Shifting our knowledge of MQ-Sign security

Lars Ran

Radboud University

Monika Trimoska

Eindhoven University of Technology

PQCrypto 2025
April 8, Taipei, Taiwan

TU/e

*Animated version at https://mtrimoska.com/slides/PQCrypto25/#0

MQ-Sign

→ Round 2 candidate in the Korean post-quantum cryptography competition (K門C).

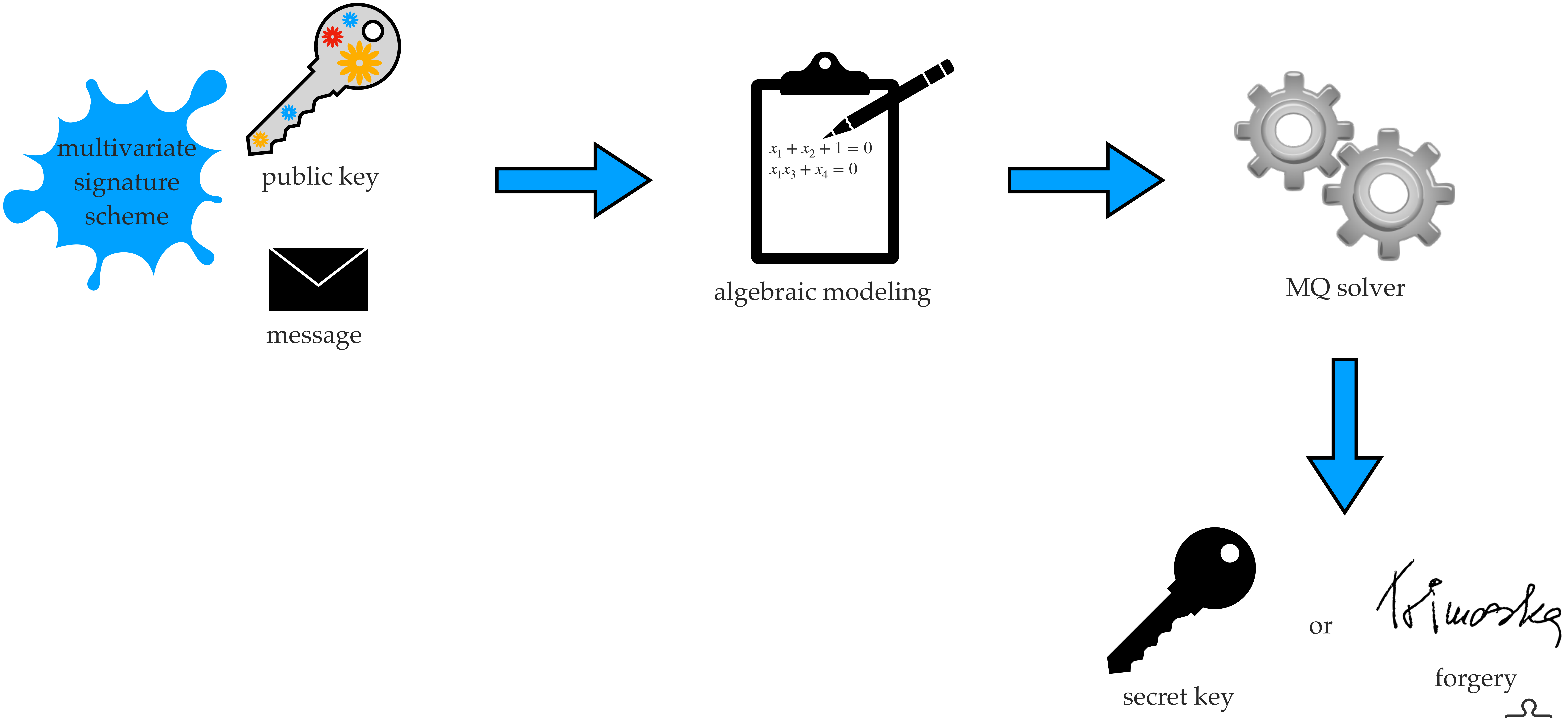
→ UOV-based digital signature algorithm with additional structure in the central map.

→ This work:

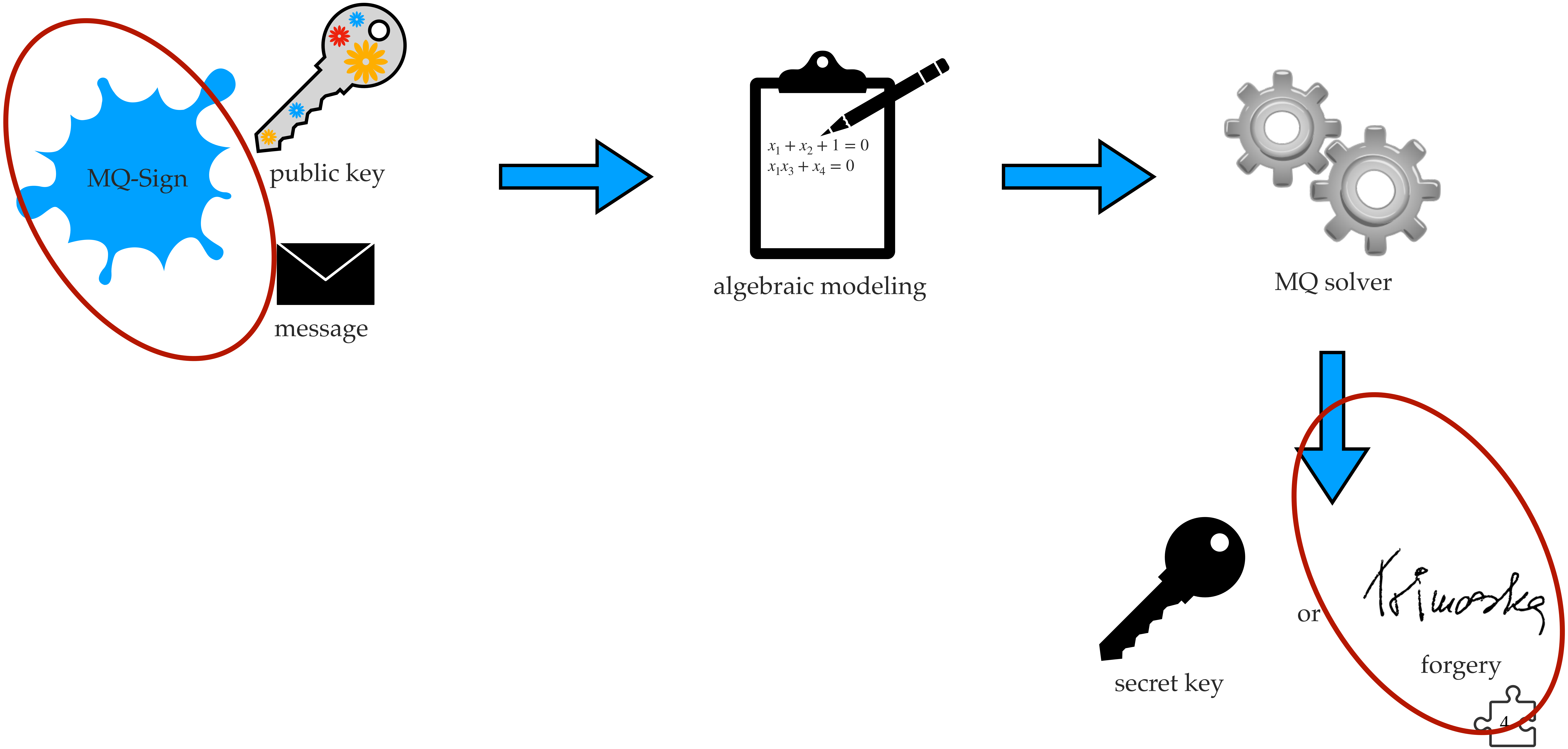
  → A universal forgery attack (not practical, but below the security level).

  → Algebraic cryptanalysis.

Algebraic cryptanalysis



Algebraic cryptanalysis




MQ-Sign
o
v

Matrix representation of quadratic forms

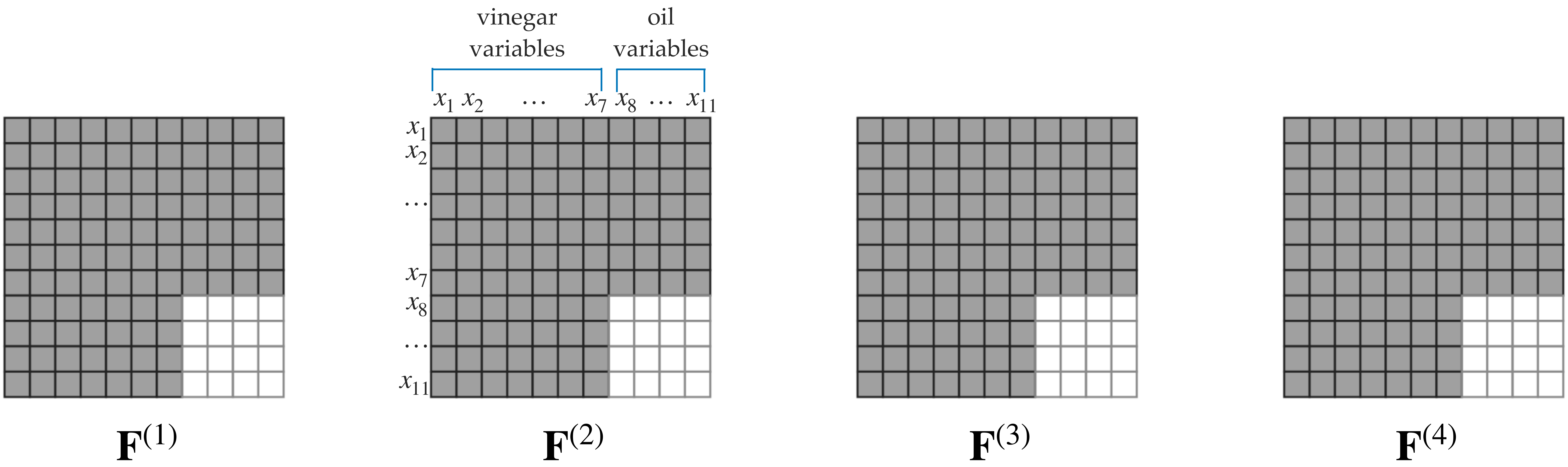
Quadratic form: $f(\mathbf{x}) = \sum \gamma_{ij} x_i x_j$

$$\mathbf{x}^\top = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \end{bmatrix} \qquad \mathbf{F} = \begin{bmatrix} \gamma_{1,1} & \frac{\gamma_{1,2}}{2} & \frac{\gamma_{1,3}}{2} & \frac{\gamma_{1,4}}{2} \\ \frac{\gamma_{2,1}}{2} & \gamma_{2,2} & \frac{\gamma_{2,3}}{2} & \frac{\gamma_{2,4}}{2} \\ \frac{\gamma_{3,1}}{2} & \frac{\gamma_{3,2}}{2} & \gamma_{3,3} & \frac{\gamma_{3,4}}{2} \\ \frac{\gamma_{4,1}}{2} & \frac{\gamma_{4,2}}{2} & \frac{\gamma_{4,3}}{2} & \gamma_{4,4} \end{bmatrix} \qquad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

so with $\mathbf{x} = (x_1, \ldots, x_n)$, we get $\mathbf{x}^\top \mathbf{F} \mathbf{x}$.

The UOV central map

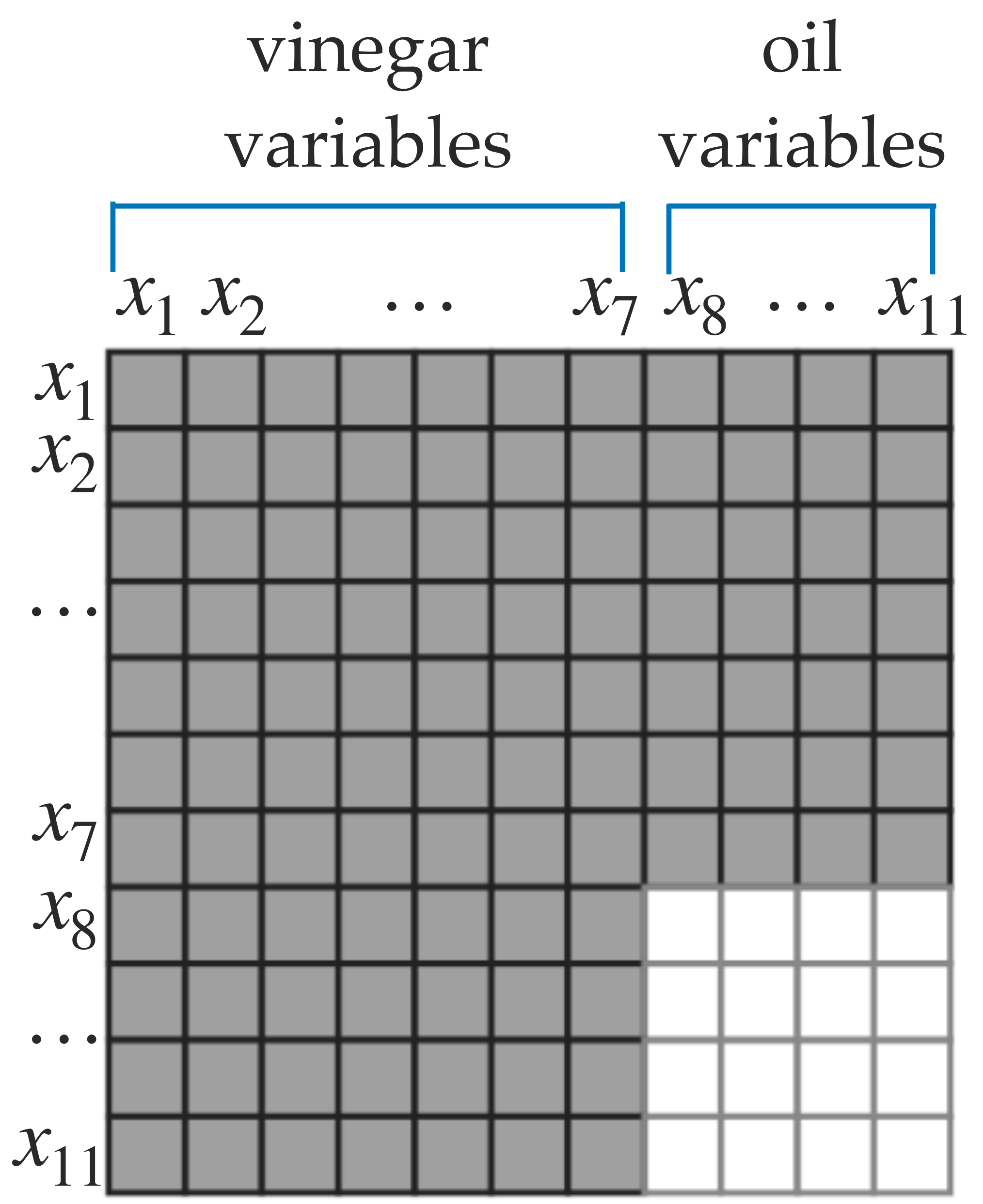
Toy example: $v = 7, m = 4$



*Grayed areas represent the entries that are possibly nonzero; blank areas denote the zero entries;

MQ-Sign

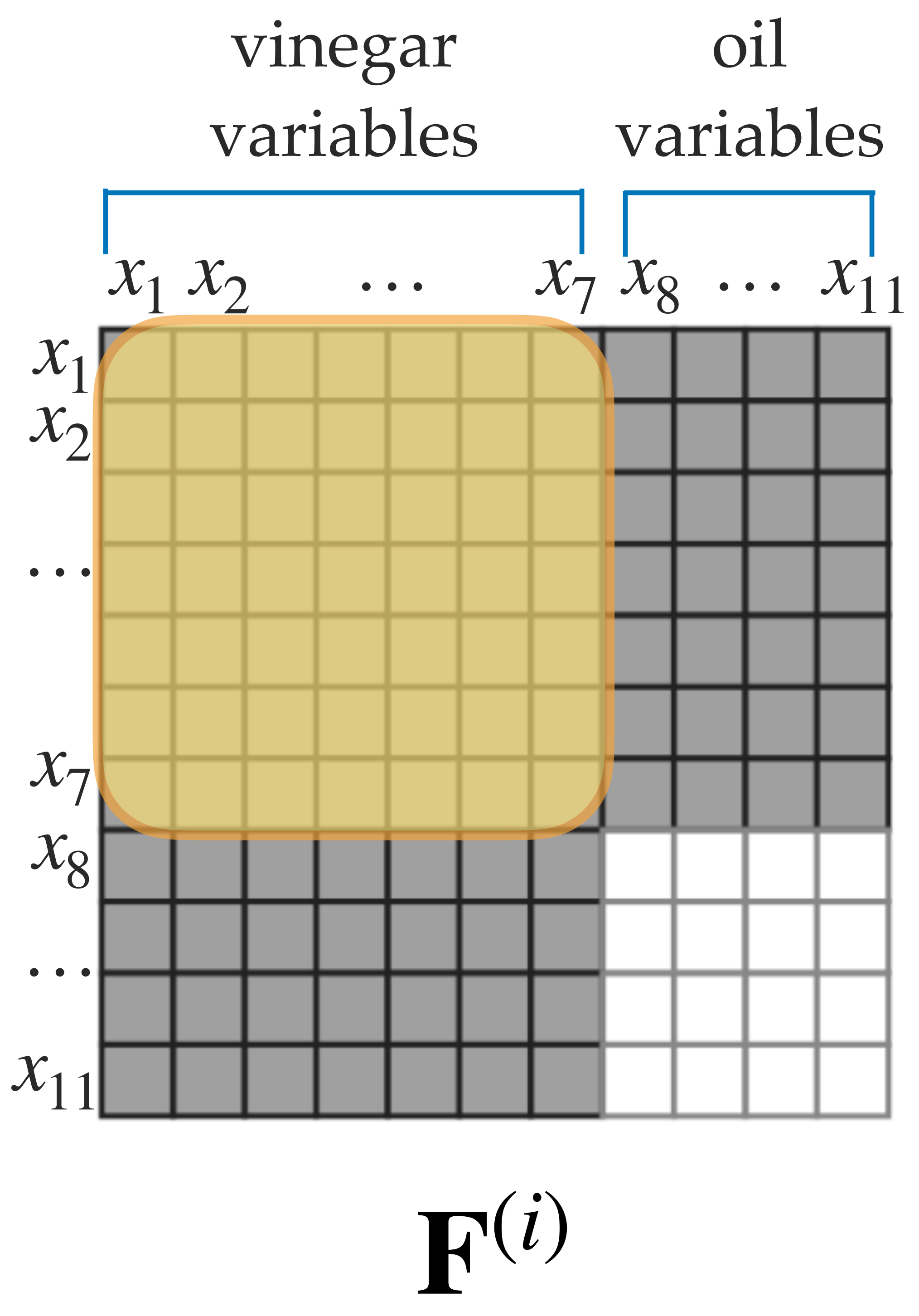
Variants with additional structure to the vinegar-vinegar or/and the vinegar-oil part, with the goal to reduce the size of the secret key.



$\mathbf{F}^{(i)}$

MQ-Sign

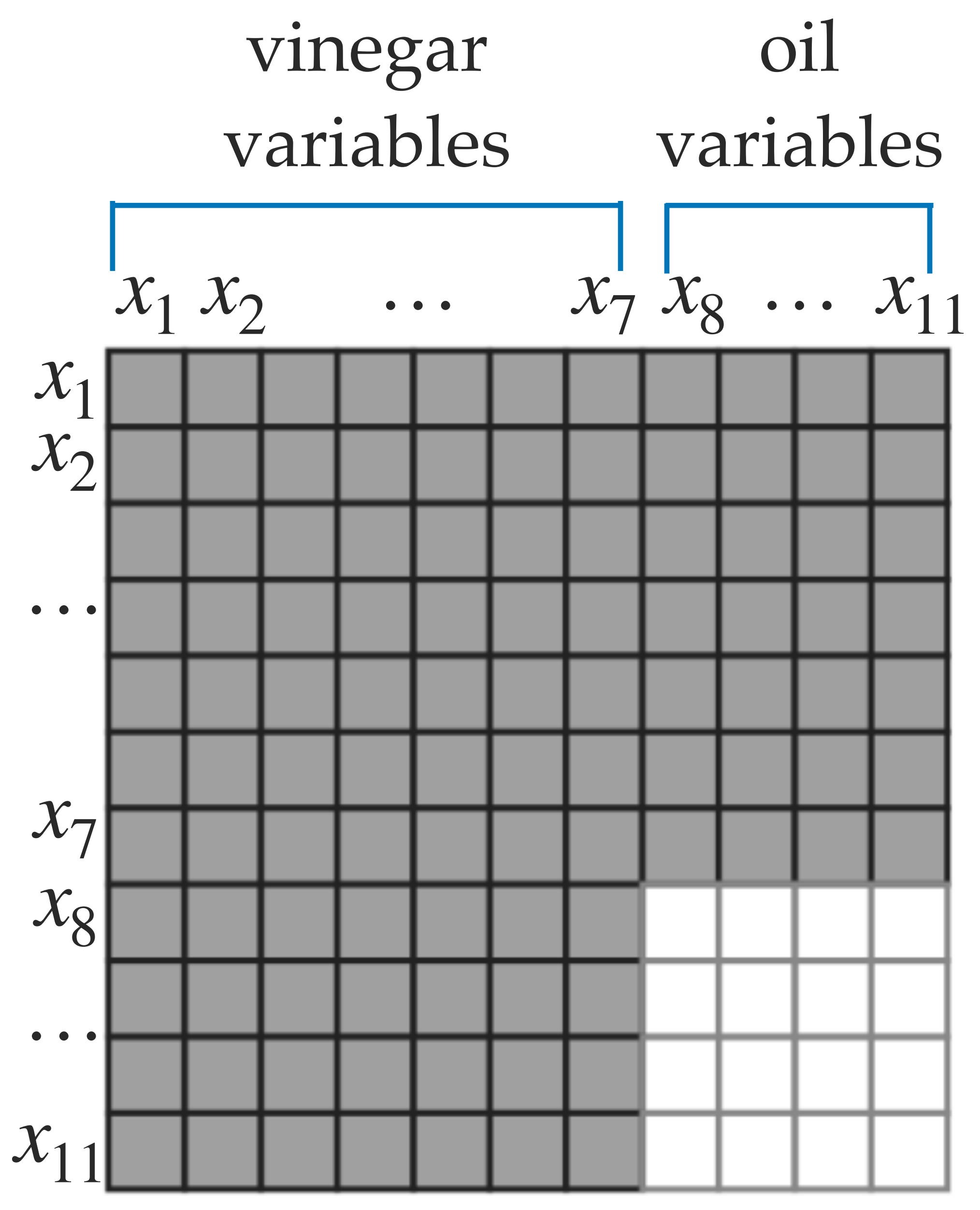
Variants with additional structure to the vinegar-vinegar or/and the vinegar-oil part, with the goal to reduce the size of the secret key.



