CLAIMS

1. A computer system for executing a machine instruction in a central processing unit, the computer system comprising:

a memory; and

a processor in communications with the memory, wherein the computer system is configured to perform a method, said method comprising:

obtaining, by a processor, a machine instruction for execution, the machine instruction being defined for computer execution according to a computer architecture, the machine instruction comprising:

at least one opcode field to provide an opcode, the opcode identifying a Vector Galois Field Multiply Sum and Accumulate operation;

a first register field;

a second register field;

a third register field;

a fourth register field; and

an extension field to be used in designating one or more registers, and wherein the first register field is combined with a first portion of the extension field to designate a first register, the second register field is combined with a second portion of the extension field to designate a second register, the third register field is combined with a third portion of the extension field to designate a third register and the fourth register field is combined with a fourth portion of the extension field to designate a fourth register,

wherein the first register comprises a first operand, the second register comprises a second operand, the third register comprises a third operand, and the fourth register comprises a fourth operand; and

executing the machine instruction, the executing comprising:

multiplying one or more elements of the second operand with one or more elements of the third operand using carryless multiplication to obtain a plurality of products;

performing a first mathematical operation on the plurality of products to obtain a first result;

performing a second mathematical operation on the first result and one or more selected elements of the fourth operand to obtain a second result; and

placing the second result in the first operand.

2. The computer system of claim 1, wherein the multiplying comprises multiplying each element of the second operand with the corresponding element of the third operand using carryless multiplication resulting in even-odd pairs of double element-sized products.

3. The computer system of claim 2, wherein the first mathematical operation comprises an exclusive OR operation, and wherein the even-odd pairs of double element-sized products are exclusive ORed with each other to obtain the first result.

4. The computer system of claim 3, wherein the second mathematical operation comprises an exclusive OR operation, and wherein the first result is exclusive ORed with a corresponding double-wide element of the fourth operand to obtain the second result.

5. The computer system of claim 1, wherein the machine instruction further comprises a mask field to specify a size of elements of one or more of the first operand, the second operand, the third operand or the fourth operand of the machine instruction.

6. The computer system of claim 5, wherein the mask field specifies the size of the elements of the second operand and the third operand of the machine instruction, and wherein the size of the elements of the first operand and the fourth operand are double the size of the elements of the second operand and the third operand.

7. A method for executing a machine instruction in a central processing unit, the method comprising:

obtaining, by a processor, a machine instruction for execution, the machine instruction being defined for computer execution according to a computer architecture, the machine instruction comprising:

at least one opcode field to provide an opcode, the opcode identifying a Vector Galois Field Multiply Sum and Accumulate operation;

a first register field;

a second register field;

a third register field;

a fourth register field; and

an extension field to be used in designating one or more registers, and wherein the first register field is combined with a first portion of the extension field to designate a first register, the second register field is combined with a second portion of the extension field to designate a second register, the third register field is combined with a third portion of the extension field to designate a third register and the fourth register field is combined with a fourth portion of the extension field to designate a fourth register,

wherein the first register comprises a first operand, the second register comprises a second operand, the third register comprises a third operand, and the fourth register comprises a fourth operand; and

executing the machine instruction, the executing comprising:

multiplying one or more elements of the second operand with one or more elements of the third operand using carryless multiplication to obtain a plurality of products;

performing a first mathematical operation on the plurality of products to obtain a first result;

performing a second mathematical operation on the first result and one or more selected elements of the fourth operand to obtain a second result; and

placing the second result in the first operand.

8. The method of claim 7, wherein the machine instruction further comprises a mask field to specify a size of elements of one or more of the first operand, the second operand, the third operand or the fourth operand of the machine instruction.

9. A computer program product for executing a machine instruction in a central processing unit, the computer program product comprising:

a computer readable storage medium readable by a processing circuit and storing instructions for execution by the processing circuit for performing a method comprising: obtaining, by a processor, a machine instruction for execution, the machine instruction being defined for computer execution according to a computer architecture, the machine instruction comprising:

at least one opcode field to provide an opcode, the opcode identifying a Vector Galois Field Multiply Sum and Accumulate operation;

a first register field;

a second register field;

a third register field;

a fourth register field; and

an extension field to be used in designating one or more registers, and wherein the first register field is combined with a first portion of the extension field to designate a first register, the second register field is combined with a second portion of the extension field to designate a second register, the third register field is combined with a third portion of the extension field to designate a third register and the fourth register field is combined with a fourth portion of the extension field to designate a fourth register,

wherein the first register comprises a first operand, the second register comprises a second operand, the third register comprises a third operand, and the fourth register comprises a fourth operand; and

executing the machine instruction, the executing comprising:

multiplying one or more elements of the second operand with one or more elements of the third operand using carryless multiplication to obtain a plurality of products;

performing a first mathematical operation on the plurality of products to obtain a first result;

performing a second mathematical operation on the first result and one or more selected elements of the fourth operand to obtain a second result; and

placing the second result in the first operand.

10. The computer program product of claim 9, wherein the multiplying comprises multiplying each element of the second operand with the corresponding element of the third operand using carryless multiplication resulting in even-odd pairs of double element-sized products.

11. The computer program product of claim 10, wherein the carryless multiplication has an order of two.

12. The computer program product of claim 10, wherein the first mathematical operation comprises an exclusive OR operation, and wherein the even-odd pairs of double element-sized products are exclusive ORed with each other to obtain the first result.

13. The computer program product of claim 12, wherein the second mathematical operation comprises an exclusive OR operation, and wherein the first result is exclusive ORed with a corresponding double-wide element of the fourth operand to obtain the second result.

14. The computer program product of claim 13, wherein the placing comprises placing the second result in a double-wide element of the first operand.

15. The computer program product of claim 9, wherein the machine instruction further comprises a mask field to specify a size of elements of one or more of the first operand, the second operand, the third operand or the fourth operand of the machine instruction.

16. The computer program product of claim 15, wherein the mask field specifies the size of the elements of the second operand and the third operand of the machine instruction.

17. The computer program product of claim 16, wherein the size of the elements of the first operand and the fourth operand are double the size of the elements of the second operand and the third operand.