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;

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

wherein a given NTT transformation operation involves $\log_2 2(n)-1$ stages of evaluation by the NTT butterfly unit, where "n" represents a degree of a polynomial associated with a set of ciphertext (C_{txt}~~txt~~) coefficient values.

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}~~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 C_{txt} operation comprises instructions 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.

16. The IC homomorphic processor chip according to any of claims 1-15, 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;

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

wherein a given NTT transformation operation involves $\log_2 2(n)-1$ stages of evaluation by the NTT butterfly unit, where "n" represents a degree of a polynomial associated with a set of ciphertext (C_{txt} txt) coefficient values.

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} txt coefficient values from the external memory;

load the set of values into a processing pipeline;

perform at least one C_{txt} 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} 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 method of operation in a homomorphic processor integrated circuit (IC) chip, the method comprising:

transforming ciphertext (C_{txt}) 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;

configuring an NTT butterfly unit in response to the mode control signal; and

wherein a given NTT transformation operation involves $\log_2 2(n)-1$ stages of evaluation by the NTT butterfly unit, where "n" represents a degree of a polynomial associated with a set of ciphertext (C_{txt}~~txt~~) coefficient values.

25. The method of operation in a homomorphic processor IC chip according to claim 24, wherein the homomorphic encryption comprises either fully homomorphic encryption or partially homomorphic encryption.

26. The method according to any of claims 24-25, 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 C_{txt} addition function.

27. The method according to claim 26, 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 C_{txt} multiplication function; and

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

28. The method according to any of claims 24-27, 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.

29. The method according to claim 28, further comprising:

pipelining multiple operations carried out by the multiple processor slices.

30. The method according to claim 29, further comprising:

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

31. The method according to claim 30, 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 C_{txt} coefficient values from the memory;

loading the set of values into a processing pipeline;

performing at least one C_{txt} operation to generate transformed values; and

storing the transformed values to a destination location in the external memory.

32. The method according to claim 31, further comprising the step of performing NTT transformations on the loaded set of values to generate corresponding transformed values in the NTT domain.

33. The method according to any one of claims 31 or 32, wherein the at least one C_{txt} 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.

34. 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 (C_{txt}) 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,

configuring the NTT butterfly unit in response to the mode control signal, and

wherein a given NTT transformation operation involves $\log_2(n)-1$ stages of evaluation by the NTT butterfly unit, where "n" represents a degree of a polynomial associated with a set of ciphertext (C_{txt}) coefficient values.

35. The method of operation in a homomorphic encryption system according to claim 34, wherein the homomorphic encryption comprises either fully homomorphic encryption or partially homomorphic encryption.

36. The method according to any of claims 34 or 35, 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 C_{txt} addition function.

37. The method according to claim 36, 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 C_{txt} multiplication function; and

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

38. The method according to any of claims 34-37, 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.

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

pipelining multiple operations carried out by the multiple processor slices.

40. The method according to claim 39, further comprising:

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

41. The method according to claim 40, 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 C_{txt} coefficient values from the memory;

loading the set of values into a processing pipeline;

performing at least one C_{txt} operation to generate transformed values; and

storing the transformed values to a destination location in the external memory.

42. The method according to claim 41 further comprising the step of performing NTT transformations on the loaded set of values to generate corresponding transformed values in the NTT domain.