The vinegar-vinegar part

MQ-Sign

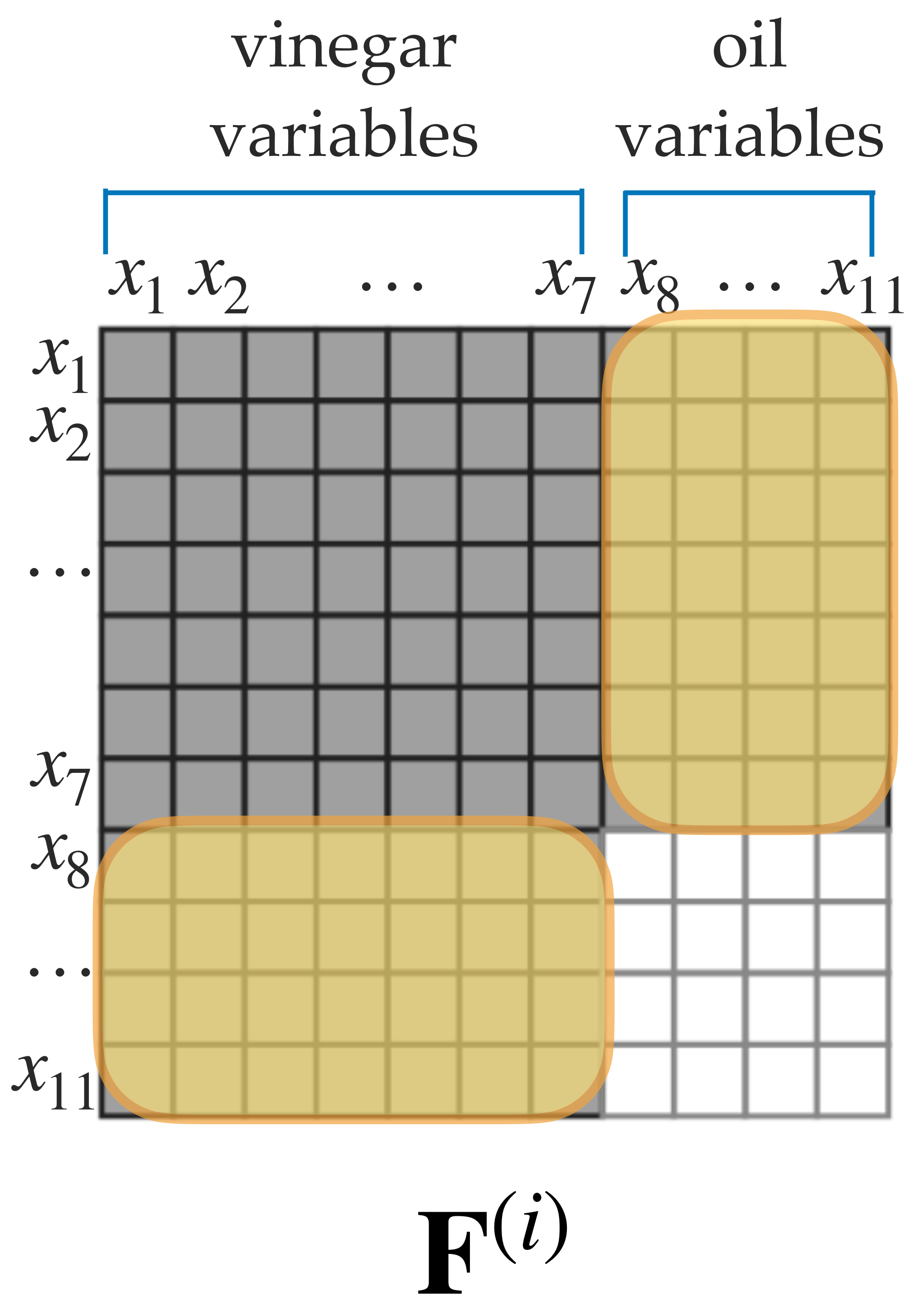
Variants with additional structure to the vinegar-vinegar or/and the vinegar-oil part, with the goal to reduce the size of the secret key.



$\mathbf{F}^{(i)}$

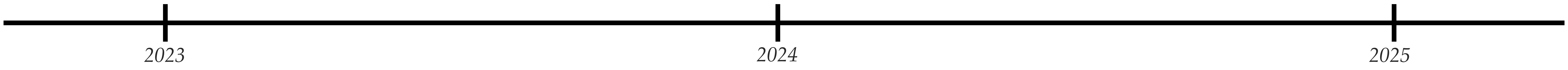
MQ-Sign

Variants with additional structure to the vinegar-vinegar or/and the vinegar-oil part, with the goal to reduce the size of the secret key.



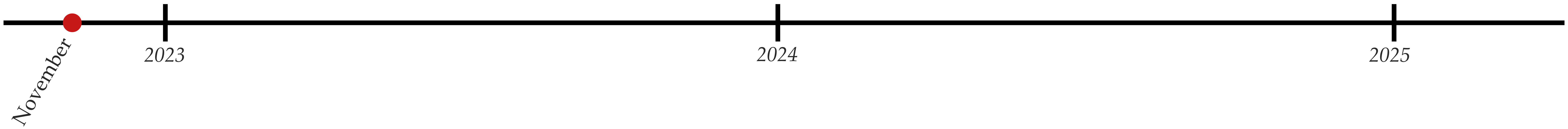
The vinegar-oil part

MQ-Sign timeline

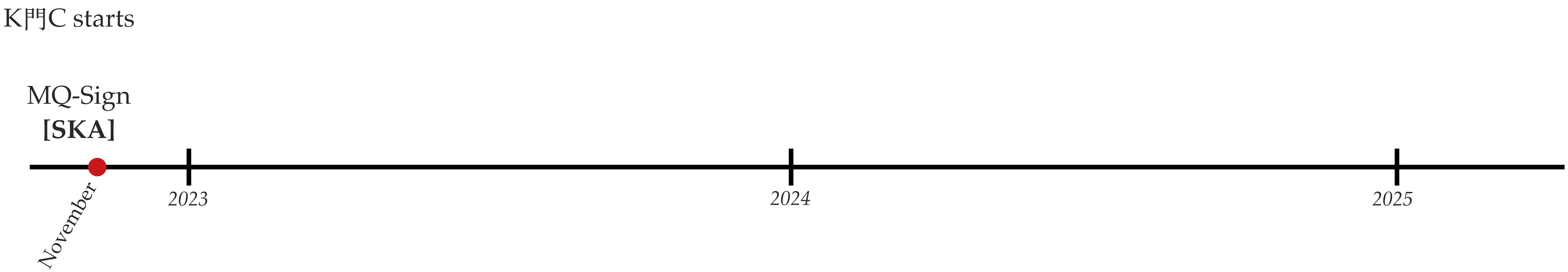


MQ-Sign timeline

K門C starts

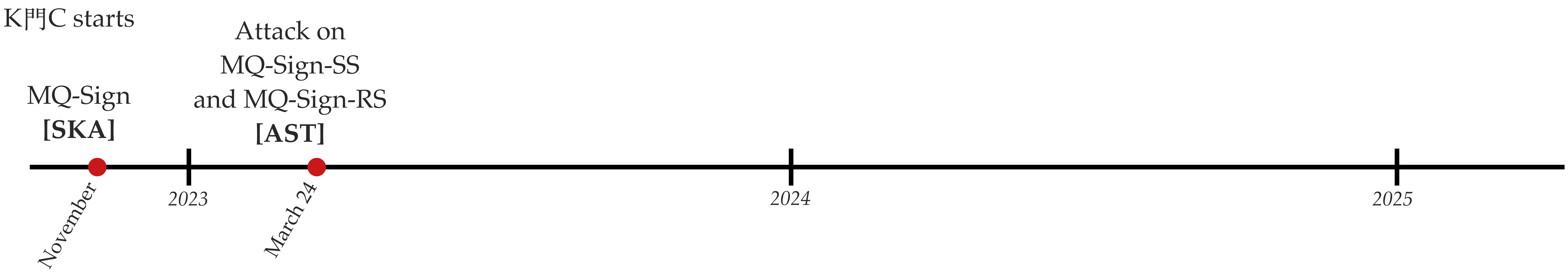


MQ-Sign timeline



[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

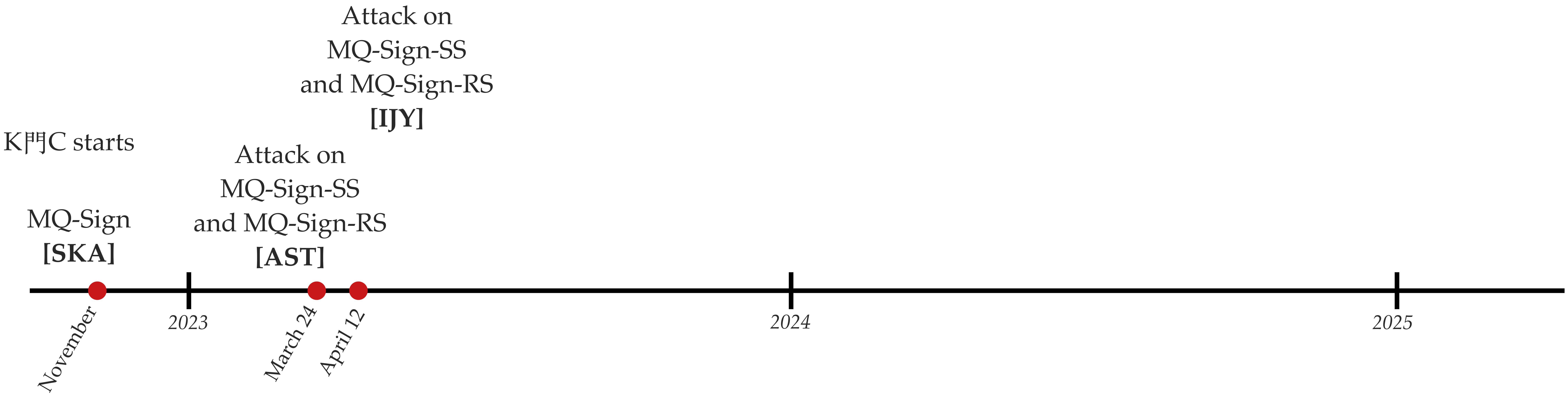
MQ-Sign timeline



[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

MQ-Sign timeline

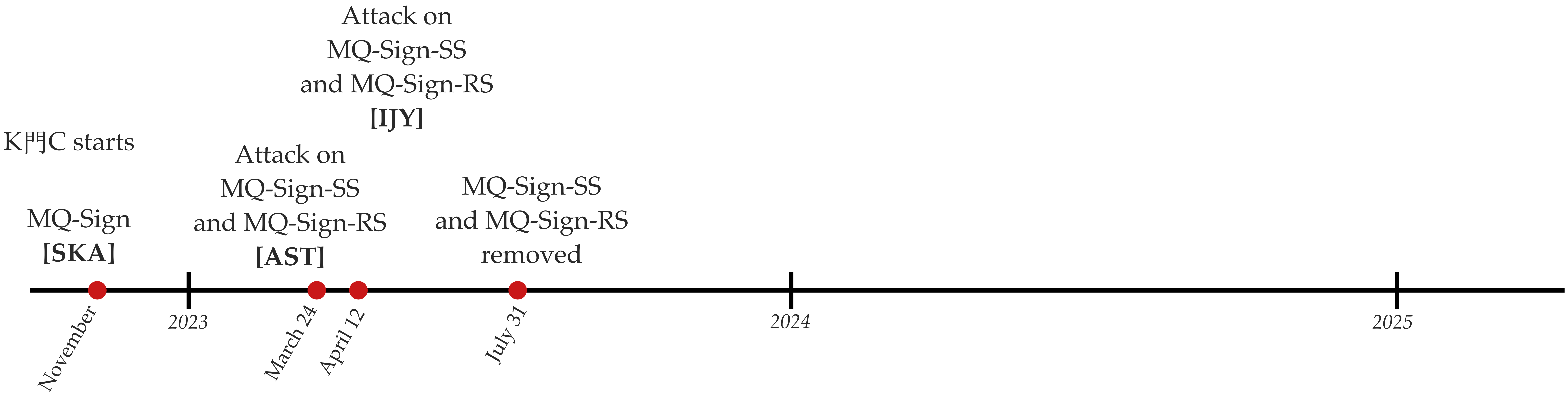


[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

MQ-Sign timeline

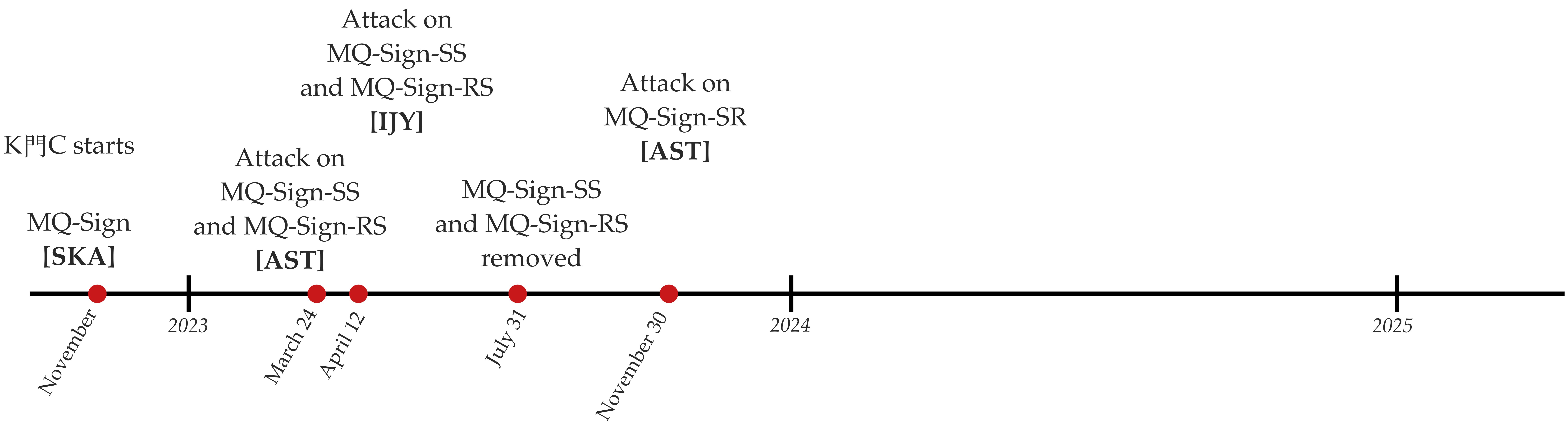


[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

MQ-Sign timeline

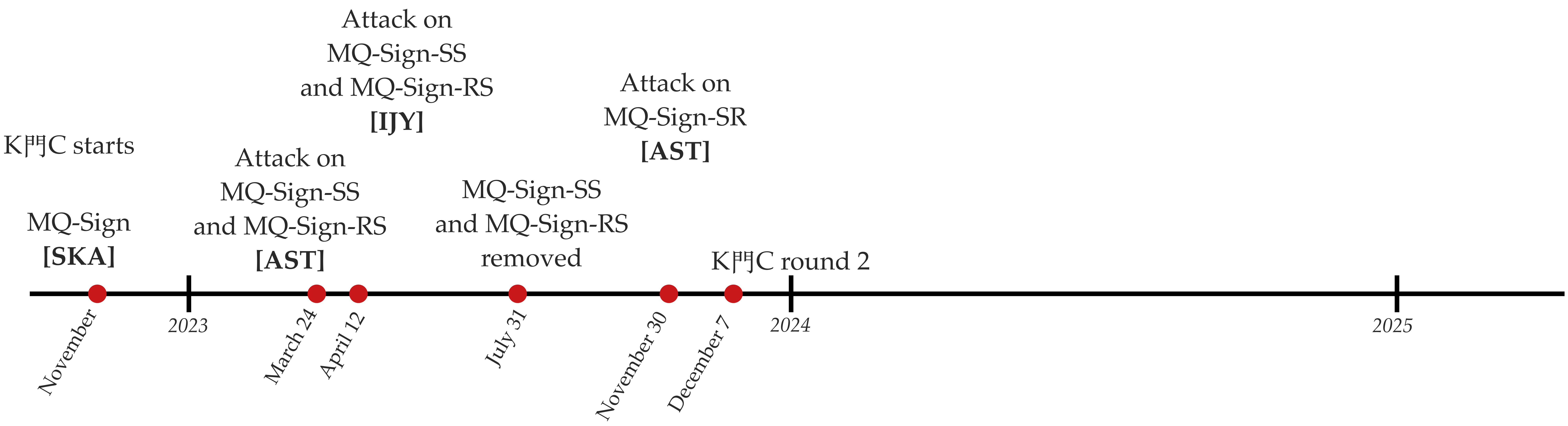


[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

MQ-Sign timeline

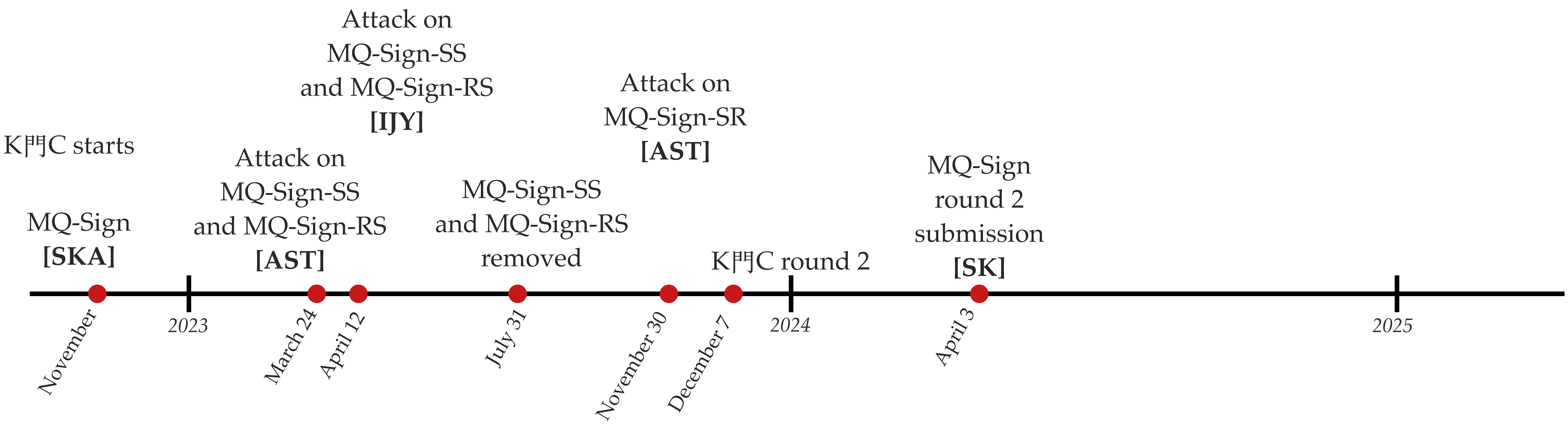


[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

MQ-Sign timeline



[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

[SK] Shim, Kwon. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2024)

MQ-Sign variants

- MQ-Sign-LR
  - The vinegar-oil part is random.
  - The vinegar-vinegar part is defined as

$$\begin{pmatrix} x_1 & x_2 & \dots & x_v \\ x_v & x_1 & \dots & x_{v-1} \\ \dots & \dots & \dots & \dots \\ x_{v-m+2} & x_{v-m+3} & \dots & x_{v-m+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \dots \\ L_v \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ \dots \\ f^{(m)} \end{pmatrix},$$

where $L_i = \sum_{j=1}^{v} \gamma_{ij} x_j$, for $i \in \{1, \dots, v\}$.

MQ-Sign variants

- MQ-Sign-LR
  - The vinegar-oil part is random.
  - The vinegar-vinegar part is defined as

$$\begin{pmatrix} x_1 & x_2 & \dots & x_v \\ x_v & x_1 & \dots & x_{v-1} \\ \dots & \dots & \dots & \dots \\ x_{v-m+2} & x_{v-m+3} & \dots & x_{v-m+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \dots \\ L_v \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ \dots \\ f^{(m)} \end{pmatrix},$$

where $L_i = \sum_{j=1}^{v} \gamma_{ij} x_j$, for $i \in \{1, \dots, v\}$.

- MQ-Sign-RR
  - A conservative variant where both the vinegar-vinegar and the vinegar-oil parts are random.
  - Equivalent to traditional UOV up to implementation choices.

MQ-Sign variants

- MQ-Sign-LR
  - The vinegar-oil part is random.
  - The vinegar-vinegar part is defined as

$$\begin{pmatrix} x_1 & x_2 & \dots & x_v \\ x_v & x_1 & \dots & x_{v-1} \\ \dots & \dots & \dots & \dots \\ x_{v-m+2} & x_{v-m+3} & \dots & x_{v-m+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \dots \\ L_v \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ \dots \\ f^{(m)} \end{pmatrix},$$

where $L_i = \sum_{j=1}^{v} \gamma_{ij} x_j$, for $i \in \{1, \dots, v\}$.

- MQ-Sign-RR
  - A conservative variant where both the vinegar-vinegar and the vinegar-oil parts are random.
  - Equivalent to traditional UOV up to implementation choices.

Equivalent secret keys

For any instance of a UOV secret key $(f', \mathbf{S}')$, there exists an equivalent secret key $(f, \mathbf{S})$ with

$$\mathbf{S} = \begin{pmatrix} \mathbf{I}_{v\times v} & \mathbf{S}_1 \\ \mathbf{0}_{m\times v} & \mathbf{I}_{m\times m} \end{pmatrix}.$$

- A key of this *equivalent keys* form is used for efficiency (fewer entries in $\mathbf{S}$).

Equivalent secret keys optimisation

Key generation $\mathbf{P} = \mathbf{S}^\top \mathbf{F} \mathbf{S}$

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_4^{(k)} \end{pmatrix} = \begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ 0 & \mathbf{I} \end{pmatrix}$$

Equivalent secret keys optimisation

Key generation $\mathbf{P} = \mathbf{S}^\top \mathbf{F} \mathbf{S}$

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_4^{(k)} \end{pmatrix} = \begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ 0 & \mathbf{I} \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_4^{(k)} \end{pmatrix} = \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ 0 & \mathsf{Upper}(\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}$$

Equivalent secret keys optimisation

Key generation $\mathbf{P} = \mathbf{S}^\top \mathbf{F} \mathbf{S}$

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_4^{(k)} \end{pmatrix} = \begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ 0 & \mathbf{I} \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_4^{(k)} \end{pmatrix} = \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ 0 & \mathsf{Upper}(\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}$$

Equivalent secret keys optimisation

Key generation $\mathbf{P} = \mathbf{S}^\top \mathbf{F} \mathbf{S}$

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_4^{(k)} \end{pmatrix} = \begin{pmatrix} \mathbf{I} & 0 \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ 0 & \mathbf{I} \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_4^{(k)} \end{pmatrix} = \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ 0 & \mathsf{Upper}(\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}$$

The specific structure is only in the part of the central that is public (in the case where the equivalent keys optimisation is used).

