(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 June 2016 (02.06.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/082857 A1

(51) International Patent Classification: *H04L 9/06* (2006.01)

(21) International Application Number: PCT/EP2014/075425

(22) International Filing Date: 24 November 2014 (24.11.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: NEC EUROPE LTD. [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventor: KARAME, Ghassan; Ringstraße 3, Heidelberg (DE).

(74) Agent: ULLRICH & NAUMANN; Schneidmühlstraße 21, 69115 Heidelberg (DE).

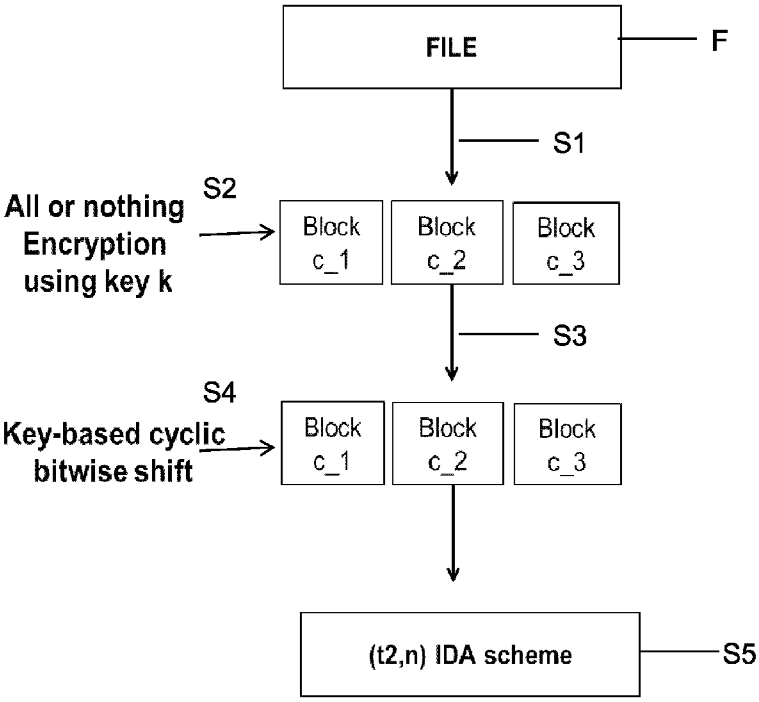
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD FOR ENCRYPTING DATA FOR DISTRIBUTED STORAGE



(57) Abstract: The present invention relates to a method for encrypting data with an encryption entity like a client, etc., comprising the steps of a) Dividing a plaintext into a number of N blocks, b) Encrypting each block with an encryption key resulting in a number of ciphertext blocks, c) Applying a linear All-Or-Nothing scheme on said ciphertext blocks, d) Transforming each outputted ciphertext block of step c) with a transformation procedure such that the information in different ciphertext blocks is transformed differently based on said encryption key and such that the transformation procedure is only revertable with knowledge of said encryption key, and e) Dispersing the transformed ciphertext blocks according to an information dispersal procedure.

# METHOD FOR ENCRYPTING DATA FOR DISTRIBUTED STORAGE

The present invention relates to a method for encrypting data with an encryption entity like a client, etc..

The present invention further relates to a system for encrypting data with an encrypting entity like a client, etc..

Although applicable to security in general the present invention will be described with regard to cloud security.

Cloud security is gaining more and more importance in many applications and services nowadays. One of the important techniques that can be used to strengthen confidentiality of data stored in the cloud is the so-called all-or-nothing encryption. All-or-nothing encryption provides semantic security of data while guaranteeing that the data can only be recovered if and only if all blocks of a ciphertext are available for download by or known to a given client. Therefore all-or-nothing encryption does not solely rely on the secrecy of the encryption key for the data: In order to acquire any meaningful information of the input plaintext it is required that any adversary has access to all the data or blocks of the ciphertext respectively. Therefore all-or-nothing encryption ensures a transparent key management process and naturally complement information dispersal techniques that can be used to efficiently store the data in a distributed storage like cloud storage.

