Implementable Witness Encryption from Arithmetic Affine Determinant Programs

[[alloc] init] Research Team (2026/175, 2026/1594)

Patrick Towa, Swiss Crypto Day, 4 September 2026

- What witness encryption is
- What it can be used for
- How to build a scheme
- How to break it
- How to fix it

Witness Encryption

NP Relation $\mathscr{R}$

Witness Encryption

NP Relation $\mathscr{R}$

$$\text{Enc}\left(1^{\lambda}, z, msg\right) \to C$$

Witness Encryption

NP Relation $\mathscr{R}$

$$\mathrm{Enc}\left(1^{\lambda}, z, msg\right) \to C$$

$$\mathrm{Dec}(w, C) \to msg$$

Witness Encryption

NP Relation $\mathscr{R}$

$\text{Enc}\left(1^{\lambda}, z, msg\right) \rightarrow C$ $\quad$ $z \iff$ 🔓

$\text{Dec}(w, C) \rightarrow msg$ $\quad$ $w \iff$ 🔑

Witness Encryption

NP Relation $\mathscr{R}$

$\text{Enc}\left(1^{\lambda}, z, msg\right) \to C$ $\qquad z \iff$ 🔓

$\text{Dec}(w, C) \to msg$ $\qquad w \iff$ 🔑

Soundness $\qquad z \notin \mathscr{L} \implies$ 🔒

Witness Encryption

NP Relation $\mathscr{R}$

$\mathrm{Enc}\left(1^\lambda, z, msg\right) \to C$ $\quad z \iff$ 🔓

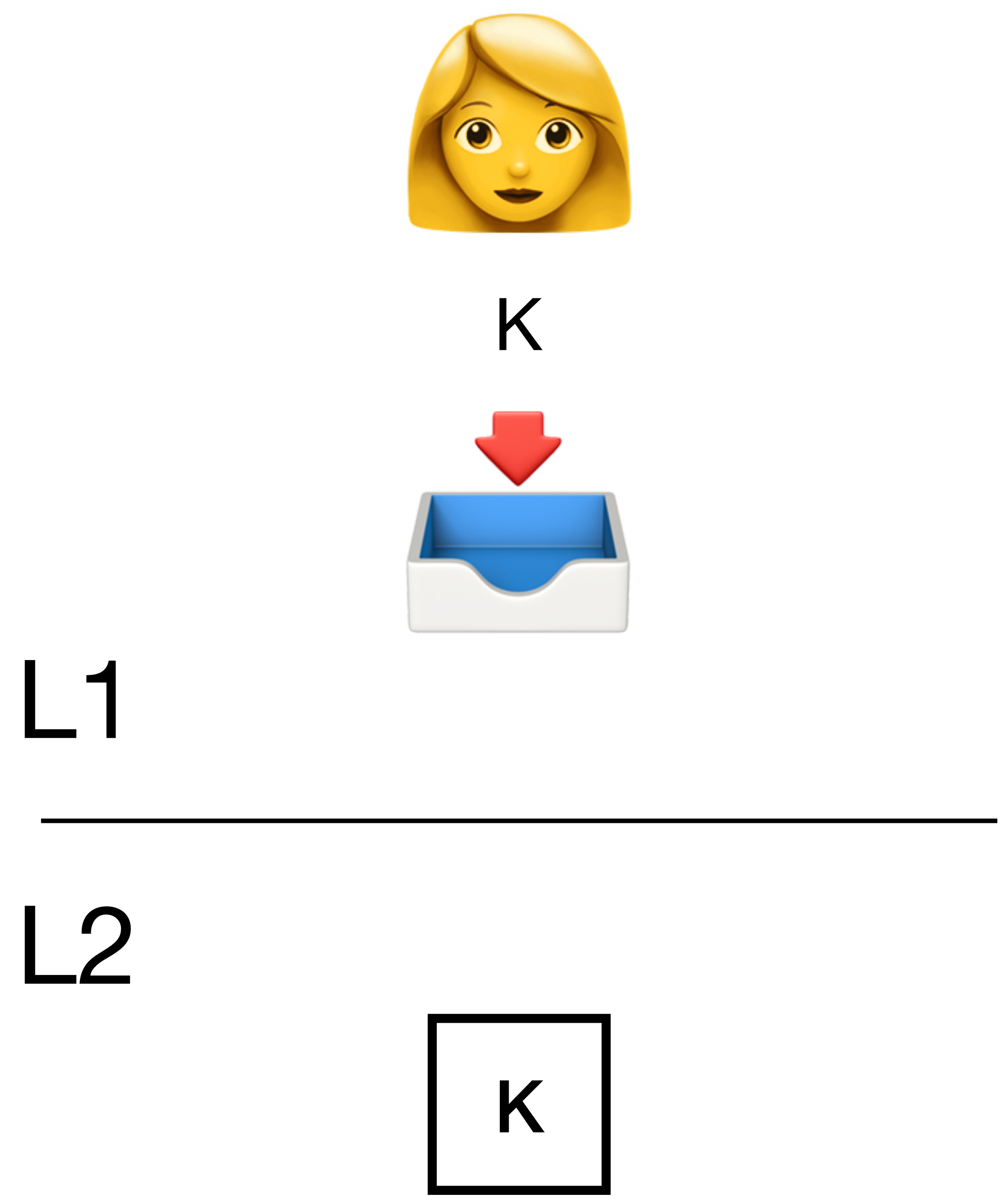
$\mathrm{Dec}(w, C) \to msg$ $\quad w \iff$ 🔑

Soundness $\quad z \notin \mathscr{L} \implies$ 🔒

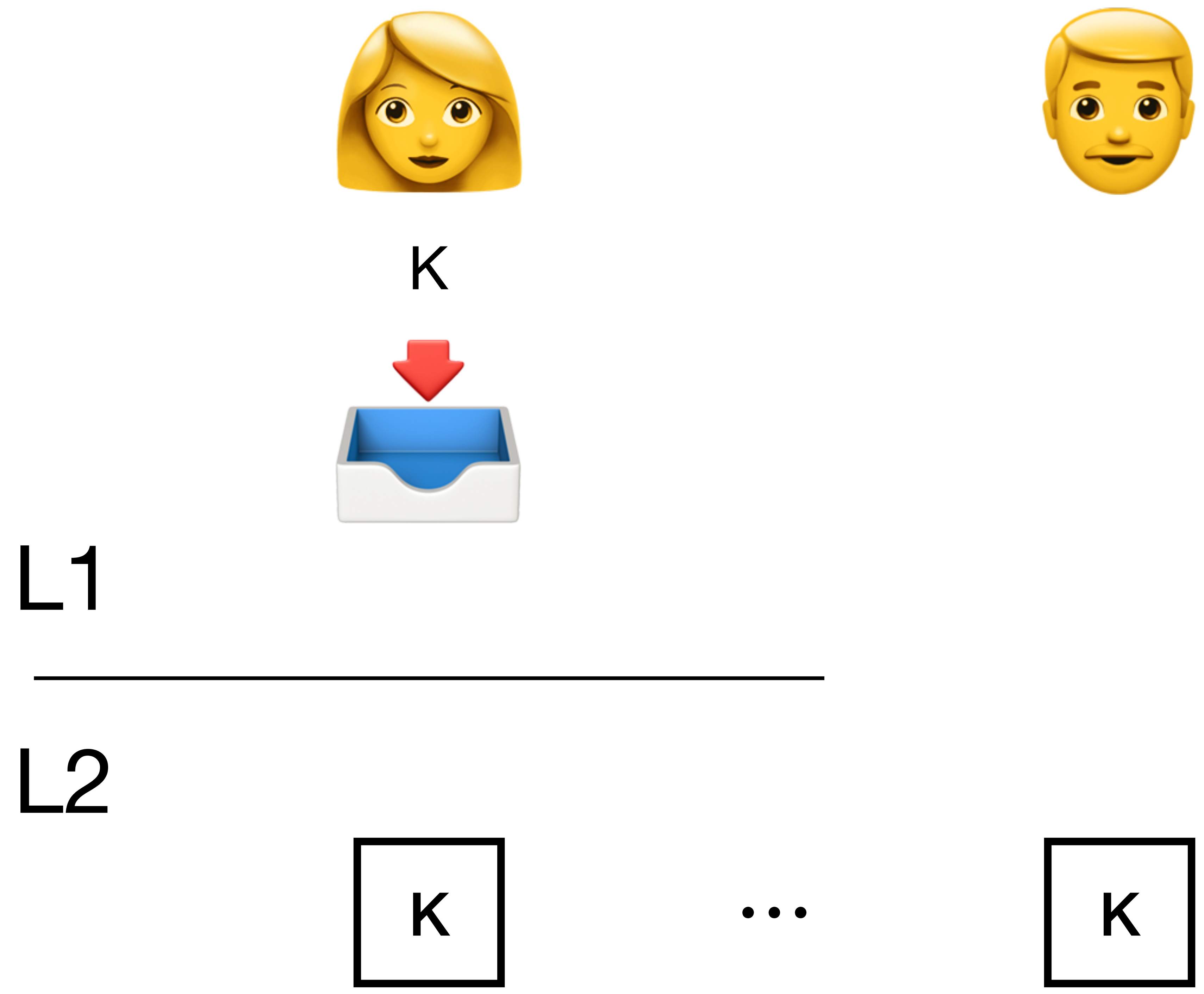
Extractability $\quad$ ⚙️ $\implies w \in \mathscr{R}(z)$

