

Protection of a cryptographic algorithm

The present invention relates to the field of cryptography and more particularly to the protection of information relating to calculations carried out according to a cryptographic algorithm.

Cryptographic algorithms allow in particular data to be encrypted and/or data to be decrypted. Such algorithms can also be used for numerous other applications. In fact, they can also serve to sign or even to authenticate certain information. They may also be used in the field of timestamping.

Such algorithms generally comprise a sequence of several operations or calculations that are successively applied to a piece of data to be encrypted in order to obtain a piece of encrypted data or again to a piece of encrypted data in order to obtain a piece of decrypted data.

Among these algorithms, some are founded on a use of private keys while others are based on a mixed use of public and secret keys.

Whatever the type of cryptographic algorithm, in order to preserve the confidential character of the algorithm, secret keys and other information, it is important that the calculations carried out remain secret.

This is because when an attacker is able to determine the calculations carried out according to a cryptographic algorithm, he may then access secret information and breach the confidential character of the data according to this algorithm.

In some algorithms the protection of the confidential character rests on the fact that the calculations are

carried out in a protected environment that is not accessible to potential attackers.

In some other algorithms the calculations may be
5 carried out in an environment accessible to potential
attackers. It is therefore necessary for such
algorithms that they are resistant to tests called
"white box" tests. These tests aim to attempt to breach
the confidential character of the algorithm from the
10 calculations carried out in the course of implementing
the algorithm.

The document "A White-Box DES Implementation for DRM
Applications" by S. Chow, P. Eisen, H. Johnson and P.C.
15 van Oorschot proposes a method allowing protection
against white-box tests, i.e. when the complete
implementation of the algorithm is available to the
attacker. The technique used is based on the use of
tables allowing the operations of the algorithm to be
20 implemented after encoding with the help of bijections
has been introduced between various rounds of the
algorithm.

However, the document "Attacking an Obfuscated Cipher
25 by Injecting Faults" by Matthias Jacob, Dan Boneh and
Edward W. Felten in 2003 discloses a method allowing
the secret information used in the execution of the
algorithm according to the method described in the
previously cited document to be found.

30

The document "White-box Cryptography and an AES
Implementation" by S. Chow, P. Eisen, H. Johnson and
P.C. van Oorschot proposes another implementation based
on similar principles to those stated by the document
35 "A White-Box DES Implementation for DRM Applications".
But encoding is added outside rounds.

The document "Cryptanalysis of a White-Box AES Implementation" by Olivier Billet, Henri Gilbert and Charaf Ech-Chatbi discloses an attack on this other implementation.

5

Hence, the protection methods of this type have weaknesses that allow the confidential character of the algorithm to be breached.

10 The present invention aims to increase the confidentiality protection level of an algorithm against white-box tests.

A first aspect of the present invention proposes a
15 method for carrying out a cryptographic calculation in an electronic component, according to a specified cryptographic algorithm including at least a first and a second cryptographic operation. The algorithm is designed to generate an encrypted data block from an
20 initial data block.

The method comprises the following steps:

(a) applying a first operational system to the initial data block and obtaining a first intermediate
25 data block, said first operational system corresponding to a combination of at least the first cryptographic operation, a first random operation that generates a determinate value with a defined probability value, a second random operation, and a bijective operation;

30 (b) applying a second operational system to the intermediate data block generated in the preceding step and obtaining a second intermediate data block, said second operational system corresponding to a combination of at least the inverse operation of the
35 bijective operation of the preceding operational system, the second cryptographic operation, and an operation that generates the value zero for a value associated with said determinate value;

(c) repeating the steps (a) and (b) N times, N being an integer determined depending on said defined probability value; and

(d) determining the encrypted data block from the
5 second intermediate data block(s) depending on the defined probability value.

Thanks to these measures, the cryptographic operations to be applied according to the algorithm to be
10 protected remain secret for any attacker. This is because they are applied to data to be encrypted in combination with at least two random operations, one of these two operations providing a determinate value with a defined probability. The effect of this first random
15 operation is advantageously only cancelled with the application of the operation that generates the value zero for a value associated with said determinate value. Hence, from the application of the first random operation and through to the application of the
20 operation that generates zero for a value associated with the determinate value, the data manipulated in the course of carrying out such calculations are protected against attacks.

