $\{d_j\}_{j \neq i}$

$ptx = v - \sum d_j \bmod p$

Building Threshold HE: Threshold Decryption

$ctx = (u, v), \mathcal{U}, p$

Compute λ_i for $\mathcal{U}$

$E_i \leftarrow D_{TDec}$

$d_i = \lambda_i sk_{\epsilon,i} u + pE_i$

d_i →

← $\{d_j\}_{j \neq i}$

$ptx = v - \sum d_j \bmod p$

Commitments and ZKPs for active security

Organization

- Build a suitable threshold HE
- Avoid rejection sampling
- Combine HE with rejection-free signature

Avoid rejection sampling

Avoid rejection sampling

- Rejection prevents leaking **s** with each query

Avoid rejection sampling

- Rejection prevents leaking **s** with each query
- Just remove it!

Avoid rejection sampling

- Rejection prevents leaking **s** with each query
- Just remove it!
  - Use the same **s** for a bounded number of queries

Avoid rejection sampling

- Rejection prevents leaking **s** with each query
- Just remove it!
  - Use the same **s** for a <u>bounded</u> number of queries
  - Analysis based on Renyi divergence(RD) [BLR+18]

Avoid rejection sampling

- Rejection prevents leaking **s** with each query
- Just remove it!
  - Use the same **s** for a bounded number of queries
  - Analysis based on Renyi divergence(RD) [BLR+18]
  - [ASY22] and “gentle noise flooding”

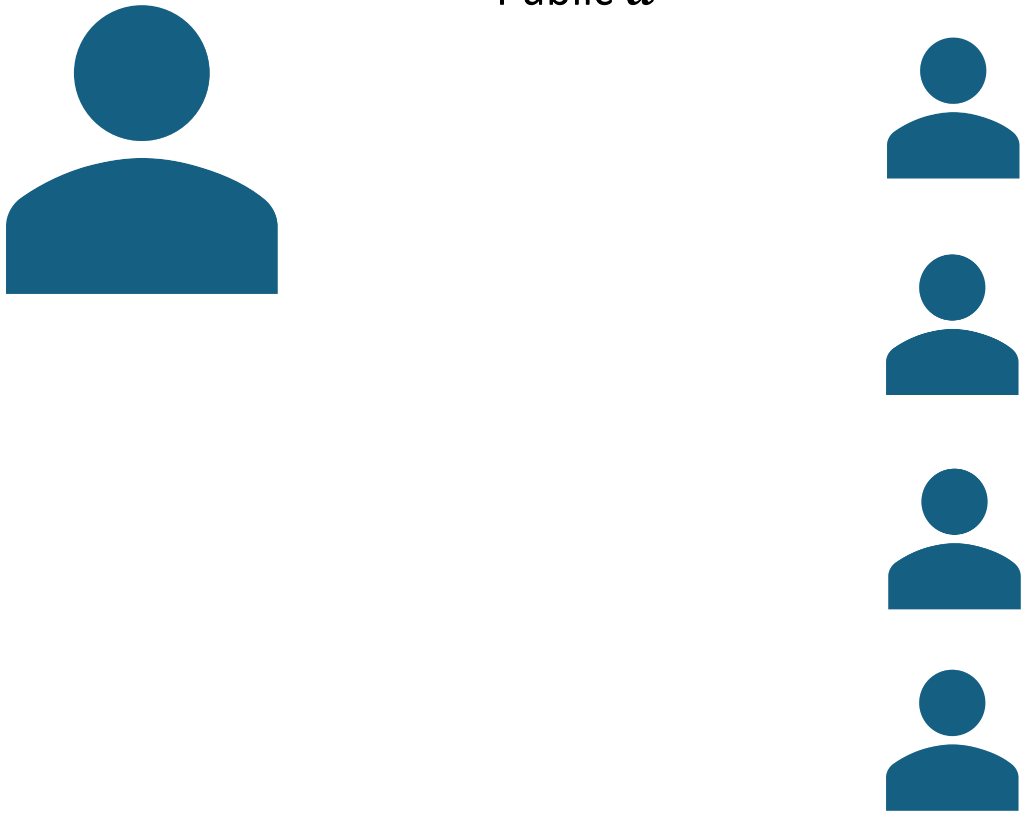
Organization

- Build a suitable threshold HE
- Deal with rejection sampling
- Combine HE with rejection-free signature

