

Method and apparatus for generating parameter(s) of an asymmetric cryptographic protocol from a blockchain, encryption or decryption method and apparatus and computer program therefor

The present invention relates to a method for generating at least one parameter characterizing a cryptographic protocol, the method being implemented by an electronic device. The invention also relates to an encryption or decryption method using a cryptographic protocol, the cryptographic protocol being characterized by at least one parameter generated via such a generating method.

The invention also relates to a program including software instructions which, when executed by a computer, carry out such a generating method or such an encryption or decryption method.

The invention also relates to an electronic device for generating at least one parameter characterizing a cryptographic protocol. The invention also relates to an electronic encryption or decryption apparatus using a cryptographic protocol, the cryptographic protocol being characterized by at least one parameter generated via such an electronic generating device.

The invention relates to the field of cryptography. Cryptography is divided into two separate parts: symmetrical cryptography and asymmetrical cryptography.

Asymmetrical cryptography makes it possible to carry out protocols for exchanging keys or electronic signatures. RSA encryption (named for the initials of its three inventors) is an asymmetrical cryptography algorithm that is slow and greedy in terms of computing time.

In particular to resolve such a drawback, cryptographic protocols, such as elliptic curves, have been developed for exchange protocols. In fact, elliptic curves are interesting for cryptography due to the existence on the $(E(\mathbb{F}_p), +)$ group of a law of addition and multiplication by a scalar. The law of multiplication by a scalar defines the so-called problem of the discrete logarithm on elliptic curves, consisting of finding the scalar k from $[k]P$ and P . This problem is difficult to solve from a calculation perspective, i.e., its resolution is not polynomial in the size of the elements.

To ensure that the problem is actually difficult, the cryptographic protocol, such as the considered elliptic curve, should be considered safe.

A cryptographic protocol, such as an elliptic curve, is considered to be safe if the cryptographic protocol is insensitive to at least one attack from among a generic attack of the Pollard's rho type, a transfer-type attack, an attack using endomorphisms derived from

complex multiplication, and a twist curve attack. The cryptographic protocol is considered rigid, if the method for generating the parameter(s) characterizing this protocol is completely explicit and does not include any arbitrary step. Generating at least one parameter characterizing a cryptographic protocol considered to be safe is therefore difficult

Document FR 3,053,862 A1 describes such a method for generating at least one parameter characterizing a cryptographic protocol, where the cryptographic protocol is considered to be safe.

This generating method comprises choosing a text and initializing the value of a counter at an initial value. It next comprises, for each parameter, obtaining a value of the parameter, by calculating an operation applied on the text and the value of the counter to obtain a result, then applying a cryptographic hash function on the result to obtain a value of the parameter, the operation and the cryptographic hash function being specific to said parameter.

However, this generating method requires an approval phase between each user and the designer of the cryptographic protocol. Indeed, users could contest the choice of the text, the designer being able to iterate the generation of parameters on different texts.

The aim of the invention is therefore to propose a method and an electronic device for generating at least one parameter characterizing a cryptographic protocol, making it possible to obtain a cryptographic protocol considered to be safe, while avoiding an approval phase between the users and the designer of the cryptographic protocol.

To that end, the invention relates to a method for generating at least one parameter characterizing a cryptographic protocol, the method being implemented by an electronic device, and comprising the following steps:

- selecting a hash contained in a block of an information blockchain, the blockchain including a first block and one or several successive blocks, each block other than the first block being connected to a single preceding block and containing a hash of the preceding block,

- initializing the value of a counter at an initial value,
- for each parameter, obtaining a value for the parameter, at least one value for the parameter being obtained by implementing the following sub-steps:

- + calculating an operation applied at least on the selected hash and the value of the counter, to obtain a result,

+ applying a cryptographic hash function on the result to obtain a value for the parameter, the operation and the cryptographic hash function being specific to said at least one parameter,

- compliance test of each obtained parameter value with at least one compliance criterion,

when at least one value is not compliant with said at least one compliance criterion, incrementing the value of the counter by adding an integer number and iterating the obtaining and test steps, and

when each value is compliant with the compliance criterion, generating parameters such that each parameter has, as value, the value compliant with said at least one compliance criterion.

The hash contained in a block of an information blockchain is a publicly verifiable random variable source, the information blockchain is accessible from a computer network, such as the Internet, and the generating method according to the invention then does not require an approval phase between the designer and the users of the cryptographic protocol.

Furthermore, the fact that each block other than the first block is connected to a single preceding block and contains a hash of the preceding block greatly limits the risks of modification or deletion of a block of the chain, such that each blockchain is considered authentic and secure.