📫 😈

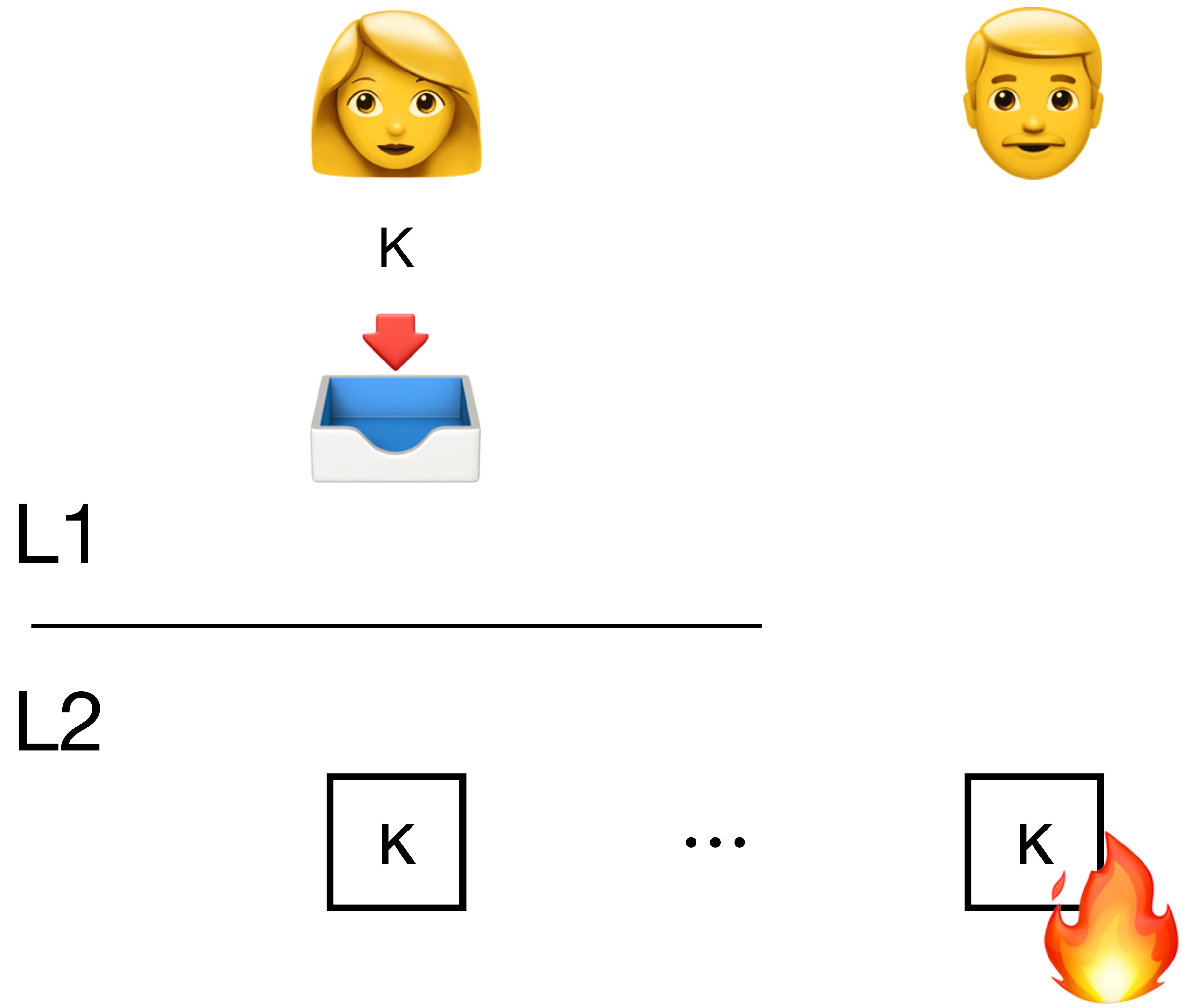
Application: BTC Vaults



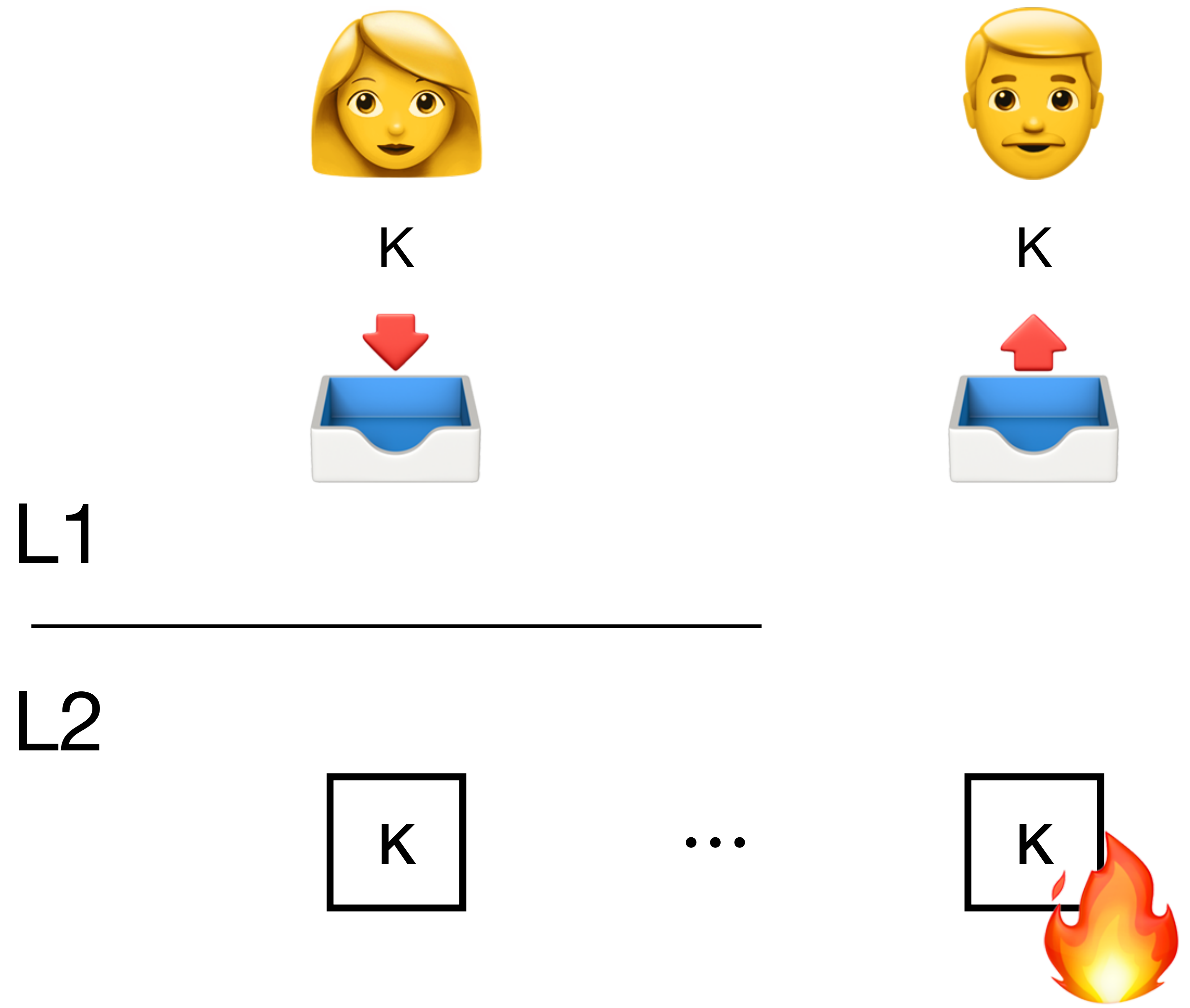
Application: BTC Vaults



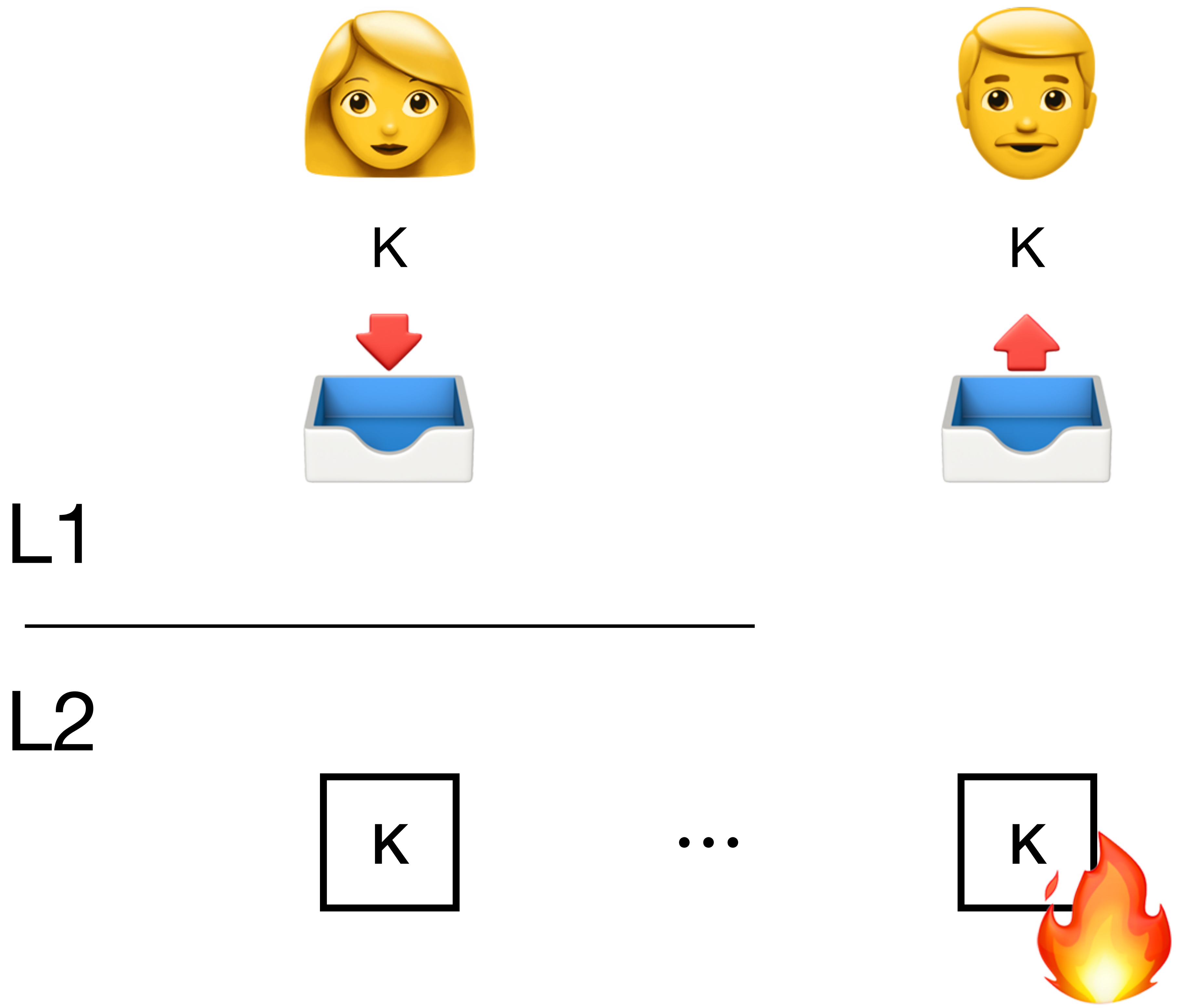
Application: BTC Vaults



Application: BTC Vaults



Application: BTC Vaults



Programmability, privacy without on-chain proof verification!

Constraint System

$A, B, C, D \in \mathbb{F}^{m \times (n+1)}$

Constraint System

$A, B, C, D \in \mathbb{F}^{m \times (n+1)}$

$x \neq 0$

$$\boxed{A}\,\boxed{x} * \boxed{B}\,\boxed{x} = \boxed{C}\,\boxed{x} * \boxed{D}\,\boxed{x}$$

Constraint System

$A, B, C, D \in \mathbb{F}^{m \times (n+1)}$

$$\forall i: \left(\sum_{j=0}^{n} a_i^j x_j\right)\left(\sum_{j=0}^{n} b_i^j x_j\right) = \left(\sum_{j=0}^{n} c_i^j x_j\right)\left(\sum_{j=0}^{n} d_i^j x_j\right)$$

Constraint System

$A, B, C, D \in \mathbb{F}^{m\times(n+1)}$

$$\forall i: \left(\sum_{j=0}^{n} a_i^j x_j\right)\left(\sum_{j=0}^{n} b_i^j x_j\right) = \left(\sum_{j=0}^{n} c_i^j x_j\right)\left(\sum_{j=0}^{n} d_i^j x_j\right)$$

$x_0 = 1$ affine solution

$x_0 = 0$ solution at ∞

Constraint System

Projective Safety

$$X_0 \prec X_1 \prec \cdots \prec X_n$$

Constraint System

Projective Safety

$$X_0 \prec X_1 \prec \cdots \prec X_n$$

$$X_{i+1}^2 = a(X_0, \ldots, X_i) \cdot b(X_0, \ldots, X_n)$$

Constraint System

Projective Safety

$$X_0 \prec X_1 \prec \cdots \prec X_n$$

$$X_{i+1}^2 = a(X_0, \ldots, X_i) \cdot b(X_0, \ldots, X_n)$$

$$X_{i+1}^2 = X_0 X_{i+1}$$

Constraint System

Projective Safety

$$X_0 \prec X_1 \prec \cdots \prec X_n$$

$$X_{i+1}^2 = a(X_0, \ldots, X_i) \cdot b(X_0, \ldots, X_n)$$

$$X_{i+1}^2 = X_0 X_{i+1}$$

Projective safety $\Longrightarrow$ no solution at ∞

Scheme

Goal: build an arithmetic affine determinant program.

$\left(M_i^j\right)_{i,j}$ such that a $\det(M(x)) = 0 \iff x$ is valid.

Scheme

Goal: build an arithmetic affine determinant program.

$\left(M_i^j\right)_{i,j}$ such that a $\det(M(x)) = 0 \iff x$ is valid.

High degree in witness vars.

Scheme

Goal: build an arithmetic affine determinant program.

$\left(M_i^j\right)_{i,j}$ such that a $\det(M(x)) = 0 \iff x$ is valid.

One time security: $M(x)$ simulatable knowing only $\det\left(M(x)\right)$

Scheme

$$a_i(x)b_i(x) - c_i(x)d_i(x)$$

$$a_i(x) = \sum_{j=0}^{n} a_i^j x_j$$

Scheme

$a_i(x)b_i(x) - c_i(x)d_i(x)$