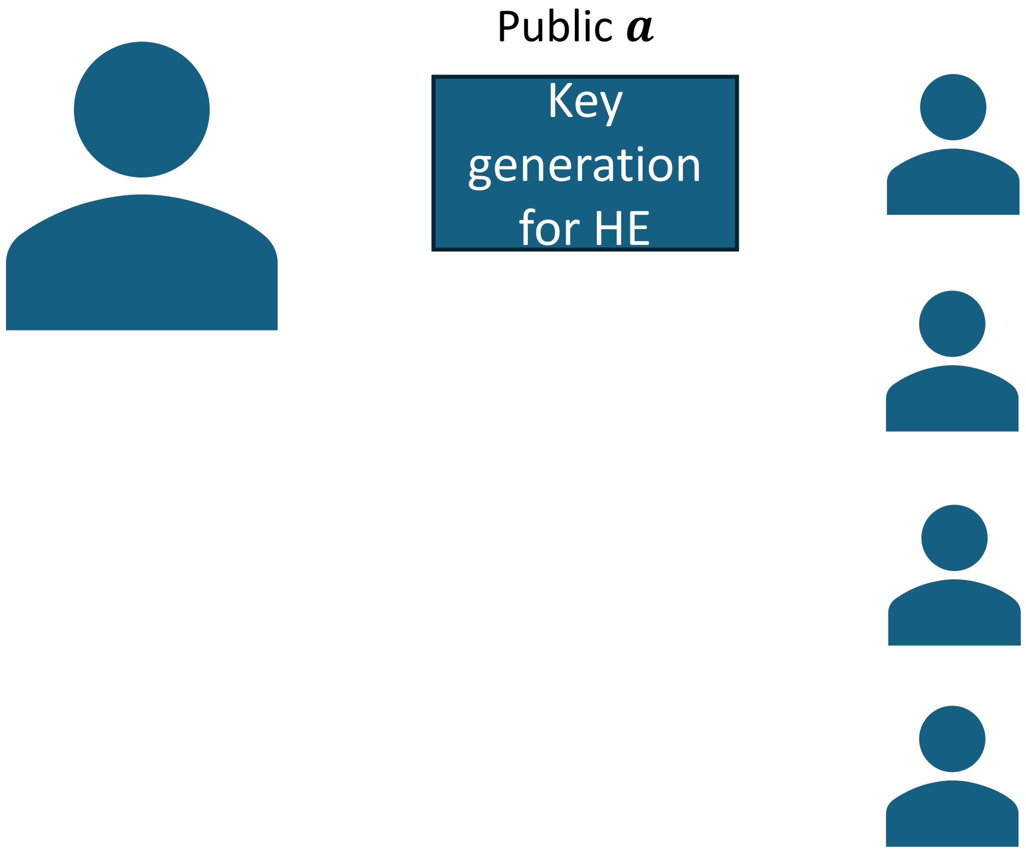
Building Signatures: Key Generation

Building Signatures: Key Generation

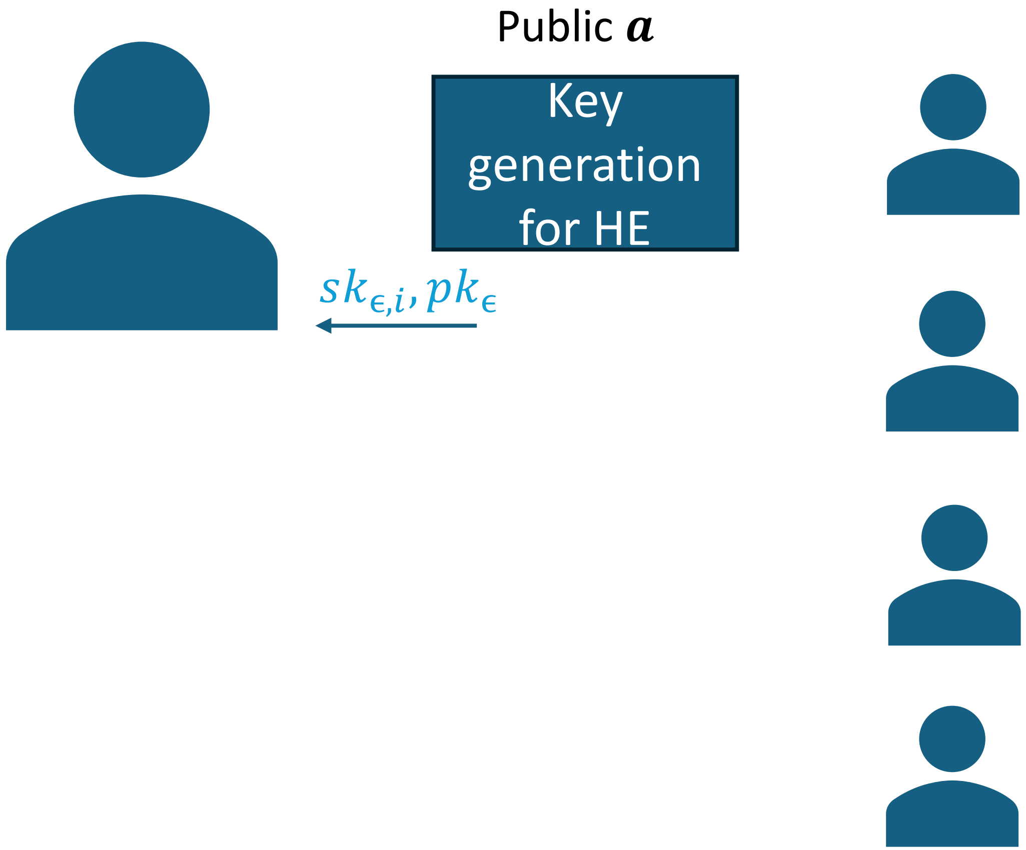
Public $\boldsymbol{a}$



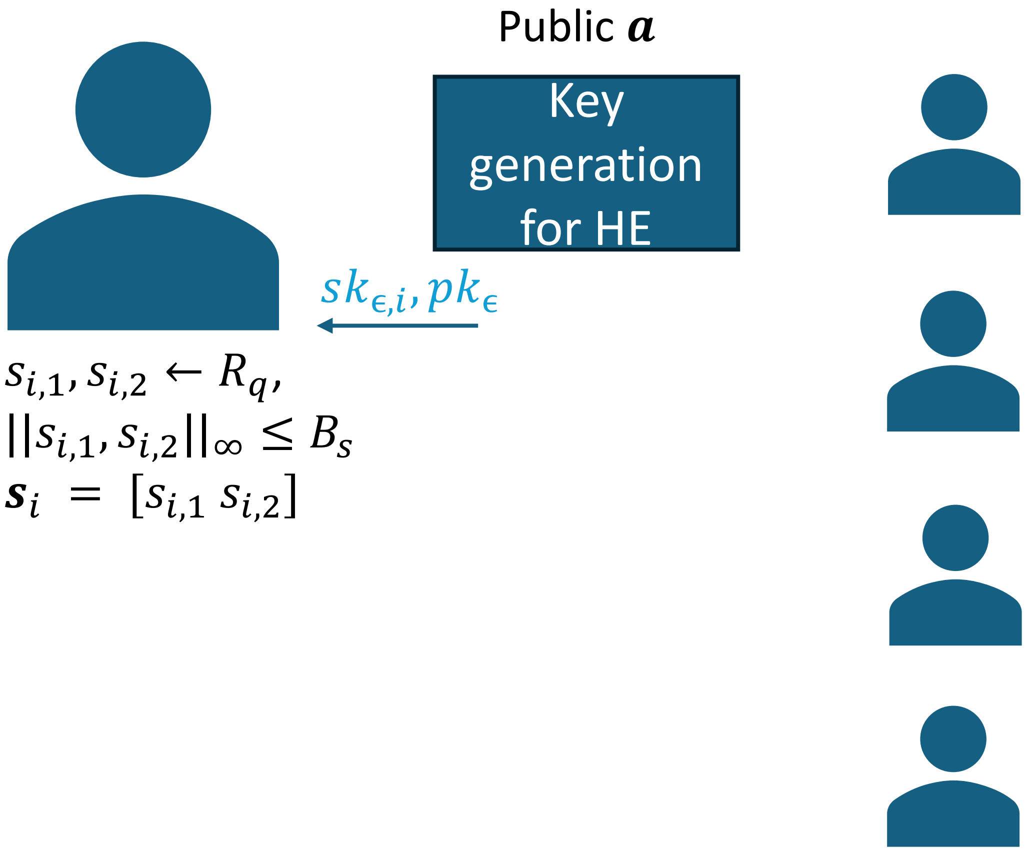
Building Signatures: Key Generation



Building Signatures: Key Generation

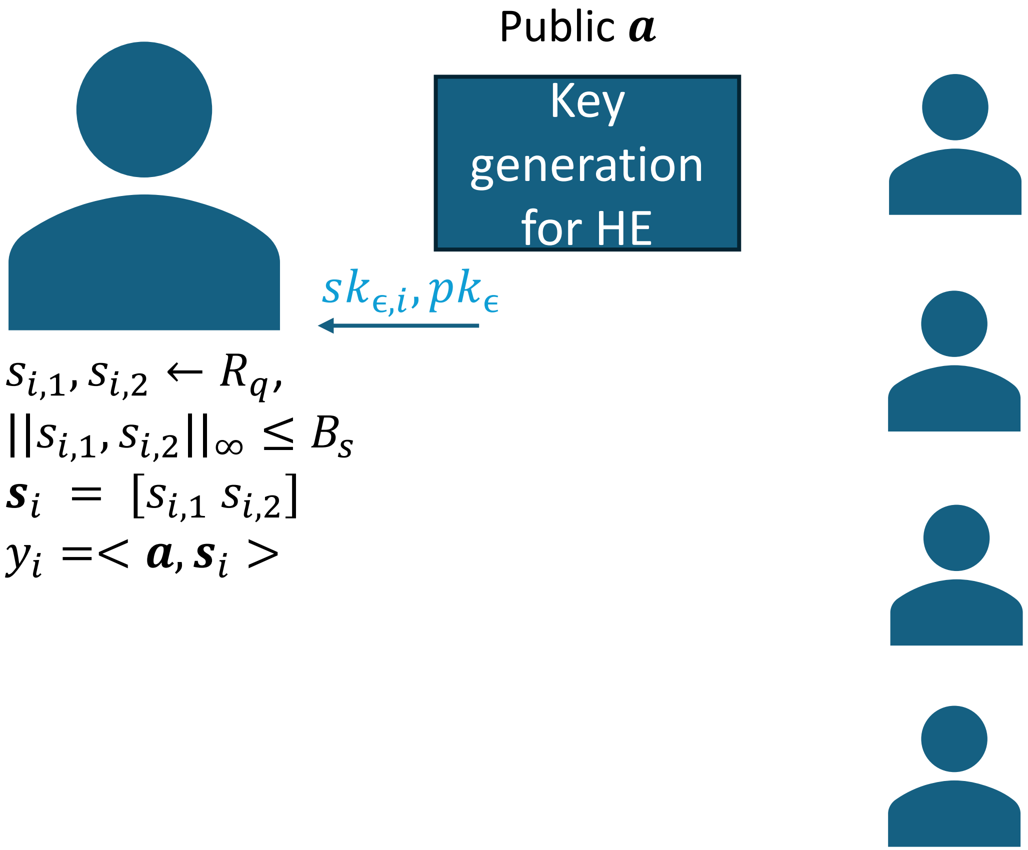


Building Signatures: Key Generation



