



Office de la Propriété

Intellectuelle  
du Canada

Un organisme  
d'Industrie Canada

Canadian  
Intellectual Property  
Office

An agency of  
Industry Canada

CA 2317775 C 2011/07/26

(11)(21) **2 317 775**

(12) **BREVET CANADIEN  
CANADIAN PATENT**

(13) **C**

(22) Date de dépôt/Filing Date: 2000/09/06  
(41) Mise à la disp. pub./Open to Public Insp.: 2001/03/07  
(45) Date de délivrance/Issue Date: 2011/07/26  
(30) Priorité/Priority: 1999/09/07 (US09/390,362)

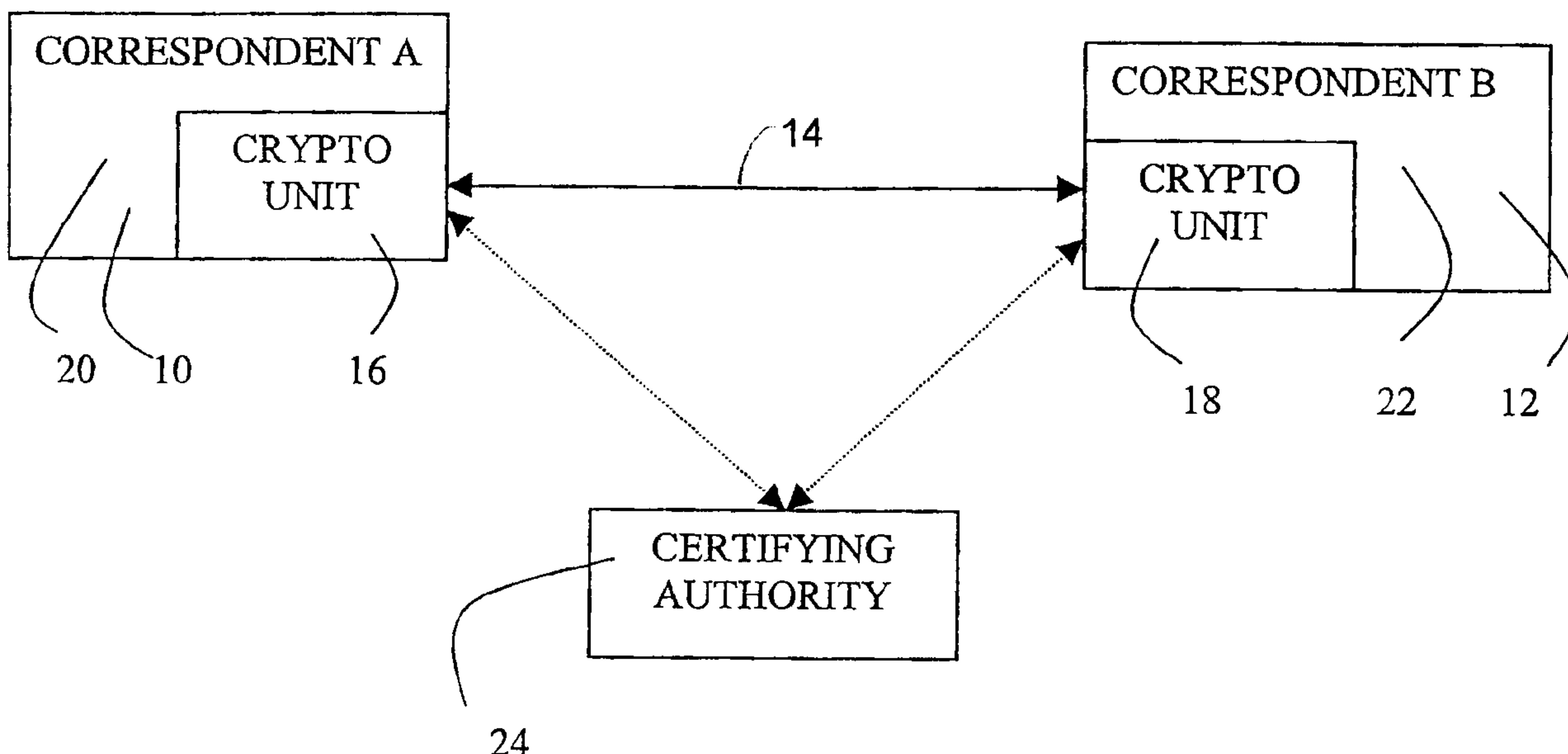
(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01)

(72) Inventeurs/Inventors:  
GALLANT, ROBERT, CA;  
LAMBERT, ROBERT J., CA;  
PINTSOV, LEON, US;  
RYAN, FREDERICK W., US;  
SINGER, ARI, US;  
VANSTONE, SCOTT ALEXANDER, CA

(73) Propriétaires/Owners:  
CERTICOM CORP., CA;  
PITNEY BOWES INC., US

(74) Agent: BLAKE, CASSELS & GRAYDON LLP

(54) Titre : SYSTEME DE SIGNATURE HYBRIDE  
(54) Title: HYBRID SIGNATURE SCHEME



(57) Abrégé/Abstract:

A signature scheme is provided in which a message is divided into a first portion which is hidden and is recovered during verification, and a second portion which is visible and is required as input to the verification algorithm. A first signature component is generated by encrypting the first portion alone. An intermediate component is formed by combining the first component and the visible portion and cryptographically hashing them. A second signature component is then formed using the intermediate component and the signature comprises the first and second components with the visible portion. A verification of the signature combines a first component derived only from the hidden portion of the message with the visible portion and produces a hash of the combination. The computed hash is used together with publicly available information to generate a bit string corresponding to the hidden portion. If the required redundancy is present the signature is accepted and the message reconstructed from the recovered bit string and the visible portion.

