



- (51) **International Patent Classification:**
H04L 9/06 (2006.01)
- (21) **International Application Number:**
PCT/US2011/064419
- (22) **International Filing Date:**
12 December 2011 (12.12.2011)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/009,205 19 January 2011 (19.01.2011) 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):** **PARAL, Zdenek** [US/US]; 5720 Park Manor Drive, San Jose, California 95118 (US). **DEVADAS, Srinivas** [US/US]; 7 Whittier Road, Lexington, Massachusetts 02420 (US).
- (74) **Agent:** **ROHLICEK, J. Robin**; 10 Fawcett Street, Cambridge, Massachusetts 02138 (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, 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.

- (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).

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))

Published:

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

[Continued on next page]

- (54) **Title:** RELIABLE PUF VALUE GENERATION BY PATTERN MATCHING

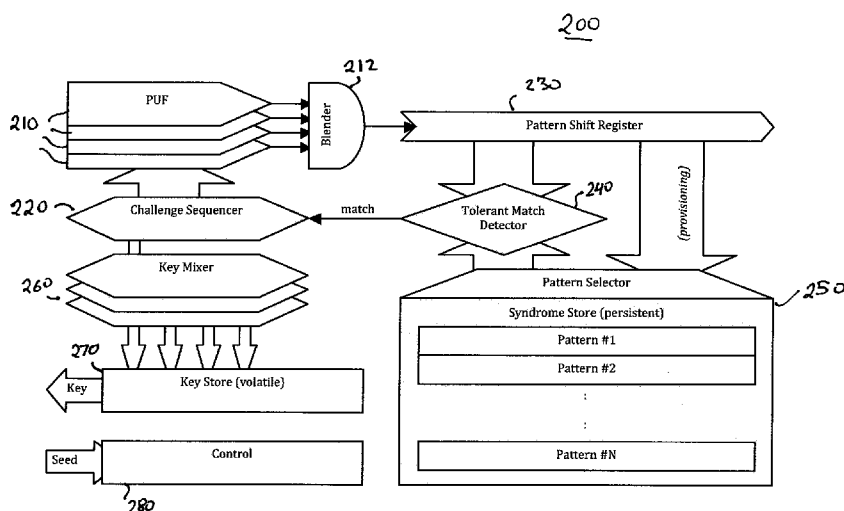


FIG. 2

- (57) **Abstract:** A method is used to reliably provision and re-generate a finite and exact sequence of bits, for use with cryptographic applications, e.g., as a key, by employing one or more challengeable Physical Unclonable Function (PUF) circuit elements. The method reverses the conventional paradigm of using public challenges to generate secret PUF responses; it exposes the response and keeps the particular challenges that generate the response secret.



— *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:
27 September 2012

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/064419

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 practicable, search terms used)

EPO-Internal, WPI Data, PAJ, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	FR 2 964 278 A1 (ST MICROELECTRONICS ROUSSET [FR]) 2 March 2012 (2012-03-02) page 5, line 21 - page 11, line 11 figures 2,3,6 -----	1-16
X	US 2009/083833 A1 (DEVADAS S; KHADELWAL V; PARAL Z; QIAOLA T; SCHUCH E G; SUH G E; VIVEK) 26 March 2009 (2009-03-26) the whole document -----	1-16



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

30 July 2012

Date of mailing of the international search report

03/08/2012

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

Information on patent family members

International application No

PCT/US2011/064419

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
FR 2964278	A1	02-03-2012	CN	102387013 A		21-03-2012
			FR	2964278 A1		02-03-2012
			US	2012066571 A1		15-03-2012

US 2009083833	A1	26-03-2009	AT	544123 T		15-02-2012
			CN	101542496 A		23-09-2009
			EP	2214117 A2		04-08-2010
			US	2009083833 A1		26-03-2009
			WO	2009079050 A2		25-06-2009
