

(51) International Patent Classification:
H04L 9/32 (2006.01)(21) International Application Number:
PCT/IB2014/061557(22) International Filing Date:
20 May 2014 (20.05.2014)

(25) Filing Language: Italian

(26) Publication Language: English

(30) Priority Data:
MO2013A000140 20 May 2013 (20.05.2013) IT(71) Applicants: **UNIVERSITÀ POLITECNICA DELLE MARCHE** [IT/IT]; Via Oberdan, 8, I-60121 Ancona (IT). **UNIVERSITÄT ZÜRICH** [CH/CH]; Prorektorat MNW, Ramistrasse, 71, CH-8006 Zurich (CH).(72) Inventors: **BALDI, Marco**; c/o Università Politecnica delle Marche, Via Oberdan, 8, I-60121 Ancona (IT). **ROSENTHAL, Joachim**; c/o Universität Zurich, Prorektorat MNW, Ramistrasse, 71, CH-8006 Zurich (CH). **SCHIPANI, Davide**; c/o Università Politecnica delle Marche, Via Oberdan, 8, I-60121 Ancona (IT).**CHIARALUCE, Franco**; c/o Università Politecnica delle Marche, Via Oberdan, 8, I-60121 Ancona (IT). **BIANCHI, Marco**; c/o Università Politecnica delle Marche, Via Oberdan, 8, I-60121 Ancona (IT).(74) Agent: **GRANA, Daniele**; c/o Brunacci & Partners S.r.l., Via Scaglia Est, 19-31, I-41126 Modena (IT).

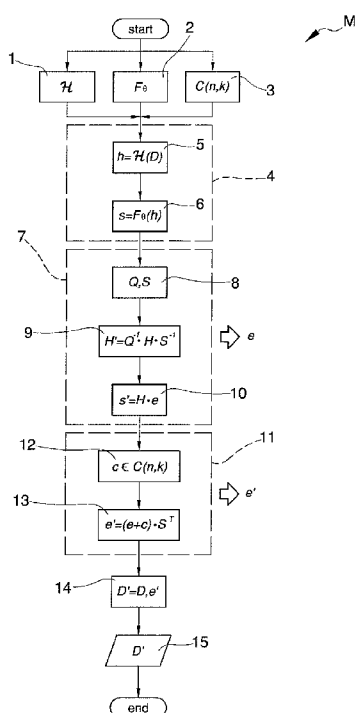
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP,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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR THE DIGITAL SIGNATURE

Fig. 1



(57) Abstract: The method for the digital signature comprises the following steps: - defining a public calculation function (7) suitable for calculating a syndrome vector (s) starting from a digital file (D) to sign; - selecting a private error corrector code (C(n, k)); - calculating the syndrome vector (s) by means of the calculation function (7) and starting from the digital file (D) to sign; - determining an error vector (e) starting from the syndrome vector (s) and by means of the error corrector code (C(n, k)); - determining a digital signature (e') starting from the error vector (e); - associating the digital signature (e') with the digital file (D) to obtain a signed digital file (D'); - wherein the syndrome vector (s) calculated by means of the calculation function (7) is made up of a sparse vector.



EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, **Published:**

LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,

GW, KM, ML, MR, NE, SN, TD, TG).

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

METHOD AND SYSTEM FOR THE DIGITAL SIGNATURE

Technical Field

The present invention relates to a method and a system for the digital signature.

Background Art

- 5 Two main systems are known for digital signature based on codes: the Kabatianskii-Krouk-Smeets (KKS) system and the Courtois-Finiasz-Sendrier (CFS) system.

In particular, the KKS system uses two codes of different dimensions to make a so-called “trapdoor” function.

- 10 Nevertheless, the KKS system has a major weak point.

In fact, it has been shown that many system parameter choices are weak with respect to the use of algorithms for finding low-weight words in linear block codes.

- This is due to the fact that the information made public in the KKS system
15 permits defining a linear block code containing many low-weight words which have bits set only in a small sub-set of possible positions. This considerably increases the efficiency of probabilistic algorithms, such as Stern’s algorithm, aimed at finding such low-weight words.

- The CFS digital signature system uses a “hash-and-sign” paradigm based on the
20 fact that only the authorized signer is able to use the error correction capacity of a secret code.

In particular, the main components of the CFS system are a private corrector code C able to correct t errors and a public hash algorithm $\mathcal{H}$.

- The private corrector code C can be described by means of a generating matrix
25 G or, in an equivalent way, by means of a parity matrix H .

In particular, if described by means of the matrix H , then the matrix $H' = S \times H$ is made public, where S is a private random matrix.

- Furthermore, the CFS system of known type comprises a function F suitable for transforming, within a reasonable time, any hash value obtained by means of the
30 algorithm $\mathcal{H}$ into a correctable syndrome s for the private corrector code C .