Forging a signature for weak targets

Forging a signature

Find $\mathbf{x}$ s.t. $\mathbf{x}^\top P^{(k)}\mathbf{x} = \mathbf{w}$, for all $1 \leq k \leq m$:

$$\begin{pmatrix} \mathbf{x}_v^\top & \mathbf{x}_m^\top \end{pmatrix} \begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_3^{(k)} \end{pmatrix} \begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_m \end{pmatrix} = w_k$$

Forging a signature

Find $\mathbf{x}$ s.t. $\mathbf{x}^\top P^{(k)}\mathbf{x} = \mathbf{w}$, for all $1 \leq k \leq m$:

$$\begin{pmatrix} \mathbf{x}_v^\top & \mathbf{x}_m^\top \end{pmatrix} \begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_3^{(k)} \end{pmatrix} \begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_m \end{pmatrix} = w_k$$

$$\mathbf{x}_v^\top \mathbf{P}_1^{(k)} \mathbf{x}_v + \mathbf{x}_v^\top \mathbf{P}_2^{(k)} \mathbf{x}_m + \mathbf{x}_m^\top \mathbf{P}_3^{(k)} \mathbf{x}_m = w_k$$

Forging a signature

Find $\mathbf{x}$ s.t. $\mathbf{x}^\top P^{(k)}\mathbf{x} = \mathbf{w}$, for all $1 \le k \le m$:

$$\begin{pmatrix}\mathbf{x}_v^\top & \mathbf{x}_m^\top\end{pmatrix}\begin{pmatrix}\mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_3^{(k)}\end{pmatrix}\begin{pmatrix}\mathbf{x}_v \\ \mathbf{x}_m\end{pmatrix} = w_k$$

$$\mathbf{x}_v^\top \mathbf{P}_1^{(k)} \mathbf{x}_v + \mathbf{x}_v^\top \mathbf{P}_2^{(k)} \mathbf{x}_m + \mathbf{x}_m^\top \mathbf{P}_3^{(k)} \mathbf{x}_m = w_k$$

Fix $\mathbf{x}_m$ to zero (rmk: we are expected to have a solution with good probability even if we fix another $v - m$ variables).

Forging a signature

Find $\mathbf{x}$ s.t. $\mathbf{x}^\top P^{(k)}\mathbf{x} = \mathbf{w}$, for all $1 \leq k \leq m$:

$$\begin{pmatrix} \mathbf{x}_v^\top & \mathbf{x}_m^\top \end{pmatrix} \begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ 0 & \mathbf{P}_3^{(k)} \end{pmatrix} \begin{pmatrix} \mathbf{x}_v \\ \mathbf{x}_m \end{pmatrix} = w_k$$

$$\mathbf{x}_v^\top \mathbf{P}_1^{(k)} \mathbf{x}_v + \mathbf{x}_v^\top \mathbf{P}_2^{(k)} \mathbf{x}_m + \mathbf{x}_m^\top \mathbf{P}_3^{(k)} \mathbf{x}_m = w_k$$

Fix $\mathbf{x}_m$ to zero (rmk: we are expected to have a solution with good probability even if we fix another $v - m$ variables).

$$\mathbf{x}_v^\top \mathbf{P}_1^{(k)} \mathbf{x}_v = w_k$$

where the $\mathbf{P}_1^{(k)}$ have a specific structure.

A toy example

$v = 8, m = 4, \mathbf{w} = (0 \quad 0 \quad 0 \quad 0).$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ f^{(2)} \\ f^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

A toy example

$v = 8, m = 4, \mathbf{w} = (0 \quad 0 \quad 0 \quad 0).$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ f^{(2)} \\ f^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

A toy example

$v = 8, m = 4, \mathbf{w} = (0 \quad 0 \quad 0 \quad 0)$.

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ f^{(2)} \\ f^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$
$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

A toy example

$v = 8, m = 4, \mathbf{w} = (0 \quad 0 \quad 0 \quad 0).$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ f^{(2)} \\ f^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$
$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$
$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

A toy example

$v = 8, m = 4, \mathbf{w} = (0 \quad 0 \quad 0 \quad 0).$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ f^{(2)} \\ f^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$
$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$
$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$
$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

A toy example

$v = 8, m = 4, \mathbf{w} = (0 \quad 0 \quad 0 \quad 0).$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ f^{(2)} \\ f^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$
$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$
$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$
$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

A toy example

Will focus on this target, before showing the generalisation.

$v = 8, m = 4, \mathbf{w} = (0 \quad 0 \quad 0 \quad 0).$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix} = \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ f^{(2)} \\ f^{(4)} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$
$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$
$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$
$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1								
x_2								
x_3								
x_4								
x_5								
x_6								
x_7								
x_8								

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_1 = x_1(\gamma_{1,1}x_1 + \gamma_{1,2}x_2 + \gamma_{1,3}x_3 + \gamma_{1,4}x_4 + \gamma_{1,5}x_5 + \gamma_{1,6}x_6 + \gamma_{1,7}x_7 + \gamma_{1,8}x_8)$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1								
x_2								
x_3								
x_4								
x_5								
x_6								
x_7								
x_8								

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_1 = x_1(\gamma_{1,1}x_1 + \gamma_{1,2}x_2 + \gamma_{1,3}x_3 + \gamma_{1,4}x_4 + \gamma_{1,5}x_5 + \gamma_{1,6}x_6 + \gamma_{1,7}x_7 + \gamma_{1,8}x_8)$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	$\gamma_{1,1}$							
x_2								
x_3								
x_4								
x_5								
x_6								
x_7								
x_8								

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_1 = x_1(\gamma_{1,1}x_1+\gamma_{1,2}x_2+\gamma_{1,3}x_3+\gamma_{1,4}x_4+\gamma_{1,5}x_5+\gamma_{1,6}x_6+\gamma_{1,7}x_7+\gamma_{1,8}x_8)$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	$\gamma_{1,1}$	$\gamma_{1,2}$						
x_2								
x_3								
x_4								
x_5								
x_6								
x_7								
x_8								

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

$$x_1L_1 = x_1(\gamma_{1,1}x_1+\gamma_{1,2}x_2+\gamma_{1,3}x_3+\gamma_{1,4}x_4+\gamma_{1,5}x_5+\gamma_{1,6}x_6+\gamma_{1,7}x_7+\gamma_{1,8}x_8)$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	$\gamma_{1,1}$	$\gamma_{1,2}$	$\gamma_{1,3}$					
x_2								
x_3								
x_4								
x_5								
x_6								
x_7								
x_8								

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

$$x_1L_1 = x_1(\gamma_{1,1}x_1+\gamma_{1,2}x_2+\gamma_{1,3}x_3+\gamma_{1,4}x_4+\gamma_{1,5}x_5+\gamma_{1,6}x_6+\gamma_{1,7}x_7+\gamma_{1,8}x_8)$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	$\gamma_{1,1}$	$\gamma_{1,2}$	$\gamma_{1,3}$	$\gamma_{1,4}$	$\gamma_{1,5}$	$\gamma_{1,6}$	$\gamma_{1,7}$	$\gamma_{1,8}$
x_2								
x_3								
x_4								
x_5								
x_6								
x_7								
x_8								

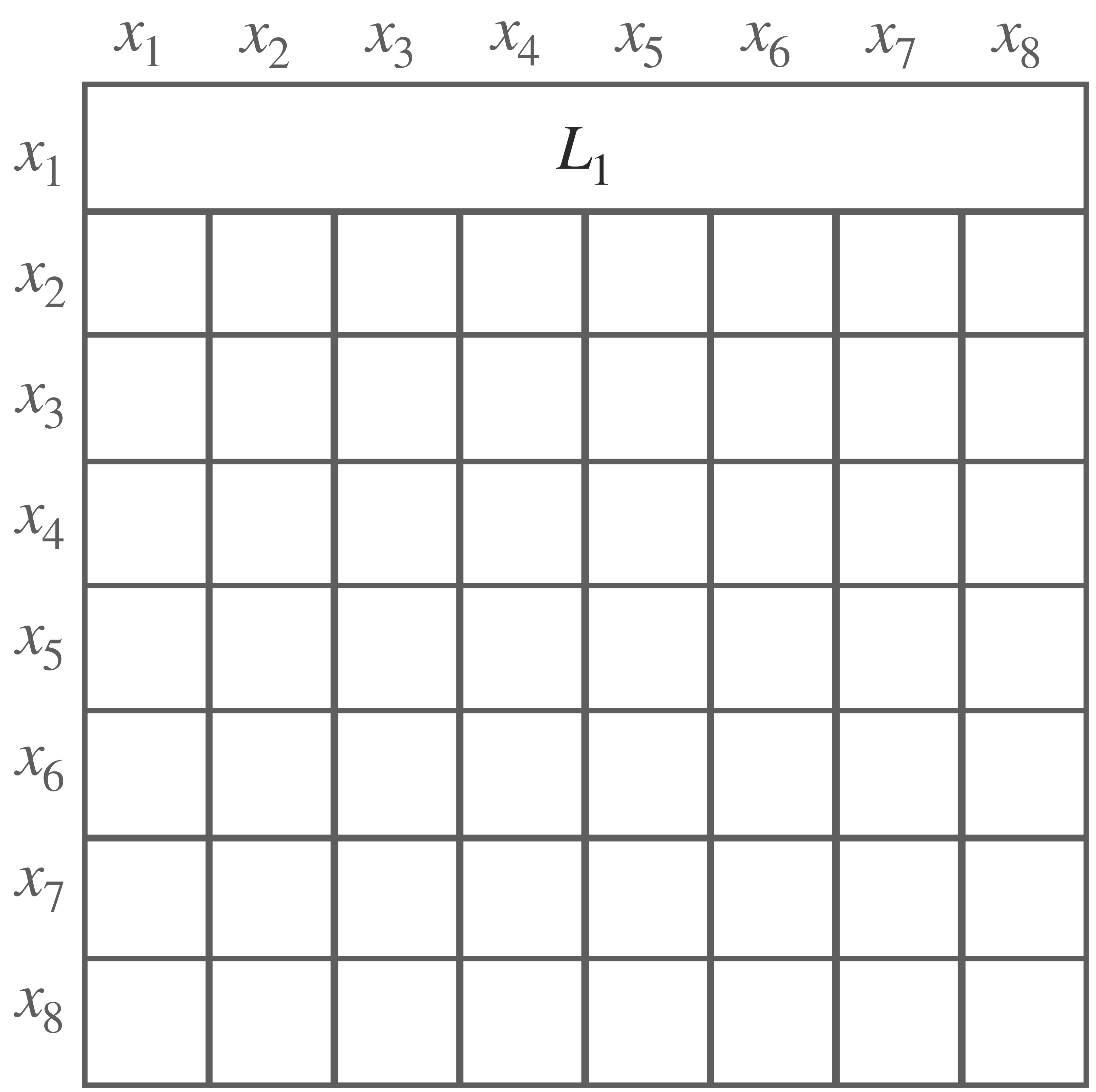
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



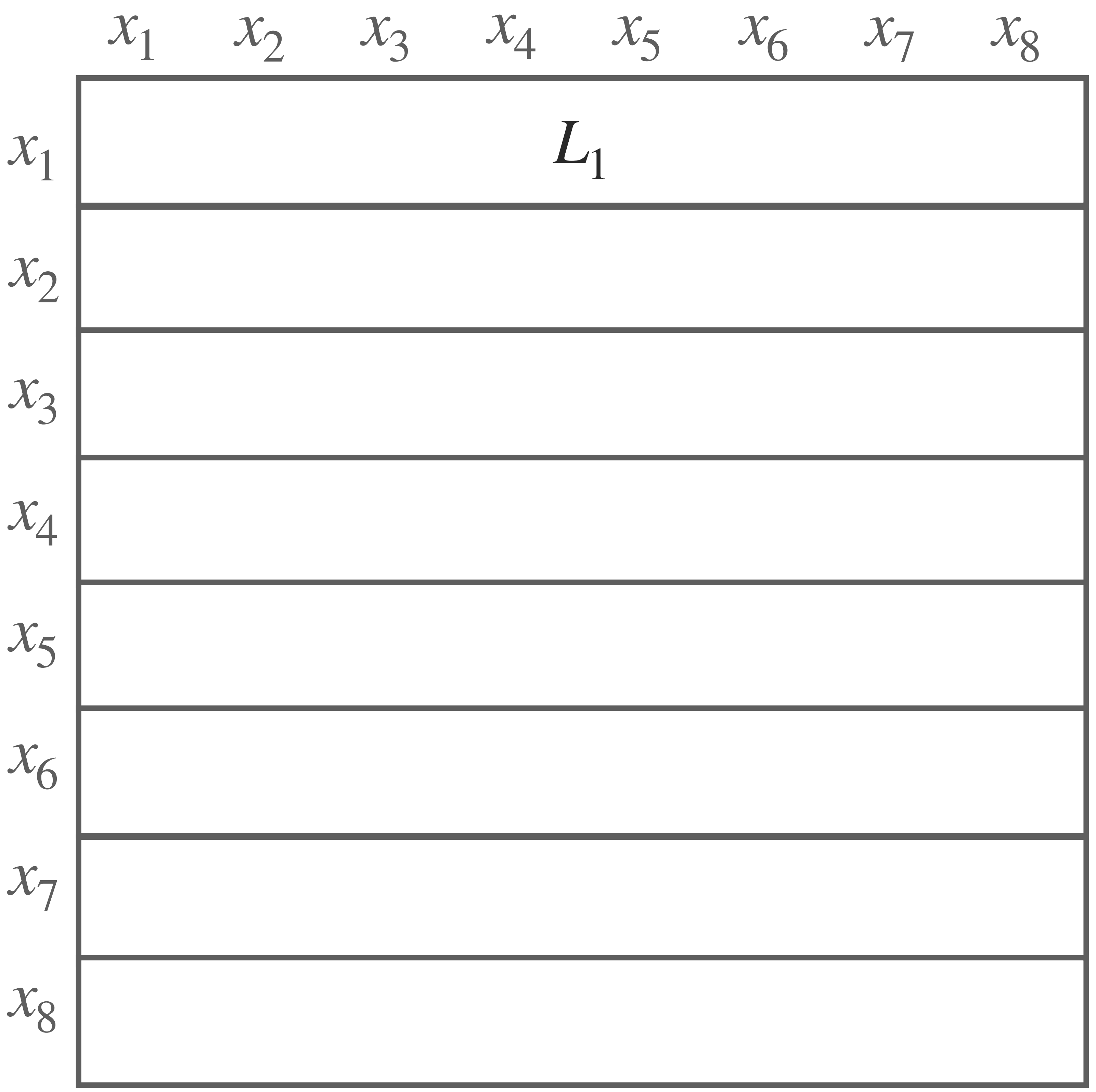
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



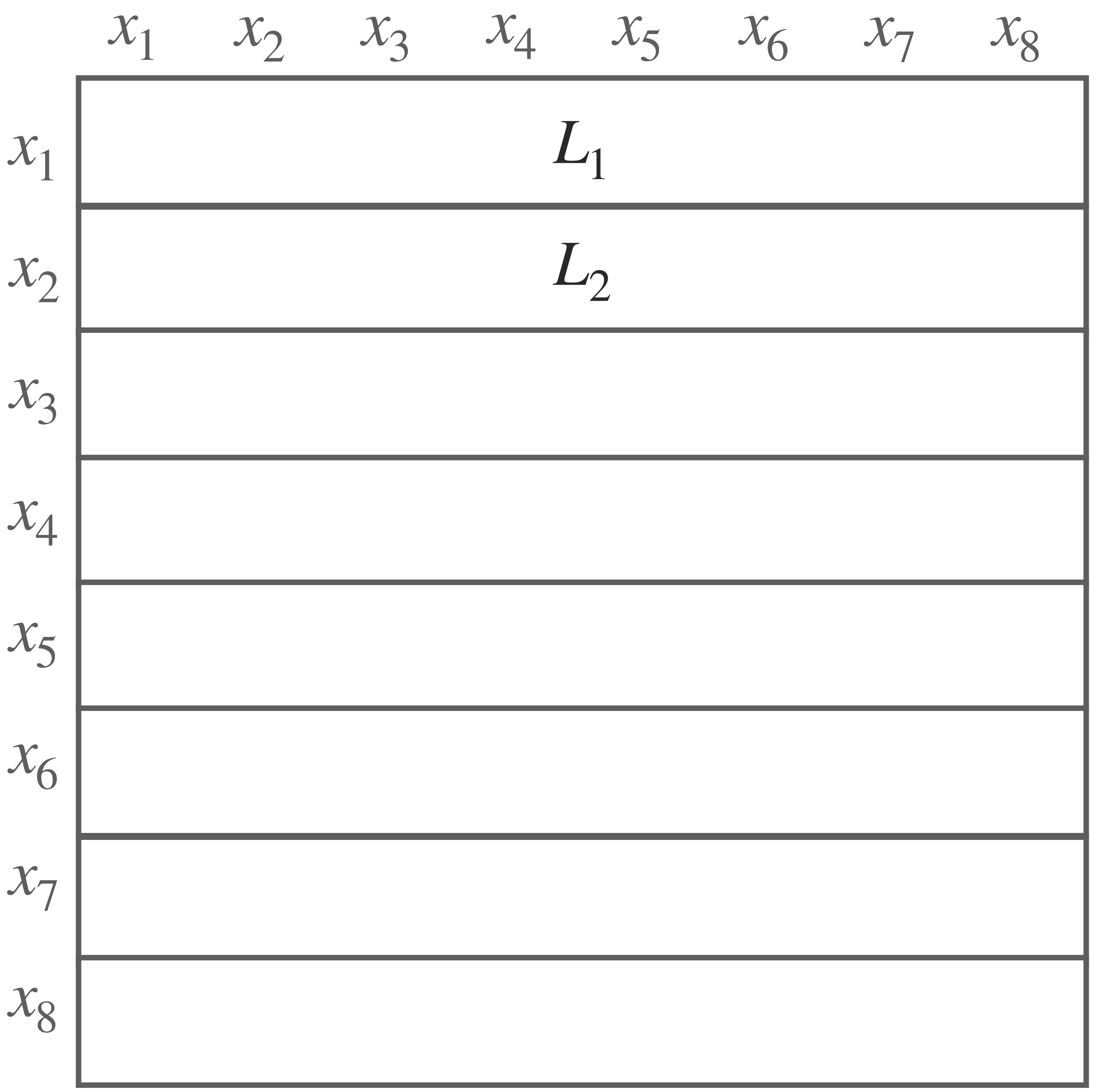
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



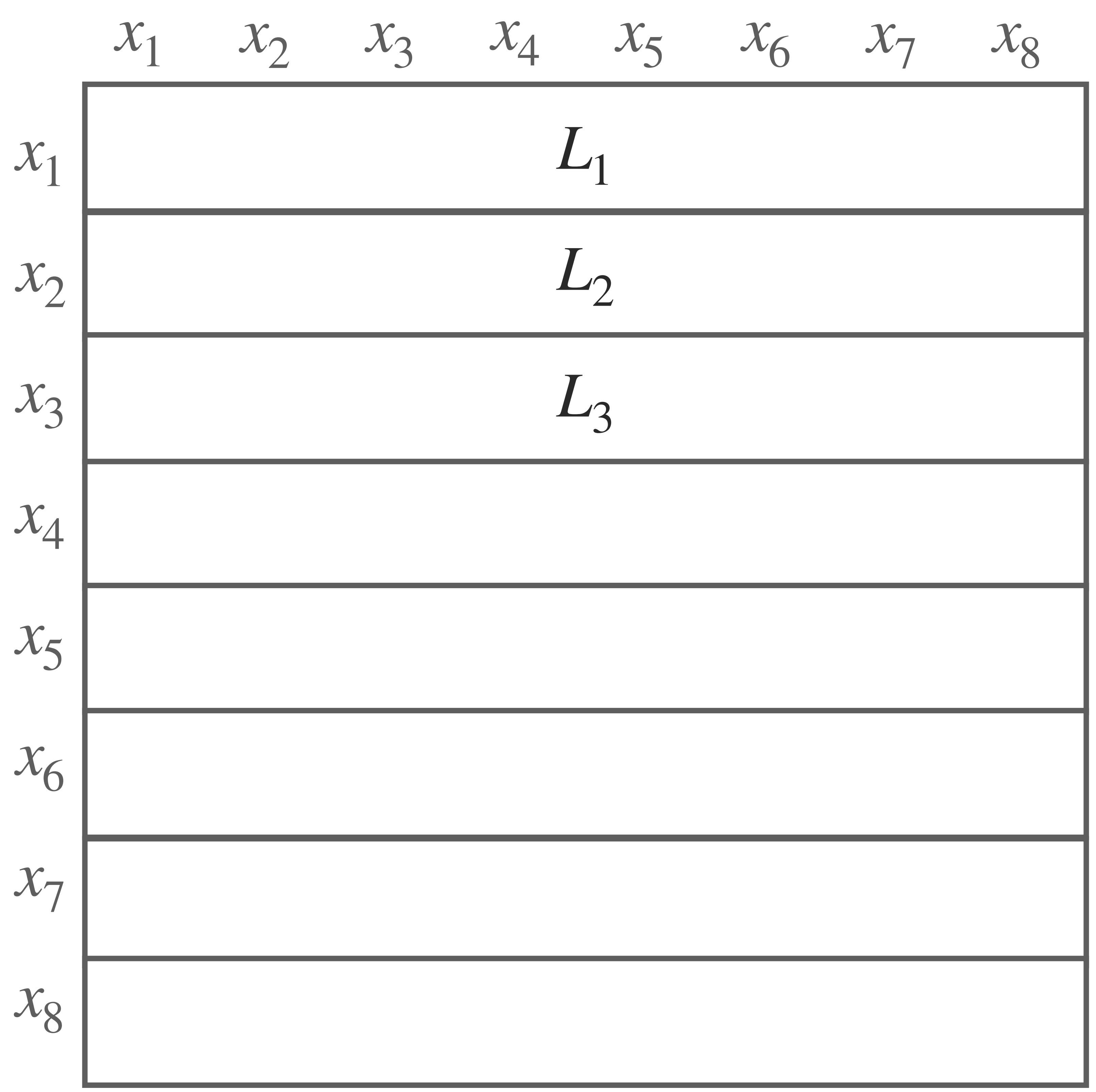
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



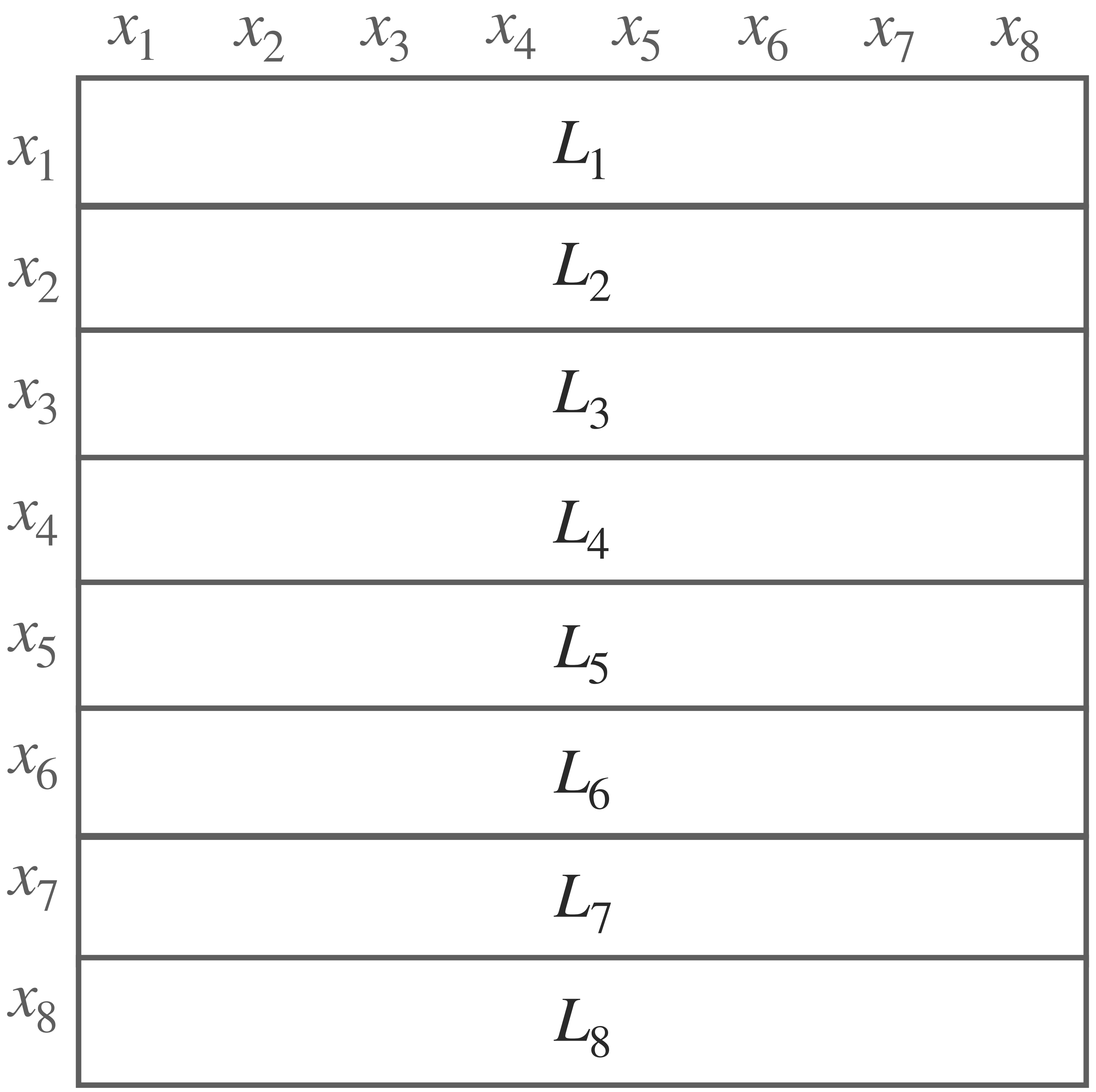
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



