Matrix Multiplication

2024.04.17

Index

1. ## Matrix Multiplication
   - Visual Understanding

2. ## Preliminary
   - Diagonal Vector
   - $\sigma(sigma), \tau(tau), \phi(phi), \psi(psi)$
   - Element-wise op. in HE

3. ## Algorithm
   - Linear Transformation
   - Homomorphic MM
   - Improvements

4. ## Advanced Options
   - Matrix Transposition
   - Rectangular MM
   - Parallel Matrix Computation

5. ## Implementation

Matrix Multiplication

Visual Understanding

A

1	2	3
4	5	6
7	8	9

3×3 행렬

×

B

1	2	3
4	5	6
7	8	9

3×3 행렬

Matrix Multiplication

Visual Understanding

$$\underset{A\,[0]\,[\;]}{\overset{A}{\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{bmatrix}}} \times \underset{B\,[\;]\,[0]}{\overset{B}{\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{bmatrix}}} = \underset{C\,[0]\,[0]}{\overset{(1 \times 1) + (2 \times 4) + (3 \times 7)}{\begin{bmatrix}30 & & \\ & & \\ & & \end{bmatrix}}}$$

Matrix Multiplication

Visual Understanding

$$\underset{A[0]\,[\,]}{\overset{A}{\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}}} \times \underset{B[\,]\,[1]}{\overset{B}{\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}}} = \underset{C[0]\,[1]}{\overset{(1 \times 2) + (2 \times 5) + (3 \times 8)}{\begin{bmatrix} 30 & 36 & \\ & & \\ & & \end{bmatrix}}}$$

Matrix Multiplication

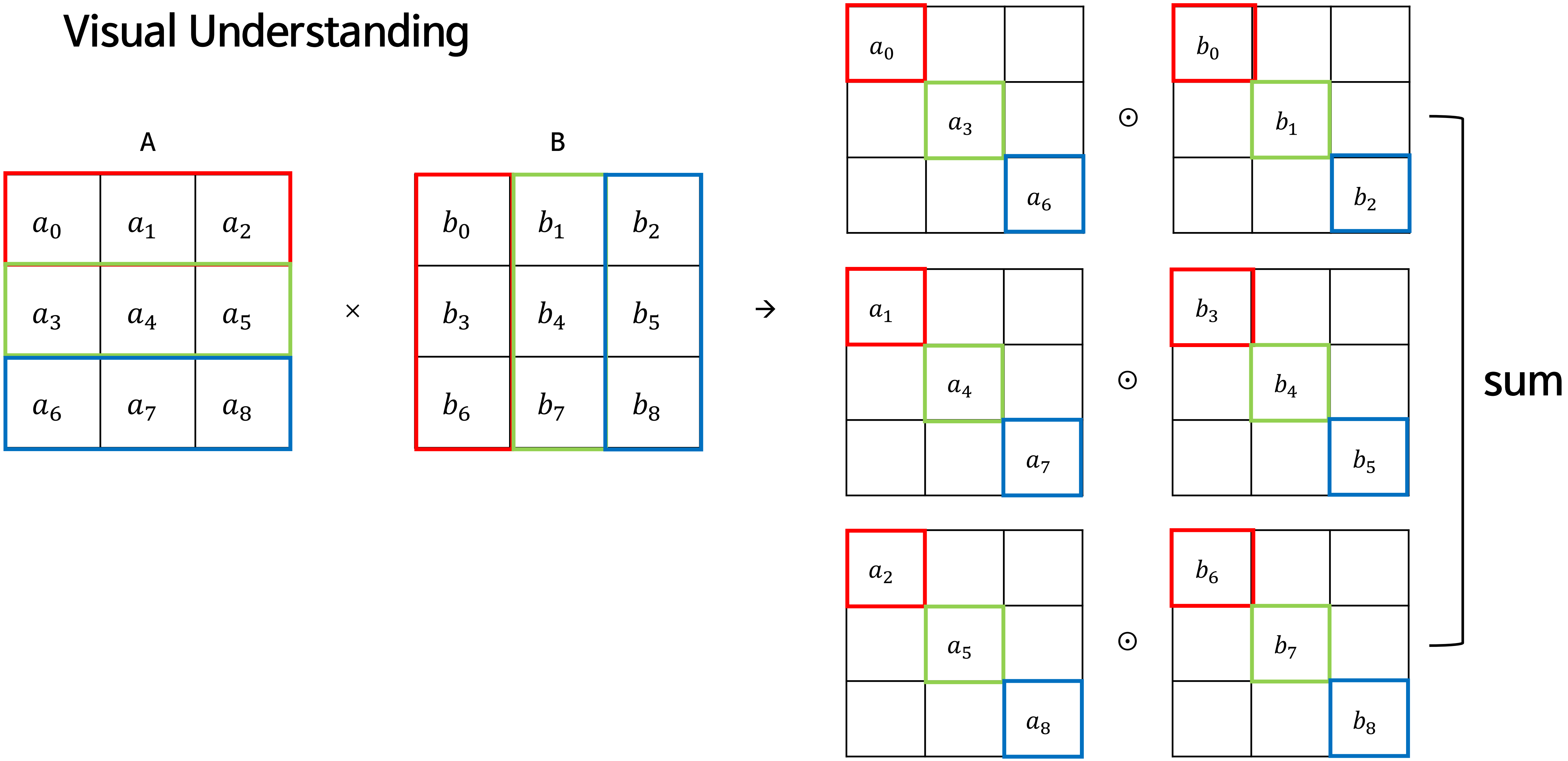
Visual Understanding

$$
\underset{A[2]\,[\,]}{\overset{A}{\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ \boxed{7} & \boxed{8} & \boxed{9} \end{bmatrix}}}
\times
\underset{B[\,]\,[2]}{\overset{B}{\begin{bmatrix} 1 & 2 & \boxed{3} \\ 4 & 5 & \boxed{6} \\ 7 & 8 & \boxed{9} \end{bmatrix}}}
=
\underset{C[2]\,[2]}{\begin{bmatrix} 30 & 36 & 42 \\ 66 & 81 & 96 \\ 102 & 126 & \boxed{150} \end{bmatrix}}
\quad (7 \times 3) + (8 \times 6) + (9 \times 9)
$$

→ Element wise representation?