Abstract

A signature scheme is provided in which a message is divided in to a first portion which is hidden and is recovered during verification, and a second portion which is visible and is required as input to the verification algorithm. A first signature component is generated by encrypting the first portion alone. An intermediate component is formed by combining 10 the first component and the visible portion and cryptographically hashing them. A second signature component is then formed using the intermediate component and the signature comprises the first and second components with the visible portion. A verification of the signature combines a first component derived only from the hidden portion of the message with the visible portion and produces a hash of the combination. The computed 15 hash is used together with publicly available information to generate a bit string corresponding to the hidden portion. If the required redundancy is present the signature is accepted and the message reconstructed from the recovered bit string and the visible portion.

## HYBRID SIGNATURE SCHEME

The present invention relates to methods and apparatus for digitally signing a message.

Digital signatures are used to sign a message generated by a correspondent so that the origin and authenticity of the message may subsequently be verified. In its basic form, a digital signature of a message is generated by signing the message with the originators private key. The message may then be recovered using the originators public key. A number of variants of this basic arrangement have been proposed with different attributes. Digital signature schemes are typically thought to fall into two generic classes, namely digital signatures with appendix and digital signatures with message recovery.

Digital signatures with appendix are categorized by the fact that the message signed is required as input to the verification algorithm. Although very popular (the DSS and ECDSA are examples of this mechanism) they may not provide as much bandwidth efficiency as other methods.

Digital signatures with message recovery are categorized by the fact that the message is not required as input to the verification algorithm. One goal when designing message recovery schemes is to defeat existential forgery attacks by defining a suitable redundancy function which will distinguish messages legitimately signed from signatures of random bit strings.

In many practical applications the data to be signed carries a certain amount of inherent redundancy. For example, four bytes of data might be reserved for the date but, in practice, 3 bytes suffice and so there are 8 bits of redundancy from this field. In order to ensure security it is necessary to provide a predetermined degree of redundancy within the message and accordingly the bandwidth efficiency is reduced.

To increase the bandwidth efficiency it is known to split the message in to two components, namely a hidden and a visible component. The hidden component is recovered during the verification process and the visible portion is used as an input to the recovery process. The hidden component must have sufficient redundancy to withstand an existential forgery attack and additional bits must be added to the message if it does not inherently possess this. In one of the proposed standards to implement such a scheme,

5 ISO 9796 Part 2, the hidden component is utilised to generate a signature component  $c$  of the form  $DES_R[H//SHA1(V)//I_A]$  where

H is the hidden component,

V is the visible component

$I_A$  is an identifier of the signer

10 SHA1(V) is a cryptographic hash of the visible component, and  
 $DES_R$  is an encryption of the bit string.

This scheme however has the disadvantage that  $c$  is at least the number of bits in SHA1(V) bits longer, and, as it is included in the signature, the required bandwidth efficiency may not be achieved. Moreover, the scheme requires invocation of two hash operations  
15 as the value  $c$  is subsequently hashed for inclusion in the signature component. This computational complexity may make it unsuitable for certain applications.

It is therefore an object of the present invention to provide a signature scheme in which the above disadvantages are obviated or mitigated.

In general terms, one aspect of the present invention provides a signature scheme  
20 in which a message is divided in to a first portion which is hidden and is recovered during verification, and a second portion which is visible and is required as input to the verification algorithm. A first signature component is generated by encrypting the first portion alone. An intermediate component is formed by combining the first component and the visible portion and cryptographically hashing them. A second signature  
25 component is then formed using the intermediate component and the signature comprises the first and second components with the visible portion.

The generation of the first component from the first portion alone reduces the necessary bandwidth and simplifies the computation. The relative sizes of the first and second portions are determined by the application itself. In this manner, the redundancy  
30 function can be application dependent as opposed to a global primitive.

Recovery of the message can be completed using the signature and the public key of the sender.

According to a further aspect of the invention there is provided a verification of a signature of a message that has been subdivided into a hidden and visible portion. The  
35 verification combines a first component derived only from the hidden portion of the

5 message with the visible portion and produces a hash of the combination. The computed hash is used together with publicly available information to generate a bit string corresponding to the hidden portion. If the required redundancy is present the signature is accepted and the message reconstructed from the recovered bit string and the visible portion.

10 Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings in which: -

Figure 1 is a schematic representation of a data communication system,

Figure 2 is a flow chart showing the signature generation,

Figure 3 is a flow chart showing the verification of the signature of figure 2, and

15 Figure 4 is a flow chart showing a further embodiment of signature generation.

Referring to Figure 1, a data communication system includes a pair of correspondents 10, 12 exchanging a message M over a communication channel 14. Each of the correspondents 10, 12 includes a cryptographic unit 16, 18 respectively and a terminal 20, 22 to generate and receive the message M. Each of the cryptographic units 20 16, 18 implements a public key encryption scheme that enables it to generate a session key, to encipher or decipher a message using the session key or sign a message using a private key whereby the message can then be recovered using a public key corresponding to the private key. The general implementation of such schemes and their operating principles are well known. The encryption scheme may be loaded into the encryption unit from a data carrier 25 coded to implement the protocol under the direction of a general purpose computer or may be implemented on a chipset as preprogrammed instructions.

In the preferred embodiment described below, the encryption scheme is based on the intractability of the discrete log problem in finite groups and is implemented in an 30 algebraic system defined on the points of an elliptic curve over a finite field, typically referred to as elliptic curve crypto systems. However, the signature scheme proposed may be applied to any ElGamal signature over any finite group.

The domain parameters of such an elliptic curve crypto system are a curve of the 35 form  $y^2 = x^3 + dx + c$  and a seed point P. One of the correspondents has a private key a,

5       $0 < a < n$  where  $n$  is the order of the point  $P$  and a corresponding public key  $Q_A = aP$ . The public key may be held in a certifying authority 24 shown in communication with the correspondents 10, 12 by ghosted lines.