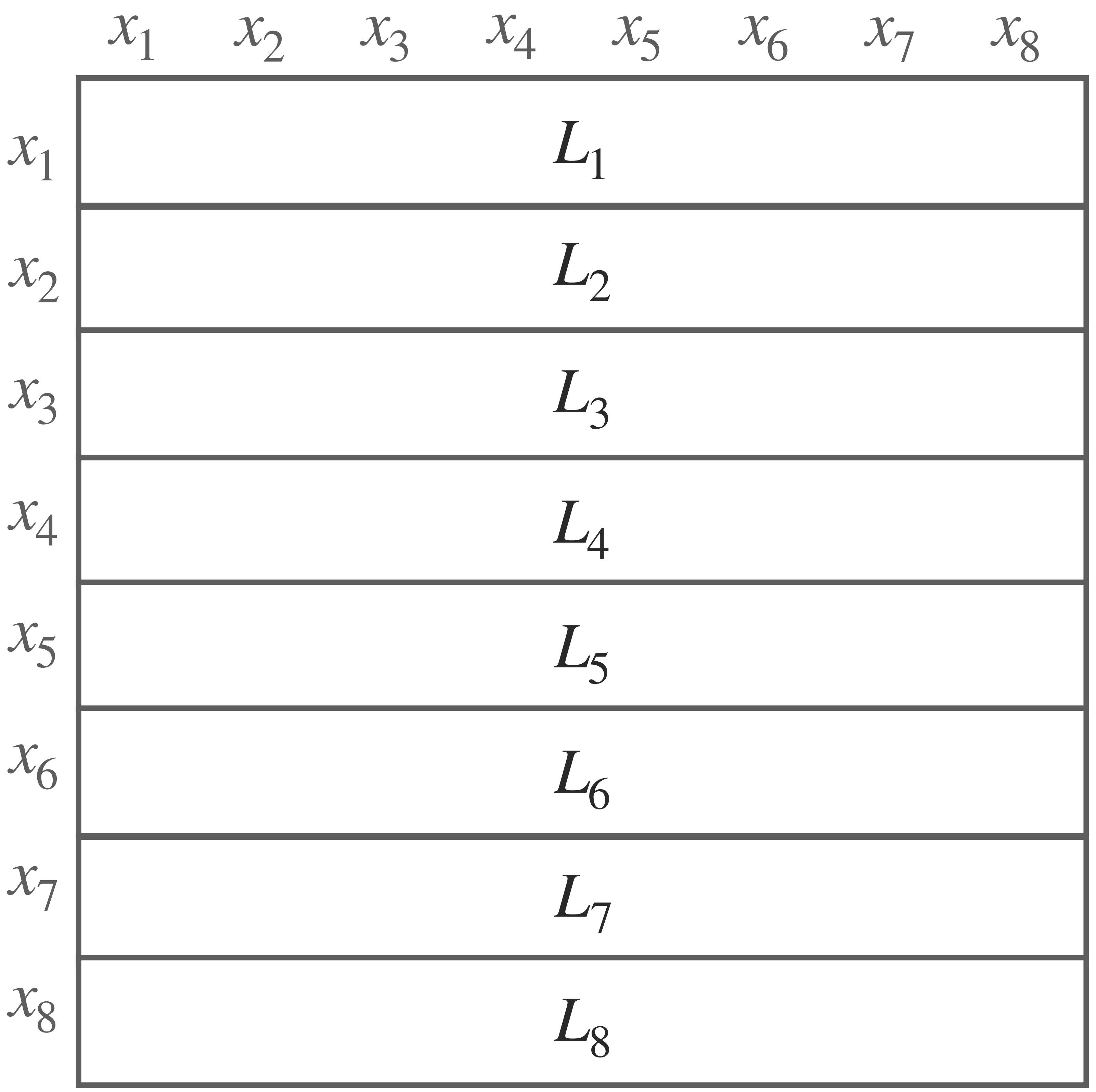
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



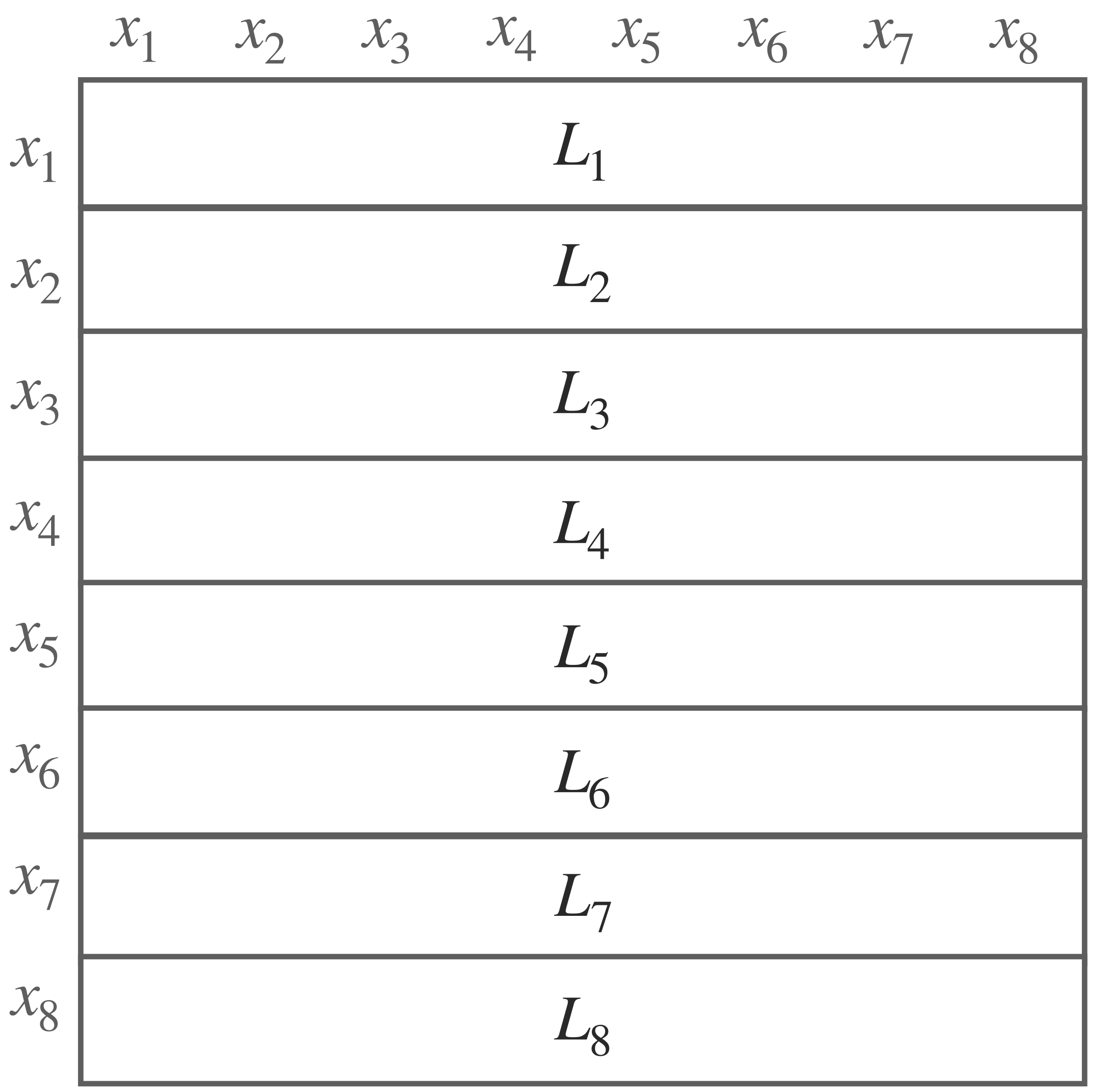
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



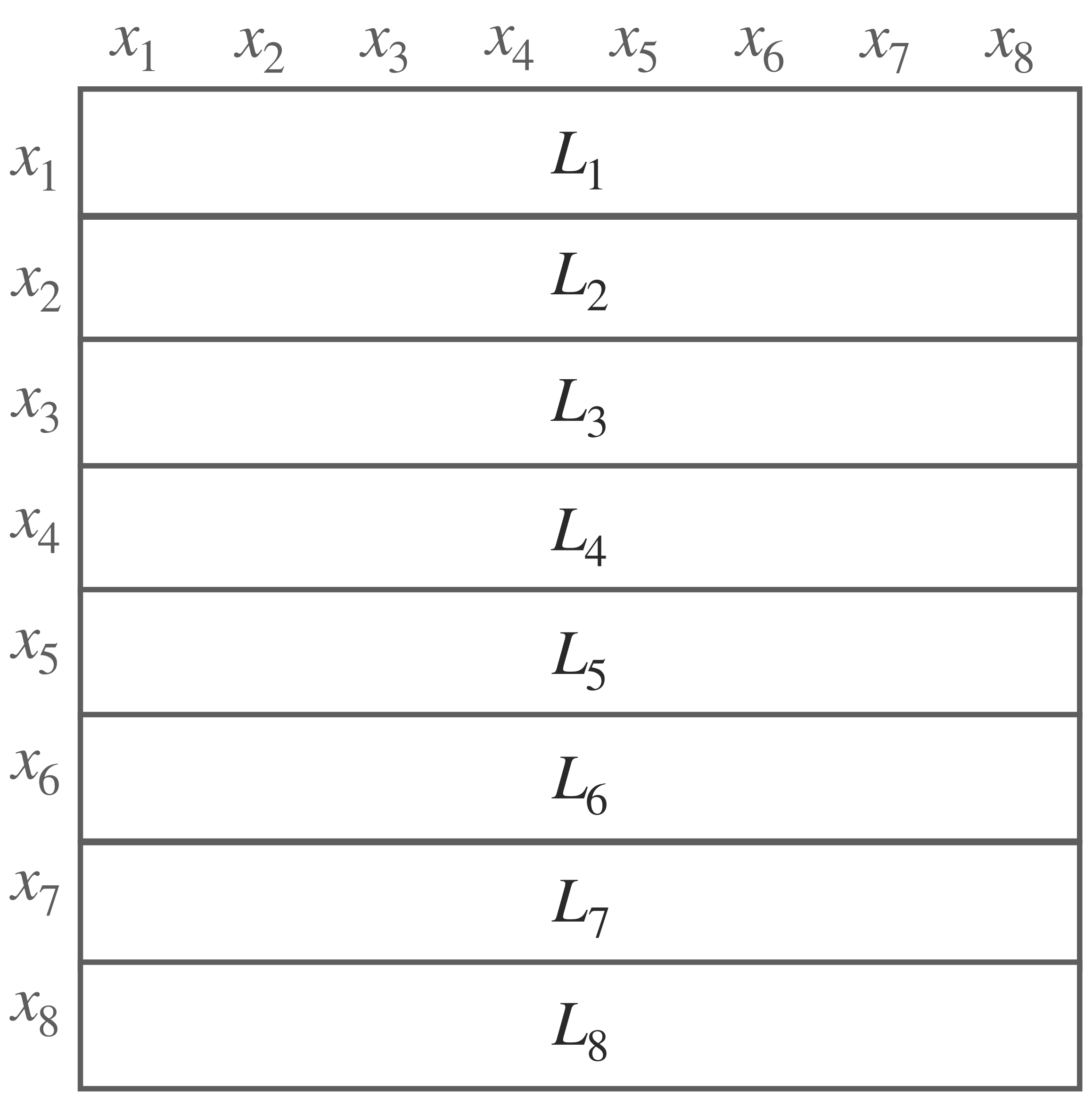
Quadratic maps in MQ-Sign-LR

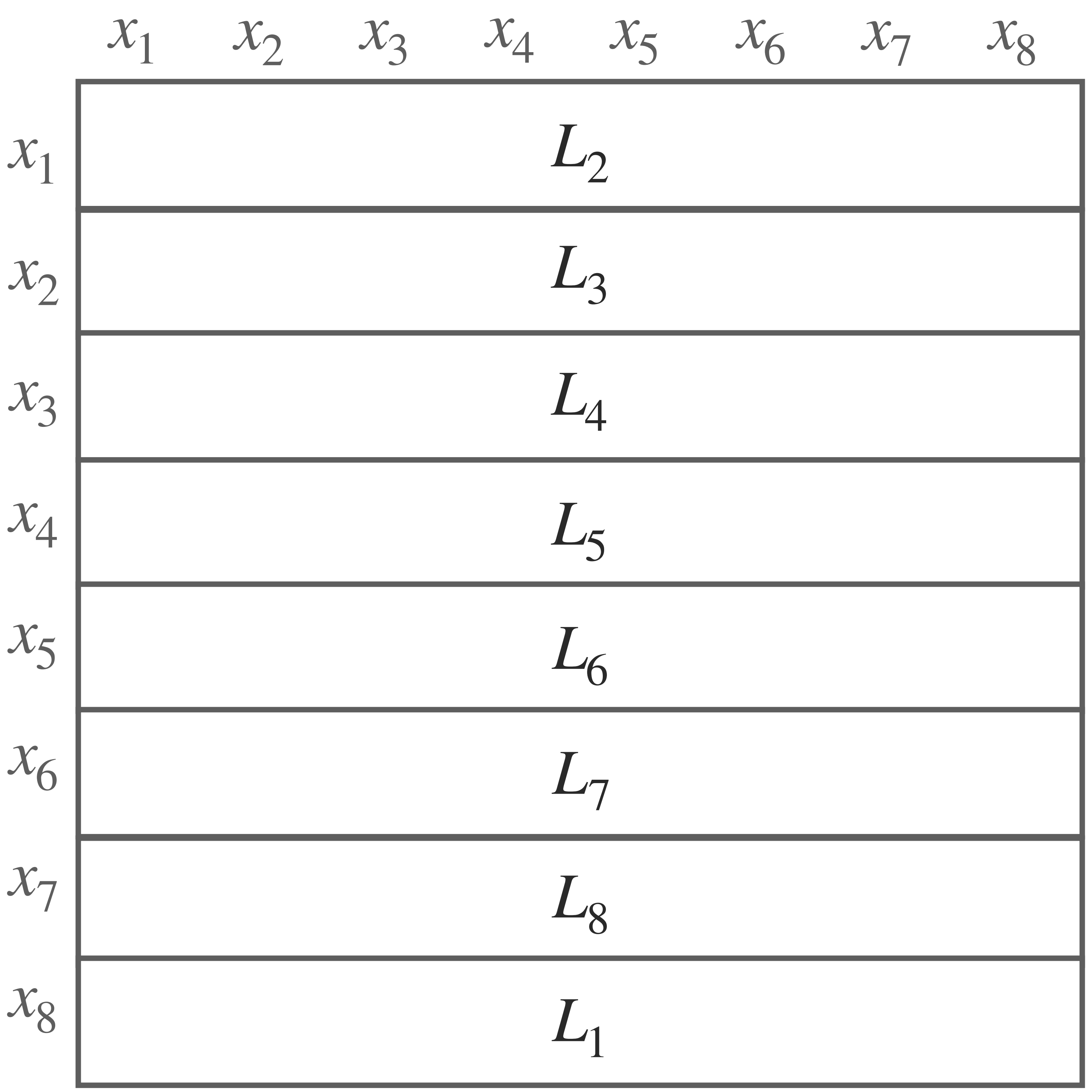
$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$





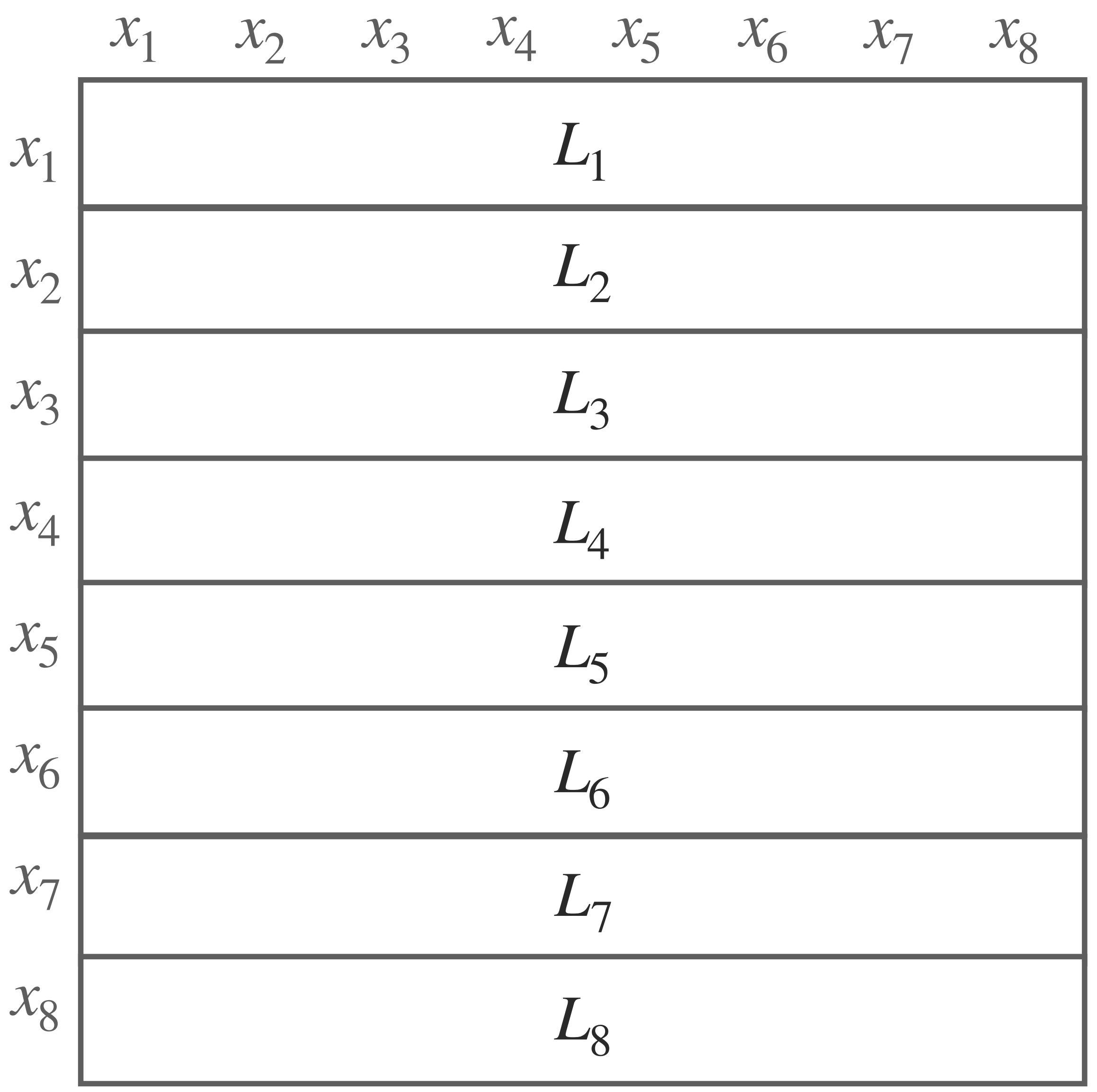
Quadratic maps in MQ-Sign-LR

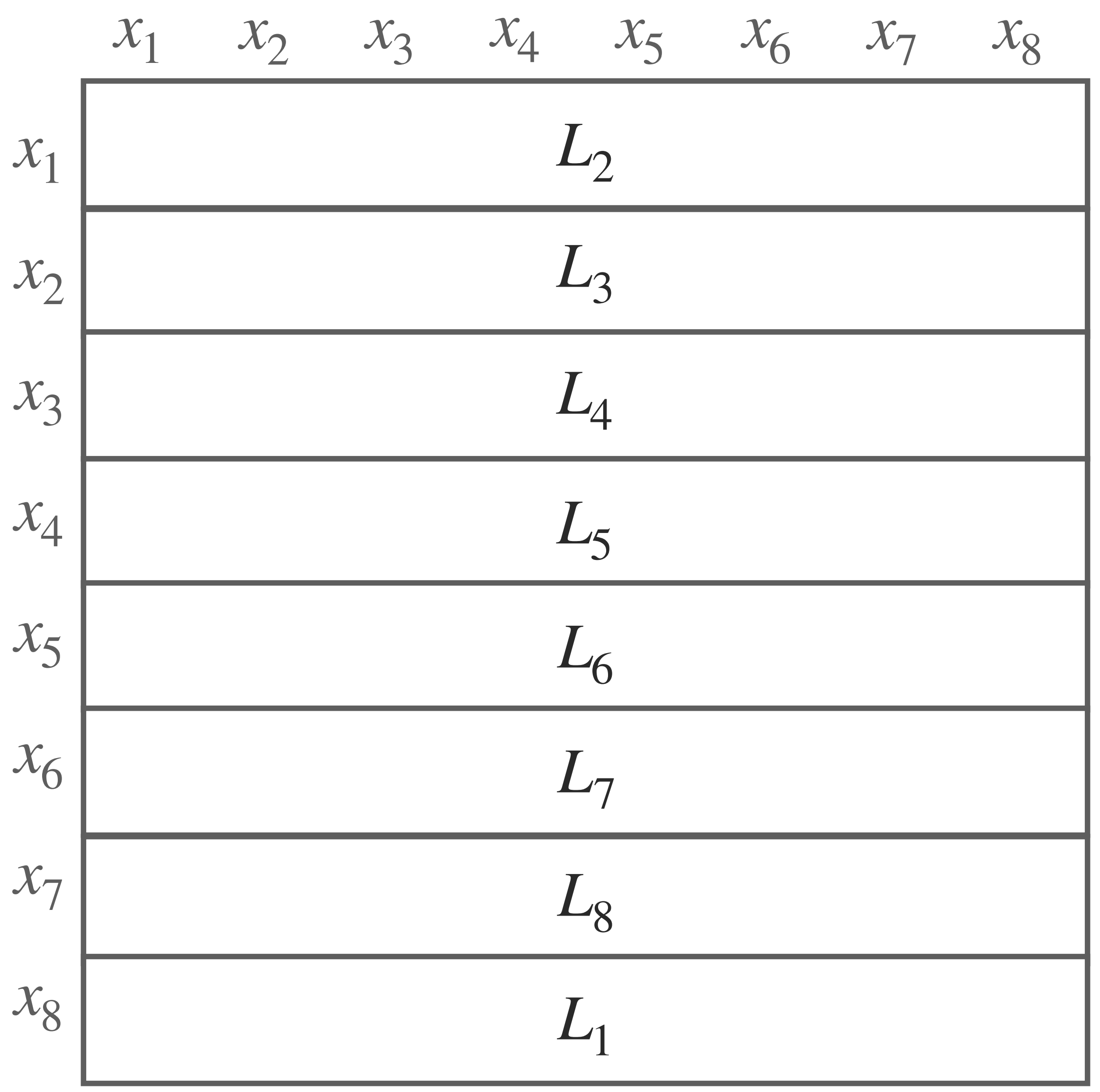
$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$