According to other advantageous aspects of the invention, the generating method comprises one or more of the following features, considered alone or according to all technically possible combinations:

- the cryptographic protocol is chosen from among the group consisting of: an elliptic curve, such as an elliptic curve according to standard X9.62; a curve belonging to a family of curves configured by at least one parameter; a key exchange protocol; and a post-quantum cryptographic protocol;

- the compliance criterion is the verification of at least one sub-criterion, preferably several sub-criteria, still more preferably all of the sub-criteria, chosen from the group consisting of:

+ insensitivity of the cryptographic protocol to an attack of the Pollard's rho type;

+ insensitivity of the cryptographic protocol to an attack of the transfer type, such as an insensitivity of the cryptographic protocol to an additive transfer and a multiplicative transfer;

- + insensitivity of the cryptographic protocol to an attack using endomorphisms derived from complex multiplication; and

- + insensitivity of the cryptographic protocol to a twist curve attack;

- the test step includes a factorization of a first number into prime numbers to verify at least one compliance criterion, the factorization being implemented on the set of prime factors below a threshold, the compliance criterion being verified when the quotient of the first number by the product of the set of prime factors below the threshold is prime;

- the method further comprises, before the obtainment step, a step for choosing a text and/or reference date, and during the calculating sub-step during the obtainment step, the operation is applied on the selected hash, the value of the counter and the reference text and/or date, to obtain said result,

the reference date preferably being the date on which the method is carried out;

- the text verifies at least one of the following properties:

- + a first property according to which the text includes more than 16 characters,

- + a second property according to which the text includes a date, such as the reference date;

- the parameters are the parameters of an elliptic curve, the parameters being a module, a first coefficient and an order, in which:

- + a value for the module is obtained by implementing a step for calculating a first operation applied on the selected hash and the value of the counter, to obtain a first result and a step for applying a first cryptographic hash function on the first result to obtain the value for the module,

- + a value for the first coefficient is obtained by implementing a step for calculating a second operation applied on the selected hash and the value of the counter, to obtain a second result and a step for applying a second cryptographic hash function on the second result to obtain the value for the first coefficient, and

- + a value of the order is obtained by implementing a determining step from values of the module and the first coefficient,

each operation preferably including a concatenation of the selected hash and the value of the counter;

- in addition, when the method further comprises, before the obtainment step, a step for choosing a text and/or reference date, the value for the module is obtained by implementing the step for calculating the first operation applied on the selected hash, the value of the counter and the text and/or reference date, and the value for the first

coefficient is obtained by implementing the step for calculating the second operation applied on the selected hash, the value of the counter and the text and/or reference date, each operation preferably including a concatenation of the selected hash, the value of the counter and the text and/or reference date;

- the parameters are the parameters of an elliptic curve, the parameters being a module, a first coefficient, a second coefficient and an order, in which:

+ a value for the module is obtained by implementing a step for calculating a first operation applied on the selected hash and the value of the counter, to obtain a first result and a step for applying a first cryptographic hash function on the first result to obtain the value for the module,

+ a value for the first coefficient is obtained by implementing a step for calculating a second operation applied on the selected hash and the value of the counter, to obtain a second result and a step for applying a second cryptographic hash function on the second result to obtain the value for the first coefficient,

+ a value for the second coefficient is obtained by implementing a step for calculating a third operation applied on the selected hash and the value of the counter, to obtain a third result and a step for applying a third cryptographic hash function on the third result to obtain a value for the second coefficient, and

- a value of the order is obtained by implementing a determining step from values of the module, the first coefficient and the second coefficient,

each operation preferably including a concatenation of the selected hash and the value of the counter;

- in addition, when the method further comprises, before the obtainment step, a step for choosing a text and/or reference date, the value for the module is obtained by implementing the step for calculating the first operation applied on the selected hash, the value of the counter and the text and/or reference date, the value for the first coefficient is obtained by implementing the step for calculating the second operation applied on the selected hash, the value of the counter and the text and/or reference date, and the value for the second coefficient is obtained by implementing the step for calculating the third operation applied on the selected hash, the value of the counter and the text and/or reference date,

each operation preferably including a concatenation of the selected hash, the value of the counter and the text and/or reference date.

The invention also relates to an encryption or decryption method using a cryptographic protocol, the cryptographic protocol being characterized by at least one parameter generated via a generating method as defined above.

The invention also relates to a computer program including software instructions which, when executed by a computer, implement a generating method as defined above or an encryption or decryption method as defined above.

The invention also relates to an electronic device for generating at least one parameter characterizing a cryptographic protocol, the device comprising:

- a selection module configured to select a hash contained in a block of an information blockchain, the blockchain including a first block and one or several successive blocks, each block other than the first block being connected to a single preceding block and containing a hash of the preceding block,

- an initialization module configured to initialize the value of a counter at an initial value,

- an obtainment module configured to obtain a value for each parameter, at least one value for the parameter being obtained by:

- + calculating an operation applied at least on the selected hash and the value of the counter, to obtain a result,

- + applying a cryptographic hash function on the result to obtain a value for the parameter, the operation and the cryptographic hash function being specific to said at least one parameter,

- a test module configured to test the compliance of each obtained parameter value with at least one compliance criterion,

- an incrementation module configured in order, when at least one value is not compliant with said at least one compliance criterion, to increment the value of the counter by adding an integer number and iterating an implementation of the obtainment and test modules, and

- a generating module configured in order, when each value is compliant with the compliance criterion, to generate parameters such that each parameter has, as value, the value compliant with said at least one compliance criterion.