10     The messages  $M$  generated by the correspondents 10, 12 are subdivided into two bit strings  $H$  and  $V$  ( i.e.  $M=H//V$ ) where  $H$  is a bit string which is hidden and recovered during the verification process and  $V$  is a bit string which is also signed but is required as input to the verification process.

15     The signature generation algorithm is set out in the flow chart of figure 2. Initially the bit string  $H$  is examined to determine if it contains redundancy above a predetermined limit sufficient to prevent an existential forgery attack. If the examination determines that the original data forming the message  $M$  contains enough redundancy then  $H$  may simply be a subset of that data. If the predetermined redundancy is not found then  $H$  may be modified to contain artificially added redundancy such as additional bytes of 0's.

20

By way of example, suppose 80 bits of redundancy is determined to be the predetermined lower limit for security reasons. If the bit string  $H$  contains no inherent redundancy then it would be necessary to add up to 10 bytes of 0's. To permit recovery of the message an indicator would be included, conveniently as a leading byte in either  $H$  or  $V$ , which tells the number of bytes of 0's added. Since the value is 0 to 10, 4 bits of the byte suffice as an indicator so the bit string contains an additional 4 bits of redundancy. If  $t$  is the number of redundancy bytes that can be added, then the data must inherently contain at least  $80-8t$  bits of redundancy.

30     To sign the message  $M = H // V$  the correspondent 10 generates a random integer  $k$ ,  $0 < k < n$  in the cryptographic unit 16. Using  $k$  correspondent 10 then computes a value of a random point  $R = kP$ .

35     A value  $c$  is then computed from the bit string  $H$  only such that  $c = SKE_R(H)$ .  $SKE_R$  refers to a symmetric-key algorithm under control of a key derived from the

5 random point R. This could be derived by applying a function, such as a hash function, to R, truncating R, or using only one of the coordinates, e.g. the x coordinate as the key. If H is smaller than the key derived from R, then one possible SKE is simply to XOR H with a truncation of bits from the key derived from R. This effectively is a one-time pad. If H is larger than the key it is possible to use a DES based algorithm or simply to XOR 10 repeatedly the key with H.

Using the bit string V, an intermediate component c' is computed such that  $c' = \text{SHA1}(c//V)$  where SHA1 is a cryptographically secure hash algorithm. If preferred, additional information such as a certificate or identifying information of correspondent 10 may be 15 incorporated in to the hashed value c'.

It will be noted that the signature component c is the same length as the hidden portion H as it is a bit wise encryption of that portion and that the intermediate component c' is obtained with a single hash operation.

20 A signature component s is then computed from the values available to the correspondent 10 using any of the known ElGamal equations. A convenient equation is the Schnorr signature algorithm where  $s = c'a + k \pmod n$ . A signature is then formed from the components (s,c,V) and forwarded to the correspondent 12.

25 Verification of the signature by correspondent 12 is performed by the application of the corresponding algorithm, as shown in figure 3 for the Schnorr signature. The correspondent 12 initially obtains an authentic copy of the public key  $Q_A$  of the correspondent 10 from the certifying authority 24. The correspondent 12 then computes a 30 value  $c'' = \text{SHA1}(c//V)$  and derives from the information available in the signature, i.e. s,c,V and the system domain parameters, the values

$$X = sP$$

$$Y = c'' Q_A$$

$$Z = X - Y$$

5 A bit string  $H'$  is then recovered by applying to the received signature component  $c$  the symmetric-key algorithm under control of a key derived from the point  $Z$  such that  $H' = SKE_Z(c)$ . The bit string  $H'$  is then examined to determine if it has the required redundancy and if so the correspondent 12 accepts the signature of  $M$  and reconstitutes the message as  $H'//V$ .

10

Because the message  $M$  is subdivided, it is only necessary for the one portion,  $H$ , to contain the requisite redundancy. The other portion  $V$ , which is sent in the clear, may have the data structure of the original data and thereby improve the bandwidth efficiency.

15

Another feature of this scheme which is of practical and commercial interest is that the information encoded in  $c$  is only available to those individuals who have the public key  $Q_A$  of correspondent 10. The data contained in  $V$  is available to all. There may be some information which correspondent 10 wants to hide from those not privy to  $Q_A$  in which case the sender, i.e. correspondent 10 puts this information into the bit string

20

$H$ .

25

For example, in one particular application where the signature is used to authenticate postage applied to mail, a mailer may not want a receiver to know how many mail pieces he has sent. The post office (which verifies postage and therefore needs this information) has the public key of the mailer, and can recover this information on verification but the receiver cannot if he does not have the mailers public key.

30

Of course, if the public key  $Q_A$  of the sender is contained in the indicium then this is also available to the receiver. Alternatively, the senders public key may be contained in a certificate that can only be recovered if the receiver has the certifying authority's public key. If this is not generally available then the contents of  $H$  will be hidden from the receiver.

5 As indicated above, alternative forms of signing equations may be used. In a further embodiment shown in the flow chart of figure 4, a signing equation similar to the ECDSA standard is used. Normally in such an arrangement:-

- $R = kP$
- 10 •  $c = DES_R(M)$
- $r' = SHA1(c)$
- $s = k^{-1} \{ SHA1(c//ID_A) + a r' \} \text{ mod } n$  where  $ID_A$  is an identifier of the sender.
- the signature is  $(s, c)$ .

15 When used with a hybrid scheme described above the scheme is modified such that

- $R = kP$
- $c = DES_R(H)$
- $r' = SHA1(c)$
- $s = k^{-1} \{ SHA1(c//V) + a r' \} \text{ mod } n$ .
- 20 • the signature is  $(s, c, V)$

Again therefore because only a portion  $H$  of the message is used to generate the first component  $c$ , only that portion requires a specified redundancy. In the balance of the message a reduced redundancy may be utilised to maintain bandwidth efficiency.