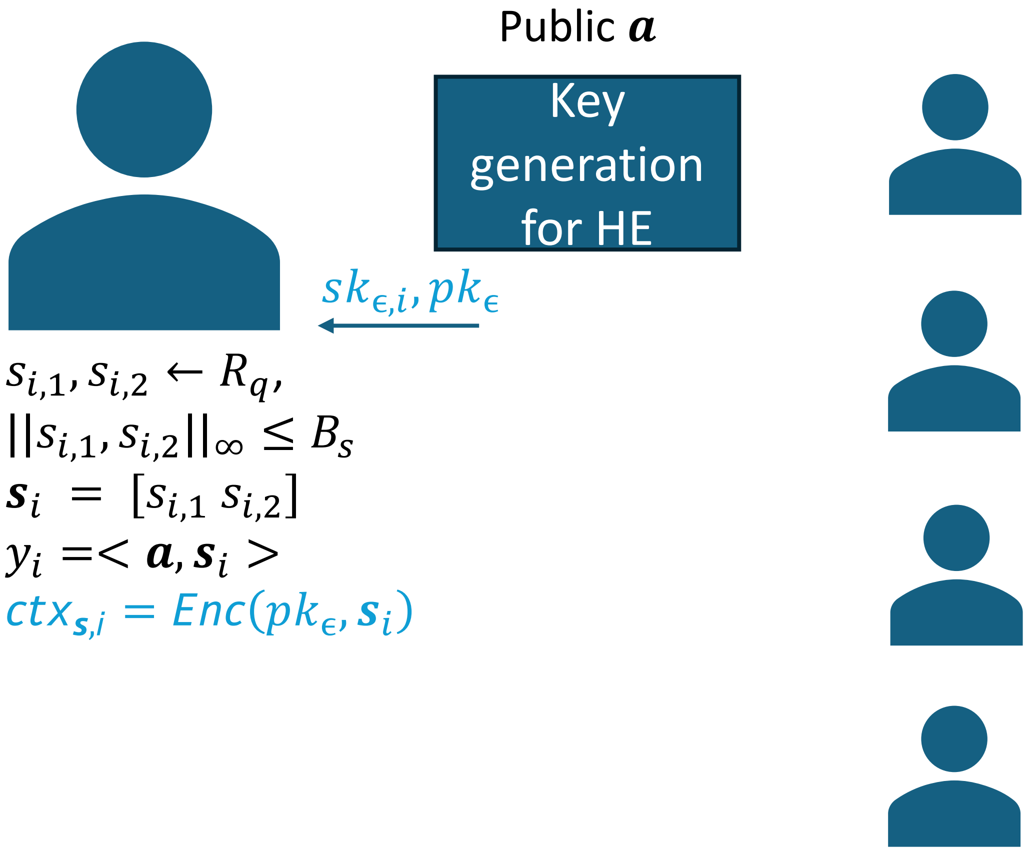
$s_{i,1}, s_{i,2} \leftarrow R_q,$
$||s_{i,1}, s_{i,2}||_\infty \leq B_s$
$\boldsymbol{s}_i = [s_{i,1}\ s_{i,2}]$

Building Signatures: Key Generation



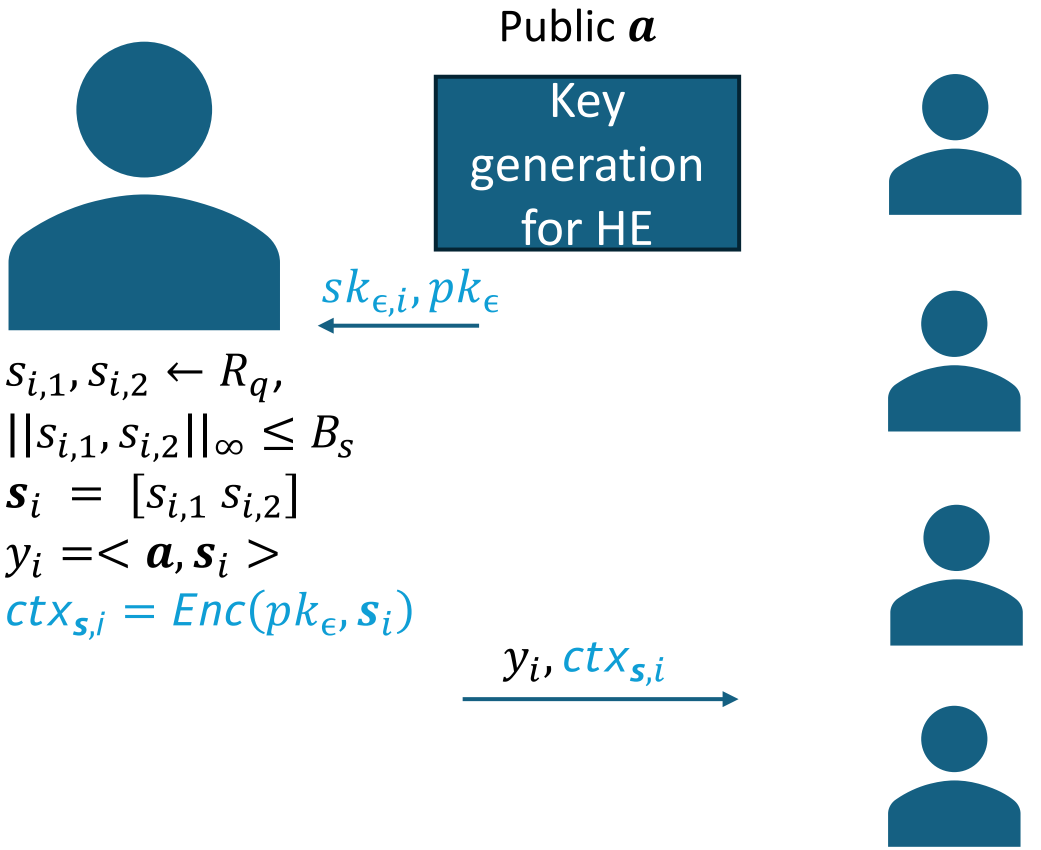
$$s_{i,1}, s_{i,2} \leftarrow R_q,$$
$$||s_{i,1}, s_{i,2}||_\infty \leq B_s$$
$$\boldsymbol{s}_i = [s_{i,1} \; s_{i,2}]$$
$$y_i =< \boldsymbol{a}, \boldsymbol{s}_i >$$

