

CLAIMS

We Claim:

1. An integrated circuit (IC) homomorphic processor chip comprising:
 - at least one processor slice, the slice including
 - local control circuitry;
 - a numeric theoretic transform (NTT) butterfly unit responsive to the local control circuitry to operate in multiple modes for performing operations on encrypted data using homomorphic encryption, each mode associated with a different configuration of the NTT butterfly unit; and
 - on-chip memory coupled to the control circuitry and the NTT butterfly unit.
2. The IC homomorphic processor chip of claim 1, wherein the NTT butterfly unit is responsive to the local control circuitry to operate in multiple modes for operations involving fully homomorphic encryption.
3. The IC homomorphic processor chip of claim 1, wherein the NTT butterfly unit is responsive to the local control circuitry to operate in multiple modes for operations involving partially homomorphic encryption.
4. The IC homomorphic processor chip according to any one of claims 1-3, wherein:
 - a first configuration for the NTT butterfly unit employs first circuitry to carry out a first ciphertext (C_{txt}) function; and
 - a second configuration for the NTT butterfly unit reuses at least a portion of the first circuitry to carry out a second C_{txt} function.
5. The IC homomorphic processor chip of claim 4, wherein:
 - the first circuitry carries out a ciphertext (C_{txt}) addition function; and
 - the second C_{txt} function comprises a C_{txt} multiplication function.

6. The IC homomorphic processor chip of claim 5, wherein:
the first circuitry includes a modular adder.
7. The IC homomorphic processor chip of claim 6, wherein:
the modular adder comprises a combinational modular adder.
8. The IC homomorphic processor chip of claim 6, wherein:
the modular adder comprises a sequential modular adder.
9. The IC homomorphic processor chip of claim 5, wherein:
the second configuration includes second circuitry comprising a modular multiplier.
10. The IC homomorphic processor chip of claim 9, wherein the modular multiplier comprises a parallel integer multiplier.
11. The IC homomorphic processor chip of claim 10, wherein the modular multiplier further comprises:
a modular reduction unit.
12. The IC homomorphic processor chip according to any of claims 1-11, wherein the IC homomorphic processor includes multiple processor slices, and wherein the IC homomorphic processor further comprises:
master control circuitry to interface the multiple processor slices with external memory via an external processor interface.
13. The IC homomorphic processor chip of claim 12, wherein the local control circuitry receives instructions from the master control circuitry to:
retrieve a set of C_{txt} coefficient values from the memory;
load the set of values into a processing pipeline;
perform at least one C_{txt} operation to generate transformed values; and
store the transformed values to a destination memory location.

14. The IC homomorphic processor chip of claim 13, wherein the instructions from the master control circuitry further comprises instructions to:
- perform NTT transformations on the loaded set of values to generate corresponding transformed values in the NTT domain.
15. The IC homomorphic processor chip according to any one of claims 13 or 14, wherein the instructions from the master control circuitry to perform at least one Ctxt operation comprises instructions to:
- perform at least one Ctxt operation from the group consisting of addition operation, subtraction operation, multiplication operation, XOR operation, XNOR operation, AND operation, equality operation, smaller than operation, larger than operation, entity operation, copy operation and negation operation.
16. The IC homomorphic processor chip according to any of claims 1-16, wherein:
- the NTT butterfly unit is realized as a single-stage unit.
17. A homomorphic encryption system, comprising:
- an integrated circuit (IC) homomorphic processor chip;
 - main memory external to the IC homomorphic processor chip;
 - a data path for transferring data between the main memory and the IC homomorphic processor chip;
 - a control path to control the transfers between the main memory and the IC homomorphic processor chip; and
 - wherein the IC homomorphic processor chip comprises
 - master control circuitry to control the transfers of data between the main memory and the IC homomorphic processor chip via the control path; and
 - multiple processor slices corresponding to a pipeline depth, each of the multiple processor slices including
 - local control circuitry;
 - a numeric theoretic transform (NTT) butterfly unit responsive to the local control circuitry to operate in multiple modes for performing operations on encrypted data using homomorphic encryption, each mode associated with a different configuration of the

NTT butterfly unit; and

on-chip memory coupled to the local control circuitry and the NTT butterfly unit.

18. The homomorphic encryption system of claim 17, wherein the homomorphic encryption comprises fully homomorphic encryption.

19. The homomorphic encryption system of claim 17, wherein the homomorphic encryption comprises partially homomorphic encryption.