The invention also relates to an electronic encryption or decryption device using a cryptographic protocol, the cryptographic protocol being characterized by at least one parameter generated via an electronic generating device as defined above.

These features and advantages of the invention will appear more clearly upon reading the following description, provided solely as a non-limiting example, and done in reference to the appended drawings, in which:

- figure 1 is a schematic illustration of an electronic device, according to the invention, for generating at least one parameter characterizing a cryptographic protocol

and an electronic encryption or decryption apparatus next using said cryptographic protocol; and

- figure 2 is a schematic illustration of a flowchart of a method, according to the invention, for generating at least one parameter characterizing a cryptographic protocol, then a method for transmitting the parameter(s) for the use of said cryptographic protocol by an encryption or decryption method.

In figure 1, an electronic encryption or decryption apparatus 5 is configured to encrypt or decrypt a message by using a cryptographic protocol, the cryptographic protocol being characterized by at least one parameter generated via an electronic generating device 10.

The electronic generating device 10 is configured to generate at least one parameter characterizing a cryptographic protocol.

The cryptographic protocol is in general any type of cryptographic protocol based on at least one random parameter.

The cryptographic protocol is for example chosen from among the group consisting of: an elliptic curve, such as an elliptic curve according to standard X9.62; a curve belonging to a family of curves configured by at least one parameter; a key exchange protocol; and a post-quantum cryptographic protocol.

The elliptic curves used in cryptography are generally given in Weierstrass form. All of the points of a finite body $\mathbb{F}_P$ verify the following equation:

$$y^2 = x^3 + A.x + B \mod P \quad (1)$$

where:

- x and y are elements of the finite body $\mathbb{F}_P$,
- P is the modulus,
- A is a first coefficient, and
- B is a second coefficient.

For each of the curves, a set of parameters makes it possible to determine the curve. In the example of equation (1), the parameters are the modulus P, the first coefficient A and the second coefficient B. These three parameters suffice to characterize the elliptic curve.

To be able to exchange information on a so-called public channel, in cryptography, other parameters are also used including the coordinates of the base point of the curve denoted (x, y), the order of the curve Q or the cofactor H. By definition, the cofactor H is the ratio between the order Q and the order of the group created by the base point (x,y); the base point is chosen such that this cofactor is very small.

In a variant, the elliptic curves are shown in forms other than the Weierstrass form, and requiring one or several random constants. For example, the electronic generating device 10 is configured to generate at least one parameter characterizing an elliptic curve in Edwards, Jacobi, Montgomery or Hessiennes form. Typically, in the Edwards
 5 formulation, instead of generating the two coefficients A and B, a single coefficient is generated that is usually denoted D, according to which the elliptic curve is written in the form:

$$x^2 + y^2 = 1 + D \cdot x^2 \cdot y^2 \quad (2)$$

where:

- 10 • x and y are elements of the finite body $\mathbb{F}_p$,
- D is the coefficient.

When the cryptographic protocol is a curve belonging to a family of curves configured by at least one parameter, the curve is for example a curve from the Barreto-Naehrig family. The curves from the Barreto-Naehrig family are generated by evaluating
 15 several polynomials in a single random variable, the variable then being obtained by implementing the generating method.

When the cryptographic protocol is a post-quantum cryptographic protocol, the protocol is for example that described by the authors Bos, Costello, Naehrig and Stebila in the document titled "*Post-quantum key exchange for the TLS protocol from the ring
 20 learning with errors problem*" from the proceedings of the IEEE Symposium on Security and Privacy (S&P) 2015. Such a post-quantum cryptographic protocol involves a constant A, for which it must be possible to prove that the generation was not dictated by malicious intent. The electronic generating device 10 is then configured to generate said constant A. This protocol is also a key exchange protocol.

25 The electronic generating device 10 comprises a selection module 12 configured to select a hash Ha contained in a block of an information blockchain, not shown, and an initialization module 14 configured to initialize a counter C at an initial value.

The electronic generating device 10 comprises an obtainment module 16 configured to obtain a value for each parameter, at least one value for the parameter
 30 being obtained by a calculating operation O applied at least on the selected hash Ha and the value of the counter C, in order to obtain a result, then by applying a cryptographic hash function H on the result to obtain a value for the parameter, the operation O and the cryptographic hash function H being specific to said at least one parameter.

35 The electronic generating device 10 comprises a test module 18 configured to test the compliance of each obtained parameter value with at least one compliance criterion.

The electronic generating device 10 comprises an incrementation module 20 configured in order, when at least one value is not compliant with said at least one compliance criterion, to increment the value of the counter C by adding an integer number and iterating an implementation of the obtainment 16 and test 18 modules; and a
 5 generating module 22 configured in order, when each value is compliant with the compliance criterion, for generating parameters such that each parameter has, as value, the value compliant with said at least one compliance criterion.