The verification for the modified scheme will change accordingly to

25 accommodate the partial message recovery and necessary redundancy.

## CLAIMS

1. A method of digitally signing a plaintext message exchanged between a pair of correspondents in a data transmission system, one of said pair of correspondents being the signer and having a private key  $a$  and a public key derived from the private key  $a$ , said public key being available to the other of said pair of correspondents, said method comprising the steps of:

subdividing said plaintext message into a first plaintext bit string  $H$  and a second plaintext bit string  $V$ ;

computing a first signature component  $c$  as a function of said first plaintext bit string  $H$  wherein the plaintext bit string  $H$  is hidden in said first signature component  $c$ ;

computing an intermediate signature component  $c'$  as a function of said first signature component  $c$  and said second plaintext bit string  $V$ ;

computing a second signature component  $s$  as a function of said intermediate signature component  $c'$  and said private key  $a$ ; and

forming a signature  $(s, c, V)$  containing said first signature component  $c$ , said second signature component  $s$ , and said second plaintext bit string  $V$  as discrete signature components;

whereby during verification, said second plaintext bit string  $V$  is available from said signature  $(s, c, V)$  as an input to a verification protocol.

2. The method according to claim 1 wherein redundancy in said first plaintext bit string  $H$  is compared to a predetermined level prior to computing said first signature component  $c$ .

3. The method according to claim 2 wherein said redundancy is adjusted to exceed a predetermined level.

4. The method according to claim 3 wherein data is added to said first plaintext bit string  $H$  to adjust said redundancy.

5. The method according to claim 4 wherein an indicator is included in said first plaintext bit string  $H$  to indicate additional data.

6. The method according to any one of claims 1 to 5 wherein said second signature component  $s$  is generated by hashing said first signature component  $c$  and said second

plaintext bit string V.

7. The method according to any one of claims 1 to 6 wherein said first signature component c is computed by applying a function to said first plaintext bit string H and said first plaintext bit string H may be recovered from said first signature component c by applying a complementary function to said first signature component c.
8. The method according to claim 7 wherein said function is encryption with an encryption key, a decryption key is computable from information available in said signature, and said complementary function is decryption with said decryption key.
9. The method according to claim 8, wherein said encryption key is a short-term derived from a random integer used in the provision of said second signature component.
10. A method of verifying a plaintext message from a signature of a purported signer in a data transmission system, said plaintext message being subdivided into a first plaintext bit string H and a second plaintext bit string V, said signature formed as a set of discrete components, said signature containing a first component computed as a function of said first plaintext bit string H whereby said bit string H is encrypted therein, and said second plaintext bit string V as a second component, said purported signer having a private key used in the computation of said signature and a corresponding public key available for use in verification, said method comprising the steps of:
  - generating a value by combining said first component with said second plaintext bit string V;
  - recovering said first plaintext bit string H from said value using publicly available information of the purported signer including said public key;
  - examining said recovered first plaintext bit string H for a predetermined characteristic; and
  - verifying said message if said predetermined characteristic is present.
11. The method according to claim 10 wherein said combining of said first component and said second plaintext bit string V includes hashing said first component and said second plaintext bit string V.

12. The method according to any one of claims 10 and 11 wherein said predetermined characteristic is the redundancy of said recovered first plaintext bit string H.

13. The method according to claim 12 wherein said signature includes a third component derived from a combination of said first component and said second plaintext bit string V and said first plaintext bit string H is recovered utilising said third component.

14. A method for authenticating a communication between a first correspondent and a second correspondent in a data transmission system, said first correspondent having a private key a and a public key derived from the private key a, said public key being available to said second correspondent, said method comprising:

    said first correspondent subdividing a plaintext message into a first plaintext bit string H and a second plaintext bit string V;

    said first correspondent computing a first signature component c as a function of said first plaintext bit string H wherein the plaintext bit string H is hidden in said first signature component c;

    said first correspondent computing an intermediate signature component c' as a function of said first signature component c and said second plaintext bit string V;

    said first correspondent computing a second signature component s as a function of said intermediate signature component c' and said private key a;

    said first correspondent forming a signature (s,c,V) containing said first signature component c, said second signature component s, and said second plaintext bit string V as discrete signature components;

    said first correspondent making available to said second correspondent, at least said first signature component c and said second plaintext bit string V;

    said second correspondent generating a value by combining said first signature component c with said second plaintext bit string V;

    said second correspondent recovering said first plaintext bit string H from said value using publicly available information of said first correspondent including said public key;

    said second correspondent examining said recovered first plaintext bit string H for a predetermined characteristic; and

    said second correspondent verifying said message if said predetermined characteristic is present.

15. A computer program product comprising a data carrier, said data carrier comprising computer executable instructions for performing the method according to any one of claims 1 to 14.

16. A cryptographic unit for digitally signing a plaintext message exchanged between a pair of correspondents in a data transmission system, one of said pair of correspondents being the signer and having a private key  $a$  and a public key derived from the private key  $a$ , said public key being available to the other of said pair of correspondents, said cryptographic unit comprising a computing device for implementing instructions, said instructions comprising:

subdividing said plaintext message into a first plaintext bit string  $H$  and a second plaintext bit string  $V$ ;

computing a first signature component  $c$  as a function of said first plaintext bit string  $H$  wherein the plaintext bit string  $H$  is hidden in said signature component  $c$ ;

computing an intermediate signature component  $c'$  as a function of said first signature component  $c$  and said second plaintext bit string  $V$ ;

computing a second signature component  $s$  as a function of said intermediate signature component  $c'$  and said private key  $a$ ; and

forming a signature  $(s, c, V)$  containing said first signature component  $c$ , said second signature component  $s$ , and said second plaintext bit string  $V$  as discrete signature components;

whereby during verification, said second plaintext bit string  $V$  is available from said signature  $(s, c, V)$  as an input to a verification protocol.

