

Method for Generating Parameters Characterizing a Cryptographic Protocol

The present invention relates to a parameter generation method for generating parameters characterizing a cryptographic protocol. The present invention also relates to a transmission method for transmitting an elliptic curve, an encryption method and a decryption method using the parameter generation method. The present invention also relates to a computer program product and a readable information storage medium for storing associated data and information.

The present invention relates to the field of cryptography. Cryptography is split into two distinct parts: symmetric cryptography and asymmetric cryptography.

Asymmetric cryptography provides the means to perform exchange protocols for exchanging keys or electronic signatures. RSA encryption (the acronym being derived from the initials of its three inventors Rivest, Shamir, and Adelman) is an asymmetric cryptographic algorithm that is slow and consumes significant computing time.

In particular, in order to overcome such a disadvantage, elliptic curves have been developed for the exchange protocols. In fact, the elliptic curves are of interest for cryptography by virtue of the existence of laws of addition and of multiplication by a scalar over the group $(E(\mathbb{F}_p), +)$. The law of multiplication by a scalar defines the problem referred to as elliptic curve discrete logarithm problem, consisting in finding the scalar k based on $[k]P$ and P . This problem is computationally difficult, that is to say that its solution is non polynomial in the bit size of the elements.

In order to ensure that the problem is indeed effectively difficult, it is necessary for the elliptic curve considered to satisfy a certain number of security criteria.

An elliptic curve is considered to be secure if the curve is not susceptible to a generic attack of various types such as a Pollard rho attack, a transfer attack, attacks using endomorphisms derived from complex multiplication, an attack on the associated curve by the phenomenon of twisting (per the accepted terminology also referred to as "twist") and considered to be rigid, that is to say, the generation method is completely explicit and has no arbitrary step.

The generation of a secure elliptic curve is therefore difficult since a number of criteria are to be satisfied; in particular the property of complete rigidity is very difficult to ensure.

There is therefore a need for a parameter generation method for generating parameters for an elliptic curve, and more generally for a cryptographic protocol, which

makes it possible to obtain in a totally rigid manner, a secure elliptic curve, and a secure cryptographic protocol, respectively.

To this end, the invention provides a parameter generation method for generating at least one parameter, the said at least one parameter characterizing a cryptographic protocol, the method including at least the steps of selection for selecting a text, of initialization for initializing the value of a counter to an initial value. The method includes at least for each parameter, the obtaining of a value for the parameter, at least one value for the parameter being obtained by means of effectively implementing the following steps of computation for computing an operation applied to the text and the value of the counter, so as to obtain a result, and of application for applying a cryptographic hash function to the result so as to obtain a value for the parameter, the operation and the cryptographic hash function being specific to the said at least one parameter. The method includes at least the step of testing for testing the compliancy of each parameter value obtained with at least one criterion, and when at least one value does not comply with the said at least one criterion, the step of incrementation for incrementing the value of the counter by adding of an integer, and of iteration for iterating the obtaining and testing steps, and when each value is in compliance with the criterion, a parameter generation step for generating the parameters such that the value of each parameter is the value which complies with the said at least one criterion.

According to some particular embodiments, the parameter generation method includes one or more of the following characteristic features, taken into consideration separately or in accordance with any technically possible combinations:

- the cryptographic protocol is selected from the group constituted of an elliptic curve, a curve belonging to a family of curves parameterized by at least one parameter and a key exchange protocol.
- the parameters are the parameters of an elliptic curve, the parameters being a modulus, a first coefficient and an order, a value for the modulus being obtained by effectively implementing a computation step of computing a first operation applied to the text and the value of the counter, so as to obtain a first result, and an application step of applying a first cryptographic hash function to the first result so as to obtain the value for the modulus, a value for the first coefficient being obtained by effectively implementing a computation step of computing a second operation applied to the text and the value of the counter, so as to obtain a second result, and an application step of applying a second cryptographic hash function to the second result so as to obtain the value for the first coefficient, and a value for

the order of the curve being obtained by effectively implementing an order value determination step for determining it based on the values of the modulus and of the first coefficient, each operation preferably including a concatenation of the text.

