

An Efficient Software Implementation of Fugue

Çağdaş Çalık

Institute of Applied Mathematics, Middle East Technical University, Ankara,
Turkey

Overview

- 1 Description of Fugue
- 2 SIMD Architecture
- 3 AES VPerm Implementation
- 4 Fugue SIMD Implementation
- 5 Benchmarks
- 6 Summary

Outline

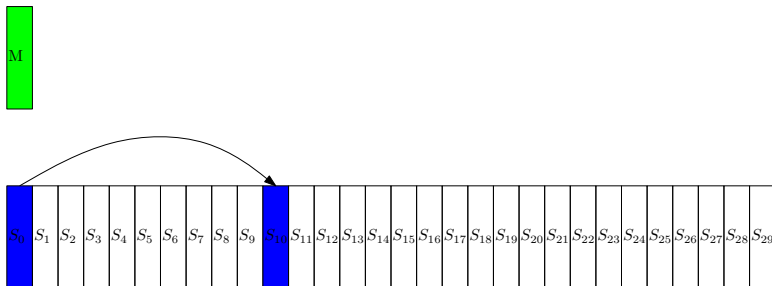
- 1 Description of Fugue
- 2 SIMD Architecture
- 3 AES VPerm Implementation
- 4 Fugue SIMD Implementation
- 5 Benchmarks
- 6 Summary

Fugue-256

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------

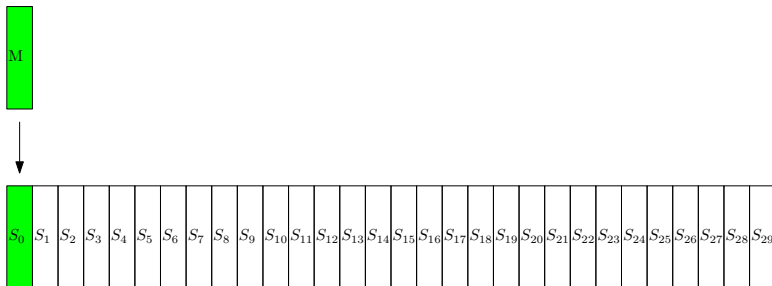
- $S_{10}+ = S_0$
- $S_0 = M$
- $S_8+ = S_0$
- $S_1+ = S_{24}$

TIX



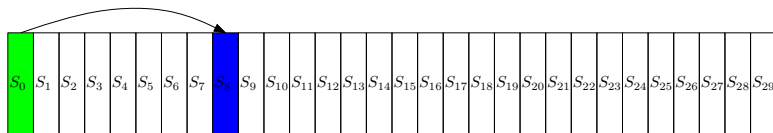
- $S_{10}+ = S_0$
- $S_0 = M$
- $S_8+ = S_0$
- $S_1+ = S_{24}$

TIX



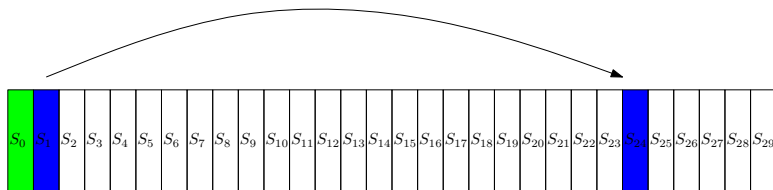
- $S_{10}+ = S_0$
- $S_0 = M$
- $S_8+ = S_0$
- $S_1+ = S_{24}$

TIX



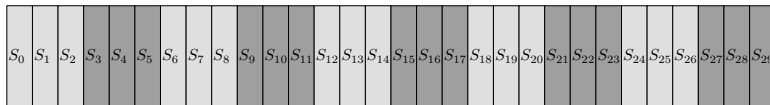
- $S_{10}+ = S_0$
- $S_0 = M$
- $S_8+ = S_0$
- $S_1+ = S_{24}$