17. The cryptographic unit according to claim 16 wherein redundancy in said first plaintext bit string  $H$  is compared to a predetermined level prior to computing said first signature component  $c$ .

18. The cryptographic unit according to claim 17 wherein said redundancy is adjusted to exceed a predetermined level.

19. The cryptographic unit according to claim 18 wherein data is added to said first plaintext bit string  $H$  to adjust said redundancy.

20. The cryptographic unit according to claim 19 wherein an indicator is included in said first plaintext bit string  $H$  to indicate additional data.

21. The cryptographic unit according to any one of claims 16 to 20 wherein said second signature component s is generated by hashing said first signature component c and said second plaintext bit string V.
22. A cryptographic unit for verifying a plaintext message from a signature of a purported signer in a data transmission system, said plaintext message being subdivided into a first plaintext bit string H and a second plaintext bit string V, said signature formed as a set of discrete components, said signature containing a first component computed as a function of said first plaintext bit string H whereby said bit string H is encrypted therein, and said second plaintext bit string V as a second component, said purported signer having a private key used in the computation of said signature and a corresponding public key available for use in verification, said cryptographic unit comprising a computing device for implementing instructions, said instructions comprising:
  - receiving said signature;
  - generating a value by combining said first component with said second plaintext bit string V;
  - recovering said first plaintext bit string H from said value using publicly available information of the purported signer including said public key;
  - examining said recovered first plaintext bit string H for a predetermined characteristic; and
  - verifying said message if said predetermined characteristic is present.
23. The cryptographic unit according to claim 22 wherein said combination of said first component and said second plaintext bit string V includes hashing a combination of said first component and said second plaintext bit string V.
24. The cryptographic unit according to any one of claims 22 and 23 wherein said predetermined characteristic is the redundancy of said recovered first plaintext bit string H.
25. The cryptographic unit according to claim 24 wherein said signature includes a third component derived from a combination of said first component and said second plaintext bit string V and said first plaintext bit string H is recovered utilising said third component.

26. The cryptographic unit according to any one of claims 16 to 21 wherein said first signature component  $c$  is computed by applying a function to said first plaintext bit string  $H$  and said first plaintext bit string  $H$  may be recovered from said first signature component  $c$  by applying a complementary function to said first signature component  $c$ .

27. The cryptographic unit according to claim 26 wherein said function is encryption with an encryption key, a decryption key is computable from information available in said signature, and said complementary function is decryption with said decryption key.

28. The cryptographic unit according to claim 27, wherein said encryption key is a short-term derived from a random integer used in the provision of said second signature component.

29. A system for authenticating a communication between a first correspondent and a second correspondent in a data transmission system, said first correspondent having a private key  $a$  and a public key derived from the private key  $a$ , said public key being available to said second correspondent, said system comprising a first cryptographic unit associated with said first correspondent and a second cryptographic unit associated with said second correspondent, said system being configured for having:

    said first cryptographic unit subdivide a plaintext message into a first plaintext bit string  $H$  and a second plaintext bit string  $V$ ;

    said first cryptographic unit compute a first signature component  $c$  as a function of said first plaintext bit string  $H$  wherein the plaintext bit string  $H$  is hidden in said signature component  $c$ ;

    said first cryptographic unit compute an intermediate signature component  $c'$  as a function of said first signature component  $c$  and said second plaintext bit string  $V$ ;

    said first cryptographic unit compute a second signature component  $s$  as a function of said intermediate signature component  $c'$  and said private key  $a$ ;

    said first cryptographic unit form a signature  $(s, c, V)$  containing said first signature component  $c$ , said second signature component  $s$ , and said second plaintext bit string  $V$  as discrete signature components;

    said first cryptographic unit make available to said second correspondent, at least said first signature component  $c$  and said second plaintext bit string  $V$ ;

    said second cryptographic unit generate a value by combining said first signature component  $c$  with said second plaintext bit string  $V$ ;

said second cryptographic unit recover said first plaintext bit string H from said value using publicly available information of said first correspondent including said public key;

    said second cryptographic unit examine said recovered first plaintext bit string H for a predetermined characteristic; and

    said second cryptographic unit verify said message if said predetermined characteristic is present.

30. A method for digitally signing a message M to restrict access to a portion of said message M comprising:

    subdividing said message M into a pair of bit strings H, V;

    hiding one of said bit strings H corresponding to said portion of said message M by encrypting said one bit string H in the generation of at least one signature component according to a mathematical function utilizing a private key having a corresponding public key such that said public key is required to recover said one bit string H from said at least one signature component;

    providing said at least one signature component and the other of said bit strings V in a signature; and

    restricting access to said public key to enable only those privy to said public key to recover said one bit string H while said other bit string V is available to all.

31. The method according to claim 30 wherein said restricting access comprises containing said public key in a certificate.

32. The method according to claim 31 wherein said certificate can only be recovered if a recipient of said signature has a certifying authority's public key, said certifying authority having issued said certificate.

33. The method according to any one of claims 30 to 32 wherein said signature comprises three components (c, s, V) including a first component c encrypting said one bit string H, a second component s generated using a combination of said first component c, said other bit string V and said private key, and a third component being said other bit string V in the clear.

34. The method according to claim 33 wherein said public key is required to generate a decryption key for recovering said one bit string H from said first component c.

35. The method according to claim 33 wherein generation of said second components also utilizes a randomly generated integer k.

36. The method according to claim 35 wherein said one bit string H is encrypted using a value R of a random point kP generated using said integer k.

37. The method according to any one of claims 30 to 36 wherein said public key is contained in indicia provided with said signature.

38. A cryptographic unit for digitally signing a message (M), said cryptographic unit comprising a computing device for implementing instructions according to the method of any one of claims 30 to 37.

39. A computer program product comprising a data carrier, said data carrier comprising computer executable instructions for performing the method according to any one of claims 30 to 37.

