MEDS

Matrix Equivalence Digital Signature

Tung Chou, Ruben Niederhagen, Edoardo Persichetti,
Lars Ran, Tovohery Hajatiana Randrianarisoa,
Krijn Reijnders, Simona Samardjiska, Monika Trimoska

Lars Ran
Oxford Post-Quantum Cryptography Summit
September 5th, 2023

Radboud University

MEDS: a new code-based signature scheme

1 Matrix Code Equivalence

2 From MCE to MEDS

3 Performance

Matrix Code Equivalence

1

Matrix Code Equivalence

matrix code

A k-dimensional subspace $\mathscr{C} \subseteq \mathbb{F}_q^{m \times n}$ equipped with the *rank metric*

$$d(C_1, C_2) = \mathrm{Rank}(C_1 - C_2) \qquad C_1, C_2 \in \mathscr{C}$$

1

Matrix Code Equivalence

matrix code

A k-dimensional subspace $\mathscr{C} \subseteq \mathbb{F}_q^{m \times n}$ equipped with the *rank metric*

$$d(C_1, C_2) = \text{Rank}(C_1 - C_2) \qquad C_1, C_2 \in \mathscr{C}$$

$\mathscr{C}$

$q = 13, \quad m = 4, \quad n = 6, \quad k = 5$

$$C = \lambda_1 \cdot \begin{bmatrix} 2 & 8 & 10 & 4 & 5 & 7 \\ 1 & 11 & 7 & 9 & 6 & 12 \\ 3 & 0 & 13 & 5 & 4 & 8 \\ 9 & 6 & 3 & 2 & 10 & 11 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 12 & 0 & 4 & 11 & 9 & 3 \\ 5 & 6 & 8 & 13 & 2 & 1 \\ 10 & 7 & 3 & 9 & 4 & 6 \\ 2 & 5 & 11 & 8 & 1 & 10 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 5 & 2 & 9 & 11 & 4 & 8 \\ 3 & 7 & 1 & 10 & 12 & 0 \\ 6 & 9 & 2 & 13 & 11 & 8 \\ 1 & 5 & 6 & 3 & 10 & 7 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 9 & 4 & 6 & 1 & 13 & 2 \\ 8 & 0 & 5 & 12 & 6 & 11 \\ 3 & 7 & 10 & 9 & 4 & 5 \\ 2 & 8 & 11 & 3 & 7 & 1 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 7 & 10 & 4 & 6 & 8 & 3 \\ 1 & 5 & 2 & 11 & 9 & 0 \\ 13 & 7 & 6 & 4 & 12 & 2 \\ 8 & 3 & 1 & 9 & 5 & 10 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

Matrix Code Equivalence

matrix code

A k-dimensional subspace $\mathscr{C} \subseteq \mathbb{F}_q^{m \times n}$ equipped with the *rank metric*

$$d(C_1, C_2) = \text{Rank}(C_1 - C_2) \qquad C_1, C_2 \in \mathscr{C}$$

$\mathscr{C}$

$q = 13, \quad m = 4, \quad n = 6, \quad k = 5$

$$C = \lambda_1 \cdot \begin{bmatrix} 2 & 8 & 10 & 4 & 5 & 7 \\ 1 & 11 & 7 & 9 & 6 & 12 \\ 3 & 0 & 13 & 5 & 4 & 8 \\ 9 & 6 & 3 & 2 & 10 & 11 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 12 & 0 & 4 & 11 & 9 & 3 \\ 5 & 6 & 8 & 13 & 2 & 1 \\ 10 & 7 & 3 & 9 & 4 & 6 \\ 2 & 5 & 11 & 8 & 1 & 10 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 5 & 2 & 9 & 11 & 4 & 8 \\ 3 & 7 & 1 & 10 & 12 & 0 \\ 6 & 9 & 2 & 13 & 11 & 8 \\ 1 & 5 & 6 & 3 & 10 & 7 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 9 & 4 & 6 & 1 & 13 & 2 \\ 8 & 0 & 5 & 12 & 6 & 11 \\ 3 & 7 & 10 & 9 & 4 & 5 \\ 2 & 8 & 11 & 3 & 7 & 1 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 7 & 10 & 4 & 6 & 8 & 3 \\ 1 & 5 & 2 & 11 & 9 & 0 \\ 13 & 7 & 6 & 4 & 12 & 2 \\ 8 & 3 & 1 & 9 & 5 & 10 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

$\mathscr{D}$

$$D = \lambda_1 \cdot \begin{bmatrix} 4 & 12 & 9 & 9 & 12 & 12 \\ 6 & 3 & 2 & 2 & 5 & 7 \\ 5 & 7 & 12 & 12 & 0 & 6 \\ 12 & 3 & 7 & 12 & 2 & 7 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 0 & 1 & 12 & 9 & 1 & 9 \\ 11 & 2 & 0 & 11 & 5 & 6 \\ 5 & 9 & 4 & 12 & 2 & 12 \\ 9 & 6 & 9 & 10 & 11 & 0 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 1 & 1 & 3 & 9 & 3 & 7 \\ 9 & 5 & 12 & 9 & 1 & 1 \\ 4 & 3 & 7 & 12 & 10 & 7 \\ 7 & 4 & 9 & 3 & 2 & 4 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 2 & 12 & 2 & 3 & 4 & 5 \\ 12 & 9 & 10 & 6 & 12 & 1 \\ 3 & 3 & 11 & 11 & 11 & 2 \\ 9 & 6 & 0 & 12 & 11 & 7 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 10 & 2 & 12 & 8 & 9 & 9 \\ 2 & 10 & 2 & 11 & 1 & 11 \\ 9 & 2 & 9 & 10 & 3 & 6 \\ 9 & 11 & 7 & 10 & 11 & 6 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

Matrix Code Equivalence

matrix code

A k-dimensional subspace $\mathscr{C} \subseteq \mathbb{F}_q^{m \times n}$ equipped with the *rank metric*

$$d(C_1, C_2) = \mathrm{Rank}(C_1 - C_2) \qquad C_1, C_2 \in \mathscr{C}$$

Two matrix codes $\mathscr{C}$ and $\mathscr{D}$ are *equivalent* if we have a linear map $\mu : \mathscr{C} \to \mathscr{D}$ that preserves the metric (isometry): $\mathrm{Rank}\, \mu(C) = \mathrm{Rank}\, C, \qquad \forall C \in \mathscr{C}$

$\mathscr{C}$

$q = 13, \quad m = 4, \quad n = 6, \quad k = 5$

$$C = \lambda_1 \cdot \begin{bmatrix} 2 & 8 & 10 & 4 & 5 & 7 \\ 1 & 11 & 7 & 9 & 6 & 12 \\ 3 & 0 & 13 & 5 & 4 & 8 \\ 9 & 6 & 3 & 2 & 10 & 11 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 12 & 0 & 4 & 11 & 9 & 3 \\ 5 & 6 & 8 & 13 & 2 & 1 \\ 10 & 7 & 3 & 9 & 4 & 6 \\ 2 & 5 & 11 & 8 & 1 & 10 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 5 & 2 & 9 & 11 & 4 & 8 \\ 3 & 7 & 1 & 10 & 12 & 0 \\ 6 & 9 & 2 & 13 & 11 & 8 \\ 1 & 5 & 6 & 3 & 10 & 7 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 9 & 4 & 6 & 1 & 13 & 2 \\ 8 & 0 & 5 & 12 & 6 & 11 \\ 3 & 7 & 10 & 9 & 4 & 5 \\ 2 & 8 & 11 & 3 & 7 & 1 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 7 & 10 & 4 & 6 & 8 & 3 \\ 1 & 5 & 2 & 11 & 9 & 0 \\ 13 & 7 & 6 & 4 & 12 & 2 \\ 8 & 3 & 1 & 9 & 5 & 10 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

$\mathscr{D}$

$$D = \lambda_1 \cdot \begin{bmatrix} 4 & 12 & 9 & 9 & 12 & 12 \\ 6 & 3 & 2 & 2 & 5 & 7 \\ 5 & 7 & 12 & 12 & 0 & 6 \\ 12 & 3 & 7 & 12 & 2 & 7 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 0 & 1 & 12 & 9 & 1 & 9 \\ 11 & 2 & 0 & 11 & 5 & 6 \\ 5 & 9 & 4 & 12 & 2 & 12 \\ 9 & 6 & 9 & 10 & 11 & 0 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 1 & 1 & 3 & 9 & 3 & 7 \\ 9 & 5 & 12 & 9 & 1 & 1 \\ 4 & 3 & 7 & 12 & 10 & 7 \\ 7 & 4 & 9 & 3 & 2 & 4 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 2 & 12 & 2 & 3 & 4 & 5 \\ 12 & 9 & 10 & 6 & 12 & 1 \\ 3 & 3 & 11 & 11 & 11 & 2 \\ 9 & 6 & 0 & 12 & 11 & 7 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 10 & 2 & 12 & 8 & 9 & 9 \\ 2 & 10 & 2 & 11 & 1 & 11 \\ 9 & 2 & 9 & 10 & 3 & 6 \\ 9 & 11 & 7 & 10 & 11 & 6 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

1

Matrix Code Equivalence

$$A = \begin{bmatrix} 0 & 0 & 5 & 7 \\ 5 & 1 & 2 & 7 \\ 0 & 4 & 4 & 0 \\ 4 & 3 & 7 & 7 \end{bmatrix} \in \mathrm{GL}_m(q)$$

$$B = \begin{bmatrix} 9 & 0 & 8 & 11 & 2 & 3 \\ 2 & 7 & 4 & 7 & 4 & 9 \\ 3 & 3 & 10 & 10 & 12 & 12 \\ 10 & 6 & 8 & 3 & 5 & 10 \\ 0 & 7 & 5 & 1 & 5 & 7 \\ 0 & 0 & 1 & 1 & 8 & 12 \end{bmatrix} \in \mathrm{GL}_n(q)$$

