

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: OYEN WIGGS GREEN & MUTALA LLP The Station 480 - 601 West Cordova Street VANCOUVER, British Columbia Canada, V6B 1G1	<p style="font-size: 2em; font-weight: bold; margin: 0;">PCT</p> <p style="margin: 0;">WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY</p> <p style="margin: 0;">(PCT Rule 43bis.1)</p>																									
Applicant's or agent's file reference W419 0009	<p style="font-weight: bold; margin: 0;">FOR FURTHER ACTION</p> <p style="margin: 0;">See paragraph 2 below</p>																									
International application No. PCT/CA2005/000163	International filing date (day/month/year) 09 February 2005 (09-02-2005)	Priority date (day/month/year) 09 February 2004 (09-02-2004)																								
International Patent Classification (IPC) or both national classification and IPC IPC ⁷ H04L-9/18																										
Applicant BOREN, STEPHEN LAURENCE ET AL																										
<p>1. This opinion contains indications relating to the following items :</p> <table style="width:100%; border: none;"> <tr> <td style="width: 10%;"><input checked="" type="checkbox"/></td> <td style="width: 20%;">Box No. I</td> <td>Basis of the opinion</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Box No. II</td> <td>Priority</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Box No. III</td> <td>Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Box No. IV</td> <td>Lack of unity of invention</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Box No. V</td> <td>Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement.</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Box No. VI</td> <td>Certain documents cited</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Box No. VII</td> <td>Certain defects in the international application</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Box No. VIII</td> <td>Certain observations on the international application</td> </tr> </table> <p>2. FURTHER ACTION If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.</p> <p>If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.</p> <p>For further options, see Form PCT/ISA/220.</p> <p>3. For further details, see notes to Form PCT/ISA/220.</p>			<input checked="" type="checkbox"/>	Box No. I	Basis of the opinion	<input type="checkbox"/>	Box No. II	Priority	<input type="checkbox"/>	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	<input type="checkbox"/>	Box No. IV	Lack of unity of invention	<input checked="" type="checkbox"/>	Box No. V	Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement.	<input type="checkbox"/>	Box No. VI	Certain documents cited	<input type="checkbox"/>	Box No. VII	Certain defects in the international application	<input checked="" type="checkbox"/>	Box No. VIII	Certain observations on the international application
<input checked="" type="checkbox"/>	Box No. I	Basis of the opinion																								
<input type="checkbox"/>	Box No. II	Priority																								
<input type="checkbox"/>	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability																								
<input type="checkbox"/>	Box No. IV	Lack of unity of invention																								
<input checked="" type="checkbox"/>	Box No. V	Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement.																								
<input type="checkbox"/>	Box No. VI	Certain documents cited																								
<input type="checkbox"/>	Box No. VII	Certain defects in the international application																								
<input checked="" type="checkbox"/>	Box No. VIII	Certain observations on the international application																								
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer <p align="center" style="font-size: 1.2em;">Lawrence J. Engel (819) 997-2936</p>																									

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims <u>1 to 23</u>	YES
	Claims <u>None</u>	NO
Inventive step (IS)	Claims <u>1 to 23</u>	YES
	Claims <u>None</u>	NO
Industrial applicability (IA)	Claims <u>1 to 23</u>	YES
	Claims <u>None</u>	NO

2. Citations and explanations :

Reference is made to the following documents in the International Search report:

D1=US 5,835,597 (A) [Coppersmith D. & Rogaway, P. (10 November 1998)]
 D2=US 6,415,032 (A) [Doland, C. (02 July 2002)]
 D3=US 2003/0016823 (A) [Chung, S. (23 January 2003)]
 D4=US 2003/0039357 (A) [Alten, A. (27 February 2003)]
 D5=US 2003/0210783 (A) [Filippi, R. (13 November 2003)]

D1 discloses a method and computer-program product for generating a pseudorandom bit string for constructing a stream cipher using a pseudorandom function that maps an index and an encryption key into a pseudorandom sequence of bits whose length can be as long as the plaintext string [col. 1, line 57 to col. 2, line 27]. The pseudorandom function [Fig. 3] begins by preprocessing the key into a table of pseudorandom values which are combined with the index to initialize a plurality of registers. The initial values of some of the registers are modified using a predetermined mixing function and then their resulting values are masked again using other pseudorandom values from the table and an appropriate masking function. These masked register values are then concatenated into a pseudorandom bit string to complete an iteration. The pseudorandom bit stream can grow to any desired length depending on the number of subsequent iterations [col. 3, line 52 to col. 7, line 59].

