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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 January 2010 (28.01.2010)

PCT

(10) International Publication Number
WO 2010/010336 A3

(51) International Patent Classification:
*H04L 9/00* (2006.01)

(21) International Application Number:
PCT/GB2009/001800

(22) International Filing Date:
20 July 2009 (20.07.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0813298.7 19 July 2008 (19.07.2008) GB

(71) Applicant *(for all designated States except US)*: **UNIVERSITY COURT OF THE UNIVERSITY OF ST ANDREWS** [GB/GB]; College Gate, North Street, St Andrews KY16 9AJ (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LIVESEY, Michael** [GB/GB]; University of St Andrews, North Haugh, Fife KY16 9SS (GB).

(74) Agents: **NAISMITH, Robert, Stewart** et al.; Marks & Clerk, Aurora, 120 bothwell Street, Glasgow G2 Js (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, 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, 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).

**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:
1 April 2010

(54) Title: MULITIPAD ENCRYPTION

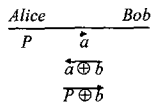



**Figure 1**

(57) Abstract: A method for protecting a message or document. The method comprises encrypting the message (P) using a first key (a) associated with a first party (Alice); sending the encrypted message to a second party (Bob); encrypting the message using a second key (b) associated with the second party, so that it is encrypted with two keys simultaneously (a+b); sending the encrypted message (a+b) to the first party (Alice); decrypting the message using the first key (a); sending the message to the second party (Bob), the message being encrypted with the second key (b), and using the second key (b) to decrypt the encrypted message, thereby exposing the original message P.

WO 2010/010336 A3

# INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2009/001800

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | "Chapter 12: Key Establishment Protocols ED - MENEZES A; OORSCHOT VAN P; VANSTONE S" [Online] 1 October 1996 (1996-10-01), [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS],, PAGE(S) 489 - 541 , XP001525012 ISBN: 9780849385230 Retrieved from the Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/ > page 500, paragraph 12.22-12.23 ----- | 1-4, 8-17, 20-30 |
| A | EP 1 289 186 A2 (COMM RES LAB INDEPENDENT ADMIN [JP] NAT INST OF INFORMATION AND [JP]) 5 March 2003 (2003-03-05) abstract; figure 1 paragraphs [0050] - [0057] ----- | 1-30 |

-/--

[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 |
|---|---|
| 26 November 2009 | 17/02/2010 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Horbach, Christian |

# INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2009/001800

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2005/074118 A1 (WILHITE ELIZABETH [US] ET AL) 7 April 2005 (2005-04-07) abstract paragraphs [0029] - [0035]; figures 2B,3,4,5 | 1-30 |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB2009/001800

**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 all searchable 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 report covers 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.:

1-30

**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: 1-30

Method, encryption/decryption device and computer program product for encrypting and decrypting a message using a first and a second key of a first and of a second device, respectively. The special technical feature is the repetition of the encryption/decryption using further keys of the two devices.

---

2. claim: 31

Method for digital authentication using random digital signatures.

---

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2009/001800

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 1289186 A2 | 05-03-2003 | CN 1405703 A | 26-03-2003 |
| | | DE 60208743 T2 | 20-07-2006 |
| | | JP 4191915 B2 | 03-12-2008 |
| | | JP 2003066834 A | 05-03-2003 |
| | | US 2003044008 A1 | 06-03-2003 |
| | | US 2009245508 A1 | 01-10-2009 |
| US 2005074118 A1 | 07-04-2005 | NONE | |