An optional addition, the electronic generating device 10 comprises a choosing module 22 configured in order, before the implementation of the obtainment module 16, to
 10 choose a text T and/or reference date D. During the implementation of the obtainment module 16, the operation O is then applied on the selected hash H, the value of the counter C, as well as the text T and/or reference date D, in order to obtain said result. The reference date D is preferably the date on which the generation of said at least one parameter characterizing the cryptographic protocol is implemented.

15 In the example of figure 1, the electronic generating device 10 comprises an information processing unit 30, for example made up of a memory 32 and a processor 34 associated with the memory 32. In this example, it further comprises input/output means 36, such as a keyboard and/or a mouse, and optionally a display screen 38.

In the example of figure 1, the selection module 12, the initialization module 14, the
 20 obtainment module 16, the test module 18, the incrementation module 20 and the generating module 22, as well as, by way of optional addition, the choosing module 24, are each made in the form of software executable by the processor 34. The memory 32 of the information processing unit 30 is then able to store selection software configured to select the hash Ha contained in the block of the information blockchain; initialization
 25 software configured to initialize the value of a counter C at an initial value; obtainment software configured to obtain the value for each parameter, at least one value for the parameter being obtained by calculating the operation O applied at least on the selected hash Ha and the value of the counter C, to obtain the result, then by applying the cryptographic hash function H on the result in order to obtain the value for the parameter,
 30 the operation O and the cryptographic hash function H being specific to said at least one parameter. The memory 32 of the information processing unit 30 is able to store test software configured to test the compliance of each obtained parameter value with at least one compliance criterion; incrementation software configured in order, when at least one value is not compliant with said at least one compliance criterion, to increment the value of
 35 the counter C by adding an integer number and iterating an implementation of the obtainment and test software; and generating software configured in order, when each

value is compliant with the compliance criterion, to generate parameters such that each parameter has, as value, the value compliant with said at least one compliance criterion. An optional addition, the memory 32 of the information processing unit 30 is able to store choosing software configured in order, before the implementation of the obtainment software, to choose the text T and/or reference date D. During the implementation of the obtainment software, the operation O is then applied on the selected hash H, the value of the counter C, as well as the text T and/or reference date D, in order to obtain said result. The processor 34 is then able to execute the selection software, the initialization software, the obtainment software, the test software, the incrementation software and the generating software, as well as, by way of optional addition, the choosing software.

In a variant that is not shown, the selection module 12 the initialization module 14, the obtainment module 16, the test module 18, the incrementation module 20 and the generating module 22, as well as, optionally and additionally, the choosing module 24, are each made in the form of a programmable logic component, such as an FPGA (Field Programmable Gate Array), or in the form of a dedicated integrated circuit, such as an ASIC (Applications Specific Integrated Circuit).

When the electronic generating device 10 is made in the form of one or several software programs, i.e., in the form of a computer program, it is further able to be stored on a medium, not shown, readable by computer. The computer-readable medium is for example a medium suitable for storing electronic instructions and able to be coupled with a bus of a computer system. As an example, the readable medium is an optical disc, a magnetic-optical disc, a ROM memory, a RAM memory, any type of non-volatile memory (for example, EPROM, EEPROM, FLASH, NVRAM), a magnetic card or an optical card. A computer program including software instructions is then stored on the readable medium.

The selection module 12 is configured to select the hash H_a contained in a respective block of the blockchain, said block containing the hash H_a being any block of the blockchain. In other words, the selected hash H_a is an element that cannot be predicted by a person other than the designer, in particular by the user, and in general by a third party.

As an optional addition, the selection module 12 is configured to select several hashes H_a , each one being contained in a respective block of a corresponding blockchain.

Each blockchain includes a first block and one or several successive blocks, each block other than the first block being connected to a single preceding block and containing a hash of the preceding block.

Each information blockchain is accessible from a computer network, in particular from the Internet, and the value of the hash used to generate the parameters characterizing the cryptographic protocol is then easily verifiable by a user of said protocol, and in general by a third party. Each selected hash is then a publicly verifiable random variable source.

Each information blockchain is preferably a blockchain associated with a cybercurrency, also called cryptocurrency, like the Bitcoin cybercurrency, the Ether cybercurrency, etc. As an example, for the blockchain associated with the Bitcoin cybercurrency, each hash is contained in a field called BlockHash, and the hash function used to calculate each hash of a preceding block is an algorithm of the SHA (Secure Hash Algorithm) type, in particular the SHA-256 algorithm. For the blockchain associated with the Ether cybercurrency, each hash is contained in a field called MixHash, and the hash function used to calculate each hash of a preceding block is an Ethash algorithm, based on an algorithm of the SHA type, in particular the SHA-3 algorithm.

The initialization module 14 is configured to initialize the counter C at an initial value, for example the value 1.

The obtainment module 16 is configured to obtain a value for each parameter, by calculating the operation O applied at least on the selected hash Ha and the value of the counter C, and as an optional addition on the text T and/or the date D, in order to obtain the result R, then by applying the cryptographic hash function H on the result R to obtain a value for the parameter.

The operation O applied on the selected hash Ha and the value of the counter C, or even applied simultaneously on the selected hash Ha, the value of the counter C, the text T and/or the date D, is a bijective operation.

