

CLAIMS

1. An apparatus comprising:
 - 5 a key scheduler, the key scheduler to generate a round key for an aes round associated with an aes round key operation based on a received key and
aes round logic to perform one of a plurality of aes round operations to
compute a result of an aes operation on an input to the aes round and the round key
for the aes round to provide a next input to a next aes round or the result of the aes
10 operation.
 2. The apparatus of claim 1, wherein the round key is stored in a data cache.

 3. The apparatus of claim 2, wherein the key scheduler to pre-compute all round keys
15 for the aes operation and to store all round keys in the data cache prior to starting
the aes operation and the aes round logic to perform each aes round operation
using the pre-computed round keys stored in the data cache.
 4. The apparatus of claim 2, wherein an aes round operation to cause the execution
20 unit to:
perform an exclusive OR (XOR) operation on an input to the round and the
round key for the aes round to produce an intermediate value;
perform a substitution operation for each byte in the intermediate value
based on values stored in a lookup table; and
25 pass results of the substitution operation through a bit-linear transform that
shifts rows in the intermediate value.
 5. The apparatus of claim 1, wherein an aes round operation for a number of aes
rounds -1 to cause the execution unit to:
30 perform an exclusive OR (XOR) operation on the input to the aes round
and the round key for the aes round to produce an intermediate value;
perform a substitution operation for each byte in the intermediate value
based on values stored in a lookup table;

pass results of the substitution operation through a bit-linear transform that shifts rows in the intermediate value; and

pass results of the substitution operation through bit linear transform that mixes columns in the intermediate value.

5

6. The apparatus of claim 5, wherein an aes round operation for a last round to cause the execution unit to:

perform an exclusive OR (XOR) operation on an input to the round and the round key for the aes round to produce an intermediate value;

10

perform a substitution operation for each byte in the intermediate value based on values stored in a lookup table; and

pass results of the substitution operation through a bit-linear transform that shifts rows in the intermediate value.

15

7. The apparatus of claim 1, wherein the result is an encrypted value.

8. The apparatus of claim 1, wherein the result is a decrypted value.

20

9. The apparatus of claim 1, wherein the key and the input for the first aes round are stored in a register file.

10. The apparatus of claim 9, wherein the register file includes a plurality of 128-bit registers.

25

11. A method comprising:

generating a round key for an aes round associated with an aes round key operation based on a received key;

performing the aes round operation on an input to the aes round and the round key for the aes round to provide a next input to a next aes round or the result of the aes operation.

30

12. The method of claim 11, further comprising:

storing the generated round key in a data cache

13. The method of claim 11, wherein generating the round key further comprising:
pre-computing all round keys for the aes operation;
storing all round keys in the data cache prior to starting the aes operation;
5 and
performing each aes round operation using the pre-computed round keys
stored in the data cache.

14. The method of claim 13, wherein performing the aes round operation comprises:
10 performing an exclusive OR (XOR) operation on an input to the round and
the round key for the aes round to produce an intermediate value;
performing a substitution operation for each byte in the intermediate value
based on values stored in a lookup table; and
passing results of the substitution operation through a bit-linear transform
15 that shifts rows in the intermediate value.

15. The method of claim 11, wherein performing the aes round operation for the
number of rounds-1 comprises:
performing an exclusive OR (XOR) operation on the input to the aes round
20 and the round key for the aes round to produce an intermediate value;
performing a substitution operation for each byte in the intermediate value
based on values stored in a lookup table;
passing results of the substitution operation through a bit-linear transform
that shifts rows in the intermediate value; and
25 passing results of the substitution operation through bit linear transform
that mixes columns in the intermediate value.

16. The method of claim 14, wherein performing the aes round operation for a last aes
round comprises:
30 performing an exclusive OR (XOR) operation on an input to the round and
the round key for the aes round to produce an intermediate value;
performing a substitution operation for each byte in the intermediate value
based on values stored in a lookup table; and

passing results of the substitution operation through a bit-linear transform that shifts rows in the intermediate value.