TIX

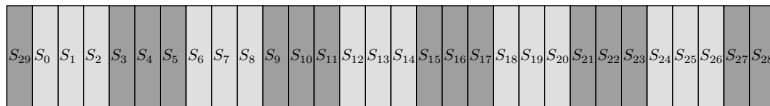


- $S_{10}+ = S_0$
- $S_0 = M$
- $S_{8}+ = S_0$
- $S_1+ = S_{24}$

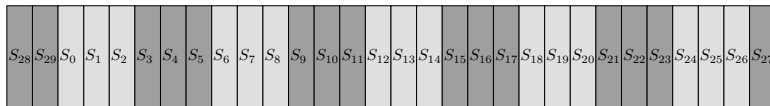
ROR3



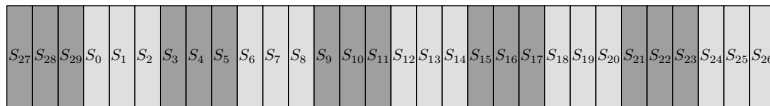
ROR3



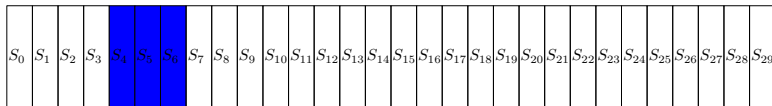
ROR3



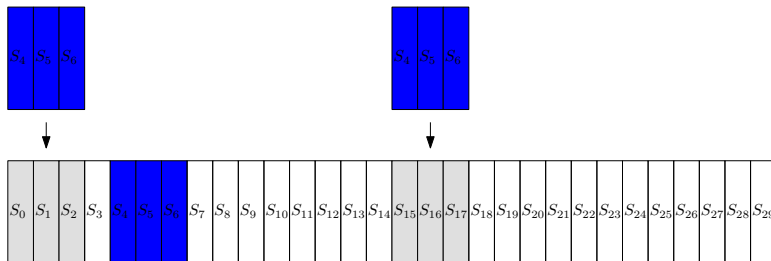
ROR3



CMIX



CMIX



Substitution

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

Substitution

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

- Each byte is replaced using AES s-box.

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	\times	x_0	$=$	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1		y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2		y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3		y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4		y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5		y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6		y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7		y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8		y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9		y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}		y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}		y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}		y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}		y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}		y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0		x_{15}		y_{15}

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 \\
 7 & 1 & 6 & 4 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5 & 4 & 7 & 1 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\
 x_1 \\
 x_2 \\
 x_3 \\
 x_4 \\
 x_5 \\
 x_6 \\
 x_7 \\
 x_8 \\
 x_9 \\
 x_{10} \\
 x_{11} \\
 x_{12} \\
 x_{13} \\
 x_{14} \\
 x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\
 y_1 \\
 y_2 \\
 y_3 \\
 y_4 \\
 y_5 \\
 y_6 \\
 y_7 \\
 y_8 \\
 y_9 \\
 y_{10} \\
 y_{11} \\
 y_{12} \\
 y_{13} \\
 y_{14} \\
 y_{15}
 \end{bmatrix}$$

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 \\
 7 & 1 & 6 & 4 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5 & 4 & 7 & 1 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15}
 \end{bmatrix}$$

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 & 0 & 0 & 0 & 4 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 & 0 & 0 & 0 & 7 \\
 7 & 1 & 6 & 4 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5 & 4 & 7 & 1 & 0 & 0 & 0 & 0 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\
 x_1 \\
 x_2 \\
 x_3 \\
 x_4 \\
 x_5 \\
 x_6 \\
 x_7 \\
 x_8 \\
 x_9 \\
 x_{10} \\
 x_{11} \\
 x_{12} \\
 x_{13} \\
 x_{14} \\
 x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\
 y_1 \\
 y_2 \\
 y_3 \\
 y_4 \\
 y_5 \\
 y_6 \\
 y_7 \\
 y_8 \\
 y_9 \\
 y_{10} \\
 y_{11} \\
 y_{12} \\
 y_{13} \\
 y_{14} \\
 y_{15}
 \end{bmatrix}$$