In detail, the method for the signature of a digital file D by means of the CFS system comprises the following steps:

- the signer calculates the hash vector $h = H(D)$;
- the signer calculates $s = F(h)$ in such a way that $s' = S^{-1} \cdot s$ corresponds to a correctable syndrome for the code C ; such calculation can be made by means of an empiric procedure, by trial and error;
- the signer applies a syndrome decoding algorithm to s' by means of C and obtains an error vector e , with weight $w \leq t$, so that $s' = H \cdot e$;
- the signer applies the digital signature to the file D , obtaining the signed file D' , where such digital signature is made up of the error vector e and of the parameters used inside the function F to obtain the s' value, which are made public;
- following the receipt of a copy of the signed file D' the verifier calculates $H' \cdot e = S \cdot H \cdot e = S \cdot s' = s$;
- the verifier also calculates $\hat{h} = H(D')$ and $\hat{s} = F(\hat{h})$ using the parameters of the function F associated with the signed file D' ;
- if $\hat{s} = s$, then the file D' is accepted; otherwise, the file D' is deemed invalid and rejected.

The CFS system is not however without its drawbacks.

In particular, the main limits of the CFS system relate to the function F . In fact, it is very hard to determine a function able to quickly transform an arbitrary hash vector into a correctable syndrome.

To overcome this drawback, the CFS system presents two possible alternative solutions:

- add a counter to the message;
- make a complete decoding.

Nevertheless, both solutions require a very careful choice of the code parameters to obtain, in a reasonable time, a correctable syndrome starting from any hash vector.

For this reason, high rate codes are generally used with limited error correction capacity.

Consequently, such choice involves the exposure of the cryptography system to attacks based on the so-called "generalized birthday attack", as well as to the

common attacks normally affecting cryptography systems based on codes.

Such limit is due mainly to the need to ensure that many vectors produced by the hash function $\mathcal{H}$ are correctable.

In addition, particularly in the case of a complete decoding being performed, the

5 complexity of decoding can be considerably high.

Description of the Invention

The main aim of the present invention is to devise a method and a system for the digital signature which permits avoiding the attacks commonly suffered by a conventional CFS type system.

10 Another object of the present invention is to devise a method and a system for the digital signature able to allow a faster processing speed, together with the use of less computational power, compared to a CFS system of known type.

Another object of the present invention is to devise a method and a system for the digital signature able to allow a reduction in the decoding complexity

15 compared to a CFS system of known type.

Another object of the present invention is to devise a method and a system for the digital signature able to allow the use of a public key of smaller size compared to a CFS system of known type.

Another object of the present invention is to devise a method and a system for
20 the digital signature which allow to overcome the mentioned drawbacks of the prior art in the ambit of a simple, rational, easy and effective to use as well as low cost solution.

The above objects are achieved by the present method for the digital signature, comprising the following steps:

- 25
- defining a public calculation function suitable for calculating a syndrome vector starting from a digital file to sign;
 - selecting a private error corrector code;
 - calculating said syndrome vector by means of said calculation function and starting from said digital file to sign;
- 30
- determining an error vector starting from said syndrome vector and by means of said error corrector code;
 - determining a digital signature starting from said error vector;

- associating said digital signature with said digital file to obtain a signed digital file;

characterized in that said syndrome vector calculated by means of said calculation function is made up of a sparse vector.

5 Brief Description of the Drawings

Other characteristics and advantages of the present invention will become evident from the description of a preferred but not exclusive embodiment of a method and a system for the digital signature, illustrated by way of an indicative, but not limitative, example in the accompanying drawings in which:

10 Figure 1 is a flow chart that schematically illustrates a phase of signature of a digital file by means of the method according to the invention;

Figure 2 is a flow chart that schematically illustrates a phase of verification of a digital file signed by means of the method according to the invention;

15 Figure 3 shows an illustrative table that shows parameters related to the possible implementations of the method and system according to the invention;

Figure 4 shows an illustrative table that shows the size values of the public key in the case of Quasi-Cyclic Low-Density Generator-Matrix (QC-LDGM) codes being used having the parameters shown in Figure 4, for different security levels.

20 Embodiments of the Invention

With particular reference to figures 1 and 2, globally indicated by M is a method for the digital signature based on codes, able to use a sub-set of the possible syndromes, selecting only those having a determinate density of no null elements.

25 A first phase of signature of a digital file D using the method according to the invention is schematically shown in the flow chart in figure 1.

The method M for the digital signature comprises defining a public calculation function Y suitable for calculating a syndrome vector s starting from a digital file D to sign.

30 Preferably, the calculation function Y comprises:

- a public hash function $\mathcal{H}$ (step 1);
- a public conversion function F_{Θ} suitable for converting a hash vector (h)

obtained by means of the hash function $\mathcal{H}$ into a syndrome vector s (step 2).

The method M for the digital signature also comprises selecting a private error corrector code $C(n, k)$ (step 3).

- 5 In particular, the error corrector code $C(n, k)$ can be defined by means of its own generating matrix G with dimensions $k \times n$ and/or by means of its own parity matrix H with dimensions $r \times n$.

The method M envisages calculating the syndrome vector s by means of the calculation function Y and starting from the digital file D to sign (step 4).

