



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 \mathcal{C}_0
- Generate **secret key** $A \in \text{GL}_m(q), B \in \text{GL}_n(q)$
- Generate **public key** $\mathcal{C}_1 = A\mathcal{C}_0B$



COMMIT

- Generate **ephemeral** $\tilde{A} \in \text{GL}_m(q), \tilde{B} \in \text{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathcal{C}} = \tilde{A}\mathcal{C}_0\tilde{B}$

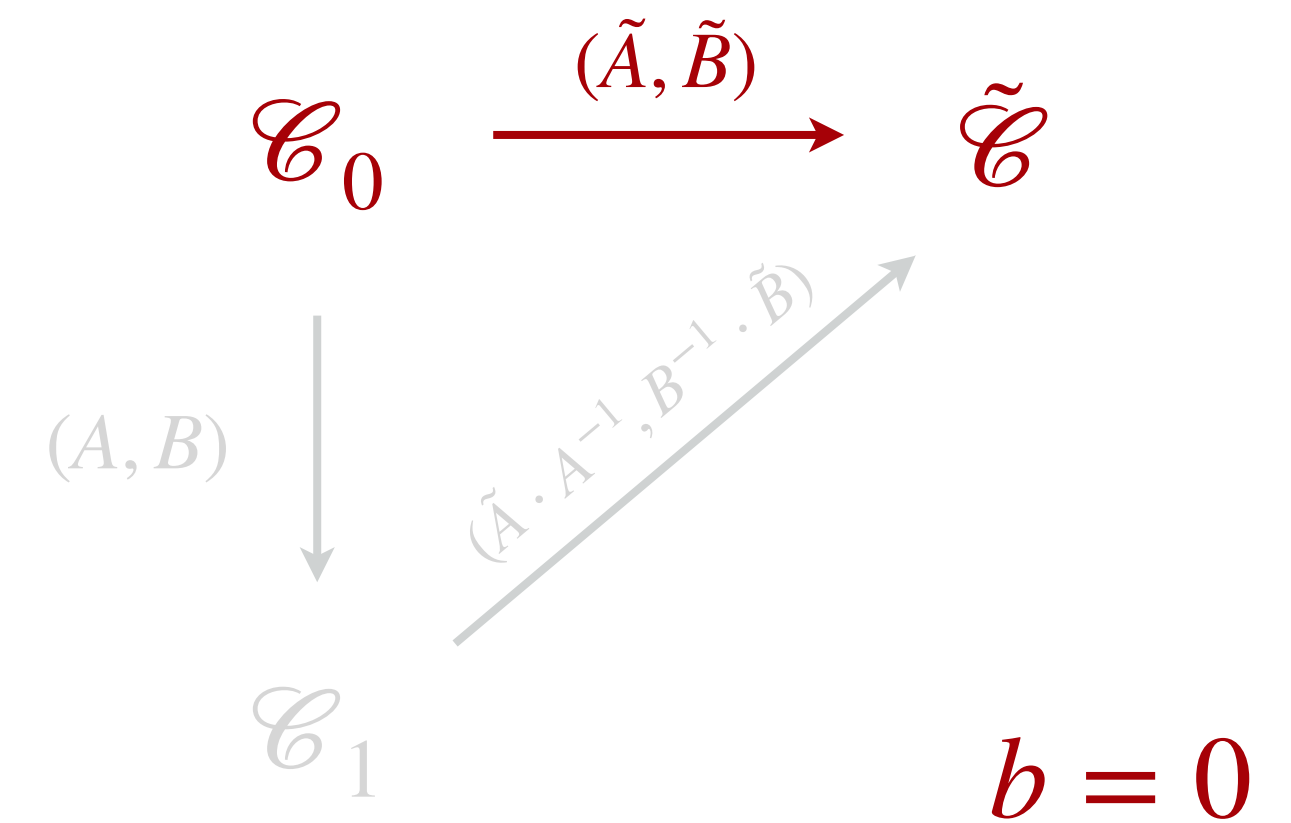
CHALLENGE

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



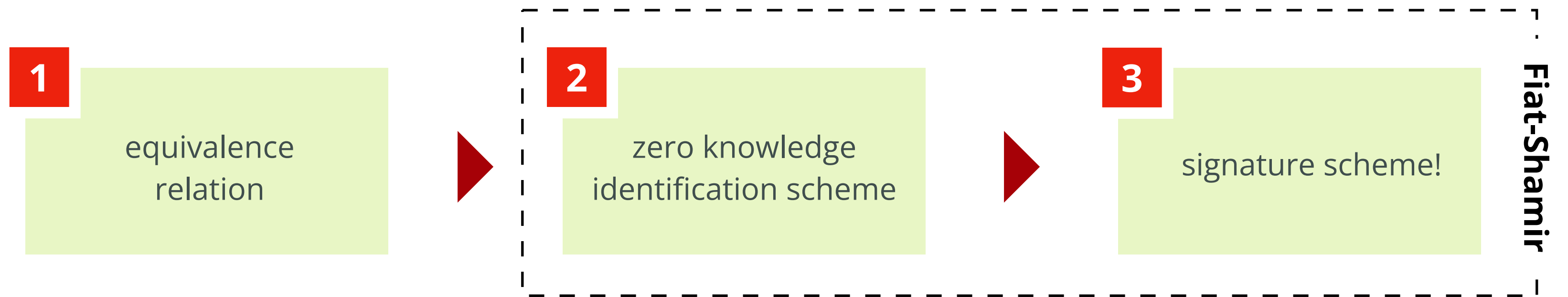
RESPONSE

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





From MCE
to MEDS



1 → 2

SETUP

- Assume parameter set q, n, m, k . and "starting" code \mathcal{C}_0
- Generate **secret key** $A \in \text{GL}_m(q), B \in \text{GL}_n(q)$
- Generate **public key** $\mathcal{C}_1 = A\mathcal{C}_0B$

COMMIT

- Generate **ephemeral** $\tilde{A} \in \text{GL}_m(q), \tilde{B} \in \text{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathcal{C}} = \tilde{A}\mathcal{C}_0\tilde{B}$

CHALLENGE

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

RESPONSE

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