25 When the method corresponds to the application of a first and of a second operational system alone, the associated value is equal to the determinate value.

It should be noted that the term "cryptographic
30 operation" corresponds to a cryptographic operation in the broad sense, i.e. that this term also denotes a succession of cryptographic operations.

The application of the first operational system may
35 correspond to the application in combination of:

- the first cryptographic operation generating a first result of the first operational system from the initial data block;

- the first random operation generating a second result of the first operational system from the initial data block;

- the second random operation generating a third result of the first operational system from the initial data block; and

- the bijective operation generating the first intermediate data block from the first, second and third results of the first operational system.

The application of the second operational system may correspond to the application in combination of:

- the inverse operation of the bijective operation of the preceding operational system generating, from the intermediate data block obtained by the preceding operational system, said first and second results of the preceding operational system;

- the second cryptographic operation generating a first result of the second operational system from the first result of the preceding operational system;

- the operation that generates the value zero for a value associated with the determinate value from the second result of the preceding operational system, hence generating a second result of the second operational system; and

- an addition of the first and the second result of the second operational system generating the second intermediate data block.

Each piece of data in the first and the second intermediate data blocks may be obtained in polynomial form from data of the initial data block and data of the first intermediate data block respectively.

The first and second operational systems may be applied in the form of tables of values to the initial data block and to the first intermediate data block respectively.

The first random operation, which generates a determinate value with a defined probability value, may be carried out in a finite mathematical space in which it generates at most one determinate set of values; and in which the operation that provides the value zero for a value associated with said determinate value also generates the value zero for the other values of said set.

10

Hence, the number N corresponding to the number of iterations of steps to determine the encrypted data block may advantageously be equal to 1.

15 When the algorithm includes a set of K additional cryptographic operation(s) between the first and second cryptographic operations, K being a positive integer, the method may furthermore comprise the following step between the step (a) and the step (b):

20 - applying a number K of successive additional system(s) operational (108) respectively associated with said set of additional cryptographic operation(s), each additional operational system generating an additional intermediate data block (114) from the intermediate data block (107) generated by the preceding operational system;

25 in which each additional operational system corresponds to a combination of at least the inverse operation (109) of the bijective operation of the preceding operational system, the additional cryptographic operation (110) associated with said additional operational system, an additional operation (111), a random operation (112) and a bijective operation (113).

35 In this case, the value associated with the determinate value for which the function is cancelled advantageously corresponds to the value resulting from the application of the additional operation on said

determinate value, or even from successive applications of additional operations on the determinate value.

5 The additional operational system may correspond to the application in combination of:

- the inverse operation of the bijective operation of the preceding operational system, generating, from the intermediate data block provided by the preceding operational system, the first, second and third results
10 of the preceding operational system;

- the additional cryptographic operation generating a first result of the additional operational system from the first result of the preceding operational system;

15 - the additional operation generating a second result of the additional operational system from the second result of the preceding operational system;

- the random operation generating a third result of the additional operational system from at least one
20 of the first, second and third results of the preceding operational system; and

- a bijective operation generating the additional intermediate data block from the first, second and third results of the additional operational system.

25

The additional operation may advantageously correspond to an identity operation and hence make the calculations easier. In such a case, the value associated with the determinate value, for which the
30 second specific operation generates a zero value, is more precisely equal to this determinate value.

Likewise, the bijective operations may advantageously correspond to linear bijective operations and hence
35 reduce the calculations.

A second aspect of the present invention proposes an electronic component for carrying out a cryptographic

calculation according to a cryptographic algorithm including at least a first and a second cryptographic operation, this electronic component being designed to implement a method for carrying out calculations
5 according to the first aspect of the present invention.

At least one of the first random operation, the second random operation and the bijective operation may differ at each repetition of the first and second operational
10 systems.

Other aspects, aims and advantages of the invention will become apparent on reading the description of one of its embodiments.

15

The invention will be better understood with the help of the drawings in which:

- Figure 1 illustrates the various steps of a cryptographic algorithm comprising a plurality of
20 cryptographic operations; and

- Figure 2 illustrates the main stages of a method of carrying out according to an embodiment of the present invention.