20. The homomorphic encryption system according to any of claims 17-19, wherein the master control circuitry schedules operations for each of the multiple processor slices to:

- retrieve a set of C_{txt} coefficient values from the external memory;
- load the set of values into a processing pipeline;
- perform at least one C_{txt} operation; and
- store the transformed values to a destination memory location.

21. The homomorphic encryption system of claim 20, wherein the scheduled operations from the master control circuitry further comprises scheduled operations for each of the multiple processor slices to:

- perform NTT transformation operations on the loaded set of values to generate corresponding transformed values in the NTT domain.

22. The homomorphic encryption system according to any one of claims 20 or 21, wherein the scheduled operations from the master control circuitry further comprises scheduled operations for each of the multiple processor slices to:

- perform at least one C_{txt} operation from the group consisting of addition operation, subtraction operation, multiplication operation, XOR operation, XNOR operation, AND operation, equality operation, smaller than operation, larger than operation, entity operation, copy operation and negation operation.

23. The homomorphic encryption system of claim 21, wherein:
each of the NTT butterfly units comprises a single-stage butterfly; and
wherein a given NTT transformation operation involves $\log(n)-1$ stages of evaluation by the NTT butterfly unit, where “n” represents a degree of a polynomial associated with the coefficient values.
24. A numeric theoretic transform (NTT) butterfly circuit comprising:
a high input word path including
a first adder/subtractor,
a first multiplier, and
first selection circuitry coupled to the first adder/subtractor and the first multiplier and including respective bypass paths to selectively bypass the first adder/subtractor and the first multiplier;
a low input word path including
a second adder/subtractor,
a second multiplier, and
second selection circuitry coupled to the second adder/subtractor and the second multiplier and including respective bypass paths to selectively bypass the second adder/subtractor and the second multiplier;
wherein the high and low input word paths are cross-coupled, and the first and second selection circuitry is responsive to different mode control signals to reconfigure the low and high input word paths into different logic processing units.
25. The NTT butterfly circuit of claim 24, wherein:
a first configuration for the NTT butterfly circuit employs first circuitry to carry out a ciphertext (C_{txt}) addition function; and
a second configuration for the NTT butterfly circuit reuses at least a portion of the first circuitry to carry out a C_{txt} multiplication function.
26. The NTT butterfly circuit of claim 24, wherein:
each of the first and second adder/subtractors comprises a combinational modular adder.

27. The NTT butterfly circuit of claim 24, wherein:
each of the first and second multipliers comprises a parallel integer multiplier.
28. The NTT butterfly circuit of claim 24, wherein each of the first and second multipliers further comprises:
a modular reduction unit.
29. The NTT butterfly circuit of claim 24, wherein:
each of the first and second adder/subtractors and multipliers includes associated critical paths; and
wherein each of the associated critical paths is bounded by register circuitry.
30. The NTT butterfly circuit of claim 24, wherein:
the NTT butterfly circuit is realized as a single-stage butterfly; and
wherein a given NTT transformation operation involves $\log(n)-1$ stages of evaluation by the NTT butterfly circuit, where “n” represents a degree of a polynomial associated with the coefficient values.
31. A method of operation in a homomorphic processor integrated circuit (IC) chip, the method comprising:
transforming ciphertext (Ctxt) symbols into a number theoretic transform (NTT) domain, the transforming including, for a given processor slice,
generating a mode control signal with local control circuitry, the mode control signal corresponding to one of multiple modes of operations involving homomorphic encryption; and
configuring an NTT butterfly unit in response to the mode control signal.
32. The method of operation in a homomorphic processor IC chip according to claim 31, wherein the homomorphic encryption comprises fully homomorphic encryption.
33. The method of operation in a homomorphic processor IC chip according to claim 31, wherein the homomorphic encryption comprises partially homomorphic encryption.

34. The method according to any of claims 31-33, wherein the mode control signal comprises a first mode control signal corresponding to a first mode of operation, and wherein the NTT butterfly unit responds to the first mode control signal by:

configuring the NTT butterfly unit to carry out a Ctxt addition function.

35. The method according to claim 34, wherein the mode control signal comprises a second mode control signal corresponding to a second mode of operation, and wherein the NTT butterfly unit responds to the second mode control signal by:

configuring the NTT butterfly unit to carry out a Ctxt multiplication function; and
reusing a portion of the NTT butterfly unit employed in the addition function to carry out the multiplication function.

36. The method according to any of claims 31-35, wherein the transforming comprises:

operating multiple processor slices in parallel, each processor slice including a copy of the local control circuitry and a copy of the NTT butterfly unit.

37. The method according to claim 36, further comprising:

pipelining multiple operations carried out by the multiple processor slices.