5 - the parameters are the parameters of an elliptic curve, the parameters being a modulus, a first coefficient, a second coefficient, and an order, a value for the modulus being obtained by effectively implementing a computation step of computing a first operation applied to the text and the value of the counter, so as to obtain a first result, and an application step of applying a first cryptographic hash function to the first result so as to obtain the value for the modulus, a value for the
10 first coefficient being obtained by effectively implementing a computation step of computing a second operation applied to the text and the value of the counter, so as to obtain a second result, and an application step of applying a second cryptographic hash function to the second result so as to obtain the value for the first coefficient, a value for the second coefficient being obtained by effectively
15 implementing a computation step of computing a third operation applied to the text and the value of the counter, so as to obtain a third result, and an application step of applying a third cryptographic hash function to the third result so as to obtain a value for the second coefficient, and a value for the order of the curve being obtained by effectively implementing an order value determination step for
20 determining it based on the values of the modulus, of the first coefficient, and of the second coefficient, each operation preferably including a concatenation of the text.

25 - the text satisfies at least one of the following properties: a first property according to which the text comprises of more than 16 characters; a second property according to which the text includes a date.

30 - in the step of testing of compliancy, the prime factorization or factoring of a first number into prime numbers is carried out in order to verify compliance with at least one criterion, the prime factorization being effectively carried out over the set of all prime factors that are lower than a threshold value, with the criterion being satisfied
when the quotient obtained by dividing the first number by the product of the set of prime factors that are lower than the threshold value is prime.

35 The present description also relates to a transmission method for transmitting an elliptic curve, the elliptic curve being characterized by the parameters generated by the parameter generation method as previously described above, in which the transmission method includes only either the transmission of the value of the counter and the value of

the order of the curve, or the transmission of the value of the counter and the value of the trace of the curve given by the difference between the modulus and the order of the curve to which is added the number 1.

5 The present description also relates to an encryption or decryption method for encryption or decryption by using a cryptographic protocol, the cryptographic protocol being characterized by the parameters generated by the parameter generation method as previously described above.

10 The invention also provides a computer program product comprising a readable information storage medium, on which is saved and stored a computer program comprising of program instructions, it being possible for the computer program to be loaded on to a data processing unit, the program being adapted so as to drive and run the operational implementation of a method as previously described above when the computer program is operationally deployed on the data processing unit.

15 The invention also provides a readable information storage medium on which is saved and stored a computer program comprising of program instructions, it being possible for the computer program to be loaded on to a data processing unit, the program being adapted so as to drive and run the operational implementation of a method as previously described above when the computer program is operationally deployed on the data processing unit.

20 Other characteristic features and advantages of the invention will become apparent upon reading the description that follows of embodiments of the invention, provided purely by way of example and with reference being made to the attached drawings which include:

- 25 - Figure 1, a schematic view of an example of a system that provides the ability to operationally implement the methods; and
- Figure 2, a flow diagram of an example of an operational implementation of a parameter generation and transmission method for generating the parameters of an elliptic curve and for transmitting an elliptic curve.

30 A system 10 and a computer program product 12 are shown in Figure 1. The interaction of the computer program product 12 with the system 10 makes it possible to implement a parameter generation method for generating the parameters of a cryptographic protocol.

The system 10 is a computer.

35 More generally, the system 10 is an electronic computing unit that is capable of manipulating and/or transforming the represented data such as electronic or physical

quantities in the records-registries of the system 10 and/or the storage memories into other similar data corresponding to the physical data in the storage memories, records-registries or other types of devices for display, transmission or data storage.

5 The system 10 includes a processor 14 comprising a data processing unit 16, storage memories 18, and a drive-reader for an information storage medium 20. The system 10 also comprises a keyboard 22 and a display unit 24.

The computer program product 12 comprises a readable information storage medium 20.

10 A readable information storage medium 20 is a storage medium that is readable by the system 10, usually by the data processing unit 14. The readable information storage medium 20 is a medium that is adapted so as to save and store electronic instructions and is capable of being coupled to a bus of an IT system.