25 An objective of the present invention is to improve the resistance to attacks against cryptographic algorithms in the course of so-called white-box tests, i.e. when the implementation of the cryptographic algorithm to be protected is accessible to potential attackers. To this
30 end, the cryptographic operations to be applied to a data block according to the determinate algorithm to be protected are changed. Hence, instead of directly and successively applying the cryptographic operations of the algorithm to be protected, respective operational
35 systems are successively applied such that, on the one hand, the output data obtained from these operational systems differ from the output data obtained from the cryptographic operations of the algorithm to be

protected and, on the other hand, the output data from the various operational systems do not allow the confidentiality of the cryptographic algorithm to be protected to be breached.

5

According to one embodiment of the present invention, each operational system is generated from each cryptographic operation of the respective algorithm. More precisely, in each operational system
10 corresponding to a determinate cryptographic operation, random variables are introduced. Then, at least two operational systems, among the operational systems thus generated from the various cryptographic operations of the algorithm to be protected, furthermore comprise a
15 first and a second specific operation respectively.

In addition to the randomness introduced by the random operations introduced in each operational system, these two specific operations enable effective improvement of
20 the protection of the cryptographic algorithm, in particular in relation to the cryptographic operations that are carried out between the two cryptographic operations to which the two operational systems that include these two specific operations correspond.

25

In fact, the output data from each operational system implemented between these two operational systems including the two specific operations may be captured by a potential attacker without that being able to
30 threaten the confidentiality of the part of the algorithm to be protected which is included between the two cryptographic operations of the algorithm that are carried out within these two operational systems.

35 With the aim of protecting all the cryptographic operations of the algorithm, the two specific operations may advantageously be introduced in the first operational system generated from the first

cryptographic operation of the algorithm and in the last operational system generated from the last cryptographic operation of the algorithm.

- 5 The first specific operation corresponds to a random function which generates an output value in a random manner, this output value assuming a determinate value with a defined probability.
- 10 The second specific operation corresponds to a function that generates the value zero as an output value for an input value corresponding to a value associated with the determinate value. Generally speaking, this associated value corresponds to the transformation
- 15 undergone by the determinate value, if need be, following the application of additional operations of additional operational systems implemented between the first and the second operational system according to an embodiment of the present invention.
- 20 Consequently, in a general case, when an application of associated first and second operational systems, as described above, is reiterated a number of times determined as a function of the value of the defined
- 25 probability, it is possible to cancel the effect of the first specific operation through that of the second specific operation associated with it. Note that each set of first and second associated operational systems may advantageously be constructed with different
- 30 associated first and second specific operations, also different random operations and bijective operations.

Insofar as the effect of the first specific operation is not cancelled, the information accessible to an

35 attacker during execution of the algorithm according to an embodiment of the present invention differs greatly from the data obtained from different steps of a direct execution of the algorithm to be protected.

The data able to be captured by an attacker at the output of each of the operational systems not only do not correspond to the data that would be obtained by directly applying the corresponding cryptographic operations, but also have a random character relative to the data that should be obtained. Hence, potential attacks during the execution of such an algorithm are in vain.

10

The present invention is described in its application to an algorithm comprising a plurality of rounds, each round being able to correspond to a plurality of cryptographic operations. However, it should be noted that no limitation is attached to the type of cryptographic algorithm. In fact the present invention may easily be applied to any cryptographic algorithm comprising at least a first and a second cryptographic operation.

20

In one embodiment of the present invention, the two specific operations are introduced in the first round and the last round. However, the introduction of these two specific operations may be foreseen at any step of the algorithm to be protected.

25

Figure 1 illustrates the steps of a cryptographic algorithm comprising a plurality of rounds. In a step 10, a round of the algorithm comprising one or more cryptographic operations is applied to an initial data block X 101 to be encrypted. The application of the cryptographic operations of this round is a round of operations R_1 . A data block Y_1 is then obtained at a step 11. It satisfies the equation:

30

$$Y_1 = R_1(X)$$

Next, in step 12, the operations of the second round R_2 of the cryptographic algorithm are applied to this

block Y_1 . A block Y_2 satisfying the following equation is then obtained:

$$Y_2 = R_2(Y_1)$$

The various rounds R_i , for i between 1 and r , are successively applied in this way. A step 14 represents the data block Y_{r-1} thus obtained at the output of the penultimate round R_{r-1} . This data block satisfies the following equation:

$$Y_{r-1} = R_{r-1}(Y_{r-2})$$

10 Next, in step 15, the operations of the last round R_r of the algorithm considered are applied to this block Y_{r-1} and, in step 16, the encrypted data block Y_r satisfying the following equation is obtained:

$$Y_r = R_r(Y_{r-1})$$

15

Figure 2 describes the steps of a method of carrying out cryptographic calculations according to an embodiment of the present invention applied to an algorithm corresponding to that described above with reference to Figure 1.

