CLAIMS

1. A device for processing homomorphically encrypted data, the device comprising:

a plurality of inter-line butterfly array blocks, each inter-line butterfly array block comprising a plurality of inter-line modulus butterfly units, each inter-line modulus butterfly unit being configured to perform a modulus butterfly operation based on a computation pair of data points received corresponding to a pair of input data points at a same row of a matrix of input data points;

a plurality of intra-line butterfly array blocks, each intra-line butterfly array block comprising a plurality of intra-line modulus butterfly units, each intra-line modulus butterfly unit being configured to perform a modulus butterfly operation based on a computation pair of data points received corresponding to a pair of input data points at a same column of the matrix of input data points; and

a clock counter communicatively coupled to each inter-line butterfly array block of the plurality of inter-line butterfly array blocks and each intra-line butterfly array block of the plurality of intra-line butterfly array blocks, and configured to output a counter signal for controlling said each inter-line butterfly array block and said each intra-line butterfly array block to operate with single cycle initiation interval, wherein during each single cycle initiation interval, at least one inter-line modulus butterfly unit and at least one intra-line modulus butterfly unit are simultaneously configured to receive a respective computation pair of data points and to each perform a corresponding modulus butterfly operation;

wherein the matrix of input data points comprises a plurality of columns of input data points, wherein a plurality of parallel input data points derived from the homomorphically encrypted data are arranged into the plurality of columns of input data points, and

wherein the plurality of inter-line butterfly array blocks and the plurality of intra-line butterfly array blocks are arranged in series to form a pipeline for processing the matrix of input data points.

2. The device according to claim 1, further comprising a data point arranging block configured to receive the plurality of parallel input data points derived from the homomorphically encrypted data and arrange the plurality of parallel input data points received into the plurality of columns of input data points to form the matrix of input data points.

3. The device according to claim 1, wherein

each inter-line butterfly array block of the plurality of inter-line butterfly array blocks comprises a plurality of first-in-first-out (FIFO) input data buffers, and

for said each inter-line butterfly array block, each FIFO input data buffer of the plurality of FIFO input data buffers is communicatively coupled to the plurality of inter-line modulus butterfly units of the inter-line butterfly array block and is configured to receive a plurality of columns of data points and output each of the plurality of columns of data points to the plurality of inter-line modulus butterfly units column-by-column in FIFO order for each of the plurality of inter-line modulus butterfly units to perform said modulus butterfly operation based on the computation pair of data points received.

4. The device according to claim 3, wherein for said each inter-line butterfly array block:

said each of the plurality of columns of data points has a number of data points being half of the number of input data points in a column of the plurality of columns of input data points, and

the plurality of inter-line modulus butterfly units of the inter-line butterfly array block has a number of inter-line modulus butterfly units being half of the number of input data points in the column of the plurality of columns of input data points.

5. The device according to claim 3, wherein for said each inter-line butterfly array block:

the inter-line butterfly array block comprises a first set of multiplexer units, each FIFO input data buffer of the plurality of FIFO input data buffers of the inter-line butterfly array being communicatively coupled to the plurality of inter-line modulus butterfly units of the inter-line butterfly array block via a multiplexer unit of the first set of multiplexer units, and

the clock counter is communicatively coupled to each multiplexer unit of the first set of multiplexer units for controlling the inter-line butterfly array block to operate with single cycle initiation interval.

6. The device according to claim 5, wherein

a first FIFO input data buffer and a third FIFO input data buffer of the plurality of FIFO input data buffers of the inter-line butterfly array block are each communicatively coupled to a first multiplexer unit of the first set of multiplexer units, the first multiplexer unit being

configured to output a column of data points of the plurality of columns of data points from a selected FIFO input data buffer amongst the first and third FIFO input data buffers to the plurality of inter-line modulus butterfly units of the inter-line butterfly array block, the selected FIFO input data buffer being selected based on the counter signal received by the first multiplexer unit of the first set of multiplexer units, and

a second FIFO input data buffer and a fourth FIFO input data buffer of the plurality of FIFO input data buffers of the inter-line butterfly array block are each communicatively coupled to a second multiplexer unit of the first set of multiplexer units, the second multiplexer unit being configured to output a column of data points of the plurality of columns of data points from a selected FIFO input data buffer amongst the second and fourth FIFO input data buffers to the plurality of inter-line modulus butterfly units of the inter-line butterfly array block, the selected FIFO input data buffer being selected based on the counter signal received by the second multiplexer unit of the first set of multiplexer units.