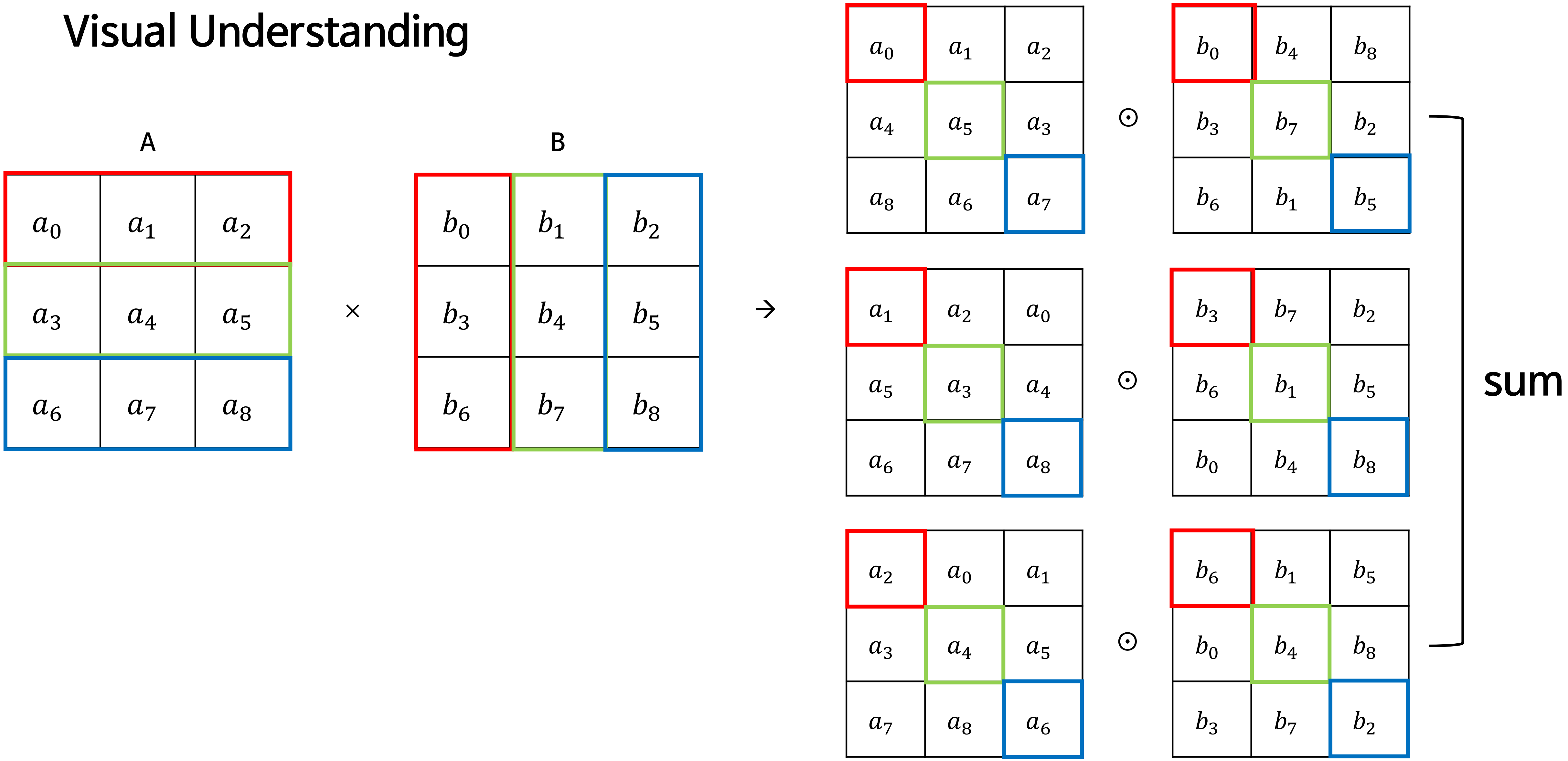
Matrix Multiplication

Visual Understanding

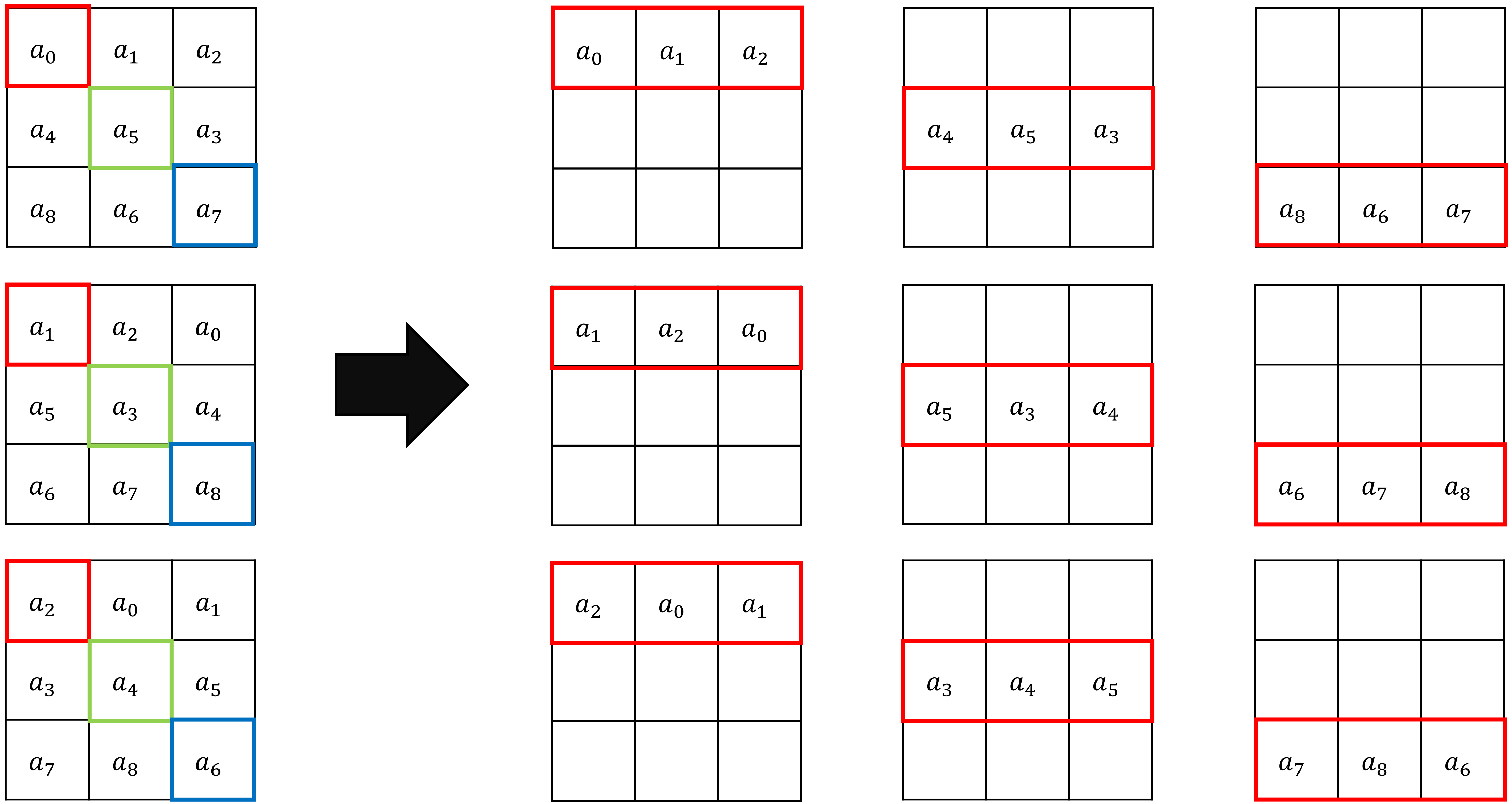


Matrix Multiplication

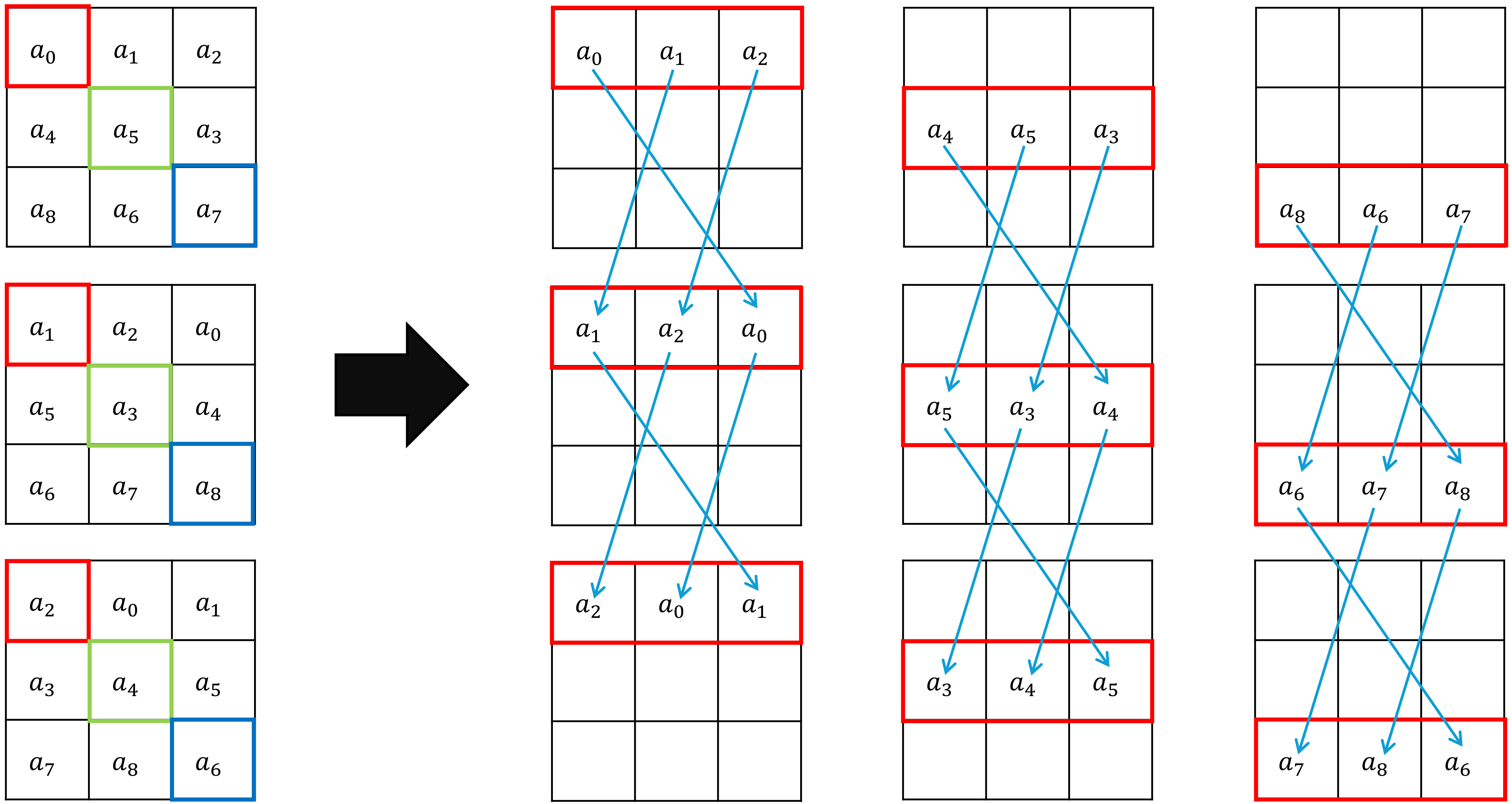
Visual Understanding



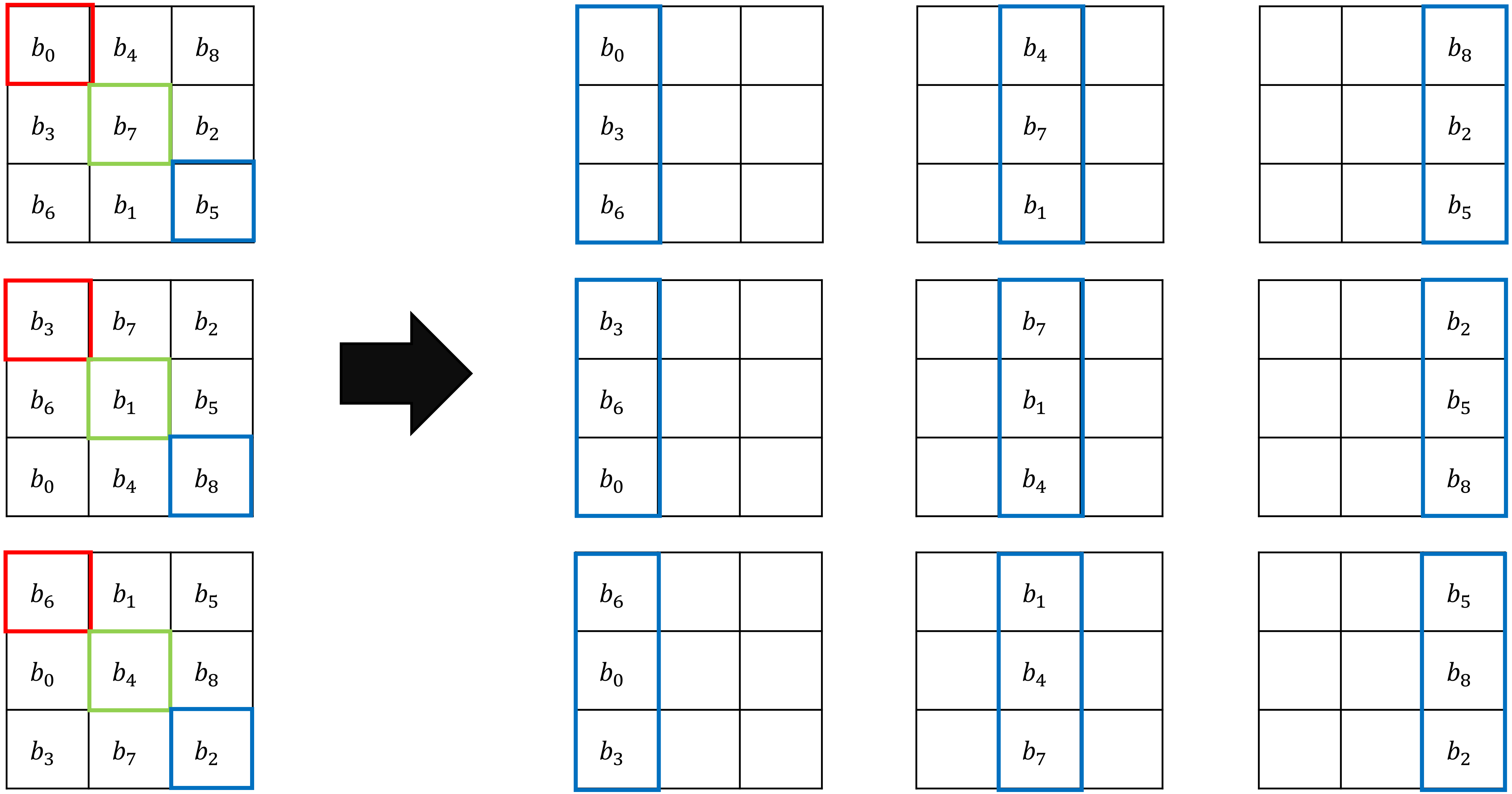
Matrix Multiplication



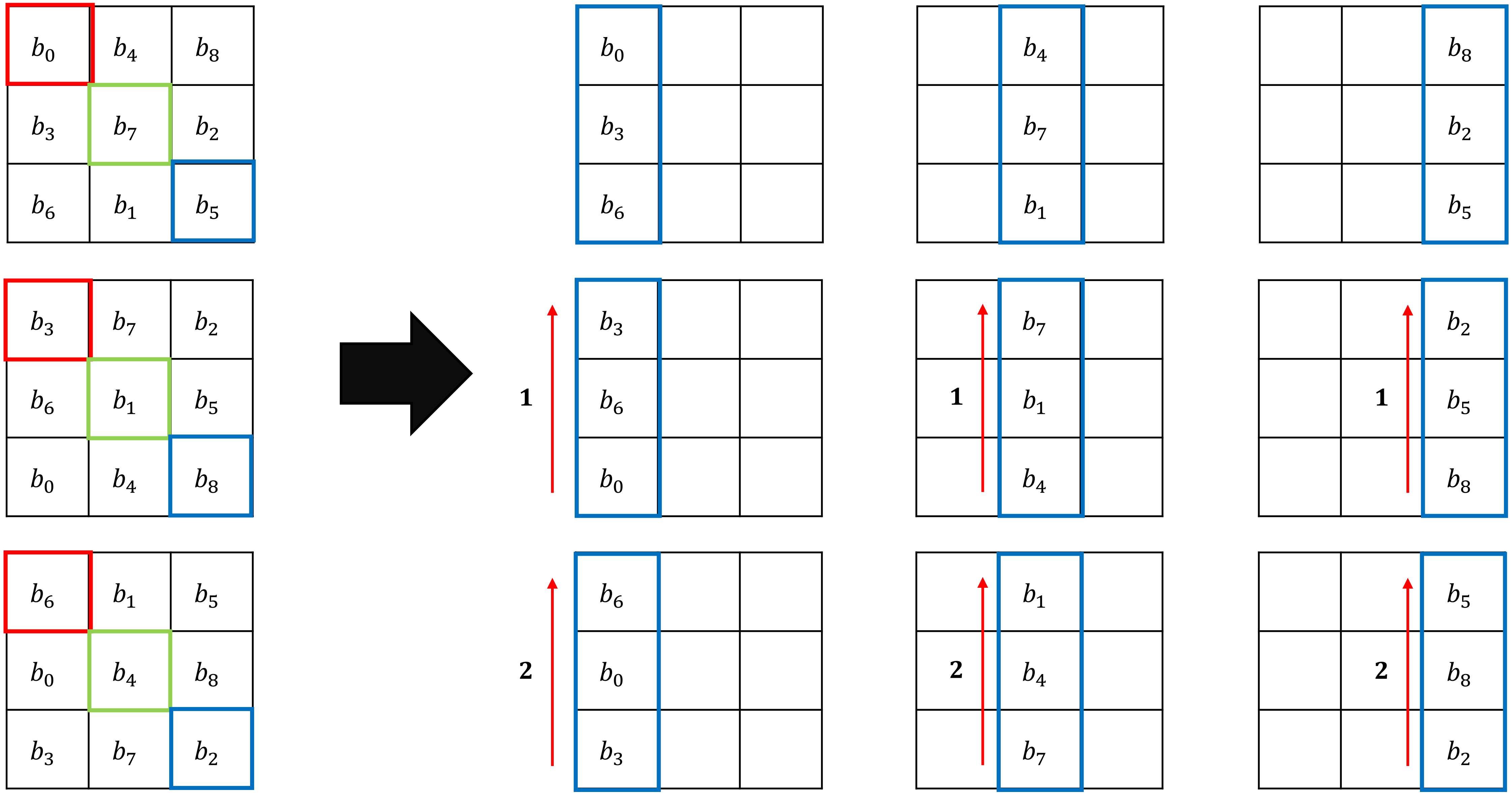
Matrix Multiplication



Matrix Multiplication



Matrix Multiplication



Matrix Multiplication

Visual Understanding

$$\overset{A}{\begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix}} \times \overset{B}{\begin{bmatrix} b_0 & b_1 & b_2 \\ b_3 & b_4 & b_5 \\ b_6 & b_7 & b_8 \end{bmatrix}}$$

Matrix Multiplication

Visual Understanding

$$
\overset{A}{\begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix}} \times \overset{B}{\begin{bmatrix} b_0 & b_1 & b_2 \\ b_3 & b_4 & b_5 \\ b_6 & b_7 & b_8 \end{bmatrix}}
\Rightarrow
$$

$$
\begin{bmatrix} a_0 & a_1 & a_2 \\ a_4 & a_5 & a_3 \\ a_8 & a_6 & a_7 \end{bmatrix} \odot \begin{bmatrix} b_0 & b_4 & b_8 \\ b_3 & b_7 & b_2 \\ b_6 & b_1 & b_5 \end{bmatrix}
$$

$$
\begin{bmatrix} a_1 & a_2 & a_0 \\ a_5 & a_3 & a_4 \\ a_6 & a_7 & a_8 \end{bmatrix} \odot \begin{bmatrix} b_3 & b_7 & b_2 \\ b_6 & b_1 & b_5 \\ b_0 & b_4 & b_8 \end{bmatrix}
$$

$$
\begin{bmatrix} a_2 & a_0 & a_1 \\ a_3 & a_4 & a_5 \\ a_7 & a_8 & a_6 \end{bmatrix} \odot \begin{bmatrix} b_6 & b_1 & b_5 \\ b_0 & b_4 & b_8 \\ b_3 & b_7 & b_2 \end{bmatrix}