By way of example, the readable information storage medium 20 is a diskette or flexible disk (that is to say "floppy disk"), an optical disk, a Compact Disc – Read-Only Memory (CD-ROM), a magneto-optical disk, a Read-Only Memory (ROM), a Random-Access Memory (RAM), an Electrically Programmable Read Only Memory. (EPROM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a magnetic card or an optical card.

20 On the readable information storage medium 20 is saved and stored a computer program comprising of program instructions.

The computer program is able to be loaded on to the data processing unit 14 and is adapted so as to drive and run the operational implementation of a parameter generation method for generating the parameters of an elliptic curve when the computer program is operationally deployed on the data processing unit 14.

25 The operation of the system 10 in interaction with the computer program product 12 will next be described with reference to Figure 2 which illustrates an example of implementation of a parameter generation method for generating the parameters of an elliptical curve.

30 The elliptic curves used in cryptography are generally given in the Weierstrass form. These are the set of points of a finite field $\mathbb{F}_p$ satisfying the following equation:

$$Y^2 = X^3 + aX + b \mod p$$

Where:

- X and Y are elements of the finite field $\mathbb{F}_p$,
- p is the modulus,
- 35 • a is the first coefficient, and

- b is the second coefficient.

For each of the curves, a set of parameters makes it possible to determine the curve.

In a simple manner, the parameters are the modulus p , the first coefficient a and the second coefficient b .

These three parameters are sufficient to characterize an elliptic curve.

In order to be able to exchange data and information over a channel referred to as a public channel, use is also made in the context of cryptography of other parameters among which the coordinates of the base point of the curve denoted by (x, y) , the order of the curve q or the cofactor h . By definition, the cofactor is the ratio between the order q and the order of the group generated by the base point (x, y) ; the base point is selected in a manner such that this cofactor is very small.

The generation method includes a phase of provisioning 50, a phase of computation 60 and a phase of testing 62 schematically represented in Figure 2.

The provisioning phase 50 comprises a step of selection of a text and of initializing of the value of a counter to an initial value.

Preferably, the selected text comprises of more than 16 characters.

According to one particular example, the text is a proprietary text belonging to the person generating the parameters, for example, an extract of a license of a product sold by that person. This license is represented schematically by a frame with a reference number 54.

In order to ensure the rigidity of the proposed method, it is recommended that the selected text be intelligible and serve to enable identifying the entity who is claiming ownership or the context for use thereof.

According to one variant, the text also includes data relating to the date of operational implementation of the method. These data are represented schematically by a frame with a reference number 56.

For example, it is possible to concatenate a part of the text and a date.

According to another example, the text itself includes the date. By way of an illustrative example, the text is "This curve was generated on [a given date]".

The counter is, moreover, initialized to an initial value, for example 1 (see the frame with a reference number 52).

The phase of computation 60 comprises a plurality of steps of computation, and of application and a step of determination.

In the first step of computation, a first operation O_1 is applied to the text and the value of the counter, so as to obtain a first result $R1$.

According to the example described, the first operation O_1 is a concatenation of the text, of the value of the counter and of a first constant C_1 . A concatenation consists of the operation of joining two character strings together end-to-end.

In the second step of computation, a second operation O_2 is applied to the text and the value of the counter, so as to obtain a second result $R2$ that is distinct from a first result $R1$.

According to the example described, the second operation O_2 is a concatenation of the text, of the value of the counter and of a second constant C_2 that is distinct from the first constant C_1 .

In the third step of computation, a third operation O_3 is applied to the text and the value of the counter, so as to obtain a third result $R3$.

According to the example described, the third operation O_3 is a concatenation of the text, of the value of the counter and of a third constant C_3 that is distinct from the first constant C_1 and distinct from the second constant C_2 .

In each of the examples described, it appears that each operation O_1 , O_2 and O_3 comprises a concatenation of the text, of the value of the counter and of a constant specializing in a unique manner each output.

In the first application step, a first cryptographic hash function $H1$ is applied to the first result $R1$ so as to obtain a value for the modulus p .

