PTO/AIA/15 (07-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	29907-0037002
First Inventor	Daniel Richard L. Brown et al.
Title	Elliptic Curve Random Number Generation
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

1. ☒ **Fee Transmittal Form.**
(PTO/SB/17 or equivalent)

2. □ **Applicant claims small entity status.**
See 37 CFR 1.27.

3. ☒ **Specification.** [*Total Pages* 15]
Both the claims and abstract must start on a new page
(For information on the preferred arrangement, see MPEP § 608.01(a))

4. ☒ **Drawing(s).** (*35 U.S.C. 113*) [*Total Sheets* 6]

5. **Inventor's Oath or Declaration.** [*Total Sheets* ____]
(including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e))
a. □ Newly executed (original or copy)
b. □ A copy from a prior application (37 CFR 1.63(d))

6. ☒ **Application Data Sheet.** **See Note below.*
See 37 CFR 1.76 (PTO/AIA/14 or equivalent)

7. □ **CD-ROM or CD-R.**
in duplicate, large table or Computer Program *(Appendix)*
□ Landscape Table on CD

8. **Nucleotide and/or Amino Acid Sequence Submission.**
(if applicable, items a. – c. are required)
a. □ Computer Readable Form (CRF)
b. Specification Sequence Listing on:
i. □ CD-ROM or CD-R (2 copies); or
ii. □ Paper
c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. □ **Assignment Papers.**
(cover sheet & document(s))
Name of Assignee ____________________

10. □ **37 CFR 3.73(c) Statement.** ■ **Power of Attorney.**
(when there is an assignee)

11. □ **English Translation Document.**
(if applicable)

12. ■ **Information Disclosure Statement.**
(PTO/SB/08 or PTO-1449)
□ Copies of citations attached

13. ■ **Preliminary Amendment.**

14. □ **Return Receipt Postcard.**
(MPEP § 503) (Should be specifically itemized)

15. □ **Certified Copy of Priority Document(s).**
(if foreign priority is claimed)

16. □ **Nonpublication Request.**
Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.

17. □ **Other:** ____________________

19. CORRESPONDENCE ADDRESS

■ The address associated with Customer Number: 94149 **OR** □ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Michael K. Henry/	Date	February 19, 2013
Name (Print/Type)	Michael K. Henry, Ph.D.	Registration No. (Attorney/Agent)	59516

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/17 (10-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if known	
Application Number	
Filing Date	February 19, 2013
First Named Inventor	Daniel Richard L. Brown et al.
Examiner Name	
Art Unit	
Practitioner Docket No.	29907-0037002

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 2314.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): ____________

☒ Deposit Account Deposit Account Number: 06-1050 Deposit Account Name: Fish & Richardson P.C.

For the above-identified deposit account, the Director is hereby authorized to (check all that apply):

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayment of fee(s)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	390	195	620	310	250	125	1260
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	390	195	620	310	760	380	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	62	31
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	460	230

Total Claims		Extra Claims		Fee ($)		Fee Paid ($)
37	-20 or HP =	17	x	62	=	1054

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		Extra Claims		Fee ($)		Fee Paid ($)
3	-3 or HP =		x	250	=	

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $320 ($160 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof		Fee ($)		Fee Paid ($)
21	- 100 =		/ 50 =	(round up to a whole number)	x		=	

4. OTHER FEE(S) **Fees Paid ($)**

Non-English specification, $130 fee (no small entity discount) ____________

Non-electronic filing fee under 37 CFR 1.16(t) for a utility application, $400 fee ($200 small entity) ____________

Other (e.g., late filing surcharge): ____________ ____________

SUBMITTED BY

Signature	/Michael K. Henry/	Registration No. (Attorney/Agent) 59516	Telephone 214-747-5070
Name (Print/Type)	Michael K. Henry, Ph.D.		Date February 19, 2013

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	
	Filing Date	2013-02-19
	First Named Inventor	Daniel Richard L. Brown et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	29907-0037002

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5442707		1995-08-01	Miyaji et al.	
	2	6044388		2000-03-28	DeBellis et al.	
	3	6088798		2000-07-01	Shimbo	
	4	6243467		2001-06-05	Reiter et al.	
	5	6263081		2001-07-01	Miyaji et al.	
	6	6307935		2001-10-01	Crandall et al.	
	7	6424712		2002-07-01	Vanstone et al.	
	8	6477254		2002-11-01	Miyazaki et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number		
	Filing Date	2013-02-19	
	First Named Inventor	Daniel Richard L. Brown et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	29907-0037002	

	9	6714648		2004-03-01	Miyazaki et al.	
	10	6738478		2004-05-01	Vanstone et al.	
	11	6882958		2005-04-01	Schmidt et al.	
	12	7013047		2006-03-01	Schmidt et al.	
	13	7062043		2006-06-01	Solinas	
	14	7062044		2006-06-01	Solinas	
	15	7092979		2006-08-01	Shim	
	16	7171000		2007-01-01	Toh et al.	
	17	7197527		2007-03-01	Naslund et al.	
	18	7200225		2007-04-01	Schroeppel	
	19	7221758		2007-05-01	Cramer et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	2013-02-19
First Named Inventor	Daniel Richard L. Brown et al.
Art Unit	
Examiner Name	
Attorney Docket Number	29907-0037002