Conventional all-or-nothing encryptions are for example disclosed in the non-patent literature of R. Rivest, “All-or-Nothing Encryption and The Package Transform”, in Proceedings of Fast Software Encryption, pages 210-218, 1997 or in the non-patent literature of Anan Desai, “The Security of All-Or-Nothing Encryption: Protecting Against Exhaustive Key Search”, in Proceedings of CRYPTO, 2000 or in the non-patent literature of Ghassan Karame, Claudio Soriente, Krzysztof Lichota, Srdjan Capkun, “Technical Report”, available from: https://eprint.iacr.org/2014/556.pdf. Such conventional all-or-nothing encryption schemes have the following steps:

- Key generation procedure: On input of a security parameter, the key generation procedure outputs an encryption key K.
- Encryption procedure: On input of a plaintext p which is comprised on m blocks of size l bits each manual input of the encryption key K, the encryption procedure outputs n = m+1 blocks of ciphertext.
- Decryption procedure: On input of the encryption key K and the entire ciphertext blocks a decryption procedure outputs the plaintext blocks p. If all ciphertext blocks are not available, then decryption procedure outputs NULL.

Further conventional linear transformations are for example disclosed in the non-patent literature of D.R. Stinson, "Something About all or Nothing (Transforms)", Designs, Codes and Cryptography, 2001.

One of the problems when outsourcing data of a cloud is, that data confidentiality should be ensured in spite of a curious cloud. Another problem lies in the data availability in spite of a cloud server that can fail.

Conventional methods rely on the one hand on encryption to provide data confidentiality and on the other hand on information dispersal algorithms IDA to disperse the data into a plurality of n chunks such that any t servers can reconstruct the data. Such information dispersal only guarantees data availability in spite of failures but does not necessarily ensure data confidentiality. This means that the shares of the information dispersed by the information dispersal algorithm and which are held by each server still leak considerable information about the original plaintext.

To address this problem so-called ramp schemes have been proposed. Such ramp schemes usually have two thresholds t1 and t2 out of n shares of data. The threshold t2 is the so-called standard reconstruction threshold which ensures data reconstructability from any t2 shares out of said n shares. The threshold t1 is the maximum number of shares that do not leak any information about the input or plaintext data. Thus, t1 is smaller than t2. Conventional information dispersal algorithm schemes are (0,t2, n) ramp schemes, since any share leaks information about the input data and therefore the threshold t1 = 0.

Conventionally such ramp schemes are constructed, for example by transforming specific information dispersal algorithm schemes, such as the Reed Solomon code to ramp schemes which is for example disclosed in the non-patent literature of H. Koga, S. Honjo, "A secret sharing scheme based on a systematic Reed-Solomon code and analysis of its security for a general class of sources", in IEEE Symposium on Information Theory, 2014 and of McEliece, R. J. and Sarwate, D. V., "On Sharing Secrets and Reed-Solomon Codes", Communication of the ACM Sept. 1981.

Other conventional constructions of ramp schemes cannot be deployed or are very difficult to deploy in practice, see for example the conventional ramp schemes as disclosed in the non-patent literature of G. R. Blakley, Catherine Meadows, "Security of Ramp Schemes", Advances in Cryptology, 1985 and of Maura B. Paterson, Douglas R. Stinson, "A simple combinatorial treatment of constructions and threshold gaps of ramp schemes". Other conventional methods are disclosed in the already above-mentioned non-patent literature of H. Koga, S. Honjo, "A secret sharing scheme based on a systematic Reed-Solomon code and analysis of its security for a general class of sources", in IEEE Symposium on InformationTheory, 2014 and make or need specific assumptions about the input data.

It is therefore an objective of the present invention to provide a method and a system for encrypting data with an encryption entity enabling a more secure ramp scheme.

It is a further objective of the present invention to provide a method and a system for encrypting data with an encrypting entity which keep the confidentiality properties of a ramp scheme, even if encryption information like an encryption key is leaked to an adversary.

It is an even further objective of the present invention to provide a method and a system for encrypting data with an encryption entity like a client enabling an efficient performance.

The aforementioned objectives are accomplished by a method of claim 1 and a system of claim 10.

In claim 1 a method for encrypting data with an encryption entity like a client, etc. is defined.

According to claim 1 the method is characterized by the steps of

a) Dividing a plaintext into a number of N blocks,

b) Encrypting each block with an encryption key resulting in a number of ciphertext blocks,

c) Applying a linear All-Or-Nothing scheme on said ciphertext blocks,

d) Transforming each outputted ciphertext block of step c) with a transformation procedure such that the information in different ciphertext blocks is transformed differently based on said encryption key and such that the transformation procedure is only revertable with knowledge of said encryption key, and

e) Dispersing the transformed ciphertext blocks according to an information dispersal procedure.