Building Signatures: Key Generation

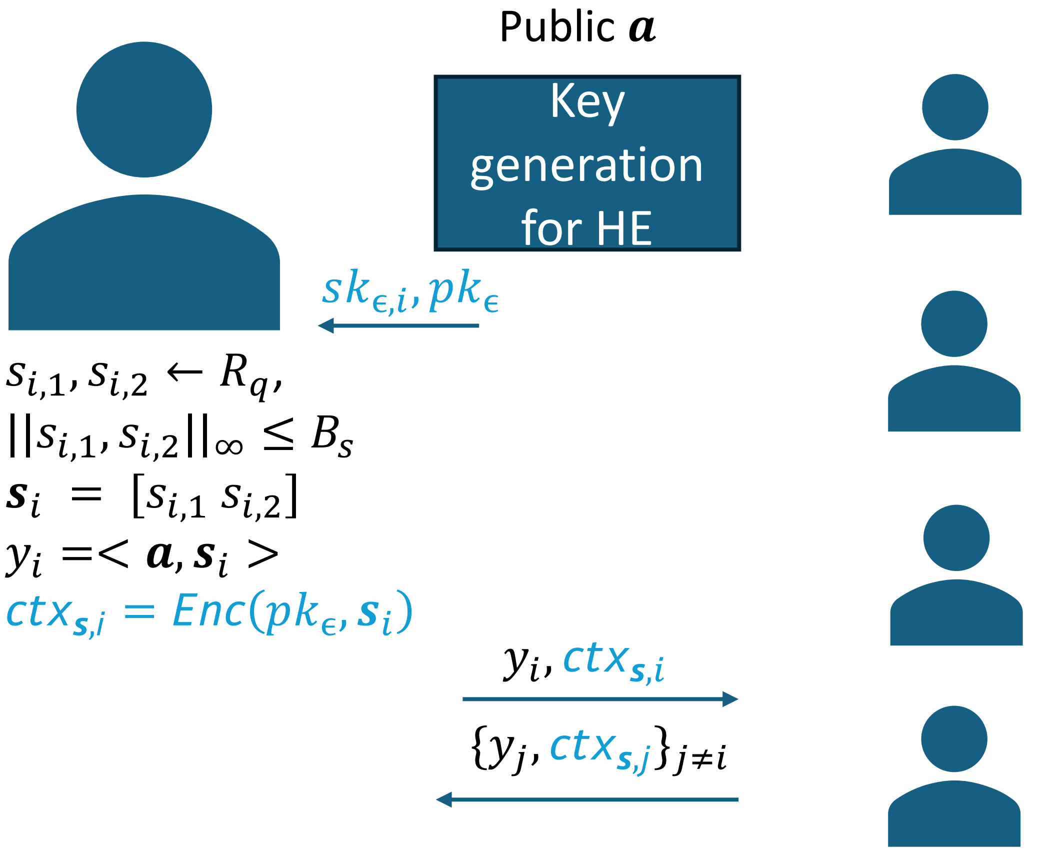


$s_{i,1}, s_{i,2} \leftarrow R_q,$
$||s_{i,1}, s_{i,2}||_{\infty} \leq B_s$
$\boldsymbol{s}_i = [s_{i,1}\ s_{i,2}]$
$y_i = < \boldsymbol{a}, \boldsymbol{s}_i >$
$ctx_{\boldsymbol{s},i} = Enc(pk_{\epsilon}, \boldsymbol{s}_i)$

Building Signatures: Key Generation

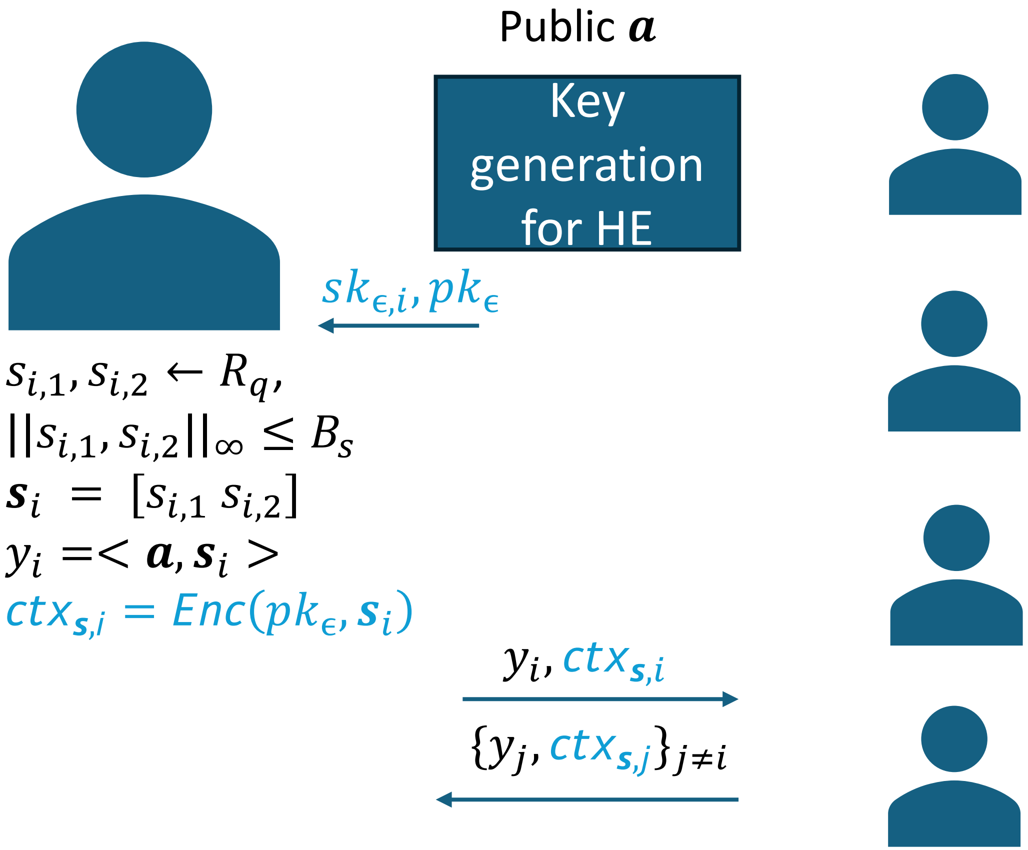


Building Signatures: Key Generation



$s_{i,1}, s_{i,2} \leftarrow R_q,$
$||s_{i,1}, s_{i,2}||_\infty \leq B_s$
$\boldsymbol{s}_i = [s_{i,1}\ s_{i,2}]$
$y_i = < \boldsymbol{a}, \boldsymbol{s}_i >$
$ctx_{\boldsymbol{s},i} = Enc(pk_{\epsilon}, \boldsymbol{s}_i)$

