

CLAIMS

1. A method of generating from a main key a sequence of sub-keys for cryptographic operations, wherein each sub-key is defined by respective bit values, the method
5 comprising:
 - operating on the main key with a transformation, wherein the transformation comprises one or more one-way functions and the main key is operated on only once to generate the sub-keys of the sequence, said sub-keys being generated in parallel; and
 - setting the respective bit values of the sub-keys of the sequence using respective
10 bit values of the one or more one-way functions;
 - the method further comprising:
 - using the sub-keys of the sequence as round keys in a block cipher with a key schedule defined by the sequence.
- 15 2. A method according to claim 1, wherein setting the respective bit values comprises setting the respective bit values of at least two of the sub-keys in accordance with respective bit values of one of the one or more one-way functions according to a pre-defined relationship.
- 20 3. A method according to claim 1, wherein setting the respective bit values comprises setting the respective bit values of all the sub-keys of the sequence in accordance with respective bit values of one of the one or more one-way function according to a pre-defined relationship.
- 25 4. A method according to claim 1 or 2, wherein operating on the main key comprises generating a plurality of intermediate outputs and applying a one-way function to each intermediate output to generate a respective one-way output, and wherein the method comprises generating one or more of the sub-keys from each one-way output.
- 30 5. A method according to claim 1, 2 or 4 comprising
 - applying a first sub-function to the main key to generate a first intermediate output;
 - applying a first one-way function to the first intermediate output; and
 - generating a first one or more of the sub-keys of the sequence from an output of the first one-way function, and
 - 35 repeatedly:
 - applying a next sub-function to the previous intermediate output to generate a next intermediate output;

applying a next one-way function to the next intermediate output; and
generating a next one or more of the sub-keys of the sequence from an
output of the next one-way function.

5 6. A method according to claim 1, 2 or 4 comprising
applying an input one-way function to the main key to generate a working key;
applying a plurality of sub-functions to the working key to generate respective
intermediate outputs;
applying an output one-way function to each intermediate output to generate a
10 respective transformation output; and
generating the sub-keys of the sequence from the transformation outputs.

7. A method of generating from a main key related forward and reverse sequences of
sub-keys for use in cryptographic operations, the method comprising:
15 generating sub-keys of the forward sequence by a method according to claim 5,
wherein the next sub-functions are applied in a forward next sub-function
sequence, and
wherein the first sub-function followed by the sub-functions of the forward
next sub-function sequence define a forward sub-function sequence;
20 generating from the main key a reverse sequence of sub-keys in accordance with a
method according to claim 5,
wherein the first sub-function is the composite function of the sub-functions
of the forward sub-function sequence, and
wherein the next sub-functions are applied in a reverse next sub-function
25 sequence and the sub-functions of the reverse next sub-function sequence correspond to
the respective inverse functions of the sub-functions of the forward next sub-functions
sequence in reverse order.

8. A method of decrypting a message encrypted with a block cipher, the block cipher
30 having a key schedule comprising round keys applied in an encryption sequence, the
encryption sequence of round keys being obtainable from a main key by a method according
to claim 5 in which the next sub-functions are applied in an encryption next sub-function
sequence and the first sub-function followed by the sub-functions of the encryption next
sub-function sequence define an encryption sub-function sequence, the method
35 comprising:
generating from the main key a decryption sequence of sub-keys in accordance with
a method according to claim 5,

wherein the first sub-function is the composite function of the sub-functions of the encryption sub-function sequence, and

wherein the next sub-functions are applied in a decryption next sub-function sequence and the sub-functions of the decryption next sub-function sequence correspond to the respective inverse functions of the sub-functions of the encryption next sub-functions sequence in reverse order; and

applying the sub-keys in the order of the decryption sequence to decrypt the message.

9. A method of processing a message with a block cipher having a key schedule, the method comprising:

encrypting a plaintext of the message with the block cipher to generate a cipher text, the encrypting comprising:

generating round keys of the key schedule in an encryption sequence from a main key by a method according to claim 5,

wherein the next sub-functions are applied in an encryption next sub-function sequence, and

the first sub-function followed by the sub-functions of the encryption next sub-function sequence define an encryption sub-function sequence;

encrypting the plaintext with a first one of the round keys in the encryption sequence to generate a first round text; and

for the remaining round keys in the encryption sequence, encrypting a previous round text with a next round key in the encryption sequence to generate a next round text, wherein the last round text is the cipher text; and

decrypting the cipher text to generate the plaintext, the decrypting comprising:

generating from the main key a decryption sequence of sub-keys in accordance with a method according to claim 5,

wherein the first sub-function is the composite function of the sub-functions of the encryption sub-function sequence, and

wherein the next sub-functions are applied in a decryption next sub-function sequence and the sub-functions of the decryption next sub-function sequence correspond to the respective inverse functions of the sub-functions of the encryption next sub-functions sequence in reverse order; and

decrypting the cipher text with a first one of the round keys in the decryption sequence to generate a first round text; and

for the remaining round keys in the decryption sequence, decrypting a previous round text with a next round key in the decryption sequence to generate a next round text, wherein the last round text is the plaintext.

- 5 10. A device for generating from a main key a sequence of sub-keys for cryptographic operations, wherein each sub-key is defined by respective bit values, the device comprising a memory for storing the main and at least one sub-key and a processor configured to:
- operate on the main key with a transformation, wherein the transformation comprises one or more one-way functions and the main key is operated on only once to
- 10 generate the sub-keys of the sequence, said sub-keys being generated in parallel; and
- set the respective bit values of the sub-keys of the sequence using respective bit values of the one or more one-way functions; and
- use the sub-keys of the sequence as round keys in a block cipher with a key schedule defined by the sequence.
- 15
11. A device according to claim 10, wherein the processor is configured to implement a method according to any one of claims 2 to 9.
12. A device for processing a message with a block cipher having a key schedule, the
- 20 device comprising a memory for storing a main key and at least one sub-key and a processor configured to:
- encrypt a plaintext of the message with the block cipher to generate a cipher text, the encrypting comprising:
- generating round keys of the key schedule in an encryption sequence from
- 25 a main key by a method as claimed in claim 5,
- wherein the next sub-functions are applied in an encryption next sub-function sequence, and
- the first sub-function followed by the sub-functions of the encryption next sub-function sequence define an encryption sub-function sequence;
- 30 encrypting the plaintext with a first one of the round keys in the encryption sequence to generate a first round text; and
- for the remaining round keys in the encryption sequence, encrypting a previous round text with a next round key in the encryption sequence to generate a next round text, wherein the last round text is the cipher text; and
- 35 decrypt the cipher text to generate the plaintext, the decrypting comprising:
- generating from the main key a decryption sequence of sub-keys in accordance with a method as claimed in claim 5,

wherein the first sub-function is the composite function of the sub-functions of the encryption sub-function sequence, and

5 wherein the next sub-functions are applied in a decryption next sub-function sequence and the sub-functions of the decryption next sub-function sequence correspond to the respective inverse functions of the sub-functions of the encryption next sub-functions sequence in reverse order; and

decrypting the cipher text with a first one of the round keys in the decryption sequence to generate a first round text; and

10 for the remaining round keys in the decryption sequence, decrypting a previous round text with a next round key in the decryption sequence to generate a next round text, wherein the last round text is the plaintext.

13. A computer program product comprising coded instructions that, when run on a processing device, implement a method according to any one of claims 1 to 9.
15

14. One or more computer readable media or a memory device storing coded instructions that, when run on a processing device, implement a method according to any one of claims 1 to 9.