$$

Matrix Multiplication

Visual Understanding

$$\begin{bmatrix} a_0 & a_1 & a_2 \\ a_4 & a_5 & a_3 \\ a_8 & a_6 & a_7 \end{bmatrix} \odot \begin{bmatrix} b_0 & b_4 & b_8 \\ b_3 & b_7 & b_2 \\ b_6 & b_1 & b_5 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & a_2 & a_0 \\ a_5 & a_3 & a_4 \\ a_6 & a_7 & a_8 \end{bmatrix} \odot \begin{bmatrix} b_3 & b_7 & b_2 \\ b_6 & b_1 & b_5 \\ b_0 & b_4 & b_8 \end{bmatrix}$$

$$\begin{bmatrix} a_2 & a_0 & a_1 \\ a_3 & a_4 & a_5 \\ a_7 & a_8 & a_6 \end{bmatrix} \odot \begin{bmatrix} b_6 & b_1 & b_5 \\ b_0 & b_4 & b_8 \\ b_3 & b_7 & b_2 \end{bmatrix}$$

$$\Rightarrow$$

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_4 & a_5 & a_3 & a_8 & a_6 & a_7 \end{bmatrix} \odot \begin{bmatrix} b_0 & b_4 & b_8 & b_3 & b_7 & b_2 & b_6 & b_1 & b_5 \end{bmatrix}$$

$$+$$

$$\begin{bmatrix} a_1 & a_2 & a_0 & a_5 & a_3 & a_4 & a_6 & a_7 & a_8 \end{bmatrix} \odot \begin{bmatrix} b_3 & b_7 & b_2 & b_6 & b_1 & b_5 & b_0 & b_4 & b_8 \end{bmatrix}$$

$$+$$

$$\begin{bmatrix} a_2 & a_0 & a_1 & a_3 & a_4 & a_5 & a_7 & a_8 & a_6 \end{bmatrix} \odot \begin{bmatrix} b_6 & b_1 & b_5 & b_0 & b_4 & b_8 & b_3 & b_7 & b_2 \end{bmatrix}$$

Preliminary

Diagonal Vector

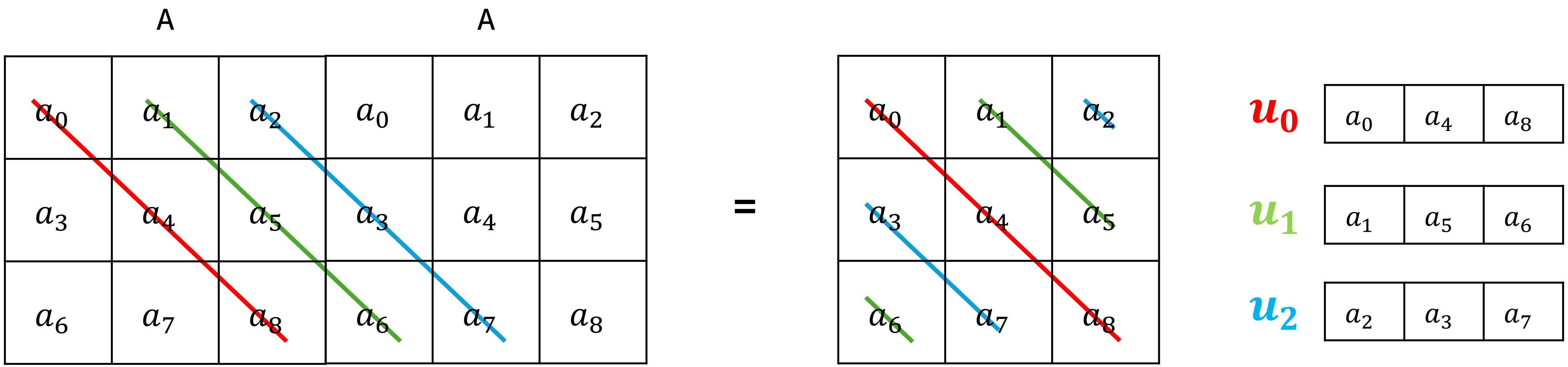
A

a_0	a_1	a_2
a_3	a_4	a_5
a_6	a_7	a_8

$\boldsymbol{u_0}$	a_0	a_4	a_8
$\boldsymbol{u_1}$	a_1	a_5	a_6
$\boldsymbol{u_2}$	a_2	a_3	a_7