- 10 In particular, the method M comprises the calculation of the hash vector h by means of the hash function $\mathcal{H}$ and starting from a digital file D to sign, according to the formula $h = H(D)$ (step 5) and, subsequently, the calculation of the syndrome vector s by means of the conversion function F_{Θ} and starting from the hash vector h , according to the formula $s = F_{\Theta}(h)$ (step 6).

- 15 Advantageously, the conversion function F_{Θ} converts the hash vector h into a corresponding syndrome vector s made up of a sparse vector (with low density of no null elements).

In particular, the sparse vector s has a predefined value of density of no null elements and has a predefined length r and a weight w smaller than r .

- 20 The conversion function F_{Θ} is suitable for converting the hash vector h into the sparse vector s according to a group of determined parameters Θ starting from the digital file D . Such parameters Θ are public and included in the digital signature of the file D itself.

- In a possible embodiment of the method M according to the invention, the
25 conversion function F_{Θ} is suitable for expanding a hash vector h of reduced dimensions so as to obtain a respective sparse vector s of bigger dimensions.

Such expansion can be obtained in various ways.

- One example consists in converting the binary hash vector h into the corresponding decimal whole number and then representing such whole number
30 according to a positional code which uses w bits set inside a vector with a r bit length.

One possible solution for achieving the function F_{Θ} in such a way that its output

depends on the parameter Θ is the following.

Given the hash vector h obtained from the file D , and having a x bit length, the value is added of a y bit binary counter m , thus obtaining the binary vector $[h|m]$. Such vector is then converted into one of the possible vectors of length r and weight w , as expounded above.

By changing the value of the counter m , a different vector is obtained with length r and weight w , consequently Θ coincides with m . Different methodologies and different implementations of the conversion function F_{Θ} cannot however be ruled out suitable for obtaining sparse vectors s starting from corresponding hash vectors h .

The use of the sparse vector s allows a more practical choice of the coding parameters compared to the solutions of known type, such as the Courtois-Finiasz-Sendrier (CFS) digital signature scheme, and permits the use of simplified decoding procedures.

Consequently, the main advantages deriving from the use of the method M are the following:

- to prevent potentially damaging attacks normally suffered by the conventional CFS system;
- to considerably reduce decoding complexity;
- to considerably reduce the dimensions of the key with respect to a conventional CFS system.

The method M also comprises the step of determining an error vector e starting from the sparse vector s (step 7).

In particular, the determination of the error vector e envisages the selection of a first matrix Q with dimensions $r \times r$ and of a second matrix S with dimensions $n \times n$ (step 8).

In particular, the first matrix Q and the sparse vector s are such that the private sparse vector s' is defined by the formula:

$$s' = Q \cdot s$$

and has weight w .

Preferably, the first matrix Q can be obtained as the sum of a low rank dense matrix R , $z < r$, with dimensions $r \times r$ and of a matrix T selected so that $Q = R +$

T is a full rank matrix.

The second matrix S is selected in the form of a non singular sparse matrix.

Subsequently, the method M envisages the determination of a public parity matrix H' (step 9) by means of the formula:

$$5 \quad H' = Q^{-1} \cdot H \cdot S^{-1}$$

where H' is the public parity matrix, Q^{-1} is the inverse of the first matrix Q , S^{-1} is the inverse of the second matrix S and H is the parity matrix of the error corrector code i .

The error vector e is calculated by means of a syndrome decoding algorithm, in
10 such a way that $s' = H \cdot e$ (step 10).

In particular, the fact is underlined that the error corrector code $C(n, k)$ is in systematic form.

In fact, if a code is systematic, then it can have a parity matrix $H_s = [P|I]$, where P is a matrix $r \times k$ and I is the identity matrix $r \times r$.

15 Consequently, each syndrome s can be obtained from the vector $e_s = [0_{1 \times k} | s^T]$, where $0_{1 \times k}$ is the vector with dimensions $1 \times k$ with all values equal to zero. In fact, checking that $H_s \cdot e_s^T = s$ is immediate.

Subsequently, the method M envisages the application of the digital signature to the digital file D , wherein the digital signature is determined according to the
20 error vector e (step 11).

In particular, the determination of the digital signature envisages the selection of a code word c belonging to the error corrector code $C(n, k)$ (step 12).

Usefully, c has a low weight w_c .

Consequently, considering that the number of vectors e corresponding to each
25 vector s' is very reduced, randomly generated error corrector codes $C(n, k)$ can be used.

In this respect, with reference to a preferred but not exclusive embodiment of the method M, the use of randomly generated codes of the LDGM (Low-Density Generator-Matrix) type represents an effective solution.

30 In particular, supposing that the generating matrix G with dimensions $k \times n$ of the secret error corrector code $C(n, k)$ is obtained by choosing its k lines as random binary vectors with dimensions $i \times n$ with weight $w_g \ll n$, then such generating

matrix G defines an LDGM type code the minimum distance of which is very likely equal to w_g .

Consequently, such code contains words of weight $w_c \geq w_g$.

A parity matrix H can be easily obtained starting from the generating matrix G .