$$\begin{bmatrix} a_i & c_i & -\xi_i & 0 \\ d_i & b_i & 0 & \xi_i \\ 0 & 0 & b_i & a_i \\ 0 & 0 & d_i & c_i \end{bmatrix}$$

Scheme

$a_i(x)b_i(x) - c_i(x)d_i(x)$

$$\begin{bmatrix} a_i & c_i & -\xi_i & 0 \\ d_i & b_i & 0 & \xi_i \\ 0 & 0 & b_i & a_i \\ 0 & 0 & d_i & c_i \end{bmatrix}$$

$= 0 \implies \text{rank} = 2$

Scheme

$$a_i(x)b_i(x) - c_i(x)d_i(x)$$

$$\begin{bmatrix} a_i & c_i & -\xi_i & 0 \\ d_i & b_i & 0 & \xi_i \\ 0 & 0 & b_i & a_i \\ 0 & 0 & d_i & c_i \end{bmatrix}$$

$$= 0 \implies \text{rank} = 2$$

$$\neq 0 \implies \text{rank} = 4$$

Scheme

$$a_i(x) = \sum_{j=0}^{n} a_i^j x_j$$

$$\begin{bmatrix} a_i^0 & c_i^0 & -\xi_i^0 & 0 \\ d_i^0 & b_i^0 & 0 & \xi_i^0 \\ 0 & 0 & b_i^0 & a_i^0 \\ 0 & 0 & d_i^0 & c_i^0 \end{bmatrix} \quad \begin{bmatrix} a_i^1 & c_i^1 & -\xi_i^1 & 0 \\ d_i^1 & b_i^1 & 0 & \xi_i^1 \\ 0 & 0 & b_i^1 & a_i^1 \\ 0 & 0 & d_i^1 & c_i^1 \end{bmatrix} \quad \cdots \quad \begin{bmatrix} a_i^n & c_i^n & -\xi_i^n & 0 \\ d_i^n & b_i^n & 0 & \xi_i^n \\ 0 & 0 & b_i^n & a_i^n \\ 0 & 0 & d_i^n & c_i^n \end{bmatrix}$$

Scheme

$$\begin{bmatrix} a_i^0 & c_i^0 & -\xi_i^0 & 0 \\ d_i^0 & b_i^0 & 0 & \xi_i^0 \\ 0 & 0 & b_i^0 & a_i^0 \\ 0 & 0 & d_i^0 & c_i^0 \end{bmatrix} \quad \begin{bmatrix} a_i^1 & c_i^1 & -\xi_i^1 & 0 \\ d_i^1 & b_i^1 & 0 & \xi_i^1 \\ 0 & 0 & b_i^1 & a_i^1 \\ 0 & 0 & d_i^1 & c_i^1 \end{bmatrix} \quad \cdots \quad \begin{bmatrix} a_i^n & c_i^n & -\xi_i^n & 0 \\ d_i^n & b_i^n & 0 & \xi_i^n \\ 0 & 0 & b_i^n & a_i^n \\ 0 & 0 & d_i^n & c_i^n \end{bmatrix}$$

x

Scheme

$$\begin{bmatrix} a_i^0 & c_i^0 & -\xi_i^0 & 0 \\ d_i^0 & b_i^0 & 0 & \xi_i^0 \\ 0 & 0 & b_i^0 & a_i^0 \\ 0 & 0 & d_i^0 & c_i^0 \end{bmatrix} \quad \begin{bmatrix} a_i^1 & c_i^1 & -\xi_i^1 & 0 \\ d_i^1 & b_i^1 & 0 & \xi_i^1 \\ 0 & 0 & b_i^1 & a_i^1 \\ 0 & 0 & d_i^1 & c_i^1 \end{bmatrix} \quad \cdots \quad \begin{bmatrix} a_i^n & c_i^n & -\xi_i^n & 0 \\ d_i^n & b_i^n & 0 & \xi_i^n \\ 0 & 0 & b_i^n & a_i^n \\ 0 & 0 & d_i^n & c_i^n \end{bmatrix}$$

$$\xleftarrow{\;x\;} \begin{bmatrix} a_i(x) & c_i(x) & -\xi_i(x) & 0 \\ d_i(x) & b_i(x) & 0 & \xi_i(x) \\ 0 & 0 & b_i(x) & a_i(x) \\ 0 & 0 & d_i(x) & c_i(x) \end{bmatrix}$$

Scheme

$$U_i^j \leftarrow \begin{bmatrix} a_i^j & c_i^j & -\xi_i^j & 0 \\ d_i^j & b_i^j & 0 & \xi_i^j \\ 0 & 0 & b_i^j & a_i^j \\ 0 & 0 & d_i^j & c_i^j \end{bmatrix}$$

