PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/28

A3

(11) International Publication Number: WO 98/59456

(43) International Publication Date: 30 December 1998 (30.12.98)

(21) International Application Number: PCT/US98/12691

(22) International Filing Date: 18 June 1998 (18.06.98)

(30) Priority Data:

08/879,708	20 June 1997 (20.06.97)	US
08/923,095	4 September 1997 (04.09.97)	US

(71) Applicant: SECURE CHOICE LLC [US/US]; P.O. Box 223719, Chantilly, VA 20153–3719 (US).

(72) Inventor: McGOUGH, Paul; 15210 Wetherburn Drive, Centreville, VA 20120 (US).

(74) Agent: FORTKORT, Michael, P.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (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, GH, GM, GW, 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, CY, 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: 1 April 1999 (01.04.99)

(54) Title: METHOD AND SYSTEM FOR PERFORMING SECURE ELECTRONIC MESSAGING

(57) Abstract

A secure electronic messaging system (SEMS) provides absolute system security and user-defined message security for electronic messaging between two public entities. These messages can be of any kind provided the contents are created using a defined master alphabet of 81 characters of less. The SEMS encrypts and decrypts source message data using a series of message keys that are derived from a private, numeric orginal key known only by both parties sending and receiving messages. The message key suite absolutely secures the original key from discovery. The secure distribution of these original keys will be under the same methods that the public entities would use to discover each other such as an opening an account, making a public inquiry for membership, etc. The SEMS translates message content character into number based on a message key suite dependent distribution of the master alphabet and then uses a series of equations to encrypt the numbers.

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

International application No.
PCT/US98/12691

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H 04L 9/28
US CL : 380/28

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)

U.S. : 380/28,42,45,44,51

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

RITTER'S CRYPTO GLOSSARY AND DICTIONARY OF TECHNICAL CRYPTOGRAPHY

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

APS: cipher,cypher,crypt,scramble,matrix,matrices,polyalphabetic,encrypted digital signature,carriage return

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,195,196 A (FEISTEL) 25 March 1980, column 3, lines 26-28, 38-40, column 4, lines 61-68, column 5, lines 1-7	1,10,12,13,21,24, 25
Y	US 4,675,477 A (THORNWALL) 23 June 1987, column 1, lines 20-38, 47-51	1,10,12,13,21,24, 25
Y,E	US 5,796,832 A (DAWAN) 18 August 1998, column 7, lines 49-58	12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search
02 DECEMBER 1998

Date of mailing of the international search report
03 FEB 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
GAIL HAYES for
Telephone No. (703) 305-9711

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