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	<div>×</div>	x_0	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1	y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2	y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3	y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4	y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5	y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6	y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7	y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8	y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9	y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}	y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}	y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}	y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}	y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}	y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0		x_{15}	y_{15}

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	\times	x_0	$=$	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1		y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2		y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3		y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4		y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5		y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6		y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7		y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8		y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9		y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}		y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}		y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}		y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}		y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}		y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0		x_{15}		y_{15}

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 & 0 & 0 & 0 & 0 & 0 \\
 7 & 1 & 6 & 4 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5 & 4 & 7 & 1 & 0 & 0 & 0 & 0 & 0 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\
 x_1 \\
 x_2 \\
 x_3 \\
 x_4 \\
 x_5 \\
 x_6 \\
 x_7 \\
 x_8 \\
 x_9 \\
 x_{10} \\
 x_{11} \\
 x_{12} \\
 x_{13} \\
 x_{14} \\
 x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\
 y_1 \\
 y_2 \\
 y_3 \\
 y_4 \\
 y_5 \\
 y_6 \\
 y_7 \\
 y_8 \\
 y_9 \\
 y_{10} \\
 y_{11} \\
 y_{12} \\
 y_{13} \\
 y_{14} \\
 y_{15}
 \end{bmatrix}$$

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	\times	x_0	$=$	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1		y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2		y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3		y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4		y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5		y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6		y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7		y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8		y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9		y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}		y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}		y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}		y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}		y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}		y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0		x_{15}		y_{15}

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	\times	x_0	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1	y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2	y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3	y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4	y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5	y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6	y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7	y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8	y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9	y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}	y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}	y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}	y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}	y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}	y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0		x_{15}	y_{15}

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	<div> <div>×</div> <div></div> <div>=</div> </div>	x_0	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1	y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2	y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3	y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4	y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5	y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6	y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7	y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8	y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9	y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}	y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}	y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}	y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}	y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}	y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0		x_{15}	y_{15}

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 & 4 & 7 & 1 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 & 7 & 1 & 0 & 4 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 & 0 & 0 & 0 & 0 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 & 1 & 6 & 4 & 7 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 & 0 & 0 & 7 & 0 \\
 \textbf{7} & \textbf{1} & \textbf{6} & \textbf{4} & \textbf{0} & \textbf{0} & \textbf{7} & \textbf{0} & \textbf{0} & \textbf{0} & \textbf{0} & \textbf{0} & \textbf{0} & \textbf{0} & \textbf{7} & \textbf{0} & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 5 & 4 & 7 & 1 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 4 & 0 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\
 x_1 \\
 x_2 \\
 x_3 \\
 x_4 \\
 x_5 \\
 x_6 \\
 x_7 \\
 x_8 \\
 x_9 \\
 x_{10} \\
 x_{11} \\
 x_{12} \\
 x_{13} \\
 x_{14} \\
 x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\
 y_1 \\
 y_2 \\
 y_3 \\
 y_4 \\
 y_5 \\
 y_6 \\
 y_7 \\
 y_8 \\
 y_9 \\
 \textbf{y_{10}} \\
 y_{11} \\
 y_{12} \\
 y_{13} \\
 y_{14} \\
 y_{15}
 \end{bmatrix}$$

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 \\
 7 & 1 & 6 & 4 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5 & 4 & 7 & 1 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\
 x_1 \\
 x_2 \\
 x_3 \\
 x_4 \\
 x_5 \\
 x_6 \\
 x_7 \\
 x_8 \\
 x_9 \\
 x_{10} \\
 x_{11} \\
 x_{12} \\
 x_{13} \\
 x_{14} \\
 x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\
 y_1 \\
 y_2 \\
 y_3 \\
 y_4 \\
 y_5 \\
 y_6 \\
 y_7 \\
 y_8 \\
 y_9 \\
 y_{10} \\
 y_{11} \\
 y_{12} \\
 y_{13} \\
 y_{14} \\
 y_{15}
 \end{bmatrix}$$