$\mathscr{C}$

$q = 13, \quad m = 4, \quad n = 6, \quad k = 5$

$$C = \lambda_1 \cdot \begin{bmatrix} 2 & 8 & 10 & 4 & 5 & 7 \\ 1 & 11 & 7 & 9 & 6 & 12 \\ 3 & 0 & 13 & 5 & 4 & 8 \\ 9 & 6 & 3 & 2 & 10 & 11 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 12 & 0 & 4 & 11 & 9 & 3 \\ 5 & 6 & 8 & 13 & 2 & 1 \\ 10 & 7 & 3 & 9 & 4 & 6 \\ 2 & 5 & 11 & 8 & 1 & 10 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 5 & 2 & 9 & 11 & 4 & 8 \\ 3 & 7 & 1 & 10 & 12 & 0 \\ 6 & 9 & 2 & 13 & 11 & 8 \\ 1 & 5 & 6 & 3 & 10 & 7 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 9 & 4 & 6 & 1 & 13 & 2 \\ 8 & 0 & 5 & 12 & 6 & 11 \\ 3 & 7 & 10 & 9 & 4 & 5 \\ 2 & 8 & 11 & 3 & 7 & 1 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 7 & 10 & 4 & 6 & 8 & 3 \\ 1 & 5 & 2 & 11 & 9 & 0 \\ 13 & 7 & 6 & 4 & 12 & 2 \\ 8 & 3 & 1 & 9 & 5 & 10 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

$\mathscr{D}$

$$D = \lambda_1 \cdot \begin{bmatrix} 4 & 12 & 9 & 9 & 12 & 12 \\ 6 & 3 & 2 & 2 & 5 & 7 \\ 5 & 7 & 12 & 12 & 0 & 6 \\ 12 & 3 & 7 & 12 & 2 & 7 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 0 & 1 & 12 & 9 & 1 & 9 \\ 11 & 2 & 0 & 11 & 5 & 6 \\ 5 & 9 & 4 & 12 & 2 & 12 \\ 9 & 6 & 9 & 10 & 11 & 0 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 1 & 1 & 3 & 9 & 3 & 7 \\ 9 & 5 & 12 & 9 & 1 & 1 \\ 4 & 3 & 7 & 12 & 10 & 7 \\ 7 & 4 & 9 & 3 & 2 & 4 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 2 & 12 & 2 & 3 & 4 & 5 \\ 12 & 9 & 10 & 6 & 12 & 1 \\ 3 & 3 & 11 & 11 & 11 & 2 \\ 9 & 6 & 0 & 12 & 11 & 7 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 10 & 2 & 12 & 8 & 9 & 9 \\ 2 & 10 & 2 & 11 & 1 & 11 \\ 9 & 2 & 9 & 10 & 3 & 6 \\ 9 & 11 & 7 & 10 & 11 & 6 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

1

Matrix Code Equivalence

$$A = \begin{bmatrix} 0 & 0 & 5 & 7 \\ 5 & 1 & 2 & 7 \\ 0 & 4 & 4 & 0 \\ 4 & 3 & 7 & 7 \end{bmatrix} \in \mathrm{GL}_m(q)$$

$$B = \begin{bmatrix} 9 & 0 & 8 & 11 & 2 & 3 \\ 2 & 7 & 4 & 7 & 4 & 9 \\ 3 & 3 & 10 & 10 & 12 & 12 \\ 10 & 6 & 8 & 3 & 5 & 10 \\ 0 & 7 & 5 & 1 & 5 & 7 \\ 0 & 0 & 1 & 1 & 8 & 12 \end{bmatrix} \in \mathrm{GL}_n(q)$$

✓ we get $ACB \in \mathscr{D}$ for all $C \in \mathscr{C}$

$\mathscr{C}$

$q = 13, \quad m = 4, \quad n = 6, \quad k = 5$

$$C = \lambda_1 \cdot \begin{bmatrix} 2 & 8 & 10 & 4 & 5 & 7 \\ 1 & 11 & 7 & 9 & 6 & 12 \\ 3 & 0 & 13 & 5 & 4 & 8 \\ 9 & 6 & 3 & 2 & 10 & 11 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 12 & 0 & 4 & 11 & 9 & 3 \\ 5 & 6 & 8 & 13 & 2 & 1 \\ 10 & 7 & 3 & 9 & 4 & 6 \\ 2 & 5 & 11 & 8 & 1 & 10 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 5 & 2 & 9 & 11 & 4 & 8 \\ 3 & 7 & 1 & 10 & 12 & 0 \\ 6 & 9 & 2 & 13 & 11 & 8 \\ 1 & 5 & 6 & 3 & 10 & 7 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 9 & 4 & 6 & 1 & 13 & 2 \\ 8 & 0 & 5 & 12 & 6 & 11 \\ 3 & 7 & 10 & 9 & 4 & 5 \\ 2 & 8 & 11 & 3 & 7 & 1 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 7 & 10 & 4 & 6 & 8 & 3 \\ 1 & 5 & 2 & 11 & 9 & 0 \\ 13 & 7 & 6 & 4 & 12 & 2 \\ 8 & 3 & 1 & 9 & 5 & 10 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

$\mathscr{D}$

$$D = \lambda_1 \cdot \begin{bmatrix} 4 & 12 & 9 & 9 & 12 & 12 \\ 6 & 3 & 2 & 2 & 5 & 7 \\ 5 & 7 & 12 & 12 & 0 & 6 \\ 12 & 3 & 7 & 12 & 2 & 7 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 0 & 1 & 12 & 9 & 1 & 9 \\ 11 & 2 & 0 & 11 & 5 & 6 \\ 5 & 9 & 4 & 12 & 2 & 12 \\ 9 & 6 & 9 & 10 & 11 & 0 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 1 & 1 & 3 & 9 & 3 & 7 \\ 9 & 5 & 12 & 9 & 1 & 1 \\ 4 & 3 & 7 & 12 & 10 & 7 \\ 7 & 4 & 9 & 3 & 2 & 4 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 2 & 12 & 2 & 3 & 4 & 5 \\ 12 & 9 & 10 & 6 & 12 & 1 \\ 3 & 3 & 11 & 11 & 11 & 2 \\ 9 & 6 & 0 & 12 & 11 & 7 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 10 & 2 & 12 & 8 & 9 & 9 \\ 2 & 10 & 2 & 11 & 1 & 11 \\ 9 & 2 & 9 & 10 & 3 & 6 \\ 9 & 11 & 7 & 10 & 11 & 6 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

1

Matrix Code Equivalence

$$A = \begin{bmatrix} 0 & 0 & 5 & 7 \\ 5 & 1 & 2 & 7 \\ 0 & 4 & 4 & 0 \\ 4 & 3 & 7 & 7 \end{bmatrix} \in \mathrm{GL}_m(q)$$

$$B = \begin{bmatrix} 9 & 0 & 8 & 11 & 2 & 3 \\ 2 & 7 & 4 & 7 & 4 & 9 \\ 3 & 3 & 10 & 10 & 12 & 12 \\ 10 & 6 & 8 & 3 & 5 & 10 \\ 0 & 7 & 5 & 1 & 5 & 7 \\ 0 & 0 & 1 & 1 & 8 & 12 \end{bmatrix} \in \mathrm{GL}_n(q)$$

✓ we get $ACB \in \mathscr{D}$ for all $C \in \mathscr{C}$

✓ the map $\mu = (A, B)$ preserves rank!

$\mathscr{C}$

$q = 13, \quad m = 4, \quad n = 6, \quad k = 5$

$$C = \lambda_1 \cdot \begin{bmatrix} 2 & 8 & 10 & 4 & 5 & 7 \\ 1 & 11 & 7 & 9 & 6 & 12 \\ 3 & 0 & 13 & 5 & 4 & 8 \\ 9 & 6 & 3 & 2 & 10 & 11 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 12 & 0 & 4 & 11 & 9 & 3 \\ 5 & 6 & 8 & 13 & 2 & 1 \\ 10 & 7 & 3 & 9 & 4 & 6 \\ 2 & 5 & 11 & 8 & 1 & 10 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 5 & 2 & 9 & 11 & 4 & 8 \\ 3 & 7 & 1 & 10 & 12 & 0 \\ 6 & 9 & 2 & 13 & 11 & 8 \\ 1 & 5 & 6 & 3 & 10 & 7 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 9 & 4 & 6 & 1 & 13 & 2 \\ 8 & 0 & 5 & 12 & 6 & 11 \\ 3 & 7 & 10 & 9 & 4 & 5 \\ 2 & 8 & 11 & 3 & 7 & 1 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 7 & 10 & 4 & 6 & 8 & 3 \\ 1 & 5 & 2 & 11 & 9 & 0 \\ 13 & 7 & 6 & 4 & 12 & 2 \\ 8 & 3 & 1 & 9 & 5 & 10 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

$\mathscr{D}$

$$D = \lambda_1 \cdot \begin{bmatrix} 4 & 12 & 9 & 9 & 12 & 12 \\ 6 & 3 & 2 & 2 & 5 & 7 \\ 5 & 7 & 12 & 12 & 0 & 6 \\ 12 & 3 & 7 & 12 & 2 & 7 \end{bmatrix} + \lambda_2 \cdot \begin{bmatrix} 0 & 1 & 12 & 9 & 1 & 9 \\ 11 & 2 & 0 & 11 & 5 & 6 \\ 5 & 9 & 4 & 12 & 2 & 12 \\ 9 & 6 & 9 & 10 & 11 & 0 \end{bmatrix} + \lambda_3 \cdot \begin{bmatrix} 1 & 1 & 3 & 9 & 3 & 7 \\ 9 & 5 & 12 & 9 & 1 & 1 \\ 4 & 3 & 7 & 12 & 10 & 7 \\ 7 & 4 & 9 & 3 & 2 & 4 \end{bmatrix} + \lambda_4 \cdot \begin{bmatrix} 2 & 12 & 2 & 3 & 4 & 5 \\ 12 & 9 & 10 & 6 & 12 & 1 \\ 3 & 3 & 11 & 11 & 11 & 2 \\ 9 & 6 & 0 & 12 & 11 & 7 \end{bmatrix} + \lambda_5 \cdot \begin{bmatrix} 10 & 2 & 12 & 8 & 9 & 9 \\ 2 & 10 & 2 & 11 & 1 & 11 \\ 9 & 2 & 9 & 10 & 3 & 6 \\ 9 & 11 & 7 & 10 & 11 & 6 \end{bmatrix} \qquad \lambda_i \in \mathbb{F}_q$$

