(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 306 670 A8

(12) # CORRECTED EUROPEAN PATENT APPLICATION

(15) Correction information:
Corrected version no 1 (W1 A2)
Corrections, see
Bibliography INID code(s) 71

(48) Corrigendum issued on:
16.11.2011 Bulletin 2011/46

(43) Date of publication:
06.04.2011 Bulletin 2011/14

(21) Application number: **10184915.6**

(22) Date of filing: **07.09.2000**

(51) Int Cl.:
H04L 9/32 $^{(2006.01)}$

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
07111040.7 / 1 830 514
00119558.5 / 1 083 700

(27) Previously filed application:
07.09.2000 EP 07111040

(71) Applicants:
- **Certicom Corp.**
  Mississauga, Ontario L4W 0B5 (CA)
- **Pitney Bowes Inc.**
  Stamford, CT 06926-0700 (US)

(72) Inventors:
- **Pintsov, Leon**
  West Hartford, CT 06117 (US)
- **Ryan, Rick**
  Oxford, CT 06478 (US)
- **Singer, Ari**
  Solon, OH 44139 (US)
- **Vanstone, Scott Alexander**
  Mississauga Ontario L4W 5L1 (CA)
- **Gallant, Robert**
  Mississauga Ontario L4W 5L1 (CA)
- **Lambert, Robert J**
  Cambridge Ontario N3C 3N3 (CA)

(74) Representative: **Finnie, Peter John et al**
Gill Jennings & Every LLP
The Broadgate Tower
20 Primrose Street
London EC2A 2ES (GB)

Remarks:
•This application was filed on 30-09-2010 as a divisional application to the application mentioned under INID code 62.
•Claims filed after the date of filing of the application (Rule 68(4) EPC).

(54) ## Hybrid digital signature scheme

(57) 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 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.

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

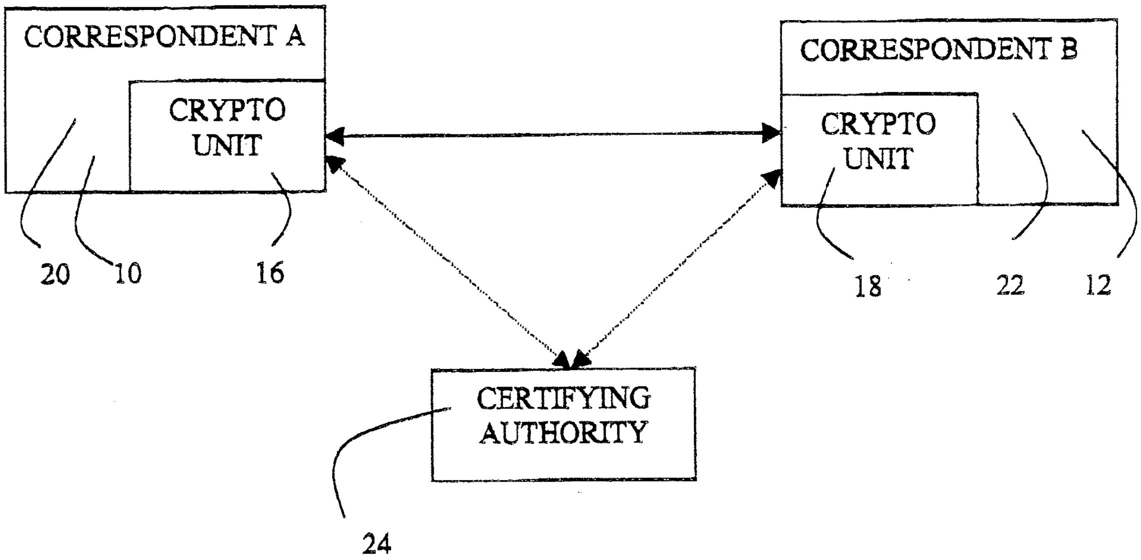
CORRESPONDENT A
CRYPTO UNIT
CORRESPONDENT B
CRYPTO UNIT
20
10
16
18
22
12
CERTIFYING AUTHORITY
24