In one embodiment of the present invention, when a operational system comprises a plurality of cryptographic operations to be applied to an initial data block $X = (x_1, \dots, x_n)$ so as to generate a data block $Z = (z_1, \dots, z_n)$ resulting from the series of successive operations, each component of the resulting data block is expressed in a polynomial form as a function of the various components $x_1, \dots, x_n$ of the initial data block X .

More precisely, when a operational system S to be applied to an initial data block X to obtain a resultant data block Z comprises a succession of operations, this data block X is decomposed into a plurality of smaller data blocks, $x_1, \dots, x_n$. Each component data block z_i of the data block Z may then be obtained in a polynomial form as a function of the

various components x_i of the initial data block. In this way, each component of the data block resulting from the application of the operations of the operational system considered is then generated in a single transformation. In such conditions, the succession and the distinction of the operations comprising the operational system applied is then difficult for a potential attacker to access.

10 The following equation may therefore be written:

$$Z=S(X) \quad [1]$$

and for i between 1 and n , a polynomial p_i exists such that:

$$z_i=p_i(x_1, \dots, x_n) \quad [2]$$

15

The following sections use the application of various cryptographic operations in the combined form expressed above.

20 In a variant, it is also possible to envisage obtaining the various components of the data block resulting from the cryptographic operations of the operational system in the form of tables of values.

25 Whichever method of application is used, either in a polynomial form or even in the form of tables of values, the operations to be applied according to an operational system are preferably applied in combination, such that each component of the data block coming from the operational system is obtained in a single transformation.

30

In one embodiment of the present invention, the algorithm to be protected is implemented by modifying the rounds of operations R_i , for i between 1 and r , as described above. In one embodiment of the present invention, at least one round of operations R_i of the algorithm is associated with an operational system S_i

35

which is a combination of at least the round of operations R_i of the algorithm to be protected, a random operation A_i , and a random operation V that generates a determinate value v with a defined probability. A combined execution of the various operations of such operational systems S_i advantageously allows a data block to be obtained resulting from the initial data block in a single transformation. Hence, a potential attacker is not able to distinguish the various operations separately.

It should be noted that the present invention is also easily applied to the case where a round of operations of the algorithm R_i corresponds to a single cryptographic operation.

In a step 102, a first operational system S_1 is applied to the initial data block 101. More precisely, in an embodiment of the present invention, this first operational system corresponds to applying to the initial data block 101 in combination:

- the first round of operations R_1 of the algorithm to be protected;
- the random operation A_1 ; and
- the first random operation V ; then

combining the various data blocks resulting from these three operations applied to the initial data block 101, so as to obtain a first intermediate data block 107. This combination is obtained by applying a bijective mapping to the results of these three aforementioned operations.

This operational system is carried out in the form of a single transformation, allowing the first intermediate data block to be obtained component by component from the initial data block, as described above. It may also be implemented in a polynomial form or even in the form of tables of values.

The following section details the operations to which the application of the first operational system S_1 according to an embodiment of the present invention
5 corresponds.

The round of operations R_1 of the algorithm considered is applied to the initial data block X 101, which can be written in the form of a data series $x_1, \dots, x_n$. A
10 first result 103 is obtained from the first operational system, denoted $Y_{1,1}$, corresponding to a data block that satisfies the following equation:

$$Y_{1,1} = R_1(X)$$

Note that $Y_{1,1}$ is equal to Y_1 as defined above with
15 reference to Figure 1. But such a result is not accessible to a potential attacker, since in the course of carrying out the operations comprising the operational system S_1 this step is mixed with other operations to be applied and described above, in
20 polynomial form or in the form of tables of values.

