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

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 (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; 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 either fully homomorphic encryption or partially homomorphic encryption.

33. The method according to any of claims 31-32, 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.

34. The method according to claim 33, 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.

35. The method according to any of claims 31-34, 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.

36. The method according to claim 35, further comprising:

pipelining multiple operations carried out by the multiple processor slices.

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

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

38. The method according to claim 37, 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.

39. The method according to claim 38, further comprising the step of performing NTT transformations on the loaded set of values to generate corresponding transformed values in the NTT domain.

40. The method according to any one of claims 38 or 39, 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.

41. 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, and

configuring the NTT butterfly unit in response to the mode control signal.

42. The method of operation in a homomorphic encryption system according to claim 41, wherein the homomorphic encryption comprises either fully homomorphic encryption or partially homomorphic encryption.

43. The method according to any of claims 41 or 42, 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.

44. The method according to claim 43, 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.

45. The method according to any of claims 41-44, 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.

46. The method according to claim 45, further comprising:

pipelining multiple operations carried out by the multiple processor slices.

47. The method according to claim 46, further comprising:

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

48. The method according to claim 47, 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.

49. The method according to claim 48 further comprising the step of performing NTT transformations on the loaded set of values to generate corresponding transformed values in the NTT domain.

50. 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.

51. The method according to claim 50, 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.

52. The method according to any of claims 50-51, further comprising:

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

53. The method according to any of claims 50-52, further comprising:

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

54. The method according to any of claims 50-53, wherein each of the first and second multipliers includes a reduction unit, and wherein the method further comprises:

operating each reduction unit.

55. The NTT butterfly circuit according to any of claims 50-54, 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.

56. 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.

57. The homomorphic processor IC chip according to claim 56, 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.

58. The homomorphic processor IC chip according to claim 57, wherein:

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

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

a memory counter coupled to the second memory unit.

60. The homomorphic processor IC chip according to any of claims 58 or 59, 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.

61. The homomorphic processor IC chip according to any of claims 56-60, wherein:

one of the multiple I/O storage units is configured as a ping-pong memory coupled to an external memory.

62. The homomorphic processor IC chip according to claim 61, 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.

63. 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 (C_{txt}) operation on a loaded set of values with a configurable numeric theoretic transform (NTT) butterfly unit coupled to the partitioned on-chip memory.

64. The method according to claim 63, further comprising:

transforming the loaded set of values to generate corresponding transformed values in the NTT domain.

65. The method according to claim 64, wherein the transforming further comprises:

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

reading a second C_{txt} from a second one of the I/O storage units in a column-by-column format.

66. The method according to claim 65, wherein the transforming further comprises:

multiplying the first C_{txt} with the second C_{txt} to generate a resulting C_{txt}; and

writing the resulting C_{txt} into a third one of the I/O storage units.

67. The method according to any of claims 63-66, 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.

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

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

transforming the first C_{txt} into a numeric theoretic transform (NTT) domain;

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

transforming the second C_{txt} into the NTT domain;

multiplying the transformed first C_{txt} with the transformed second C_{txt} to generate a resulting C_{txt}; and

storing the resulting C_{txt} in a third memory unit.

69. A circuit, comprising:

number theoretic transform (NTT) logic including a

high input word path,

a low input word path, and

selection circuitry having a control signal input; wherein

for a first mode of operation,

the selection circuitry is responsive to a first control signal to configure the high input word path and the low input word path into a first logic processing unit; and

wherein for a second mode of operation,

the selection circuitry is responsive to a second control signal to configure the high input word path and the low input word path into a second logic processing unit different than the first logic processing unit.

70. A configurable number theoretic transform (NTT) butterfly circuit, comprising:

a high input word path;

a low input word path;

cross-coupling logic responsive to a first mode control signal to configure the high and low input word paths for carrying out NTT transformation operations, wherein a given NTT transformation operation involves an initial NTT step followed by $\log_2(n)-1$ stages of evaluation by the NTT butterfly circuit, where "n" represents a degree of a polynomial associated with the coefficient values; and

wherein the cross-coupling logic is responsive to a second mode control signal to configure the high input word path and the low input word path into a second logic processing unit different than the first logic processing unit.

71. A method of operation for a number theoretic transform (NTT) butterfly circuit including a high input word path, a low input word path, and selection circuitry having a control signal input, the method comprising:

for a first mode of operation,

configuring the high input word path and the low input word path into a first logic processing unit in response to the selection circuitry receiving a first control signal; and

for a second mode of operation,

configuring the high input word path and the low input word path into a second logic processing unit different than the first logic processing unit, the configuring carried out by the selection circuitry in response to receiving a second control signal different than the first control signal.

72. A method of operating a number theoretic transform (NTT) butterfly circuit, comprising:

enabling a high input word path;

enabling a low input word path;

cross-coupling the high and low input word paths in response to a first mode control signal to configure the high and low input word paths for carrying out NTT transformation operations in a first mode, wherein a given NTT transformation operation involves an initial NTT step followed by $\log_2(n)$-1 stages of evaluation by the NTT butterfly circuit, where "n" represents a degree of a polynomial associated with the coefficient values; and

reconfiguring the high and low input word paths into a second logic processing unit for use during a second mode, the second logic processing unit different than the first logic processing unit, the reconfiguring carried out in response to a second mode control signal.