Preliminary

Diagonal Vector



Preliminary

Permutations – σ(sigma)

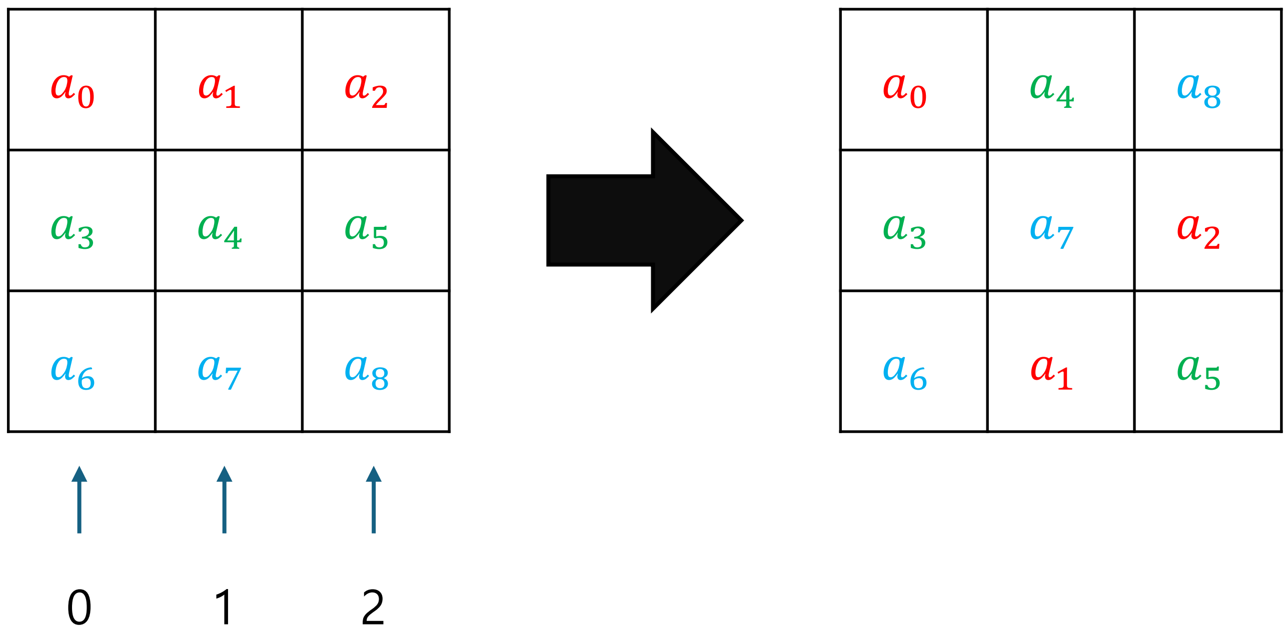
$$\boldsymbol{\sigma(A)_{i,j} = A_{i,i+j}}$$

$$\begin{array}{c} 0 \leftarrow \\ 1 \leftarrow \\ 2 \leftarrow \end{array} \begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix} \Rightarrow \begin{bmatrix} a_0 & a_1 & a_2 \\ a_4 & a_5 & a_3 \\ a_8 & a_6 & a_7 \end{bmatrix}$$

Preliminary

Permutations − τ (tau)

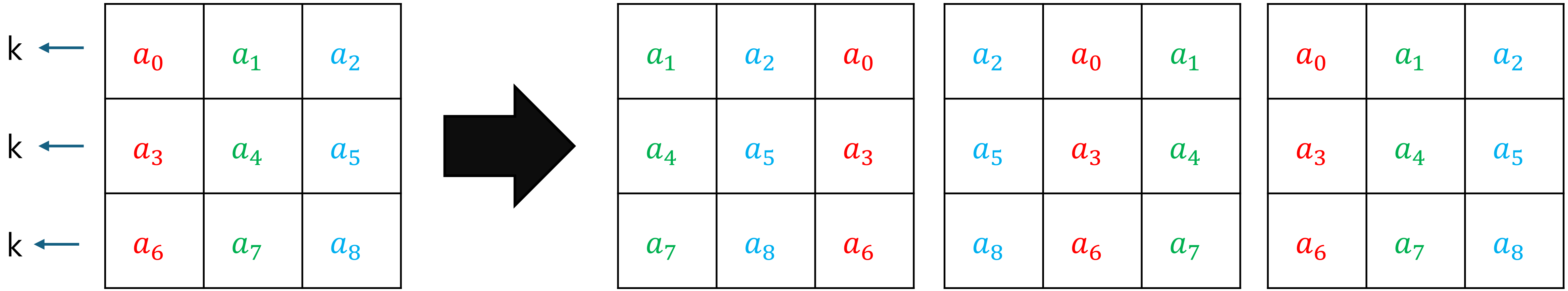
$$\boldsymbol{\tau(A)_{i,j} = A_{i+j,i}}$$



Preliminary

Permutations − ϕ (phi)

$$\boldsymbol{\phi(A)^{k}}_{\boldsymbol{i,j}} = \boldsymbol{A_{i,j+k}}$$

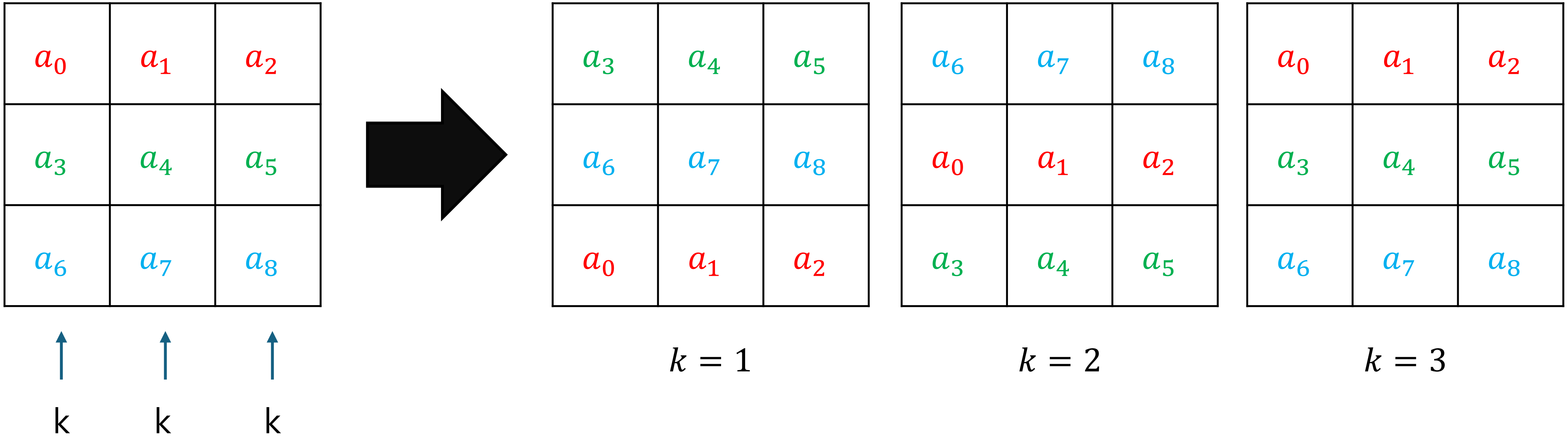


$k = 1$ $\quad$ $k = 2$ $\quad$ $k = 3$

Preliminary

Permutations $-\psi$ (psi)

$$\psi(A)^{k}{}_{i,j} = A_{i+k,j}$$



Preliminary

Permutations

$$\sigma(A)_{i,j} = A_{i,i+j} \qquad \tau(A)_{i,j} = A_{i+j,i}$$

$$\begin{array}{cc} 0 \leftarrow & \\ 1 \leftarrow & \\ 2 \leftarrow & \end{array}\begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix} \qquad \begin{array}{ccc} & \begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix} & \\ & \begin{array}{ccc} \uparrow & \uparrow & \uparrow \\ 0 & 1 & 2 \end{array} & \end{array}$$

$$\phi(A)^{k}{}_{i,j} = A_{i,j+k} \qquad \psi(A)^{k}{}_{i,j} = A_{i+k,j}$$

$$\begin{array}{cc} k \leftarrow & \\ k \leftarrow & \\ k \leftarrow & \end{array}\begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix} \qquad \begin{array}{c} \begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix} \\ \begin{array}{ccc} \uparrow & \uparrow & \uparrow \\ k & k & k \end{array} \end{array}$$

Preliminary

Element-wise op. in HE

Addition$(+)$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$+$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8

$=$

a_0+b_0	a_1+b_1	a_2+b_2	a_3+b_3	a_4+b_4	a_5+b_5	a_6+b_6	a_7+b_7	a_8+b_8

Multiplication$(\odot)$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$\times$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8

$=$

$a_0\times b_0$	$a_1\times b_1$	$a_2\times b_2$	$a_3\times b_3$	$a_4\times b_4$	$a_5\times b_5$	$a_6\times b_6$	$a_7\times b_7$	$a_8\times b_8$