- 5 With reference instead to the selection of the code word c with weight w_c , it can be observed that such code word can be easily obtained by adding together w_c/w_g lines of the generating matrix G selected randomly. In this respect, it is pointed out that w_c must be a multiple of w_g . In other cases, a code word can in any case be obtained with a weight close to w_c by linearly combining lines of G .

- 10 Consequently, using LDGM type codes, the signer can easily generate a high enough number of random code words with a moderately reduced weight w_c .

Such codes have both the parity matrix and the generating matrix in the form of sparse matrices consisting of cyclic sub-matrices with dimensions $p \times p$. It follows that the length and the dimension of the code are both multiples of the

- 15 whole p , i.e., $n = n_0 p$, $k = k_0 p$.

As shown by way of example in the table of figure 4, the use of the codes QC-LDGM permits reducing the dimensions of the public key by a factor equal to p compared to the case of non nearly cyclic LDGM codes.

Subsequently, the method M comprises the determination of the digital

- 20 signature e' (step 13) by means of the formula:

$$e' = (e + c) \cdot S^T$$

where e indicates the error vector, c indicates the code word and S^T indicates the transposed matrix of the second matrix S .

In particular, the density of e' must be determined so that it is:

- 25 - high enough to prevent attacks aimed at recovering the bond between the public syndrome and the contents of e' ;
 - low enough to prevent attacks aimed at falsifying valid signatures without however knowing the secret key.

Usefully, the use of the code word c allows avoiding the possibility of falsifying

- 30 valid signatures by linearly combining previously intercepted signatures.

In particular, it can be observed that in the case of such code word c not being used, then the digital signature e' can be rewritten as $e' = N(s)$, where N is a

bijjective and linear map from the group of public syndromes to the group of the valid signatures.

Consequently, anyone wanting to falsify a signature for a public syndrome s_x could express s_x as a linear combination of previously intercepted public syndromes, i.e., as $s_x = s_{i1} + s_{i2} + \dots + s_{iN}$, and falsify a valid signature by combining together in a linear way the corresponding signatures, i.e., as $e'_x = e'_{i1} + e'_{i2} + \dots + e'_{iN}$.

To avoid such risk, the signer therefore adds the random code word c with weight $w_c \ll n$ to the error vector e , before multiplication by the matrix S^T .

10 This way, the map N becomes a similar map dependent on the code word c and no longer has as its image a group of valid signatures.

Nevertheless, if the choice of the word i is completely random and independent from the file D , the signature obtained for a given file can change every time the file is signed, and this leaves the system open to attacks which exploit many
15 different signatures of the same file.

In order to avoid this vulnerability, the selection of the code word c can be tied to the file to sign, so as to always select the same word c for the same file D .

This can be obtained, e.g., using the syndrome vector s as initial seed of the pseudo-random generator used to select the lines of the matrix G to be
20 combined linearly to obtain the word c .

Once the digital signature e' has been determined, the method M envisages the application of the digital signature e' to the digital file D , to obtain a signed digital file D' (step 14) and the subsequent sending of the signed digital file D' (step 15).

25 The signed digital file D' can be sent using conventional and typically unsecure transmission means such as, for example, the Internet.

A phase of verification of the signature of a signed digital file D' using the method according to the invention is schematically shown in the flow chart in figure 2.

30 In particular, following the receipt of a copy of the signed digital file D' (step 16) a check is made of the correspondence between a comparison syndrome vector $\hat{s}$ and the syndrome vector s , determined starting from the received

digital signature e' .

Preferably, such verification comprises the following steps:

- calculating the hash vector $\hat{h}$ by means of the public hash function H and starting from the copy of the digital file D (step 17);
- 5 - calculating the comparison syndrome vector $\hat{s}$ by means of the public conversion function F_{Θ} and starting from the hash vector $\hat{h}$ (step 18);
- checking whether the weight $w_{\hat{s}}$ of the comparison syndrome vector $\hat{s}$ is equal to the weight w of the sparse vector s (step 19);
- if the comparison syndrome vector $\hat{s}$ has weight $w_{\hat{s}}$ different to weight w of the sparse vector s , then the signed digital file D' is considered not reliable and is therefore rejected (step 22).

Different embodiments cannot however be ruled out wherein, for example, the comparison syndrome vector $\hat{s}$ is calculated starting from the copy of the digital file D , by means of the public calculation function Y .

- 15 Such check also comprises the calculation of the syndrome vector s starting from the received digital signature e' (step 20).

In particular, the digital signature e' and the public matrix H' being known, the syndrome vector s is calculated by means of the following formula:

$$H' \cdot e'^T = Q^{-1} \cdot H \cdot S^{-1} \cdot S \cdot (e^T + c^T) = Q^{-1} \cdot H \cdot (e^T + c^T) = Q^{-1} \cdot H \cdot e^T = Q^{-1} \cdot s' = s.$$

20

- Subsequently, the method M envisages a control step suitable for checking whether the digital signature e' has weight $w_{e'}$ less or the same as a predefined value v , where $v = (m_T w + w_c) \cdot m_S$ (step 21), where m_T is the weight of line and of column of the matrix T while m_S is the weight of line and of column of the matrix S .
- 25

If the digital signature e' has weight $w_{e'}$ greater than the value v , then the signed digital file D' is considered not to be reliable and is therefore rejected (step 22).