In claim 10 a system for encrypting data with an encryption entity like a client, etc. is defined.

According to claim 10 the system is characterized by one or more encryption entities like clients, adapted to or adapted to cooperate with each other to perform the steps of

a) Dividing a plaintext into a number of N blocks,

b) Encrypting each block with an encryption key resulting in a number of ciphertext blocks,

c) Applying a linear All-Or-Nothing scheme on said ciphertext blocks,

d) Transforming each outputted ciphertext block of step c) with a transformation procedure such that the information in different ciphertext blocks is transformed differently based on said encryption key and such that the transformation procedure is only revertable with knowledge of said encryption key, and

e) Dispersing the transformed ciphertext blocks according to an information dispersal procedure.

According to the invention it has been recognized that a secure ramp scheme which can use any information dispersal algorithm scheme is provided.

According to the invention it has been further recognized that only a small performance "penalty" compared with a conventional ramp scheme is present although security is enhanced.

According to the invention it has been even further recognized that the ramp scheme functionality is preserved even with the encryption key is leaked to an adversary.

According to the invention it has been even further recognized that the present invention provides a secure way to ensure file access revocation even if the owner has been revoked access and still retains access to the encryption key and to parts of the ciphertext blocks. In this case the present invention ensures that the revoked user cannot acquire any meaningful bit of information about the original file.

According to the invention it has been further recognized that linear transforms or schemes are much faster than an encryption round for instance.

According to the invention it has been even further recognized that a linear all-or-nothing transformation when compassed with an information dispersal algorithm is not secure. Since an information dispersal algorithm might entail linear operations then a linear all-or-nothing transform together with an information dispersal algorithm might still partially leak information about the input plaintext.

In other words the present invention comprises the steps of encrypt the data into n ciphertext blocks using an encryption key K, then apply an all-or-nothing scheme on the encrypted data, use a function based on key K to transform the bits of each ciphertext block in such a way that the function cannot be reverted without knowledge of the encryption key K in such that bits in different blocks are transformed independently at least in the computational sense. Finally any (t2, n) information dispersal algorithm scheme is applied resulting in a (t2, t2, n) ramp scheme keeping the ramp scheme properties even if the encryption key K is given or leaked to an adversary.

Further features, advantages and preferred embodiments are described in the following subclaims:

According to a preferred embodiment the linear all-or-nothing scheme is performed by applying a matrix multiplication with a matrix, wherein the matrix elements on the diagonal are 0 and all other matrix elements are 1. This enables to provide a linear all-or-nothing transformation scheme in an easy and efficient way.

According to a further preferred embodiment the matrix multiplication is performed by XOR- and AND-operations. This enables an efficient computation of the multiplication and addition operations of the matrix-multiplication.

According to a further preferred embodiment the transformation procedure performs a keyed bit permutation per ciphertext block using the index of the corresponding ciphertext block as additional random information. This enables an efficient transformation in particular in terms of security and performance.

According to a further preferred embodiment the transformation procedure performs a keyed block cipher encryption per ciphertext block using the index of the corresponding ciphertext block as additional random information. This provides an alternative transformation procedure which can also be efficiently performed.

According to a further preferred embodiment the transformation procedure performs a cyclic bitwise operation, preferably per ciphertext block. This enables that bitwise shifting can be executed in small clock cycles and is as such a fast operation.

According to a further preferred embodiment the cyclic bitwise shifting per ciphertext block is performed using a trapdoor function with input of the encryption key and index of the respective ciphertext block, preferably by using the trapdoor function modulo the size of the corresponding ciphertext block. This enables in an easy and efficient way to provide a cyclic bitwise shifting.

According to a further preferred embodiment the cyclic bitwise shifting is performed on all ciphertext blocks simultaneously using a function, preferably a one way cryptographic function, with input of the encryption key and modulo the size of all ciphertext blocks. This allows an even faster execution of the transformation procedure and enhances the security.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end it is to be referred to the patent claims subordinate to patent claim 1 on the one hand and to the following explanation of preferred embodiments of the invention by way of example, illustrated by the figure on the other hand. In connection with the explanation of the preferred embodiments of the invention by the aid of the figure, generally preferred embodiments and further developments of the teaching will be explained.