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}		S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_2	x_6	x_{10}	x_{14}		S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}	
x_3	x_7	x_{11}	x_{15}		S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}		

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	\times	x_0	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1	y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2	y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3	y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4	y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5	y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6	y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7	y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8	y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9	y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}	y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}	y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}	y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}	y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}	y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0	x_{15}	y_{15}	

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	\times	x_0	$=$	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1		y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2		y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3		y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4		y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5		y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6		y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7		y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8		y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9		y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}		y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}		y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}		y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}		y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}		y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0	x_{15}	y_{15}		

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 \\
 7 & 1 & 6 & 4 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5 & 4 & 7 & 1 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15}
 \end{bmatrix}$$

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

$$\begin{bmatrix}
 1 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 1 & 1 & 4 & 7 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 7 & 1 & 1 & 4 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 4 & 7 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 4 & 7 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 7 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 7 & 1 & 0 & 4 \\
 4 & 7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 6 & 4 & 7 & 1 & 7 & 0 & 0 & 0 \\
 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 1 & 6 & 4 & 7 \\
 7 & 1 & 6 & 4 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 \\
 0 & 0 & 0 & 7 & 4 & 7 & 1 & 6 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 5 & 4 & 7 & 1 \\
 1 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 \\
 0 & 0 & 4 & 0 & 7 & 1 & 5 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\
 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 4 & 7 & 1 & 5 & 0 & 0 & 0 & 0
 \end{bmatrix}
 \times
 \begin{bmatrix}
 x_0 \\
 x_1 \\
 x_2 \\
 x_3 \\
 x_4 \\
 x_5 \\
 x_6 \\
 x_7 \\
 x_8 \\
 x_9 \\
 x_{10} \\
 x_{11} \\
 x_{12} \\
 x_{13} \\
 x_{14} \\
 x_{15}
 \end{bmatrix}
 =
 \begin{bmatrix}
 y_0 \\
 y_1 \\
 y_2 \\
 y_3 \\
 y_4 \\
 y_5 \\
 y_6 \\
 y_7 \\
 y_8 \\
 y_9 \\
 y_{10} \\
 y_{11} \\
 y_{12} \\
 y_{13} \\
 y_{14} \\
 y_{15}
 \end{bmatrix}$$

Super-MIX

x_0	x_4	x_8	x_{12}	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}	S_{28}	S_{29}
x_1	x_5	x_9	x_{13}																										
x_2	x_6	x_{10}	x_{14}																										
x_3	x_7	x_{11}	x_{15}																										

1	4	7	1	1	0	0	0	1	0	0	0	1	0	0	0	\times	x_0	$=$	y_0
0	1	0	0	1	1	4	7	0	1	0	0	0	1	0	0		x_1		y_1
0	0	1	0	0	0	1	0	7	1	1	4	0	0	1	0		x_2		y_2
0	0	0	1	0	0	0	1	0	0	0	1	4	7	1	1		x_3		y_3
0	0	0	0	0	4	7	1	1	0	0	0	1	0	0	0		x_4		y_4
0	1	0	0	0	0	0	0	1	0	4	7	0	1	0	0		x_5		y_5
0	0	1	0	0	0	1	0	0	0	0	0	7	1	0	4		x_6		y_6
4	7	1	0	0	0	0	1	0	0	0	1	0	0	0	0		x_7		y_7
0	0	0	0	7	0	0	0	6	4	7	1	7	0	0	0		x_8		y_8
0	7	0	0	0	0	0	0	0	7	0	0	1	6	4	7		x_9		y_9
7	1	6	4	0	0	7	0	0	0	0	0	0	0	7	0		x_{10}		y_{10}
0	0	0	7	4	7	1	6	0	0	0	7	0	0	0	0		x_{11}		y_{11}
0	0	0	0	4	0	0	0	4	0	0	0	5	4	7	1		x_{12}		y_{12}
1	5	4	7	0	0	0	0	0	4	0	0	0	4	0	0		x_{13}		y_{13}
0	0	4	0	7	1	5	4	0	0	0	0	0	0	4	0		x_{14}		y_{14}
0	0	0	4	0	0	0	4	4	7	1	5	0	0	0	0		x_{15}		y_{15}