38. The method according to claim 37, further comprising:

interfacing the multiple processor slices with external memory via an external processor interface, the interfacing controlled by master control circuitry.

39. The method according to claim 38, wherein the master control circuitry generates instructions for the local control circuitry of the multiple slices, the local control circuitry responsive to the instructions to carry out the steps including:

retrieving a set of Ctxt coefficient values from the memory;
loading the set of values into a processing pipeline;
performing at least one Ctxt operation to generate transformed values; and
storing the transformed values to a destination location in the external memory.

40. The method according to claim 39, further comprising the step of performing NTT transformations on the loaded set of values to generate corresponding transformed values in the NTT domain.

41. The method according to any one of claims 39 or 40, wherein the at least one Ctxt operation is selected from the group consisting of addition operation, subtraction operation, multiplication operation, XOR operation, XNOR operation, AND operation, equality operation, smaller than operation, larger than operation, entity operation, copy operation and negation operation.

42. A method of operation in a homomorphic encryption system, the method comprising:
providing a homomorphic processor integrated circuit (IC) chip including a configurable numeric theoretic transform (NTT) butterfly unit;
interfacing the homomorphic processor IC chip with external memory via a data path and a control path; and
transforming ciphertext (Ctxt) symbols into an NTT domain, the transforming including, for a given processor slice,
generating a mode control signal with local control circuitry, the mode control signal corresponding to one of multiple modes of operations involving homomorphic encryption, and
configuring the NTT butterfly unit in response to the mode control signal.

43. The method of operation in a homomorphic encryption system according to claim 42, wherein the homomorphic encryption comprises fully homomorphic encryption.

44. The method of operation in a homomorphic encryption system according to claim 42, wherein the homomorphic encryption comprises partially homomorphic encryption.

44. The method according to any of claims 42-44, wherein the mode control signal comprises a first mode control signal corresponding to a first mode of operation, and wherein the NTT butterfly unit responds to the first mode control signal by:
configuring the NTT butterfly unit to carry out a Ctxt addition function.

45. The method according to claim 44, wherein the mode control signal comprises a second mode control signal corresponding to a second mode of operation, and wherein the NTT butterfly unit responds to the second mode control signal by:
- configuring the NTT butterfly unit to carry out a Ctxt multiplication function; and
 - reusing a portion of the NTT butterfly unit employed in the addition function to carry out the multiplication function.
46. The method according to any of claims 42-45, wherein the transforming comprises:
- operating multiple processor slices in parallel, each processor slice including a copy of the local control circuitry and a copy of the NTT butterfly unit.
47. The method according to claim 46, further comprising:
- pipelining multiple operations carried out by the multiple processor slices.
48. The method according to claim 47, further comprising:
- interfacing the multiple processor slices with external memory via an external processor interface, the interfacing controlled by master control circuitry.
49. The method according to claim 48, wherein the master control circuitry generates instructions for the local control circuitry of the multiple slices, the local control circuitry responsive to the instructions to carry out the steps including:
- retrieving a set of Ctxt coefficient values from the memory;
 - loading the set of values into a processing pipeline;
 - performing at least one Ctxt operation to generate transformed values; and
 - storing the transformed values to a destination location in the external memory.
50. The method according to claim 49 further comprising the step of performing NTT transformations on the loaded set of values to generate corresponding transformed values in the NTT domain.
51. The method according to any of claims 49 or 50, wherein the at least one Ctxt operation is selected from the group consisting of addition operation, subtraction operation, multiplication

operation, XOR operation, XNOR operation, AND operation, equality operation, smaller than operation, larger than operation, entity operation, copy operation and negation operation.

52. A method of operation in a numeric theoretic transform (NTT) butterfly circuit, the circuit including a high input word path and a low input word path, the high input word path including a first adder/subtractor, and a first multiplier, the low input word path including a second adder/subtractor, and a second multiplier, wherein the method comprises:

selectively bypassing the second adder/subtractor and the second multiplier; and
reconfiguring the low and high input word paths into different logic processing units in response to different mode control signals.

53. The method according to claim 52, wherein the reconfiguring comprises:

in response to receiving a first mode control signal, configuring the NTT butterfly circuit to carry out a ciphertext (C_{txt}) addition function; and

in response to receiving a second mode control signal, configuring the NTT butterfly circuit to carry out a C_{txt} multiplication function.

54. The method according to any of claims 52-53, further comprising:

employing a combinational modular adder for each of the first and second adder/subtractors.

55. The method according to any of claims 52-54, further comprising:

employing a parallel integer multiplier for each of the first and second multipliers.

