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

$$\mathscr{C}_0 \xrightarrow{(A,B)} \mathscr{C}_1$$

2

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

### COMMIT

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

$$\begin{array}{ccc} \mathscr{C}_0 & \xrightarrow{(\tilde{A},\tilde{B})} & \tilde{\mathscr{C}} \\ \\ (A,B)\downarrow & & \\ \\ \mathscr{C}_1 & & \end{array}$$