Next, when the function V is applied to the initial data block, a second result 104 is obtained from this first operational system in the form of a data block
25 satisfying the following equation:

$$Y_{1,2} = V(X)$$

By applying the random operation A_1 to the initial data block X , a third result 105 is obtained from the first
30 operational system in the form of a data block $Y_{1,3}$ satisfying the following equation:

$$Y_{1,3} = A_1(X)$$

In a manner not allowing distinction of the three
35 results described above output from the first operational system, a combination 106 of these three results is carried out to generate the first intermediate data block 107, corresponding to the

carrying out of the first round of the algorithm according to an embodiment of the present invention.

Hence, at the output of the first operational system S_1
5 the intermediate data block XI_1 is obtained, satisfying the following equation:

$$XI_1 = M_1(Y_{1,1}; Y_{1,2}; Y_{1,3})$$

where M_1 is the bijective combination applied in the first operational system S_1 .

10

Advantageously, the intermediate data block XI_1 differs from the data block Y_1 obtained from the first round according to the cryptographic algorithm with reference to Figure 1. Such a difference does not enable the data
15 block Y_1 , which is equal to the data block $Y_{1,1}$, to be found from the data block XI_1 .

Then a second operational system 108, corresponding to carrying out the second round of the algorithm to be
20 protected according to an embodiment of the present invention, is applied to the first intermediate data block 107. It corresponds to the combined application of an inverse operation of the bijective operation from the preceding operational system, the second round of
25 operations from the algorithm to be protected R_2 , a random operation A_2 , an operation corresponding to the identity I_2 , and a bijective operation M_2 .

This second operational system corresponds to the
30 application of the operations described separately in detail in the following sections, but which are applied component by component in a single transformation, as for all the operational systems described according to an embodiment of the present invention.

35

This operational system corresponds to the application first of the inverse operation M_1^{-1} 109 of the operation M_1 on the data block XI_1 so as to obtain in a distinct

manner the three results described for the first operational system $Y_{1,1}$; $Y_{1,2}$ and $Y_{1,3}$.

5 Next, the cryptographic operations of the round R_2 of the cryptographic algorithm are then applied to the first result $Y_{1,1}$ 110, and a first result $Y_{2,1}$ is then obtained from the second operational system S_2 , satisfying the following equation:

$$Y_{2,1}=R_2(Y_{1,1})$$

10 Then the operation I_2 is applied to the second result from the preceding operational system $Y_{1,2}$ and a second result 111 is obtained from the second operational system, satisfying the following equation:

$$Y_{2,2}=Y_{1,2}$$

15 In the example described below, the identity operation is considered. But this operation may be different from an identity operation. More generally, this operation may be any operation at all.

20 The random operation A_2 is then applied to the third result from the preceding operational system $Y_{1,3}$ to obtain a third result 112 of the second operational system, satisfying the following equation:

$$Y_{2,3}=A_2(Y_{1,1}; Y_{1,2}; Y_{1,3})$$

25

In a variant, it is possible to envisage the random operation taking any subset of the three results $Y_{1,1}$; $Y_{1,2}$; $Y_{1,3}$ as input.

30 Next, referred to as 113, a bijective operation M_2 is then applied to the first, second and third results from the second operational system to obtain a third intermediate data block 114 XI_2 . This data block 114 satisfies the following equation:

35
$$XI_2=M_2(Y_{2,1}; Y_{2,2}; Y_{2,3})$$

In one embodiment of the present invention, the operational systems S_i , for i between 2 and $r-1$,

correspond to the application of operations similar to those described with reference to the second operational system.

5 From the above description it is easy to deduce variants of the application of the present invention in which the operations may differ depending on the operational systems. Thus, for example, it is possible to envisage that in some operational systems the
10 function I previously described is an identity function, while in others it is any function differing from the identity function.

Next, the final operational system 116 S_r corresponds
15 to the combined application of an operation corresponding to the inverse operation 117 of the bijective operation M_{r-1} from the preceding operational system, the round of operations R_r of the algorithm to be protected, and an operation Z_v that generates the
20 value zero for a value associated with the determinate value v . The following sections detail the separate application of these various operations. It should be noted that, as in each operational system S_i , these operations are applied in combination.

25

The preceding operational system S_{r-1} generates an $(r-1)$ th intermediate data block XI_{r-1} , referred to as 115. The inverse operation 117 of the bijective operation M_{r-1}^{-1} generates the first and second result of the
30 operational system S_{r-1} from the intermediate data block XI_{r-1} .