Building Signatures: Key Generation



$s_{i,1}, s_{i,2} \leftarrow R_q,$

$||s_{i,1}, s_{i,2}||_{\infty} \leq B_s$

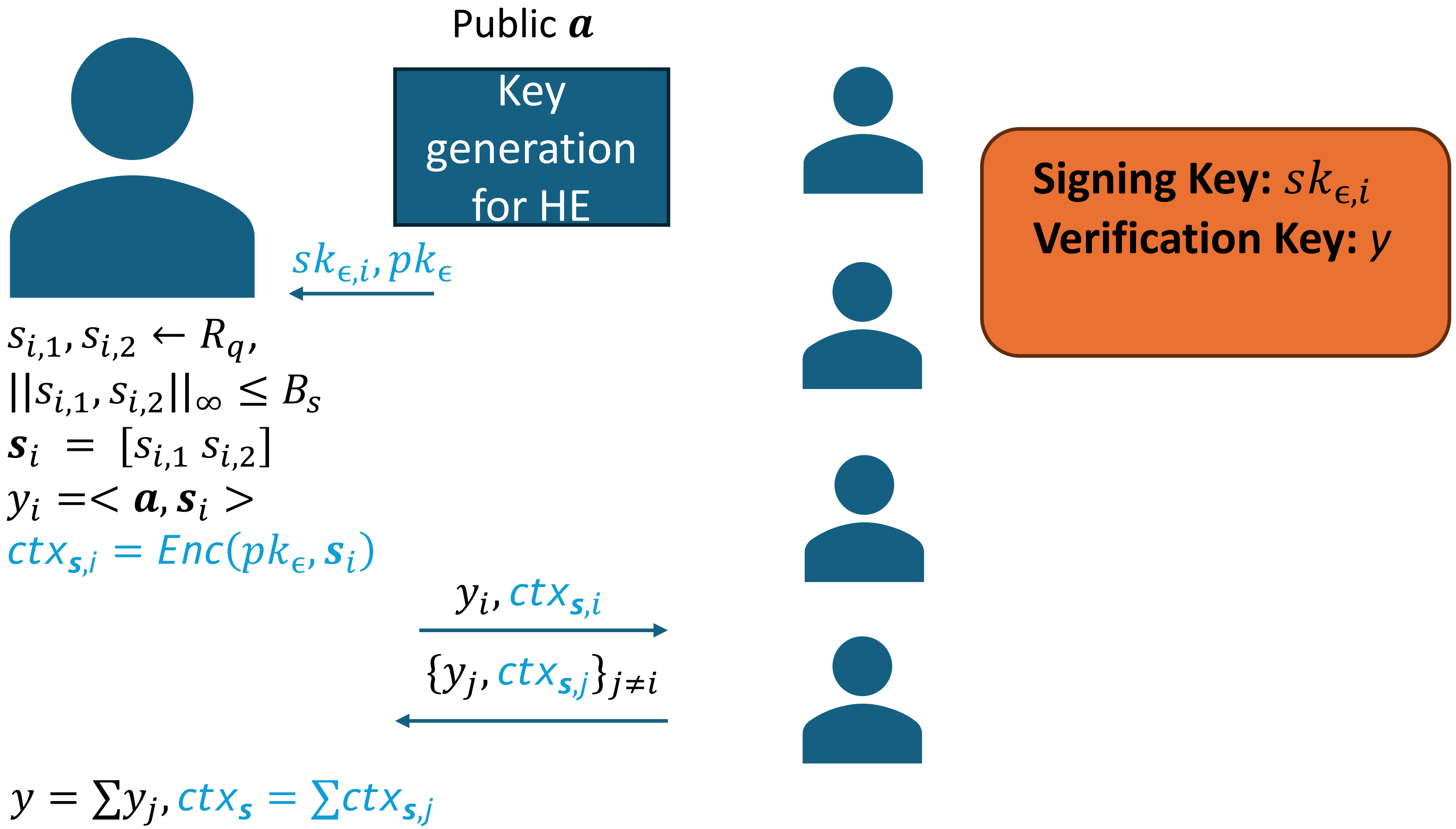
$\boldsymbol{s}_i = [s_{i,1} \; s_{i,2}]$

$y_i = < \boldsymbol{a}, \boldsymbol{s}_i >$

$ctx_{\boldsymbol{s},i} = Enc(pk_{\epsilon}, \boldsymbol{s}_i)$

$y = \sum y_j, ctx_{\boldsymbol{s}} = \sum ctx_{\boldsymbol{s},j}$

Building Signatures: Key Generation



Building Signatures: Key Generation

Public $\boldsymbol{a}$

Key generation for HE

$sk_{\epsilon,i}, pk_{\epsilon}$

$s_{i,1}, s_{i,2} \leftarrow R_q,$
$||s_{i,1}, s_{i,2}||_{\infty} \leq B_s$
$\boldsymbol{s}_i = [s_{i,1}\ s_{i,2}]$
$y_i = < \boldsymbol{a}, \boldsymbol{s}_i >$
$ctx_{\boldsymbol{s},i} = Enc(pk_{\epsilon}, \boldsymbol{s}_i)$

$y_i, ctx_{\boldsymbol{s},i}$

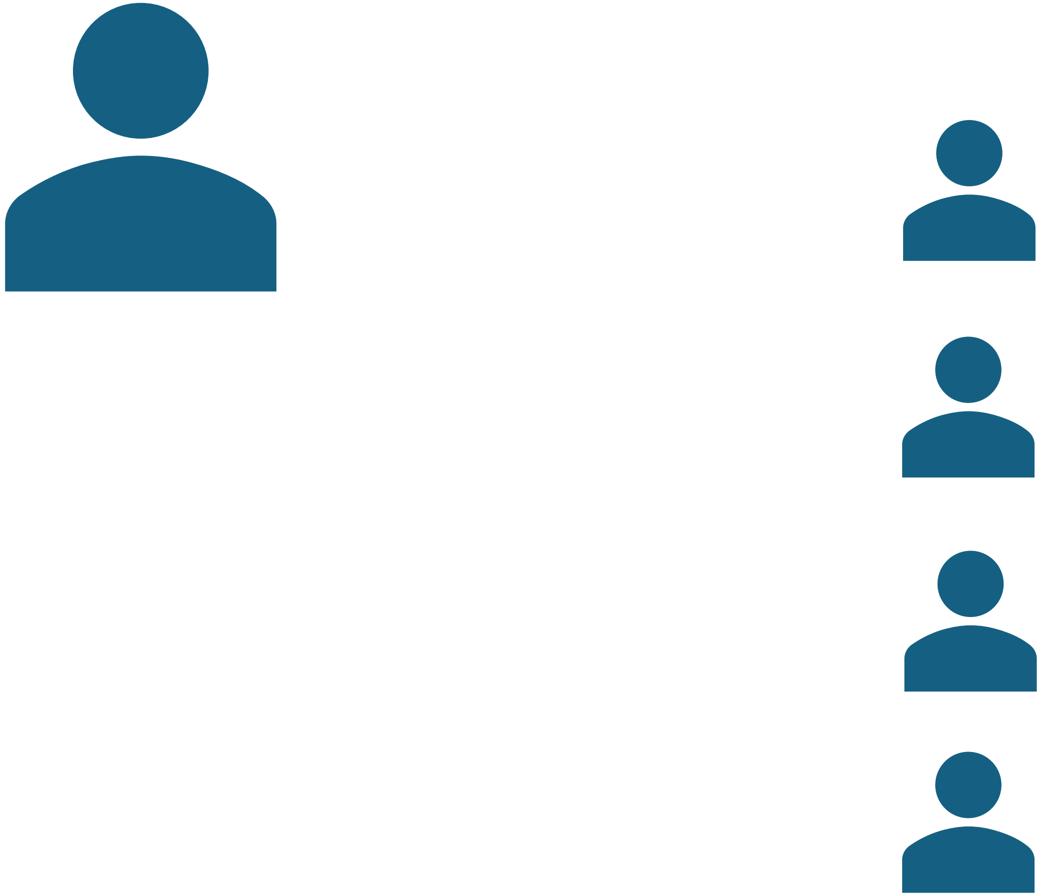
$\{y_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$