In the drawing the only

Figure shows a part of a method according to a first embodiment of the present invention.

The only figure shows a part of a method according to a first embodiment of the present invention.

In the following a multi-cloud storage system is considered which can leverage a number of commodity cloud providers with the goal of distributing trust across administrative domains. This model is receiving attention nowadays with leading cloud-service providers offering products for multi-cloud systems. For instance in the following a system of a number of s storage servers is considered and a collection of users. Each server appropriately authenticates users.

In the figure a file F should be encrypted. Based on an embodiment of the invention it is assumed that an encryption procedure exists such that on an input of a plaintext bitstream p, a random seed S this encryption procedure divides the file F into blocks p1, ..., pN, where N is odd such that each block has size l. Here it is assumed that l is the block size of the particular block cipher used. The set of input blocks is then encrypted under key K resulting in a ciphertext $\underline{c}$ = {S, $\underline{c1}$, ..., $\underline{cN}$}. Further it is assumed that S = $\underline{c0}$.

Then, a linear transformation to $\underline{c}$ is applied. More specifically, M is assumed to be an (N+1)-by-(N+1) matrix where a matrix element M_{i,j}=0 if i=j and m_{i,j}=1, otherwise.

Then c=$\underline{c}$.M, is computed where addition and multiplication are implemented by means of XOR and AND operations, respectively. This transform can be efficiently computed in 2(N+1) XOR operations by calculating:

t = c0 XOR ... XOR cN
$\underline{ci}$ = t XOR ci

Given the encryption key K, inverting the resulting ciphertext c entails computing $\underline{c}$=c.$M^{-1}$ and decrypting $\underline{c}$. M is invertible with M=$M^{-1}$.

Before applying a (t2,n) IDA scheme such as Reed Solomon coding in each block $\underline{ci}$, a cyclic bitwise operation per block is used by an amount of f(K,i) mod |$\underline{ci}$|, where f(.) is a trapdoor function. The bitwise shift can be executed in small clock cycles on a computer and is as such considered a fast operation. Alternatively, a faster approach is to shift the bits of all the blocks using f(K) modulo the size of all the output blocks of ci. f could be a hash function. Optionally a block permutation can be additionally performed after the bitwise shifting enhancing the security.

Then a (t2,n) IDA proecedure is applied over the output blocks. The result is a (t2-2, t2, n) ramp scheme in this particular embodiment.

Besides being a secure ramp scheme, the technique also can act as a secure way to ensure file access revocation even if the owner has been revoked access but still retains access to the key and to parts of the ciphertext blocks (less than half of the entire file). Indeed, in this case, the technique ensures that the revoked user cannot acquire any meaningful bit of information about the original file.

Besides a keyed cyclic bitwise shifting, for example a keyed bit permutation using the block index as an additional seat or a keyed block cipher encryption per block using the block index S an additional seat can be used.

For encrypting the file F in a first step S1 the file F is divided into a number of chunks. Then in a second step S2 an all-or-nothing encryption using the encryption key k is applied on the divided blocks resulting in n ciphertext blocks c1, c2, ....

In a third step S3 a linear all-or-nothing scheme is applied on the n ciphertext blocks c1, c2, .....

In a fourth step S4 a key-based cyclic bitwise shift to transform the bits of each ciphertext block c1, c2, ... is performed in such a way that this shift cannot be reverted without the knowledge of the encryption key K in such that the bits in different ciphertext blocks c1, c2, ... are transformed independently at least in a computational sense.

In a fifth step S5 any (t2, n) information dispersal algorithm scheme is applied.

In summary the present invention enables the construction of a secure ramp scheme using any (t2, n) information dispersal algorithm IDA scheme with only small performance penalty. The present invention preserves the ramp scheme functionality even if the encryption key is leaked to an adversary.

The present invention preferably provides a method for encrypting data comprising the steps of:

1) Encrypt the data into n ciphertext blocks using a key K.
2) Apply a linear all or nothing scheme on the data.
3) Use a function based on key K to transform the bits of each ciphertext block in such a way that the function cannot be reverted without knowledge of K, and such that the bits in different blocks are transformed independently (at least in the computational sense).
4) Apply any (t2, n) IDA scheme.

