

Chiffrement homomorphe

Boite à outils RevoLUT



ZAMA
TFHE-rs

Blind Array Access

Blind Matrix Access

$(\boxed{i}, \boxed{j}) \rightarrow$

$F[0,0]$	$F[0,1]$	$F[0,2]$	$F[0,3]$	$F[0,4]$	$F[0,5]$	$F[0,6]$	$F[0,7]$
$F[1,0]$	$F[1,1]$	$F[1,2]$	$F[1,3]$	$F[1,4]$	$F[1,5]$	$F[1,6]$	$F[1,7]$
$F[2,0]$	$F[2,1]$	$F[2,2]$	$F[2,3]$	$F[2,4]$	$F[2,5]$	$F[2,6]$	$F[2,7]$
$F[3,0]$	$F[3,1]$	$F[3,2]$	$F[3,3]$	$F[3,4]$	$F[3,5]$	$F[3,6]$	$F[3,7]$
$F[4,0]$	$F[4,1]$	$F[4,2]$	$F[4,3]$	$F[4,4]$	$F[4,5]$	$F[4,6]$	$F[4,7]$

$\boxed{F[i,j]}$

Chiffrement homomorphe

Boite à outils RevoLUT



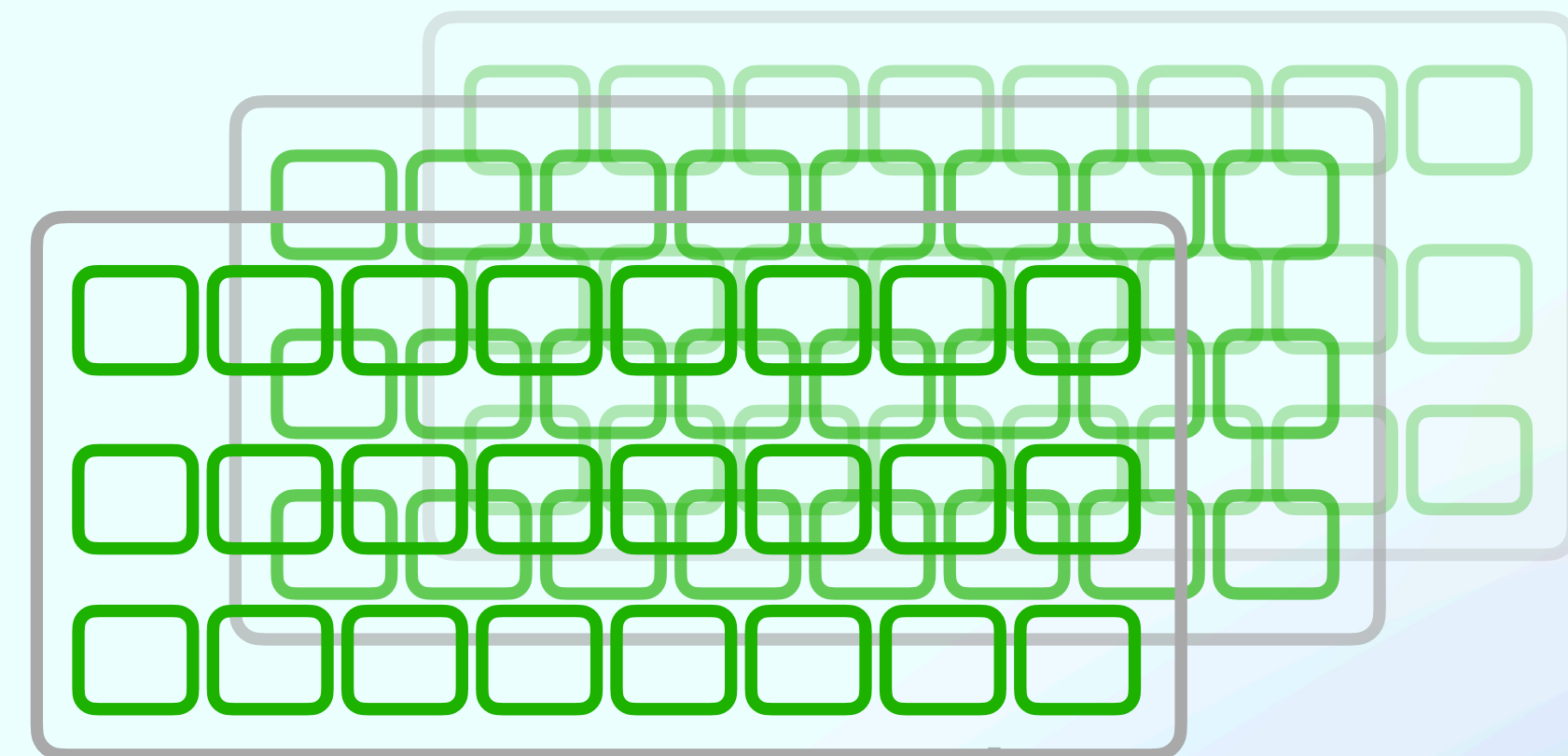
ZAMA
TFHE-rs

Blind Array Access

Blind Matrix Access

Blind Tensor Access

$(\boxed{i}, \boxed{j}) \rightarrow$



$F_1[i, j]$ $F_2[i, j]$ $F_3[i, j]$