



(51) International Patent Classification:

H04B 10/12 (2006.01) *H04L* 9/14 (2006.01)
H04L 12/28 (2006.01)

(21) International Application Number:

PCT/US2009/040330

(22) International Filing Date:

13 April 2009 (13.04.2009)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/046,654 21 April 2008 (21.04.2008) US
12/414,963 31 March 2009 (31.03.2009) US

(71) Applicant (for all designated States except US):
TEKNOVUS, INC. [US/US]; 1351 Redwood Way,
Petaluma, CA 94954 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HIRTH, Ryan, E.**
[US/US]; 318 Spring Beauty Ct., Windsor, CA 95492

(US). **BOYD, Edward, W.** [US/US]; 1806 Pembridge
Street, Petaluma, CA 94954 (US). **HO, Ngo, Thanh** [US/
US]; 3800 Indian Springs Trail, Arlington, TX 76016
(US).

(74) Agent: **YAO, Shun;** Park, Vaughan & Fleming LLP,
2820 Fifth Street, Davis, CA 95618-7759 (US).

(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, 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, ST, 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,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR DATA PRIVACY IN PASSIVE OPTICAL NETWORKS

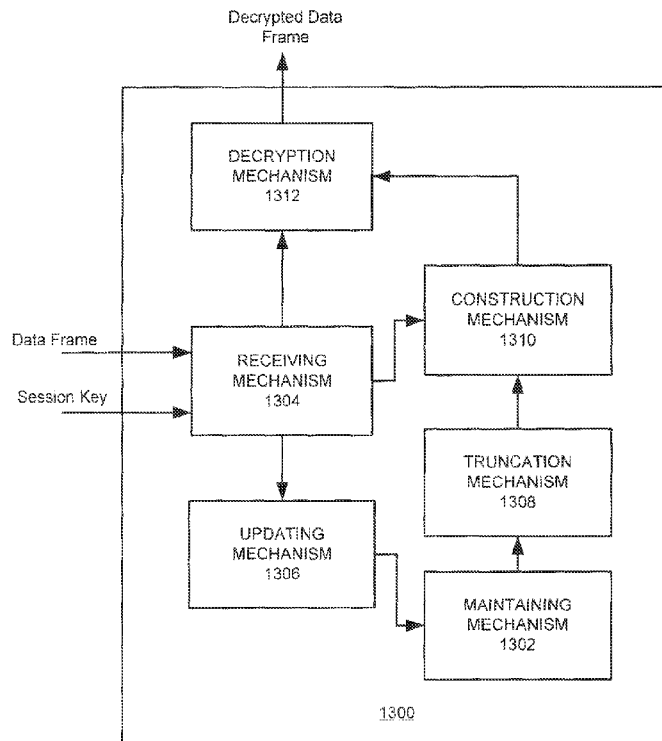


FIG. 13

(57) Abstract: One embodiment provides a system for decrypting data frames in an Ethernet passive optical network (EPON). During operation, the system maintains a local cipher counter at a local node, and receives from a remote node a data frame which is encrypted based on a remote input block and a session key. The remote input block is constructed based on the remote cipher counter and a remote block counter. The system updates the local cipher counter based on a received field located in a preamble of the data frame, truncates the local cipher counter by discarding a number of least significant bits, and constructs for the received data frame a local input block based on the truncated local cipher counter, the received field, and a local block counter. The system then decrypts the data frame based on the local input block and the session key.



TM), European (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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— *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 January 2010

Published:

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

A. CLASSIFICATION OF SUBJECT MATTER***H04B 10/12(2006.01)i, H04L 12/28(2006.01)i, H04L 9/14(2006.01)i***

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 H04B

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

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and applications for Utility models since 1975

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

eKOMPASS(KIPO internal) : "EPON, encrypt, decrypt, key, preamble"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2005-0201554 A1 (KRAMER et al.) 15 Sep. 2005 See whole text.	1,7,12-15,21,26,27 2-6,8-11,16-20,22-25
A	US 2007-0133791 A1 (HAN et al.) 14 Jun. 2007 Abstract, Fig.1, page 3-4	1,14,15
A	US 2004-0136712 A1 (STISCIA et al.) 15 Jul. 2004 Abstract, Fig.2	1,14,15
A	US 2004-0028409 A1 (KIM et al.) 12 Feb. 2004 Abstract, Fig.3, page 2-3	1,14,15
A	US 2004-0073788 A1 (KIM et al.) 15 Apr. 2004 Abstract, Fig.4	1,14,15
A	US 2006-0136715 A1 (HAN et al.) 22 Jun. 2006 Abstract, Fig. 9	1,14,15



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 application or patent 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 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

16 NOVEMBER 2009 (16.11.2009)

Date of mailing of the international search report

17 NOVEMBER 2009 (17.11.2009)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-
gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

LEE, Jin Ick

Telephone No. 82-42-481-5770



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/040330

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005-201554 A1	15.09.2005	US 07349537 B2 WO 2005-086950 A2 WO 2005-086950 A3	25.03.2008 22.09.2005 07.12.2006
US 2007-0133791 A1	14.06.2007	KR 10-0798921 B1	29.01.2008
US 2004-0136712 A1	15.07.2004	US 07385995 B2 US 2004-0141759 A1 US 2004-0136534 A1 WO 2004-064263 A2 WO 2004-064263 A3	10.06.2008 22.07.2004 15.07.2004 29.07.2004 29.07.2004
US 2004-0028409 A1	12.02.2004	JP 3805329 B2 JP 03-805329 B2 JP 2004-072775 A KR 20040013601 A KR 10-0594153 B1	02.08.2006 19.05.2006 04.03.2004 14.02.2004 28.06.2006
US 2004-0073788 A1	15.04.2004	JP 3774455 B2 JP 03-774455 B2 JP 2004-129272 A KR 10-2004-0029767 A US 07305551 B2	17.05.2006 24.02.2006 22.04.2004 08.04.2004 04.12.2007
US 2006-0136715 A1	22.06.2006	KR 10-0723832 B1	31.05.2007