1

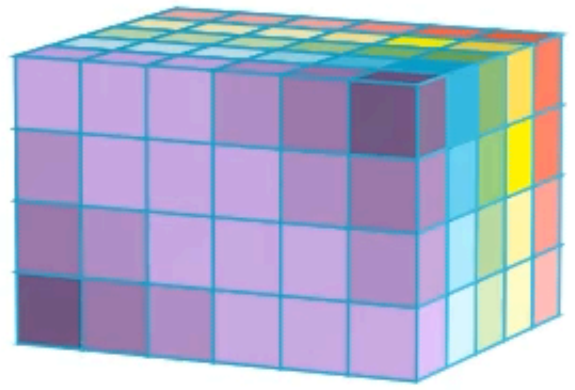
Matrix Code Equivalence

3-tensor

Can think of a matrix code as a 3-tensor over $\mathbb{F}_q$

Equivalence then becomes *tensor isomorphism*

$$\mathscr{C} \subseteq \mathbb{F}_q^{m\times n\times k}$$



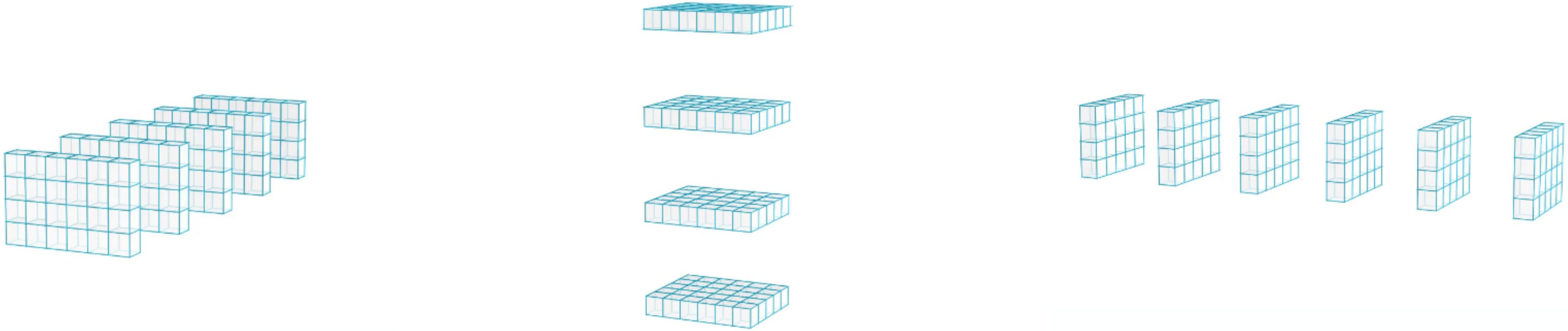
1

Matrix Code Equivalence

symmetry

Viewed as a 3-tensor, we can see $\mathscr{C}$ using three orientations

- a k-dimensional code in $\mathbb{F}_q^{m\times n}$
- an m-dimensional code in $\mathbb{F}_q^{n\times k}$
- an n-dimensional code in $\mathbb{F}_q^{m\times k}$



1

Matrix Code Equivalence

combinatorial

Attacks using isometry-invariant substructures

***Example**: find low-rank codewords in both codes and construct collisions using the birthday paradox*

- Graph-based algorithm
- Leon’s like algorithm

$$\tilde{\mathcal{O}}(q^{\min(n,m,k)})$$

1

Matrix Code Equivalence

combinatorial

Attacks using isometry-invariant substructures

***Example**: find low-rank codewords in both codes and construct collisions using the birthday paradox*

- Graph-based algorithm
- Leon’s like algorithm

$$\tilde{\mathcal{O}}(q^{\min(n,m,k)})$$

algebraic

Attacks reducing MCE to solving a system of polynomial equations using Gröbner basis techniques

***Example**: use the tensor isomorphism formulation to get a trilinear system*
***or**, consider transformed codewords AC_iB as dual to the dual code $\mathcal{D}^{\perp}$*

- direct modelling
- minor’s modelling
- *improved* modelling

$$\mathcal{O}\left(n^{\omega\frac{n}{4}}\right)$$

1

Matrix Code Equivalence

equations

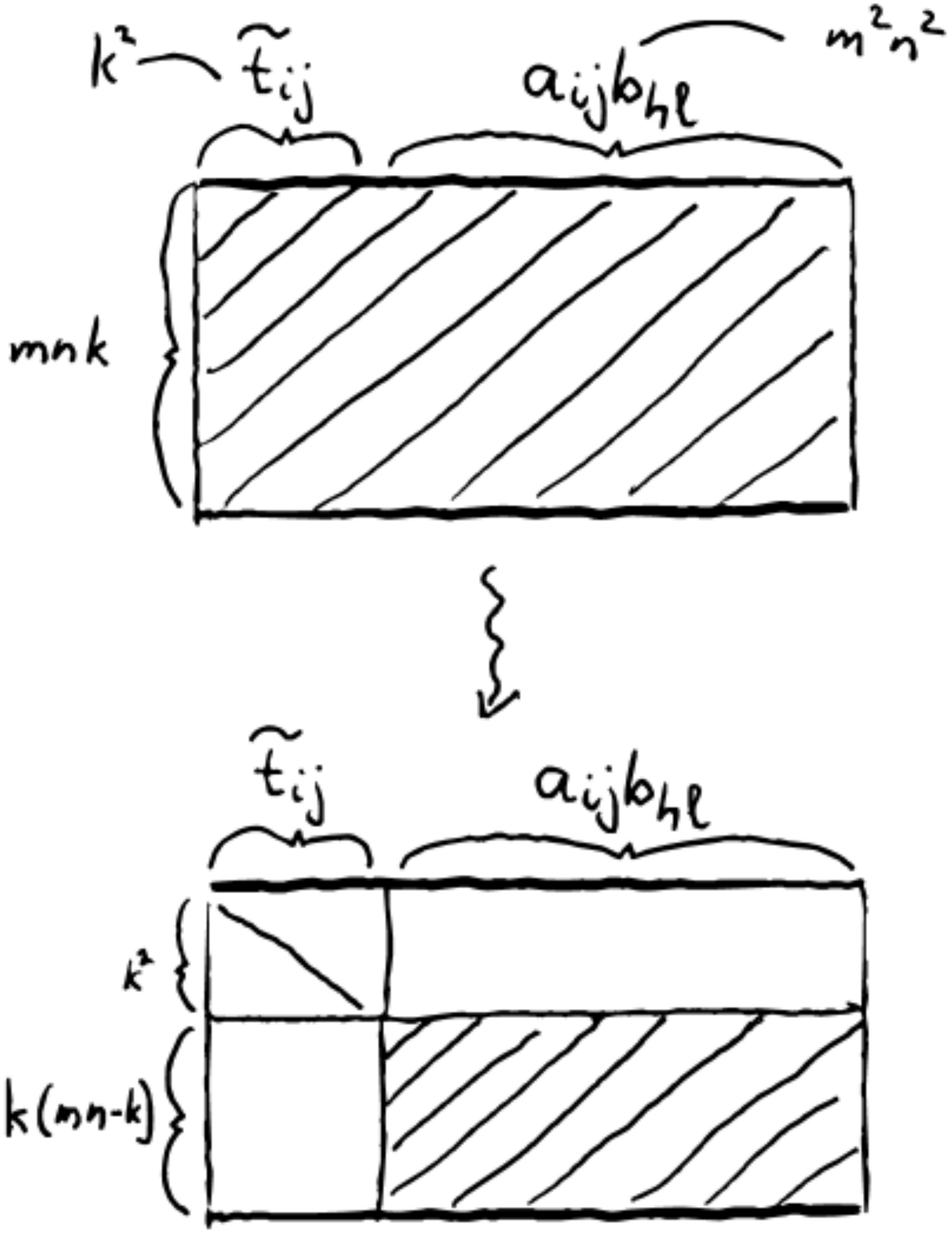
$$\mathscr{C}(Ax, By, z) = \mathscr{D}(x, y, T^{-1}z)$$