D2 discloses a method of encrypting a message of n bits using a pseudo-random sequence of integers using a key K and a pair of prime numbers p and q where $q=2p+1$. A sequence of bits used to encrypt the message is generated from the least or most significant bit from each integer number [col. 3, lines 23-44]. The sequence of integers has a repeating period that depends on the value of p and not the bit length of key K ([col. 4, lines 32-56], [col. 5, line 46 to col. 6, line 9]). Furthermore, a constant offset value F can be added to the encrypting bit sequence as long as $p>N+F$ where N is the largest anticipated message length to improve the security of the stream cipher [col. 6, line 10 to col. 7, line 9].

D3 discloses a method and apparatus for encrypting a bit stream in real-time by combining the output of an irrational number generator with an input bit stream [0017-0020]. D3 describes how the irrational number generator, using an initial key and a buffer, can be used to implement a stream cipher [0039] since most irrational numbers are statistically random and the output bit stream generated will be close to a one-time pad ([0033], Fig. 6).

D4 discloses a system and method for enciphering a sequence of clear text data values by using a non-cyclic pseudo-random number generator used in a Vernam cipher based cryptosystem [0009]. Encrypting or decrypting bytes of data is performed using final pad created from a private and secret source of derived random bits, periodically random cryptographic keys and values delivered from a secured server to control the random reshuffling of the private and secret source of derived random bits and, finally, the secure server replaces the private and secret source of derived random bits with a fresh set of random bits ([0010],[0063] to [0070]).

(continued in Supplemental Box)

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made :

Reference to international application PCT/CA03/01538 appears to be incorrect and should be corrected as per PCT Rule 5.

Reference to the elements of Figure 1 should be included in the Description as per PCT Rule 5(iv).

A general statement found on page 16, line 2, referring top the “spirit” of the invention implies that the extent of protection may be expanded in some vague and not precisely defined way, which does not comply with PCT Article 6.

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of: Box V

D5 discloses a system for providing a pseudo random bit stream to encrypt an information data stream and a method for encrypting/decrypting data using a plurality of sub-keys [Abstract]. D5 describes using a long secure key (1 MB in length) and selecting sub-keys of varied length from random positions of the long key, overlapping positions of the long key, reversing the bit order of the long key and rotating bit values of each sub-key based on the significance of the sub-key (arbitrarily assigned) ([0036] to [0042]) to generate the pseudo random bit streams ([0059], [0060]). Both the source and the destination of the encrypted information stream must use the same secure long key and the same manner of selection and operation of subkeys ([0063] to [0104], Fig. 2-4, claims 1-4).

The following observation is made:

Claims 1 to 23 define a method and computer product for encrypting electronic communications by generating a random key of variable length by creating multiple random sub-keys having non-repeating lengths and randomly combining said sub-keys in a random fashion to form a Super-Key whose length is independent of the length of a plaintext message being encrypted.

A non-repeating Super Key is formed by combining unique non-repeating sub-keys whose lengths are a prime number (>10). First seed is selected from a random source and verified as not being a perfect square. An iteration algorithm for generating and selecting the bytes of a sub-key is repeated 4 digits at a time until a string of random data equal to the prime number non-repeating length of the sub-key being created is completed. This process is repeated for each sub-key and repeated as often as necessary to form multiple sub-keys of sufficient non-repeating length to create the Super-Key in combination with the other sub-keys. The Super-Key created only until all the data is encrypted.

A starting offset for the Super-Key is generated by XORing selected bytes of the sub-keys until all selected bytes of each sub-key have been XORed and then the resulting value is put through a substitution cipher to de-linearize the Super-Key. As each byte of the Super-Key is generated, the corresponding byte of the plaintext message is then encrypted with the corresponding byte of the Super-Key by the XOR function (or another mathematical function). Once all the bytes have been encrypted the generation of the Super-Key terminates.