Afterwards, the comparison is also made between the comparison syndrome vector $\hat{s}$ and the syndrome vector s (step 23).

- 30 If the comparison syndrome vector $\hat{s}$ is different from the syndrome vector s , then the signed digital file D' is considered not reliable and is therefore rejected (step 22).

If the comparison syndrome vector $\hat{s}$ corresponds to the syndrome vector s , then the signed digital file D' is considered to be reliable and is accepted (step 24).

By way of example only, the figure 3 shows representative parameters of application examples of the method M according to the invention.

- 5 In particular, such examples refer to the use of LFGM type error corrector codes.

In particular, by way of example the table in figure 4 shows the dimension values of the public key in the event of QC-LDGM codes being used having parameters with security levels shown in figure 4, where the dimension of the
10 public key is expressed in kibibytes (1 KiB = 1024×8 bits).

It is also pointed out that the method according to the invention is implemented by means of one or more computer programs running on one or more electronic processors.

In particular, the method according to the invention can be implemented by
15 means of a system for the digital signature, composed of one or more hardware devices and/or one or more computer programs, comprising:

- calculation means of the sparse vector s by means of the calculation function Y and starting from the digital file D to sign;
- means of determination of the error vector e starting from the syndrome
20 vector s and by means of the error corrector code $C(n, k)$;
- means of determination of the digital signature e' starting from the error vector e ;
- means of association of the digital signature e' with the digital file D to obtain the signed digital file D' .

25 Preferably, the calculation means of the syndrome vector s comprise:

- first calculation means of the hash vector h by means of the hash function $\mathcal{H}$ and starting from the digital file D to sign;
- second calculation means of the sparse vector s , by means of the conversion function F_{θ} and starting from the hash vector h .

30 Different embodiments cannot however be ruled out whereby, for example, the calculation means of the syndrome vector s consist of the calculation function Y . Furthermore, the means for determining the error vector e comprise:

- selection means of the first matrix Q and of a second matrix S , wherein the first matrix Q and the sparse vector s are such that the private sparse vector s' defined by the formula

$$s' = Q \cdot s$$

5 has weight w , where Q indicates the first matrix and s indicates the sparse vector;

- means for determining the public matrix H' by means of the formula

$$H' = Q^{-1} \cdot H \cdot S^{-1}$$

10 where H' is the public matrix, Q is the first matrix, S is the second matrix and H is the parity matrix of the error corrector code $C(n, k)$;

- calculation means of the error vector e by means of a syndrome decoding algorithm, in such a way that $s' = H \cdot e$, where e indicates the error vector.

The means of association of the digital signature with the digital file D 15 comprise:

- selection means of a code word c belonging to the error corrector code $C(n, k)$ where, preferably, the code word c is always the same for a given file D ;
- means for determining the digital signature by means of the formula

20
$$e' = (e + c) \cdot S^T$$

where e' indicates the digital signature vector, e indicates the error vector, c indicates the code word and S^T indicates the transposed matrix of the second matrix S .

The system also comprises means for verifying the correspondence between:

- 25
- the comparison syndrome vector $\hat{s}$, calculated by means of the public calculation function Y and starting from the received digital file D ;
 - the sparse vector s , determined starting from the received digital signature e' .

Preferably, the verification means comprise:

- 30
- calculation means of a hash vector $\hat{h}$ by means of the public hash function H and starting from the copy of the signed digital file D' ;
 - calculation means of the comparison syndrome vector $\hat{s}$ by means of the

public conversion function (F_{Θ}) and starting from the hash vector $\hat{h}$;

- calculation means of the sparse vector (s) by means of the following formula:

$$H' \cdot e'^T = Q^{-1} \cdot H \cdot S^{-1} \cdot S \cdot (e^T + c^T) = Q^{-1} \cdot H \cdot (e^T + c^T) = Q^{-1} \cdot H \cdot e^T = Q^{-1} \cdot$$

5 $s' = s.$

Furthermore, the verification means comprise control means suitable for controlling that the weight of the vector $\hat{s}$ is equal to the preset value w and that the weight $w_{e'}$ of the digital signature vector e' is less than or the same as $v = (m_{TW} + w_c)m_s$.

- 10 It has in fact been ascertained how the described invention achieves the proposed objects.

In particular, the fact is underlined that the method and the system for the digital signature according to the invention permit avoiding the attacks commonly suffered by a conventional CFS type system.

- 15 Furthermore, the method and the system according to the invention permit reducing the decoding complexity and the dimensions of the key and therefore permit a higher processing speed and make possible the use of less computational power, with consequent economic and energy savings.

