

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
3 November 2005 (03.11.2005)

PCT

(10) International Publication Number  
**WO 2005/101975 A3**

(51) International Patent Classification:  
**G06F 1/02** (2006.01) **H04L 9/00** (2006.01)

(74) Agents: **LUZZATTO**, Kfir et al.; P.O. Box 5352, 84152 Beer Sheva (IL).

(21) International Application Number:  
PCT/IL2005/000429

(22) International Filing Date: 21 April 2005 (21.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/565,304 22 April 2004 (22.04.2004) US  
60/624,463 3 November 2004 (03.11.2004) US

(71) Applicant (for all designated States except US):  
**FORTRESS GB LTD.** [GB/GB]; BMA Building,  
Tavistock Square, London, Greater London WC1H 9LG  
(GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GRESSEL**, Carmi  
David [IL/IL]; Kvutzat Urim, 85530 Mobile Post Negev  
(IL). **SLOBODKIN**, Michael [IL/IL]; 41/13 Shimon  
Street, 89014 Arad (IL). **GRANOT**, Ran [IL/IL]; 83  
Sharon Street, 81400 Yavne (IL). **KROTMAN**, Roy  
[IL/IL]; 4 Oley HaGardom Street, 75230 Rishon Le  
Zion (IL). **BICK**, Yehonatan [IL/IL]; 72 Azar Street,  
44415 Kfar Saba (IL). **FITERMAN**, Mark [IL/IL];  
34 David HaReuveni Street, 84515 Beer Sheva (IL).  
**VAGO**, Gabriel [GB/GB]; 46 Cranbourne Gardens,  
London, Greater London NW11 OJD (GB). **INGHER**,  
Amir [IL/IL]; 14 Samuel Falberg Street, Ramot, 84686  
Beer Sheva (IL). **APPLE**, Uzi [IL/GB]; 46 Cranbourne  
Gardens, London, Greater London NW11 OJD (GB).

(81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,  
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,  
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,  
KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA,  
MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM,  
PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM,  
SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN,  
YU, 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, HU, IE, IS, IT, LT, LU, MC, 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

(88) Date of publication of the international search report:  
8 March 2007

(15) Information about Correction:

Previous Correction:

see PCT Gazette No. 39/2006 of 28 September 2006

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ACCELERATED THROUGHPUT SYNCHRONIZED WORD STREAM CIPHER, MESSAGE AUTHENTICATOR AND ZERO-KNOWLEDGE OUTPUT RANDOM NUMBER GENERATOR

(57) Abstract: Systems and methods are disclosed, especially designed for very compact hardware implementations, to generate random number strings with a high level of entropy at maximum speed. For immediate deployment of software implementations, certain permutations have been introduced to maintain the same level of unpredictability which is more amenable to hi-level software programming, with a small time loss on hardware execution; typically when hardware devices communicate with software implementations. Particular attention has been paid to maintain maximum correlation immunity, and to maximize non-linearity of the output sequence. Good stream ciphers are based on random generators which have a large number of secured internal binary variables, which lead to the page synchronized stream ciphering. The method for parsed page synchronization which is presented is especially valuable for Internet applications, where occasionally frame sequences are often mixed. The large number of internal variables with fast diffusion of individual bits wherein the masked message is fed back into the machine variables is potentially ideal for message authentication procedures.

WO 2005/101975 A3

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL05/00429

## A. CLASSIFICATION OF SUBJECT MATTER

IPC: **G06F 1/02**( 2006.01);**H04L 9/00**( 2006.01)

USPC: 708/252;380/46

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)

U.S. : 708/250,252; 380/46

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)  
Please See Continuation Sheet

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,825,023 A (LEE et al) 25 July 1989, figures 1-4.	1,10,18,27,36 and 44.
A	US 2003/0072059 A1 (THOMAS et al.) 17 April 2003, figures 6-8.	1,10,18,27,36 and 44.

☐ 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	"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
"E"	earlier application or patent published on or after the international filing date	"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
"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)	"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
"O"	document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

18 July 2006 (18.07.2006)

Date of mailing of the international search report

08 DEC 2006

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Facsimile No. (571) 273-3201

Authorized officer

Chuong D. Ngo  
Telephone No. (571) 272-2100

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/IL05/00429

## 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.: 4,5,7,9,13,14,16,21,22,24,30,31,33,35,39,40,42,47,48 and 50.  
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:  
Please See Continuation 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 additional fees, this Authority did not invite payment of any 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.: 1-25 and 27-51

### 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.

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IL05/00429

### BOX III. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claim(s) 1-25 and 27-51, drawn to a random number generation.

Group II, claim(s) 26, drawn to a synchronization of transmitted stream ciphered messages.

The inventions listed as Groups I and II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they clearly lack the same or corresponding special technical features.

Continuation of B. FIELDS SEARCHED Item 3:

EAST:

search term: random generator, non-linear shift register, hash, cipher.