7. The device according to claim 6, wherein for each inter-line butterfly array block from a first inter-line butterfly array block to a penultimate inter-line butterfly array block of the plurality of inter-line butterfly array blocks:

the inter-line butterfly array block further comprises a second set of multiplexer units, each FIFO input data buffer of the plurality of FIFO input data buffers of an immediately subsequent inter-line butterfly array block of the plurality of inter-line butterfly array blocks with respect to the inter-line butterfly array block is communicatively coupled to the plurality of inter-line modulus butterfly units of the inter-line butterfly array block via a multiplexer unit of the second set of multiplexer units, and

the clock counter is communicatively coupled to each multiplexer unit of the second set of multiplexer units for controlling the inter-line butterfly array block to operate with single cycle initiation interval.

8. The device according to claim 7, wherein

a first FIFO input data buffer and a second FIFO input data buffer of the plurality of FIFO input data buffers of the immediately subsequent inter-line butterfly array block are each communicatively coupled to a first multiplexer unit of the second of multiplexer units, the first multiplexer unit being configured to output a first portion of a column of data points from the plurality of inter-line modulus butterfly units of the inter-line butterfly array block to a selected

FIFO input data buffer amongst the first and second FIFO input data buffers, the selected FIFO input data buffer being selected based on the counter signal received by the first multiplexer unit of the second set of multiplexer units, and

the third FIFO input data buffer and the fourth FIFO input data buffer of the plurality of FIFO input data buffers of the immediately subsequent inter-line butterfly array block are each communicatively coupled to a second multiplexer unit of the second set of multiplexer units, the second multiplexer unit being configured to output a second portion of a column of data points from the plurality of inter-line modulus butterfly units of the inter-line butterfly array block to a selected FIFO input data buffer amongst the third and fourth FIFO input data buffers, the selected FIFO input data buffer being selected based on the counter signal received by the second multiplexer unit of the second set of multiplexer units.

9. The device according to claim 7, wherein

the first inter-line butterfly array block further comprises a third set of multiplexer units,

the first and second FIFO input data buffers of the plurality of FIFO input data buffers of the first inter-line butterfly array block are each communicatively coupled to a first multiplexer unit of the third set of multiplexer units, the first multiplexer unit being configured to output a first portion of a column of data points from an input register to a selected FIFO input data buffer amongst the first and second FIFO input data buffers, the selected FIFO input data buffer being selected based on the counter signal received by the first multiplexer unit of the third set of multiplexer units,

the third and fourth FIFO input data buffers of the plurality of FIFO input data buffers of the first inter-line butterfly array block are each communicatively coupled to a second multiplexer unit of the third set of multiplexer units, the second multiplexer unit being configured to output a second portion of the column of data points from the input register to a selected FIFO input data buffer amongst the third and fourth FIFO input data buffers, the selected FIFO input data buffer being selected based on the counter signal received by the second multiplexer unit of the third set of multiplexer units, and

the clock counter is communicatively coupled to each multiplexer unit of the third set of multiplexer units for controlling the first inter-line butterfly array block to operate with single cycle initiation interval.

10. The device according to claim 5, wherein a last inter-line butterfly array block of the plurality of inter-line butterfly array blocks further comprises:

a second set of multiplexer units;

a third multiplexer unit; and

a plurality of FIFO output data buffers, wherein

each FIFO output data buffer of the plurality of FIFO output data buffers of the inter-line butterfly array is communicatively coupled to the plurality of inter-line modulus butterfly units of the last inter-line butterfly array block via a multiplexer unit of the second set of multiplexer units, and

the third multiplexer unit is configured to output a column of data points from a selected FIFO output data buffer amongst the plurality of FIFO output data buffers, the selected FIFO output data buffer being selected based on the counter signal received by the third multiplexer unit, and

the clock counter is communicatively coupled to each multiplexer unit of the second set of multiplexer units and the third multiplexer unit for controlling the last inter-line butterfly array block to operate with single cycle initiation interval.

11. The device according to claim 1, wherein

each intra-line butterfly array block of the plurality of intra-line butterfly array blocks comprises an input register,

for said each intra-line butterfly array block, the input register is communicatively coupled to the plurality of intra-line modulus butterfly units of the intra-line butterfly array block and is configured to receive a column of data points and output the column of data points to the plurality of intra-line modulus butterfly units for each of the plurality of intra-line modulus butterfly units to perform said modulus butterfly operation based on the computation pair of data points received.

12. The device according to claim 1, further comprising a weight modulus multiplication block comprising a plurality of modulus multiplication units, each modulus multiplication unit being configured to perform a modulus multiplication operation based on a data point received.

