

(51) International Patent Classification:  
H04L 9/08 (2006.01)(21) International Application Number:  
PCT/GB2010/001737(22) International Filing Date:  
15 September 2010 (15.09.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
0916182.9 15 September 2009 (15.09.2009) GB  
1010166.5 17 June 2010 (17.06.2010) GB(71) Applicant (for all designated States except US): EADS  
DEFENCE AND SECURITY SYSTEMS LIMITED  
[GB/GB]; Quadrant House, Celtic Springs, Coedkernew,  
Newport NP10 8FZ (GB).

(72) Inventor; and

(75) Inventor/Applicant (for US only): FRANCIS, Patrick,  
Jonathan [GB/GB]; EADS Defence And Security Sys-  
tems Limited, Quadrant House, Celtic Springs, Coed-  
kernew, Newport NP10 8FZ (GB).(74) Agents: CRITTEN, Matthew, Peter et al.; Abel & Im-  
ray, 20 Red Lion Street, London WC1R 4PQ (GB).(81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AL, AM,  
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,  
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,  
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,  
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,  
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,  
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,  
SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,  
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (unless otherwise indicated, for every  
kind of regional protection available): ARIPO (BW, GH,  
GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG,  
ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ,  
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,  
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,  
LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK,  
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,  
GW, ML, MR, NE, SN, TD, TG).

## Declarations under Rule 4.17:

— as to the identity of the inventor (Rule 4.17(i))

## Published:

— with international search report (Art. 21(3))

— before the expiration of the time limit for amending the  
claims and to be republished in the event of receipt of  
amendments (Rule 48.2(h))

(88) Date of publication of the international search report:

7 July 2011

(54) Title: KEY GENERATION FOR MULTI-PARTY ENCRYPTION

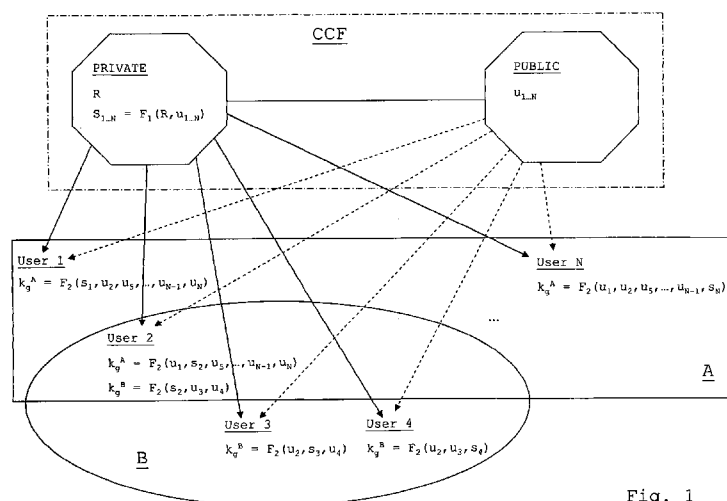


Fig. 1

(57) Abstract: A method of encrypting data to be accessed only by a group of users comprises a user in the group receiving a user secret  $s_i = f_1(R, u_i)$ , the user secret having been created by operating a first one-way function  $f_1$  on parameters comprising a root key  $R$  and a public identifier  $u_i$  for the user. The user in the group receives a public identifier  $u_j$  for each of the other users in the group. The user in the group obtains a group key by operating a second one-way function  $f_2$  on parameters comprising the user secret  $s_i$  and the public identifiers for the other users in the group  $u_1, u_2, \dots, u_{j-1}, u_{j+1}, \dots, u_{N-1}, u_N$ , wherein said second one-way function/band said first one-way function  $f_1$  satisfy:  $f_2(f_1(R, u_1), u_2, \dots, u_n) = f_2(f_1(R, u_2), u_1, u_3, u_4, \dots, u_n) = \dots = f_2(f_1(R, u_n), u_1, u_2, \dots, u_{n-1})$ . The user in the group encrypts the data using the group key.

# INTERNATIONAL SEARCH REPORT

International application No  
PCT/GB2010/001737

A. CLASSIFICATION OF SUBJECT MATTER  
INV. H04L9/08  
ADD.

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)  
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, INSPEC, WPI Data

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02/33883 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; GRUMIAUX FREDERIC [NL]) 25 April 2002 (2002-04-25) abstract page 4 - page 5 claim 2	1-20
A	----- US 2006/191020 A1 (MILLER JOHN L [GB]) 24 August 2006 (2006-08-24) abstract paragraph [0023]	1-20
A	----- US 5 369 705 A (BIRD RAYMOND F [US] ET AL) 29 November 1994 (1994-11-29) abstract column 2, line 33 - line 68 -----	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family 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

19 May 2011

Date of mailing of the international search report

25/05/2011

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040,  
Fax: (+31-70) 340-3016

Authorized officer

San Millán Maeso, J

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/GB2010/001737

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
W0 0233883	A2	25-04-2002	CN 1401171 A	05-03-2003
			EP 1329051 A2	23-07-2003
			JP 2004512734 T	22-04-2004
			US 2003133576 A1	17-07-2003
-----				
US 2006191020	A1	24-08-2006	NONE	
-----				
US 5369705	A	29-11-1994	JP 2601983 B2	23-04-1997
			JP 6061999 A	04-03-1994
-----				