A hash function is a particular function that, based on data provided as input, computes a digital 'fingerprint' that serves to rapidly, though incompletely, identify the original data.

According to the example provided, the hash function $H1$ is the function SHA-1 (Secure Hash Algorithm 1).

In the case illustrated, the value obtained for the modulus p is equal to the value rendered as a hexadecimal number, of the result obtained by application of the first cryptographic hash function $H1$ to the first result $R1$.

In the second application step, a second cryptographic hash function $H2$ is applied to the second result $R2$ so as to obtain a value for the first coefficient a .

According to the example illustrated, the first cryptographic hash function $H1$ and the second cryptographic hash function $H2$ are identical.

In addition, similarly to the first application step, the value obtained for the first coefficient a is equal to the value rendered as a hexadecimal number, of the result

obtained by application of the second cryptographic hash function H2 to the second result R2.

In the third application step, a third cryptographic hash function H3 is applied to the third result R3 so as to obtain a value for the second coefficient b.

5 According to the example illustrated, the first cryptographic hash function H1 and the third cryptographic hash function H3 are identical.

In addition, similarly to the first application step, the value obtained for the second coefficient b is equal to the value rendered as a hexadecimal number, of the result obtained by application of the third hash function H3 to the third result R3.

10 During the determination step, the value that is determined is the value of the order q corresponding to the values of the modulus p, of the first coefficient a, and of the second coefficient b.

Such a value of the order q is determined, for example, by making use of the Schoof algorithm or the version thereof as improved by Elkies and Atkin (also referred to as Schoof–Elkies–Atkin algorithm, SEA).

15 During the phase of testing 62, a compliancy test for testing compliance of the values of the modulus p, of the first coefficient a, of the second coefficient b, and of the order q is carried out.

20 The values of the modulus p, of the first coefficient a, of the second coefficient b, and of the order q are considered to be compliant if the values of the modulus p, of the first coefficient a, of the second coefficient b, and of the order q satisfy a criterion.

For example, the criterion is selected so as to ensure that the elliptic curve obtained based on the values of the modulus p, of the first coefficient a, of the second coefficient b, and of the order q, is secure.

25 According to a particular embodiment, the preceding security criterion is considered fulfilled upon a plurality of sub-criteria being satisfied by the values of the modulus p, of the first coefficient a, of the second coefficient b, and of the order q.

According to a first sub-criterion, the elliptic curve is not susceptible to a Pollard rho attack.

30 For example, according to the first sub-criterion, the size of the subgroup q is greater than twice the level of security.

The level of security depends on the intended application and constitutes an objective to be achieved. In concrete terms, the level of security corresponds to the logarithm of the minimum number of operations that it is necessary to carry out in order to

break the system. By way of example, for civil applications, 128 bits of security are recommended.

According to a second sub-criterion, the elliptic curve is not susceptible to an additive transfer and a multiplicative transfer. For example, an expression of the second sub-criterion is that $p^k = 1 [q]$ implies that k is an integer that is greater than or equal to 30. The number k is known as the embedding degree of the curve considered.

According to a third sub-criterion, the elliptic curve is not susceptible to an attack using endomorphisms derived from complex multiplication. For example, an expression of the third sub-criterion is to require that the discriminant be greater than a threshold value. The term 'discriminant', is understood herein to refer to the absolute value of the square-free part of $((p+1-q)^2 - 4p)$.

According to a third sub-criterion, the elliptic curve is not susceptible to an attack which consists of injecting a fault into the execution of the computation in order to force the computation to converge towards the "twist" curve of the initial curve. The equation of the "twist" curve is given by:

$$dY^2 = X^3 + aX + b \mod p$$

where d is an element of the finite field $\mathbb{F}_p$ that does not admit a square root.

By way of a variant, the preceding security criterion is considered fulfilled upon any combination of the sub-criteria previously mentioned above being satisfied by the values of the modulus p , of the first coefficient a , of the second coefficient b , and of the order q .

According to one variant, the compliancy testing step involves the prime factorization or factoring of a first number into prime numbers in order to verify compliance with at least one criterion. According to one variant, the prime factorization may be carried out only on the set of prime factors that are lower than a threshold value, with the criterion being satisfied when the quotient obtained by dividing the first number by the product of the set of prime factors that are lower than the threshold value is prime.