13. The device according to claim 1, wherein the plurality of intra-line butterfly array blocks are arranged after the plurality of inter-line butterfly array blocks in the pipeline.

14. The device according to claim 13, wherein the pipeline is configured to perform a discrete Galois transform (DGT) of the plurality of parallel input data points.

15. The device according to claim 1, wherein the plurality of inter-line butterfly array blocks are arranged after the plurality of intra-line butterfly array blocks in the pipeline.

16. The device according to claim 15, wherein the pipeline is configured to perform an inverse discrete Galois transform (iDGT) of the plurality of parallel input data points.

17. The device according to claim 1, wherein

the plurality of parallel input data points has 2^n number of parallel input data points,

the matrix has 2^r number of rows of input data points and 2^{n-r} number of columns of input data points, wherein $n \geq 4$, $r \geq 2$ and $r < n$,

the plurality of inter-line butterfly array blocks has q number of inter-line butterfly array blocks, wherein $q = n - r$, and

the plurality of intra-line butterfly array blocks has r number of intra-line butterfly array blocks.

18. The device according to claim 1, wherein the device is a field-programmable gate array (FPGA) device or an application specific integrated circuit (ASIC) device.

19. A system comprising:

a memory;

a device for processing homomorphically encrypted data; and

at least one processor communicatively coupled to the memory and configured to:

send, from the memory, a plurality of parallel input data points derived from homomorphically encrypted data to the device for processing by the device; and

receive, at the memory, a plurality of parallel output data points produced by the device from processing the plurality of parallel input data points,

wherein the device comprises:

a plurality of inter-line butterfly array blocks, each inter-line butterfly array block comprising a plurality of inter-line modulus butterfly units, each inter-line modulus

butterfly unit being configured to perform a modulus butterfly operation based on a computation pair of data points received corresponding to a pair of input data points at a same row of a matrix of input data points;

a plurality of intra-line butterfly array blocks, each intra-line butterfly array block comprising a plurality of intra-line modulus butterfly units, each intra-line modulus butterfly unit being configured to perform a modulus butterfly operation based on a computation pair of data points received corresponding to a pair of input data points at a same column of the matrix of input data points; and

a clock counter communicatively coupled to each inter-line butterfly array block of the plurality of inter-line butterfly array blocks and each intra-line butterfly array block of the plurality of intra-line butterfly array blocks, and configured to output a counter signal for controlling said each inter-line butterfly array block and said each intra-line butterfly array block to operate with single cycle initiation interval, wherein during each single cycle initiation interval, at least one inter-line modulus butterfly unit and at least one intra-line modulus butterfly unit are simultaneously configured to receive a respective computation pair of data points and to each perform a corresponding modulus butterfly operation;

wherein the matrix of input data points comprises a plurality of columns of input data points, wherein a plurality of parallel input data points derived from the homomorphically encrypted data are arranged into the plurality of columns of input data points, and

wherein the plurality of inter-line butterfly array blocks and the plurality of intra-line butterfly array blocks are arranged in series to form a pipeline for processing the matrix of input data points.

20. A method of forming a device for processing homomorphically encrypted data, the method comprising:

providing a plurality of inter-line butterfly array blocks, each inter-line butterfly array block comprising a plurality of inter-line modulus butterfly units, each inter-line modulus butterfly unit being configured to perform a modulus butterfly operation based on a computation pair of data points received corresponding to a pair of input data points at a same row of a matrix of input data points;

providing a plurality of intra-line butterfly array blocks, each intra-line butterfly array block comprising a plurality of intra-line modulus butterfly units, each intra-line modulus butterfly unit being configured to perform a modulus butterfly operation based on a

computation pair of data points received corresponding to a pair of input data points at a same column of the matrix of input data points; and

providing a clock counter communicatively coupled to each inter-line butterfly array block of the plurality of inter-line butterfly array blocks and each intra-line butterfly array block of the plurality of intra-line butterfly array blocks, and configured to output a counter signal for controlling said each inter-line butterfly array block and said each intra-line butterfly array block to operate with single cycle initiation interval, wherein during each single cycle initiation interval, at least one inter-line modulus butterfly unit and at least one intra-line modulus butterfly unit are simultaneously configured to receive a respective computation pair of data points and to each perform a corresponding modulus butterfly operation;

wherein the matrix of input data points comprises a plurality of columns of input data points, wherein a plurality of parallel input data points derived from the homomorphically encrypted data are arranged into the plurality of columns of input data points, and

wherein the plurality of inter-line butterfly array blocks and the plurality of intra-line butterfly array blocks are arranged in series to form a pipeline for processing the matrix of input data points.