$y = \sum y_j, ctx_{\boldsymbol{s}} = \sum ctx_{\boldsymbol{s},j}$

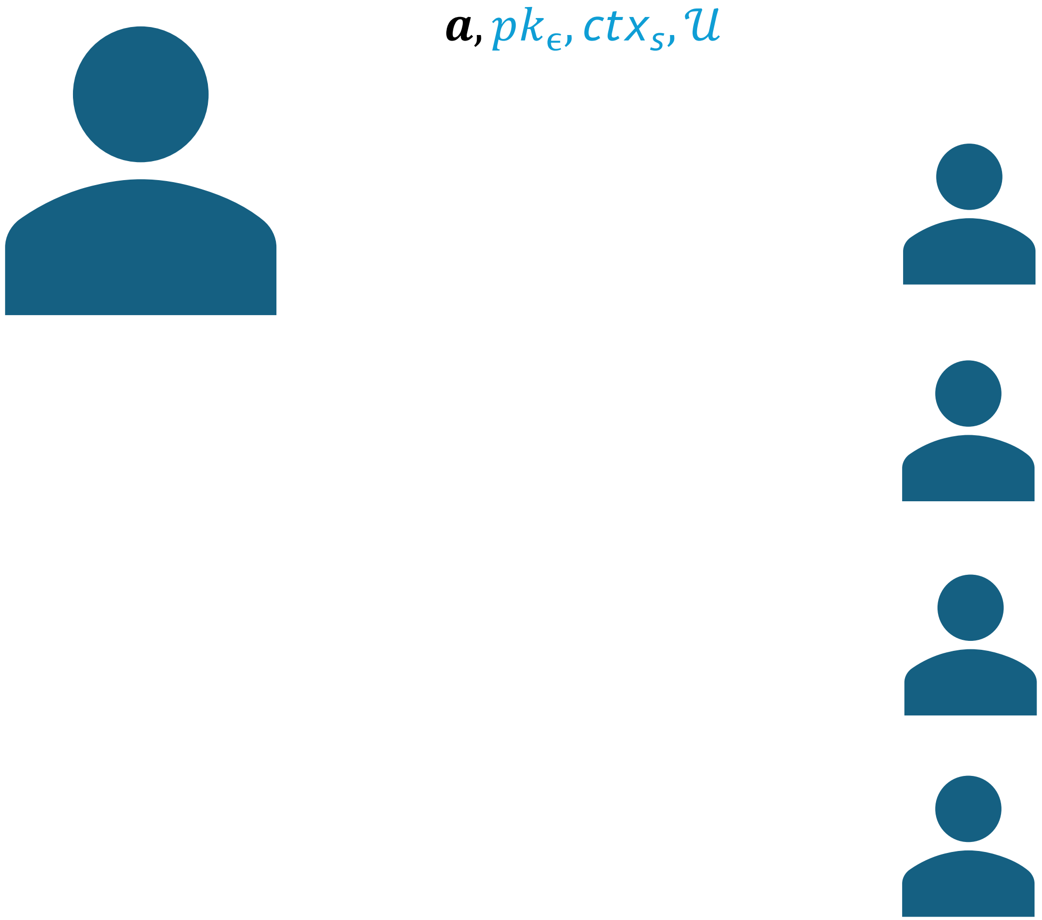
Signing Key: $sk_{\epsilon,i}$
Verification Key: y

Commitments and ZKPs for active security

Building Signatures: Signing



Building Signatures: Signing



Building Signatures: Signing

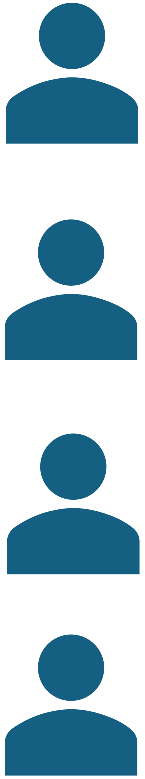
$\boldsymbol{a}, pk_{\epsilon}, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_{\infty} \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i =< \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$



Building Signatures: Signing

$\boldsymbol{a}, pk_\epsilon, ctx_s, \mathcal{U}$

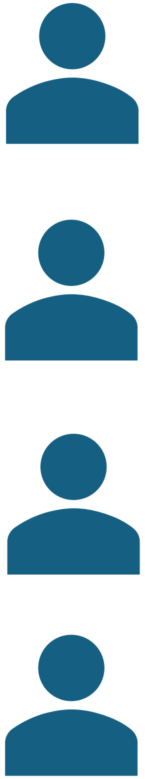
$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = < \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{r,i} = Enc(pk_\epsilon, \boldsymbol{r}_i)$

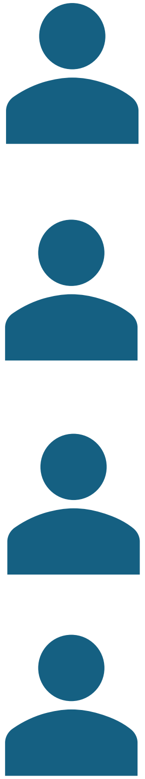


Building Signatures: Signing

$\boldsymbol{a}, pk_{\epsilon}, ctx_{s}, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_{\infty} \leq B_s$
$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i =< \boldsymbol{a}, \boldsymbol{r}_i >$
$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$
$com_i = Com_{ck}(w_i; \rho_i)$
$ctx_{\boldsymbol{r},i} = Enc(pk_{\epsilon}, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →



Building Signatures: Signing

$\boldsymbol{a}, pk_{\epsilon}, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_{\infty} \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i =< \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_{\epsilon}, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →

← $\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$

Building Signatures: Signing

$\boldsymbol{a}, pk_\epsilon, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}],\ w_i =< \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu),\ \rho_i \leftarrow \{0,1\}^*$

