(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2008 (19.06.2008)

PCT

(10) International Publication Number
WO 2008/071703 A3

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/EP2007/063712

(22) International Filing Date:
11 December 2007 (11.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/611,128 14 December 2006 (14.12.2006) US

(71) Applicant *(for all designated States except US)*: **Telefonaktiebolaget LM Ericsson (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GEHRMANN, Christian** [SE/SE]; Skördevägen 2C, S-227 38 Lund (SE). **SMEETS, BEN** [SE/SE]; Dalbackavägen 11, S-240 10 Dalby (SE).

(74) Agents: **ONSHAGE, Anders** et al.; Ericsson AB, Nya Vattentornet, S-221 83 Lund (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: EFFICIENT DATA INTEGRITY PROTECTION

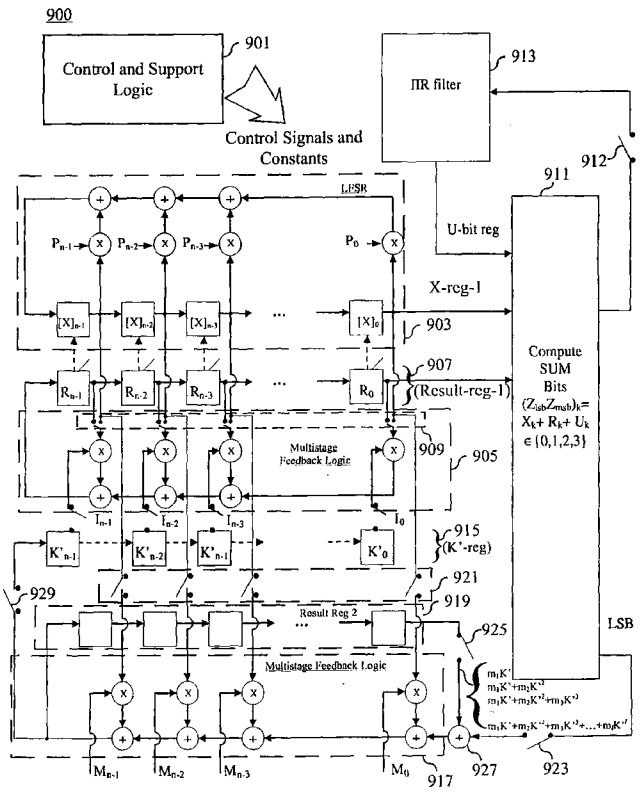


FIG. 9

(57) Abstract: A message authentication code, MAC, is generated in an electronic circuit, wherein the MAC integrit y protects a data value, PD. A random challenge word, RND, is received from a source that is external to the electronic circuit. A first function G(RND,K) is evaluated that generates a first encrypted value, K', from RND and K, wherein K is a secret key value that is stored on the electronic circuit. A second function F(RND,K) is evaluated that generates a second encrypted value, K", from RND and K. The MAC is then generated in accordance with MAC = K" + m_1K' + m_2 K'^2 +... + m_l K'^l, wherein m_1, m_2,..., m_l are derived by representing the data value, PD, as an l- tuple of elements in a field, GF(2^n), wherein n is an integer greater than zero. A hardware-efficient arrangement is also disclosed for generating this and other MACs.

WO 2008/071703 A3

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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 receipt of amendments*

(88) Date of publication of the international search report:
18 September 2008

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/063712

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32

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, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2001/021253 A1 (FURUYA SOICHI [JP] ET AL) 13 September 2001 (2001-09-13) abstract paragraph [0115] - paragraph [0358] figures 1-34	1,13
A	MENEZES A J ED - MENEZES ET AL: "Handbook of applied cryptography, PASSAGE" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 203-212,-,358-359, XP002443775 ISBN: 0-8493-8523-7 paragraph [06.3] paragraph [9.5.4]	1,13

-/--

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

[X] 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	Date of mailing of the international search report
8 May 2008	29/07/2008

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	Dujardin, Corinne

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/063712

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIER B: "Applied Cryptography, PASSAGE" APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, 1996, pages 372-388,459, XP002443776 ISBN: 0-471-11709-9 paragraph [16.2] paragraph [16.4] page 459, line 8 - last line	1,13
A	WO 01/50676 A (HONEYWELL INC [US]) 12 July 2001 (2001-07-12) abstract page 9, line 6 - page 16, line 10 figures 1-3	1,13
A	US 2004/107233 A1 (KIM WON JONG [KR] ET AL) 3 June 2004 (2004-06-03) paragraph [0029] - paragraph [0048]; figures 4,5,7	1,13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2007/063712

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 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 No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

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

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers allsearchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search reportcovers 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.:

1-24

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-24

   Apparatus or method for generating an authentication code wherein an LFSR circuitry and an additional circuitry are caused to function together as a key generator, in a first mode of operation, and as a multiplier, in a second mode of operation.

   ---

2. claims: 25-32

   Apparatus or method for generating a message authentication code MAC that integrity protects a data value PD, and wherein a random challenge word RND is received, the evaluation of a first function G(RND, K) generates a encrypted first value K' from RND and from a secret value K, the evaluation of a second function F(RND, K) generates a second encrypted value K'' from RND and fom the secret value K, and a MAC is generated as MAC=K'' + m1.K' + m2.K' 2 + ... + ml.K' l, with m1, m2, ..., ml representing the data value PD, as an l-tuple of elements in a field GF(2 n).

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/063712

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001021253 A1	13-09-2001	CA 2337306 A1	09-09-2001
		EP 1133099 A2	12-09-2001
		JP 3864675 B2	10-01-2007
		JP 2001324925 A	22-11-2001
WO 0150676 A	12-07-2001	AU 5514701 A	16-07-2001
		CA 2392739 A1	12-07-2001
		EP 1234403 A2	28-08-2002
		JP 2003519960 T	24-06-2003
		US 6804354 B1	12-10-2004
US 2004107233 A1	03-06-2004	KR 20040048471 A	10-06-2004