56. The method according to any of claims 52-55, wherein each of the first and second multipliers includes a reduction unit, and wherein the method further comprises:

operating each reduction unit.

57. The NTT butterfly circuit according to any of claims 52-56, wherein the NTT butterfly circuit is realized as a single-stage butterfly, and wherein the transforming comprises:

operating the NTT butterfly circuit through $\log(n)-1$ stages of evaluation, where “n” represents a degree of a polynomial associated with coefficient values.

58. A homomorphic processor integrated circuit (IC) chip for transforming ciphertext (C_{txt}) symbols into a number theoretic transform (NTT) domain, the IC homomorphic processor chip comprising:

at least one processor slice, the slice including

local control circuitry;

an NTT butterfly unit; and

on-chip memory coupled to the control circuitry and the NTT butterfly unit, the on-chip memory partitioned into separately accessible storage units for homomorphic processing functions, the on-chip memory including

multiple input/output (I/O) storage units,

a bit decomposed polynomial storage unit, and

a twiddle factor memory unit.

59. The homomorphic processor IC chip according to claim 58, wherein:

a first one of the I/O storage units stores ciphertexts (C_{txts}) in a row-by-row format; and

a second one of the I/O storage units stores C_{txts} in a column-by-column format.

60. The homomorphic processor IC chip according to claim 59, wherein:

a third one of the I/O storage units stores output C_{txts} resulting from a multiplication operation involving a first C_{txt} from the first storage unit multiplied with a second C_{txt} from the second storage unit.

61. The homomorphic processor IC chip according to claim 60, further comprising:

a memory counter coupled to the second memory unit.

62. The homomorphic processor IC chip according to any of claims 60-61, wherein:

a single row transformation of a C_{txt} in a given row of the first one of the I/O storage units results in a corresponding resulting row in the third one of the I/O storage units.

63. The homomorphic processor IC chip according to any of claims 58-63, wherein:
one of the multiple I/O storage units is configured as a ping-pong memory coupled to an external memory.
64. The homomorphic processor IC chip according to claim 63, wherein the ping-pong memory includes:
a first sub-array to carry out a first memory operation; and
a second sub-array to carry out a second operation concurrent with the first memory operation.
65. The homomorphic processor IC chip according to any of claims 58-63, wherein the on-chip memory comprises DRAM.
66. A method of operation in a homomorphic processor integrated circuit (IC) chip, the method comprising:
partitioning on-chip memory into separately accessible storage units for homomorphic processing functions, the on-chip memory including multiple input/output (I/O) storage units, a bit decomposed polynomial storage unit, and a twiddle factor memory unit; and
performing at least one ciphertext (Ctxt) operation on a loaded set of values with a configurable numeric theoretic transform (NTT) butterfly unit coupled to the partitioned on-chip memory.
67. The method according to claim 66, further comprising:
transforming the loaded set of values to generate corresponding transformed values in the NTT domain.
68. The method according to any one of claims 66 or 67, wherein the at least one Ctxt operation is selected from the group consisting of addition operation, subtraction operation, multiplication operation, XOR operation, XNOR operation, AND operation, equality operation, smaller than operation, larger than operation, entity operation, copy operation and negation operation.

69. The method according to any of claims 67-68, wherein the transforming further comprises:

reading a first ciphertext (Ctxt) from a first one of the I/O storage units in a row-by-row format; and

reading a second Ctxt from a second one of the I/O storage units in a column-by-column format.

70. The method according to claim 69, wherein the transforming further comprises:

multiplying the first Ctxt with the second Ctxt to generate a resulting Ctxt; and
writing the resulting Ctxt into a third one of the I/O storage units.

71. The method according to any of claims 66-70, wherein one of the multiple I/O storage units includes respective first and second sub-arrays configured as a ping-pong memory unit, wherein the method further comprises:

operating the first sub-array to carry out a first operation; and

operating the second sub-array to carry out a second operation concurrent with the first operation.

72. A method of operation in a homomorphic processor integrated circuit (IC) chip, the method comprising:

retrieving a first ciphertext (Ctxt) from a first on-chip memory unit, the first Ctxt retrieved via a row format read operation;

transforming the first Ctxt into a numeric theoretic transform (NTT) domain;

retrieving a second ciphertext (Ctxt) from a second on-chip memory unit, the second Ctxt retrieved via a column format read operation;

transforming the second Ctxt into the NTT domain;

multiplying the transformed first Ctxt with the transformed second Ctxt to generate a resulting Ctxt; and

storing the resulting Ctxt in a third memory unit.