40. A method of accessing information in a message M subdivided into a pair of bit strings H, V from a signature, said method comprising:

obtaining said signature, said signature comprising at least one signature component that hides one of said bit strings H by encrypting said one bit string H in the generation of said at least one signature component according to a mathematical function utilizing a private key having a corresponding public key such that said public key is required to recover said one bit string H from said at least one signature component, and comprising the other of said pair of bit strings V;

if permitted, obtaining said public key, wherein access to said public key is restricted to enable only those privy to said public key to recover said one bit string H while said other bit string V is available to all; and

utilizing said public key to decrypt said one of said bit strings H to provide access to information in said one bit string H.

41. The method according to claim 40 wherein said public key is accessed from a certificate.

42. The method according to claim 41 wherein said certificate can only be recovered if a recipient of said signature has a certifying authority's public key, said certifying authority having issued said certificate.

43. The method according to any one of claims 40 to 42 wherein said signature comprises three components (c, s, V) including a first component c encrypting said one bit string H, a second component s generated using a combination of said first component c, said other bit string V and said private key, and a third component being said other bit string V in the clear.

44. The method according to claim 43 wherein said public key is used to generate a decryption key for recovering said one bit string H from said first component c.

45. The method according to claim 43 wherein generation of said second component s also utilizes a randomly generated integer k.

46. The method according to claim 45 wherein said one bit string H has been encrypted using a value R of a random point kP generated using said integer k.

47. The method according to any one of claims 40 to 56 wherein said public key is obtained from indicia provided with said signature.

48. A cryptographic unit configured to access information in a message M subdivided into a pair of bit strings H, V by performing the method according to any one of claims 40 to 47.

49. A computer program product comprising a data carrier, said data carrier comprising computer executable instructions for performing the method according to any one of claims 40 to 47.