1

Matrix Code Equivalence

equations

$$\mathscr{C}(Ax, By, z) = \mathscr{D}(x, y, T^{-1}z)$$

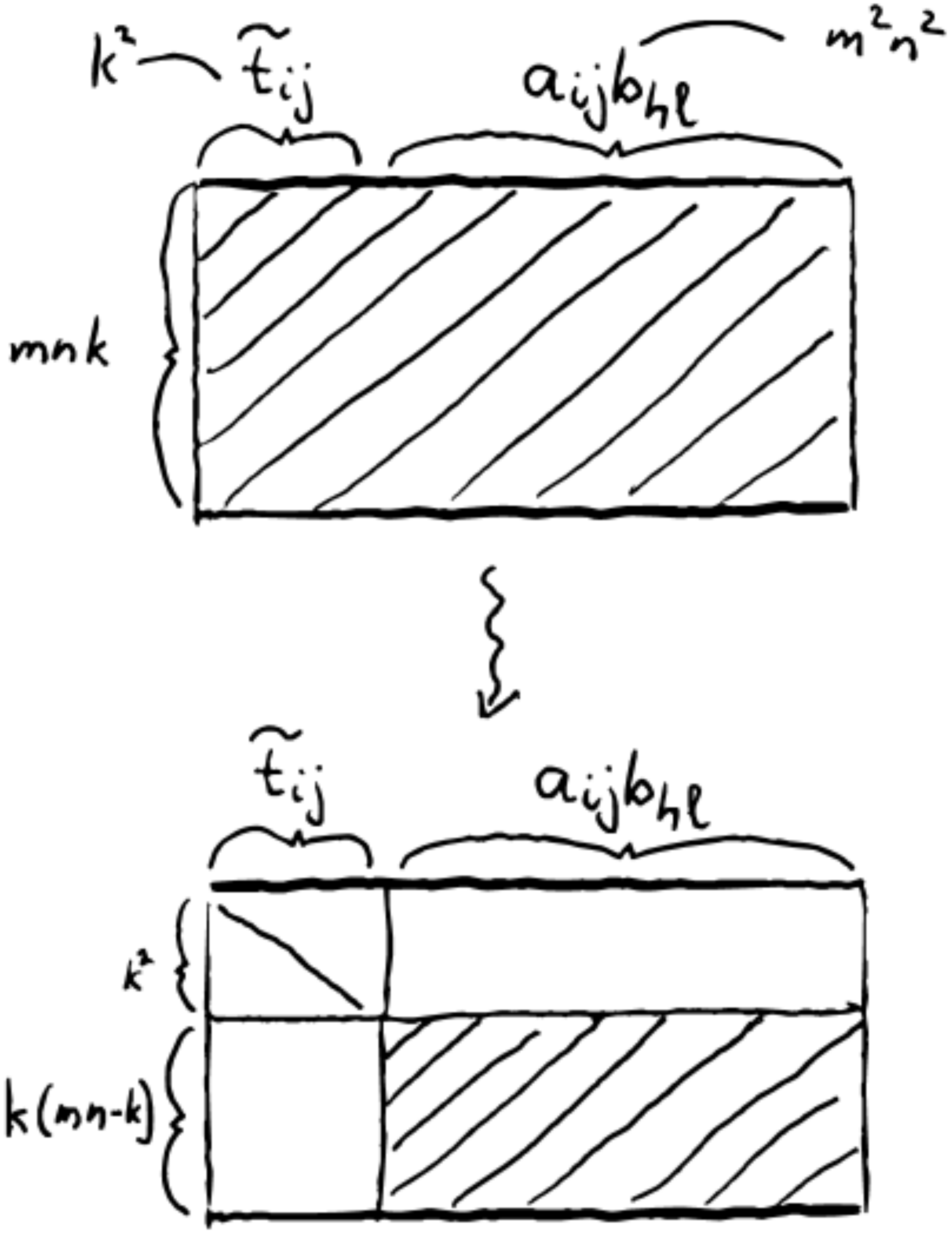


1

Matrix Code Equivalence

equations

$$\mathscr{C}(Ax, By, z) = \mathscr{D}(x, y, T^{-1}z)$$



system

Three bilinear systems:

$$\mathscr{C}(Ax, By, z) = \mathscr{D}(x, y, T^{-1}z)$$

$$\mathscr{C}(Ax, y, Tz) = \mathscr{D}(x, B^{-1}y, z)$$

$$\mathscr{C}(x, By, Tz) = \mathscr{D}(A^{-1}x, y, z)$$

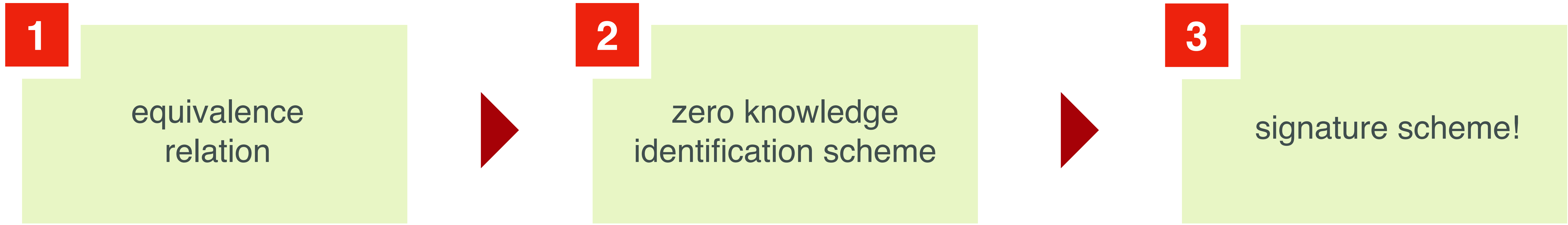
Equations:
$k(nm - k) + m(kn - m) + n(mk - n)$

Variables:
$n^2 + m^2 + k^2$

From MCE to MEDS

2

From MCE to MEDS



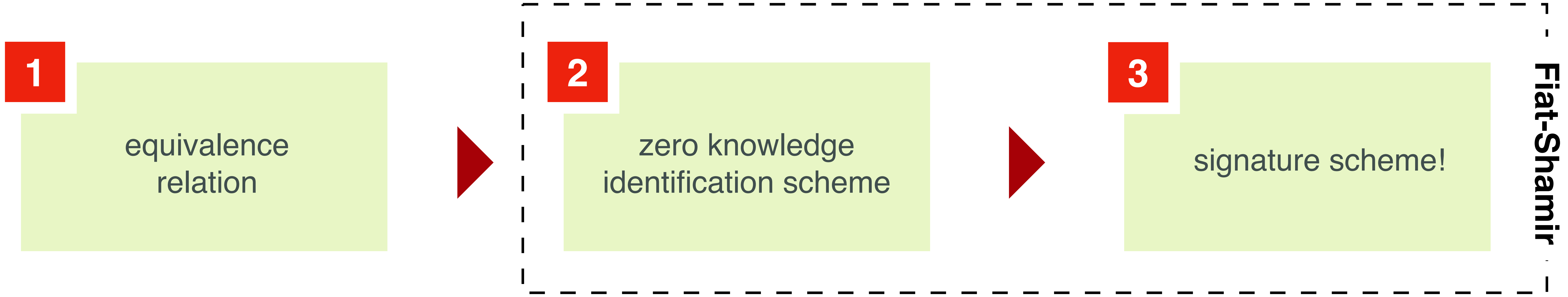
1 equivalence relation

2 zero knowledge identification scheme

3 signature scheme!

2

From MCE to MEDS



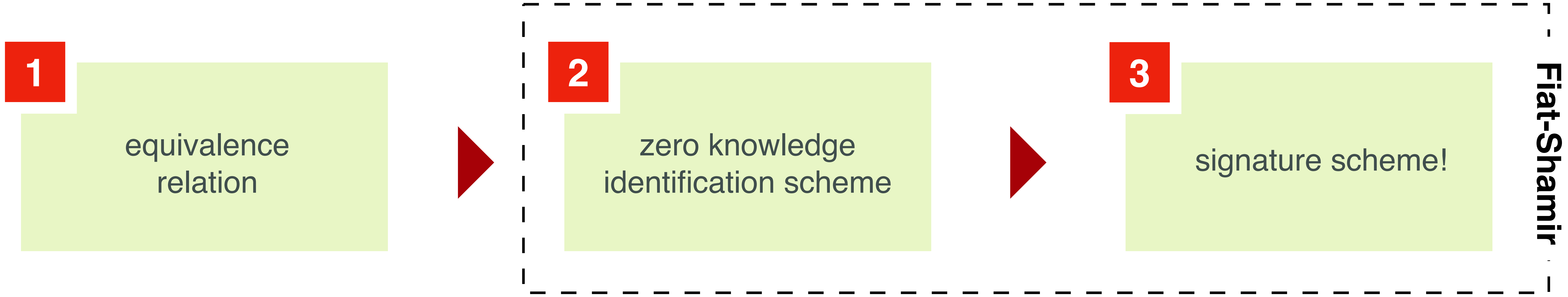
1 equivalence relation

2 zero knowledge identification scheme

3 signature scheme!

2

From MCE to MEDS

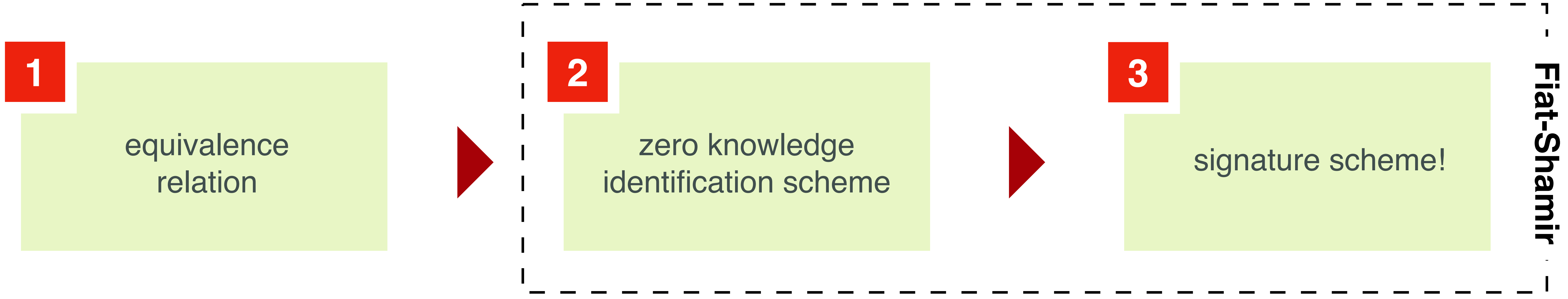


1 → 2

SETUP

- Assume parameter set $q, n, m, k.$ and “starting” code $\mathscr{C}$
- Generate **secret key** $A \in \mathrm{GL}_\mathrm{m}(q)$, $B \in \mathrm{GL}_n(q)$
- Generate **public key** $\mathscr{D} = A\mathscr{C}B$

$$\begin{tikzcd}
\mathscr{C} \arrow[d, "{(A, B)}"'] \\
\mathscr{D}
\end{tikzcd}$$