CLAIMS

- 1) Method (M) for the digital signature, comprising the following steps:
 - defining a public calculation function (Y) suitable for calculating a syndrome vector (s) starting from a digital file (D) to sign;
 - 5 - selecting a private error corrector code ($C(n, k)$);
 - calculating said syndrome vector (s) by means of said calculation function (Y) and starting from said digital file (D) to sign;
 - determining an error vector (e) starting from said syndrome vector (s) and by means of said error corrector code ($C(n, k)$);
 - 10 - determining a digital signature (e') starting from said error vector (e);
 - associating said digital signature (e') with said digital file (D) to obtain a signed digital file (D');

characterized in that said syndrome vector (s) calculated by means of said calculation function (Y) is made up of a sparse vector.
- 15 2) Method (M) according to claim 1, characterized in that, following the receipt of a copy of said signed digital file (D'), it comprises the step of verifying the correspondence between:
 - a comparison syndrome vector ($\hat{s}$), calculated by means of said calculation function (Y) starting from the received digital file (D);
 - 20 - said sparse vector (s), determined starting from the received digital signature (e').
- 3) Method (M) according to one or more of the preceding claims, characterized in that said calculation function (Y) comprises:
 - a public hash function ($\mathcal{H}$);
 - 25 - a public conversion function (F_Θ) suitable for converting a hash vector (h) obtained by means of said hash function ($\mathcal{H}$) into said sparse vector (s);

and in that said step of calculating the syndrome vector (s) comprises the steps of:

 - calculating said hash vector (h) by means of said hash function ($\mathcal{H}$) and starting from said digital file (D) to sign;
 - 30 - calculating said sparse vector (s), by means of said conversion function (F_Θ) and starting from said hash vector (h).

- 4) Method (M) according to one or more of the preceding claims, characterized in that said sparse vector (s) has a predefined value of density of no null elements, a predefined length (r) and a predefined weight w .
- 5) Method (M) according to one or more of the preceding claims, characterized in that said conversion function (F_{θ}) is suitable for converting said hash vector (h) into said sparse vector (s) according to a group of determined public parameters (θ) starting from said digital file (D).
- 6) Method (M) according to one or more of the preceding claims, characterized in that said step of calculating the sparse vector (s) by means of said conversion function (F_{θ}) and starting from said hash vector (h) comprises the step of expanding said hash vector (h) into a sparse vector (s) of bigger dimensions.
- 7) Method (M) according to one or more of the preceding claims, characterized in that said step of calculating the sparse vector (s) by means of said conversion function (F_{θ}) and starting from said hash vector (h) comprises the step of adding the value of a binary counter (m), thus obtaining a binary vector ($[h|m]$), and the step of converting said binary vector ($[h|m]$) into a predefined length (r) and predefined weight (w) vector.
- 8) Method (M) according to one or more of the preceding claims, characterized in that said error corrector code ($C(n, k)$) is defined by means of its own generating matrix (G) and/or by means of its own parity matrix (H) in systematic form.
- 9) Method (M) according to one or more of the preceding claims, characterized in that said step of determining an error vector (e) comprises:
- selecting a first matrix (Q) and a second matrix (S), wherein said first matrix (Q) and said sparse vector (s) are such that a private sparse vector (s') defined by the formula

$$s' = Q \cdot s$$

has a predefined weight w , where Q indicates said first matrix and s indicates said sparse vector;

- determining a public matrix (H') by means of the formula

$$H' = Q^{-1} \cdot H \cdot S^{-1}$$

where H' is said public matrix, Q is said first matrix, S is said second matrix and H is a parity control matrix of said error corrector code ($C(n, k)$);

- calculating said error vector (e) by means of a syndrome decoding algorithm, so that $s' = H \cdot e$, where e indicates said error vector.

5 10) Method (M) according to one or more of the preceding claims, characterized in that said step of associating the digital signature with the digital file (D) comprises:

- selecting a code word (c) belonging to said error corrector code ($C(n, k)$);
- determining said digital signature by means of the formula

$$10 \quad e' = (e + c) \cdot S^T$$

where e' indicates a digital signature vector, e indicates said error vector, c indicates said code word and S^T indicates a transposed matrix of said second matrix S .

11) Method (M) according to one or more of the preceding claims, characterized in that said step of verifying comprises:

- calculating a hash vector ($\hat{h}$) by means of said public hash function ($\mathcal{H}$) and starting from said copy of the signed digital file (D').
- calculating said comparison syndrome vector ($\hat{s}$) by means of said public conversion function (F_θ) and starting from said hash vector ($\hat{h}$);
- 20 - calculating said sparse vector (s) by means of the following formula:

$$H' \cdot e'^T = Q^{-1} \cdot H \cdot S^{-1} \cdot S \cdot (e^T + c^T) = Q^{-1} \cdot H \cdot (e^T + c^T) = Q^{-1} \cdot H \cdot e^T = Q^{-1} \cdot s' = s.$$

12) Method (M) according to one or more of the preceding claims, characterized in that said step of verifying comprises checking that the weight ($w_{\hat{s}}$) of the comparison syndrome vector ($\hat{s}$) is equal to the weight (w) of the syndrome vector (s), and/or that the weight ($w_{e'}$) of said vector of digital signature (e') is less than or equal to $v = (m_T w + w_c) m_S$.

