

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

[US/US]; 1358 Franchere Place, Sunnyvale, California 94087 (US).

(21) International Application Number:
PCT/US2012/034985

(74) Agent: ROHLICEK, J. Robin; 321 Summer Street, Boston, Massachusetts 02210 (US).

(22) International Filing Date:
25 April 2012 (25.04.2012)

(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, QA, RO, RS, RU, RW, 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.

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/103,451 9 May 2011 (09.05.2011) US(71) Applicant (for all designated States except US):
VERAYO, INC. [US/US]; 1054 S. De Anza Blvd., Suite #201, San Jose, California 95129 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BARES, William Henry** [US/US]; 1655 Parkview Green Circle, San Jose, California 95131 (US). **DEVADAS, Srinivas** [US/US]; 7 Whittier Road, Lexington, Massachusetts 02420 (US). **KHANDELWAL, Vivek** [US/US]; 3191 Pruneridge Ave., Santa Clara, California 95051 (US). **PARAL, Zdenek** [US/US]; 5720 Park manor Drive, San Jose, California 95118 (US). **SOWELL, Richard** [US/US]; 1628 Hester Ave., San Jose, California 95128 (US). **ZHOU, Tonghang**

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: MESSAGE SIGNATURE USING PUF AND SIMULATED VERIFICATION

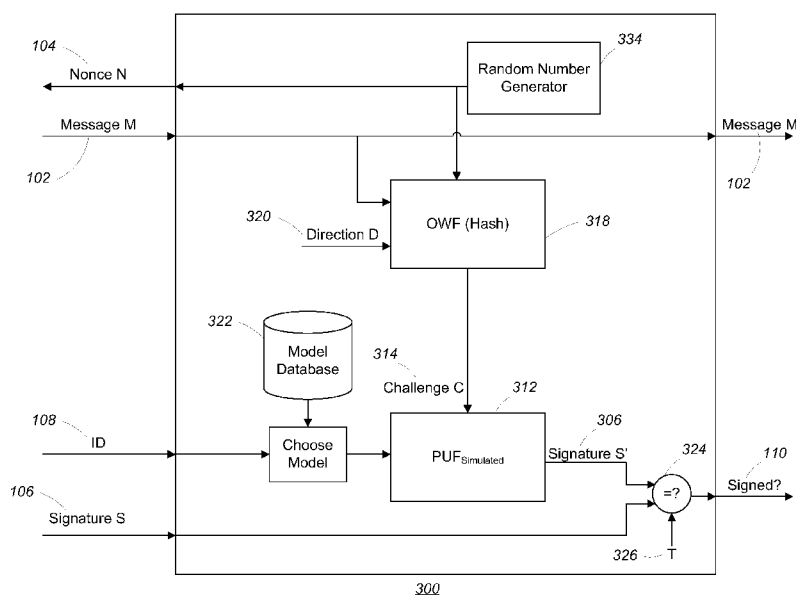


FIG. 3

(57) Abstract: A message is signed using a PUF without having to exactly regenerate a cryptographic key. Another party that shares information about the PUF is able to verify the signature to a high degree of accuracy (i.e., high probability of rejection of a forged signature and a low probability of false rejection of a true signature). In some examples, the information shared by a recipient of a message signature includes a parametric model of operational characteristics of the PUF used to form the signature.

**Declarations under Rule 4.17:**

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))
- 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:

16 May 2013

Published:

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/034985

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32
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 practicable, search terms used)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/293384 A1 (POTKONJAK MIODRAG [US]) 18 November 2010 (2010-11-18) abstract paragraph [0054] - paragraph [0059] figures 1,7	1-5
A	----- US 2011/055649 A1 (KOUSHANFAR FARINAZ [US] ET AL) 3 March 2011 (2011-03-03) paragraph [0014] - paragraph [0021] figures 2-5 -----	1-5

☐

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 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

10 August 2012

Date of mailing of the international search report

22/03/2013

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

Bec, Thierry

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/034985

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.:

1-5

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: 1-5

refers to a signature generation and verification method using a circuit partially emulated.

2. claims: 6-13

refers to a system to sign a message by challenging a PUF circuit on different point

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/034985

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2010293384	A1	18-11-2010	NONE	

US 2011055649	A1	03-03-2011	NONE	