1 → 2

SETUP

- Assume parameter set $q, n, m, k.$ and “starting” code $\mathscr{C}$
- Generate **secret key** $A \in \mathrm{GL}_{\mathrm{m}}(q)$, $B \in \mathrm{GL}_n(q)$
- Generate **public key** $\mathscr{D} = A\mathscr{C}B$

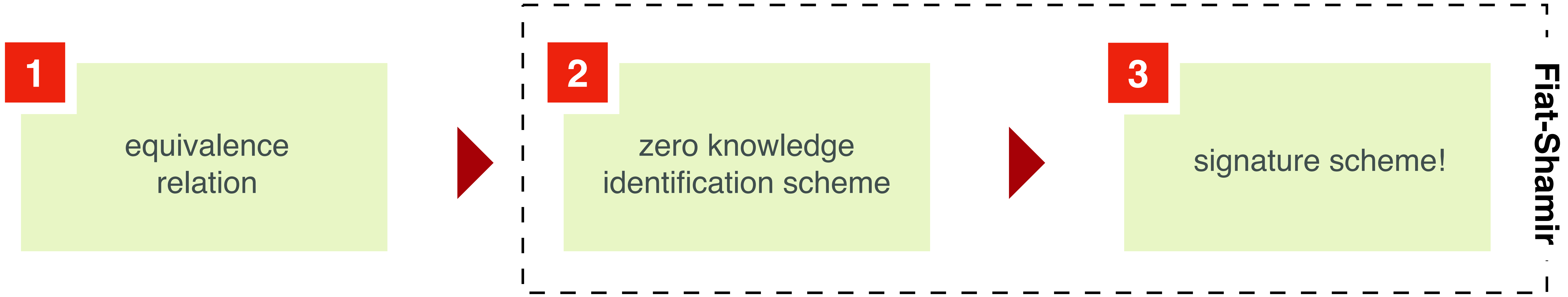
COMMIT

- Generate **ephemeral** $\tilde{A} \in \mathrm{GL}_{\mathrm{m}}(q)$, $\tilde{B} \in \mathrm{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathscr{C}} = \tilde{A}\mathscr{C}\tilde{B}$

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "(\tilde{A}, \tilde{B})"] \arrow[d, "(A, B)"'] & \tilde{\mathscr{C}} \\
\mathscr{D} &
\end{tikzcd}$$

2

From MCE to MEDS



1 → 2

SETUP

- Assume parameter set $q, n, m, k.$ and “starting” code $\mathscr{C}$
- Generate **secret key** $A \in \mathrm{GL}_\mathrm{m}(q)$, $B \in \mathrm{GL}_n(q)$
- Generate **public key** $\mathscr{D} = A\mathscr{C}B$

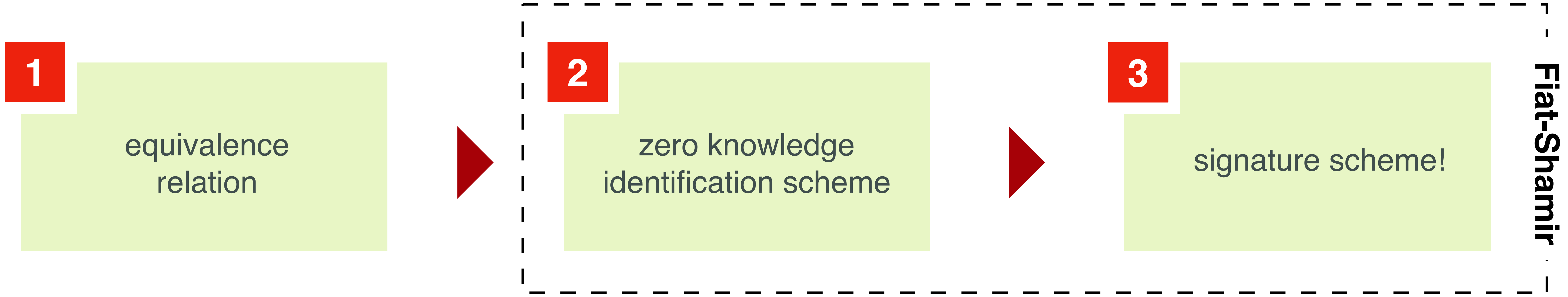
COMMIT

- Generate **ephemeral** $\tilde{A} \in \mathrm{GL}_\mathrm{m}(q)$, $\tilde{B} \in \mathrm{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathscr{C}} = \tilde{A}\mathscr{C}\tilde{B}$

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "{(\tilde{A}, \tilde{B})}"] \arrow[d, "{(A, B)}"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "{(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})}"] &
\end{tikzcd}$$

2

From MCE to MEDS



1 → 2

SETUP

- Assume parameter set q, n, m, k. and “starting” code $\mathscr{C}$
- Generate **secret key** $A \in \mathrm{GL}_{\mathrm{m}}(q), B \in \mathrm{GL}_n(q)$
- Generate **public key** $\mathscr{D} = A\mathscr{C}B$

COMMIT

- Generate **ephemeral** $\tilde{A} \in \mathrm{GL}_{\mathrm{m}}(q), \tilde{B} \in \mathrm{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathscr{C}} = \tilde{A}\mathscr{C}\tilde{B}$

CHALLENGE

- Pick a bit $b \in \{0,1\}$

RESPONSE

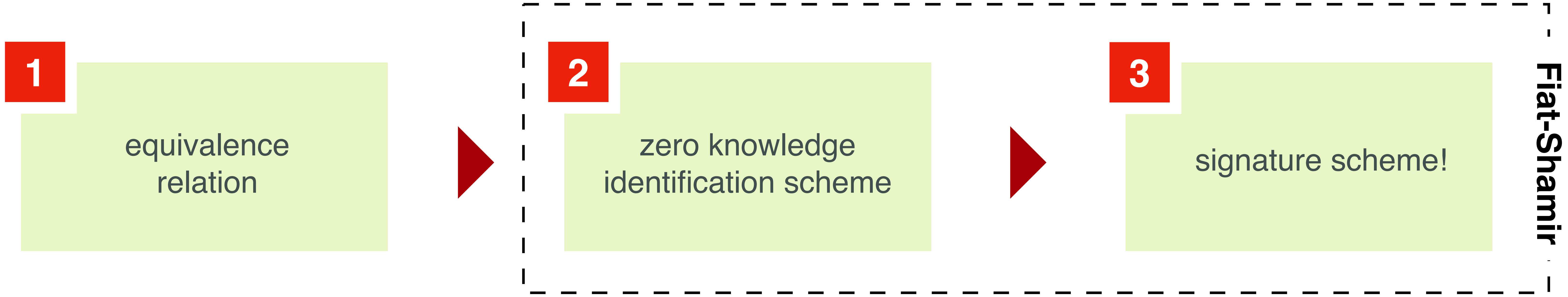
- if $b = 0$, reply with $(\tilde{A}, \tilde{B})$
- if $b = 1$, reply with $(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})$

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "(\tilde{A}, \tilde{B})"] \arrow[d, "(A, B)"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})"'] &
\end{tikzcd}$$

$$b = 0$$

2

From MCE to MEDS



1 → 2

SETUP

- Assume parameter set $q, n, m, k.$ and “starting” code $\mathscr{C}$
- Generate **secret key** $A \in \mathrm{GL}_m(q), B \in \mathrm{GL}_n(q)$
- Generate **public key** $\mathscr{D} = A\mathscr{C}B$

COMMIT

- Generate **ephemeral** $\tilde{A} \in \mathrm{GL}_m(q), \tilde{B} \in \mathrm{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathscr{C}} = \tilde{A}\mathscr{C}\tilde{B}$

CHALLENGE

- Pick a bit $b \in \{0,1\}$

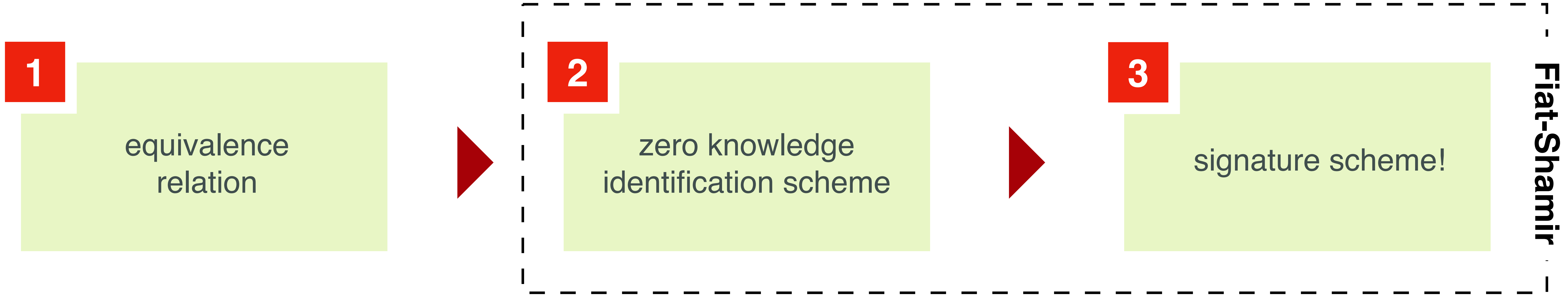
RESPONSE

- if $b = 0$, reply with $(\tilde{A}, \tilde{B})$
- if $b = 1$, reply with $(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})$

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "(\tilde{A}, \tilde{B})"] \arrow[d, "(A, B)"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})"] &
\end{tikzcd}$$

$b = 1$

From MCE to MEDS



1 equivalence relation

2 zero knowledge identification scheme

3 signature scheme!