13) System for the digital signature, comprising:

- calculation means of syndrome vector (s) by means of a calculation function (Y) and starting from a digital file (D) to sign;
- 30 - means of determination of an error vector (e) starting from said syndrome vector (s) and by means of an error corrector code ($C(n, k)$);

- means of determination of a digital signature (e') starting from said error vector (e);
- means of association of said digital signature (e') with said digital file (D) to obtain a signed digital file (D');

5 characterized in that said syndrome vector (s) calculated by means of said calculation function (Y) is made up of a sparse vector.

14) System according to claim 13, characterized in that it comprises verification means of the correspondence between:

- a comparison syndrome vector ($\hat{s}$), calculated by means of said calculation
10 function (Y) starting from the received digital file (D);
- said sparse vector (s), determined starting from the received digital signature (e').

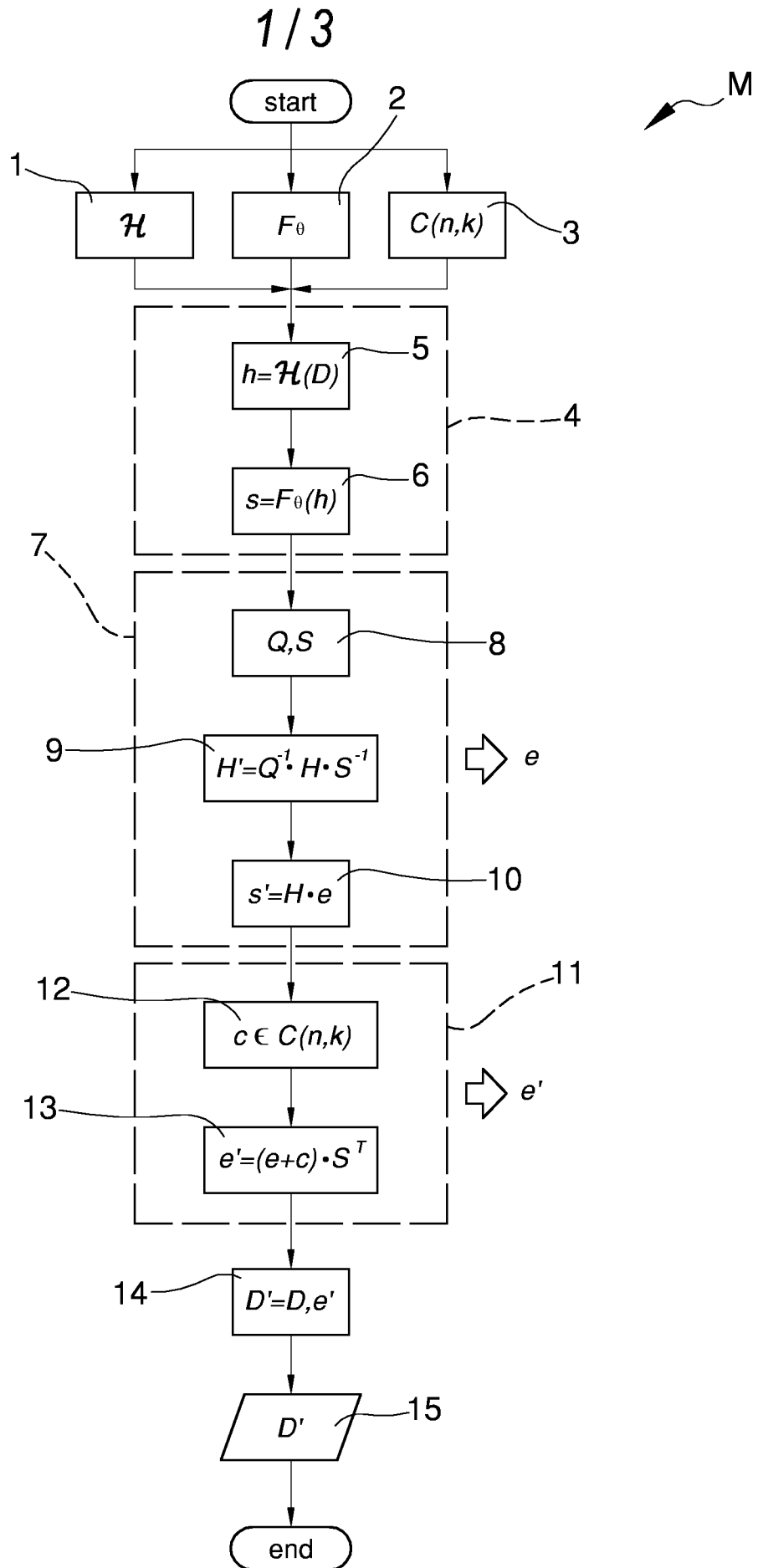
15) System according to one or more of the claims 13 and 14, characterized in that said calculation function (Y) comprises:

- 15 - a public hash function ($\mathcal{H}$);
- a public conversion function (F_Θ) suitable for converting a hash vector (h) obtained by means of said hash function ($\mathcal{H}$) into said sparse vector (s);

and in that said calculation means of the syndrome vector (s) comprise:

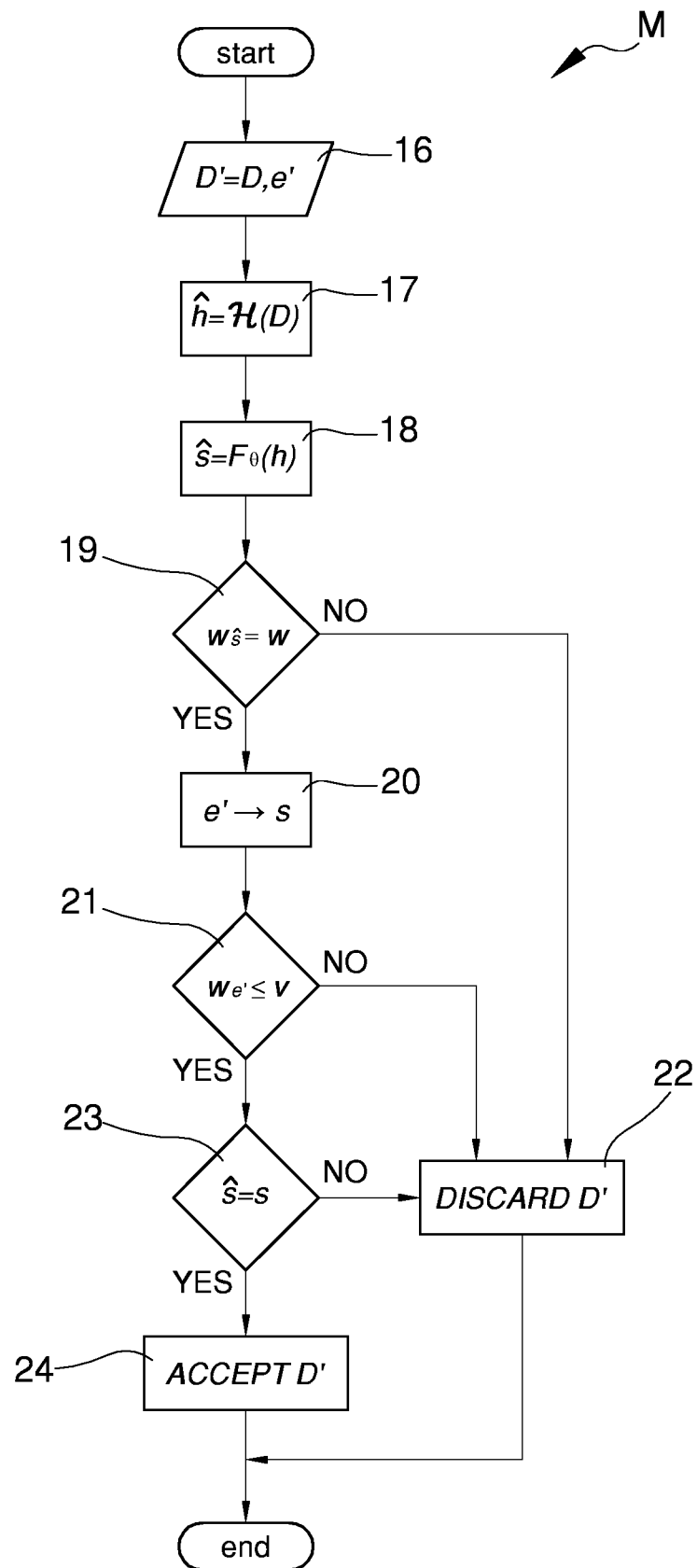
- first calculation means of said hash vector (h) by means of said hash
20 function ($\mathcal{H}$) and starting from said digital file (D) to sign;
- second calculation means of said sparse vector (s), by means of said conversion function (F_Θ) and starting from said hash vector (h).

Fig. 1



2 / 3

Fig. 2



3 / 3

Security level (bit)	Length of the private code (n)	Size of the private code (k)	Weight of the public syndrome (w)
80	9800	4900	18
120	24960	10000	23
160	46000	16000	29

Fig. 3

Length of the private code (n)	Size of the private code (k)	Side of the circulant blocks (p)	Size of the public key (KiB)
9800	4900	50	117
24960	10000	80	570
46000	16000	100	1685

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2014/061557

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/32
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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

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

EP0-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BARRETO P S L M ET AL: "One-time signature scheme from syndrome decoding over generic error-correcting codes", JOURNAL OF SYSTEMS & SOFTWARE, ELSEVIER NORTH HOLLAND, NEW YORK, NY, US, vol. 84, no. 2, 1 February 2011 (2011-02-01), pages 198-204, XP027571185, ISSN: 0164-1212 [retrieved on 2010-09-21] the whole document -----	1-8, 13-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

4 August 2014

Date of mailing of the international search report

11/08/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Di Felice, M