Rotation$(\rho(\boldsymbol{a};l))$

a_0	a_1	a_2	…	a_4	a_5	a_6	a_7	…

$\Rightarrow$

a_l	a_{l+1}	a_{l+2}	…	a_0	a_1	a_2	a_3	…

Algorithm

Linear Transformation (Algorithm 1)

목표: 벡터 내 원소의 순서를 변경

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1

9×9 행렬 U

a_0
a_1
a_2
a_3
a_4
a_5
a_6
a_7
a_8

9×1 벡터 $\boldsymbol{m}$

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$$\boldsymbol{u}_k = (\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1})$$

$$\begin{aligned} &\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; {\color{red}0}) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \\ &= (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \end{aligned}$$

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	1	1	1	1	1	1	1	1
1	a_1	1	1	1	1	1	1	1
1	1	a_2	1	1	1	1	1	1
1	1	1	a_3	1	1	1	1	1
1	1	1	1	a_4	1	1	1	1
1	1	1	1	1	a_5	1	1	1
1	1	1	1	1	1	a_6	1	1
1	1	1	1	1	1	1	a_7	1
1	1	1	1	1	1	1	1	a_8

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$$\boldsymbol{u}_k = (\boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1})$$

$$\begin{aligned} &\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; 0) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \\ &= (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \end{aligned}$$

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	1	1	1	1	1	1	1	1
1	a_1	1	1	1	1	1	1	1
1	1	a_2	1	1	1	1	1	1
1	1	1	a_3	1	1	1	1	1
1	1	1	1	a_4	1	1	1	1
1	1	1	1	1	a_5	1	1	1
1	1	1	1	1	1	a_6	1	1
1	1	1	1	1	1	1	a_7	1
1	1	1	1	1	1	1	1	a_8

$$\boldsymbol{u_k} = (\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1})$$

$$\begin{aligned} &\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; {\color{red}0}) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \\ &= (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \end{aligned}$$

$$\begin{aligned} &\boldsymbol{u}_1 \odot \rho(\boldsymbol{m}; {\color{red}1}) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, {\color{red}a_0}) \\ &= (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, {\color{red}a_0}) \end{aligned}$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	a_1	1	1	1	1	1	1	1
a_0	a_1	a_2	1	1	1	1	1	1
1	1	a_2	a_3	1	1	1	1	1
1	1	1	a_3	a_4	1	1	1	1
1	1	1	1	a_4	a_5	1	1	1
1	1	1	1	1	a_5	a_6	1	1
1	1	1	1	1	1	a_6	a_7	1
1	1	1	1	1	1	1	a_7	a_8
1	1	1	1	1	1	1	1	a_8

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$$\boldsymbol{u}_k = (\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1})$$

$$\begin{aligned} &\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; 0) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \\ &= (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \end{aligned}$$

$$\begin{aligned} &\boldsymbol{u}_1 \odot \rho(\boldsymbol{m}; 1) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0) \\ &= (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0) \end{aligned}$$

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$\boldsymbol{u_k} = (\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1})$

$$\begin{aligned} &\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; 0) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \\ &= (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) \end{aligned}$$

$$\begin{aligned} &\boldsymbol{u}_1 \odot \rho(\boldsymbol{m}; 1) \\ &= (1,1,1,1,1,1,1,1,1) \odot (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0) \\ &= (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0) \end{aligned}$$

…

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; 0) = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$$
$$+$$
$$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m}; 1) = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0)$$
$$+$$
$$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m}; 2) = (a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0, a_1)$$
$$+$$
$$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m}; 3) = (a_3, a_4, a_5, a_6, a_7, a_8, a_0, a_1, a_2)$$
$$+$$
$$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m}; 4) = (a_4, a_5, a_6, a_7, a_8, a_0, a_1, a_2, a_3)$$
$$+$$
$$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m}; 5) = (a_5, a_6, a_7, a_8, a_0, a_1, a_2, a_3, a_4)$$
$$+$$
$$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m}; 6) = (a_6, a_7, a_8, a_0, a_1, a_2, a_3, a_4, a_5)$$
$$+$$
$$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m}; 7) = (a_7, a_8, a_0, a_1, a_2, a_3, a_4, a_5, a_6)$$
$$+$$
$$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m}; 8) = (a_8, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$$

Algorithm

Linear Transformation (Algorithm 1)

$$\boxed{U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)}$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; 0) = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$$
$$+$$
$$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m}; 1) = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0)$$
$$+$$
$$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m}; 2) = (a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0, a_1)$$
$$+$$
$$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m}; 3) = (a_3, a_4, a_5, a_6, a_7, a_8, a_0, a_1, a_2)$$
$$+$$
$$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m}; 4) = (a_4, a_5, a_6, a_7, a_8, a_0, a_1, a_2, a_3)$$
$$+$$
$$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m}; 5) = (a_5, a_6, a_7, a_8, a_0, a_1, a_2, a_3, a_4)$$
$$+$$
$$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m}; 6) = (a_6, a_7, a_8, a_0, a_1, a_2, a_3, a_4, a_5)$$
$$+$$
$$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m}; 7) = (a_7, a_8, a_0, a_1, a_2, a_3, a_4, a_5, a_6)$$
$$+$$
$$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m}; 8) = (a_8, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$$

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

$$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m}; 0) = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$$
$$+$$
$$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m}; 1) = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0)$$
$$+$$
$$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m}; 2) = (a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_0, a_1)$$
$$+$$
$$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m}; 3) = (a_3, a_4, a_5, a_6, a_7, a_8, a_0, a_1, a_2)$$
$$+$$
$$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m}; 4) = (a_4, a_5, a_6, a_7, a_8, a_0, a_1, a_2, a_3)$$
$$+$$
$$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m}; 5) = (a_5, a_6, a_7, a_8, a_0, a_1, a_2, a_3, a_4)$$
$$+$$
$$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m}; 6) = (a_6, a_7, a_8, a_0, a_1, a_2, a_3, a_4, a_5)$$
$$+$$
$$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m}; 7) = (a_7, a_8, a_0, a_1, a_2, a_3, a_4, a_5, a_6)$$
$$+$$
$$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m}; 8) = (a_8, a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$$

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0

sigma matrix

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

a_0
a_1
a_2
a_4
a_5
a_3
a_8
a_6
a_7

$U^\sigma \cdot \boldsymbol{m}$

=

a_0	a_1	a_2
a_4	a_5	a_3
a_8	a_6	a_7

Algorithm

Linear Transformation (Algorithm 1)

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0

sigma matrix
$LinTrans(ct.A; U^{\sigma})$

1	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0	1
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	1	0
0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0
0	0	1	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0

tau matrix
$LinTrans(ct.B; U^{\tau})$

0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0	0

phi matrix
$LinTrans(ct.A0; V^{1})$

0	0	0	1	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0

psi matrix
$LinTrans(ct.B0; W^{1})$

Algorithm

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

Linear Transformation (Algorithm 1)

1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0

sigma matrix
$LinTrans(ct.A; U^{\sigma})$

1	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0	1
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	1	0
0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0
0	1	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0

tau matrix
$LinTrans(ct.B; U^{\tau})$

Algorithm

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

Linear Transformation (Algorithm 1)

0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0	0

phi matrix

$LinTrans(ct.A0; V^1)$

0	0	0	1	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0

psi matrix

$LinTrans(ct.B0; W^1)$

Algorithm

Homomorphic Matrix Multiplication(Algorithm 2)

목표

$$\begin{array}{|c|c|c|c|c|c|c|c|c|}\hline a_0 & a_1 & a_2 & a_4 & a_5 & a_3 & a_8 & a_6 & a_7 \\ \hline \end{array} \odot \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline b_0 & b_4 & b_8 & b_3 & b_7 & b_2 & b_6 & b_1 & b_5 \\ \hline \end{array}$$

$$\begin{array}{|c|c|c|c|c|c|c|c|c|}\hline a_1 & a_2 & a_0 & a_5 & a_3 & a_4 & a_6 & a_7 & a_8 \\ \hline \end{array} \odot \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline b_3 & b_7 & b_2 & b_6 & b_1 & b_5 & b_0 & b_4 & b_8 \\ \hline \end{array}$$

$$\begin{array}{|c|c|c|c|c|c|c|c|c|}\hline a_2 & a_0 & a_1 & a_3 & a_4 & a_5 & a_7 & a_8 & a_6 \\ \hline \end{array} \odot \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline b_6 & b_1 & b_5 & b_0 & b_4 & b_8 & b_3 & b_7 & b_2 \\ \hline \end{array}$$

Algorithm

Homomorphic Matrix Multiplication (Algorithm 2)

목표

$$\begin{array}{|c|c|c|c|c|c|c|c|c|}\hline a_0 & a_1 & a_2 & a_4 & a_5 & a_3 & a_8 & a_6 & a_7 \\ \hline \end{array} \odot \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline b_0 & b_4 & b_8 & b_3 & b_7 & b_2 & b_6 & b_1 & b_5 \\ \hline \end{array}$$

$ct.A0 = LinTrans(ct.A; U^{\sigma})$ $ct.B0 = LinTrans(ct.B; U^{\tau})$

$$\begin{array}{|c|c|c|c|c|c|c|c|c|}\hline a_1 & a_2 & a_0 & a_5 & a_3 & a_4 & a_6 & a_7 & a_8 \\ \hline \end{array} \odot \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline b_3 & b_7 & b_2 & b_6 & b_1 & b_5 & b_0 & b_4 & b_8 \\ \hline \end{array}$$

$$\begin{array}{|c|c|c|c|c|c|c|c|c|}\hline a_2 & a_0 & a_1 & a_3 & a_4 & a_5 & a_7 & a_8 & a_6 \\ \hline \end{array} \odot \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline b_6 & b_1 & b_5 & b_0 & b_4 & b_8 & b_3 & b_7 & b_2 \\ \hline \end{array}$$

Algorithm

Homomorphic Matrix Multiplication (Algorithm 2)