Fiat-Shamir

1 → 2

SETUP

- Assume parameter set $q, n, m, k.$ and “starting” code $\mathscr{C}$
- Generate **secret key** $A \in \mathrm{GL}_m(q)$, $B \in \mathrm{GL}_n(q)$
- Generate **public key** $\mathscr{D} = A\mathscr{C}B$

COMMIT

- Generate **ephemeral** $\tilde{A} \in \mathrm{GL}_m(q)$, $\tilde{B} \in \mathrm{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathscr{C}} = \tilde{A}\mathscr{C}\tilde{B}$

CHALLENGE

- Pick a bit $b \in \{0,1\}$

RESPONSE

- if $b = 0$, reply with $(\tilde{A}, \tilde{B})$
- if $b = 1$, reply with $(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})$

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "{(\tilde{A}, \tilde{B})}"] \arrow[d, "{(A, B)}"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "{(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})}"] &
\end{tikzcd}$$

soundness 1/2

2

From MCE to MEDS

naive approach

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "{(\tilde{A}, \tilde{B})}"] \arrow[d, "{(A, B)}"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "{(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})}"] &
\end{tikzcd}$$

repeat t times

$$\begin{tikzcd}
\mathscr{C} \arrow[d] & \mathscr{C} \arrow[d] & \mathscr{C} \arrow[d] & \mathscr{C} \arrow[d] & \mathscr{C} \arrow[d] \arrow[r, "{(\tilde{A}, \tilde{B})(\tilde{A}, \tilde{B})(\tilde{A}, \tilde{\tilde{B}})(\tilde{A}, \tilde{\tilde{B}})(\tilde{A}, \tilde{\tilde{B}})}"] & \tilde{\mathscr{C}} \\
\mathscr{D} & \mathscr{D} & \mathscr{D} & \mathscr{D} & \mathscr{D} \arrow[ur, "{(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})}"] &
\end{tikzcd}$$

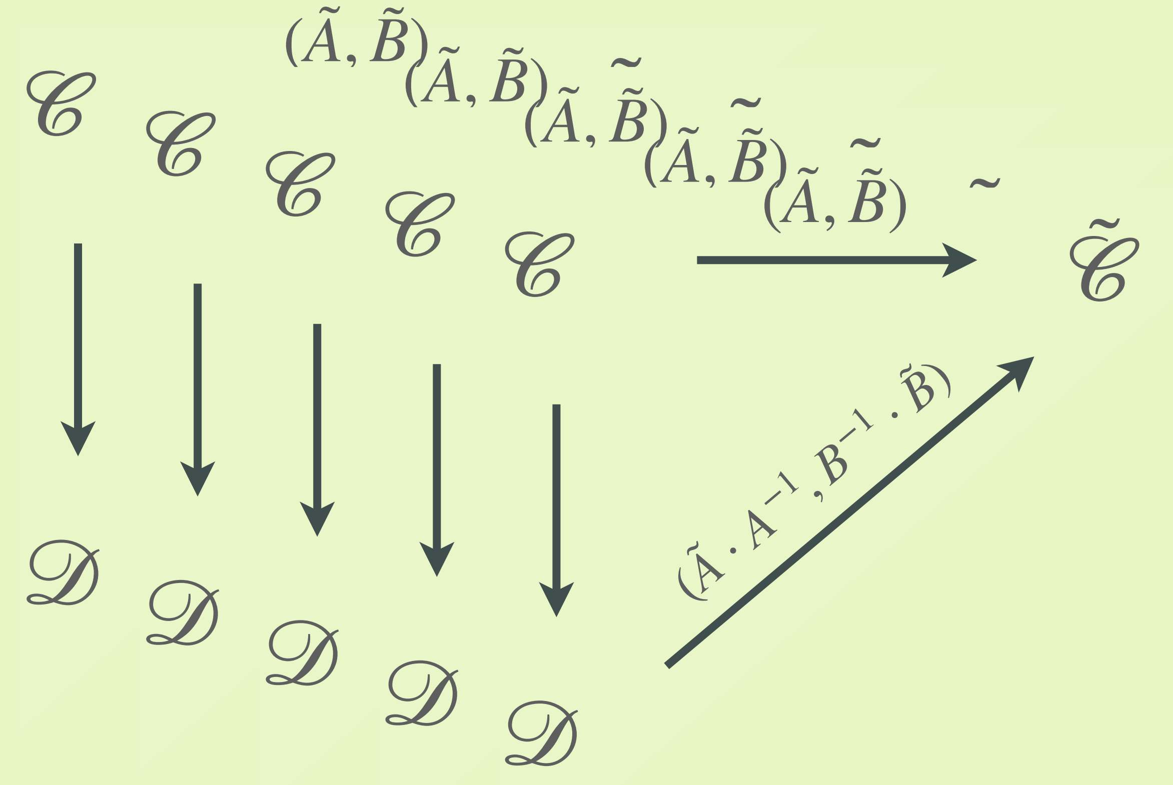
2

From MCE to MEDS

naive approach

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "(\tilde{A}, \tilde{B})"] \arrow[d, "(A, B)"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})"] &
\end{tikzcd}$$

repeat t times



1

[1]

multiple pk

$$\begin{tikzcd}
 & \mathscr{C} \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathscr{D}_1 \cdots & \mathscr{D}_i & \cdots \mathscr{D}_s
\end{tikzcd}$$

provide s public keys,
$b \in \{1, \ldots, s\}$
response is an isometry
$\mathscr{D}_b \to \tilde{\mathscr{C}}$ or $\mathscr{C} \to \tilde{\mathscr{C}}$

[1] L. De Feo and S. D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. EUROCRYPT 2019.
[2] W. Beullens, S, Katsumata, and F. Pintore. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. ASIACRYPT 2020.

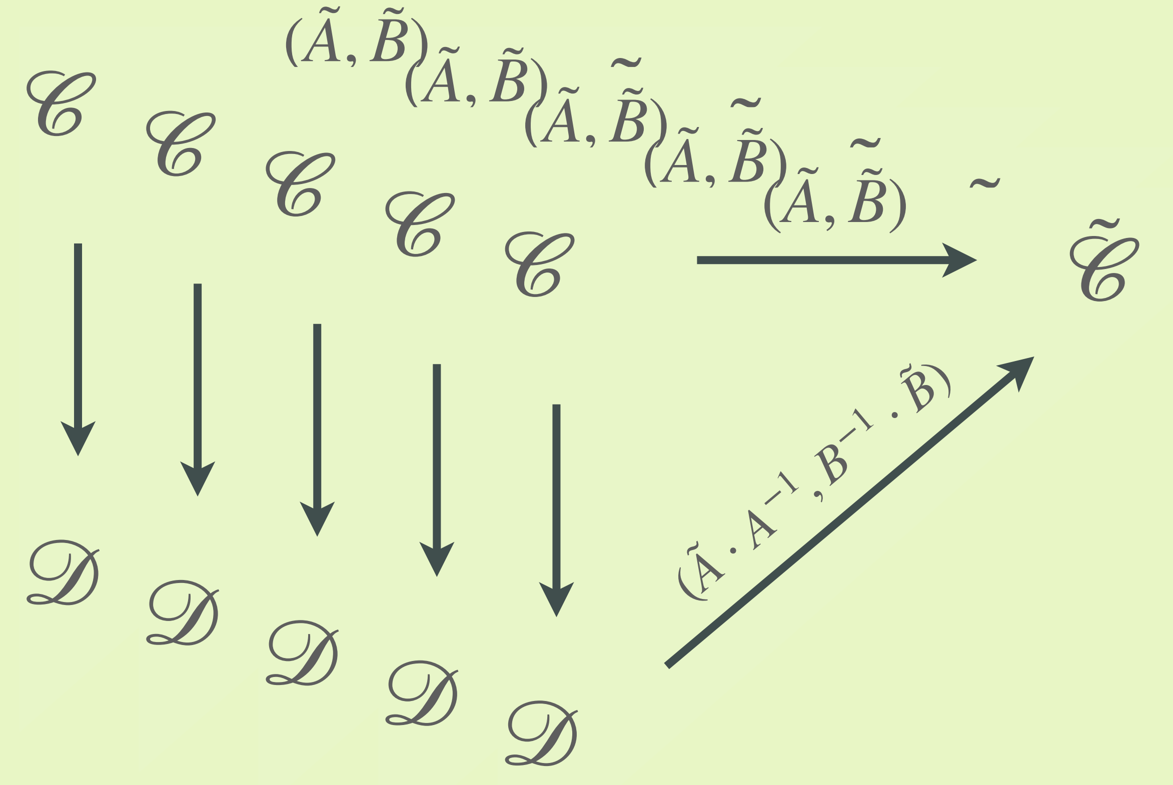
2

From MCE to MEDS

naive approach

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "(\tilde{A},\tilde{B})"] \arrow[d, "(A,B)"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "(\tilde{A}\cdot A^{-1},B^{-1}\cdot\tilde{B})"] &
\end{tikzcd}$$

repeat t times



1

multiple pk

[1]

$$\begin{tikzcd}
 & \mathscr{C} \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathscr{D}_1 \cdots & \mathscr{D}_i & \cdots \mathscr{D}_s
\end{tikzcd}$$

provide s public keys, $b \in \{1,\ldots,s\}$ response is an isometry $\mathscr{D}_b \to \tilde{\mathscr{C}}$ or $\mathscr{C} \to \tilde{\mathscr{C}}$

2

fix weight

[2]

- generate $\mathscr{C} \to \tilde{\mathscr{C}}$ from seed
- respond to $b = 0$ with seed
- response much cheaper!

▼

adjust probability so that $b = 0$ appears more

[1] L. De Feo and S. D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. EUROCRYPT 2019.
[2] W. Beullens, S, Katsumata, and F. Pintore. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. ASIACRYPT 2020.