The applied operation O is preferably a concatenation, i.e., a concatenation of the selected hash Ha and the value of the counter C, or even also of the text T and/or the date. A concatenation consists of placing two character chains end to end, such as the character chain corresponding to the selected hash Ha and that corresponding to the value of the counter C. In a variant, the applied operation O is a multiplication, or even an addition.

The entity on which said operation O is applied in order to obtain the result R is also called seed. In other words, the seed includes the selected hash Ha and the value of the counter C. As an optional addition, the seed includes one or several selected hashes Ha, the value of the counter C, the text T and/or the date D.

The cryptographic hash function H next applied on the result R in order to obtain a value of the parameter is for example an algorithm of type SHA, such as one of algorithms SHA-256, SHA-384, SHA-512, SHA-512/256 and SHA-512/224, or algorithm SHA-3.

5 The test module 18 is configured to test the compliance of each obtained parameter value with at least one compliance criterion.

The compliance criterion is for example the verification of at least one sub-criterion chosen from the group consisting of:

- insensitivity of the cryptographic protocol to an attack of the Pollard's rho type;
- insensitivity of the cryptographic protocol to an attack of the transfer type, such
- 10 as an insensitivity of the cryptographic protocol to an additive transfer and a multiplicative transfer;
- insensitivity of the cryptographic protocol to an attack using endomorphisms derived from complex multiplication; and
- insensitivity of the cryptographic protocol to a twist curve attack.

15 The compliance criterion is preferably the verification of several sub-criteria from the group defined above, still more preferably the verification of each of the sub-criteria from said group.

In other words, the test module 18 is preferably configured to verify whether the cryptographic protocol characterized by the obtained parameter value(s) is insensitive to

20 the Pollard's rho-type attack, the transfer attack, the attack using endomorphisms from the complex multiplication, or the twist curve attack, preferably insensitive to several of these attacks, still more preferably insensitive to each of these attacks.

In a variant or additionally, the test module 18 is configured to factor a first number into prime numbers to verify at least one compliance criterion, the factorization being

25 implemented on the set of prime factors below a threshold, the compliance criterion then being verified when the quotient of the first number by the product of the set of prime factors below the threshold is prime.

At the end of the test implemented by the test module 18, when at least one value is not compliant with said at least one compliance criterion, the incrementation module 20

30 is configured to increment the value of the counter C by adding an integer number, such as the integer number equal to 1, and iterating an implementation of the obtainment 16 and test 18 modules.

Otherwise, when each value is compliant with the compliance criterion, the generating module 22 is configured to generate the parameter(s) characterizing the

35 cryptographic protocol, such that each parameter has, as value, the value compliant with said at least one compliance criterion.

As an optional addition, the choosing module 22 is configured to choose the text T and/or the reference date D to be further included in the seed. The chosen text T preferably includes more than 16 characters. The text T is for example a proprietary text of the person generating the parameters, for example, an excerpt from a license for a product sold by this person.

In order to improve the rigidity of the proposed process, it is recommended that the chosen text T be intelligible and make it possible to identify the party claiming ownership thereof or the usage context.

In a variant or additionally, the seed also includes data relative to the implementation date of the method. The seed then includes the reference date D chosen via the choosing module 22, the reference date D preferably being the date on which the generating method is implemented.

As another optional addition, the choosing module 22 is configured to concatenate part of the text T and the reference date D. According to another example, the text T itself includes the reference date D. As an illustration, this text is "*This curve was generated on such a date*".

The operation of the electronic generating device 10 according to the invention will now be explained in light of figure 2 showing a flowchart of the generating method according to the invention, followed by a transmission of the parameter(s) for the use of said cryptographic protocol by an encryption or decryption method.

The generating method includes an initial phase 50 for providing the seed, the provision phase 50 including a step 52 for selecting one or several hashes H_a , each one being contained in a respective block of a corresponding blockchain, a step 54 for initializing the counter C at an initial value, such as the value 1, as well as an optional step 56, then shown in dotted lines in figure 2, for choosing the text T and/or the reference date D to further be included in the seed.

After the initial provision phase 50, the generating method includes a step 60 for obtaining at least one value for each parameter, via the implementation, for each parameter, of the following sub-steps, not shown:

- + calculating the operation O applied on the seed including the selected hash H_a and the value of the counter C, to obtain the result R,

- + applying the cryptographic hash function H on the result R to obtain a value for the parameter, the operation O and the cryptographic hash function H being specific to said at least one parameter.

As an example, in order to generate three separate parameters characterizing the cryptographic protocol, such as the modulus P, the first coefficient A and the second

coefficient B characterizing a respective elliptic curve, the obtainment step 60 includes three calculating sub-steps and three application sub-steps.

In the first calculating sub-step, a first operation O_1 is applied on the seed, in particular including the selected hash H_a and the value of the counter C , to obtain the first result R_1 . According to the described example, the first operation O_1 is a concatenation of the selected hash H_a , the value of the counter C and a first constant C_1 .