Outline

- 1 Description of Fugue
- 2 SIMD Architecture**
- 3 AES VPerm Implementation
- 4 Fugue SIMD Implementation
- 5 Benchmarks
- 6 Summary

- 16 xmm registers, each 128-bits wide. (16-bytes, 8-words, 4-dwords, 2-quadwords)
- Binary operations, integer arithmetic, shifts, shuffles, etc.
- A necessary instruction: **pshufb** can be used as a 4×8 s-box.

Outline

- 1 Description of Fugue
- 2 SIMD Architecture
- 3 AES VPerm Implementation**
- 4 Fugue SIMD Implementation
- 5 Benchmarks
- 6 Summary

SUBSTITUTE

```

movaps t1, xmmword ptr k_s0F      ; 1 : i
pandn t1, s0                       ; 1 = ijj4
psrld t1, 4                        ; 1 = i
pand s0, xmmword ptr k_s0F        ; 0 = k
movaps t2, xmmword ptr k_inv + 16 ; 2 : a/k
pshufb t2, s0                     ; 2 = a/k
pxor s0, t1                       ; 0 = j
movaps t3, xmmword ptr k_inv      ; 3 : 1/i
pshufb t3, t1                    ; 3 = 1/i
pxor t3, t2                       ; 3 = iak = 1/i + a/k
movaps t4, xmmword ptr k_inv      ; 4 : 1/j
pshufb t4, s0                    ; 4 = 1/j
pxor t4, t2                       ; 4 = jak = 1/j + a/k
movaps t2, xmmword ptr k_inv      ; 2 : 1/iak
pshufb t2, t3                    ; 2 = 1/iak
pxor t2, s0                       ; 2 = io
movaps t3, xmmword ptr k_inv      ; 3 : 1/jak
pshufb t3, t4                    ; 3 = 1/jak
xorps t3, t1                      ; 3 = jo

```

- Mike Hamburg,
*Accelerating AES with
Vector Permute
Instructions*, CHES 2009.

SUBSTITUTE

```

movaps t1, xmmword ptr k_s0F      ; 1 : i
pandn t1, s0                       ; 1 = ijj4
psrld t1, 4                        ; 1 = i
pand s0, xmmword ptr k_s0F        ; 0 = k
movaps t2, xmmword ptr k_inv + 16 ; 2 : a/k
pshufb t2, s0                     ; 2 = a/k
pxor s0, t1                       ; 0 = j
movaps t3, xmmword ptr k_inv      ; 3 : 1/i
pshufb t3, t1                     ; 3 = 1/i
pxor t3, t2                       ; 3 = iak = 1/i + a/k
movaps t4, xmmword ptr k_inv      ; 4 : 1/j
pshufb t4, s0                     ; 4 = 1/j
pxor t4, t2                       ; 4 = jak = 1/j + a/k
movaps t2, xmmword ptr k_inv      ; 2 : 1/iak
pshufb t2, t3                     ; 2 = 1/iak
pxor t2, s0                       ; 2 = io
movaps t3, xmmword ptr k_inv      ; 3 : 1/jak
pshufb t3, t4                     ; 3 = 1/jak
xorps t3, t1                      ; 3 = jo

```

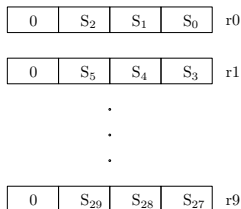
- Mike Hamburg, *Accelerating AES with Vector Permute Instructions*, CHES 2009.
- A fast and constant time implementation of AES with SIMD instructions.

