

Claims

1. A method for encrypting data based on all-or-nothing encryption, characterized by the steps of
 - a) Providing data to be encrypted, preferably in form of a plaintext bitstream, and an encryption key, preferably wherein the encryption key may be secret or publicly known,
 - b) Dividing said data into an odd number of blocks, such that each of said blocks has the same size
 - c) Encrypting said blocks, preferably using symmetric encryption, with said encryption key obtaining an intermediate ciphertext comprising the encrypted blocks, and
 - d) Linear transforming the intermediate ciphertext ~~based on additive contravalence operations to~~ using a single matrix multiplication with a vector representing the intermediate ciphertext to obtain a final ciphertext,
wherein after step d) the final ciphertext comprises blocks, wherein each block is represented by the sum of all encrypted blocks of the intermediate ciphertext prior to step d) without the corresponding encrypted block corresponding to the same position in the intermediate ciphertext prior to step d).
2. The method according to claim 1, characterized in that the encryption key is publicly known.
- ~~3. The method according to one of the claims 1-2, characterized in that linear transforming the intermediate ciphertext is performed using a single matrix multiplication with a vector representing the intermediate ciphertext.~~
- ~~43.~~ 43. The method according to claim ~~31~~, characterized in that the matrix is provided invertible and identical to its invertible, preferably wherein the matrix is provided in form of a diagonal matrix having the value 1 on the diagonal and the value 0 otherwise.
- ~~54.~~ 54. The method according to one of the claims ~~3-41-3~~, characterized in that the vector-matrix multiplication is performed using XOR- and AND-operations.

- ~~6.~~ The method according to one of the claims 1-5, characterized in that after step d) the final ciphertext, preferably represented in form of a vector, comprises blocks, wherein each block is represented by the sum of all encrypted blocks of the intermediate ciphertext prior to step d) without the corresponding encrypted block corresponding to the same position in the intermediate ciphertext prior to step d).
75. The method according to one of the claims 1-~~64~~, characterized in that steps c)-d) are performed by
- 7a5a) recursively encrypting each plaintext block of the actual round using the encryption key combined, preferably via an XOR-operation, with an encrypted plaintext block of the round before resulting in corresponding blocks of the intermediate ciphertext,
- 7b5b) directly summing up all intermediate ciphertext blocks according to step 7a5a), and
- 7e5c) generating the blocks of the final ciphertext by directly summing up the result of step 7b5b) and the corresponding block of the intermediate ciphertext.
86. The method according to one of the claims 1-75, characterized in that the blocks of the final ciphertext are distributed among at least two different storage servers, preferably providing at least two different storage services.
97. The method according to claim 86, characterized in that each storage server stores at least two blocks of the final ciphertext.
- ~~108.~~ The method according to one of the claims 1-97, characterized in that random data is added as a block into the intermediate ciphertext, preferably added at the beginning of the intermediate ciphertext.

449. The method according to one of the claims 1-408, characterized in that for performing encryption according to step b) a semantically secure encryption and symmetric encryption scheme is used, preferably counter mode encryption, cipher block chaining mode encryption, output feedback mode encryption and/or cipher feedback mode encryption.
4210. The method according to ~~one of the claims 1-11~~ claim 8, characterized in that even intermediate ciphertext blocks are generated based on an XOR-operation with the corresponding plaintext block and the result of an encryption of ~~the random seed~~ said random data and the respective even number and odd ciphertext blocks are a result of an encryption of the corresponding plaintext block and an XOR-operation with the previously generated even intermediate ciphertext block.
4311. A system for encrypting data based on an all-or-nothing encryption, preferably in form of a computer, one or more processors and/or security modules, preferably for performing with a method according to one of the claims 1-4210, characterized by
an input module operable to provide data to be encrypted, preferably in form of a plaintext bitstream, and an encryption key,
an encryption module operable to divide said data provided by the input module into an odd number of blocks, such that each of said blocks has the same size and to encrypt said blocks, preferably using symmetric encryption, with said encryption key obtaining an intermediate ciphertext comprising the encrypted blocks, and
a transformation module operable to transform linearly the intermediate ciphertext ~~based on additive contravalance operations~~ using a single matrix multiplication with a vector representing the intermediate ciphertext to obtain a final ciphertext,
wherein after said linear transformation the final ciphertext comprises blocks, wherein each block is represented by the sum of all encrypted blocks of the intermediate ciphertext prior to said linear transformation without the corresponding encrypted block corresponding to the same position in the intermediate ciphertext prior to said linear transformation.