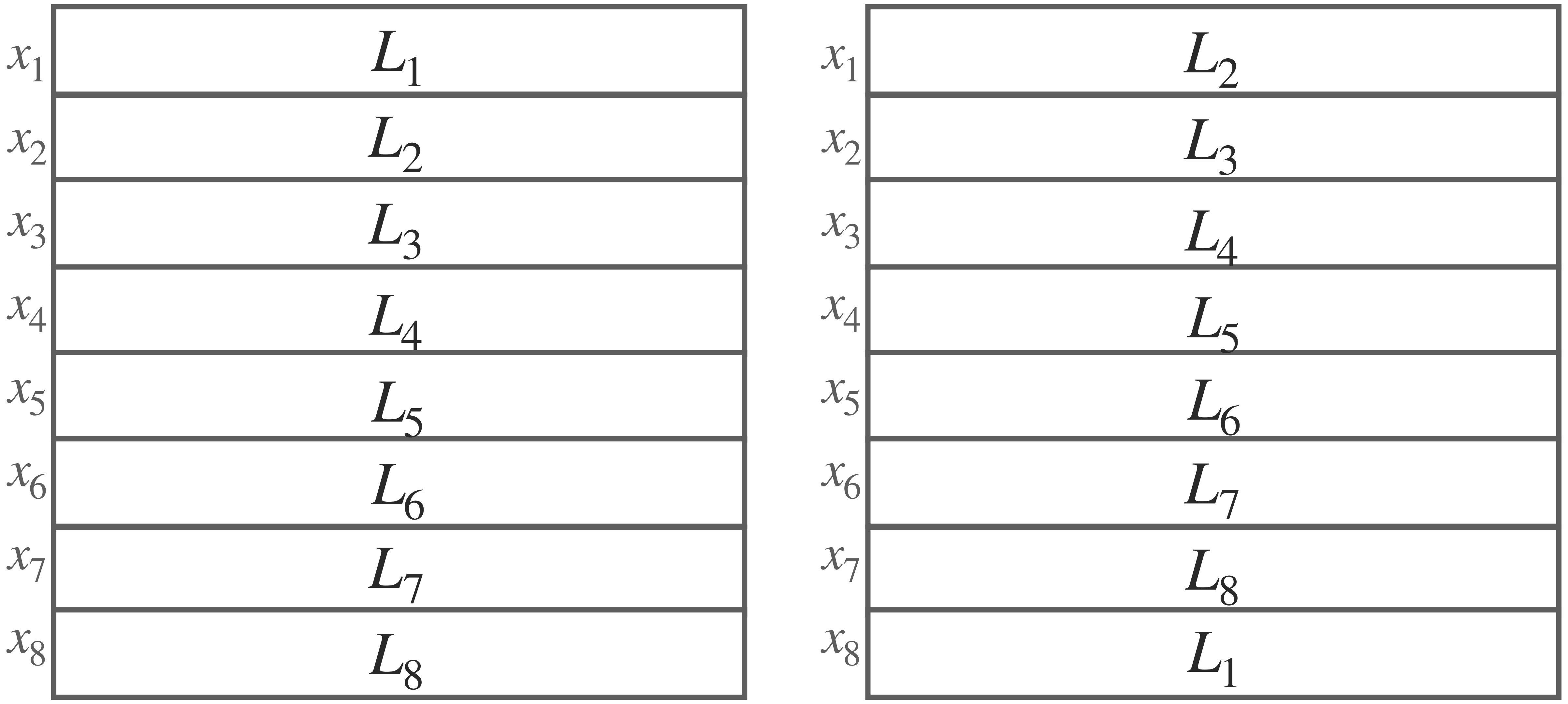
Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$



Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

x_1	L_1
x_2	L_2
x_3	L_3
x_4	L_4
x_5	L_5
x_6	L_6
x_7	L_7
x_8	L_8

x_1	L_2
x_2	L_3
x_3	L_4
x_4	L_5
x_5	L_6
x_6	L_7
x_7	L_8
x_8	L_1

x_1	L_2
x_2	L_3
x_3	L_4
x_4	L_5
x_5	L_6
x_6	L_7
x_7	L_8
x_8	L_1

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

x_1	L_1
x_2	L_2
x_3	L_3
x_4	L_4
x_5	L_5
x_6	L_6
x_7	L_7
x_8	L_8

x_1	L_2
x_2	L_3
x_3	L_4
x_4	L_5
x_5	L_6
x_6	L_7
x_7	L_8
x_8	L_1

x_1	L_3
x_2	L_4
x_3	L_5
x_4	L_6
x_5	L_7
x_6	L_8
x_7	L_1
x_8	L_2

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

x_1	L_1
x_2	L_2
x_3	L_3
x_4	L_4
x_5	L_5
x_6	L_6
x_7	L_7
x_8	L_8

x_1	L_2
x_2	L_3
x_3	L_4
x_4	L_5
x_5	L_6
x_6	L_7
x_7	L_8
x_8	L_1

x_1	L_3
x_2	L_4
x_3	L_5
x_4	L_6
x_5	L_7
x_6	L_8
x_7	L_1
x_8	L_2

x_1	L_3
x_2	L_4
x_3	L_5
x_4	L_6
x_5	L_7
x_6	L_8
x_7	L_1
x_8	L_2

Quadratic maps in MQ-Sign-LR

$$x_1L_1 + x_2L_2 + x_3L_3 + x_4L_4 + x_5L_5 + x_6L_6 + x_7L_7 + x_8L_8 = 0$$

$$x_1L_2 + x_2L_3 + x_3L_4 + x_4L_5 + x_5L_6 + x_6L_7 + x_7L_8 + x_8L_1 = 0$$

$$x_1L_3 + x_2L_4 + x_3L_5 + x_4L_6 + x_5L_7 + x_6L_8 + x_7L_1 + x_8L_2 = 0$$

$$x_1L_4 + x_2L_5 + x_3L_6 + x_4L_7 + x_5L_8 + x_6L_1 + x_7L_2 + x_8L_3 = 0$$

x_1	L_1	x_1	L_2	x_1	L_3	x_1	L_4
x_2	L_2	x_2	L_3	x_2	L_4	x_2	L_5
x_3	L_3	x_3	L_4	x_3	L_5	x_3	L_6
x_4	L_4	x_4	L_5	x_4	L_6	x_4	L_7
x_5	L_5	x_5	L_6	x_5	L_7	x_5	L_8
x_6	L_6	x_6	L_7	x_6	L_8	x_6	L_1
x_7	L_7	x_7	L_8	x_7	L_1	x_7	L_2
x_8	L_8	x_8	L_1	x_8	L_2	x_8	L_3

Forging a signature

$$\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$

$$\mathbf{x}_v^\top \mathbf{P}_1^{(2)} \mathbf{x}_v = 0$$

$$\dots$$

$$\mathbf{x}_v^\top \mathbf{P}_1^{(m)} \mathbf{x}_v = 0$$

Forging a signature

$$\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\mathbf{x}_v^\top \mathbf{P}_1^{(2)} \mathbf{x}_v = 0$$
$$\ldots$$
$$\mathbf{x}_v^\top \mathbf{P}_1^{(m)} \mathbf{x}_v = 0$$

T is the matrix representing the permutation corresponding to a cyclic upward row shift.

$$\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\mathbf{x}_v^\top \mathbf{T}\mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\ldots$$
$$\mathbf{x}_v^\top \mathbf{T}^{m-1}\mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$

Forging a signature

$$\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\mathbf{x}_v^\top \mathbf{P}_1^{(2)} \mathbf{x}_v = 0$$
$$\dots$$
$$\mathbf{x}_v^\top \mathbf{P}_1^{(m)} \mathbf{x}_v = 0$$

$$\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\mathbf{x}_v^\top \mathbf{T}\mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\dots$$
$$\mathbf{x}_v^\top \mathbf{T}^{m-1}\mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$

T is the matrix representing the permutation corresponding to a cyclic upward row shift.

In our example:

1							
	1						
		1					
			1				
				1			
					1		
						1	
							1

Forging a signature

$$\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\mathbf{x}_v^\top \mathbf{P}_1^{(2)} \mathbf{x}_v = 0$$
$$\ldots$$
$$\mathbf{x}_v^\top \mathbf{P}_1^{(m)} \mathbf{x}_v = 0$$

$$\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\mathbf{x}_v^\top \mathbf{T}\mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$
$$\ldots$$
$$\mathbf{x}_v^\top \mathbf{T}^{m-1}\mathbf{P}_1^{(1)} \mathbf{x}_v = 0$$

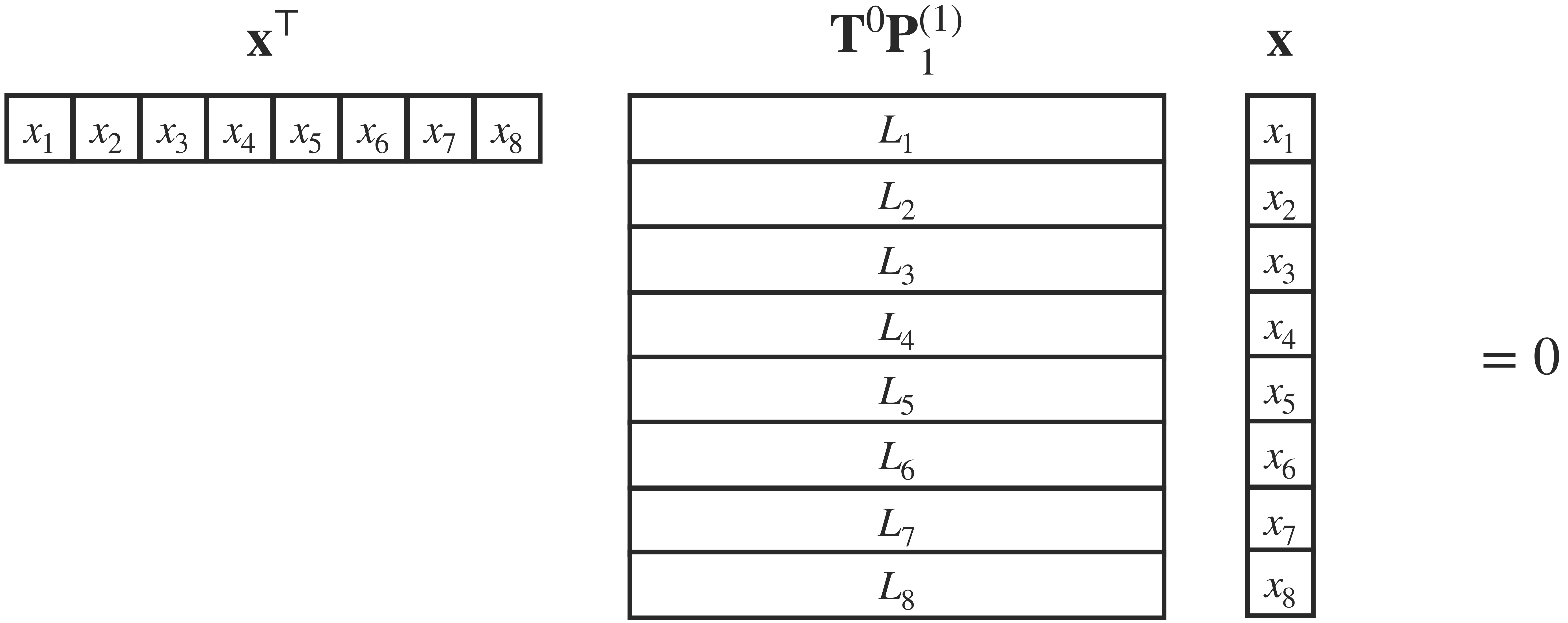
T is the matrix representing the permutation corresponding to a cyclic upward row shift.

In our example:

	1						
		1					
			1				
				1			
					1		
						1	
							1
1							

Forging a signature

First view: **T** permutes the rows of the quadratic map.



Forging a signature

First view: **T** permutes the rows of the quadratic map.

$$\mathbf{x}^\top \; \mathbf{T}^0\mathbf{P}_1^{(1)} \; \mathbf{x} = 0$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8

$\mathbf{T}^0\mathbf{P}_1^{(1)}$	$\mathbf{x}$
L_2	x_1
L_3	x_2
L_4	x_3
L_5	x_4
L_6	x_5
L_7	x_6
L_8	x_7
L_1	x_8

$= 0$

Forging a signature

First view: **T** permutes the rows of the quadratic map.

$$\underbrace{\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \end{pmatrix}}_{\mathbf{x}^\top} \underbrace{\begin{pmatrix} L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \\ L_1 \end{pmatrix}}_{\mathbf{T}^1\mathbf{P}_1^{(1)}} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}}_{\mathbf{x}} = 0$$

Forging a signature

First view: **T** permutes the rows of the quadratic map.

$$\mathbf{x}^\top \; \mathbf{T}^1\mathbf{P}_1^{(1)} \; \mathbf{x}$$

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \end{bmatrix} \begin{bmatrix} L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \\ L_1 \\ L_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = 0$$

Forging a signature

First view: $\mathbf{T}$ permutes the rows of the quadratic map.

$$\underbrace{\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \end{pmatrix}}_{\mathbf{x}^\top} \underbrace{\begin{pmatrix} L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \\ L_1 \\ L_2 \end{pmatrix}}_{\mathbf{T}^2\mathbf{P}_1^{(1)}} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}}_{\mathbf{x}} = 0$$

Forging a signature

First view: $\mathbf{T}$ permutes the rows of the quadratic map.

$$\underbrace{\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \end{bmatrix}}_{\mathbf{x}^\top} \underbrace{\begin{bmatrix} L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \\ L_1 \\ L_2 \\ L_3 \end{bmatrix}}_{\mathbf{T}^2\mathbf{P}_1^{(1)}} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix}}_{\mathbf{x}} = 0$$

Forging a signature

First view: $\mathbf{T}$ permutes the rows of the quadratic map.

$$\mathbf{x}^\top \; \mathbf{T}^3\mathbf{P}_1^{(1)} \; \mathbf{x} = 0$$

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \end{pmatrix} \begin{pmatrix} L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \\ L_1 \\ L_2 \\ L_3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = 0$$

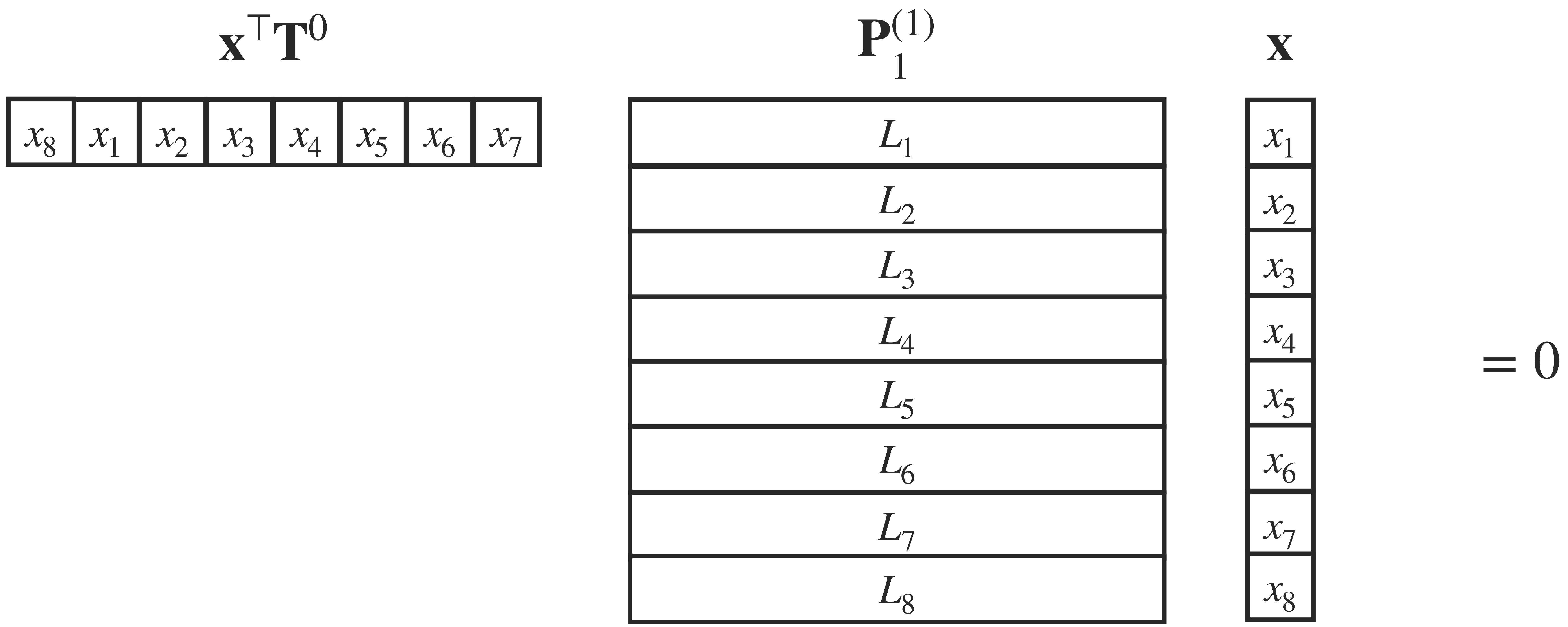
Forging a signature

Second view: **T** permutes the columns of the left vector.

$$\underbrace{\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \end{bmatrix}}_{\mathbf{x}^\top \mathbf{T}^0} \underbrace{\begin{bmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{bmatrix}}_{\mathbf{P}_1^{(1)}} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix}}_{\mathbf{x}} = 0$$

Forging a signature

Second view: $\mathbf{T}$ permutes the columns of the left vector.



Forging a signature

Second view: $\mathbf{T}$ permutes the columns of the left vector.

$$\underbrace{\begin{pmatrix} x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \end{pmatrix}}_{\mathbf{x}^\top \mathbf{T}^1} \underbrace{\begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix}}_{\mathbf{P}_1^{(1)}} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}}_{\mathbf{x}} = 0$$

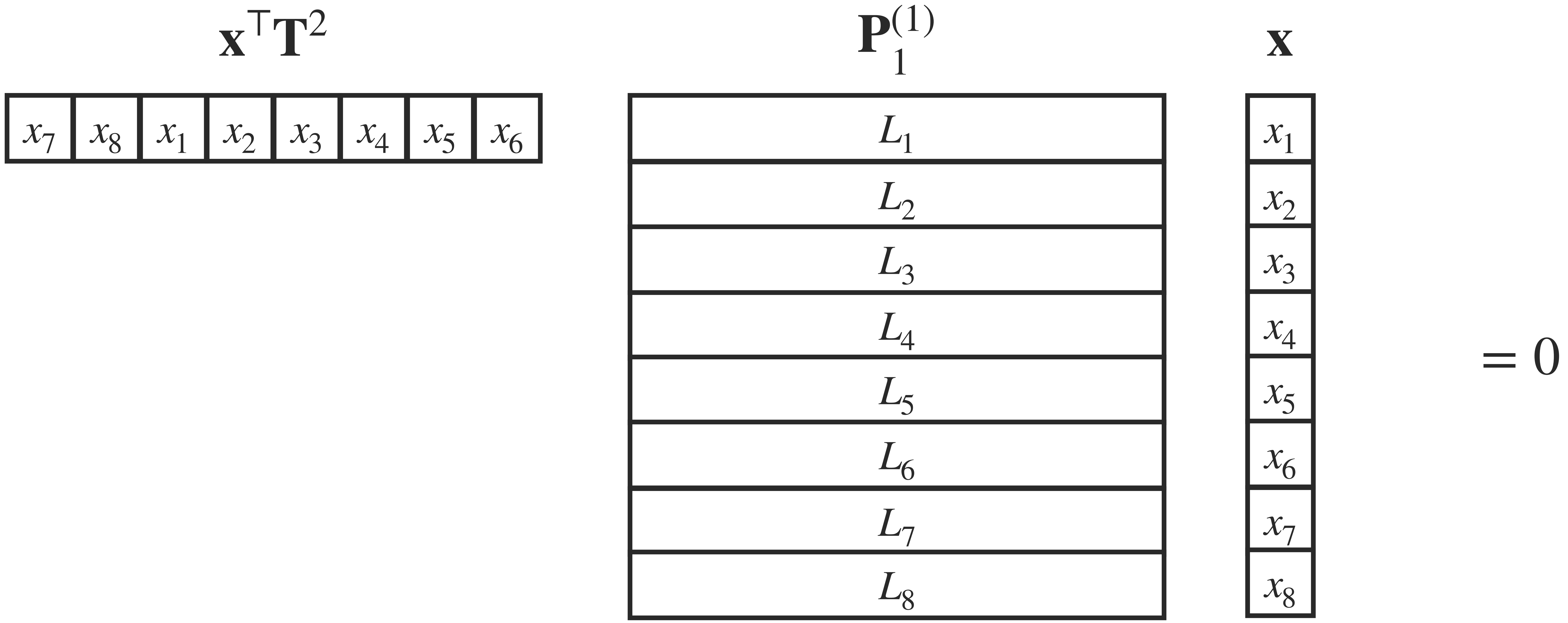
Forging a signature

Second view: **T** permutes the columns of the left vector.

$$
\underbrace{\begin{pmatrix} x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix}}_{\mathbf{x}^\top \mathbf{T}^1}
\underbrace{\begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix}}_{\mathbf{P}_1^{(1)}}
\underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}}_{\mathbf{x}}
= 0
$$

Forging a signature

Second view: **T** permutes the columns of the left vector.