17. The method of claim 11, wherein the result is an encrypted value.

18. The method of claim 11, wherein the result is a decrypted value.

19. The method of claim 11, wherein the key and the input for a first aes round are stored in a register file.

20. The method of claim 20, wherein the register file includes a plurality of 128-bit registers.

21. An article including a machine-accessible medium having associated information, wherein the information, when accessed, results in a machine performing:

generating a round key for an aes round associated with an aes round key operation based on a received key; and

performing the aes round operation on an input to the aes round and the round key for the aes round to provide a next input to a next aes round or the result of the aes operation.

22. The article of claim 21, further comprising:

storing the generated round key in a data cache

23. The article of claim 21, wherein if the number of aes rounds is equal to 1, prior to performing the sequence of aes round operations, loading a pre-computed round key for the aes round based on the key.

24. A system comprising:

a dynamic random access memory to store data and instructions; and

a processor coupled to said memory to execute the instructions, the processor comprising:

a key scheduler, the key scheduler to generate a round key for an aes round associated with an aes round key operation based on a received key; and

aes round logic to perform one of a plurality of aes round operations to compute a result of an aes operation on an input to the aes round and the round key for the aes round to provide a next input to a next aes round or the result of the aes operation.

25. The system of claim 24, wherein the round key is stored in a data cache.

10 26. The system of claim 24, wherein the key scheduler to pre-compute all round keys for the aes operation and to store all round keys in the data cache prior to starting the aes operation and the aes round logic to perform each aes round operation using the pre-computed round keys stored in the data.

15

CLAIMS

[Claim 1]

A processor comprising:

a decode unit to receive a first instruction to perform an Advanced Encryption Standard (AES) round of an AES algorithm and a second instruction to generate a round key for the AES round, the first instruction to have a source operand that is to include input data for the AES round, and the first instruction to have a source operand that is to include the round key for the AES round and the second instruction to have a source operand that is to include a previous round key for a previous AES round;

a key scheduler, in response to the second instruction, to generate the round key for the AES round based on the previous round key; and

an execution unit coupled with the decode unit, the execution unit, in response to the first instruction, to store a result in a destination of the first instruction, the result to include the input data transformed by the AES round using the round key.

[Claim 2]

The processor of claim 1, wherein

the first instruction is to perform an AES encryption round.

[Claim 3]

The processor of claim 1, wherein

the first instruction is to perform an AES decryption round.

[Claim 4]

The processor of claim 1, wherein

the source operand that is to include the input data is stored in a register, and wherein

the source operand that is to include the round key is stored in a register.

[Claim 5]

The processor of claim 4, wherein

the registers comprise 128-bit registers.

[Claim 6]

The processor of any one of claims 1 to 5, wherein

the execution unit, in response to the first instruction, is to overwrite the input data with the result.

[Claim 7]

The processor of claim 1, wherein
the execution unit, in response to the first instruction, is to perform operations comprising:
performing an S-Box lookup;
shifting rows;
mixing columns; and
adding round keys.

[Claim 8]

The processor of claim 1, wherein
the second instruction has an immediate, and wherein
the key scheduler is to generate the round key for the AES round based on the previous round key and the immediate, and wherein
the second instruction has a different opcode from the first instruction.

[Claim 9]

The processor of claim 1, wherein:
the decode unit is to receive a third instruction to perform a last AES round of the AES algorithm, the third instruction to have a source operand that is to include input data for the last AES round, and the third instruction to have a source operand that is to include a last round key for the last AES round; and
the execution unit, in response to the third instruction, to store a second result in a destination of the third instruction, the second result to include the input data for the last AES round transformed by the last AES round using the last round key for the last AES round, wherein the third instruction has a different opcode from the first instruction.

[Claim 10]

The processor any one of claims 1 to 9, wherein
the processor comprises a general-purpose processor.