Scheme

$$U_i^j \leftarrow \begin{bmatrix} a_i^j & c_i^j & -\xi_i^j & 0 \\ d_i^j & b_i^j & 0 & \xi_i^j \\ 0 & 0 & b_i^j & a_i^j \\ 0 & 0 & d_i^j & c_i^j \end{bmatrix}$$

$$L_i \in_R \mathbb{F}^{2m+1\times 4}, R_i \in_R \mathbb{F}^{4\times 2m+1}$$

Scheme

$$U_i^j \leftarrow \begin{bmatrix} a_i^j & c_i^j & -\xi_i^j & 0 \\ d_i^j & b_i^j & 0 & \xi_i^j \\ 0 & 0 & b_i^j & a_i^j \\ 0 & 0 & d_i^j & c_i^j \end{bmatrix}$$

$$L_i \in_R \mathbb{F}^{2m+1\times 4}, R_i \in_R \mathbb{F}^{4\times 2m+1}$$

$$M_i^j \leftarrow L_i U_i^j R_i \in \mathbb{F}^{2m+1}$$

Scheme

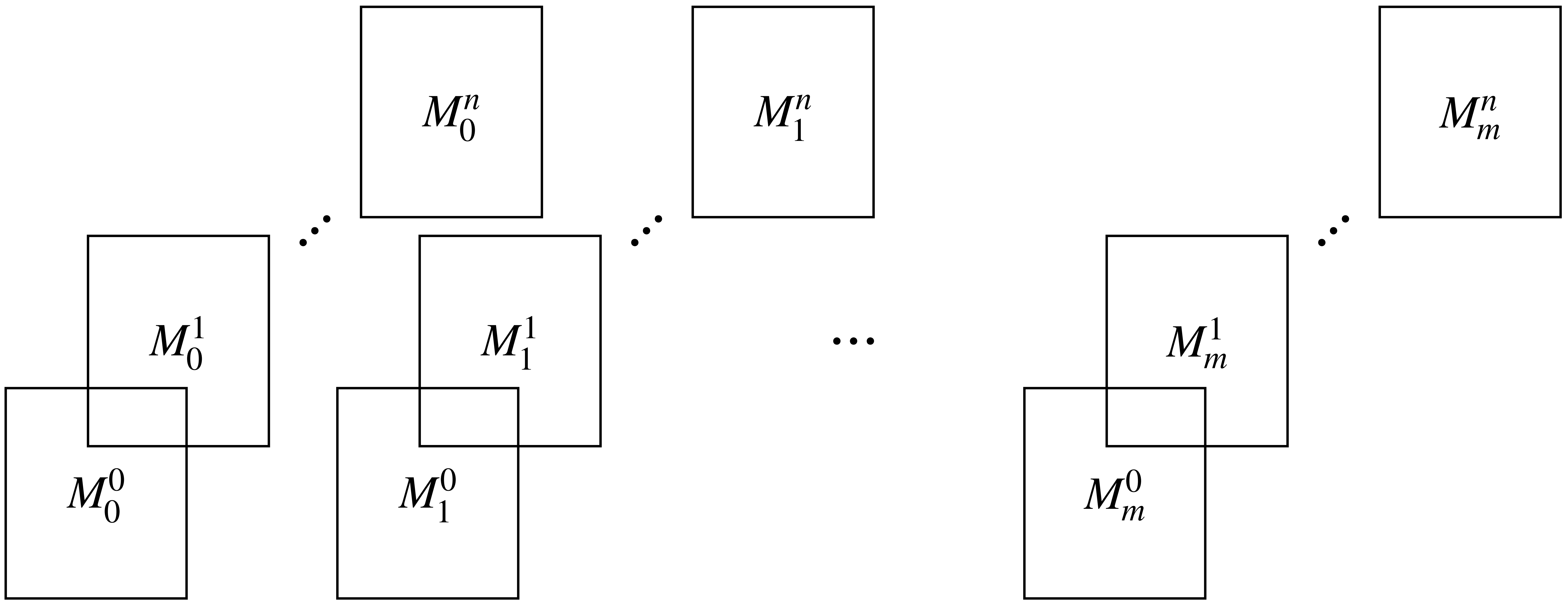
$$U_i^j \leftarrow \begin{bmatrix} a_i^j & c_i^j & -\xi_i^j & 0 \\ d_i^j & b_i^j & 0 & \xi_i^j \\ 0 & 0 & b_i^j & a_i^j \\ 0 & 0 & d_i^j & c_i^j \end{bmatrix}$$

$$L_i \in_R \mathbb{F}^{2m+1\times 4}, R_i \in_R \mathbb{F}^{4\times 2m+1}$$

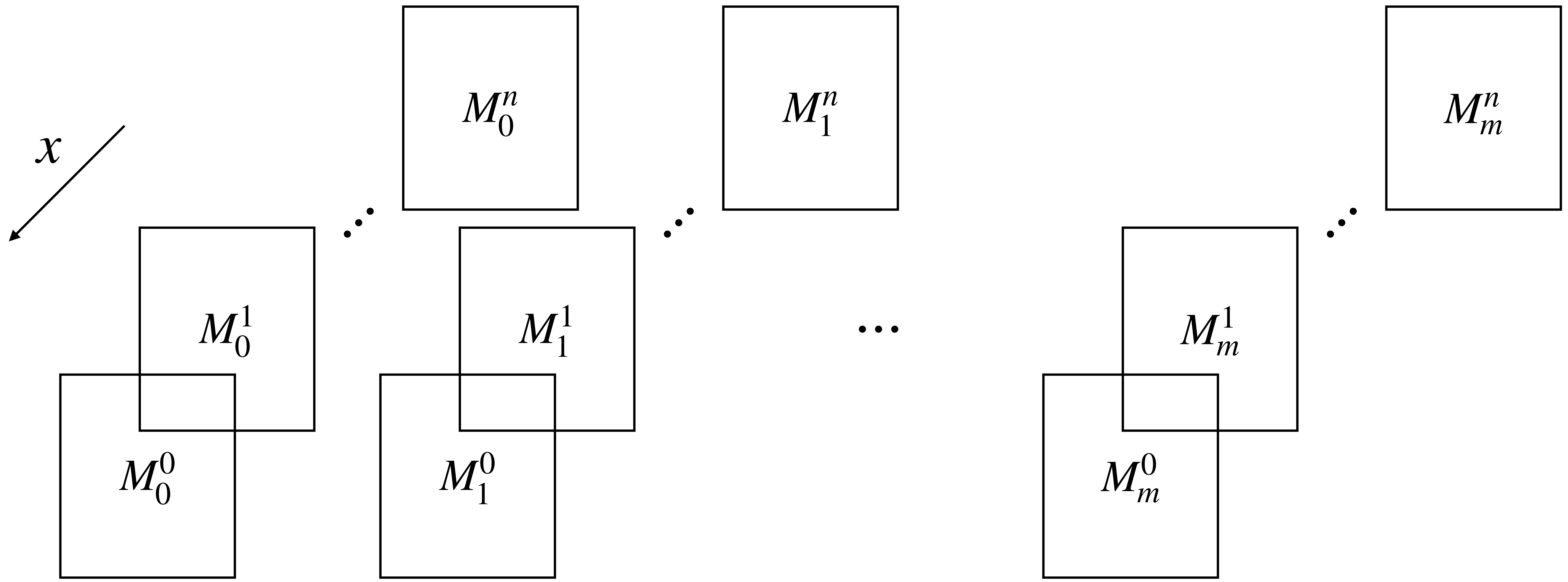
$$M_i^j \leftarrow L_i U_i^j R_i \in \mathbb{F}^{2m+1}$$