The round of operations R_r of the algorithm to be protected is applied to the first result $Y_{r-1,1}$ and a
35 first result 118 of the operational system S_r is obtained, satisfying the following equation:

$$Y_{r,1} = R_r(Y_{r-1,1})$$

The operation Z_v is applied to the second result of the preceding operational system $Y_{r-1,2}$ and a second result 119 is obtained, satisfying the following equation:

$$Y_{r,2}=Z_v(Y_{r-1,2})$$

5

Now, this second result $Y_{r-1,2}$ corresponds to the second result of the first operational system $Y_{1,2}$. In fact, in the case where the operations $I_2, \dots, I_{r-1}$ are considered to be the identity operation, it has not been transformed by the various operational systems that have succeeded the first operational system.

10

Hence, it is possible to write:

$$Y_{r,2}=Z_v(V(X))$$

15

In the case where the operations $I_2, \dots, I_{r-1}$ are different from the identity operation, this last equation is no longer satisfied. But, in this case, the function V is advantageously chosen so as to generate the value zero for the value associated with the determinate value $V(X)$, i.e. for the value which results from the transformations of $V(X)$ in the various additional operational systems.

20

Next, the first and second results are finally combined to generate an r -th intermediate data block 120 XI_r . This last intermediate data block satisfies the following equation:

$$XI_r=Y_{r,1}+Y_{r,2}$$

30

In a general case, a minimum number of repetitions of different versions of the algorithm to be protected according to an embodiment of the present invention is determined depending on the defined probability value with which the operation V generates the determinate value v .

35

Hence, for example, if the defined probability value is equal to $2/3$, the application of the set of successive operational systems respectively associated with the set of cryptographic operations of the algorithm, as defined above, should be repeated at least three times so as to be able to determine after execution that data block among the last intermediate data blocks obtained which corresponds to the encrypted data block according to the initial algorithm to be protected, i.e. that which corresponds to the data block Y_r . The set of successive operational systems of each of the applications satisfies the characteristics described according to an embodiment of the present invention, but these sets of operational systems may differ from each other at each new application. They may in particular be based on different random operations and different bijective operations.

Thanks to the measures described in the preceding sections, when the function V is introduced in the first operational system and the function Z_v is introduced in the last operational system, no piece of data accessible to a potential attacker provides information about the intermediate output data corresponding to the direct execution of the algorithm to be protected.

The following sections describe a particular case of the application of the present invention in which the data block encrypted according to the algorithm to be protected is determined by executing the method of execution according to an embodiment of the present invention a single time.

When placed in the finite body $GF(2)$, any polynomial P can take only two values, either 0 or 1. It is possible to choose:

$$V(X) = (P(X) + v_1, \dots, P(X) + v_m)$$

Hence, $V(X)$ can assume only two different values, either:

$$v = (v_1, \dots, v_n); \text{ or}$$

$$v' = (v_1+1, \dots, v_n+1).$$

5

In such a context, if the function Z_v assumes the value 0 at the values v and v' , then a single iteration of the execution of the algorithm to be protected according to an embodiment of the present invention
10 suffices to obtain the data block encrypted according to said algorithm.

CLAIMS

1. Method for carrying out a cryptographic calculation in an electronic component, according to a specified cryptographic algorithm including at least a first and a second cryptographic operation, said algorithm being designed to generate an encrypted data block from an initial data block;

said method comprising the following steps:

10 (a) applying a first operational system (102) to the initial data block and obtaining a first intermediate data block, said first operational system corresponding to a combination of at least the first cryptographic operation (103), a first random operation 15 (104) that generates a determinate value with a defined probability value, a second random operation (105), and a bijective operation (106);

(b) applying a second operational system (116) to the intermediate data block generated in the preceding step and obtaining a second intermediate data block, 20 said second operational system corresponding to a combination of at least the inverse (117) operation of the bijective operation of the preceding operational system, the second cryptographic operation (118), and 25 an operation that generates the value zero for a value associated with said determinate value (119);

(c) repeating the steps (a) and (b) N times, N being an integer determined depending on said defined probability value; and

30 (d) determining the encrypted data block from the second intermediate data block(s) depending on the defined probability value.

