



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/08	A3	(11) International Publication Number: WO 97/16902 (43) International Publication Date: 9 May 1997 (09.05.97)
(21) International Application Number: PCT/US96/17479 (22) International Filing Date: 1 November 1996 (01.11.96) (30) Priority Data: 552,029 2 November 1995 (02.11.95) US (71) Applicant: TRI-STRATA SECURITY, INC. [US/US]; Suite 100, Lagoon Drive #3, Redwood City, CA 94065 (US). (72) Inventor: ATALLA, Martin, M.; 18 Monte Vista, Atherton, CA 94027 (US). (74) Agent: MACPHERSON, Alan, H.; Skjerven, Morrill, MacPherson, Franklin & Friel, Suite 700, 25 Metro Drive, San Jose, CA 95110 (US).		(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, HU, 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, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), 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 <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i> (88) Date of publication of the international search report: 28 August 1997 (28.08.97)
(54) Title: UNIFIED END-TO-END SECURITY METHODS AND SYSTEMS FOR OPERATING ON INSECURE NETWORKS		
(57) Abstract Secure transmission of a message is achieved by using a one-time encryption key derived at the receiver and the sender from information present at both the sender and the receiver, but wherein the information from which the encryption key is derived is not transmitted between the sender and the receiver. A plurality of bytes, known as a master signature, is randomly generated and stored at the sender, wherein each byte is uniquely identified by an address. A first random subset of this plurality of bytes, called an access signature, and the addresses in the master signature of the bytes in this access signature, are stored at the receiver. To generate an encryption key, the receiver selects a second random subset of bytes, known as a session signature, from the access signature and sends the addresses in the master signature of the bytes in this session signature to the sender. The sender uses these addresses to identify the bytes in this session signature which bytes are used at both the sender and the receiver to derive the encryption key. If desired, these bytes can be used directly as the encryption key but preferably, these bytes are passed through a session signature-to-session key converter using an irreversible algorithm to generate a one-time encryption key to be used to encrypt the message to be sent between the sender and the receiver. The master signature can also be derived from the digitized video image of the user, which allows a card containing the master signature to be used as described above but also with a video monitor to visually identify the user.		

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.

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

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 96/17479

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

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 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.
X A	EP 0 032 107 A (GRETAG) 15 July 1981 see page 4, last paragraph - page 5, line 14 see page 6, line 16 - line 26 see page 12, paragraph 2 ---	37,79,98 1,2,13, 18,20, 48,49
A	EP 0 447 063 A (GENERAL INSTRUMENT) 18 September 1991 see column 3, line 46 - column 4, line 4 see column 5, line 24 - line 41 see column 6, line 41 - line 53 --- -/--	1,14,15, 37,79

☒ Further documents are listed in the continuation of box C.

☒ 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

3 July 1997

Date of mailing of the international search report

21.07.97

Name and mailing address of the ISA

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

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

Intern. Application No

PCT/US 96/17479

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	IEEE IN HOUSTON. GLOBECOM '93. IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, INCLUDING A COMMUNICATIONS THEORY MINI-CONFERENCE. TECHNICAL PROGRAM CONFERENCE RECORD (CAT. NO.93CH3250-8), PROCEEDINGS OF GLOBECOM '93. IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, ISBN 0-7803-0917-0, 1993, NEW YORK, NY, USA, IEEE, USA, pages 164-170 vol.1, XP000428048 TSUBAKIYAMA H ET AL: "Security for information data broadcasting system with conditional-access control" see page 165, right-hand column, paragraph 1; figure 3	3,12,20, 34,41, 50,57,68
A	US 5 351 293 A (MICHENER ET AL.) 27 September 1994 see column 5, line 50 - column 6, line 35	29,31
X	GB 2 223 614 A (WARING) 11 April 1990 see page 2, line 9 - line 30 see page 5, line 18 - line 20 see page 6, line 7 - line 18 see page 8, line 6 - line 25 see page 10, line 28 - line 35 see page 11, line 15 - line 18 see page 12, line 7 - line 10	42,45, 85,88
A	DE 42 43 908 A (GAO) 30 June 1994 see column 2, line 10 - line 15 see column 3, line 38 - line 46 see column 5, line 1 - line 21 see column 2, line 37 - line 50	42,45, 85,88
A	NL 9 200 876 A (FACIES) 16 December 1993 see page 2, line 7 - page 3, line 31	42,45, 85,88
A	US 5 115 467 A (ESSERMAN ET AL.) 19 May 1992 see column 3, line 1 - line 64 see column 4, line 18 - line 35 see column 4, line 58 - line 65	92
X	WO 95 09498 A (MOTOROLA) 6 April 1995 see abstract	36,78,96
A	see page 5, last line - page 6, line 28 see page 7, line 1 - line 9	35,77, 100

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 96/ 17479

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see annex

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/210

1. Subject: claims 1-34, 37-41, 48-76, 79-84, 93-95, 98, 99
Method or system for securing transmission wherein the encryption key is identified at the sender by means of addresses sent from the receiver.
2. Subject: claims 35, 36, 77, 78
Method or system where in a hub or central telephone office a first encryption key is encrypted using a second encryption key and where the first encryption key is decrypted at the receiver
3. Subject: claims 42-47, 85-90
Method and system for generating a user memory card identifying a user by providing a digital image of the user.
4. Subject: claims 91 and 92
Method of protecting a signature held by a network computer.
5. Subject: claims 96, 97 100
Method of transmitting data from a sender to a receiver through a hub where the data are decrypted and re-encrypted at the hub to be decrypted at the receiver.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. Application No

PCT/US 96/17479

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 32107 A	15-07-81	JP 1014592 B JP 1528828 C JP 56142574 A US 4369434 A	13-03-89 15-11-89 06-11-81 18-01-83
EP 447063 A	18-09-91	US 5151938 A AU 639076 B AU 7279091 A CA 2037778 A JP 4220743 A	29-09-92 15-07-93 19-09-91 14-09-91 11-08-92
US 5351293 A	27-09-94	NONE	
GB 2223614 A	11-04-90	NONE	
DE 4243908 A	30-06-94	NONE	
NL 9200876 A	16-12-93	NONE	
US 5115467 A	19-05-92	NONE	
WO 9509498 A	06-04-95	US 5410602 A EP 0671091 A FI 952405 A JP 8504073 T	25-04-95 13-09-95 17-05-95 30-04-96