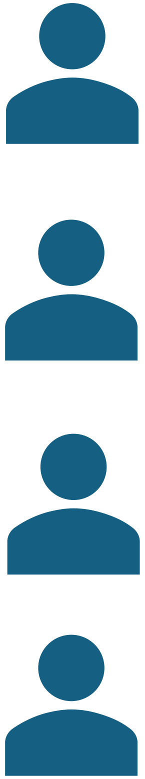
$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_\epsilon, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →

← $\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$

$c = H(\sum com_i\ , \mu)$



Building Signatures: Signing

$\boldsymbol{a}, pk_{\epsilon}, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \le B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = < \boldsymbol{a}, \boldsymbol{r}_i >$

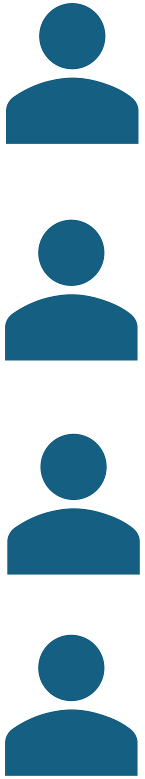
$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_{\epsilon}, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →

← $\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$



$c = H(\sum com_i\ , \mu)$

$ctx_{\boldsymbol{z}} = c\ ctx_{\boldsymbol{s}} + \sum ctx_{\boldsymbol{r},j}$

Building Signatures: Signing

$\boldsymbol{a}, pk_\epsilon, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = < \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_\epsilon, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →

$\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$ ←

$c = H(\sum com_i\ , \mu)$

$ctx_{\boldsymbol{z}} = c\ ctx_{\boldsymbol{s}} + \sum ctx_{\boldsymbol{r},j}$

$ds_i = TDec(ctx_{\boldsymbol{z}}, sk_{\epsilon,i}, \mathcal{U})$

Building Signatures: Signing

$\boldsymbol{a}, pk_\epsilon, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \le B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = < \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_\epsilon, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →

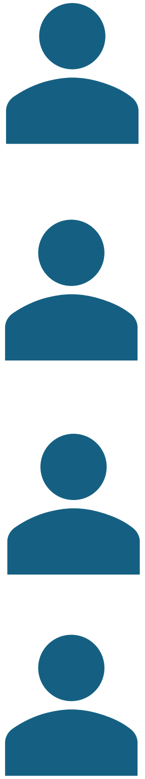
$\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$ ←

$c = H(\sum com_i, \mu)$

$ctx_{\boldsymbol{z}} = c\ ctx_{\boldsymbol{s}} + \sum ctx_{\boldsymbol{r},j}$

$ds_i = TDec(ctx_{\boldsymbol{z}}, sk_{\epsilon,i}, \mathcal{U})$

w_i, ρ_i, ds_i →



Building Signatures: Signing

$\boldsymbol{a}, pk_{\epsilon}, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = < \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_{\epsilon}, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →

$\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$ ←

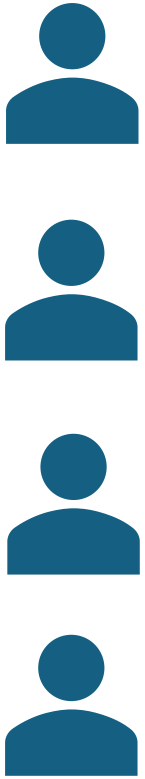
$c = H(\sum com_i, \mu)$

$ctx_{\boldsymbol{z}} = c\ ctx_{\boldsymbol{s}} + \sum ctx_{\boldsymbol{r},j}$

$ds_i = TDec(ctx_{\boldsymbol{z}}, sk_{\epsilon,i}, \mathcal{U})$

w_i, ρ_i, ds_i →

$\{w_i, \rho_i, ds_i\}_{j \neq i}$ ←



Building Signatures: Signing

$\boldsymbol{a}, pk_\epsilon, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = \langle \boldsymbol{a}, \boldsymbol{r}_i \rangle$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_\epsilon, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i} \rightarrow$

$\leftarrow \{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$ctx_{\boldsymbol{z}} = c\ ctx_{\boldsymbol{s}} + \sum ctx_{\boldsymbol{r},j}$

$ds_i = TDec(ctx_{\boldsymbol{z}}, sk_{\epsilon,i}, \mathcal{U})$

$w_i, \rho_i, ds_i \rightarrow$

$\leftarrow \{w_i, \rho_i, ds_i\}_{j \neq i}$

$\boldsymbol{z} = Comb(ctx_{\boldsymbol{z}}, \{ds_j\}, \mathcal{U}), \rho = \sum \rho_i$

Building Signatures: Signing

$\boldsymbol{a}, pk_{\epsilon}, ctx_{s}, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_{\infty} \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = < \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_{\epsilon}, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$

$\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$

$c = H(\sum com_i, \mu)$

$ctx_{\boldsymbol{z}} = c\ ctx_{\boldsymbol{s}} + \sum ctx_{\boldsymbol{r},j}$

$ds_i = TDec(ctx_{\boldsymbol{z}}, sk_{\epsilon,i}, \mathcal{U})$

w_i, ρ_i, ds_i

$\{w_i, \rho_i, ds_i\}_{j \neq i}$

$\boldsymbol{z} = Comb(ctx_{\boldsymbol{z}}, \{ds_j\}, \mathcal{U}), \rho = \sum \rho_i$

Signature: $(c, \boldsymbol{z}, \rho)$

Building Signatures: Signing

$\boldsymbol{a}, pk_\epsilon, ctx_s, \mathcal{U}$

$r_{i,1}, r_{i,2} \leftarrow R_q, ||r_{i,1}, r_{i,2}||_\infty \leq B_s$

$\boldsymbol{r}_i = [r_{i,1}\ r_{i,2}], w_i = < \boldsymbol{a}, \boldsymbol{r}_i >$

$ck = H(y, \mu), \rho_i \leftarrow \{0,1\}^*$

$com_i = Com_{ck}(w_i; \rho_i)$

$ctx_{\boldsymbol{r},i} = Enc(pk_\epsilon, \boldsymbol{r}_i)$

$com_i, ctx_{\boldsymbol{r},i}$ →

← $\{com_j, ctx_{\boldsymbol{s},j}\}_{j \neq i}$

$c = H(\sum com_i\ , \mu)$

$ctx_{\boldsymbol{z}} = c\ ctx_{\boldsymbol{s}} + \sum ctx_{\boldsymbol{r},j}$

$ds_i = TDec(ctx_{\boldsymbol{z}}, sk_{\epsilon,i}, \mathcal{U})$

w_i, ρ_i, ds_i →

← $\{w_i, \rho_i, ds_i\}_{j \neq i}$

$\boldsymbol{z} = Comb(ctx_{\boldsymbol{z}}, \{ds_j\}, \mathcal{U}), \rho = \sum \rho_i$

Signature: $(c, \boldsymbol{z}, \rho)$

Commitments and ZKPs for active security

- Security?

- Security?
  - Threshold unforgeability from underlying unforgeability + HE indistinguishability + RLWE + commitment/ZKP security(active only)

- Security?
  - Threshold unforgeability from underlying unforgeability + HE indistinguishability + RLWE + commitment/ZKP security(active only)
- Efficiency?