For example, in order to test that the order of the twist curve has at least one prime factor that is greater than 2^{100} , to commence all prime factors up to 2^{80} are first extracted by the Elliptic Curve Method (ECM) (also referred to as Lenstra elliptic-curve factorization method). If the residue is prime and satisfies the criterion, the curve is declared to be secure with respect to the criterion, otherwise, if the residue is composite or lower than the threshold, the curve is rejected.

According to the example described, the criterion is satisfied if the set of the following sub-criteria is satisfied:

- the modulus p is a prime number and is comprised between 2^{l-1} and 2^l ;

- the order q is a prime number and is comprised between 2^{l-1} and 2^l ;
- the degree of embedding of the curve and the degree of embedding of the twist curve are greater than 2^{100} ;
- the order of the twist curve has at least one prime factor that is greater than 2^{100} ; and
- the discriminant of the curve is greater than 2^{100} .

As can be seen in Figure 2, two cases exist and are represented schematically by the arrows 64 and 66.

According to the arrow 64, the values of the modulus p , of the first coefficient a , of the second coefficient b , and of the order q are not in compliance with the criterion.

In this case, the value of the counter is incremented by the adding of an integer.

For example, the integer is equal to 1.

The phase of computation 60 and the phase of testing 62 are then iterated.

According to the arrow 66, the values of the modulus p , of the first coefficient a , of the second coefficient b , and of the order q are in compliance with the criterion.

In this case, parameters are generated, the parameters being such that the values of the modulus p , of the first coefficient a , of the second coefficient b , and of the order q are those values of the modulus p , of the first coefficient a , of the second coefficient b , and of the order q that are in compliance with the criterion.

Otherwise formulated, the phase of computation 60 and the phase of testing 62 are iterated as long as the values of the modulus p , of the first coefficient a , of the second coefficient b , and of the order q are not in compliance with the criterion.

The parameters generated at the conclusion of the generation method are the first values of the modulus p , of the first coefficient a , of the second coefficient b , and of the order q that satisfy the criterion.

Once the modulus p , the first coefficient a , the second coefficient b , and the order q have been generated by means of the preceding method, the base point may be selected so as to be the point having co-ordinates (x, y) of the curve for the abscissa x that is smallest and for even ordinate y such that the order of the point having co-ordinates (x, y) is q .

Preferably, the point is selected in a non-arbitrary manner.

The Applicant has carried out tests showing that the computation converges with the order of a few times l^2 iterations. Several curves have been generated thanks to this method, and for different levels of security. This validates the method.

The method makes it possible to generate multiple secure elliptic curves in a manner that is proven to be completely rigid.

In addition, the curves are connected to a text which makes it possible to authenticate the curve, which provides the ability to easily envisage a periodic change of the curves, for example by a periodic change of the text.

In the case illustrated, the periodic change is applied to the data relating to the date.

This also makes it possible to avoid replay thereof. This signifies that an attacker is not able to force updating with an obsolete curve (being passed for legitimate), since they do not control the date, which is derived from a trusted clock.

In addition, the uniqueness obtained by the generation makes possible the compression of the transmission of parameters, such that it is sufficient to transmit the value of the counter and the value of the order q in order to obtain the elliptic curve.

This appears schematically in the second space $E2$ of Figure 2 (the space $E1$ corresponding to the generation space).

In the step 68, the value of the counter and the value of the order q are transmitted.

In the step 70, the text is provided.

As is schematically illustrated in the steps 72 and 74, the same steps as in the construction are reapplied, except that here the right value of the counter is known. Thus, the operations $O1$, $O2$ and $O3$ are applied so as to obtain intermediate results in the step 72, then the cryptographic hash functions $H1$, $H2$ and $H3$ are applied to the intermediate results so as to obtain the modulus p , the first coefficient a and the second coefficient b .

The transmission is thus easier since only the value of the counter and the value of the order q are transmitted. It should be noted that the transmission of q simply prevents the receiver from recomputing the order of the curve (which would not be reasonable).