목표

a_0	a_1	a_2	a_4	a_5	a_3	a_8	a_6	a_7

$\odot$

b_0	b_4	b_8	b_3	b_7	b_2	b_6	b_1	b_5

$ct.A0 = LinTrans(ct.A; U^{\sigma})$

$ct.B0 = LinTrans(ct.B; U^{\tau})$

a_1	a_2	a_0	a_5	a_3	a_4	a_6	a_7	a_8

$\odot$

b_3	b_7	b_2	b_6	b_1	b_5	b_0	b_4	b_8

$LinTrans(ct.A0; V^1)$

$LinTrans(ct.B0; W^1)$

a_2	a_0	a_1	a_3	a_4	a_5	a_7	a_8	a_6

$\odot$

b_6	b_1	b_5	b_0	b_4	b_8	b_3	b_7	b_2

Algorithm

Homomorphic Matrix Multiplication (Algorithm 2)

목표

a_0	a_1	a_2	a_4	a_5	a_3	a_8	a_6	a_7	$\odot$	b_0	b_4	b_8	b_3	b_7	b_2	b_6	b_1	b_5

$ct.A0 = LinTrans(ct.A; U^{\sigma})$ $ct.B0 = LinTrans(ct.B; U^{\tau})$

a_1	a_2	a_0	a_5	a_3	a_4	a_6	a_7	a_8	$\odot$	b_3	b_7	b_2	b_6	b_1	b_5	b_0	b_4	b_8

$LinTrans(ct.A0; V^1)$ $LinTrans(ct.B0; W^1)$

a_2	a_0	a_1	a_3	a_4	a_5	a_7	a_8	a_6	$\odot$	b_6	b_1	b_5	b_0	b_4	b_8	b_3	b_7	b_2

$LinTrans(ct.A0; V^2)$ $LinTrans(ct.B0; W^2)$

Algorithm

Homomorphic Matrix Multiplication (Algorithm 2)

Step 1

$$ct.A0 = LinTrans(ct.A; U^{\sigma})$$
$$ct.B0 = LinTrans(ct.B; U^{\tau})$$

Step 2

$$ct.Ak = LinTrans(ct.A0; V^{k})$$
$$ct.Bk = LinTrans(ct.B0; W^{k})$$

Step 3

$$ct.AB = \sum_{k=0}^{d-1} ct.Ak \odot ct.Bk$$

Algorithm

Further Improvements (BSGS)

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\leftarrow 6$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\leftarrow 0$

a_6	a_7	a_8	a_0	a_1	a_2	a_3	a_4	a_5

$$\odot$$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8

$$\downarrow$$

a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	a_3b_6	a_4b_7	a_5b_8

Algorithm

Further Improvements (BSGS)

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\longleftarrow$ 6

$\odot$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\longleftarrow$ 0

a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	a_3b_6	a_4b_7	a_5b_8

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\longleftarrow$ 3

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\longleftarrow$ -3

a_3	a_4	a_5	a_6	a_7	a_8	a_0	a_1	a_2

$\odot$

b_6	b_7	b_8	b_0	b_1	b_2	b_3	b_4	b_5

$\downarrow$

3 $\longleftarrow$	a_3b_6	a_4b_7	a_5b_8	a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5

Algorithm

Further Improvements (BSGS)

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\longleftarrow$ 6

$$\odot$$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\longleftarrow$ 0

$$\boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\longleftarrow$ 3

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\longleftarrow$ -3

a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	a_3b_6	a_4b_7	a_5b_8

a_3b_6	a_4b_7	a_5b_8	a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	$\longleftarrow$ 3

Algorithm

Further Improvements (BSGS)

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\leftarrow$ 6

$\odot$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\leftarrow$ 0

$$\boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\leftarrow$ 3

$\odot$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\leftarrow$ -3

a_3b_6	a_4b_7	a_5b_8	a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	$\leftarrow$ 3

$\downarrow$

a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	a_3b_6	a_4b_7	a_5b_8

$$\rho(\boldsymbol{m}; j)$$

$$\odot$$

$$\rho\left(\boldsymbol{u}_{i+j}^{\sigma}; -i\right)$$

Algorithm

Further Improvements (BSGS)

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\leftarrow$ 6

$$\odot$$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\leftarrow$ 0

$$\boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	$\leftarrow$ 3

$$\odot$$

b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	$\leftarrow$ -3

a_3b_6	a_4b_7	a_5b_8	a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	$\leftarrow$ 3

$$\downarrow$$

a_6b_0	a_7b_1	a_8b_2	a_0b_3	a_1b_4	a_2b_5	a_3b_6	a_4b_7	a_5b_8

$$\left.\begin{array}{c}\rho(\boldsymbol{m}; j)\\ \odot \\ \rho(\boldsymbol{u}^{\sigma}_{i+j}; -i)\end{array}\right) \boldsymbol{m}_{i,j}$$

$$\rho(\boldsymbol{m}_{i,j};\ i)$$

Algorithm

Further Improvements (BSGS)

$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) = (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$

$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) = (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)$

$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) = (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)$

$\Rightarrow$

$\rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0)$

$\rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1)$

$\rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)$

$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) = (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)$

$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) = (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)$

$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) = (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)$

$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) = (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)$

$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) = (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)$

$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) = (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)$

Algorithm

Further Improvements (BSGS)

$$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) = (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$$
$$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) = (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)$$
$$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) = (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)$$

$$\Rightarrow \quad \rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0), \quad \rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1), \quad \rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)$$

$$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) = (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)$$
$$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) = (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)$$
$$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) = (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)$$

$$\Rightarrow \quad \rho(\boldsymbol{u}_3;-3) \odot \rho(\boldsymbol{m};0), \quad \rho(\boldsymbol{u}_4;-3) \odot \rho(\boldsymbol{m};1), \quad \rho(\boldsymbol{u}_5;-3) \odot \rho(\boldsymbol{m};2)$$

$$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) = (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)$$
$$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) = (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)$$
$$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) = (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)$$

Algorithm

Further Improvements (BSGS)

$$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) = (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$$
$$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) = (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)$$
$$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) = (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)$$

$$\Rightarrow \quad \rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0), \quad \rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1), \quad \rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)$$

$$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) = (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)$$
$$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) = (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)$$
$$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) = (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)$$

$$\Rightarrow \quad \rho(\boldsymbol{u}_3;-3) \odot \rho(\boldsymbol{m};0), \quad \rho(\boldsymbol{u}_4;-3) \odot \rho(\boldsymbol{m};1), \quad \rho(\boldsymbol{u}_5;-3) \odot \rho(\boldsymbol{m};2)$$

$$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) = (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)$$
$$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) = (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)$$
$$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) = (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)$$

$$\Rightarrow \quad \rho(\boldsymbol{u}_6;-6) \odot \rho(\boldsymbol{m};0), \quad \rho(\boldsymbol{u}_7;-6) \odot \rho(\boldsymbol{m};1), \quad \rho(\boldsymbol{u}_8;-6) \odot \rho(\boldsymbol{m};2)$$

Algorithm

Further Improvements (BSGS)

$$
\left.\begin{aligned}
\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) &= (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)\\
\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) &= (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)\\
\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) &= (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)
\end{aligned}\right] \Rightarrow \left.\begin{aligned}
&\rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0)\\
&\rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1)\\
&\rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)
\end{aligned}\right] \Rightarrow \rho(\boldsymbol{u}_{0-2};0)
$$

$$
\left.\begin{aligned}
\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) &= (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)\\
\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) &= (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)\\
\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) &= (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)
\end{aligned}\right] \Rightarrow \begin{aligned}
&\rho(\boldsymbol{u}_3;-3) \odot \rho(\boldsymbol{m};0)\\
&\rho(\boldsymbol{u}_4;-3) \odot \rho(\boldsymbol{m};1)\\
&\rho(\boldsymbol{u}_5;-3) \odot \rho(\boldsymbol{m};2)
\end{aligned}
$$

$$
\left.\begin{aligned}
\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) &= (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)\\
\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) &= (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)\\
\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) &= (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)
\end{aligned}\right] \Rightarrow \begin{aligned}
&\rho(\boldsymbol{u}_6;-6) \odot \rho(\boldsymbol{m};0)\\
&\rho(\boldsymbol{u}_7;-6) \odot \rho(\boldsymbol{m};1)\\
&\rho(\boldsymbol{u}_8;-6) \odot \rho(\boldsymbol{m};2)
\end{aligned}
$$

Algorithm

Further Improvements(BSGS)

$$\left.\begin{aligned}
\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) &= (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)\\
\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) &= (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)\\
\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) &= (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)
\end{aligned}\right] \Rightarrow \left.\begin{aligned}
&\rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0)\\
&\rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1)\\
&\rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)
\end{aligned}\right] \Rightarrow \rho(\boldsymbol{u}_{0-2};0)$$

$$\left.\begin{aligned}
\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) &= (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)\\
\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) &= (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)\\
\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) &= (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)
\end{aligned}\right] \Rightarrow \left.\begin{aligned}
&\rho(\boldsymbol{u}_3;-3) \odot \rho(\boldsymbol{m};0)\\
&\rho(\boldsymbol{u}_4;-3) \odot \rho(\boldsymbol{m};1)\\
&\rho(\boldsymbol{u}_5;-3) \odot \rho(\boldsymbol{m};2)
\end{aligned}\right] \Rightarrow \rho(\boldsymbol{u}_{3-5};3)$$

$$\left.\begin{aligned}
\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) &= (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)\\
\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) &= (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)\\
\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) &= (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)
\end{aligned}\right] \Rightarrow \left.\begin{aligned}
&\rho(\boldsymbol{u}_6;-6) \odot \rho(\boldsymbol{m};0)\\
&\rho(\boldsymbol{u}_7;-6) \odot \rho(\boldsymbol{m};1)\\
&\rho(\boldsymbol{u}_8;-6) \odot \rho(\boldsymbol{m};2)
\end{aligned}\right] \Rightarrow \rho(\boldsymbol{u}_{6-8};6)$$

