

Claims

1. A system for storing data on a distributed storage network comprising:
 5 a processor, a memory and instructions store on the memory and executable by the processor to:
 receive a data;
 randomise the data;
 apply an Information Dispersal Algorithm (IDA) to the randomised data to
 10 obtain slices of data; and
 store the slices of data on the distributed storage network, wherein the instruction to randomise the data comprises instructions to:
 divide the data into a plurality of blocks, $m_1, \dots, m_n$, each block being k bit length;
 generate an Initialisation Vector (IV) comprising random number of k bit length;
 15 randomise a first block of the plurality of blocks, m_1 , using the IV;
 randomise the rest of the plurality of blocks, $m_2, \dots, m_n$, each of the rest of the plurality of blocks is randomised using the randomised data from the previous block; and
 generate an additional block for storing IV.
- 20 2. The system according to claim 1 wherein the instruction to randomise the first block of the plurality of blocks, m_1 , using the IV comprises instruction to:
 apply an XOR function to a hash of IV and the first block m_1 , expressed in the following expression, $m'_1 = h(IV) \oplus m_1$.
- 25 3. The system according to anyone of claims 1-2 wherein the instruction to randomise the rest of the plurality of blocks, $m_2, \dots, m_n$, each of the rest of the plurality of blocks is randomised using the randomised data from the previous block comprises instruction to:
 apply, for current block, an XOR function to hash of previous randomised block,
 30 m'_{i-1} , with the current block m_i , expressed in the following expression, $m'_i = h(m'_{i-1}) \oplus m_i$
 where $i = 2..n$.
4. The system according to anyone of claims 1-3 wherein the instruction to generate the additional block for storing IV comprises instruction to:

apply an XOR function to a hash of one of the randomised blocks, m'_j , and the IV , expressed with the following expression, $m'_0 = h(m'_j) \oplus IV$ where j is selected from $1 \dots n$.

5. The system according to anyone of claims 1-4 further comprising instructions to:
 5 retrieve slices of data;
 apply the IDA to reconstruct the slices of data to obtain the randomised data; and
 de-randomise the randomised data to obtain the data.

6. The system according to claim 5 wherein the instruction to de-randomise the
 10 randomised data to obtain the data comprises instructions to:

divide the randomised data into a plurality of randomised blocks, $\dots m'_n$, each
 randomised block being k bit length;

determine the IV based on the additional randomised block, m'_0 ;

de-randomise a first block of the plurality of randomised blocks, m'_1 , using the IV ;

15 de-randomise the rest of the plurality of randomised blocks, $m'_2, \dots, m'_n$, each of
 the rest of the plurality of randomised blocks is de-randomised using the previous
 randomised block; and

arrange the de-randomised block to form the data.

7. The system according to claim 6 wherein the instruction to determine the IV based
 20 on the additional randomised block, m'_0 , comprises instruction to:

apply an XOR function to a hash of a selected randomised block with the
 additional randomised block, m'_0 , expressed in the following expression, $IV = h(m'_j) \oplus m'_0$
 where j is selected from $1 \dots n$.

8. The system according to anyone of claims 6-7 wherein the instruction to de-
 randomise the first block of the plurality of randomised blocks, m'_1 , using the IV comprises
 instruction to:

25 apply an XOR function to the hash of IV and the first randomised block m'_1 ,
 30 expressed in the following expression, $m_1 = h(IV) \oplus m'_1$.

9. The system according to anyone of claims 6-8 wherein the instruction to de-
 randomise the rest of the plurality of randomised blocks, $m'_2, \dots, m'_n$, each of the rest of
 the plurality of randomised blocks is de-randomised using the previous randomised block
 35 comprises instruction to:

apply, for current randomised block, an XOR function to hash of previous randomised block, m'_{i-1} , with the current randomised block m'_i , expressed in the following expression, $m_i = h(m'_{i-1}) \oplus m'_i$ where $i = 2..n$.

5 10. The system according to anyone of claims 6-9 wherein the de-randomised blocks are arranged with the following expression, $F = m_1, \dots, m_n$.

11. A method for storing data on a distributed storage network comprising:
 receiving a data;
 10 randomising the data;
 applying an Information Dispersal Algorithm (IDA) to the randomised data to obtain slices of data; and
 storing the slices of data on the distributed storage network, wherein the step of randomising the data comprises:
 15 dividing the data into a plurality of blocks, $m_1, \dots, m_n$, each block being k bit length;
 generating an Initialisation Vector (IV) comprising random number of k bit length;
 randomising a first block of the plurality of blocks, m_1 , using the IV;
 randomising the rest of the plurality of blocks, $m_2, \dots, m_n$, each of the rest of the plurality of blocks is randomised using the randomised data from the previous block; and
 20 generating an additional block for storing IV.

12. The method according to claim 11 wherein the step of randomising the first block of the plurality of blocks, m_1 , using the IV comprises:
 applying an XOR function to a hash of IV and the first block m_1 , expressed in the
 25 following expression, $m'_1 = h(IV) \oplus m_1$.

13. The method according to anyone of claims 11-12 wherein the step of randomising the rest of the plurality of blocks, $m_2, \dots, m_n$, comprises:
 applying, for current block, an XOR function to hash of previous randomised block,
 30 m'_{i-1} , with the current block m_i , expressed in the following expression, $m'_i = h(m'_{i-1}) \oplus m_i$ where $i = 2..n$.

14. The method according to anyone of claims 11-13 wherein the step of generating the additional block for storing IV comprises:

applying an XOR function to a hash of one of the randomised blocks, m'_j , and the IV , expressed with the following expression, $m'_0 = h(m'_j) \oplus IV$ where j is selected from $1 \dots n$.

- 5 15. The method according to anyone of claims 11-14 further comprising:
retrieving the slices of data from the distributed storage network;
applying the IDA to reconstruct the slices of data to obtain the randomised data;
and
de-randomising the randomised data to obtain the data.

10

16. The method according to claim 15 wherein the step of de-randomising the randomised data to obtain the data comprises:

dividing the randomised data into a plurality of randomised blocks, $\dots m'_n$, each randomised block being k bit length;

- 15 determining the IV based on the additional randomised block, m'_0 ;
de-randomising a first block of the plurality of randomised blocks, m'_1 , using the IV ;
de-randomising the rest of the plurality of randomised blocks, $m'_2, \dots, m'_n$, each of the rest of the plurality of randomised blocks is de-randomised using the previous randomised block; and

- 20 arranging the de-randomised block to form the data.

17. The method according to claim 16 wherein the step of determining the IV based on the additional randomised block, m'_0 , comprises:

- 25 applying an XOR function to a hash of a selected randomised block with the additional randomised block, m'_0 , expressed in the following expression, $IV = h(m'_j) \oplus m'_0$ where j is selected from $1 \dots n$.

18. The method according to anyone of claims 16-17 wherein the step of de-randomising the first block of the plurality of randomised blocks, m'_1 , using the IV comprises:

- 30 applying an XOR function to the hash of IV and the first randomised block m'_1 , expressed in the following expression, $m_1 = h(IV) \oplus m'_1$.

19. The method according to anyone of claims 16-18 wherein the step de-randomising the rest of the plurality of randomised blocks, $m'_2, \dots, m'_n$, comprises:

35

applying, for current randomised block, an XOR function to hash of previous randomised block, m'_{i-1} , with the current randomised block m'_i , expressed in the following expression, $m_i = h(m'_{i-1}) \oplus m'_i$ where $i = 2..n$.

- 5 20. The method according to anyone of claims 16-19 wherein the de-randomised blocks are arranged with the following expression, $F = m_1, \dots, m_n$.