In the second calculating sub-step, a second operation O_2 is applied on the seed, in particular including the selected hash H_a and the value of the counter C , to obtain a second result R_2 different from the first result R_1 . According to the described example, the second operation O_2 is a concatenation of the selected hash H_a , the value of the counter C and a second constant C_2 different from the first constant C_1 .

In the third calculating sub-step, a third operation O_3 is applied on the seed, in particular including the selected hash H_a and the value of the counter C , to obtain the third result R_3 . According to the described example, the third operation O_3 is a concatenation of the selected hash H_a , the value of the counter C and a third constant C_3 different from the first constant C_1 and different from the second constant C_2 .

In each of the described examples, it appears that each operation O_1 , O_2 and O_3 includes a concatenation of the selected hash H_a , the value of the counter C and a constant uniquely specializing each output.

In the first application sub-step, a first cryptographic hash function H_1 is applied on the first result R_1 to obtain a value for the modulus P . In the illustrated case, the obtained value for the modulus P is equal to the value in hexadecimal of the result obtained by application of the first cryptographic hash function H_1 on the first result R_1 .

In the second application sub-step, a second cryptographic hash function H_2 is applied on the second result R_2 to obtain a value for the first coefficient A. According to the illustrated example, the first cryptographic hash function H_1 and the second cryptographic hash function H_2 are identical.

Furthermore, similarly to the first application sub-step, the value obtained for the first coefficient A is equal to the value in hexadecimal of the result obtained by application of the second cryptographic hash function H_2 on the second result R_2 .

In the third application sub-step, a third cryptographic hash function H_3 is applied on the third result R_3 to obtain a value for the second coefficient B. According to the illustrated example, the first cryptographic hash function H_1 and the third cryptographic hash function H_3 are identical.

Furthermore, similarly to the first application sub-step, the value obtained for the second coefficient B is equal to the value in hexadecimal of the result obtained by application of the third cryptographic hash function H_3 on the third result R_3 .

During a complementary determining sub-step, included in the obtainment step 60, the value is determined of the order Q corresponding to the values of the modulus P, the first coefficient A and the second coefficient B.

Such a value of the order Q is determined, for example, by using Schoof's algorithm or its version improved by Wilkies and Atkin, also called SEA algorithm.

The generating method includes, after the obtaining step 60, a step 62 for testing the compliance of each parameter value obtained with at least one compliance criterion, i.e., in the example described above, a test of the compliance of the values of the modulus P, the first coefficient A, the second coefficient B and the order Q.

The values of the modulus P, the first coefficient A, the second coefficient B and the order Q are considered to be compliant if the values of the modulus P, the first coefficient A, the second coefficient B and the order Q verify at least one compliance criterion.

For example, the compliance criterion is chosen so that the cryptographic protocol, such as the elliptic curve obtained from values of the modulus P, the first coefficient A, the second coefficient B and the order Q, is secure.

As an example, the preceding security requirement is fulfilled once the parameter(s) of the cryptographic protocol, such as the values of the modulus P, the first coefficient A, the second coefficient B and the order Q for the elliptic curve in Weierstrass form, verify one or several sub-criteria described hereinafter, and preferably each of these sub-criteria.

According to a first sub-criterion, the cryptographic protocol, such as the elliptic curve, is not sensitive to a Pollard's rho attack.

For example, according to the first sub-criterion, the size of the sub-group Q is greater than two times the security level.

The security level depends on the targeted application and constitutes an objective to be achieved. Concretely, the security level corresponds to the algorithm of the minimum number of operations that must be carried out to break the system. As an example, for civilian applications, 128 bits of security is recommended.

According to a second sub-criterion, the cryptographic protocol, such as the elliptic curve, is not sensitive to an additive transfer and a multiplicative transfer. For example, an expression of the second sub-criterion is that $P^k = 1 [Q]$ means that k is an integer greater than or equal to 30. The number k is called degree of embedding of the considered curve.

According to a third sub-criterion, the cryptographic protocol, such as the elliptic curve, is not sensitive to an attack using endomorphisms from multiplication. For example, one expression of the third sub-criterion is to require that the discriminant be above a threshold value. A discriminant here refers to the absolute value of the part without square factors of $((P+1-Q)^2-4*P)$.

According to a fourth sub-criterion, the cryptographic protocol, such as the elliptic curve, is not sensitive to an attack that consists of injecting a fault into the execution of the calculation to force the calculation to converge toward the twist curve of the initial curve. The twist curve equation is given by:

$$D.y^2 = x^3 + A.x + B \mod P \quad (1)$$

where:

- D is an element of the finite body $\mathbb{F}_p$ not allowing a square root,
- x and y are elements of the finite body $\mathbb{F}_p$,
- P is the modulus,
- A is a first coefficient, and
- B is a second coefficient.

In a variant, the preceding security requirement is fulfilled once the parameter(s) of the cryptographic protocol, such as the values of the modulus P, the first coefficient A, the second coefficient B and the order Q for the elliptic curve in Weierstrass form, verify any combination of the sub-criteria previously mentioned.