Same L_i and R_i for all j

Scheme



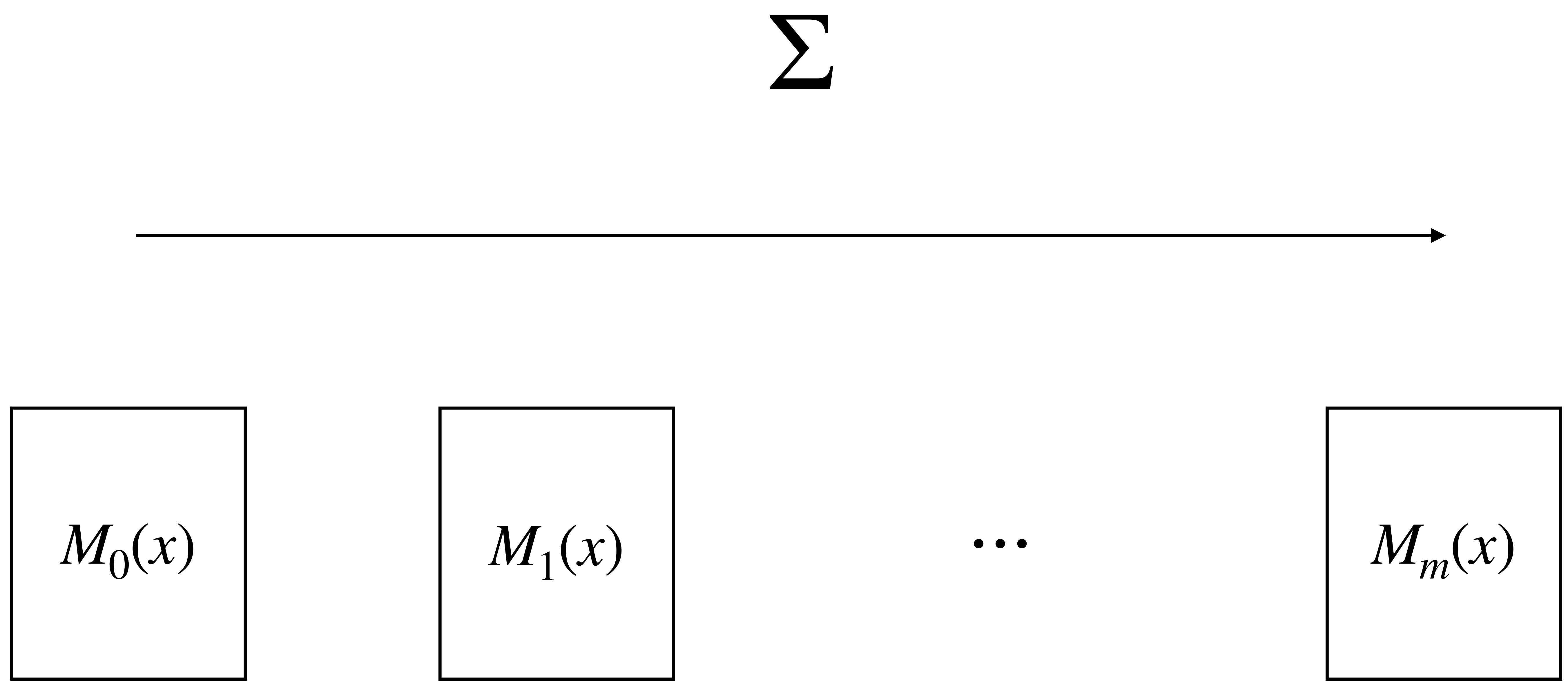
Scheme



Scheme

$$\boxed{M_0(x)} \quad \boxed{M_1(x)} \quad \cdots \quad \boxed{M_m(x)}$$

Scheme



Scheme

$$\boxed{M(x)}$$

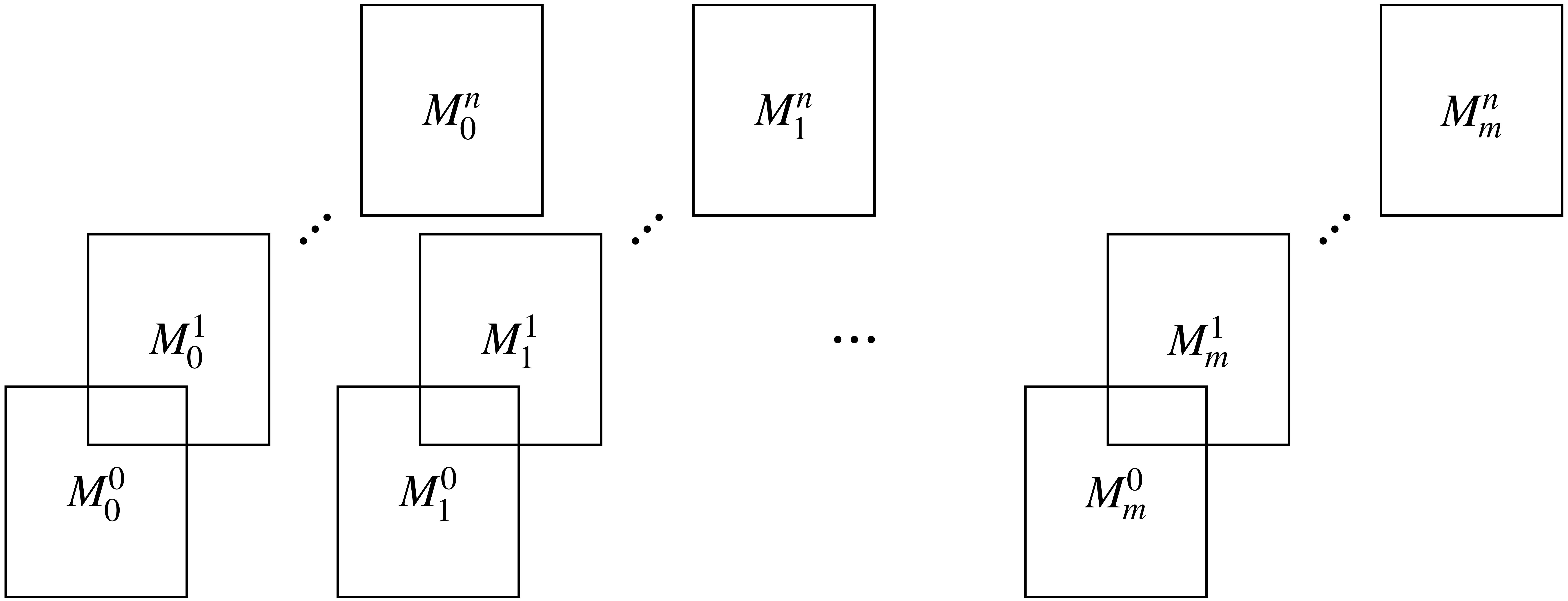
Scheme

$$x \text{ valid} \iff \det = 0$$

$$\boxed{M(x)}$$

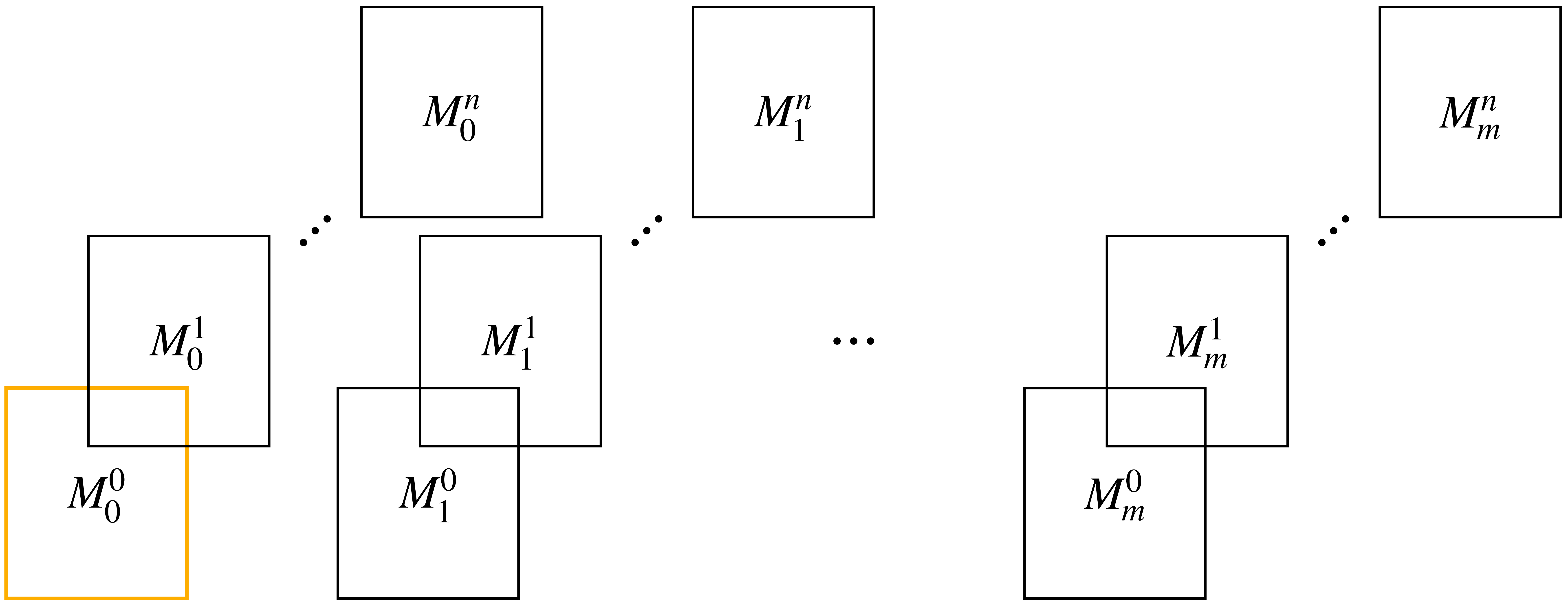
Scheme

