PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10

A3

(11) International Publication Number: **WO 98/34202**

(43) International Publication Date: 6 August 1998 (06.08.98)

(21) International Application Number: PCT/CA98/00056

(22) International Filing Date: 3 February 1998 (03.02.98)

(30) Priority Data:
9702152.1 3 February 1997 (03.02.97) GB

(71) Applicant: CERTICOM CORP. [CA/CA]; Suite 103, 200 Matheson Boulevard West, Mississauga, Ontario L5R 3L7 (CA).

(72) Inventor: VANSTONE, Scott, A.; 539 Sandbrook Court, Waterloo, Ontario N2T 2H4 (CA).

(74) Agents: ORANGE, John, R., S. et al.; Orange & Associates, Toronto Dominion Bank Tower, Suite 3600, Toronto–Dominion Centre, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
10 December 1998 (10.12.98)

(54) Title: DATA CARD VERIFICATION SYSTEM

(57) Abstract

A method of verifying a pair of correspondents in electronic transaction, the correspondents each including first and second signature schemes and wherein the first signature scheme is computationally more difficult in signing than verifying and the second signature scheme is computationally more difficult in verifying than signing. The method comprises the step of the first correspondent signing information according to the first signature scheme and transmitting the first signature to the second correspondent, the second correspondent verifying the first signature received from the first correspondent, wherein the verification is performed according to the first signature scheme. The second correspondent then signs information according to the second signature scheme and transmits the second signature to the first correspondent, the first correspondent verifies the second signature received from the second correspondent, wherein the verification is performed according to the second signature algorithm; the transaction is rejected if either verification fails. The method thereby allows one of the correspondents to participate with relatively little computing power while maintaining security of the transaction.

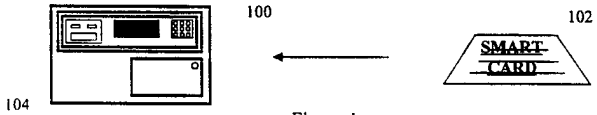

Figure 1a

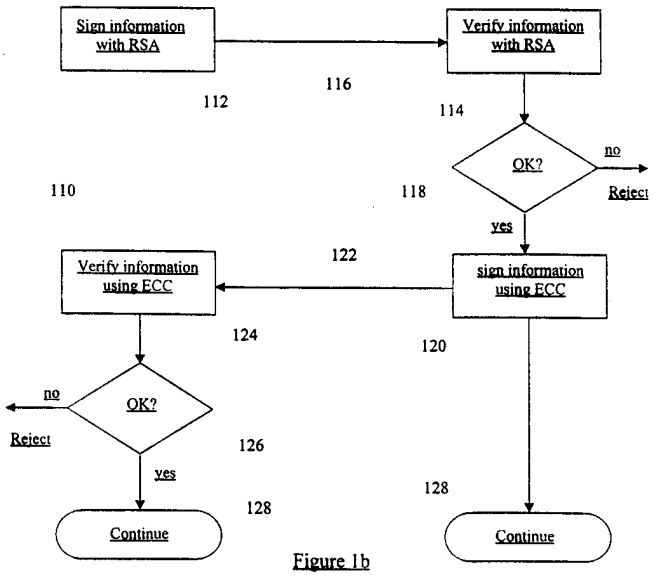

Figure 1b

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

Inter. ..nal Application No
PCT/CA 98/00056

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

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)
IPC 6 G07F 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 practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MIYAJI A: "ELLIPTIC CURVES SUITABLE FOR CRYPTOSYSTEMS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, vol. E77-A, no. 1, 1 January 1994, pages 98-104, XP000439669 see the whole document ---	1-6
A	EP 0 588 339 A (NIPPON TELEGRAPH & TELEPHONE) 23 March 1994 see abstract; claims; figures --- -/--	1-6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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	Date of mailing of the international search report
16 October 1998	26/10/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter. ...nal Application No
PCT/CA 98/00056