Outline

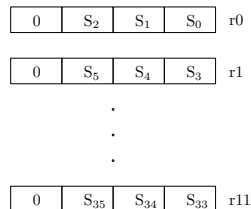
- 1 Description of Fugue
- 2 SIMD Architecture
- 3 AES VPerm Implementation
- 4 Fugue SIMD Implementation**
- 5 Benchmarks
- 6 Summary

Representation of the State

Fugue-256



Fugue-512



TIX & CMIX

TIX256

```

pshufd t1, r0, 0f3h      ; t1 = 0 0 S0 0
xorps r3, t1             ; S10 += S0
movss t1, dword ptr [msg] ; t1 = 0 0 0 I
TRANSFORM_INPUT t1, t2, t3
movss r0, t1             ; S0 = I
pslldq t1, 8             ; t1 = 0 S0 0 0
xorps r2, t1             ; S8 += S0
pshufd t1, r8, 0f3h      ; t1 = 0 0 S24 0
xorps r0, t1             ; S1 += S24

```

CMIX

```

movaps t, r1             ; t = 0 S5 S4 S3
shufps t, r2, 0c9h       ; t = 0 S6 S5 S4
xorps a, t               ; add to columns 0,1,2
xorps b, t               ; add to columns s/2, s/2+1, S/2+2

```

Super-MIX

Table: Super-Mix using 13 permutations

1x	0	1	2	3	7	1	2	2	11	12	1	6	15	0	5	10
	3	4	6	7	8	8	6	7	*	*	*	*	*	*	*	*
	4	5	9	11	12	13	13	11	*	*	*	*	*	*	*	*
	8	9	10	14	*	*	*	*	*	*	*	*	*	*	*	*
	12	13	14	15	*	*	*	*	*	*	*	*	*	*	*	*
4x	1	6	11	12	5	10	15	0	9	14	3	4	4	2	2	3
	*	*	*	*	*	*	*	*	*	*	*	*	8	9	7	7
	*	*	*	*	*	*	*	*	*	*	*	*	13	13	14	8
5x	*	*	*	*	*	*	*	*	*	*	*	*	12	1	6	11
6x	*	*	*	*	*	*	*	*	8	13	2	7	*	*	*	*
7x	2	7	8	13	6	11	12	1	4	1	0	3	14	3	4	9
	*	*	*	*	*	*	*	*	10	9	6	5	*	*	*	*
	*	*	*	*	*	*	*	*	12	15	14	11	*	*	*	*

Table: Super-Mix using 11 permutations

1x	0 3 4 8	1 4 5 9	2 6 9 10	3 7 11 14	7 8 12 *	1 8 13 *	2 6 13 *	2 7 11 *	11 * * *	12 * * *	1 * * *	6 * * *	15 * * *	0 * * *	5 * * *	10 * * *
2x	12	13	14	15	*	*	*	*	8	13	2	7	12	1	6	11
4x	1 12 *	6 13 *	11 14 *	12 15 *	5 * *	10 * *	15 * *	0 * *	9 8 *	14 13 *	3 2 *	4 7 *	4 8 13	2 9 13	2 7 14	3 7 8
7x	2 12 *	7 13 *	8 14 *	13 15 *	6 * *	11 * *	12 * *	1 * *	4 10 12	1 9 15	0 6 14	3 5 11	14 * *	3 1 *	4 6 *	9 11 *