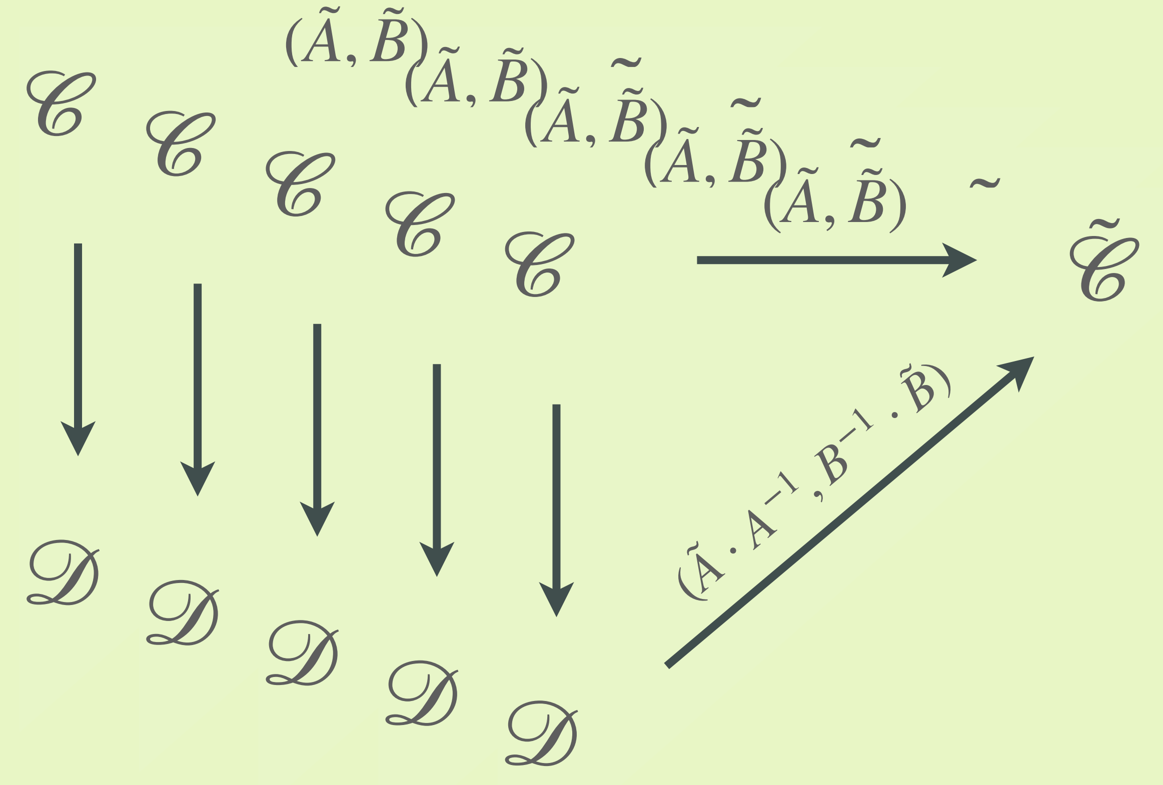
2

From MCE to MEDS

naive approach

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "(\tilde{A}, \tilde{B})"] \arrow[d, "(A, B)"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})"] &
\end{tikzcd}$$

repeat t times



1 multiple pk [1]

$$\begin{tikzcd}
 & \mathscr{C} \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathscr{D}_1 \cdots & \mathscr{D}_i & \cdots \mathscr{D}_s
\end{tikzcd}$$

provide s public keys, $b \in \{1, \ldots, s\}$
response is an isometry $\mathscr{D}_b \to \tilde{\mathscr{C}}$ or $\mathscr{C} \to \tilde{\mathscr{C}}$

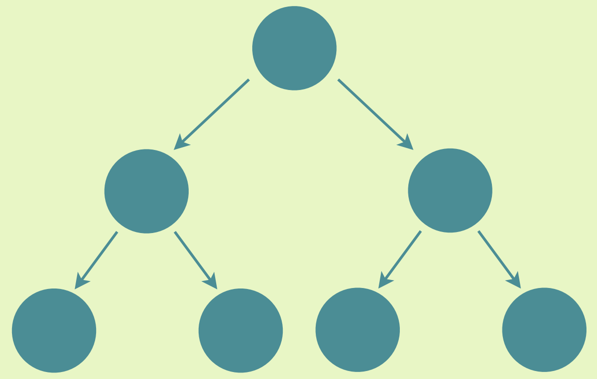
2 fix weight [2]

- generate $\mathscr{C} \to \tilde{\mathscr{C}}$ from seed
- respond to $b = 0$ with seed
- response much cheaper!

adjust probability so that $b = 0$ appears more

3 seed tree [2]

instead of sending t seeds, send tree



to reveal nodes $N_1, \ldots, N_w$, communicate $N_1 \ldots, N_w$ and for the $t - w$ remaining nodes only appropriate parent nodes

[1] L. De Feo and S. D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. EUROCRYPT 2019.
[2] W. Beullens, S, Katsumata, and F. Pintore. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. ASIACRYPT 2020.

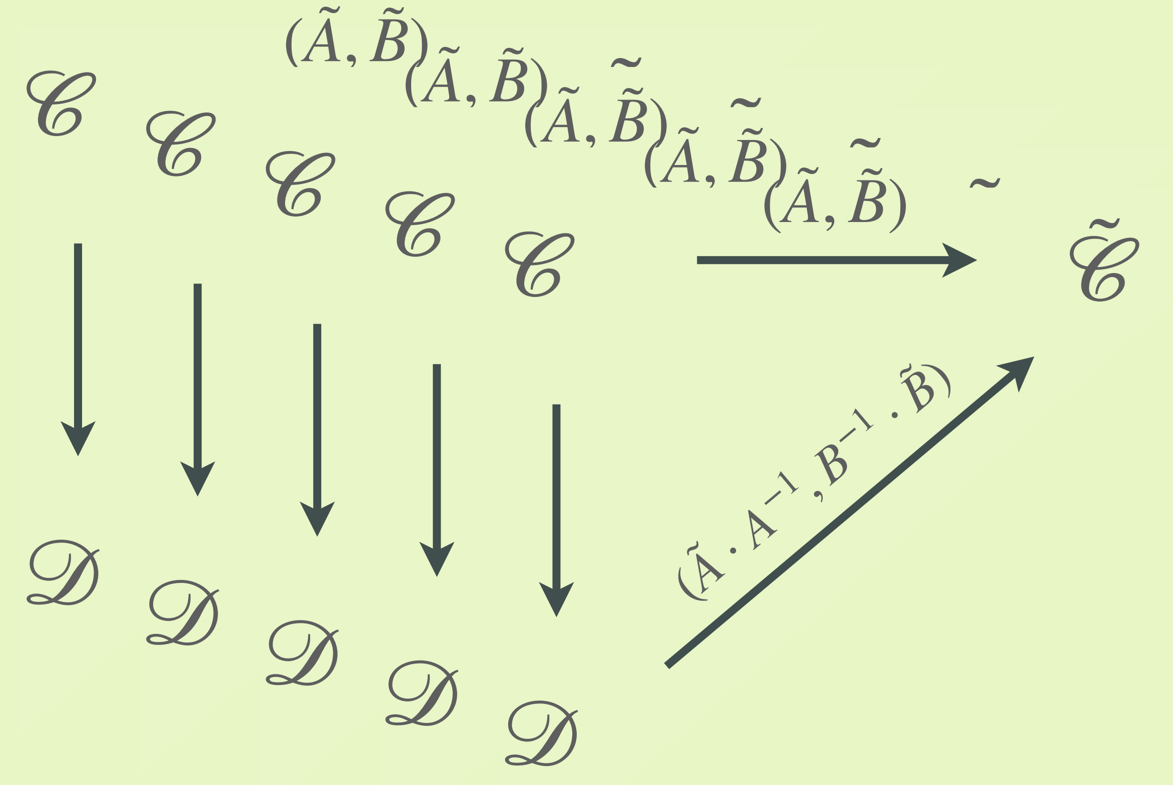
2

From MCE to MEDS

naive approach

$$\begin{tikzcd} \mathscr{C} \arrow[r, "(\tilde{A},\tilde{B})"] \arrow[d, "(A,B)"'] & \tilde{\mathscr{C}} \\ \mathscr{D} \arrow[ur, "(\tilde{A}\cdot A^{-1},B^{-1}\cdot\tilde{B})"] & \end{tikzcd}$$

repeat t times



1 multiple pk [1]

$$\begin{tikzcd} & & \mathscr{C} \arrow[dll] \arrow[d] \arrow[drr] & & \\ \mathscr{D}_1 & \cdots & \mathscr{D}_i & \cdots & \mathscr{D}_s \end{tikzcd}$$

provide s public keys,
$b \in \{1,\ldots,s\}$
response is an isometry
$\mathscr{D}_b \to \tilde{\mathscr{C}}$ or $\mathscr{C} \to \tilde{\mathscr{C}}$

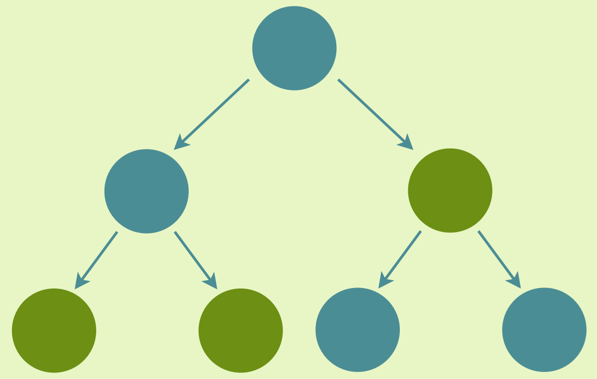
2 fix weight [2]

- generate $\mathscr{C} \to \tilde{\mathscr{C}}$ from seed
- respond to $b = 0$ with seed
- response much cheaper!

adjust probability so that
$b = 0$ appears more

3 seed tree [2]

instead of sending t seeds, send tree



to reveal nodes $N_1,\ldots,N_w$,
communicate $N_1\ldots,N_w$ and for the
$t-w$ remaining nodes only appropriate
parent nodes

[1] L. De Feo and S. D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. EUROCRYPT 2019.
[2] W. Beullens, S, Katsumata, and F. Pintore. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. ASIACRYPT 2020.

