

CLAIMS

1. A computer program product for facilitating processing in 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 comprising:

obtaining an instruction to perform a plurality of operations, including ciphering and authentication; and

executing the instruction, the executing including:

ciphering one set of data provided by the instruction to obtain ciphered data;

placing the ciphered data in a designated location;

authenticating an additional set of data provided by the instruction, the authenticating generating at least a part of a message authentication tag; and

storing the at least a part of the message authentication tag in a selected location.

2. The computer program product of claim 1, wherein the executing further comprises authenticating the ciphered data.

3. The computer program product of claim 1, wherein the additional set of data includes at least one block of data of one or more blocks of data, and wherein the executing further includes:

determining whether the additional set of data includes a last block of data to be authenticated; and

performing the authenticating based on whether the additional set of data includes the last block of data to be authenticated.

4. The computer program product of claim 3, wherein the determining comprises checking a last additional authenticated data control of the instruction to determine whether the additional set of data includes the last block of data to be authenticated.

5. The computer program product of claim 1, wherein the one set of data includes at least one block of data of one or more blocks of data, and wherein the executing further includes:

determining whether the one set of data includes a last block of data to be ciphered;
and

performing the ciphering based on whether the one set of data includes the last block of data to be ciphered.

6. The computer program product of claim 5, wherein the determining comprises checking a last text control of the instruction to determine whether the one set of data includes the last block of data to be ciphered.

7. The computer program product of claim 1, wherein the ciphering includes encrypting the one set of data based on a control provided by the instruction being set to a selected value.

8. The computer program product of claim 1, wherein the ciphering includes decrypting the one set of data based on a control provided by the instruction being set to a particular value.

9. The computer program product of claim 1, wherein the authenticating of the additional set of data includes using a hash technique to generate the at least a part of the message authentication tag.

10. The computer program product of claim 9, wherein the hash technique uses a hash subkey stored in a parameter block used by the instruction, based on a hash subkey supplied control of the instruction being set to a chosen value.

11. The computer program product of claim 1, wherein the one set of data includes at least a portion of a message and the additional set of data includes routing information for the message.

12. A computer system for facilitating processing in a computing environment, the computer system comprising:

a memory; and

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

obtaining an instruction to perform a plurality of operations, including ciphering and authentication; and

executing the instruction, the executing including:

ciphering one set of data provided by the instruction to obtain ciphered data;

placing the ciphered data in a designated location;

authenticating an additional set of data provided by the instruction, the authenticating generating at least a part of a message authentication tag; and

storing the at least a part of the message authentication tag in a selected location.

13. The computer system of claim 12, wherein the executing further comprises authenticating the ciphered data.

14. The computer system of claim 12, wherein the additional set of data includes at least one block of data of one or more blocks of data, and wherein the executing further includes:

determining whether the additional set of data includes a last block of data to be authenticated, the determining checking a last additional authenticated data control of the instruction to determine whether the additional set of data includes the last block of data to be authenticated; and

performing the authenticating based on whether the additional set of data includes the last block of data to be authenticated.

15. The computer system of claim 12, wherein the one set of data includes at least one block of data of one or more blocks of data, and wherein the executing further includes:

determining whether the one set of data includes a last block of data to be ciphered, the determining checking a last text control of the instruction to determine whether the one set of data includes the last block of data to be ciphered; and

performing the ciphering based on whether the one set of data includes the last block of data to be ciphered.

16. The computer system of claim 12, wherein the authenticating of the additional set of data includes using a hash technique to generate the at least a part of the message authentication tag, and wherein the hash technique uses a hash subkey stored in a parameter block used by the instruction, based on a hash subkey supplied control of the instruction being set to a chosen value.

17. A computer-implemented method of facilitating processing in a computing environment, the computer-implemented method comprising:

- obtaining, by a processor, an instruction to perform a plurality of operations, including ciphering and authentication; and

- executing the instruction, the executing including:

- ciphering one set of data provided by the instruction to obtain ciphered data;

- placing the ciphered data in a designated location;

- authenticating an additional set of data provided by the instruction, the

- authenticating generating at least a part of a message authentication tag; and

- storing the at least a part of the message authentication tag in a selected location.

18. The computer-implemented method of claim 17, wherein the executing further comprises authenticating the ciphered data.

19. The computer-implemented method of claim 17, wherein the additional set of data includes at least one block of data of one or more blocks of data, and wherein the executing further includes:

- determining whether the additional set of data includes a last block of data to be authenticated, the determining checking a last additional authenticated data control of the instruction to determine whether the additional set of data includes the last block of data to be authenticated; and

- performing the authenticating based on whether the additional set of data includes the last block of data to be authenticated.

20. The computer-implemented method of claim 17, wherein the one set of data includes at least one block of data of one or more blocks of data, and wherein the executing further includes:

- determining whether the one set of data includes a last block of data to be ciphered, the determining checking a last text control of the instruction to determine whether the one set of data includes the last block of data to be ciphered; and

- performing the ciphering based on whether the one set of data includes the last block of data to be ciphered.