In a variant or additionally, the compliance test step involves factoring a first number into prime numbers to verify at least one criterion. The factorization is implemented on the set of prime factors below a threshold, the associated compliance criterion being verified when the quotient of the first number by the product of the set of prime factors below the threshold is prime.

For example, to test that the order of the twist curve includes at least one prime factor greater than 2^{100} , one begins by extracting all of the prime factors up to 2^{80} using the ECM method (also called Lenstra factorization for elliptic curves). If the remainder is prime and verifies the compliance criterion, the curve is declared secure with respect to the criterion; otherwise, if the remainder is composite or below the threshold, the curve is rejected.

According to the described example, the compliance criterion is verified if all of the following sub-criteria are met:

- the modulus P is a prime number, and is between 2^{L-1} and 2^L ;
- the order Q is a prime number, and is between 2^{L-1} and 2^L ;

- the degree of embedment of the curve and the degree of embedment of the twist curve are greater than 2^{100} ;
- the order of the twist curve includes at least one prime factor greater than 2^{100} , and
- the discriminant of the curve is greater than 2^{100} .

When, at the end of the test step 62, at least one obtained parameter value is not compliant with said at least one compliance criterion, the generating method comprises a step (shown by the arrow 64) for incrementing the value of the counter C by adding an integer number, like the integer number equal to 1, and iterating the obtainment 60 and test 62 steps.

When, at the end of the test step 62, each obtained parameter value is compliant with the compliance criterion, the generating method then comprises a step (shown by the arrow 66) for generating parameters such that each parameter has, as value, the value compliant with said at least one compliance criterion.

In other words, the obtainment 60 and test 62 steps are iterated as long as the obtained value(s) of parameter(s) of the cryptographic protocol are not compliant with the compliance criterion.

In other words, the parameter(s) generated at the end of the generating method are the first values of said parameter(s) verifying the compliance criterion.

Once the parameter(s) of the cryptographic protocol, such as the modulus P, the first coefficient A, the second coefficient B and the order Q, generated by the generating method according to the invention, the base point is able to be chosen as being the point with coordinates (x,y) of the curve with the smallest x-axis and even y-axis such that the order of the point with coordinates (x,y) is q. Preferably, the point is not chosen arbitrarily.

Performed tests show that the calculation converges with the order of several times L^2 iterations. Several curves have thus been generated using this generating method according to the invention, and for different security levels.

The generating method then makes it possible to generate multiple cryptographic protocols, such as elliptic curves, secure in a manner proven to be completely rigid, while not requiring an approval phase among the users and the designer of the cryptographic protocol.

Furthermore, the cryptographic protocols are connected to the hash or hashes Ha, or even to the text T, which makes it possible to authenticate the cryptographic protocol, which makes it easily possible to consider a periodic change of cryptographic protocols, for example by a periodic change of at least one hash Ha and/or of the text T.

Also additionally, the periodic change is for example applied via a periodic change of the reference date D . This also makes it possible to avoid replay thereof. This means that an attacker cannot force the update with an obsolete protocol (passed off as legitimate), since he does not control the reference date D , which is derived from a trusted clock.

Furthermore, the uniqueness obtained by the generation makes it possible to compress the transmission of the parameters, such that it for example suffices to transmit the value of the counter C and the value of the order Q to obtain the elliptic curve.

This appears schematically in a second area $E2$ of figure 2, associated with the use of the parameter(s) generated by the generating method according to the invention, a first area $E1$ associated with steps 50 to 66 corresponding to the generation of the parameter(s).

During a step 68, the value of the counter C and the value of the order Q are sent to the user.

In step 70, the selected hash or hashes H_a , or even as an optional addition the text T and/or the reference date D , are provided.

As illustrated schematically by steps 72 and 74, the same steps are reapplied as during construction, except that here the correct value of the counter C is known. Thus, each operation O , such as the operations O_1 , O_2 and O_3 in the example of the parameters P , A and B of the elliptic curve, is applied to obtain intermediate results R in step 72, then each cryptographic hash function H , like the cryptographic hash functions H_1 , H_2 and H_3 in the example of the parameters P , A and B of the elliptic curve, is applied to the respective intermediate result R to obtain, in step 74, the corresponding parameter of the cryptographic protocol, such as the modulus P , the first coefficient A and the second coefficient B of the elliptic curve.

The transmission is thus easier, since only the value of the counter C and the value of the order Q are sent. It should be noted that the transmission of the order Q simply prevents the user from recalculating the order of the curve.

Furthermore, according to a more elaborate variant, it suffices to send, in addition to the value of the counter C , the trace of the curve defined as the quantity $(P+1-Q)$, over only $L/2$ bits.

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

According to this variant, the transmission of all of the parameters of the cryptographic protocol from the designer to the user requires only $L/2 + 48$ bits, L being the length in bits of the order Q and 48 the number of bits associated with the value of the counter C .

5 The cryptographic protocol thus determined via the generation of the parameter(s) characterizing it is usable for multiple cryptographic applications, such as radio sets, tracking systems or geolocation receivers.