Table: Super-Mix using 10 permutations

1x	0	1	2	7	8	1	2	2	11	12	1	6	15	0	5	10	+
	4	5	6	3	7	8	13	11	10	15	14	5	12	9	10	14	
	3	4	9	11	12	13	6	7	*	*	*	*	8	13	14	15	
	12	13	14	15	*	*	*	*	*	*	*	*	12	13	14	15	
2x	*	*	*	*	8	13	2	7	10	15	14	5	12	1	6	11	
4x	1	6	11	12	5	10	15	0	9	14	3	4	4	2	2	3	+
	13	13	14	8	8	13	2	7	10	15	14	5	8	9	7	7	
	13	13	14	8	8	13	2	7	8	13	2	7	13	13	14	8	
7x	2	7	8	13	6	11	12	1	4	1	0	3	14	3	4	9	+
	*	*	*	*	*	*	*	*	12	9	6	11	12	1	6	11	

Optimizations

- Working in the transformed basis.
- Inline functions & loop unrolling.
- Combining subrounds.
- Microarchitectural optimizations.

Outline

- 1 Description of Fugue
- 2 SIMD Architecture
- 3 AES VPerm Implementation
- 4 Fugue SIMD Implementation
- 5 Benchmarks**
- 6 Summary

Table: Benchmarks for Intel Core 2 Duo E8400 in cycles/byte

	Implementation	Fugue-224,-256	Fugue-384	Fugue-512
this paper	assembly	15.85	24.87	32.49
jutla-ssse3	intrinsics	18.41	N/A	N/A
jutla-sse4	intrinsics	17.45	N/A	N/A
opt-64	C	27.61	41.53	55.28

Table: Benchmarks for Intel Core 2 Duo E8400 in cycles/byte

	Implementation	Fugue-224,-256	Fugue-384	Fugue-512
this paper	assembly	15.85	24.87	32.49
jutla-ssse3	intrinsics	18.41	N/A	N/A
jutla-sse4	intrinsics	17.45	N/A	N/A
opt-64	C	27.61	41.53	55.28

Table: Benchmarks for Intel Core i7-920 in cycles/byte

	Implementation	Fugue-224,-256	Fugue-384	Fugue-512
this paper	assembly	16.57	23.95	31.10
jutla-ssse3	intrinsics	20.97	N/A	N/A
jutla-sse4	intrinsics	38.50	N/A	N/A
opt-64	C	27.66	41.26	55.16

Outline

- 1 Description of Fugue
- 2 SIMD Architecture
- 3 AES VPerm Implementation
- 4 Fugue SIMD Implementation
- 5 Benchmarks
- 6 Summary**

Summary

- A fast SIMD implementation of hash function Fugue.

Summary

- A fast SIMD implementation of hash function Fugue.
- Resistant to cache-timing attacks.

Summary

- A fast SIMD implementation of hash function Fugue.
- Resistant to cache-timing attacks.
- All four Fugue versions available for Windows & Linux.

Summary

- A fast SIMD implementation of hash function Fugue.
- Resistant to cache-timing attacks.
- All four Fugue versions available for Windows & Linux.
- Tuned for Intel Core 2 Duo and Core i7.

Summary

- A fast SIMD implementation of hash function Fugue.
- Resistant to cache-timing attacks.
- All four Fugue versions available for Windows & Linux.
- Tuned for Intel Core 2 Duo and Core i7.
- Requires SSE4 instruction set support (SSSE3 also possible) and 64-bit mode.

Summary

- A fast SIMD implementation of hash function Fugue.
- Resistant to cache-timing attacks.
- All four Fugue versions available for Windows & Linux.
- Tuned for Intel Core 2 Duo and Core i7.
- Requires SSE4 instruction set support (SSSE3 also possible) and 64-bit mode.

Future Work

- SIMD vs. AES-NI?

Summary

- A fast SIMD implementation of hash function Fugue.
- Resistant to cache-timing attacks.
- All four Fugue versions available for Windows & Linux.
- Tuned for Intel Core 2 Duo and Core i7.
- Requires SSE4 instruction set support (SSSE3 also possible) and 64-bit mode.

Future Work

- SIMD vs. AES-NI?
- Other candidates: ECHO, Grøstl and Shavite-3?