Algorithm

Further Improvements (BSGS)

$$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) = (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$$
$$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) = (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)$$
$$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) = (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)$$
$$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) = (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)$$
$$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) = (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)$$
$$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) = (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)$$
$$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) = (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)$$
$$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) = (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)$$
$$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) = (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)$$

$$\rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0)$$
$$\rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1)$$
$$\rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)$$
$$\rho(\boldsymbol{u}_3;-3) \odot \rho(\boldsymbol{m};0)$$
$$\rho(\boldsymbol{u}_4;-3) \odot \rho(\boldsymbol{m};1)$$
$$\rho(\boldsymbol{u}_5;-3) \odot \rho(\boldsymbol{m};2)$$
$$\rho(\boldsymbol{u}_6;-6) \odot \rho(\boldsymbol{m};0)$$
$$\rho(\boldsymbol{u}_7;-6) \odot \rho(\boldsymbol{m};1)$$
$$\rho(\boldsymbol{u}_8;-6) \odot \rho(\boldsymbol{m};2)$$

$$\rho(\boldsymbol{u}_{0-2};0)$$
$$\rho(\boldsymbol{u}_{3-5};3)$$
$$\rho(\boldsymbol{u}_{6-8};6)$$

$$\sum(\boldsymbol{u}_k \odot \rho(\boldsymbol{m};k))$$

Algorithm

Further Improvements(BSGS)

$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) = (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$

$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) = (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)$

$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) = (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)$

$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) = (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)$

$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) = (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)$

$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) = (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)$

$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) = (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)$

$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) = (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)$

$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) = (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)$

rot(8), mult(9), add(8)

$\Rightarrow$

$\rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0)$

$\rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1)$

$\rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)$

$\rho(\boldsymbol{u}_3;-3) \odot \rho(\boldsymbol{m};0)$

$\rho(\boldsymbol{u}_4;-3) \odot \rho(\boldsymbol{m};1)$

$\rho(\boldsymbol{u}_5;-3) \odot \rho(\boldsymbol{m};2)$

$\rho(\boldsymbol{u}_6;-6) \odot \rho(\boldsymbol{m};0)$

$\rho(\boldsymbol{u}_7;-6) \odot \rho(\boldsymbol{m};1)$

$\rho(\boldsymbol{u}_8;-6) \odot \rho(\boldsymbol{m};2)$

$\Rightarrow$

$\rho(\boldsymbol{u}_{0-2};0)$

$\rho(\boldsymbol{u}_{3-5};3)$

$\rho(\boldsymbol{u}_{6-8};6)$

$\Rightarrow \sum(\boldsymbol{u}_k \odot \rho(\boldsymbol{m};k))$

Algorithm

Further Improvements (BSGS)

$$u_0 \odot \rho(m;0) = (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$$
$$u_1 \odot \rho(m;1) = (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)$$
$$u_2 \odot \rho(m;2) = (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)$$
$$u_3 \odot \rho(m;3) = (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)$$
$$u_4 \odot \rho(m;4) = (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)$$
$$u_5 \odot \rho(m;5) = (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)$$
$$u_6 \odot \rho(m;6) = (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)$$
$$u_7 \odot \rho(m;7) = (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)$$
$$u_8 \odot \rho(m;8) = (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)$$

rot(8), mult(9), add(8)

Precompute

$$\rho(u_0;0) \odot \rho(m;0)$$
$$\rho(u_1;0) \odot \rho(m;1)$$
$$\rho(u_2;0) \odot \rho(m;2)$$
$$\Rightarrow \rho(u_{0-2};0)$$

$$\rho(u_3;-3) \odot \rho(m;0)$$
$$\rho(u_4;-3) \odot \rho(m;1)$$
$$\rho(u_5;-3) \odot \rho(m;2)$$
$$\Rightarrow \rho(u_{3-5};3)$$

$$\rho(u_6;-6) \odot \rho(m;0)$$
$$\rho(u_7;-6) \odot \rho(m;1)$$
$$\rho(u_8;-6) \odot \rho(m;2)$$
$$\Rightarrow \rho(u_{6-8};6)$$

$$\Rightarrow \sum(u_k \odot \rho(m;k))$$

rot(4), mult(9), add(8)

Algorithm

Further Improvements(BSGS)

$d = 9$
$k = \sqrt{d} \cdot i + j$

$$U \cdot \boldsymbol{m} = \sum_{0 \le l < n} \boldsymbol{u}_l \odot \rho(\boldsymbol{m}; l)$$

$$\rho(\boldsymbol{m}; j) \odot \rho\left(\boldsymbol{u}^{\sigma}_{\sqrt{d} \cdot i + j}; -\sqrt{d} \cdot i\right)$$

$$\sum_{\sqrt{-d} < i < \sqrt{d}} \rho\Big(\sum_{0 \le j < \sqrt{d}} \boldsymbol{m}_{i,j};\ \sqrt{d} \cdot i\Big)$$

Algorithm

1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0

sigma matrix

Further Improvements (BSGS)

$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0) = (a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$

$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1) = (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0)$

$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2) = (a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1)$

~~$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3) = (a_3,a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2)$~~

~~$\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4) = (a_4,a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3)$~~

~~$\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5) = (a_5,a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4)$~~

~~$\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6) = (a_6,a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5)$~~

$\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7) = (a_7,a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6)$

$\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8) = (a_8,a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7)$

rot(4), mult(5), add(4)

Precompute

$\rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0)$

$\rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1)$

$\rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)$

$\Rightarrow \rho(\boldsymbol{u}_{0-2};0)$

~~$\rho(\boldsymbol{u}_3;-3) \odot \rho(\boldsymbol{m};0)$~~

~~$\rho(\boldsymbol{u}_4;-3) \odot \rho(\boldsymbol{m};1)$~~

~~$\rho(\boldsymbol{u}_5;-3) \odot \rho(\boldsymbol{m};2)$~~

$\Rightarrow$ ~~$\rho(\boldsymbol{u}_{3-5};3)$~~

~~$\rho(\boldsymbol{u}_6;-6) \odot \rho(\boldsymbol{m};0)$~~

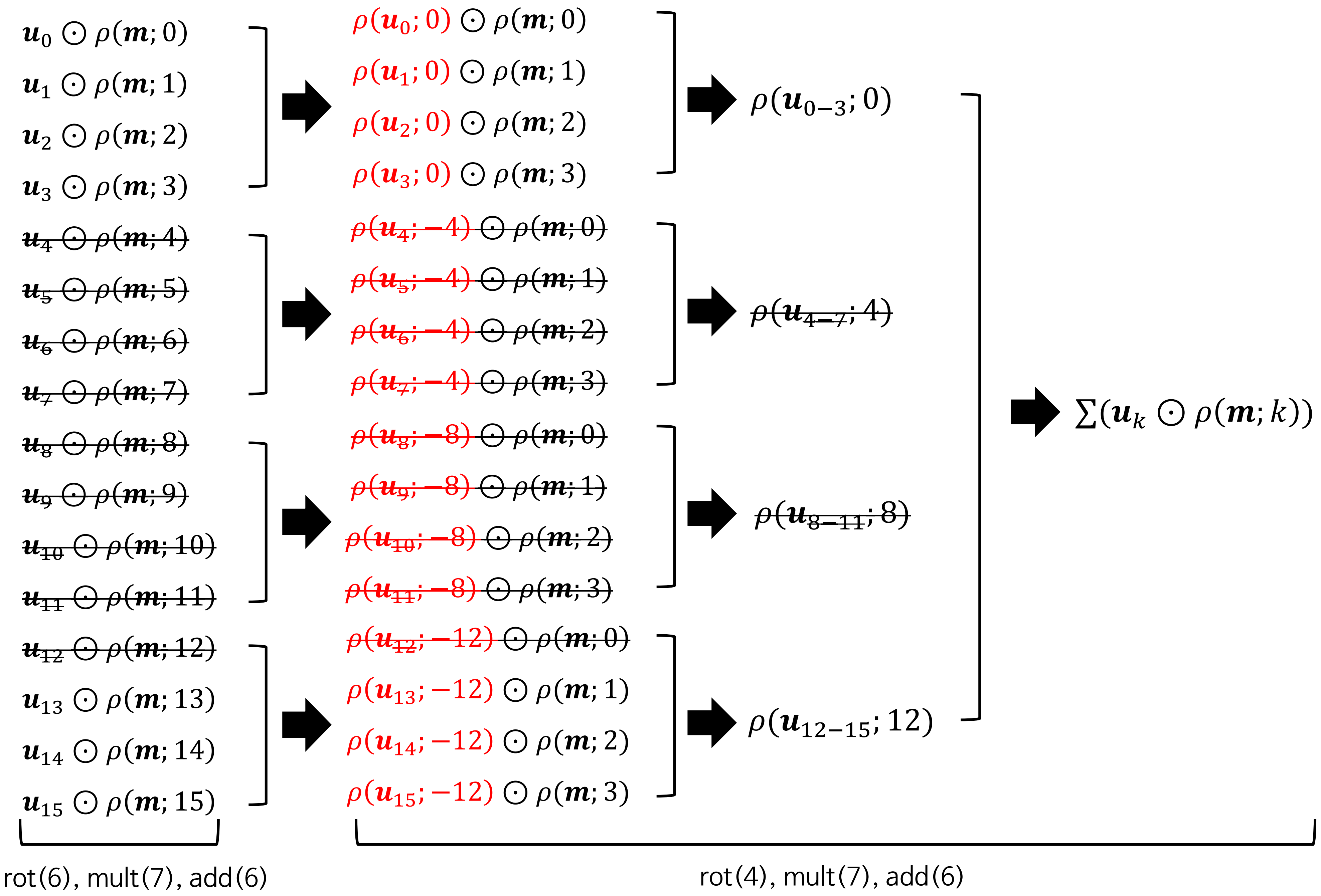
$\rho(\boldsymbol{u}_7;-6) \odot \rho(\boldsymbol{m};1)$

$\rho(\boldsymbol{u}_8;-6) \odot \rho(\boldsymbol{m};2)$

$\Rightarrow \rho(\boldsymbol{u}_{6-8};6)$

$\Rightarrow \sum(\boldsymbol{u}_k \odot \rho(\boldsymbol{m};k))$

rot(3), mult(5), add(4)