[Claim 11]

A processor comprising:
a plurality of 128-bit registers;

a decode unit to receive a first instruction to perform an Advanced Encryption Standard (AES) encryption round and a second instruction to generate a round key for the AES encryption round, the first instruction to indicate a first 128-bit register of the plurality that is to include information to be encrypted, and the first instruction to indicate a second 128-bit register of the plurality that is to include the round key for the AES encryption round, and the second instruction to have a source operand that is to include a previous round key for a previous AES encryption round;

a key scheduler, in response to the second instruction, to generate the round key for the AES encryption round based on the previous round key; and

an execution unit coupled with the decode unit and the plurality of 128-bit registers, the execution unit, in response to the first instruction, to store a result in a destination of the first instruction, the result to include the information from the first 128-bit register transformed by the AES encryption round using the round key.

[Claim 12]

The processor of claim 11, wherein

the execution unit, in response to the first instruction, is to perform operations comprising:

performing an S-Box lookup;

shifting rows;

mixing columns; and

adding round keys.

[Claim 13]

The processor of claim 11 or 12, wherein

the processor comprises a general-purpose processor.

[Claim 14]

A processor comprising:

a plurality of 128-bit registers;

a decode unit to receive a first instruction to perform an Advanced Encryption Standard (AES) decryption round and a second instruction to generate a round key for the AES decryption round, the first instruction to indicate a first 128-bit register of the plurality that is to include information to be decrypted, and the first instruction to indicate a second 128-bit register of the plurality that is to include the round key for the AES decryption round, and the second instruction to have a source operand that is to include a previous round key for a previous AES decryption round;

a key scheduler, in response to the second instruction, to generate the round key for the AES decryption round based on the previous round key; and

an execution unit coupled with the decode unit and the plurality of 128-bit registers, the execution unit, in response to the first instruction, to store a result in a destination of the first instruction, the result to include the information from the first 128-bit register transformed by the AES decryption round using the round key.

[Claim 15]

The processor of claim 14, wherein

the processor comprises a general-purpose processor.

[Claim 16]

A processor comprising:

a decode unit to receive an instruction to generate a round key for an Advanced Encryption Standard (AES) round, the instruction to have a source operand that is to include a previous round key for a previous AES round; and

a key scheduler coupled with the decode unit, the key scheduler, in response to the instruction, to store the round key for the AES round in a destination of the instruction.

[Claim 17]

The processor of claim 16, wherein

the instruction has an immediate, and wherein the key scheduler is to generate the round key for the AES round based on the immediate, wherein

the destination comprises a 128-bit register.

[Claim 18]

A processor comprising:

a decode unit to receive and decode a plurality of instructions including at least:

a first instruction to generate a first round key for a first given Advanced Encryption Standard (AES) encryption round, the first instruction to have a first instruction source operand that is to include a key to be used to generate the first round key;

a second instruction to perform a second given AES encryption round, the second instruction to have a second instruction first source operand that is to include input data for the second given AES encryption round, and the second instruction to have a second instruction second source operand that is to include a second round key for the second given AES encryption round; and

a third instruction to perform an AES encryption last round, the third instruction to have a third instruction first source operand that is to include input data for the AES encryption last round, and the third instruction to have a third instruction second source operand that is to include a last round key for the AES encryption last round;

a key scheduler, in response to the first instruction, to generate the first round key for the first given AES encryption round based on the key from the first instruction source operand; and

an execution unit, coupled with the decode unit, the execution unit:

in response to the second instruction, to store a result of the second instruction in a destination of the second instruction, the result of the second instruction to include the input data for the second given AES encryption round transformed by the second given AES encryption round using the second round key; and

in response to the third instruction, to store a result of the third instruction in a destination of the third instruction, the result of the third instruction to include the input data for the AES encryption last round transformed by the AES encryption last round using the last round key.

[Claim 19]

The processor of claim 18, wherein

the first instruction has a first opcode, the second instruction has a second opcode different from the first opcode, and the third instruction has a third opcode different from the first and second opcodes.

[Claim 20]

The processor of claim 18, wherein

the first instruction has an immediate, and wherein

the key scheduler is to generate the first round key based on the immediate.

[Claim 21]

The processor of any one of claims 18 to 20, wherein

the processor comprises a general-purpose processor.