In addition, according to a more developed embodiment, it is sufficient to transmit, in addition to the value of the counter, the trace of the curve defined as the quantity $(p+1-q)$, over only $1/2$ bits.

In fact, by exploiting the Hasse bound, it appears that the difference between $(p+1)$ and q is bounded in absolute value by twice the root of p . Thus, the value of the counter makes it possible to obtain the modulus p , and the $1/2$ bits of the trace make it possible to deduce all the bits of the order q .

Such an embodiment includes the transmission of the entirety of the parameters of curves from the designer to the user in $l/2 + 48$ bits, with l being the length in bits of the order q and 48 being the number of bits associated with the value of the counter.

5 It is possible for the elliptic curve thus generated via the generation of parameters to be used for multiple cryptographic applications, such as radio stations or locating-tracking systems.

Each of the proposed methods can be operationally implemented by making use of any computer or any other type of device. Multiple systems may be used with programs that effectively implement the above methods but it is also possible to envisage the use of
10 devices dedicated to the operational implementation of the above-noted methods, it being possible for the latter to be inserted in the devices that are capable of measuring the data provided. In addition, the proposed embodiments are not linked to a particular programming language. Incidentally, this implies that multiple programming languages may be used in order to operationally implement one of the previously detailed methods.

15 In addition, the proposed method is usable for any type of cryptographic protocol based on at least one random parameter.

More precisely, the proposed method is applicable for the generation of at least one parameter characterizing a cryptographic protocol.

20 In such a case, the method includes the step of selection, the step of initialization, a step of obtaining a value for each parameter characterizing the cryptographic protocol and the step of testing.

For at least one parameter, the value obtaining step comprises the effective implementation of a step of computing an operation applied to the text and the value of the counter, so as to obtain a result, and of application of a cryptographic hash function to the
25 result so as to obtain a value for the parameter, the operation and the cryptographic hash function being specific to the said at least one parameter.

Several particular examples of such a use of the method are described the following section.

30 For example, the method is applicable also for generating curves presented in various models other than the Weierstrass model, and requiring one or more random constants. For example, the method is used for generating curves in the form of Edwards -, Jacobi -, Montgomery -, or Hessiennes curves. Typically, in the Edwards formulation, instead of generating the two coefficients a and b , a single coefficient is generated that is usually denoted by d according to which an elliptic curve is written in the
35 form $x^2 + y^2 = 1 + d \cdot x^2 \cdot y^2$.

According to another example, the method is applied for the generation of parameters characterizing curves belonging to a family parameterized by one or more random elements. By way of illustration, the curves of the Barreto-Naehrig family are generated by the evaluation of several polynomials in a single random variable, the variable being obtained by effectively implementing the method.

According to yet another example, the method is applied to a quantum key exchange protocol such as the protocol described by the authors Bos, Costello, Naehrig and Stebila in the document entitled "*Post-quantum key exchange for the TLS protocol from the ring learning with errors problem*" deriving from the conference proceedings of the IEEE Symposium on Security and Privacy (S & P) 2015. Such a protocol implies a constant a , in respect to which it must be possible to provide proof that the generation was not dictated by malicious intentions.

The methods and embodiments described here above are capable of being combined with one another, in whole or in part, in order to give rise to other embodiments of the invention.

CLAIMS

1.- A method for generating at least one parameter, the said at least one parameter characterizing a cryptographic protocol, the method including at least the following steps of:

5

- selecting a text;
- initializing the value of a counter to an initial value;
- for each parameter, obtaining a value for the parameter, at least one value for the parameter being obtained by means of effectively implementing the following steps of:

10

- computing an operation applied to the text and the value of the counter, so as to obtain a result,
- applying a cryptographic hash function to the result so as to obtain a value for the parameter, the operation and the cryptographic hash function being specific to the said at least one parameter;

15

- testing the compliancy of each parameter value obtained with at least one criterion;

when at least one value does not comply with the said at least one criterion, incrementing the value of the counter by adding of an integer, and of iteration for iterating the steps of obtaining and testing; and

20

when each value is in compliance with the criterion, generating the parameters such that the value of each parameter is the value which complies with the said at least one criterion.