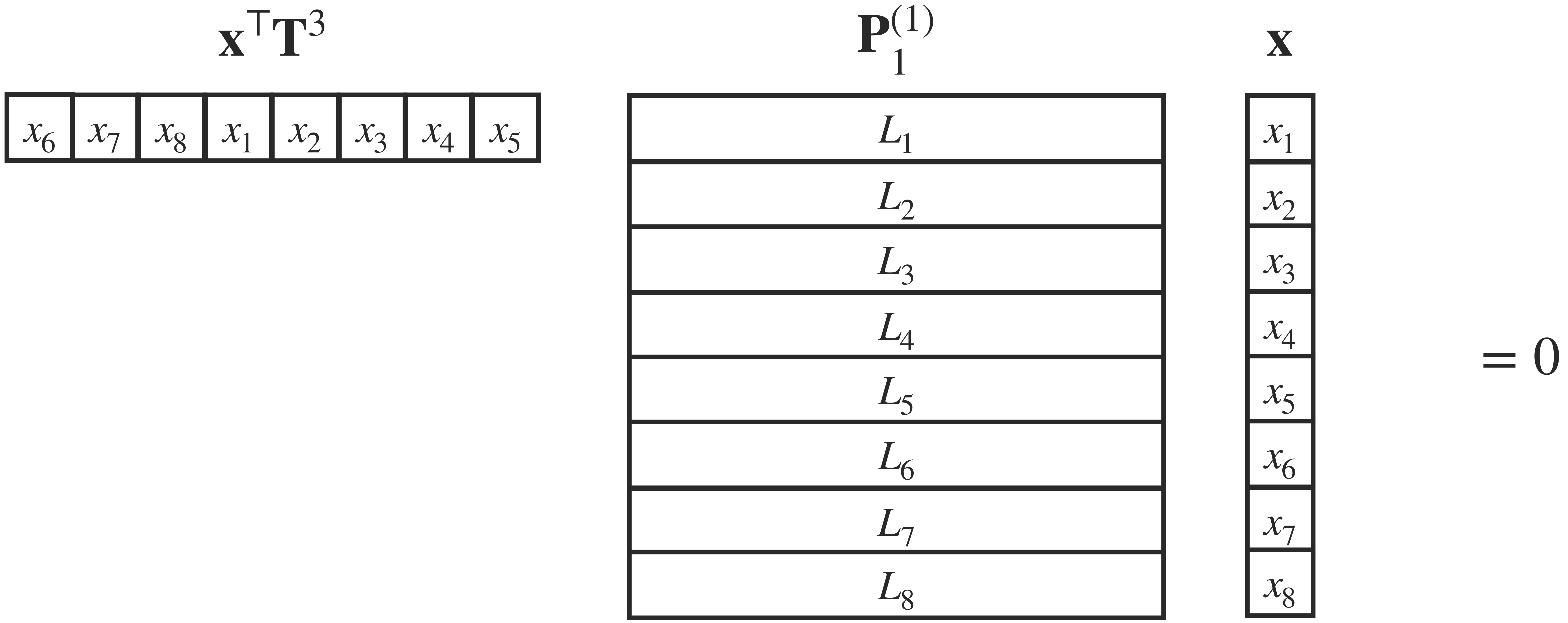
Forging a signature

Second view: **T** permutes the columns of the left vector.

$$\underbrace{\begin{bmatrix} x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 & x_5 \end{bmatrix}}_{\mathbf{x}^\top \mathbf{T}^2} \underbrace{\begin{bmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{bmatrix}}_{\mathbf{P}_1^{(1)}} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix}}_{\mathbf{x}} = 0$$

Forging a signature

Second view: $\mathbf{T}$ permutes the columns of the left vector.

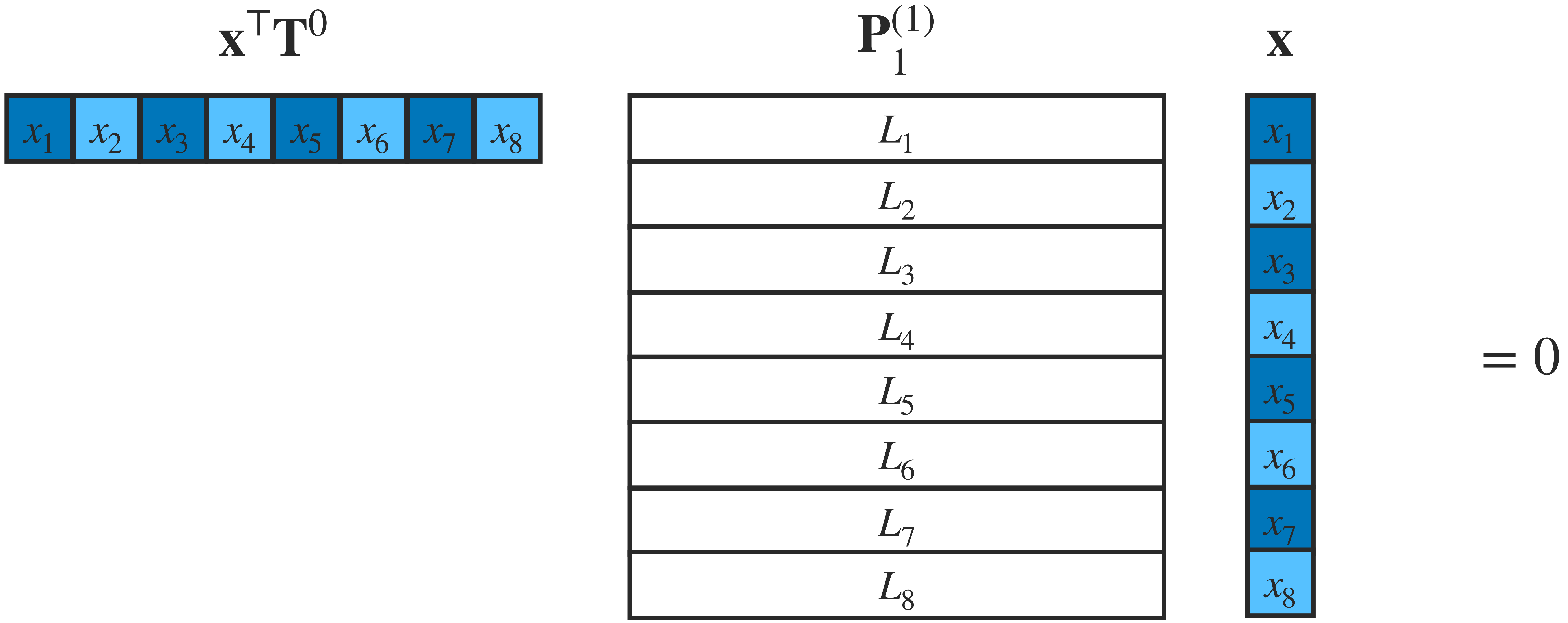


Attack

Vectors that have a repeating subsequence need to satisfy fewer constraints.

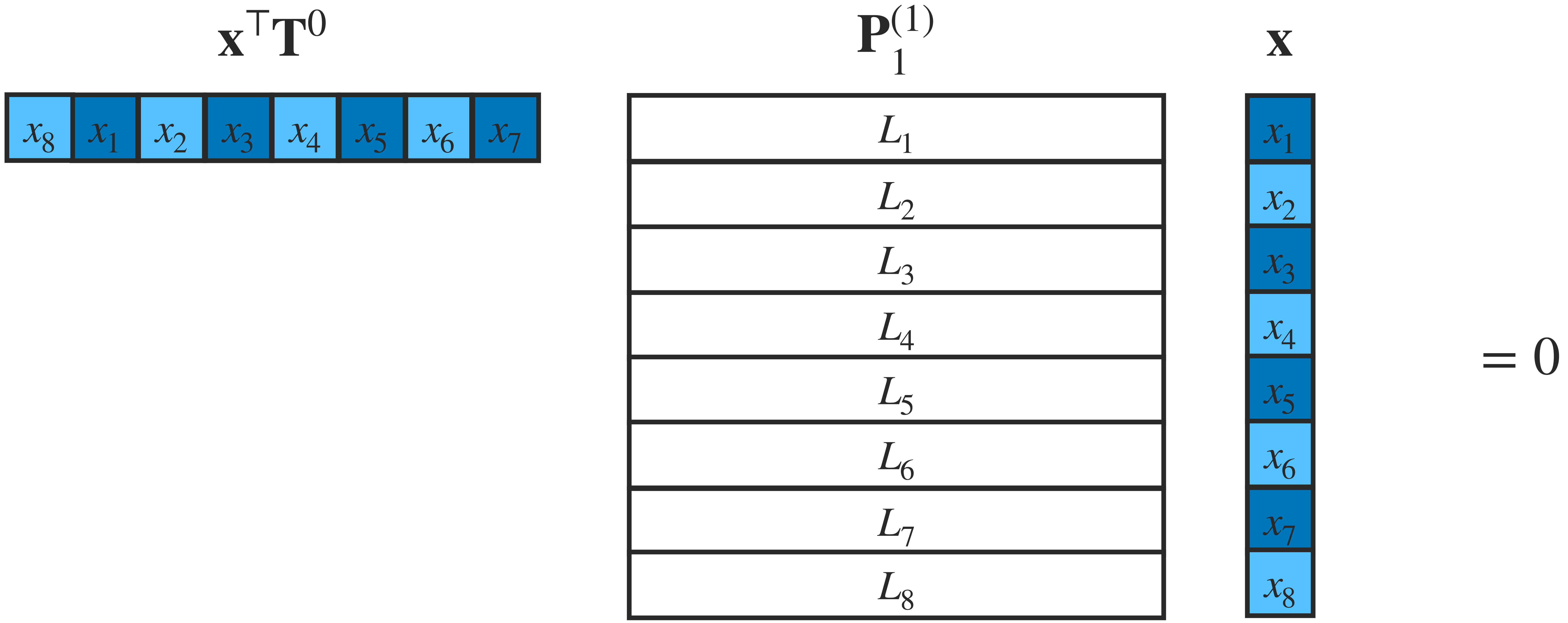
Attack

Example: $\mathbf{x}$ is a 2-periodic vector.



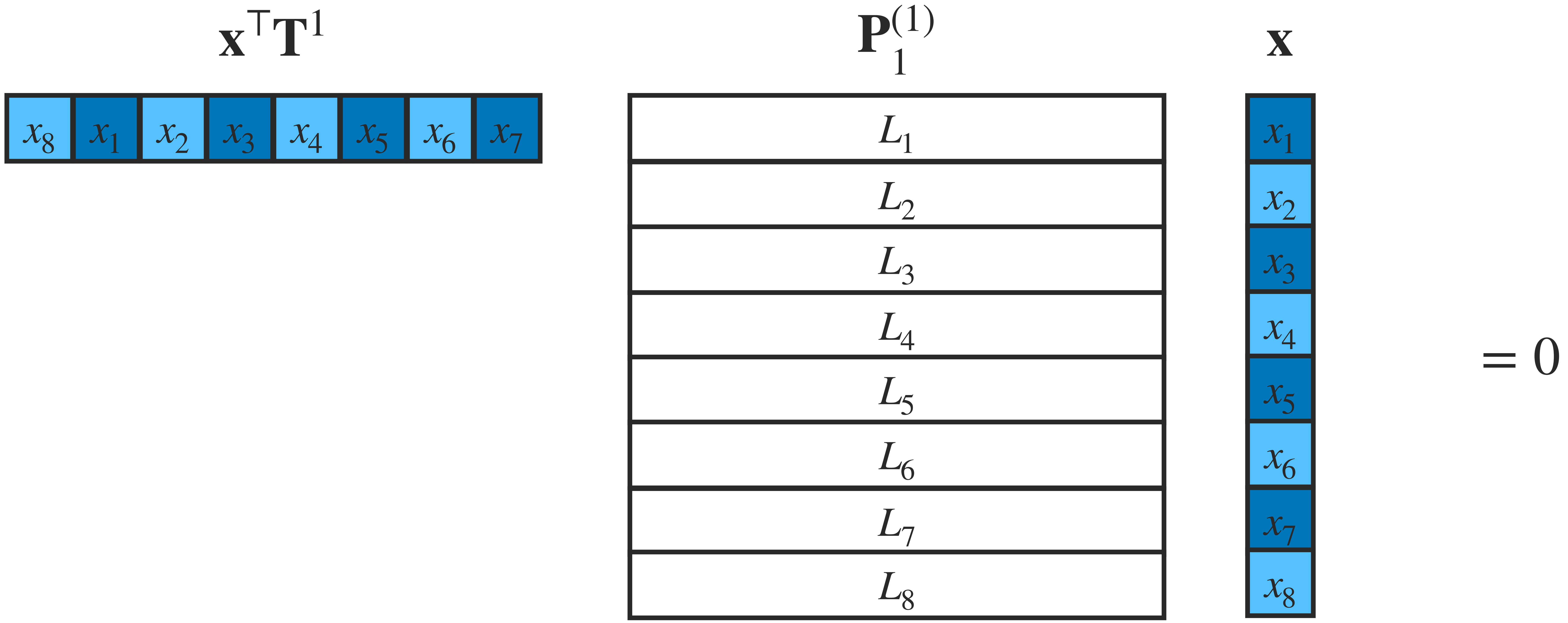
Attack

Example: $\mathbf{x}$ is a 2-periodic vector.



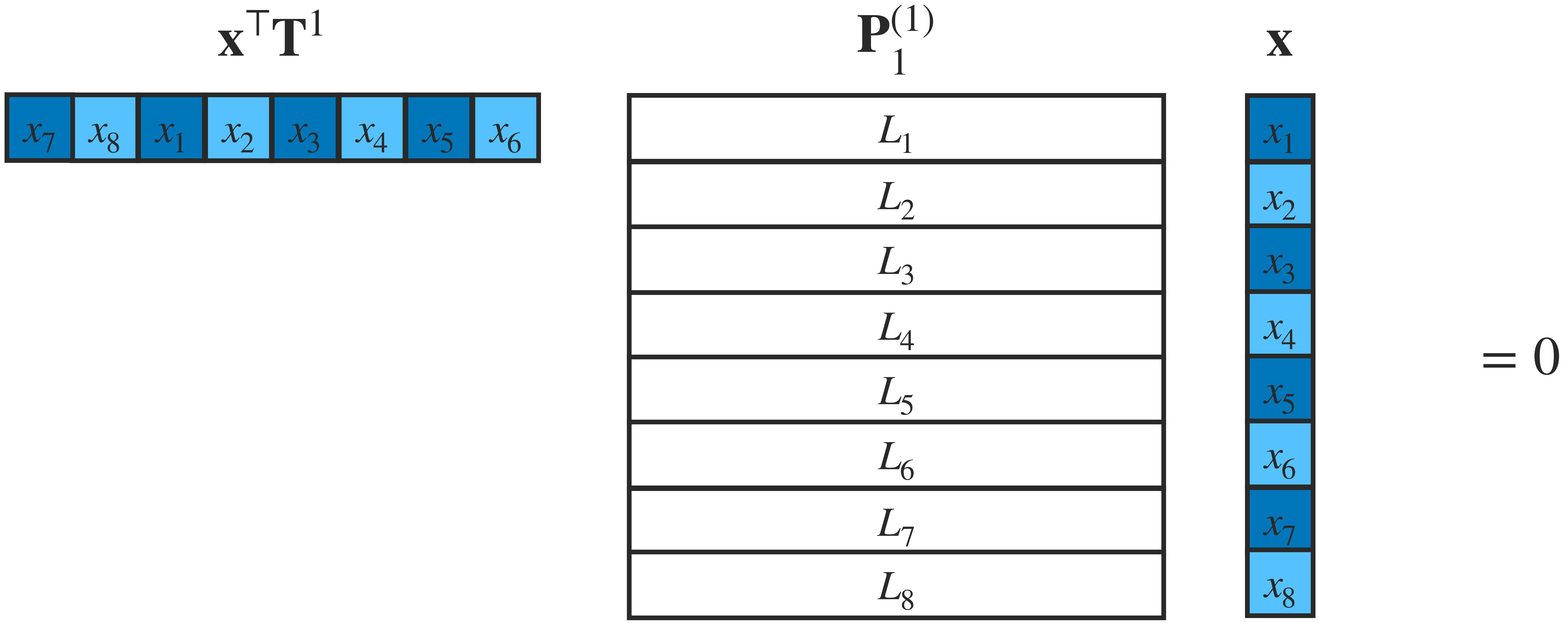
Attack

Example: $\mathbf{x}$ is a 2-periodic vector.



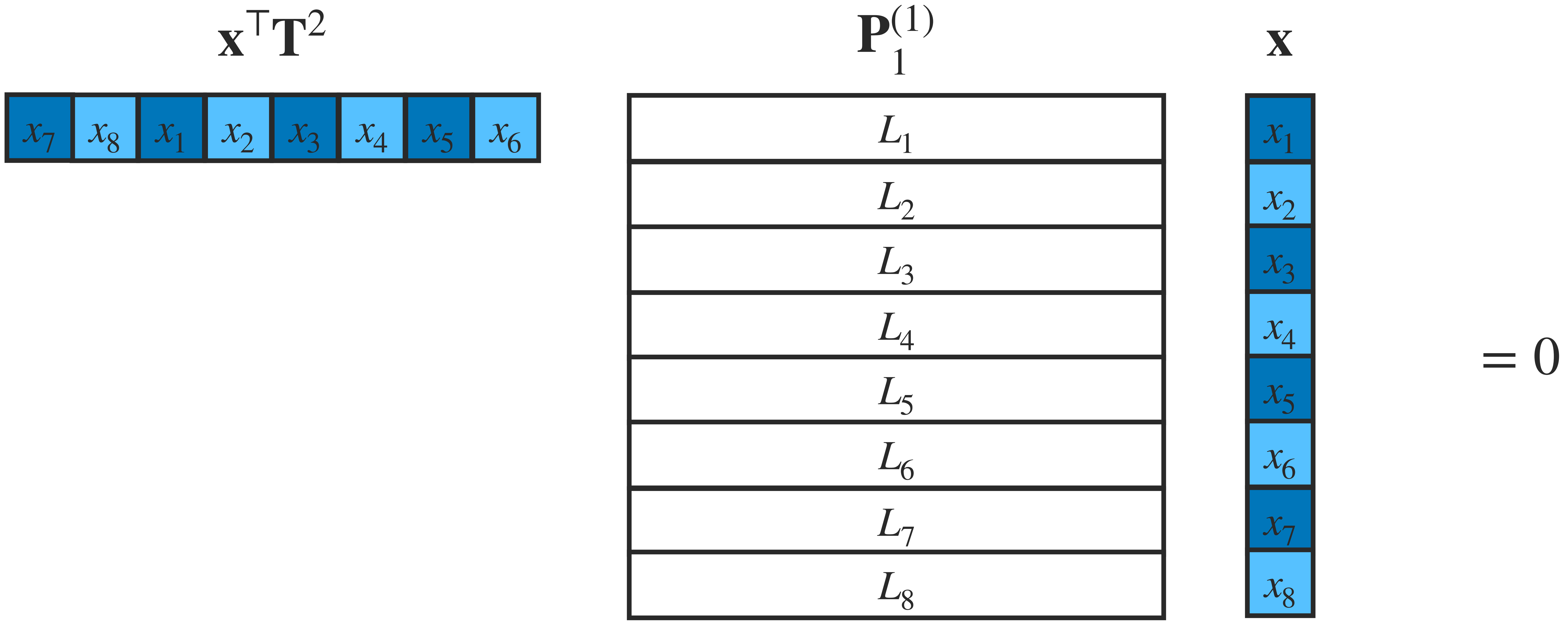
Attack

Example: **x** is a 2-periodic vector.



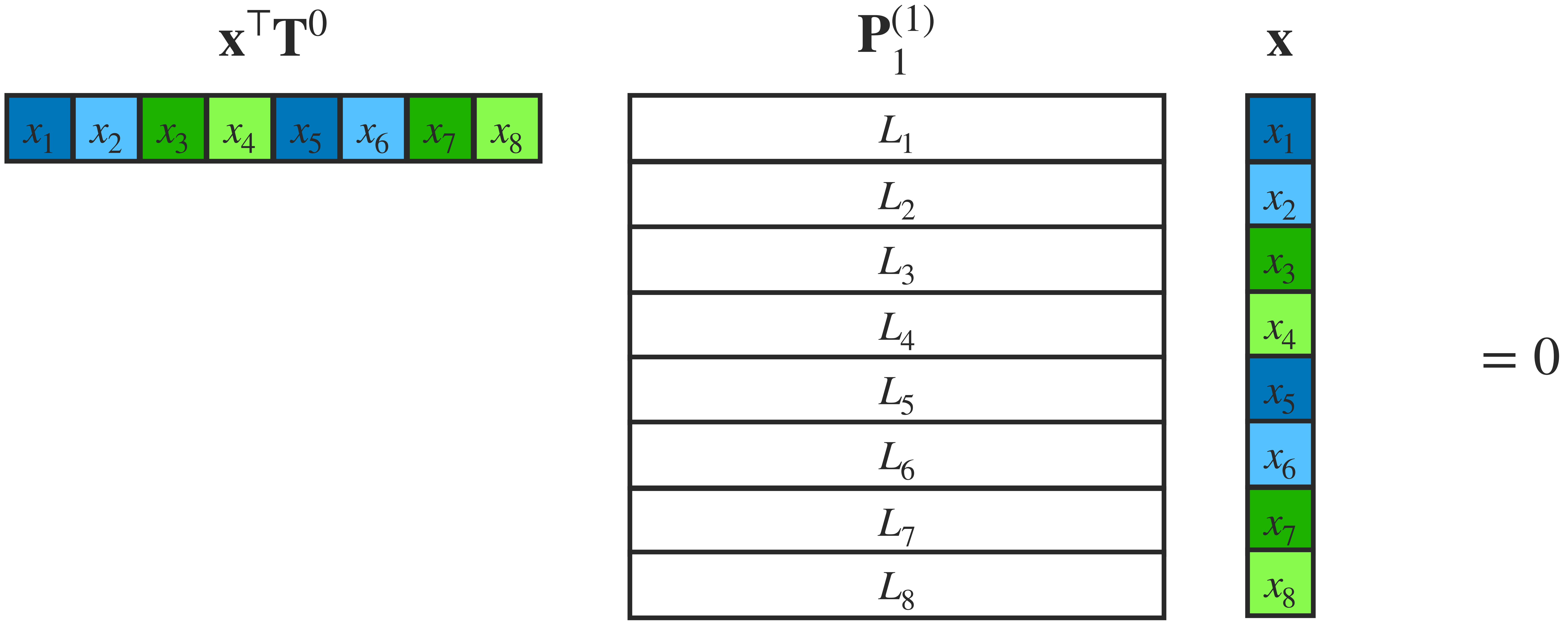
Attack

Example: $\mathbf{x}$ is a 2-periodic vector.