$\mathrm{Enc}\left(1^\lambda, (A, B, C, D), msg\right)$



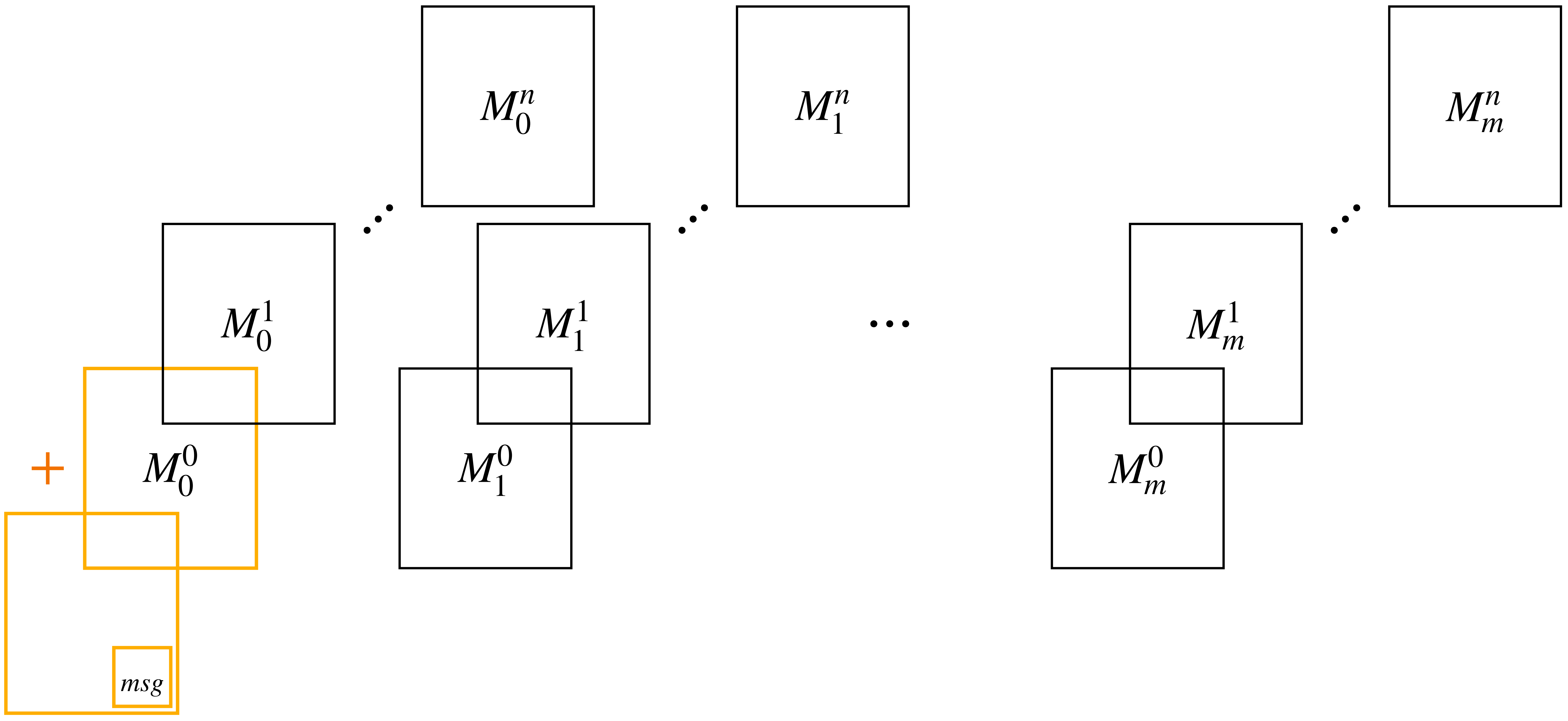
Scheme

$\mathrm{Enc}\left(1^{\lambda}, (A, B, C, D), msg\right)$



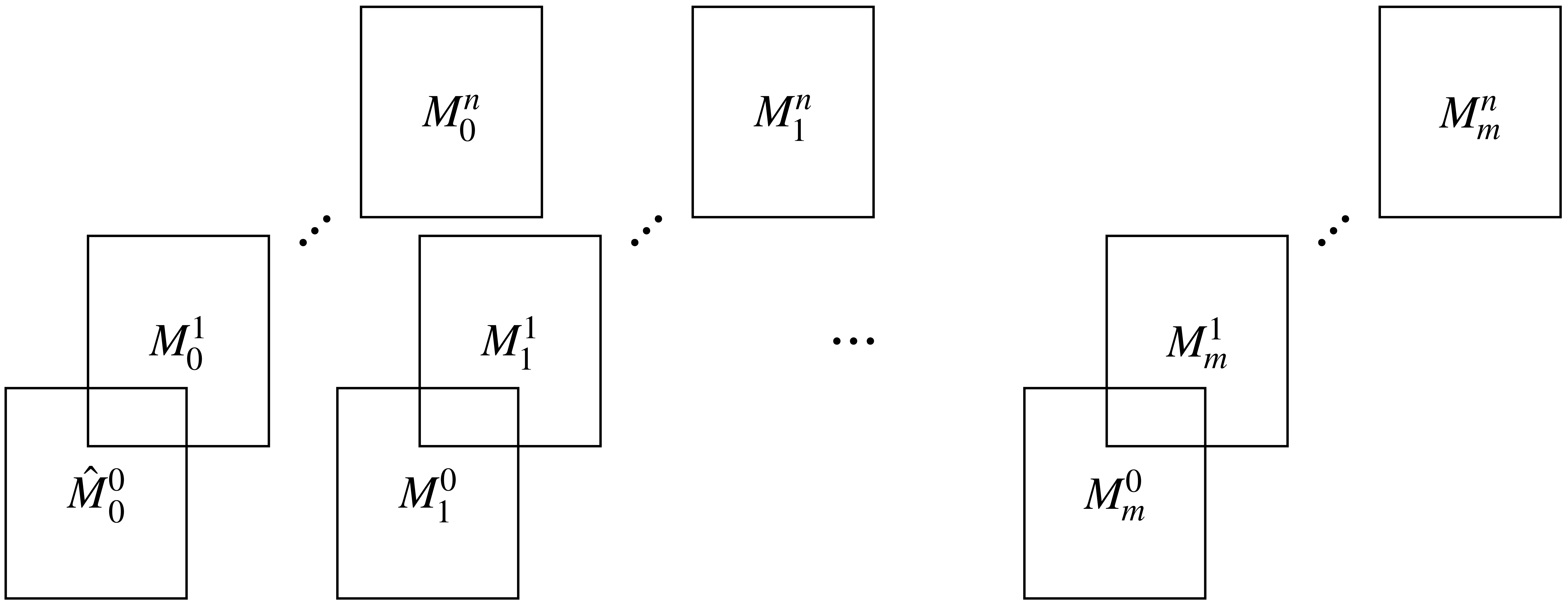
Scheme

$\mathrm{Enc}\left(1^{\lambda}, (A, B, C, D), msg\right)$



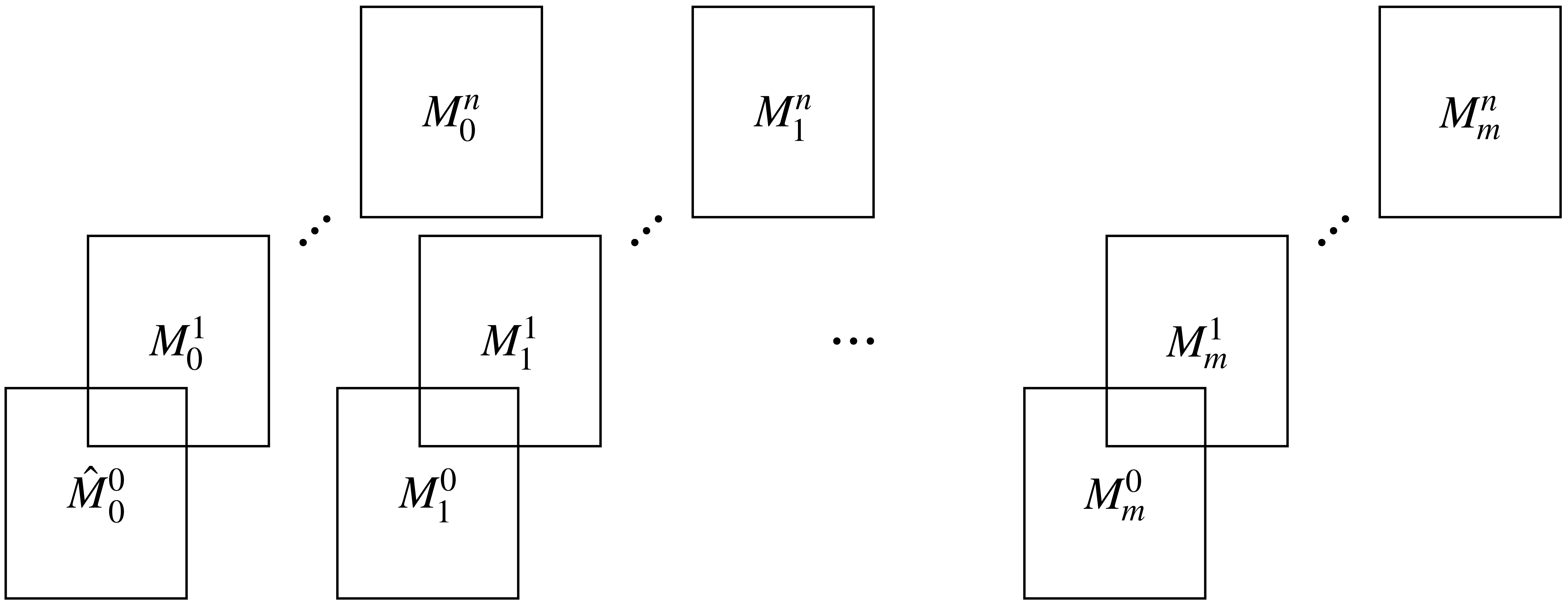
Scheme

$\mathrm{Enc}\left(1^{\lambda}, (A, B, C, D), msg\right)$