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication,where appropriate. of the relevant passages	Relevant to claim No.
A	SCHNORR C P: "EFFICIENT SIGNATURE GENERATION BY SMART CARDS" JOURNAL OF CRYPTOLOGY, vol. 4, no. 3, 1 January 1991, pages 161-174, XP000574352 see the whole document	1-6
A	US 5 218 637 A (ANGEBAUD DIDIER ET AL) 8 June 1993 see the whole document	1,2,5,6
A	WO 91 16691 A (JONHIG LTD) 31 October 1991 see page 5, line 25 - page 6, line 7 see page 15, line 28 - page 18, line 6; claims 7-11; figures 4,5	1-6
A	KENJI KOYAMA ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR APPLICATIONS" IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, vol. E75 - D, no. 1, 1 January 1992, pages 50-57, XP000301174 see the whole document	1-6
A	WALEFFE D DE ET AL: "CORSAIR: A SMART CARD FOR PUBLIC KEY CRYPTOSYSTEMS" ADVANCES IN CRYPTOLOGY - PROCEEDINGS OF CRYPTO, SANTA BARBARA, AUG. 11 - 15, 1990, no. CONF. 10, 1 January 1990, pages 502-513, XP000260013 MENEZES A J;VANSTONE S A see the whole document	1,2,4-6
A	US 4 748 668 A (SHAMIR ADI ET AL) 31 May 1988 see abstract; figures	1,5,6
A	FR 2 536 928 A (FRANCE ETAT) 1 June 1984 see the whole document	1
A	KOBLITZ N: "ELLIPTIC CURVE CRYPTOSYSTEMS" MATHEMATICS OF COMPUTATION, vol. 48, no. 177, January 1987, pages 203-209, XP000671098	
A	US 4 890 323 A (BEKER HENRY J ET AL) 26 December 1989	

5

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter- ional Application No
PCT/CA 98/00056

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0588339 A	23-03-1994	JP 6103425 A	15-04-1994
		JP 6103426 A	15-04-1994
		JP 6162289 A	10-06-1994
		JP 6162287 A	10-06-1994
		JP 6161354 A	07-06-1994
		EP 0856821 A	05-08-1998
		EP 0856822 A	05-08-1998
		US 5396558 A	07-03-1995
		US 5446796 A	29-08-1995
		US 5502765 A	26-03-1996
US 5218637 A	08-06-1993	FR 2620248 A	10-03-1989
		FR 2663141 A	13-12-1991
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		EP 0311470 A	12-04-1989
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5140634 A	18-08-1992
		DE 69108786 D	18-05-1995
		DE 69108786 T	16-11-1995
		EP 0461983 A	18-12-1991
		JP 6084026 A	25-03-1994
WO 9116691 A	31-10-1991	AT 127949 T	15-09-1995
		AU 653721 B	13-10-1994
		AU 7664491 A	11-11-1991
		CA 2058982 A	13-10-1991
		CN 1057535 A,B	01-01-1992
		DE 69112975 D	19-10-1995
		DE 69112975 T	29-02-1996
		DK 479982 T	13-11-1995
		EP 0479982 A	15-04-1992
		ES 2034929 T	16-11-1995
		GR 92300099 T	16-03-1993
		GR 3017457 T	31-12-1995
		HK 175596 A	27-09-1996
		NO 303198 B	08-06-1998

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 98/00056

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9116691 A		PL 169723 B	30-08-1996
		US 5623547 A	22-04-1997
		US 5778067 A	07-07-1998
US 4748668 A	31-05-1988	AU 592207 B	04-01-1990
		AU 7526687 A	14-01-1988
		DE 3782099 A	12-11-1992
		EP 0252499 A	13-01-1988
		JP 2511464 B	26-06-1996
		JP 63101987 A	06-05-1988
FR 2536928 A	01-06-1984	NONE	
US 4890323 A	26-12-1989	AU 590082 B	26-10-1989
		AU 7326487 A	26-11-1987
		EP 0246823 A	25-11-1987
		GB 2190820 A,B	25-11-1987
		HK 78690 A	12-10-1990
		JP 63010839 A	18-01-1988