

Encrypted CNN Layer

The diagram illustrates the architecture of an Encrypted CNN Layer, showing the flow of data through two parallel processing paths.

Inputs:

- Weights:** A 2x2 matrix with elements w_{ij} , w_{i+1j} , w_{ij+1} , and w_{i+1j+1} .
- Filters:** A 4x4 matrix with elements 1, 1, 0, 0 in the first two rows and 0, 0, 0, 0 in the last two rows.
- Cyphertext:** A 4x4 matrix with elements 0, 1, 2, 3 in the first row, 4, 5, 6, 7 in the second, 8, 9, 10, 11 in the third, and 12, 13, 14, 15 in the fourth.

Processing:

The Cyphertext is processed through two parallel paths, each involving element-wise multiplication ($*$) and summation ($+$).

Top Path:

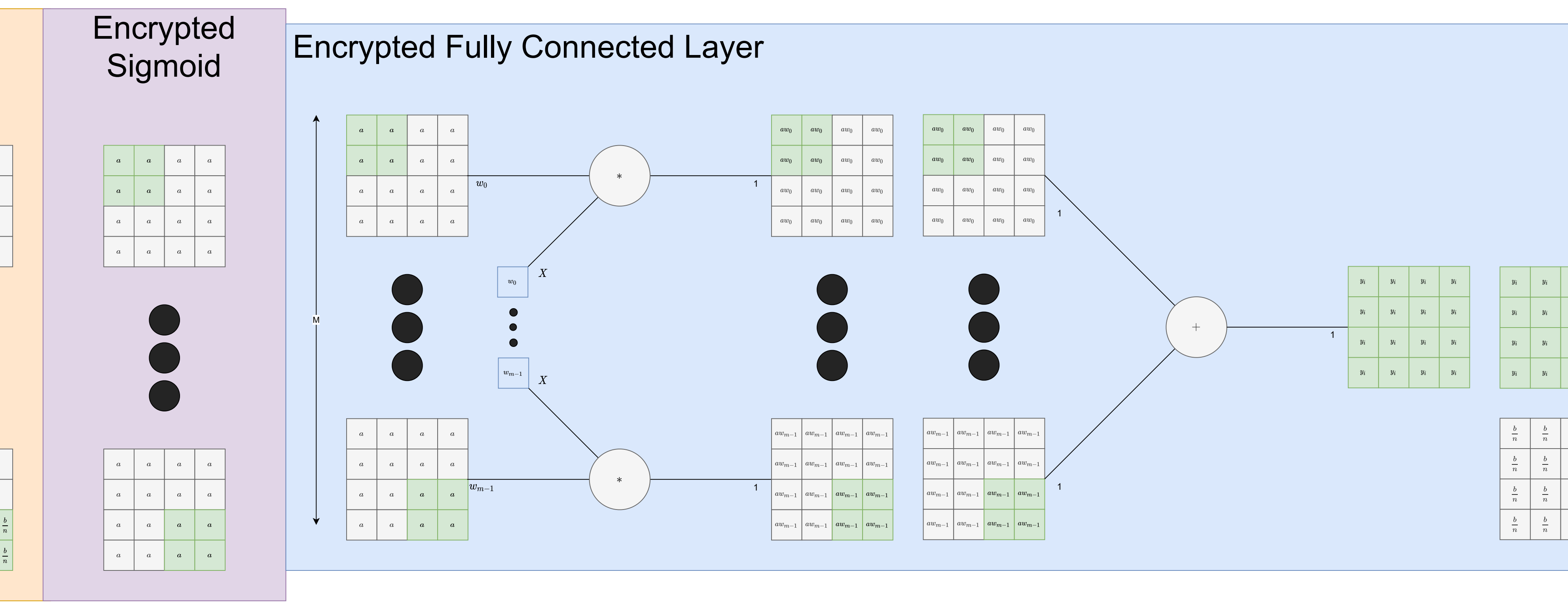
- The Cyphertext is multiplied element-wise by the Filters.
- The result is summed over the last dimension (indicated by the $+$ symbol).
- The final output is a 4x4 matrix of encrypted values.

Bottom Path:

- The Cyphertext is multiplied element-wise by the Filters.
- The result is summed over the last dimension (indicated by the $+$ symbol).
- The final output is a 4x4 matrix of encrypted values.

Output:

The final output is a 4x4 matrix of encrypted values, represented by the last 4x4 matrix in the diagram.

[illegible]

The diagram illustrates a neural network layer with three input grids, a central addition node, and two output grids.

Input Grids (Left):

- Top-left grid (green):

y_i	y_i
y_i	y_i
y_i	y_i
y_i	y_i
- Bottom-left grid (pink):

$\frac{b}{n}$	$\frac{b}{n}$
$\frac{b}{n}$	$\frac{b}{n}$
$\frac{b}{n}$	$\frac{b}{n}$
$\frac{b}{n}$	$\frac{b}{n}$

Central Node: A circle containing a plus sign (+), representing an addition operation.

Output Grids (Right):

- Top-right grid (green):

y_i	y_i	y_i	y_i
y_i	y_i	y_i	y_i
y_i	y_i	y_i	y_i
y_i	y_i	y_i	y_i
- Bottom-right grid (pink):

a	a	a
a	a	a
a	a	a
a	a	a

Connections:

- A line connects the top-left grid to the central node, labeled with a weight of 1.
- A line connects the bottom-left grid to the central node, labeled with a weight of 1.
- A line connects the central node to the top-right grid, labeled with a weight of 1.

Decrypted Sum

The diagram illustrates a neural network layer for calculating the decrypted sum. It features three input boxes labeled \hat{y}_i (green) and three bias boxes labeled b_i (green). The inputs are connected to three addition nodes (circles with a $+$ sign). Each addition node has two inputs: one from an input box and one from a bias box, with a weight of 1 indicated on each connection. The outputs of these three addition nodes are connected to a single larger addition node (circle with a $+$ sign). The output of this final node is connected to an output box labeled \hat{y} (green). A vertical double-headed arrow on the left indicates the dimension N for the input and bias vectors.

Decrypted Loss

The diagram illustrates the decrypted loss function. It features a central white circle with a minus sign ($-$) inside. Two green square boxes are connected to this circle by lines. The top-left box contains the variable y and is connected to the circle with a line labeled 1 . The bottom-left box contains the variable \hat{y} and is connected to the circle with a line labeled -1 . A single line connects the right side of the circle to a green square box labeled $loss$, with a weight of 1 indicated on the line.

SS

1

loss