The present invention provides in particular embedding of a keyed-based trapdoor transformation of bits of the output of an all-or-nothing encryption in such a way that bits in different blocks are transformed independently. Even further the present invention provides a construction of a secure ramp scheme based on any (t2, n) information dispersal algorithm IDA scheme keeping the ramp scheme confidentiality properties even if the encryption key is leaked to an adversary.

Many modifications and other embodiments of the invention set forth herein will come to mind to the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

# Claims

1. A method for encrypting data (F) with an encryption entity like a client, etc.
   characterized by the steps of
   a) Dividing (S1) a plaintext (F) into a number of N blocks,
   b) Encrypting (S2) each block with an encryption key (K) resulting in a number of ciphertext blocks (c1, c2)
   c) Applying (S3) a linear All-Or-Nothing scheme on said ciphertext blocks (c1, c2, …),
   d) Transforming (S4) each outputted ciphertext block ($\underline{c1}$, $\underline{c2}$, …) of step c) with a transformation procedure such that the information in different ciphertext blocks ($\underline{c1}$, $\underline{c2}$, …) is transformed differently based on said encryption key (K) and such that the transformation procedure is only revertable with knowledge of said encryption key (K), and
   e) Dispersing (S5) the transformed ciphertext blocks according to an information dispersal procedure (IDA).

2. The method according to claim 1, characterized in that the linear All-Or-Nothing scheme is performed by applying a matrix multiplication with a matrix, wherein the matrix elements on the diagonal are zero and all other matrix elements are one.

3. The method according to claim 2, characterized in that the matrix multiplication is performed by XOR- and AND-operations.

4. The method according to one of the claims 1-3, characterized in that the transformation procedure performs a keyed bit permutation per block using the index (i) of the corresponding ciphertext block ($\underline{ci}$) as additional random information.

5. The method according to one of the claims 1-3, characterized in that the transformation procedure performs a keyed block cipher encryption per ciphertext block (ci) using the index of the corresponding block as additional random information.

6. The method according to one of the claims 1-3, characterized in that the transformation procedure performs a cyclic bitwise operation, preferably per ciphertext block (c1, c2, ...).

7. The method according to claim 6, characterized in that the cyclic bitwise shifting per ciphertext block (c1, c2, ...) is performed using a trapdoor function with input of the  encryption key (K) and index (i) of the respective ciphertext block (c1, c2, ...), preferably by using the trapdoor function modulo the size of the corresponding ciphertext block (c1, c2, ...).

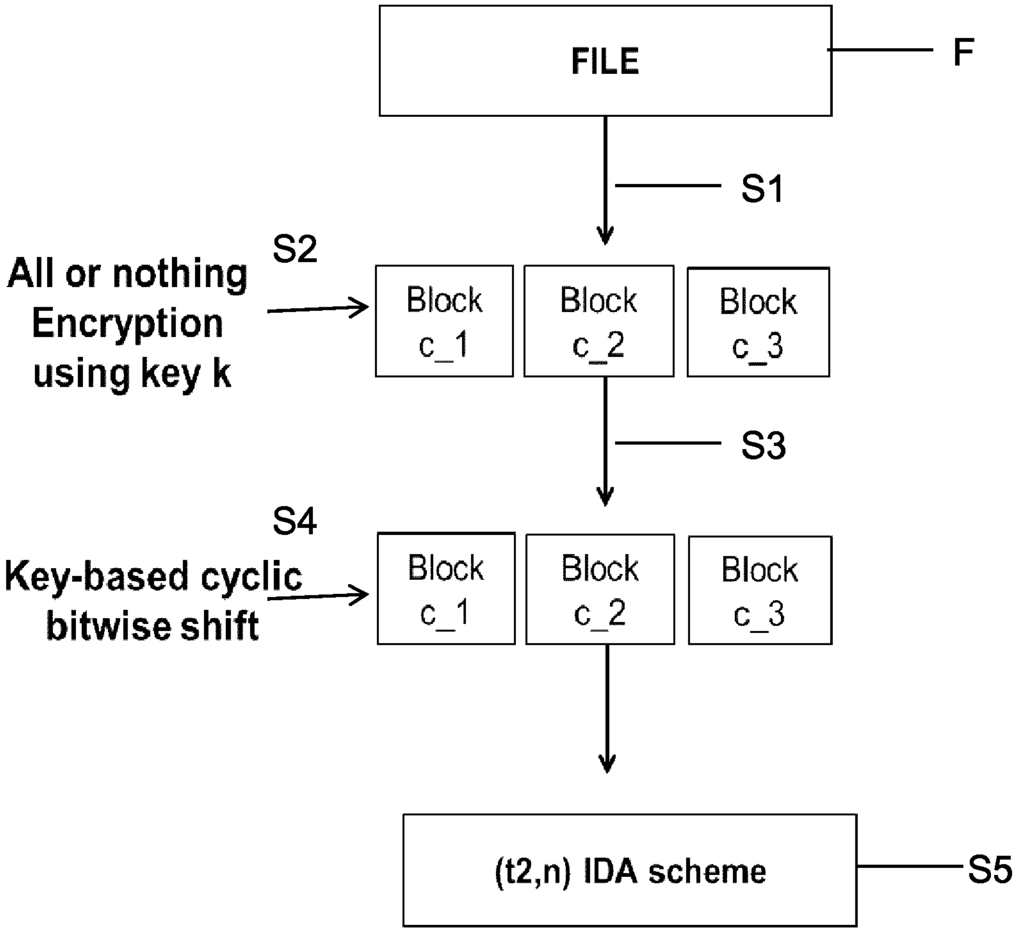
8. The method according to claim 6, characterized in that the cyclic bitwise shifting is performed on all blocks simultaneously using a function, preferably a one way cryptographic function, with input of the encryption key and modulo the size of all ciphertext blocks (c1, c2, ...).