10 One can thus see that the electronic generating device 10 and the generating method according to the invention make it possible to obtain a cryptographic protocol considered to be safe, while not requiring an approval phase between the user and the designer of the cryptographic protocol.

20
CLAIMS

1. A method for generating at least one parameter (P, A, B) characterizing a cryptographic protocol, the method being implemented by an electronic device (10), and comprising the following steps:

- selecting (52) a hash (Ha) contained in a block of an information blockchain, the blockchain including a first block and one or several successive blocks, each block other than the first block being connected to a single preceding block and containing a hash of the preceding block,

- initializing (54) the value of a counter (C) at an initial value,
- for each parameter (P, A, B), obtaining (60) a value for the parameter (P, A, B), at least one value for the parameter (P, A, B) being obtained by implementing the following sub-steps:

+ calculating an operation applied at least on the selected hash (Ha) and the value of the counter (C), to obtain a result (R),

+ applying a cryptographic hash function (H) on the result (R) to obtain a value for the parameter (P, A, B), the operation (O) and the cryptographic hash function (H) being specific to said at least one parameter,

- compliance test (62) of each obtained parameter value (P, A, B) with at least one compliance criterion,

when at least one value is not compliant with said at least one compliance criterion, incrementing (64) the value of the counter (C) by adding an integer number and iterating the obtaining and test steps, and

when each value is compliant with the compliance criterion, generating (66) parameters (P, A, B) such that each parameter (P, A, B) has, as value, the value compliant with said at least one compliance criterion.

2.- The method according to claim 1, wherein the cryptographic protocol is chosen from among the group consisting of: an elliptic curve, such as an elliptic curve according to standard X9.62; a curve belonging to a family of curves configured by at least one parameter; a key exchange protocol; and a post-quantum cryptographic protocol.

3.- The method according to claim 1 or 2, wherein the compliance criterion is the verification of at least one sub-criterion, preferably several sub-criteria, still more preferably all of the sub-criteria, chosen from the group consisting of:

- insensitivity of the cryptographic protocol to an attack of the Pollard's rho type;

- insensitivity of the cryptographic protocol to an attack of the transfer type, such as an insensitivity of the cryptographic protocol to an additive transfer and a multiplicative transfer;

- insensitivity of the cryptographic protocol to an attack using endomorphisms derived from complex multiplication; and

- insensitivity of the cryptographic protocol to a twist curve attack.

4.- The method according to claim 1 or 2, wherein, the test step (62) includes a factorization of a first number into prime numbers to verify at least one compliance criterion, the factorization being implemented on the set of prime factors below a threshold, the compliance criterion being verified when the quotient of the first number by the product of the set of prime factors below the threshold is prime.

5.- The method according to any one of the preceding claims, wherein the method further comprises, before the obtainment step, a step (56) for choosing a text (T) and/or reference date (D), and during the calculating sub-step during the obtainment step, the operation (O) is applied on the selected hash (Ha), the value of the counter (C) and the reference text (T) and/or date (D), to obtain said result (R),

the reference date (D) preferably being the date on which the method is carried out.

6.- The method according to claim 5, wherein the text (T) verifies at least one of the following properties:

- a first property according to which the text (T) includes more than 16 characters,

- a second property according to which the text (T) includes a date, such as the reference date (D).

7.- An encryption or decryption method using a cryptographic protocol, the cryptographic protocol being characterized by at least one parameter (P, A, B) generated via such a generating method according to any one of the preceding claims.

8. A computer program comprising software instructions which, when executed by a computer, carry out a method according to any one of the preceding claims.

9. An electronic device (10) for generating at least one parameter (P, A, B) characterizing a cryptographic protocol, the device (10) comprising:

- a selection module (12) configured to select a hash (Ha) contained in a block of an information blockchain, the blockchain including a first block and one or several successive blocks, each block other than the first block being connected to a single preceding block and containing a hash of the preceding block,

5 - an initialization module (14) configured to initialize the value of a counter (C) at an initial value,

 - an obtainment module (16) configured to obtain a value for each parameter (P, A, B), at least one value for the parameter (P, A, B) being obtained by:

 + calculating an operation (O) applied at least on the selected hash (Ha) and the value of the counter (C), to obtain a result (R),

 + applying a cryptographic hash function (H) on the result (R) to obtain a value for the parameter (P, A, B), the operation (O) and the cryptographic hash function (H) being specific to said at least one parameter,

15 - a test module (18) configured to test the compliance of each obtained parameter value (P, A, B) with at least one compliance criterion,

 - an incrementation module (20) configured in order, when at least one value is not compliant with said at least one compliance criterion, to increment the value of the counter (C) by adding an integer number and iterating an implementation of the obtainment (16) and test (18) modules, and

20 - a generating module (22) configured in order, when each value is compliant with the compliance criterion, to generate parameters (P, A, B) such that each parameter (P, A, B) has, as value, the value compliant with said at least one compliance criterion.

25 10.- An electronic encryption or decryption apparatus (5) using a cryptographic protocol, the cryptographic protocol being characterized by at least one parameter (P, A, B) generated via such an electronic generating device (10) according to the preceding claim.