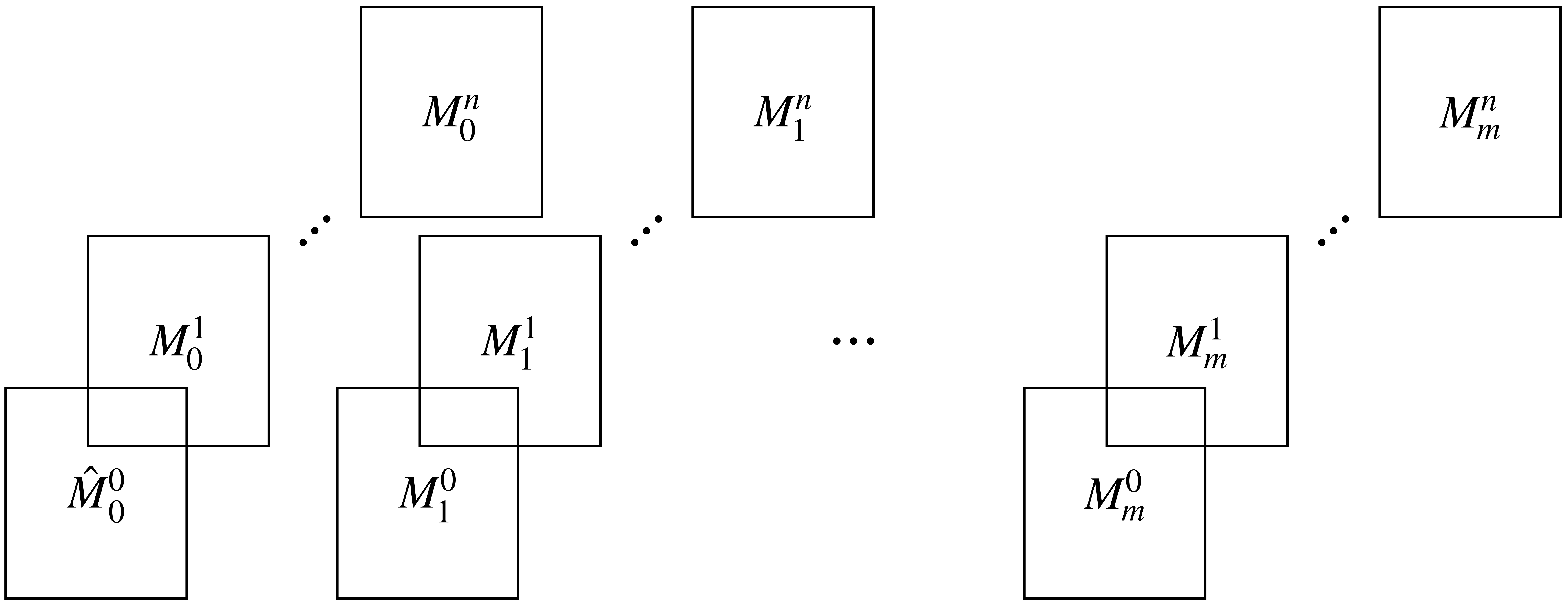
Scheme

$$\mathrm{Enc}\left(1^\lambda, (A, B, C, D), msg\right) \to C$$



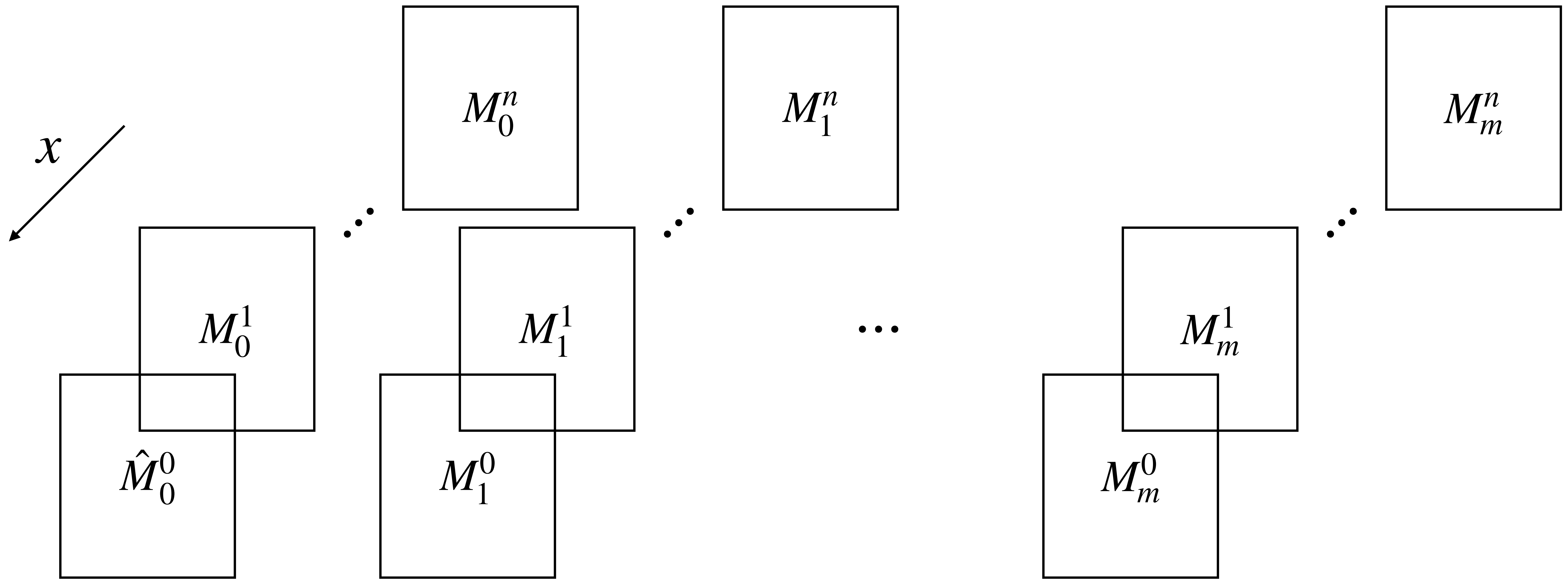
Scheme

Dec (x, C)



Scheme

Dec (x, C)



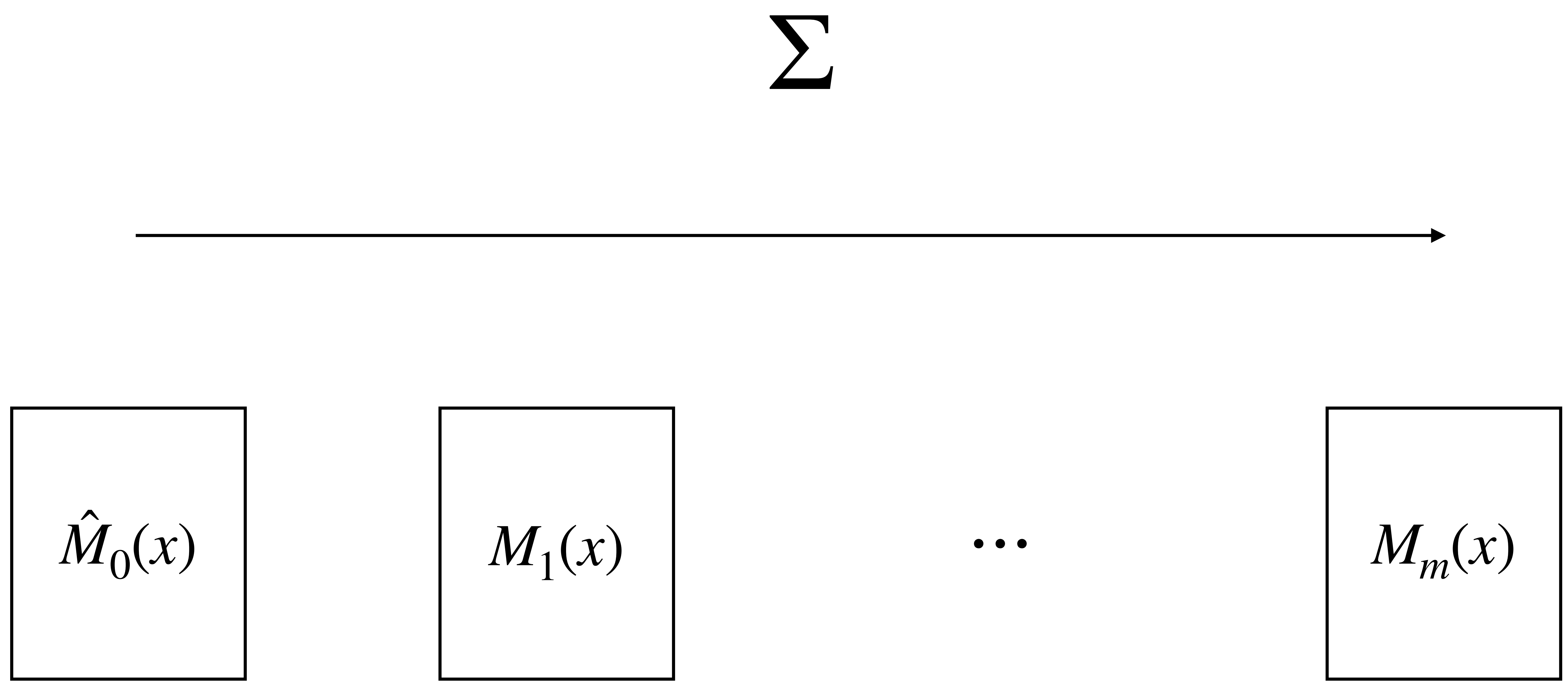
Scheme

Dec (x, C)

$$\boxed{\hat{M}_0(x)} \quad \boxed{M_1(x)} \quad \cdots \quad \boxed{M_m(x)}$$

Scheme

Dec (x, C)



Scheme

Dec (x, C)