2. Method for carrying out a cryptographic calculation according to Claim 1, in which the application of the 35 first operational system corresponds to the application in combination of:

- the first cryptographic operation generating a first result (103) of the first operational system from the initial data block;

- the first random operation generating a second
5 result (104) of the first operational system from the initial data block;

- the second random operation generating a third result (105) of the first operational system from the initial data block; and

- 10 - the bijective operation (106) generating the first intermediate data block (107) from the first, second and third results of the first operational system; and

in which the application of the second operational
15 system corresponds to the application in combination of:

- the inverse operation (117) of the bijective operation of the preceding operational system generating, from the intermediate data block obtained
20 by the preceding operational system, said first and second results of the preceding operational system;

- the second cryptographic operation (118) generating a first result of the second operational system from the first result of the preceding
25 operational system;

- the operation that generates the value zero for a value associated with the determinate value (119) from the second result of the preceding operational system, hence generating a second result of the second
30 operational system; and

- an addition of the first and the second result of the second operational system generating the second intermediate data block (120).

35 3. Method for carrying out a cryptographic calculation according to Claim 1 or 2, in which each piece of data in the first and the second intermediate data blocks may be obtained in polynomial form from data of the

initial data block and data of the intermediate data block respectively.

4. Method for carrying out a cryptographic calculation according to Claim 1 or 2, in which the first and second operational systems are applied in the form of tables of values to the initial data block and to the first intermediate data block respectively.

10 5. Method for carrying out a cryptographic calculation according to any one of the preceding claims, in which the first random operation, which generates a determinate value with a defined probability value, is carried out in a finite mathematical space in which it
15 generates at most one determinate set of values; and in which the operation that provides the value zero for a value associated with said determinate value also generates the value zero for the values of said set that are different from said determinate value.

20

6. Method for carrying out a cryptographic calculation according to any one of the preceding claims, furthermore comprising, when the algorithm includes a set of K additional cryptographic operation(s) between
25 the first and second cryptographic operations, K being a positive integer, the following step between the step (a) and the step (b):

- applying a number K of successive additional operational system(s) (108) respectively associated
30 with said set of additional cryptographic operation(s), each additional operational system generating an additional intermediate data block (114) from the intermediate data block (107) generated by the preceding operational system;

35 in which each additional operational system corresponds to a combination of at least the inverse operation (109) of the bijective operation of the preceding operational system, the additional cryptographic

operation (110) associated with said additional operational system, an additional operation (111), a random operation (112) and a bijective operation (113).

5 7. Method for carrying out a cryptographic calculation according to Claim 6, in which each additional operational system corresponds to the application in combination of:

10 - the inverse operation (109) of the bijective operation of the preceding operational system, generating, from the intermediate data block provided by the preceding operational system, the first (131), second (132) and third (133) results of the preceding operational system;

15 - the additional cryptographic operation (110) generating a first result (134) of the additional operational system from the first result of the preceding operational system;

20 - the additional operation (111) generating a second result of the additional operational system from the second result (132) of the preceding operational system;

25 - the random operation (112) generating a third result (136) of the additional operational system from at least one of the first, second and third results of the preceding operational system; and

30 - a bijective operation (113) generating the additional intermediate data block from the first, second and third results of the additional operational system.

8. Method for carrying out a cryptographic calculation, in which the additional operation (111) is an identity operation and in which the value associated with the
35 determinate value is equal to the determinate value.

9. Electronic component for carrying out a cryptographic calculation according to a cryptographic

algorithm including at least a first and a second cryptographic operation, said algorithm being designed to generate an encrypted data block from an initial data block, said component comprising:

5 - first means for applying a first operational system (102) to the initial data block and generating a first intermediate data block, said first operational system corresponding to a combination of at least the first cryptographic operation, a first random operation
10 that generates a determinate value with a defined probability value, a second random operation, and a bijective operation;

 - second means for applying a second operational system (116) to the intermediate data block generated
15 by the preceding means and generating a second intermediate data block, said second operational system corresponding to a combination of at least an inverse operation of the bijective operation of the preceding means, the second cryptographic operation, and an
20 operation that generates the value zero for a value associated with said determinate value;

 - means for repeating the application of the first and second operational systems N times, N being an integer determined depending on said defined
25 probability value; and

 - means for determining the encrypted data block from the second intermediate data block(s) depending on the defined probability value.

30 10. Electronic component for carrying out a cryptographic calculation according to Claim 9, in which at least one of the first random operation, the second random operation and the bijective operation differs at each repetition of the first and second
35 operational systems.