FIG.1

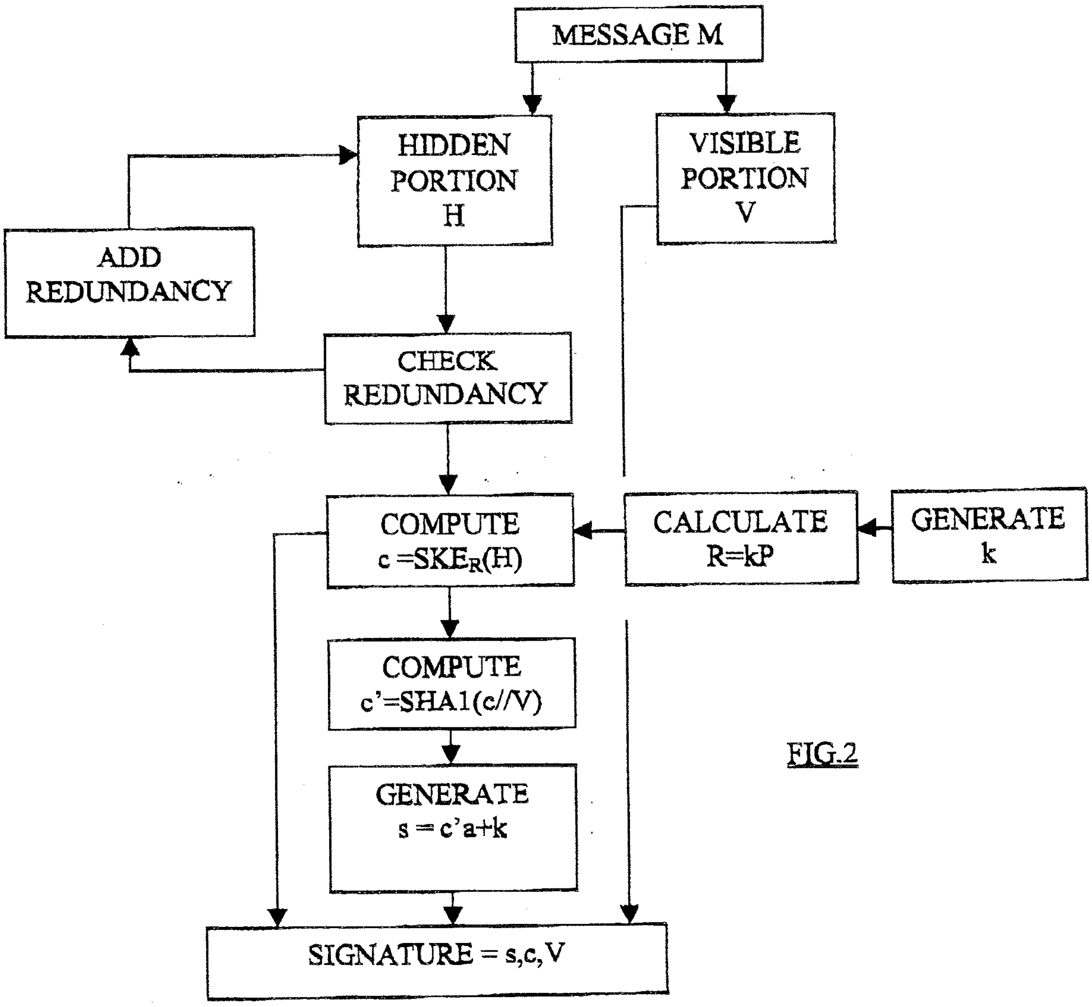
MESSAGE M
HIDDEN PORTION H
VISIBLE PORTION V
ADD REDUNDANCY
CHECK REDUNDANCY
COMPUTE c =SKE_R(H)
CALCULATE R=kP
GENERATE k
COMPUTE c'=SHA1(c//V)
GENERATE s = c'a+k
SIGNATURE = s,c,V

FIG.2