25

2.- The method according to claim 1, wherein the cryptographic protocol is selected from the group constituted of an elliptic curve, a curve belonging to a family of curves parameterized by at least one parameter and a key exchange protocol.

30

3.- the method for generating according to claim 1, wherein the parameters are the parameters of an elliptic curve, the parameters being a modulus (p), a first coefficient (d), and an order (q), wherein:

- a value for the modulus (p) is obtained by implementing a step of computing a first operation (O_1) applied to the text and the value of the counter, so as to obtain a first result (R1), and a step of applying a first cryptographic hash function (H1) to the first result (R1) so as to obtain the value for the modulus (p);

- a value for the first coefficient (d) is obtained by implementing a step of computing a second operation (O_2) applied to the text and the value of the counter, so as to obtain a second result (R2), and a step of applying a second cryptographic hash function (H2) to the second result (R2) so as to obtain the value for the first coefficient (d);
5 and

- a value for the order (q) is obtained by implementing a step for determining based on the values of the modulus (p) and of the first coefficient (d),
each operation (O_1 , O_2) preferably including a concatenation of the text.

10 4.- The method for generating according to claim 1, wherein the parameters are the parameters of an elliptic curve, the parameters being a modulus (p), a first coefficient (a), a second coefficient (b), and an order (q), in which:

- a value for the modulus (p) is obtained by implementing a step of computing a first operation (O_1) applied to the text and the value of the counter, so as to obtain a first
15 result (R1), and a step of applying a first cryptographic hash function (H1) to the first result (R1) so as to obtain the value for the modulus (p);

- a value for the first coefficient (a) is obtained by implementing a step of computing a second operation (O_2) applied to the text and the value of the counter, so as to obtain a second result (R2), and a step of applying a second cryptographic hash
20 function (H2) to the second result (R2) so as to obtain the value for the first coefficient (a);

- a value for the first coefficient (a) is obtained by effectively implementing a computation step of computing a third operation (O_3) applied to the text and the value of the counter, so as to obtain a third result (R3), and an application step of applying a third
25 cryptographic hash function (H3) to the third result (R3) so as to obtain a value for the second coefficient (b); and

- a value for the order (q) is obtained by implementing a step for determining, based on the values of the modulus (p), of the first coefficient (a), and of the second coefficient (b),

each operation (O_1 , O_2 , O_3) preferably including a concatenation of the text.

30

5.- The method according to any one of claims 1 to 4, wherein the text satisfies at least one of the following properties:

- a first property according to which the text comprises of more than 16 characters;
- a second property according to which the text includes a date.

35

6.- The method according to any one of claims 1 to 5, wherein, in the step of testing of compliancy, a factoring of a first number into prime numbers is carried out in order to verify compliance with at least one criterion, the factoring being carried out over the set of all prime factors that are lower than a threshold value, with the criterion being satisfied when the quotient obtained by dividing the first number by the product of the set of prime factors that are lower than the threshold value is prime.

7.- A method for transmitting an elliptic curve, the elliptic curve being characterized by the parameters generated by the method for generating according to claim 3 or 4, in which the transmission method includes only either the transmission of the value of the counter and the value of the order (q), or the transmission of the value of the counter and the value of the trace of the curve given by the difference between the modulus (p) and the order (q) to which is added the number 1.

8.- A method for encryption or decryption by using a cryptographic protocol, the cryptographic protocol being characterized by the parameters generated by the method for generating according to any one of claims 1 to 6.

9.- A computer program product comprising a readable information storage medium, on which is stored a computer program comprising of program instructions the computer program being loadable on to a data processing unit and adapted to lead to the carrying out of a method according to any one of claims 1 to 8 when the computer program is carried out on the data processing unit.

10.- A readable information storage medium on which is stored a computer program comprising program instructions, the computer program being loadable onto a data processing unit and adapted to lead to the carrying out of a method according to any one of claims 1 to 8 when the computer program is carried out on the data processing unit.