CLAIMS

What is claimed is:

1. A computer-implemented method of facilitating processing within a computing environment, the computer-implemented method characterised as comprising:

obtaining (500) an instruction to provide an output to be used in a cryptographic operation, the instruction being a single architected instruction (502), the single architected instruction using a register to provide a function code (306) of a scalar multiply function to be performed by the instruction of a plurality of scalar multiply functions supported by the instruction, each scalar multiply function of the plurality of scalar multiply functions supported by the instruction having a corresponding function code, and the plurality of scalar multiply functions supported by the instruction including a plurality of elliptic-curve digital signature algorithm functions for a plurality of primes, and a plurality of Edwards-curve digital signature algorithm functions for a plurality of primes; and

executing the instruction (504), the executing comprising:

determining (506), using the register, the function code of the scalar multiply function to be performed of the plurality of scalar multiply functions supported by the instruction;

obtaining input (508) for the scalar multiply function to be performed, the input comprising at least one source component and a scalar value; and

performing the scalar multiply function (510) using the input to provide an output to be used in a cryptographic operation.

2. The method of claim 1, wherein the performing the scalar multiply function comprises performing (514) scalar multiplication of a point on an elliptic curve, the point specified by the at least one source component.

3. The method of claim 2, wherein the point on the elliptic curve is specified by a first source component of the at least one source component and a second source component of the at least one source component, and wherein the first source component and the second source component are input to the instruction via a parameter block located using a register associated with the instruction (516).

4. The method of either of claims 2 or 3, wherein the performing the scalar multiply function comprises performing (518) a series of point additions and point doublings along the elliptic curve.

5. The method of any of the preceding claims, wherein the performing (520) the scalar multiply function comprises using the following equation: (Xr, Yr) < = d * (Xs, Ys), wherein Xs and Ys are the at least one source component and are coordinates of a point on an elliptic curve, d is the scalar value, * is scalar multiply, and Xr and Yr are resulting coordinates of the scalar multiply function, the resulting coordinates being the output.

6. The method of claim 5, wherein the d comprises a plurality of bits which are scanned from one bit to another bit (522).

7. The method of claim 6, wherein the one bit is a most significant bit of d and the other bit is a least significant bit of d (524).

8. The method of either of claims 6 or 7, wherein the performing the scalar multiply function further comprises for a bit of the plurality of bits of d equal to a select value, a point addition occurs, and after each bit is scanned, a point doubling occurs.

9. A computer system for facilitating processing within a computing environment, the computer system comprising:

a memory (104); and

a processor (102) coupled to the memory, wherein the computer system is configured to perform a method comprising:

obtaining an instruction to provide an output to be used in a cryptographic operation, the instruction being a single architected instruction, the single architected instruction using a register to provide a function code of a scalar multiply function to be performed by the instruction of a plurality of scalar multiply functions supported by the instruction, each scalar multiply function of the plurality of scalar multiply functions supported by the instruction having a corresponding function code, and the plurality of scalar multiply functions supported by the instruction including a plurality of elliptic-curve digital signature algorithm functions for a plurality of primes, and a plurality of Edwards-curve digital signature algorithm functions for a plurality of primes; and

executing the instruction, the executing comprising:

determining, using the register, the function code of the scalar multiply function to be performed of the plurality of scalar multiply functions supported by the instruction;

obtaining input for the scalar multiply function to be performed, the input comprising at least one source component and a scalar value; and

performing the scalar multiply function using the input to provide an output to be used in a cryptographic operation.

10. The computer system of claim 9, wherein the performing the scalar multiply function comprises performing scalar multiplication of a point on an elliptic curve, the point specified by the at least one source component.

11. The computer system of claim 10, wherein the point on the elliptic curve is specified by a first source component of the at least one source component and a second source component of the at least one source component, and wherein the first source component and the second source component are input to the instruction via a parameter block located using a register associated with the instruction.

12. The computer system of either of claims 10 or 11, wherein the performing the scalar multiply function comprises performing a series of point additions and point doublings along the elliptic curve.

13. The computer system of claim 9, wherein the performing the scalar multiply function comprises using the following equation: (Xr, Yr) < = d * (Xs, Ys), wherein Xs and Ys are the at least one source component and are coordinates of a point on an elliptic curve, d is the scalar value, * is scalar multiply, and Xr and Yr are resulting coordinates of the scalar multiply function, the resulting coordinates being the output.

14. The computer system of claim 13, wherein the d comprises a plurality of bits which are scanned from one bit to another bit.

15. The computer system of claim 14, wherein the one bit is a most significant bit of d and the other bit is a least significant bit of d.

16. The computer system of either of claims 14 or 15, wherein the performing the scalar multiply function further comprises for a bit of the plurality of bits of d equal to a select value, a point addition occurs, and after each bit is scanned, a point doubling occurs.

17. A computer program product for facilitating processing within a computing environment, 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 according to any of claims 1 to 8.

18. A computer program stored on a computer readable medium and loadable into the internal memory of a digital computer, comprising software code portions, when said program is run on a computer, for performing the method of any of claims 1 to 8.