

WHAT IS CLAIMED IS:

1. A method for generating one or more round keys for a cryptographic operation, the method comprising:
 - obtaining one or more first inputs (1105) and one or more second inputs (1105);
 - performing (1110), by at least one electronic circuit, a bit-mixer operation (500, 600, 700, 1000) on each of the one or more first inputs and the one or more second inputs; and
 - generating (1115), by at least one electronic circuit, one or more round keys based on the performing, wherein the one or more first inputs (1105) comprise a plurality of equal sized subkeys from a key material that is divided into a plurality of equal sized key material sub-blocks or a cipher key.
2. The method of claim 1, wherein the one or more second inputs (1105) comprise randomly generated fixed data, one or more previous round keys, or a round number.
3. The method of claim 1, further comprising generating the one or more first inputs from a shorter key by applying a cryptographic function, a bit-mixer with hard coded key material, a counter input, or combinations thereof.
4. The method of claim 3, wherein the cryptographic function comprises a cipher, a hash function, or a stream generator.
5. The method of any one of claims 1-2, wherein the key material is secret and shared between communicating parties, hardcoded, or randomly generated.
6. The method of any one of claims 1, 2, or 5, wherein the cipher key is combined with hardcoded key material by exclusive-OR “XOR” operation on portions of the cipher key with portions of the key material.
7. The method of any one of claims 1-2, further comprising selecting the bit-mixer, wherein the bit-mixer operation has the properties comprising every input bit affects every output bit, changes in the input bit cause, on average, half of output bits to change; changes in the input bits

yield output values without correlation to the input bits or to a change pattern of the input, keys are employed to make their behavior unpredictable to an observer not knowing the keys, and fixed lengths of the input bits and output values can be independently and arbitrarily chosen.

8. The method of any one of claims 1, 2, or 7, wherein the generating by an XOR tree (1000) further comprising performing a scrambling operation on an output of the performing.

9. The method of any one of claims 1, 2, 7, or 8, further comprising producing a block of data with the one or more previously generated round keys.

10. The method of any one of claims 1, 2, 7, 8, or 9, further comprising repeating the performing and the generating the one or more round keys for a cryptographic cipher.

11. The method of any one of claims 1, 2, 7, 8, 9, or 10, wherein the bit-mixer operation comprises an exclusive-OR “XOR” tree (1000) comprising a plurality of negated-AND “NAND” gates or a plurality of multiplexers for selecting data to be merged, a substitution-permutation network (700), or a double-mix Feistel network (500, 600), or a Rotate-Add-XOR “RAX” construction.

12. The method of claim 11, wherein the XOR tree (1000) further comprises:
performing a negative-AND “NAND” logical operation on each first input of the one or more first inputs with each second input of the one or more second inputs to select which of the plurality of first inputs to input into an XOR logical operation, wherein an output of the XOR tree produces output with respect to the plurality of first inputs that are used as inputs.

13. The method of claim 12, further comprising performing a scramble operation to the output of the XOR tree to make the bit-mixer function nonlinear.

14. The method of any one of claims 11-12, wherein the substitution-permutation network (700) further comprises:

performing a non-linear substitution operation on each of the plurality of first inputs;

performing a permutation operation on each output of the substitution operation; and
performing a XOR operation on each output of the permutation operation with the one or
the first inputs or one of the second inputs.

15. The method of any one of claims 11, 12, or 14, wherein, in the double-mix Feistel
network (500, 600), each of the one or more first inputs are divided into an initial left half and
initial right half, the method further comprises:

calculating an updated left half and an updated right half for each round of a plurality of
rounds,

wherein the calculating the updated left half comprises applying a first function to an
input left half to produce a first result, and mixing the first result with an input right half, wherein
calculating the updated right half comprises applying a second function to the input left half to
produce a second result, and mixing the second result with a round key, and

wherein the input left half and input right half are the initial left half and initial right half
for a first of the plurality of rounds, and the updated left half and updated right half for an
immediately preceding round for each round thereafter.

16. A system for generating one or more round keys for a cryptographic operation, the
system comprising one or more logic circuits operable to:

obtain one or more first inputs and one or more second inputs (1105);

perform, by at least one electronic circuit, a bit-mixer operation on each of the one or
more first inputs and the one or more second inputs (1110); and

generate, by at least one electronic circuit, one or more round keys based on the
performing (1115), wherein the one or more first inputs (1105) comprise a plurality of equal
sized subkeys from a key material that is divided into a plurality of equal sized key material sub-
blocks or a cipher key.

17. The system of claim 16, wherein the one or more second inputs (1105) comprise a
random input, one or more previous round keys, a round number.

18. The system of any one of claims 16-17, wherein the cryptographic operation comprises a cipher, a hash function, or a stream generator.

19. The system of any one of claims 16-18, wherein the bit-mixer operation comprises an exclusive-OR “XOR” tree (1000), a substitution-permutation network (700), or a double-mix Feistel network (500, 600), or a Rotate-Add-XOR “RAX” construction.