5

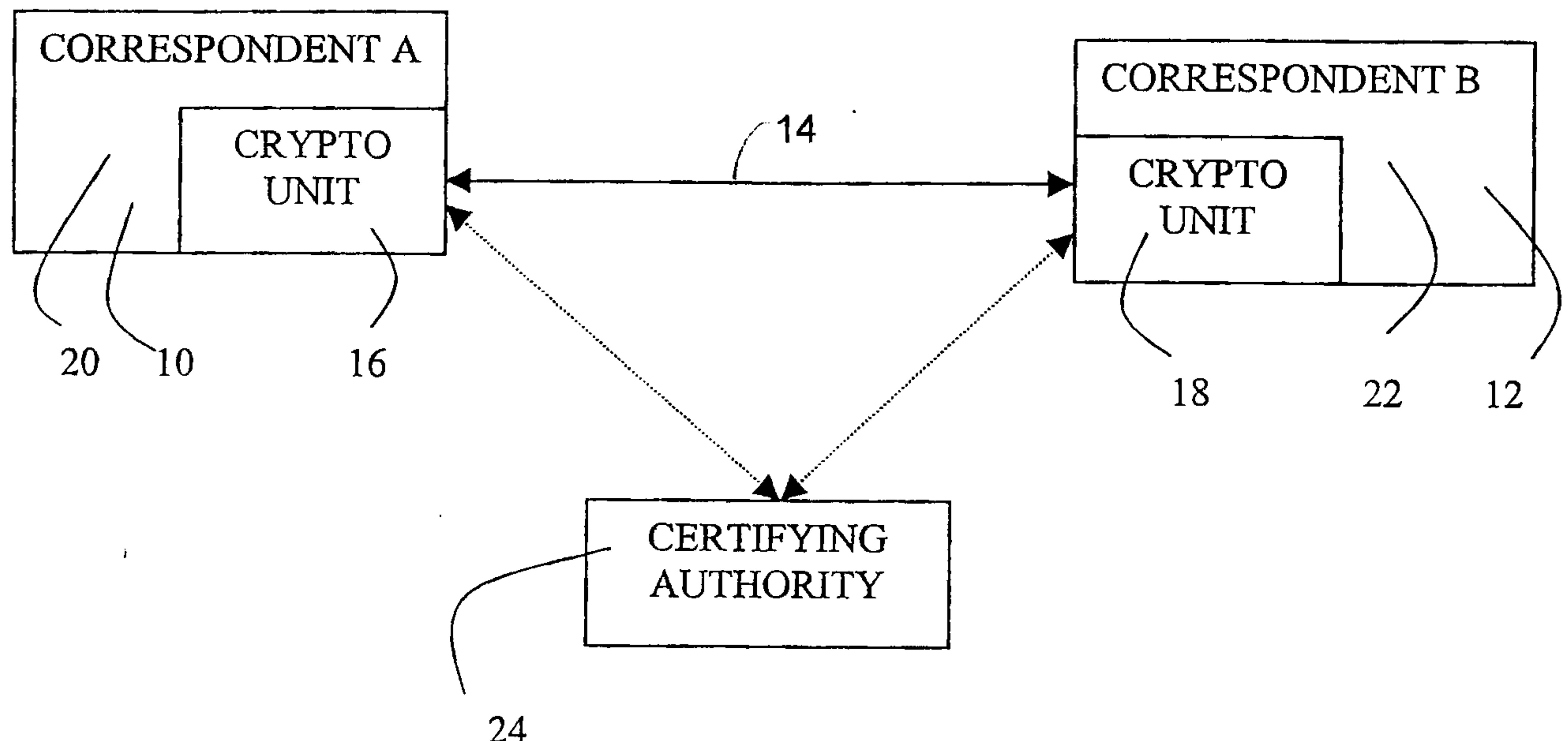


FIG.1

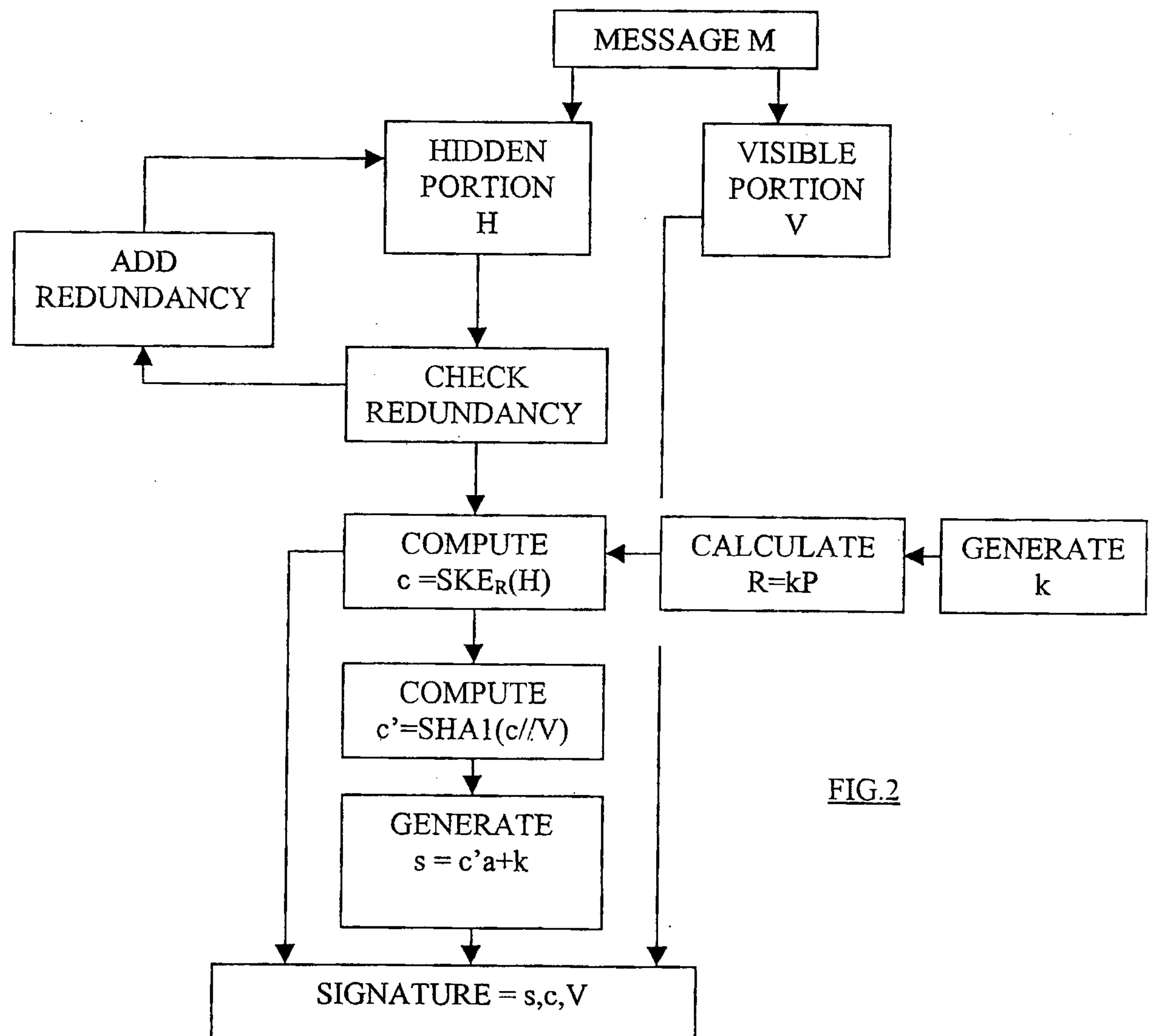


FIG.2

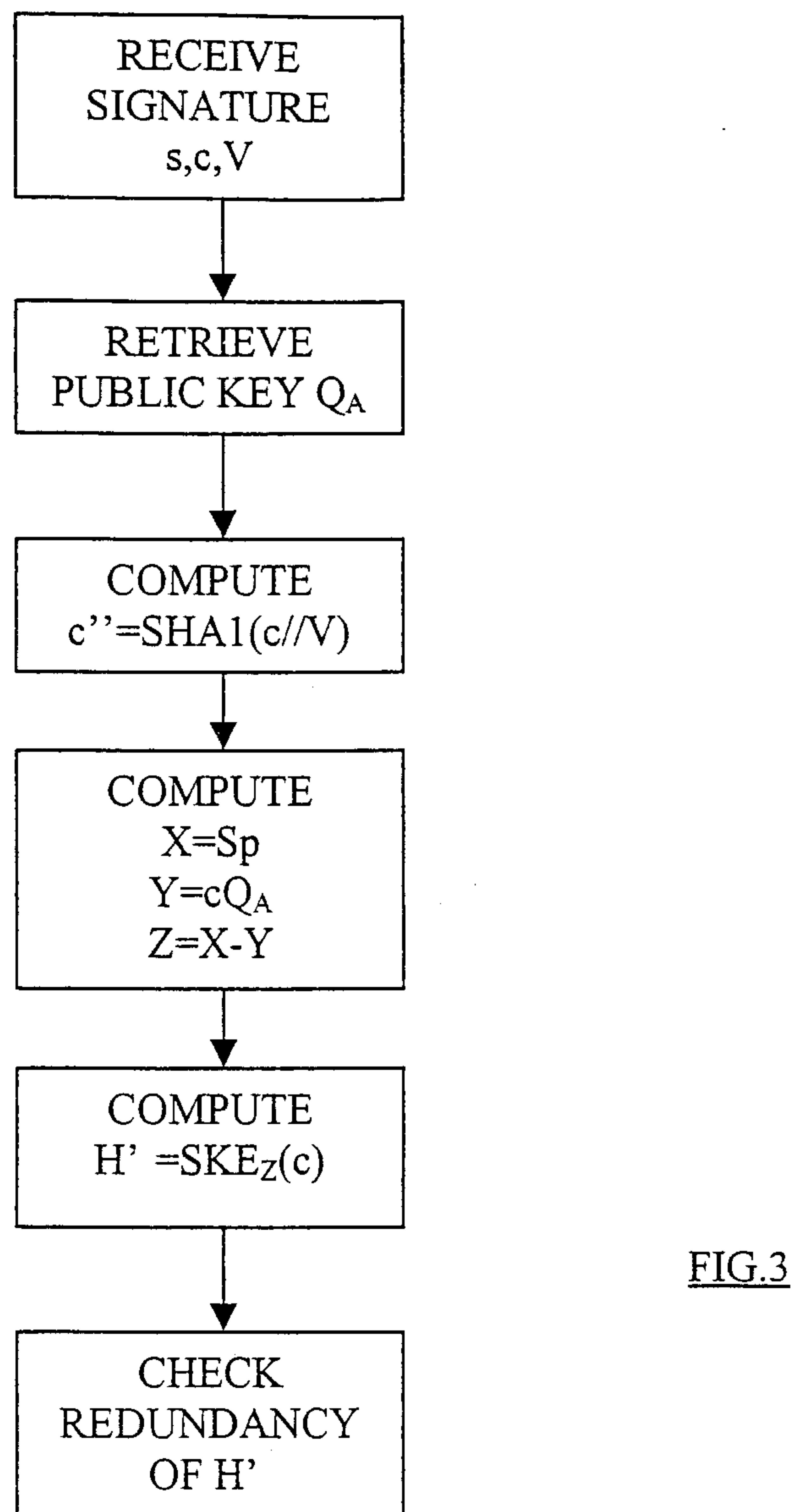