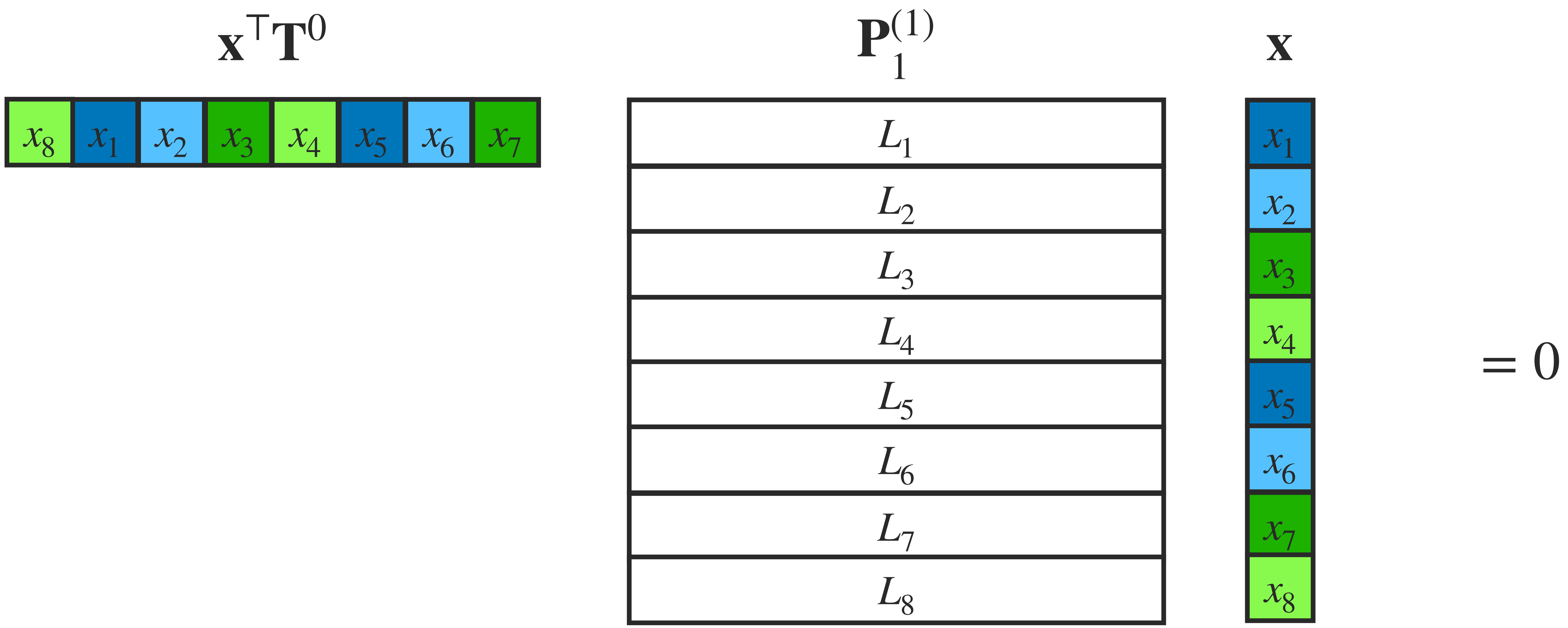
Attack

Example: $\mathbf{x}$ is a 4-periodic vector.



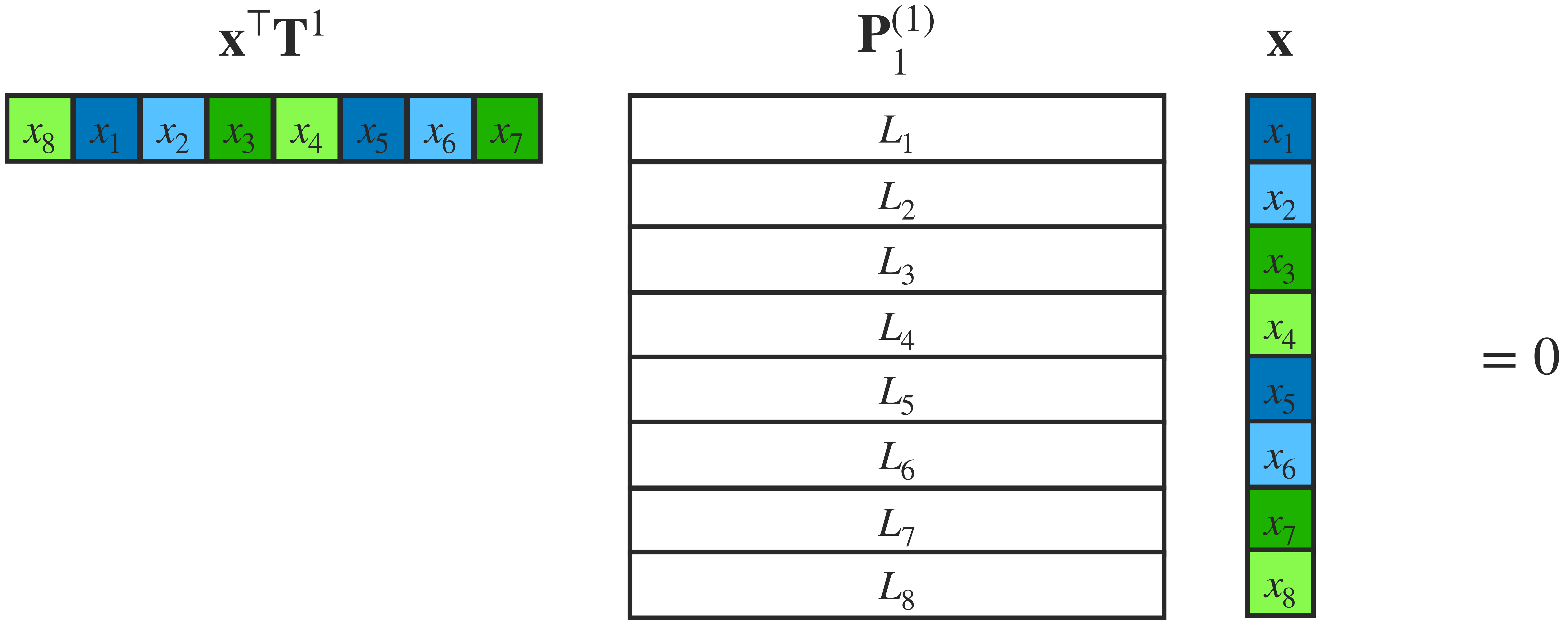
Attack

Example: $\mathbf{x}$ is a 4-periodic vector.



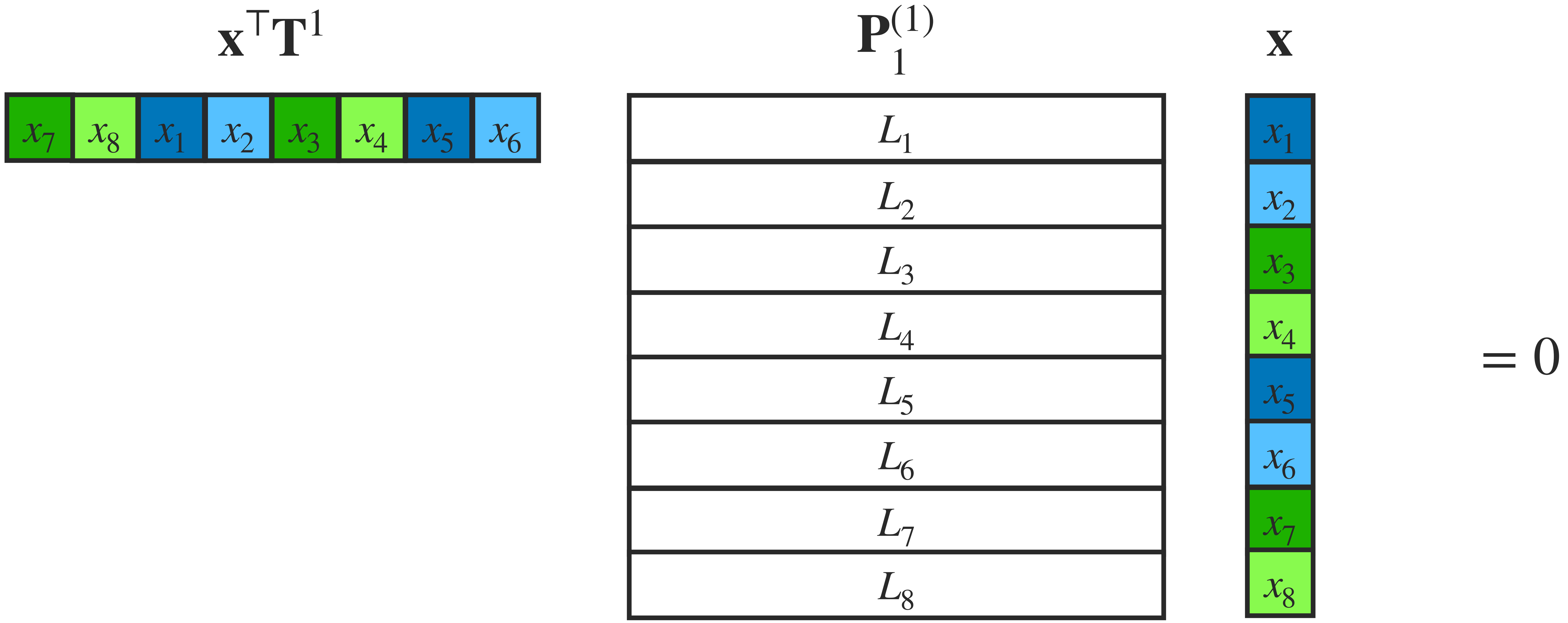
Attack

Example: $\mathbf{x}$ is a 4-periodic vector.



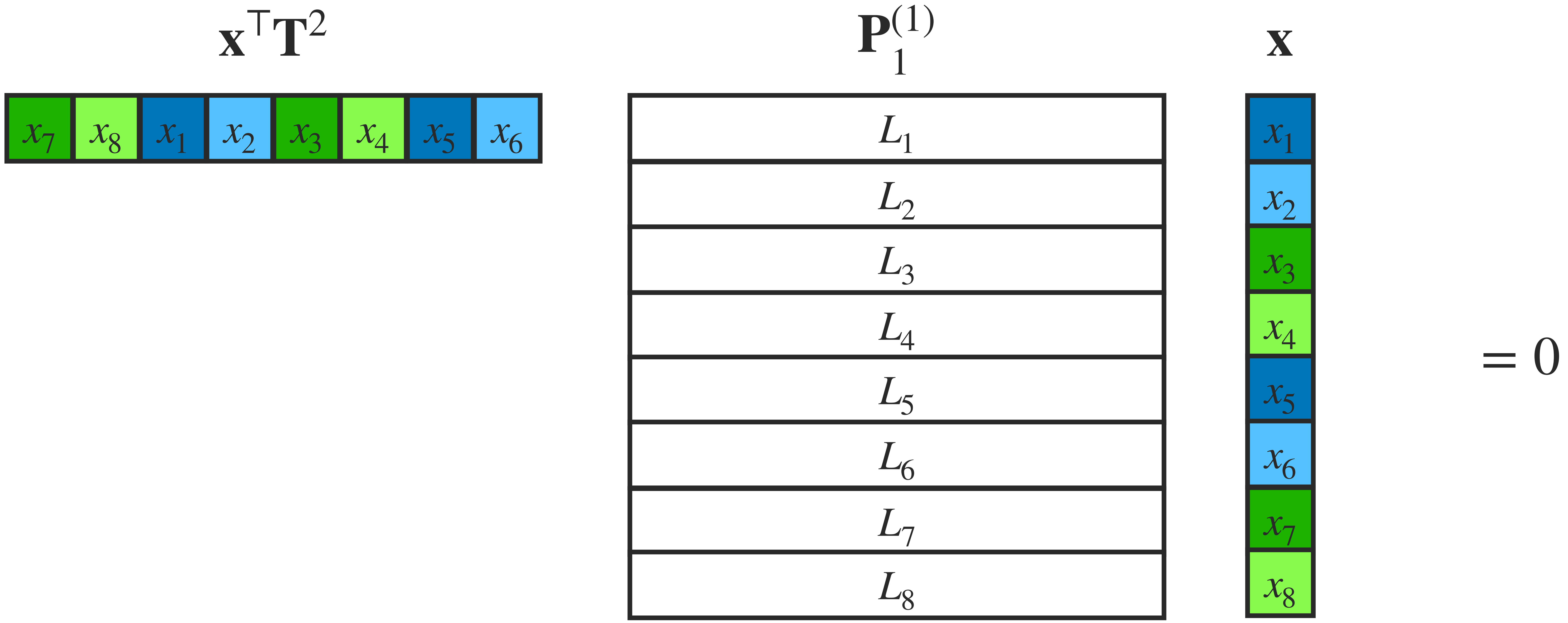
Attack

Example: $\mathbf{x}$ is a 4-periodic vector.



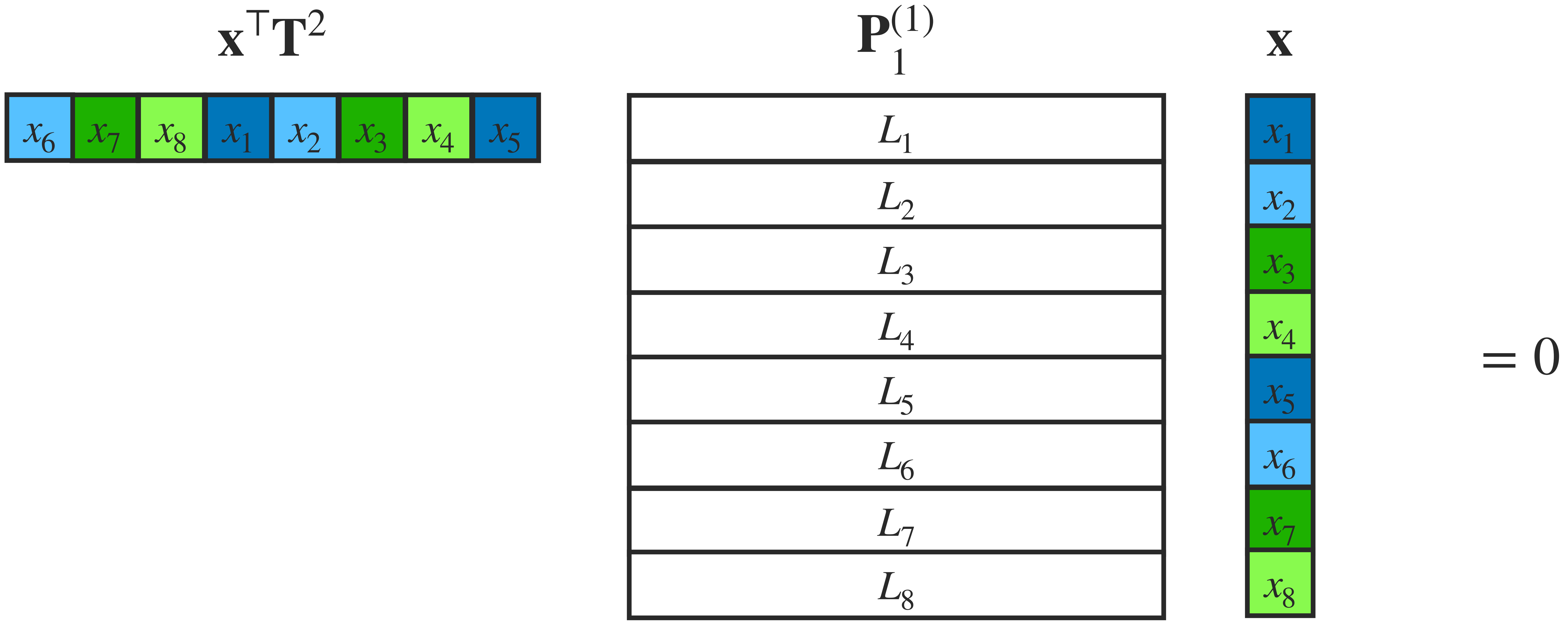
Attack

Example: **x** is a 4-periodic vector.



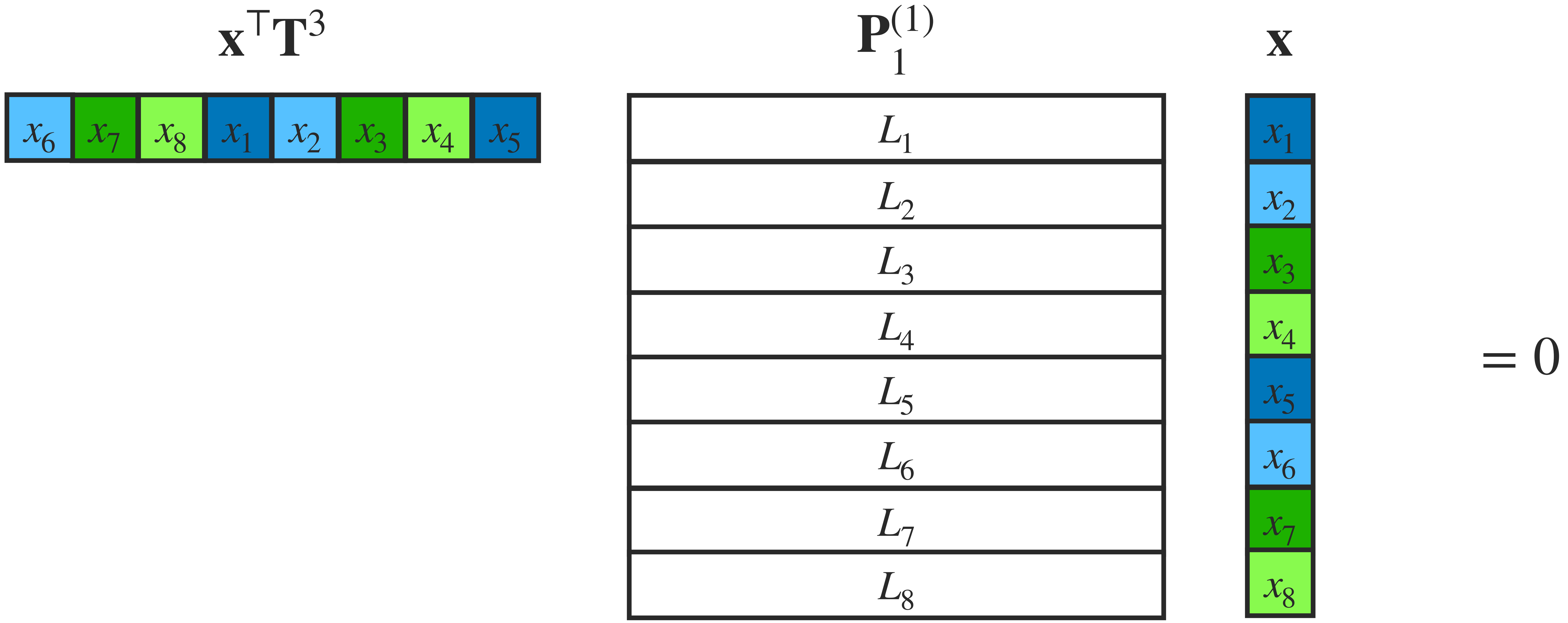
Attack

Example: $\mathbf{x}$ is a 4-periodic vector.



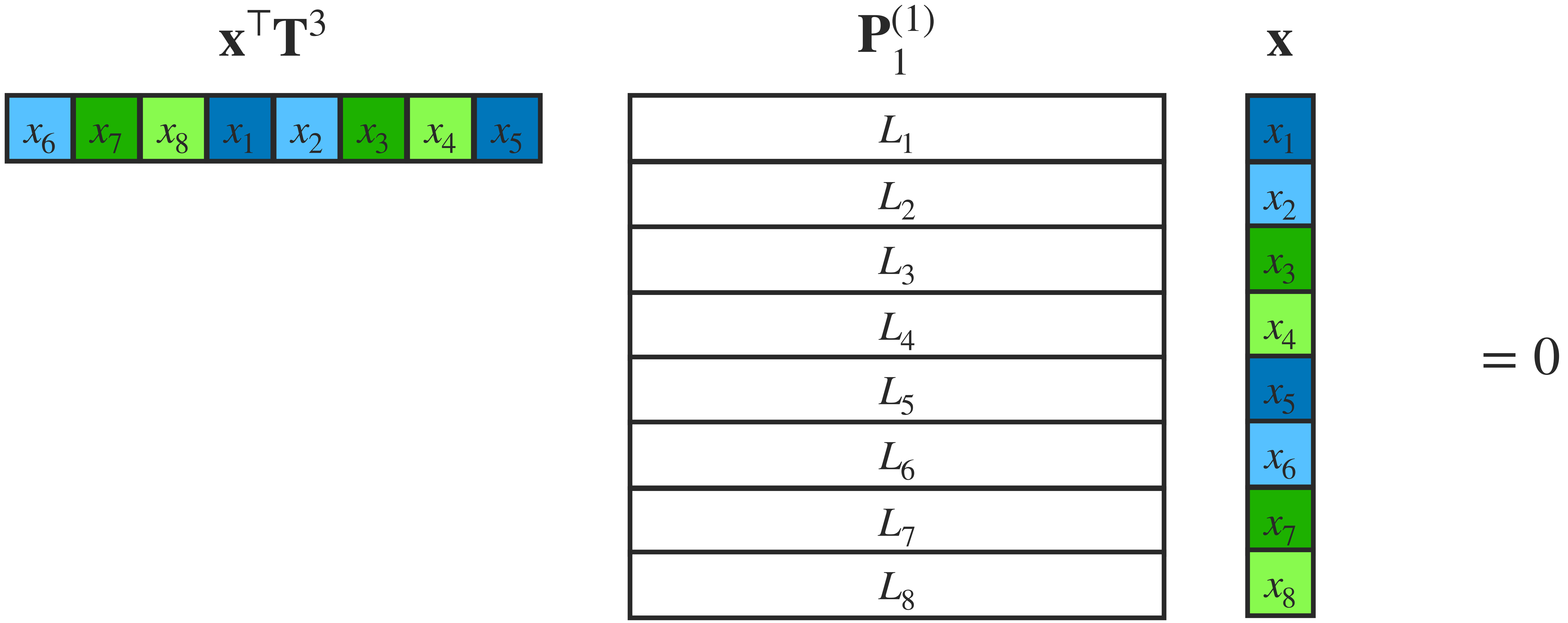
Attack

Example: $\mathbf{x}$ is a 4-periodic vector.



Attack

Example: $\mathbf{x}$ is a 4-periodic vector (if a 5th equation existed).



Attack

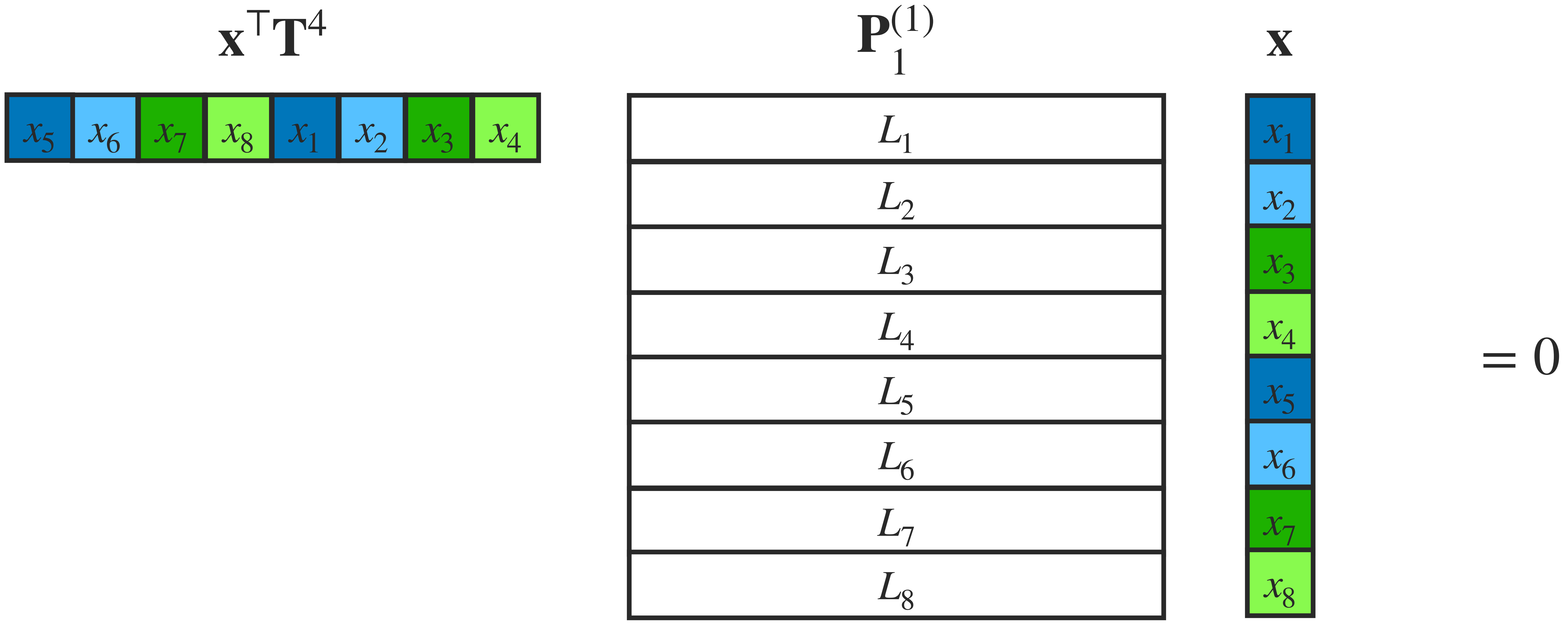
Example: $\mathbf{x}$ is a 4-periodic vector (if a 5th equation existed).

$$\mathbf{x}^\top \mathbf{T}^3 \; \mathbf{P}_1^{(1)} \; \mathbf{x} = 0$$

$$\begin{bmatrix} x_5 & x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 \end{bmatrix} \begin{bmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = 0$$

Attack

Example: $\mathbf{x}$ is a 4-periodic vector (if a 5th equation existed).



