

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
20 March 2003 (20.03.2003)

PCT

(10) International Publication Number  
**WO 03/024140 A3**

(51) International Patent Classification<sup>7</sup>: **H04Q 7/38**

Viabes Industrial Estate, Basingstoke, Hampshire RG22 4PD (GB). **SHAHAF, Mark** [IL/IL]; Motorola Communications Israel, Limited, 3 Kremenetski Street, 67899 Tel Aviv (IL).

(21) International Application Number: PCT/GB02/04138

(22) International Filing Date:  
11 September 2002 (11.09.2002)

(74) Agent: **MCCORMACK, Derek**; Motorola European Intellectual, Property Operations, Midpoint, Alencon Link, Basingstoke, Hampshire RG21 7PL (GB).

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
0121979.9 11 September 2001 (11.09.2001) GB

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(71) Applicant (*for all designated States except US*): **MOTOROLA INC** [US/US]; 1303 E.Algonquin Road, Schaumburg, IL 60196 (US).

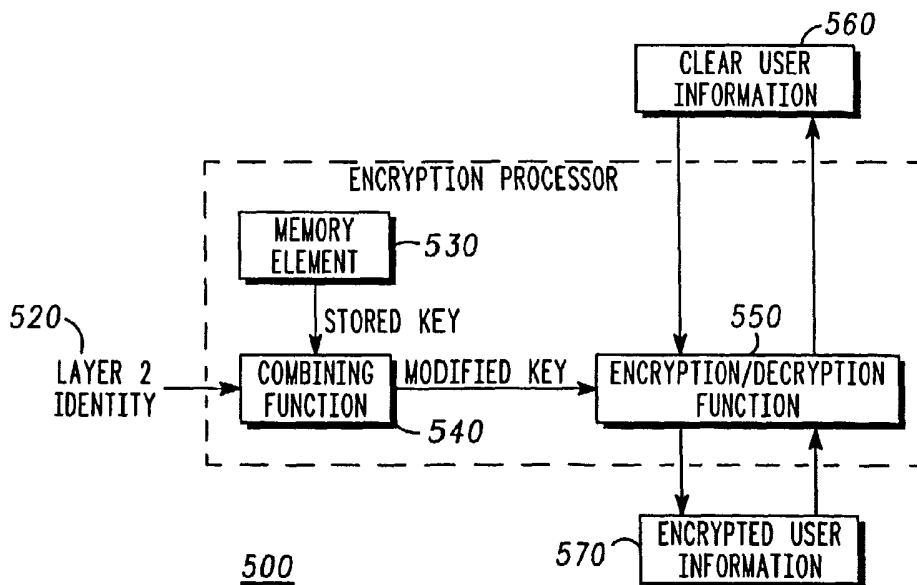
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **CHATER-LEA, David, John** [GB/GB]; Motorola Limited, Jays Close,

[Continued on next page]

(54) Title: COMMUNICATIONS METHODS, SYSTEMS AND TERMINALS



(57) Abstract: A method of encrypting information to be transmitted by a transmitting terminal in a communication system providing secure communications between a plurality of terminals employing an encryption protocol that uses a shared encryption key in each of the plurality of terminals, the method including modifying the share encryption key in the transmitting terminal to provide a modified encryption key and encrypting the information to be transmitted using the modified encryption key, characterised in that the share encryption key is modified by combining with the shared encryption key identifier code used in the communication system to identify the transmitting terminal. A corresponding method of decryption and a system and mobile radio terminal using the method are also described.



WO 03/024140 A3



ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**(88) Date of publication of the international search report:**  
5 June 2003

**Published:**

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# INTERNATIONAL SEARCH REPORT

Internat	Application No
PCT/GB	02/04138

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC 7 H04Q7/38

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 7 H04Q 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)  
 EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 357 571 A (BANWART DEAN E) 18 October 1994 (1994-10-18)	1-7, 10-17, 20, 21, 23-25, 27, 28, 30-33
Y	column 2, line 25 - line 56  column 4, line 1 - line 14 column 5, line 20 - line 59  -----  -/--	8, 9, 18, 19, 22, 26, 29

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.
- \*8\* document member of the same patent family

Date of the actual completion of the international search

17 April 2003

Date of mailing of the international search report

25/04/2003

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

Schut, G

**INTERNATIONAL SEARCH REPORT**

Internat:	Application No
PCT/GB	02/04138

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>"Terrestrial Trunked Radio (TETRA);Voice plus Data (V+D); Part 7: Security; 3 Definitions, symbols and abbreviations; 4.2 Air Interface key management mechanisms; 4.5 OTAR Protocols; A.2 OTAR PDUs"</p> <p>ETSI EN 300392-7 V2.1.1, XX, XX, 16 February 2001 (2001-02-16), pages ,12-15,21-28,47-65,110-115, XP002224025 paragraph '4.2.4! paragraph '4.5.2!</p> <p align="center">---</p>	<p>8,9,18, 19,22, 26,29</p>
A	<p>PARKINSON D W: "TETRA SECURITY" BT TECHNOLOGY JOURNAL, BT LABORATORIES, GB, vol. 19, no. 3, July 2001 (2001-07), pages 81-88, XP001096932 ISSN: 1358-3948</p> <p align="center">-----</p>	

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Internat	Application No
PCT/GB	02/04138

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
US 5357571	A	18-10-1994	AU	663258 B2	28-09-1995
			AU	6480394 A	27-01-1995
			BR	9402606 A	04-04-1995
			CA	2126054 A1	02-01-1995
			CN	1105168 A ,B	12-07-1995
			CZ	9401538 A3	18-01-1995
			DE	4423209 A1	19-01-1995
			FR	2708403 A1	03-02-1995
			GB	2279537 A ,B	04-01-1995
			MX	9405038 A1	31-01-1995
			PL	304010 A1	09-01-1995
			RU	2121231 C1	27-10-1998

---