Claims 1- 23 are considered novel, having inventive step and being industrially applicable and hence meet the criteria set out in PCT Articles 33(2), 33(3) and 33(4). The prior art (D1 to D5) does not teach or fairly suggest alone or in combination, a method of generating a random key, or one-time pad, of variable length by combining randomly multiple non-repeating sub-keys whose random lengths are a prime number into a Super-Key whose length is independent of the length of a plaintext message. This is considered a new, inventive and useful method for generating a stream cipher.

PATENT COOPERATION TREATY
PCT
INTERNATIONAL SEARCH REPORT
(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference W419 0009	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below
International application No. PCT/CA2005/000163	International filing date (day/month/year) 09 February 2005 (09-02-2005)
(Earliest) Priority date (day/month/year) 09 February 2004 (09-02-2004)	
Applicant BOREN, STEPHEN LAURENCE ET AL	

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. **Certain claims were found unsearchable** (see Box No. II).

3. **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

the text is approved as submitted by the applicant.

the text has been established by this Authority to read as follows :

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 2

as suggested by the applicant.

as selected by this authority, because the applicant failed to suggest a figure.

as selected by this Authority, because this figure better characterizes the invention.

b. none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000163

A. CLASSIFICATION OF SUBJECT MATTER

IPC⁷ H04L-9/18
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)
IPC⁷ H04L-9/18 (using keywords)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
WEST, Delphion, Canadian Patent Database
Keywords :pseudo-random number/sequence generator, encryption, subkey, multi-key, cipher stream, one-time pad

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No(s).
A	US5,835,597 "Software-Efficient Pseudorandom Function and the Use Thereof for Decryption"; Coppersmith D., Rogaway, P. (10 November 1998) [col. 1, line 57 to col. 2, line 27], Fig. 3, [col. 3, line 52 to col. 7, line 59]	1- 23
A	US6,415,032 "Encryption Technique Using Stream Cipher and Block Cipher"; Doland, C. (02 July 2002) [col. 3, lines 23-44], [col. 4, lines 32-56], [col. 5, line 46 to col. 6, line 9], [col. 6, line 10 to col. 7, line 9]	1- 23
A	US2003/0016823 "Method and Apparatus of Using Irrational Numbers in Random Number Generators for Cryptography"; Chung, S. (23 January 2003) [0017-0020], [0039], [0033], Fig. 6	1- 23

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents :	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 18 May 2005 (18-05-2005)	Date of mailing of the international search report 26 May 2005 (26-05-2005)
---	--

Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer Lawrence J. Engel (819) 997-2936
---	--

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000163

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No(s).
A	US2003/0039357 "System and methods for a Vernam Stream Cipher, a Keyed One-Way Hash and a Non-Cyclic Pseudo-Random Number Generator"; Alten, A. (27 February 2003) [0009], [0010], [0063] to [0070]	1- 23
A	US2003/0210783 "Method and System of Encryption"; Filippi, R.(13 November 2003) Abstract, [0036] to [0042], [0059], [0060], [0063] to [0104], Fig. 2-4, claims 1-4	1- 23

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2005/000163

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US5835597	10-11-1998	DE69431390D D1	24-10-2002
		DE69431390T T2	05-06-2003
		EP0658022 A2	14-06-1995
		JP3320928B2 B2	03-09-2002
		SG44363 A1	19-12-1997
		US5454039 A	26-09-1995
		US5675652 A	07-10-1997
		US5677952 A	14-10-1997
		US5835597 A	10-11-1998
US6415032	02-07-2002	US6415032 B1	02-07-2002
US2003/016823	23-01-2003	US2003016823 A1	23-01-2003
US2003/039357	27-02-2003	US2003039357 A1	27-02-2003
		WO03019842 A2	06-03-2003
US2003/210783	13-11-2003	AU9169201 A	13-02-2002
		AUPQ904100D D0	17-08-2000
		US2003152233 A1	14-08-2003
		US2003210783 A1	13-11-2003
		WO0211359 A2	07-02-2002
		WO2004068784 A1	12-08-2004