$\boldsymbol{u}_0 \odot \rho(\boldsymbol{m};0)$
$\boldsymbol{u}_1 \odot \rho(\boldsymbol{m};1)$
$\boldsymbol{u}_2 \odot \rho(\boldsymbol{m};2)$
$\boldsymbol{u}_3 \odot \rho(\boldsymbol{m};3)$
$\cancel{\boldsymbol{u}_4 \odot \rho(\boldsymbol{m};4)}$
$\cancel{\boldsymbol{u}_5 \odot \rho(\boldsymbol{m};5)}$
$\cancel{\boldsymbol{u}_6 \odot \rho(\boldsymbol{m};6)}$
$\cancel{\boldsymbol{u}_7 \odot \rho(\boldsymbol{m};7)}$
$\cancel{\boldsymbol{u}_8 \odot \rho(\boldsymbol{m};8)}$
$\cancel{\boldsymbol{u}_9 \odot \rho(\boldsymbol{m};9)}$
$\cancel{\boldsymbol{u}_{10} \odot \rho(\boldsymbol{m};10)}$
$\cancel{\boldsymbol{u}_{11} \odot \rho(\boldsymbol{m};11)}$
$\cancel{\boldsymbol{u}_{12} \odot \rho(\boldsymbol{m};12)}$
$\boldsymbol{u}_{13} \odot \rho(\boldsymbol{m};13)$
$\boldsymbol{u}_{14} \odot \rho(\boldsymbol{m};14)$
$\boldsymbol{u}_{15} \odot \rho(\boldsymbol{m};15)$
$\rho(\boldsymbol{u}_0;0) \odot \rho(\boldsymbol{m};0)$
$\rho(\boldsymbol{u}_1;0) \odot \rho(\boldsymbol{m};1)$
$\rho(\boldsymbol{u}_2;0) \odot \rho(\boldsymbol{m};2)$
$\rho(\boldsymbol{u}_3;0) \odot \rho(\boldsymbol{m};3)$
$\cancel{\rho(\boldsymbol{u}_4;-4) \odot \rho(\boldsymbol{m};0)}$
$\cancel{\rho(\boldsymbol{u}_5;-4) \odot \rho(\boldsymbol{m};1)}$
$\cancel{\rho(\boldsymbol{u}_6;-4) \odot \rho(\boldsymbol{m};2)}$
$\cancel{\rho(\boldsymbol{u}_7;-4) \odot \rho(\boldsymbol{m};3)}$
$\cancel{\rho(\boldsymbol{u}_8;-8) \odot \rho(\boldsymbol{m};0)}$
$\cancel{\rho(\boldsymbol{u}_9;-8) \odot \rho(\boldsymbol{m};1)}$
$\cancel{\rho(\boldsymbol{u}_{10};-8) \odot \rho(\boldsymbol{m};2)}$
$\cancel{\rho(\boldsymbol{u}_{11};-8) \odot \rho(\boldsymbol{m};3)}$
$\cancel{\rho(\boldsymbol{u}_{12};-12) \odot \rho(\boldsymbol{m};0)}$
$\rho(\boldsymbol{u}_{13};-12) \odot \rho(\boldsymbol{m};1)$
$\rho(\boldsymbol{u}_{14};-12) \odot \rho(\boldsymbol{m};2)$
$\rho(\boldsymbol{u}_{15};-12) \odot \rho(\boldsymbol{m};3)$
$\rho(\boldsymbol{u}_{0-3};0)$
$\cancel{\rho(\boldsymbol{u}_{4-7};4)}$
$\cancel{\rho(\boldsymbol{u}_{8-11};8)}$
$\rho(\boldsymbol{u}_{12-15};12)$
$\sum(\boldsymbol{u}_k \odot \rho(\boldsymbol{m};k))$
rot(6), mult(7), add(6)
rot(4), mult(7), add(6)

Advanced Options

Matrix Transposition

A

a_0	a_1	a_2
a_3	a_4	a_5
a_6	a_7	a_8

A

a_0	a_3	a_6
a_1	a_4	a_7
a_2	a_5	a_8

Advanced Options

Matrix Transposition

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \end{bmatrix}
\Rightarrow
\begin{bmatrix} a_0 \\ a_3 \\ a_6 \\ a_1 \\ a_4 \\ a_7 \\ a_2 \\ a_5 \\ a_8 \end{bmatrix}
$$

transpose matrix
$LinTrans(ct.A; U^T)$

Advanced Options

Rectangular MM

$$\underset{A}{\begin{array}{|c|c|c|c|}\hline a_0 & a_1 & a_2 & a_3 \\ \hline a_4 & a_5 & a_6 & a_7 \\ \hline a_8 & a_9 & a_{10} & a_{11} \\ \hline a_{12} & a_{13} & a_{14} & a_{15} \\ \hline \end{array}} \times \underset{B}{\begin{array}{|c|c|}\hline b_0 & b_1 \\ \hline b_2 & b_3 \\ \hline b_4 & b_5 \\ \hline b_6 & b_7 \\ \hline \end{array}} = \underset{AB}{\begin{array}{|c|c|}\hline c_0 & c_1 \\ \hline c_2 & c_3 \\ \hline c_4 & c_5 \\ \hline c_6 & c_7 \\ \hline \end{array}}$$

Advanced Options

Rectangular MM

$$
\overset{A}{\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{bmatrix}}
\times
\begin{array}{cc} \text{B} & \text{B} \\ \begin{bmatrix} b_0 & b_1 \\ b_2 & b_3 \\ b_4 & b_5 \\ b_6 & b_7 \end{bmatrix} & \begin{bmatrix} b_0 & b_1 \\ b_2 & b_3 \\ b_4 & b_5 \\ b_6 & b_7 \end{bmatrix} \end{array}
$$

Advanced Options

Parallel Computation

$d = 2$
$g = 4$

$$\overset{A}{\begin{bmatrix} a_0 & a_1 \\ a_2 & a_3 \end{bmatrix}} \times \overset{A}{\begin{bmatrix} a_0 & a_1 \\ a_2 & a_3 \end{bmatrix}} \qquad \overset{B}{\begin{bmatrix} b_0 & b_1 \\ b_2 & b_3 \end{bmatrix}} \times \overset{B}{\begin{bmatrix} b_0 & b_1 \\ b_2 & b_3 \end{bmatrix}}$$

$$\overset{C}{\begin{bmatrix} c_0 & c_1 \\ c_2 & c_3 \end{bmatrix}} \times \overset{C}{\begin{bmatrix} c_0 & c_1 \\ c_2 & c_3 \end{bmatrix}} \qquad \overset{D}{\begin{bmatrix} d_0 & d_1 \\ d_2 & d_3 \end{bmatrix}} \times \overset{D}{\begin{bmatrix} d_0 & d_1 \\ d_2 & d_3 \end{bmatrix}}$$

Advanced Options

Parallel Computation

g개의 $d \times d$ 행렬

$(g \bmod d^2 = 0)$을 가정

$$\iota_g : \boldsymbol{a} \mapsto \left(A_k = \left(a_{g\cdot(d\cdot i+j)+k}\right)\right)_{0\le k<g}$$

$$\rho(\boldsymbol{a}; l) \to \rho(\boldsymbol{a}; g \cdot l)$$

Advanced Options

Parallel Computation

A|B|C|D

a_0	b_0	c_0	d_0
a_1	b_1	c_1	d_1
a_2	b_2	c_2	d_2
a_3	b_3	c_3	d_3

$\times$

A|B|C|D

a_0	b_0	c_0	d_0
a_1	b_1	c_1	d_1
a_2	b_2	c_2	d_2
a_3	b_3	c_3	d_3

$$\iota_g : \boldsymbol{a} \mapsto \left(A_k = \left(a_{g\cdot(d\cdot i+j)+k}\right)\right)_{0\le k<g}$$

Advanced Options

Parallel Computation

1	0	0	0
0	1	0	0
0	0	0	1
0	0	1	0

sigma matrix of 2×2

$\boldsymbol{u}_0$	1	1	0	0
$\boldsymbol{u}_1$	0	0	1	0
$\boldsymbol{u}_3$	0	0	0	1

a_0	b_0	c_0	d_0
a_1	b_1	c_1	d_1
a_2	b_2	c_2	d_2
a_3	b_3	c_3	d_3

A|B|C|D

Advanced Options

Parallel Computation

1	0	0	0
0	1	0	0
0	0	0	1
0	0	1	0

sigma matrix of 2×2

$\boldsymbol{u}_0$	1	1	0	0
$\boldsymbol{u}_1$	0	0	1	0
$\boldsymbol{u}_3$	0	0	0	1

a_0	b_0	c_0	d_0
a_1	b_1	c_1	d_1
a_2	b_2	c_2	d_2
a_3	b_3	c_3	d_3

A|B|C|D

Advanced Options

Parallel Computation

1	1	0	0
1	1	0	0
1	1	0	0
1	1	0	0

$\boldsymbol{u}_0$

a_0	b_0	c_0	d_0
a_1	b_1	c_1	d_1
a_2	b_2	c_2	d_2
a_3	b_3	c_3	d_3

A|B|C|D

Advanced Options

Parallel Computation

$\cancel{u_0}$	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0

A|B|C|D	a_0	b_0	c_0	d_0	a_1	b_1	c_1	d_1	a_2	b_2	c_2	d_2	a_3	b_3	c_3	d_3

Advanced Options

Parallel Computation

$\boldsymbol{u}_0$	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
A|B|C|D	a_0	b_0	c_0	d_0	a_1	b_1	c_1	d_1	a_2	b_2	c_2	d_2	a_3	b_3	c_3	d_3

Advanced Options

Parallel Computation

$\boldsymbol{u}_0$	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
A|B|C|D	a_0	b_0	c_0	d_0	a_1	b_1	c_1	d_1	a_2	b_2	c_2	d_2	a_3	b_3	c_3	d_3

$\boldsymbol{u}_1$	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
$1 \leftarrow$ A|B|C|D	a_0	b_0	c_0	d_0	a_1	b_1	c_1	d_1	a_2	b_2	c_2	d_2	a_3	b_3	c_3	d_3

Advanced Options

Parallel Computation

$\boldsymbol{u}_0$	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
A|B|C|D	a_0	b_0	c_0	d_0	a_1	b_1	c_1	d_1	a_2	b_2	c_2	d_2	a_3	b_3	c_3	d_3

$\boldsymbol{u}_1$	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
$1 \leftarrow$ A|B|C|D	a_1	b_1	c_1	d_1	a_2	b_2	c_2	d_2	a_3	b_3	c_3	d_3	a_0	b_0	c_0	d_0

$$\rho(\boldsymbol{a}; l) \rightarrow \rho(\boldsymbol{a}; g \cdot l)$$

Implementation

[Matrix Multiplication - Colab]