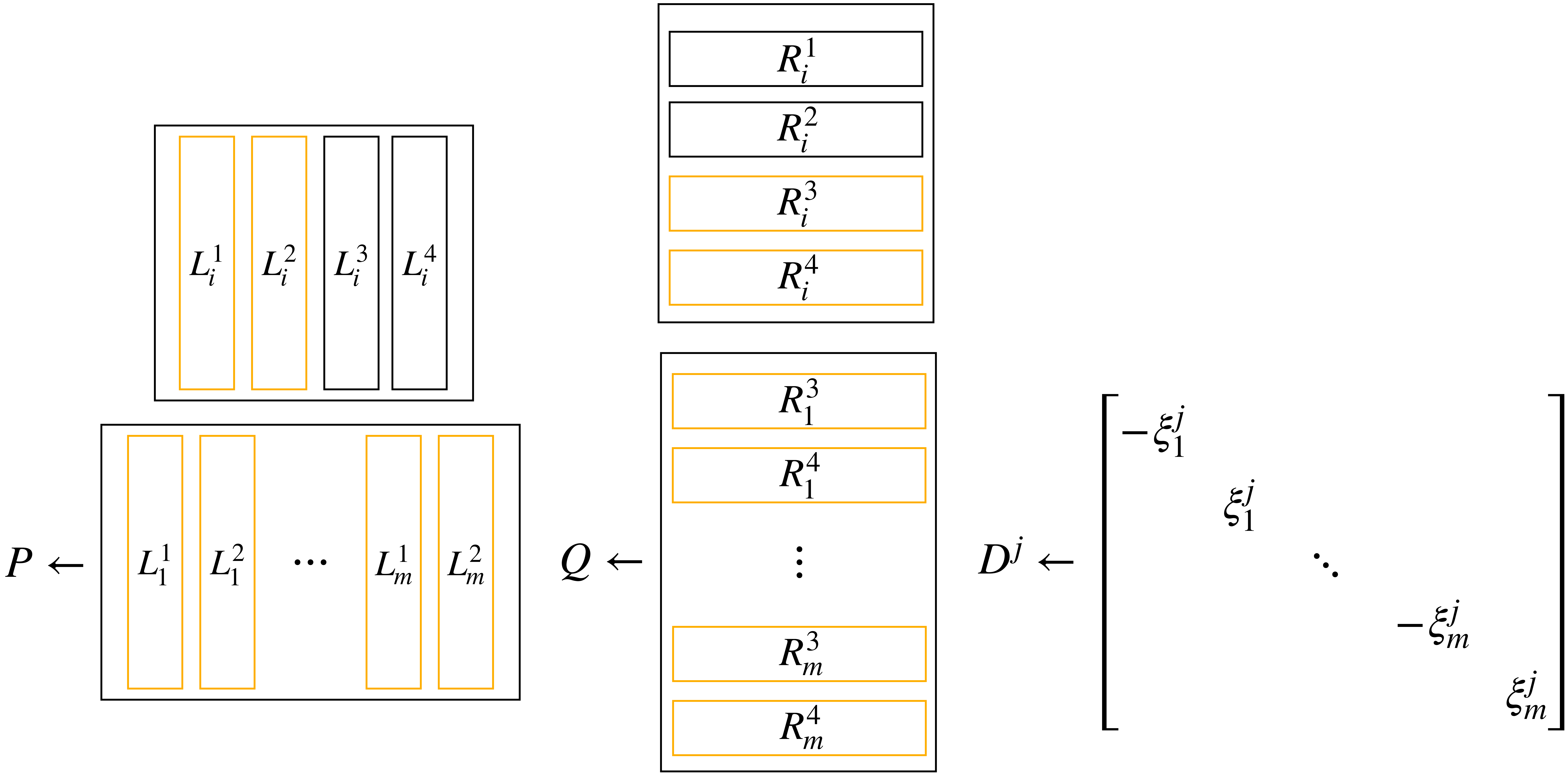
$$\boxed{\hat{M}(x)}$$

Scheme

$\text{Dec}\,(x, C)$

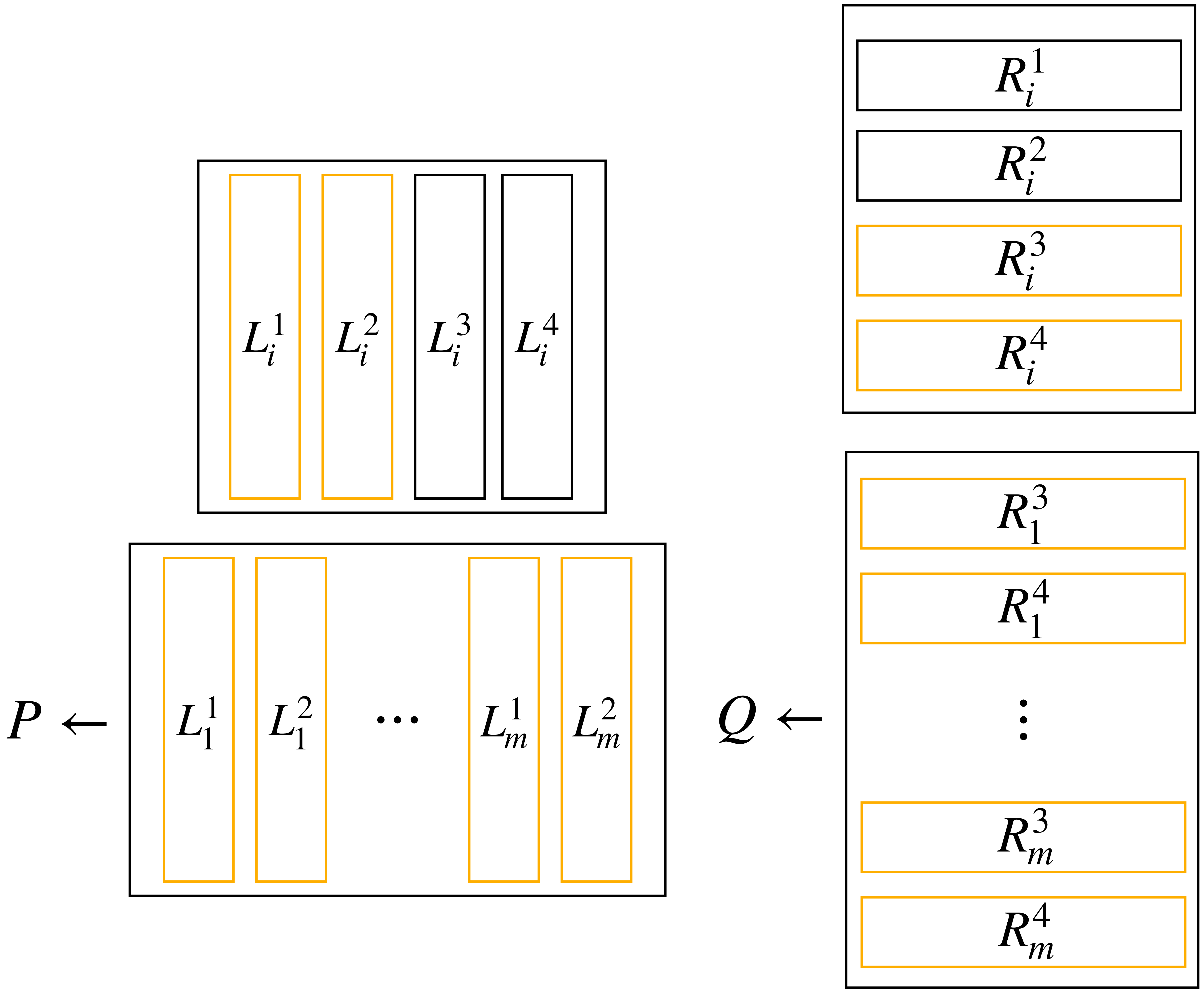
Solve for t: $\det\left(\hat{M}(x) - t \cdot x_0 \cdot E_{2m+1,2m+1}\right) = 0$

Attacks



L_i^1 L_i^2 L_i^3 L_i^4
$P \leftarrow$
L_1^1 L_1^2 $\cdots$ L_m^1 L_m^2
R_i^1
R_i^2
R_i^3
R_i^4
$Q \leftarrow$
R_1^3
R_1^4
$\vdots$
R_m^3
R_m^4
$D^j \leftarrow$
$-\xi_1^j$
ξ_1^j
$\ddots$
$-\xi_m^j$
ξ_m^j

Attacks



$$D(x) \leftarrow \sum_j x_j D^j$$

$$D^j \leftarrow \begin{bmatrix} -\xi_1^j & & & & \\ & \xi_1^j & & & \\ & & \ddots & & \\ & & & -\xi_m^j & \\ & & & & \xi_m^j \end{bmatrix}$$

Attacks

$$M_i(x) = PD(x)Q + N_i(x)$$

$N_i(x)$ only depends on $a_i(x), b_i(x), c_i(x), d_i(x)$, not $\xi_i(x)$

Attacks

$$M_i(x) = PD(x)Q + N_i(x)$$

$N_i(x)$ only depends on $a_i(x), b_i(x), c_i(x), d_i(x)$, not $\xi_i(x)$

$\mathrm{rank}(N_i(x))$ is low if the circuit is sparse!

(i.e., if each variable participates in only a few gates)

Attacks

$[U, V] = UV - VU$

Diagonal matrices commute $\Longrightarrow$ $\left[M_i^{-1} M_j, M_i^{-1} M_k\right]$ has low rank!

Recover L_i and R_i, then recover msg in $O\left(n^4\right)$ operations

Counter

1) Replace each entry with a $q \times q$ block

Block-diagonal matrices do not commute

$$U_i^j \leftarrow \begin{bmatrix} a_i^j & c_i^j & -\xi_i^j & 0 \\ d_i^j & b_i^j & 0 & \xi_i^j \\ 0 & 0 & b_i^j & a_i^j \\ 0 & 0 & d_i^j & c_i^j \end{bmatrix}$$

Counter

1) Replace each entry with a $q \times q$ block

Block-diagonal matrices do not commute

$$U_i^j \leftarrow \begin{bmatrix} a_i^j & c_i^j & -\xi_i^j & 0 \\ d_i^j & b_i^j & 0 & \xi_i^j \\ 0 & 0 & b_i^j & a_i^j \\ 0 & 0 & d_i^j & c_i^j \end{bmatrix}$$

2) Quadratic arithmetic program:

$$p_A(X) \cdot p_B(X) - p_C(X) \cdot p_D(X) = Z(X)H(X)$$

Counter

1) Replace each entry with a $q \times q$ block

Block-diagonal matrices do not commute

$$U_i^j \leftarrow \begin{bmatrix} a_i^j & c_i^j & -\xi_i^j & 0 \\ d_i^j & b_i^j & 0 & \xi_i^j \\ 0 & 0 & b_i^j & a_i^j \\ 0 & 0 & d_i^j & c_i^j \end{bmatrix}$$

2) Quadratic arithmetic program: $p_A(X) \cdot p_B(X) - p_C(X) \cdot p_D(X) = Z(X)H(X)$

Evaluate a multiple random points. Break one circuit constraint $\Longrightarrow$ break a large fraction (no sparsity)

Counter

QAP $\implies U_i^j$ matrices of size 8 (rank 4 or 8)

M_i^j matrices of size $4qN_{\text{QAP}} + 1$

$q \approx \sqrt{n} \approx \sqrt{m}$

$n \leftarrow 2^{14}$

$N_{\text{QAP}} \leftarrow 4$

Ciphertexts $\approx$ 8 TB.

Thank you!

https://ia.cr/2026/175

https://ia.cr/2026/1594