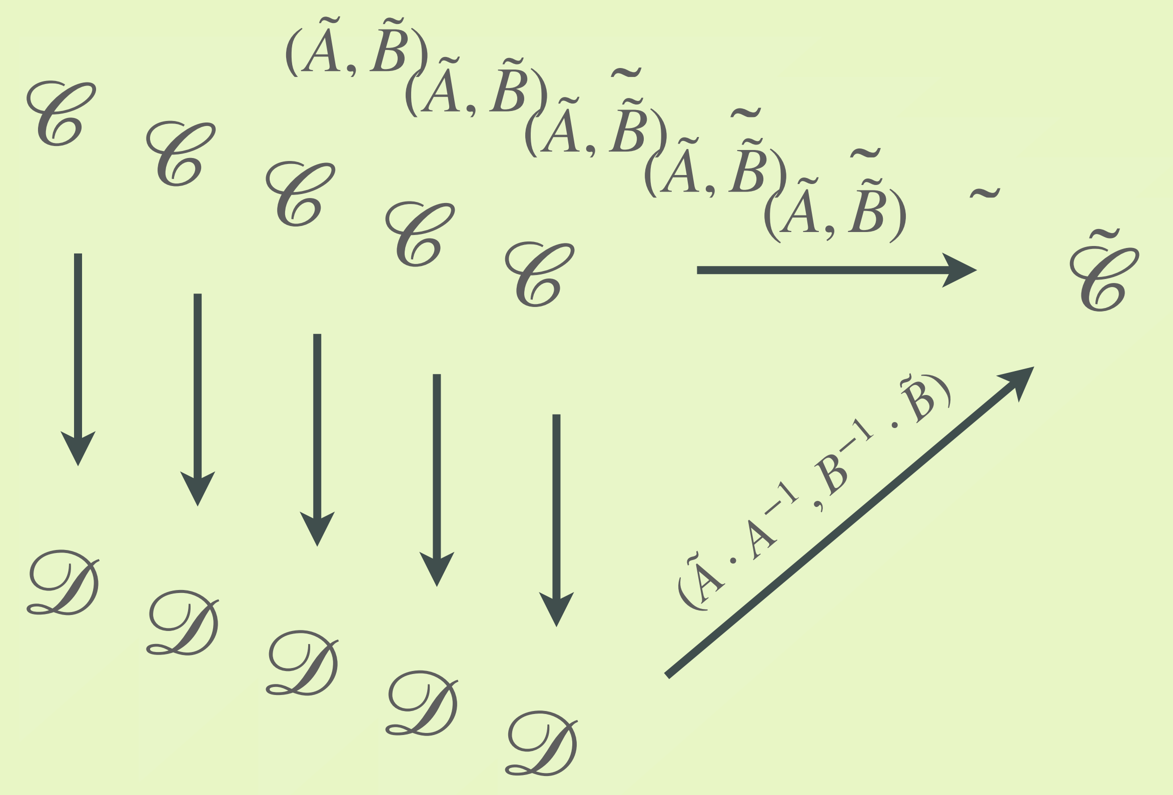
2

From MCE to MEDS

naive approach

$$\begin{tikzcd}
\mathscr{C} \arrow[r, "(\tilde{A}, \tilde{B})"] \arrow[d, "(A, B)"'] & \tilde{\mathscr{C}} \\
\mathscr{D} \arrow[ur, "(\tilde{A} \cdot A^{-1}, B^{-1} \cdot \tilde{B})"] &
\end{tikzcd}$$

repeat t times



1 multiple pk

[1]

$$\begin{tikzcd}
 & \mathscr{C} \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathscr{D}_1 \cdots & \mathscr{D}_i & \cdots \mathscr{D}_s
\end{tikzcd}$$

provide s public keys,
$b \in \{1, \ldots, s\}$
response is an isometry
$\mathscr{D}_b \to \tilde{\mathscr{C}}$ or $\mathscr{C} \to \tilde{\mathscr{C}}$

2 fix weight

[2]

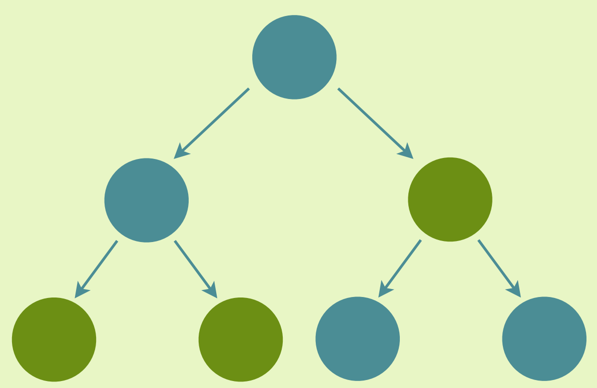
- generate $\mathscr{C} \to \tilde{\mathscr{C}}$ from seed
- respond to $b = 0$ with seed
- response much cheaper!

adjust probability so that
$b = 0$ appears more

3 seed tree

[2]

instead of sending t seeds, send tree



to reveal nodes $N_1, \ldots, N_w$,
communicate $N_1 \ldots, N_w$ and for the
$t - w$ remaining nodes only appropriate
parent nodes

4 compression

[3,4]

instead of generating A_i, B_i from seed
and computing $\mathscr{D}_i = A_i \cdot \mathscr{C} \cdot B_i$

generate part of $\mathscr{D}_i$ from seed.
compute appropriate A_i, B_i
and rest of $\mathscr{D}_i$

Note: this does not break MCE!

[3] J. Ding, M-S Chen, A. Petzoldt, D. Schmidt, B-Y. Yang, M. Kannwischer, and J. Patarin. Rainbow. NIST 2020.
[4] W. Beullens, M-S. Chen, S-H. Hung, M. Kannwischer, B. Peng, C-J. Shih, and B-Y. Yang. Oil and Vinegar: Modern parameters and implementations.

Performance of MEDS

3

Performance

parameters	q	n = m = k	t	s	w	Public Key	Signature	Keygen	Signing	Verification
			(rounds)	(no. of pk's)	(seed tree)	(bytes)	(bytes)	(ms)	(ms)	(ms)
MEDS-9923	4093	14	1152	4	14	9923	9896	1.00	272.66	271.36
MEDS-13220	4093	14	192	5	20	13220	12976	1.32	46.79	46.04
MEDS-41711	4093	22	608	4	26	41711	41080	5.16	772.10	769.46
MEDS-69497	4093	22	160	5	36	55604	54736	6.75	203.83	200.37
MEDS-134180	2039	30	192	5	52	134180	132528	23.55	857.81	848.72
MEDS-167717	2039	30	112	6	66	167717	165464	29.39	506.21	494.15

3

Performance

parameters	q	n = m = k	t (rounds)	s (no. of pk's)	w (seed tree)	**Public Key** (bytes)	**Signature** (bytes)	**Keygen** (ms)	**Signing** (ms)	**Verification** (ms)
MEDS-9923	4093	14	1152	4	14	9923	9896	1.00	272.66	271.36
MEDS-13220	4093	14	192	5	20	13220	12976	1.32	46.79	46.04
MEDS-41711	4093	22	608	4	26	41711	41080	5.16	772.10	769.46
MEDS-69497	4093	22	160	5	36	55604	54736	6.75	203.83	200.37
MEDS-134180	2039	30	192	5	52	134180	132528	23.55	857.81	848.72
MEDS-167717	2039	30	112	6	66	167717	165464	29.39	506.21	494.15

advantages

- single hardness assumption: **MCE**
- simple design and arithmetic
- great flexibility in sizes
- *generic*: room for improvements!

3

Performance

parameters	q	n = m = k	t (rounds)	s (no. of pk's)	w (seed tree)	Public Key (bytes)	Signature (bytes)	Keygen (ms)	Signing (ms)	Verification (ms)
MEDS-9923	4093	14	1152	4	14	9923	9896	1.00	272.66	271.36
MEDS-13220	4093	14	192	5	20	13220	12976	1.32	46.79	46.04
MEDS-41711	4093	22	608	4	26	41711	41080	5.16	772.10	769.46
MEDS-69497	4093	22	160	5	36	55604	54736	6.75	203.83	200.37
MEDS-134180	2039	30	192	5	52	134180	132528	23.55	857.81	848.72
MEDS-167717	2039	30	112	6	66	167717	165464	29.39	506.21	494.15

advantages

- single hardness assumption: **MCE**
- simple design and arithmetic
- great flexibility in sizes
- *generic*: room for improvements!

limitations

- resulting pk's and sig's still large
- scaling to higher parameters
- needs more research on **MCE**
- *opportunity*: lots of cool research!

3

Performance

parameters	q	n = m = k	t	s	w	Public Key	Signature	Keygen	Signing	Verification
			(rounds)	(no. of pk's)	(seed tree)	(bytes)	(bytes)	(ms)	(ms)	(ms)
MEDS-9923	4093	14	1152	4	14	9923	9896	1.00	272.66	271.36
MEDS-13220	4093	14	192	5	20	13220	12976	1.32	46.79	46.04
MEDS-41711	4093	22	608	4	26	41711	41080	5.16	772.10	769.46
MEDS-69497	4093	22	160	5	36	55604	54736	6.75	203.83	200.37
MEDS-134180	2039	30	192	5	52	134180	132528	23.55	857.81	848.72
MEDS-167717	2039	30	112	6	66	167717	165464	29.39	506.21	494.15

advantages

- single hardness assumption: **MCE**
- simple design and arithmetic
- great flexibility in sizes
- *generic*: room for improvements!

limitations

- resulting pk's and sig's still large
- scaling to higher parameters
- needs more research on **MCE**
- *opportunity*: lots of cool research!

advancing

- new technique to reduce sig. size
- MEDS-13220 to **2088** bytes (-84%)
- still analysing security of technique
- *explore*: potential for new ideas!

Thank you for your attention!

https://www.meds-pqc.org/