- Security?
  - Threshold unforgeability from underlying unforgeability + HE indistinguishability + RLWE + commitment/ZKP security(active only)
- Efficiency?

Scheme, # of Signatures	Public key (KB)	Signature (KB)	# of Rounds	Distributed Key Generation	Identifiable Abort
This work, β=1	2.6	8.5	2	✓	✓
This work, β=365	3.1	10.4	2	✓	✓
This work, $β=2^{64}$	13.6	46.6	2	✓	✓
TRaccoon [dPKM+24]*, $β=2^{60}$	3.9	12.7	3	✗**	✗

* = Public after our submission
**= Can use ours

Conclusion

Conclusion

- Built two-round lattice-based threshold signatures

Conclusion

- Built two-round lattice-based threshold signatures
  - Supports distributed key generation + identifiable abort

Conclusion

- Built two-round lattice-based threshold signatures
  - Supports distributed key generation + identifiable abort
  - Simple linear HE with distributed key generation as a building block

Conclusion

- Built two-round lattice-based threshold signatures
  - Supports distributed key generation + identifiable abort
  - Simple linear HE with distributed key generation as a building block
  - Somewhat practical sizes, comparable to recent constructions

Conclusion

- Built two-round lattice-based threshold signatures
  - Supports distributed key generation + identifiable abort
  - Simple linear HE with distributed key generation as a building block
  - Somewhat practical sizes, comparable to recent constructions

- Future Work

Conclusion

- Built two-round lattice-based threshold signatures
  - Supports distributed key generation + identifiable abort
  - Simple linear HE with distributed key generation as a building block
  - Somewhat practical sizes, comparable to recent constructions

- Future Work
  - Protocol optimizations

Conclusion

- Built two-round lattice-based threshold signatures
  - Supports distributed key generation + identifiable abort
  - Simple linear HE with distributed key generation as a building block
  - Somewhat practical sizes, comparable to recent constructions

- Future Work
  - Protocol optimizations
  - Adaptive security

Conclusion

- Built two-round lattice-based threshold signatures
  - Supports distributed key generation + identifiable abort
  - Simple linear HE with distributed key generation as a building block
  - Somewhat practical sizes, comparable to recent constructions

- Future Work
  - Protocol optimizations
  - Adaptive security
  - Same framework, different problems

Thank You!

Full Version:
https://ia.cr/2023/1318

References

- [ASY22] Shweta Agrawal, Damien Stehl´e, and Anshu Yadav. “Round-Optimal Lattice-Based Threshold Signatures, Revisited”. In Mikolaj Boja´nczyk,Emanuela Merelli, and David P. Woodruff, editors, 49th International Colloquium on Automata, Languages, and Programming (ICALP 2022), volume 229 of Leibniz International Proceedings in Informatics (LIPIcs), pages 8:1–8:20, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik.
- [BGG+18] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai. “Threshold cryptosystems from threshold fully homomorphic encryption”. In Hovav Shacham and Alexandra Boldyreva, editors, Advances in Cryptology – CRYPTO 2018, Part I, volume 10991 of Lecture Notes in Computer Science, pages 565–596, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany.

- [BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. “(Leveled) fully homomorphic encryption without bootstrapping”. In Shafi Goldwasser, editor, ITCS 2012: 3rd Innovations in Theoretical Computer Science, pages 309–325, Cambridge, MA, USA, January 8–10, 2012. Association for Computing Machinery.
- [BLR+18] Shi Bai, Tancr`ede Lepoint, Adeline Roux-Langlois, Amin Sakzad, Damien Stehl´e, and Ron Steinfeld. “Improved security proofs in lattice-based cryptography: Using the R´enyi divergence rather than the statistical distance”. Journal of Cryptology, 31(2):610–640, April 2018. 1.2, 4, 2.

- [CCL+20] Guilhem Castagnos, Dario Catalano, Fabien Laguillaumie, Federico Savasta, and Ida Tucker. “Bandwidth-efficient threshold EC-DSA”. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors,PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part II, volume 12111 of Lecture Notes in Computer Science, pages 266–296, Edinburgh, UK, May 4–7, 2020. Springer, Heidelberg, Germany.
- [CGG+20] Ran Canetti, Rosario Gennaro, Steven Goldfeder, Nikolaos Makriyannis, and Udi Peled. “UC non-interactive, proactive, threshold ECDSA with identifiable aborts”. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, ACM CCS 2020: 27th Conference on Computer and Communications Security, pages 1769–1787, Virtual Event, USA, November 9–13, 2020. ACM Press.

- [CGRS23] Hien Chu, Paul Gerhart, Tim Ruffing, and Dominique Schr¨oder. “Practical Schnorr threshold signatures without the algebraic group model”. In Helena Handschuh and Anna Lysyanskaya, editors, Advances in Cryptology – CRYPTO 2023, Part I, volume 14081 of Lecture Notes in Computer Science, pages 743–773, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Heidelberg, Germany.
- [CS19] Daniele Cozzo and Nigel P. Smart. “Sharing the LUOV: Threshold post-quantum signatures”. In Martin Albrecht, editor, 17th IMA International Conference on Cryptography and Coding, volume 11929 of Lecture Notes in Computer Science, pages 128–153, Oxford, UK, December 16–18, 2019. Springer, Heidelberg, Germany.

- [DJN+20] Ivan Damg˚ard, Thomas Pelle Jakobsen, Jesper Buus Nielsen, Jakob Illeborg Pagter, and Michael Bæksvang Østergaard. “Fast threshold ECDSA with honest majority”. In Clemente Galdi and Vladimir Kolesnikov, editors, SCN 20: 12th International Conference on Security in Communication Networks, volume 12238 of Lecture Notes in Computer Science, pages 382–400, Amalfi, Italy, September 14–16, 2020. Springer, Heidelberg, Germany.
- [DOTT21] Ivan Damg˚ard, Claudio Orlandi, Akira Takahashi, and Mehdi Tibouchi.“Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices”. In Juan Garay, editor, PKC 2021: 24th International Conference on Theory and Practice of Public Key Cryptography, Part I, volume 12710 of Lecture Notes in Computer Science, pages 99–130, Virtual Event, May 10–13, 2021. Springer, Heidelberg, Germany.

- [dPKM+24] Rafael del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, and Markku-Juhani O. Saarinen. Threshold raccoon: Practical threshold signatures from standard lattice assumptions, 2024. Appeared in EUROCRYPT 2024. Available at https://eprint.iacr.org/2024/184.
- [KG20] Chelsea Komlo and Ian Goldberg. "FROST: Flexible round-optimized Schnorr threshold signatures". In Orr Dunkelman, Michael J. Jacobson Jr., and Colin O'Flynn, editors, SAC 2020: 27th Annual International Workshop on Selected Areas in Cryptography, volume 12804 of Lecture Notes in Computer Science, pages 34–65, Halifax, NS, Canada (Virtual Event), October 21-23, 2020. Springer, Heidelberg, Germany.

- [Lin24] Yehuda Lindell. “Simple three-round multiparty schnorr signing with full Simulatability”. IACR Communications in Cryptology, 1(1), 2024.