9. The method according to one of the claims 6-8, characterized in that the ciphertext blocks (c1, c2, ...) are permuted after the cyclic bitwise operation.

10. A system for encrypting data (F) with an encryption entity like a client, etc.
characterized by one or more encryption entities like clients, adapted to or adapted to cooperate with each other to perform the steps of
    a) Dividing (S1) a plaintext (F) into a number of N blocks,
    b) Encrypting (S2) each block with an encryption key (K) resulting in a number of ciphertext blocks (c1, c2, ...),
    c) Applying (S3) a linear All-Or-Nothing scheme on said ciphertext blocks (c1, c2, ...),

d) Transforming (S4) each outputted ciphertext block ($\underline{c1}$, $\underline{c2}$, …) of step c) with a transformation procedure such that the information in different ciphertext blocks ($\underline{c1}$, $\underline{c2}$, …) is transformed differently based on said encryption key (K) and such that the transformation procedure is only revertable with knowledge of said encryption key (K), and

e) Dispersing (S5) the transformed ciphertext blocks according to an information dispersal procedure (IDA).


FILE
F
S1
S2
All or nothing Encryption using key k
Block c_1
Block c_2
Block c_3
S3
S4
Key-based cyclic bitwise shift
Block c_1
Block c_2
Block c_3
(t2,n) IDA scheme
S5

Figure

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/075425

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | GHASSAN O KARAME ET AL: "Securing Cloud Data in the New Attacker Model", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,,<br>vol. 20140718:123221,<br>16 July 2014 (2014-07-16), pages 1-19, XP061016652,<br>[retrieved on 2014-07-16]<br>sections 4 and 6<br>-----<br>-/-- | 1-10 |

☒ Further documents are listed in the continuation of Box C.

□ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| | |
|---|---|
| Date of the actual completion of the international search<br>24 August 2015 | Date of mailing of the international search report<br>31/08/2015 |
| Name and mailing address of the ISA/<br>European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Authorized officer<br>Billet, Olivier |

# INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/075425

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | KEVIN D BOWERS ET AL: "HAIL: A High-Availability and Integrity Layer for Cloud Storage",<br>INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,,<br>vol. 20090420:191549,<br>20 April 2009 (2009-04-20), pages 1-20,<br>XP061003119,<br>[retrieved on 2009-04-20]<br>section 5.4<br>----- | 1-10 |
| T | DANIEL SLAMANIG ET AL: "On cloud storage and the cloud of clouds approach",<br>INTERNET TECHNOLOGY AND SECURED TRANSACTIONS, 2012 INTERNATIONAL CONFERECE FOR, IEEE,<br>10 December 2012 (2012-12-10), pages 649-655, XP032340691,<br>ISBN: 978-1-4673-5325-0<br>----- | |