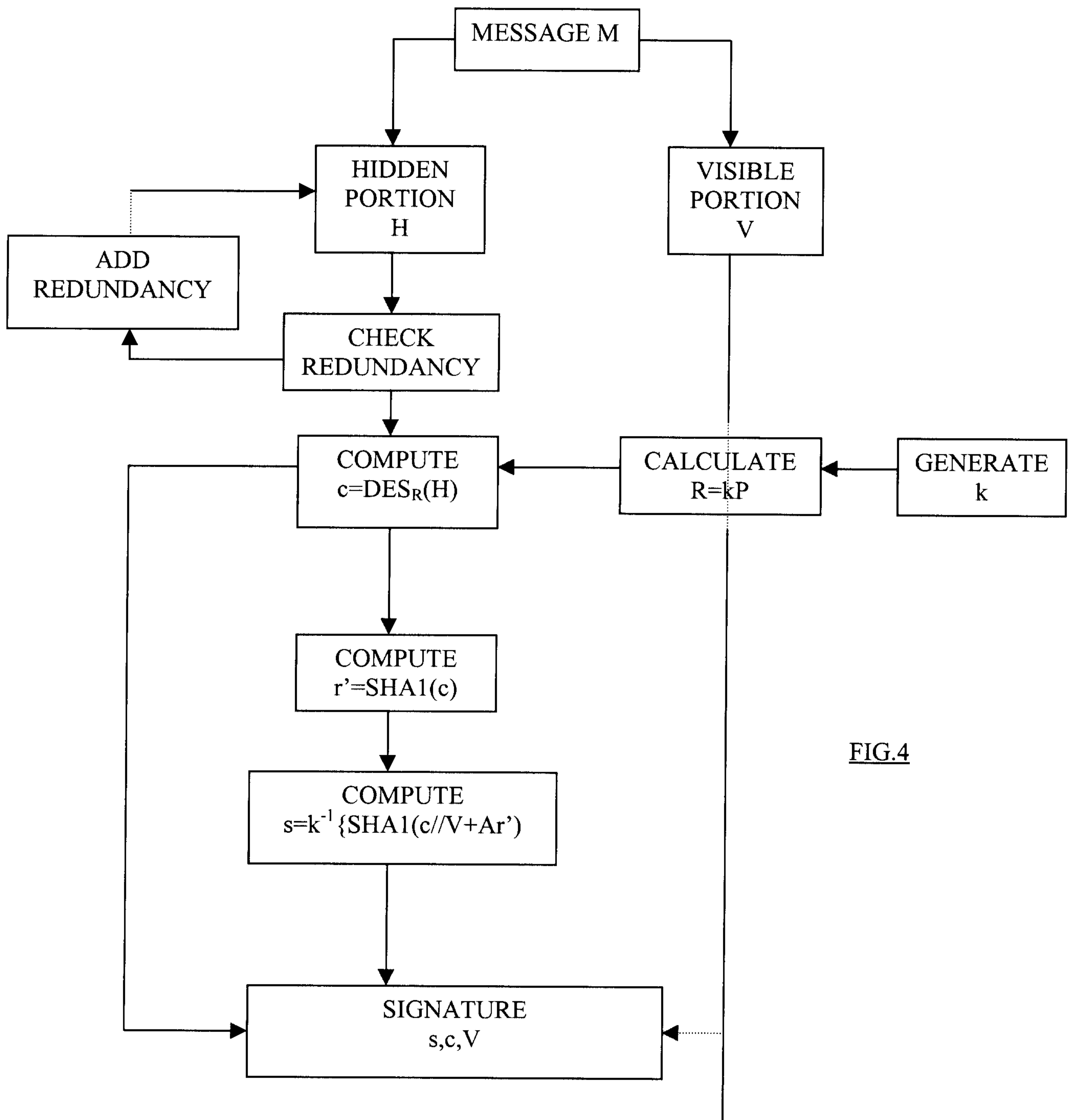


FIG.3



**FIG.4**

CORRESPONDENT A

CRYPTO  
UNIT

20 10

16

14

CORRESPONDENT B

CRYPTO  
UNIT

18

22

12

CERTIFYING  
AUTHORITY