

1 → **2**

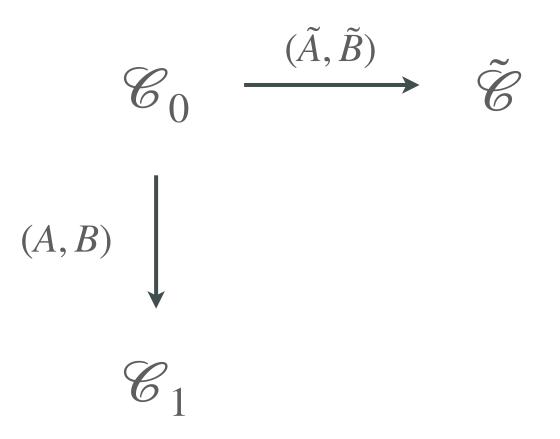
SETUP

- Assume parameter set q, n, m, k. and "starting" code \mathscr{C}_0
- Generate **secret key** $A \in GL_m(q)$, $B \in GL_n(q)$
- Generate **public key** $\mathscr{C}_1 = A\mathscr{C}_0 B$

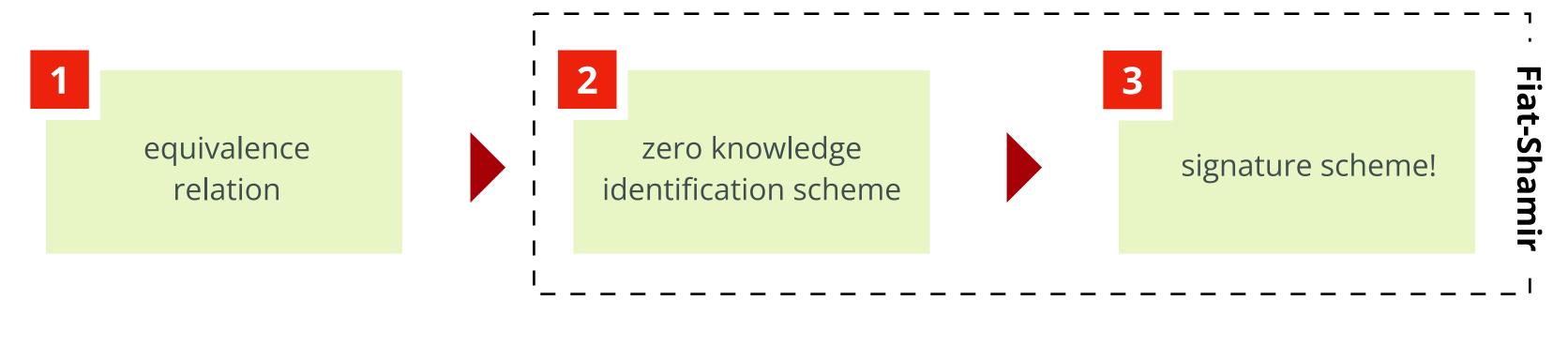


COMMIT

- Generate **ephemeral** $\tilde{A} \in \mathrm{GL}_{\mathrm{m}}(q)$, $\tilde{B} \in \mathrm{GL}_{n}(q)$
- Generate **ephemeral code** $\tilde{\mathscr{C}} = \tilde{A}\mathscr{C}_0\tilde{B}$







1 → **2**

SETUP

- Assume parameter set q, n, m, k. and "starting" code \mathscr{C}_0
- Generate **secret key** $A \in GL_m(q)$, $B \in GL_n(q)$
- Generate **public key** $\mathscr{C}_1 = A\mathscr{C}_0 B$



COMMIT

- Generate **ephemeral** $\tilde{A} \in GL_m(q)$, $\tilde{B} \in GL_n(q)$
- Generate **ephemeral code** $\tilde{\mathscr{C}} = \tilde{A}\mathscr{C}_0\tilde{B}$