Attack

Example: $\mathbf{x}$ is a 4-periodic vector (if a 5th equation existed).

$$\underbrace{\begin{pmatrix} x_5 & x_6 & x_7 & x_8 & x_1 & x_2 & x_3 & x_4 \end{pmatrix}}_{\mathbf{x}^\top \mathbf{T}^4} \underbrace{\begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \\ L_7 \\ L_8 \end{pmatrix}}_{\mathbf{P}_1^{(1)}} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}}_{\mathbf{x}} = 0$$

! We obtain repeating equations only because we needed to solve for target $\mathbf{w} = (0000)$, which is a 1-periodic target.

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

→ d' does not need to divide m: for $m > kd'$, append the corresponding $(k+1)d' - m$ equations.

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

→ d' does not need to divide m: for $m > kd'$, append the corresponding $(k+1)d' - m$ equations.

Example. $v = 72$, $m = 46$ (MQ-Sign security level I parameters).

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

→ d' does not need to divide m: for $m > kd'$, append the corresponding $(k+1)d' - m$ equations.

Example. $v = 72$, $m = 46$ (MQ-Sign security level I parameters).

- Having a 1-periodic target, we can look for a d-periodic solution for d in $\{1,2,3,4,6,8,9,12,18,24,36\}$.

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

→ d' does not need to divide m: for $m > kd'$, append the corresponding $(k+1)d' - m$ equations.

Example. $v = 72$, $m = 46$ (MQ-Sign security level I parameters).

- Having a 1-periodic target, we can look for a d-periodic solution for d in $\{1,2,3,4,6,8,9,12,18,24,36\}$.

- Having a 2-periodic target, we can look for a d-periodic solution for d in $\{2,4,6,8,12,18,24,36\}$.

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

→ d' does not need to divide m: for $m > kd'$, append the corresponding $(k+1)d' - m$ equations.

Example. $v = 72$, $m = 46$ (MQ-Sign security level I parameters).

- Having a 1-periodic target, we can look for a d-periodic solution for d in $\{1,2,3,4,6,8,9,12,18,24,36\}$.
- Having a 2-periodic target, we can look for a d-periodic solution for d in $\{2,4,6,8,12,18,24,36\}$.
- Having a 12-periodic target, we can look for a d-periodic solution for d in $\{12,24,36\}$.

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

→ d' does not need to divide m: for $m > kd'$, append the corresponding $(k+1)d' - m$ equations.

Example. $v = 72$, $m = 46$ (MQ-Sign security level I parameters).

- Having a 1-periodic target, we can look for a d-periodic solution for d in $\{1,2,3,4,6,8,9,12,18,24,36\}$.
- Having a 2-periodic target, we can look for a d-periodic solution for d in $\{2,4,6,8,12,18,24,36\}$.
- Having a 12-periodic target, we can look for a d-periodic solution for d in $\{12,24,36\}$.
- Having an 18-periodic target, we can look for a d-periodic solution for d in $\{18,36\}$.
- Having an 24-periodic target, we can look for a d-periodic solution for d in $\{24\}$.
- Having an 36-periodic target, we can look for a d-periodic solution for d in $\{36\}$.

Generalisation to other periodic targets

Having a d'-periodic target, for $d' \mid v$,

→ we can look for d-periodic solutions for any d such that $d' \mid d$ and $d \mid v$.

→ d' does not need to divide m: for $m > kd'$, append the corresponding $(k+1)d' - m$ equations.

Example. $v = 72$, $m = 46$ (MQ-Sign security level I parameters).

- Having a 1-periodic target, we can look for a d-periodic solution for d in $\{1,2,3,4,6,8,9,12,18,24,36\}$.
- Having a 2-periodic target, we can look for a d-periodic solution for d in $\{2,4,6,8,12,18,24,36\}$.
- Having a 12-periodic target, we can look for a d-periodic solution for d in $\{12,24,36\}$.
- Having an 18-periodic target, we can look for a d-periodic solution for d in $\{18,36\}$.
- Having an 24-periodic target, we can look for a d-periodic solution for d in $\{24\}$.
- Having an 36-periodic target, we can look for a d-periodic solution for d in $\{36\}$.

We call such d'-periodic targets weak targets.

Algebraic attack outline

→ For a d'-periodic target, we build the system comprised of the first d equations (for the largest d we can solve for) in the forgery modelisation.

$$\begin{aligned}
\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_1 \\
\mathbf{x}_v^\top \mathbf{T} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_2 \\
\dots \\
\mathbf{x}_v^\top \mathbf{T}^{d-1} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_{d-1}.
\end{aligned}$$

Algebraic attack outline

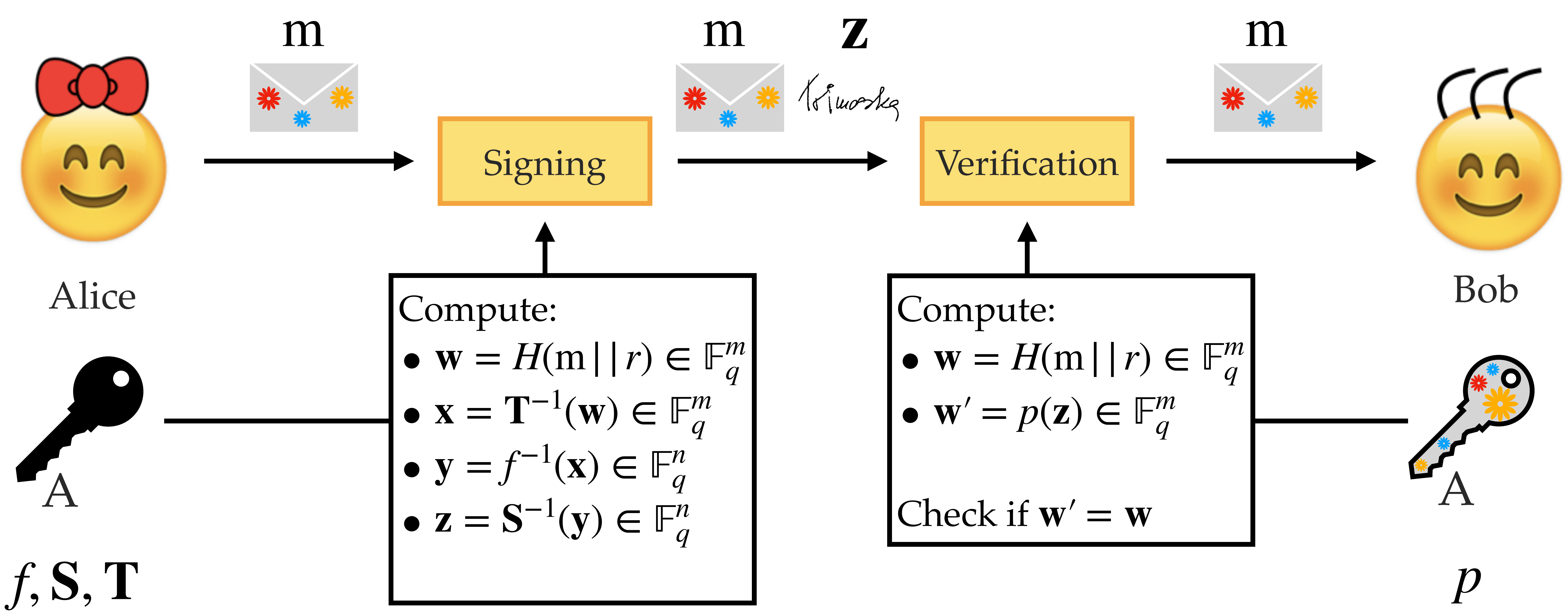
- For a d'-periodic target, we build the system comprised of the first d equations (for the largest d we can solve for) in the forgery modelisation.

$$
\begin{aligned}
\mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_1 \\
\mathbf{x}_v^\top \mathbf{T} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_2 \\
\ldots \\
\mathbf{x}_v^\top \mathbf{T}^{d-1} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_{d-1}.
\end{aligned}
$$

- We solve this system using FXL with an improved guessing strategy developed for these systems with a specific structure.

Towards a universal forgery attack

The trapdoor construction



Overall attack outline

For a chosen d

Overall attack outline

For a chosen d

→ Choose randomly salt r.

→ Compute $\mathbf{w} = H(\mathrm{m}||r)$.

Until $\mathbf{w}$ is d-periodic (includes all $d'|d$).

Overall attack outline

For a chosen d

→ Choose randomly salt r.

→ Compute $\mathbf{w} = H(\mathrm{m}||r)$.

Until $\mathbf{w}$ is d-periodic (includes all $d'|d$).

→ Solve the system of equations

$$\begin{aligned} \mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_1 \\ \mathbf{x}_v^\top \mathbf{T} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_2 \\ \ldots \\ \mathbf{x}_v^\top \mathbf{T}^{d-1} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_{d-1}. \end{aligned}$$

Overall attack outline

For a chosen d

→ Choose randomly salt r.

→ Compute $\mathbf{w} = H(\mathrm{m}||r)$.

Until $\mathbf{w}$ is d-periodic (includes all $d'|d$).

→ Solve the system of equations

$$\begin{aligned} \mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_1 \\ \mathbf{x}_v^\top \mathbf{T} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_2 \\ \cdots \\ \mathbf{x}_v^\top \mathbf{T}^{d-1} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_{d-1}. \end{aligned}$$

→ If no solution

repeat.

Overall attack outline

For a chosen d

→ Choose randomly salt r.

→ Compute $\mathbf{w} = H(\mathrm{m}\,||\,r)$.

Until $\mathbf{w}$ is d-periodic (includes all $d' \,|\, d$).

→ Solve the system of equations

$$\begin{aligned} \mathbf{x}_v^\top \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_1 \\ \mathbf{x}_v^\top \mathbf{T} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_2 \\ \cdots \\ \mathbf{x}_v^\top \mathbf{T}^{d-1} \mathbf{P}_1^{(1)} \mathbf{x}_v &= w_{d-1}. \end{aligned}$$

→ If no solution

repeat.

Else: ✓ Trimoska

Complexity estimates

$$\min_{d|v, d<m} p_{d,q}^{-1}(\mathrm{C}_{S(d,q)} + q^{m-d}\,\mathrm{C}_H)$$

Complexity estimates

$$\min_{d|v, d<m} p_{d,q}^{-1}(C_{S(d,q)} + q^{m-d}\, C_H)$$

Complexity of solving the system of equations with parameters d and q

Complexity estimates

$$\min_{d|v, d<m} p_{d,q}^{-1}(C_{S(d,q)} + q^{m-d} C_H)$$

Complexity of solving the system of equations with parameters d and q

Complexity of computing one hash

Complexity estimates

$$\min_{d|v, d<m} p_{d,q}^{-1}\left(C_{S(d,q)} + q^{m-d}\, C_H\right)$$

Probability that the resulting system has a solution

Complexity of solving the system of equations with parameters d and q

Complexity of computing one hash

Complexity estimates

Level	q	v	m	$\log_2$ cost
I	256	72	46	108
III	256	112	72	172
V	256	148	96	216

Complexity estimates

Level	q	v	m	$\log_2$ cost
I	256	72	46	108
III	256	112	72	172
V	256	148	96	216

! We compute the complexity $C_{S(d,q)}$ under the assumption that the system is semi-regular, while the system clearly has a specific structure.

Complexity estimates

Level	q	v	m	$\log_2$ cost
I	256	72	46	108
III	256	112	72	172
V	256	148	96	216

! We compute the complexity $C_{S(d,q)}$ under the assumption that the system is semi-regular, while the system clearly has a specific structure.

→ Not precise enough for choosing parameters, for instance.

Countermeasures

→ Increasing parameter sizes.

Countermeasures

→ Increasing parameter sizes. ✗

Countermeasures

→ Increasing parameter sizes. ✗

→ Choosing parameters such that v (the number of vinegar variables and hence the length of the vector in our attack) is prime.

Countermeasures

→ Increasing parameter sizes. ✘

→ Choosing parameters such that v (the number of vinegar variables and hence the length of the vector in our attack) is prime. ✓ ?

Countermeasures

→ Increasing parameter sizes. ✗

→ Choosing parameters such that v (the number of vinegar variables and hence the length of the vector in our attack) is prime. ✓ ?

→ Including linear and constant factors in the central map.

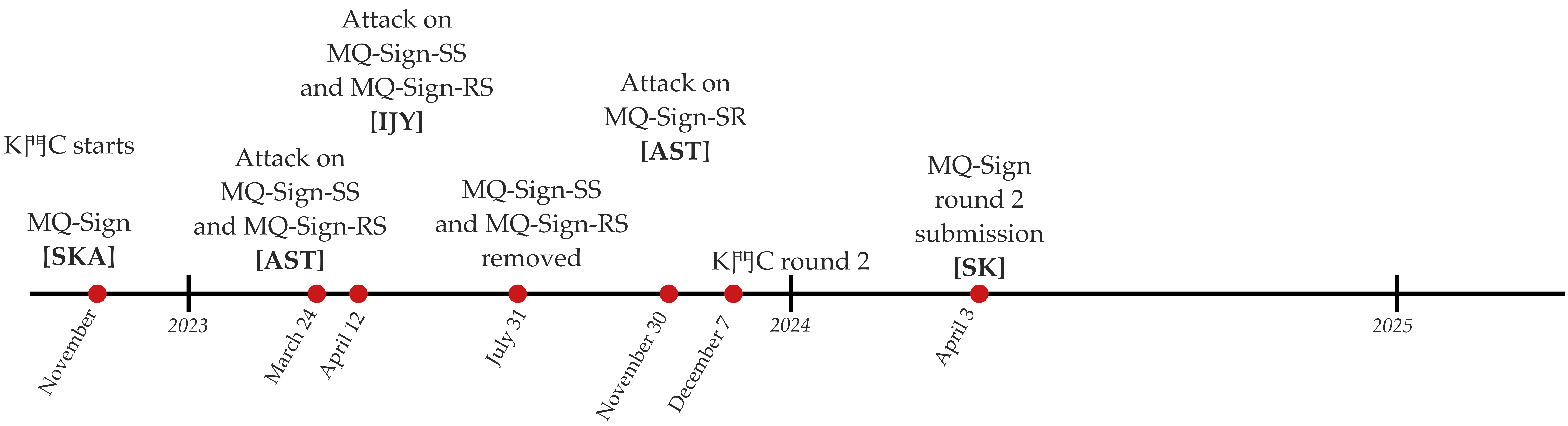
Countermeasures

→ Increasing parameter sizes. ✗

→ Choosing parameters such that v (the number of vinegar variables and hence the length of the vector in our attack) is prime. ✓ ?

→ Including linear and constant factors in the central map. ?

MQ-Sign timeline



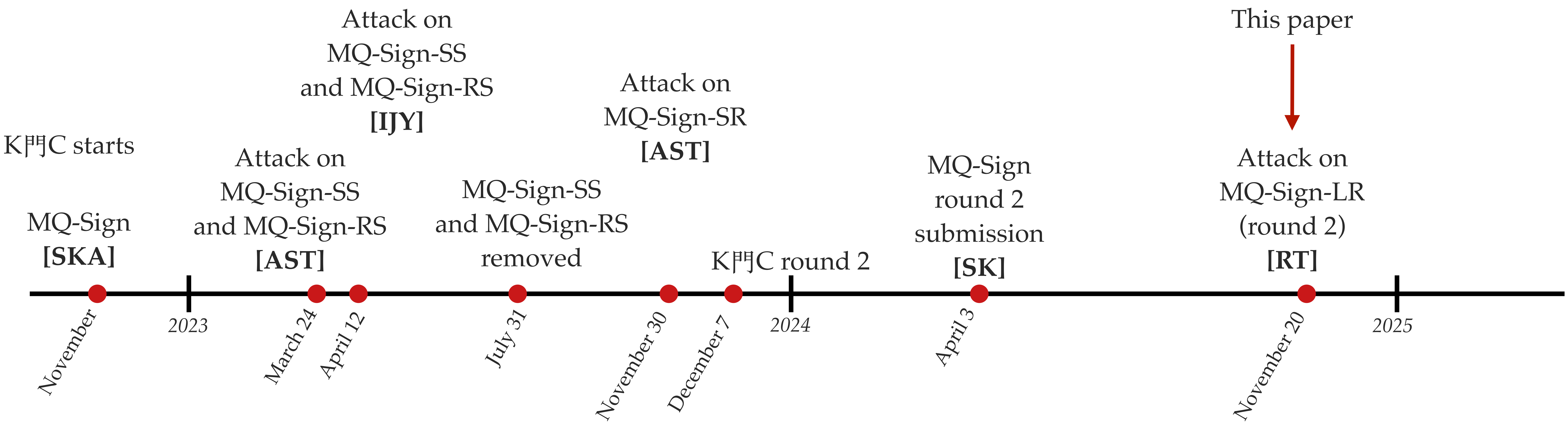
[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

[SK] Shim, Kwon. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2024)

MQ-Sign timeline



[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

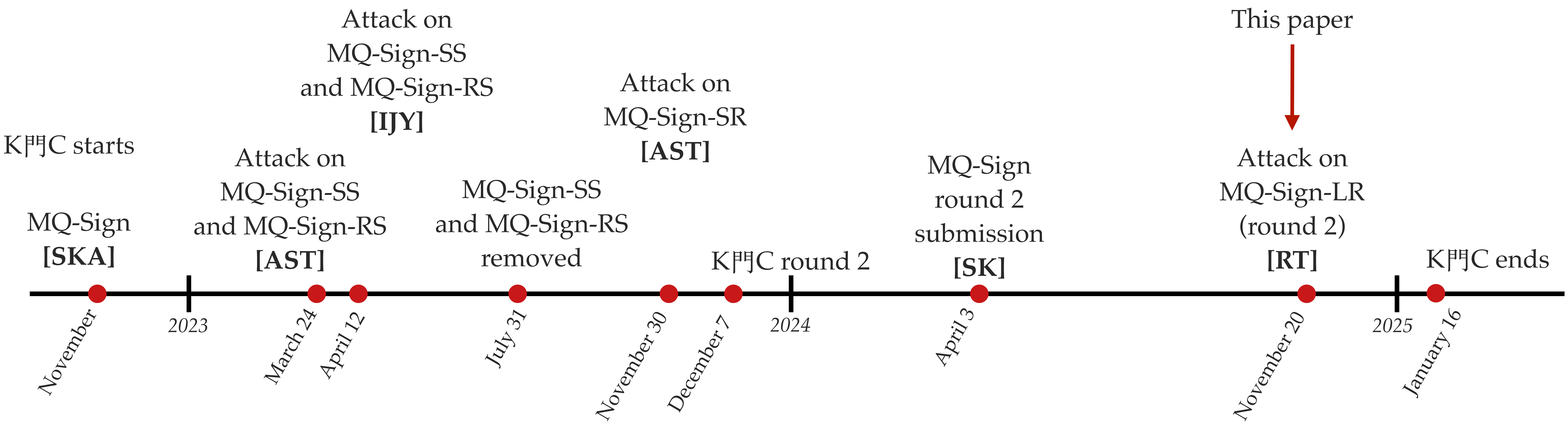
[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

[SK] Shim, Kwon. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2024)

[RT] Ran, Trimoska. Shifting our knowledge of MQ-Sign security. (2024)

MQ-Sign timeline



[SKA] Shim, Kim, An. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

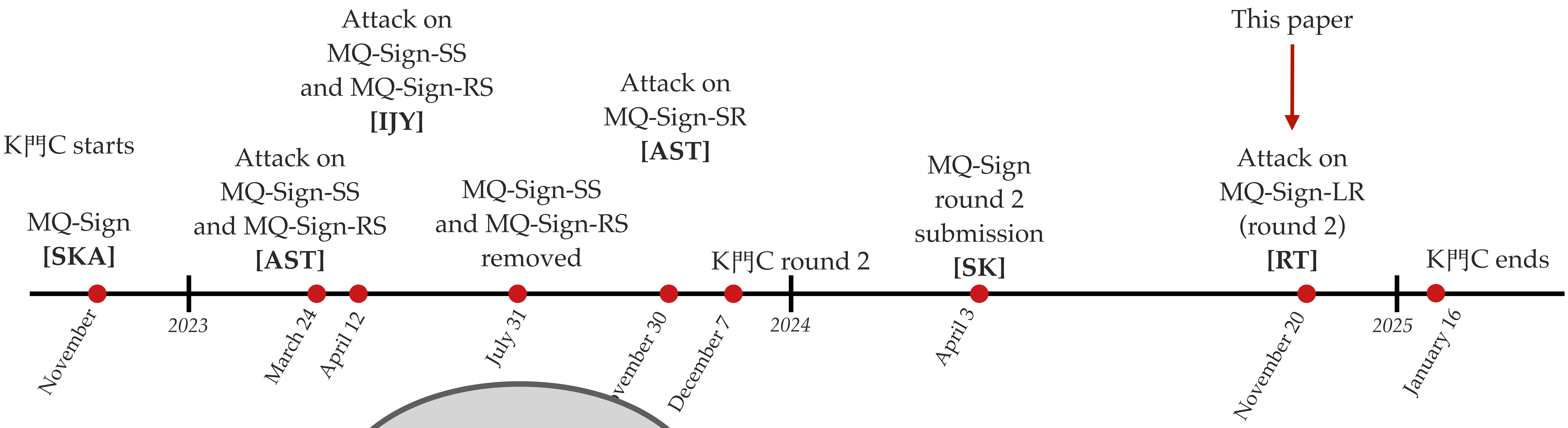
[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

[SK] Shim, Kwon. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2024)

[RT] Ran, Trimoska. Shifting our knowledge of MQ-Sign security. (2024)

MQ-Sign timeline



Thank you !

[SKA] Shim, Kim, An. MQ-Sign. A N… Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2022)

[AST] Aulbach, Samardjiska, Trimoska. Practical key-recovery attack on MQ-Sign and more. (2023)

[IJY] Ikematsu, Jo, Yasuda. A security analysis on MQ-Sign. (2023)

[SK] Shim, Kwon. MQ-Sign. A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. (2024)

[RT] Ran, Trimoska. Shifting our knowledge of MQ-Sign security. (2024)