	20	7225341		2007-05-01	Yoshino et al.	
	21	7308096		2007-12-01	Okeya et al.	
	22	7480795		2009-01-01	Vanstone	
	23	7418099		2008-08-01	Vanstone	
	24	7542568		2009-06-01	Ohmori et al.	
	25	7599491		2009-10-01	Lambert	
	26	7639799		2009-12-01	Lauter et al.	
	27	7650507		2010-01-01	Crandall et al.	
	28	7680270		2010-03-01	Srungaram	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	
	Filing Date	2013-02-19
	First Named Inventor	Daniel Richard L. Brown et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	29907-0037002

	1	20020044649		2002-04-01	Gallant et al.	
	2	20030081785		2003-05-01	Boneh et al.	
	3	20040102242		2004-05-27	Poelmann et al.	
	4	20050036609		2005-02-01	Eisentraeger et al.	
	5	20050251680		2005-11-01	Brown et al.	
	6	20060129800		2006-06-01	Lauter et al.	
	7	20060285682		2006-12-01	Sarangarajan et al.	
	8	20070248224		2007-10-01	Buskey et al.	
	9	20080056499		2008-03-01	Vanstone	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	
Filing Date	2013-02-19
First Named Inventor	Daniel Richard L. Brown et al.
Art Unit	
Examiner Name	
Attorney Docket Number	29907-0037002

	1	2001/13218	WO		2001-02-22	Siemens Aktiengesellschaft		□
	2	2001/35573	WO		2001-05-17	Schroeppel		□
	3	2381397	CA		2001-02-22	AlliedSignal Inc.		□
	4	2001-222220	JP		2001-08-17	Koden Electronics Co. Ltd.		□
	5	2003-507761	JP		2003-02-25	Siemens Aktiengesellschaft		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	ANS X9.62-2005; "Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA)"; November 16, 2005; 163 pages.	□
	2	ANSI X9.82; "Part 3 for X9F1" October 2003; 175 pages.	□
	3	ANS X9.82; "Part 3 - Draft"; June 2004; 189 pages.	□
	4	Barker, Elaine and John Kelsey; "Recommendation for Random Number Generation Using Deterministic Random Bit Generators"; NIST Special Publication 800-90; National Institute of Standards and Technology; December 2005; 130 pages.	□

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2013-02-19
	First Named Inventor	Daniel Richard L. Brown et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	29907-0037002

	5	Barker, Elaine and John Kelsey; "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)"; NIST Special Publication 800-90; National Institute of Standards and Technology; March 2007; 133 pages.	□
	6	Blum, Manuel and Silvio Micali; "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits"; SIAM Journal on Computing; Vol. 13, No. 4; November 1984; pp. 850-864.	□
	7	Brown, Daniel R.L.; "Conjecture Security of the ANSI-NIST Elliptic Curve RNG"; Cryptology ePrint Archive; Report 2006/117; March 29, 2006; 14 pages. Internet: <http://eprint.iacr.org>.	□
	8	El Mahassni, Edwin and Igor Shparlinksi; "On the Uniformity of Distribution of Congruential Generators over Elliptic Curves"; Sequences and Their Applications: Proceedings of SETA '01; 2002' pp. 257-264.	□
	9	Gjoesteen, Kristian; "Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005"; March 16, 2006; 8 pages.	□
	10	Goldreich, Oded; "Foundations of Cryptography Basic Tools'; Cambridge University Press; 2001; pages 30-183.	□
	11	Guerel, Nicolas; "Extracting Bits from Coordinates of a Point of an Elliptic Curve"; Cryptology ePrint Archive; Report 2005/324; 2005; 9 pages. Internet: <http://eprint.iacr.org>	□
	12	Johnson, Don B.; "X9.82 Part 3 - Number Theoretic DRBGs"; NIST RNG Workshop; July 20, 2004; Internet: <http://csrc.nist.gov/groups/ST/tooklit/documents/rng/NumberTheoreticDRBG.pdf>	□
	13	Kaliski, Burton S., Jr.; "A Pseudo-Random Bit Generator Based on Elliptic Logarithms"; Advances in Cryptology; CRYPTO 1986; Vol. 263; pp. 84-103.	□
	14	Lee, K. et al.; "Elliptic Curve Random Number Generation"; Electrical and Electronic Technology 2001; Proceedings of IEEE Region 10 International Conference; August 19-22, 2001; pp. 239-241.	□
	15	Lichota, Dr. RW; "Verifying the Correctness of Cryptographic Protocols Using 'Convince'" IEEE; December 13, 1996; pp. 119-122.	□

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number		
	Filing Date	2013-02-19	
	First Named Inventor	Daniel Richard L. Brown et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	29907-0037002	

	16	Luby, Michael; "Pseudorandomness and Cryptographic Applications"; Princeton University Press; 1996; pp. 70-74.	□
	17	Satoh, A.; "Scalable Dual-Field Elliptical Curve Cryptographic Processor"; IEEE, Volume 52; April 2003; pp. 452-456.	□
	18	Extended European Search Report issued in European Application No. 06704329.9 on November 12, 2009; 6 pages.	□
	19	Official Action issued in Canadian Application No. 2,594,670 on August 9, 2012; 4 pages (Ref.: 29907-0037CA1).	□
	20	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on March 10, 2010; 4 pages.	□
	21	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on July 22, 2010; 4 pages.	□
	22	Communication pursuant to Article 94(3) EPC issued in European Application No. 06704329.9 on June 15, 2011; 4 pages.	□
	23	Office Action issued in Japanese Application No. 2007-551522 on August 26, 2011; 18 pages (Ref.: 29907-0037JP1).	□
	24	Office Action issued in Japanese Application No. 2007-551522 on Janaury 18, 2012; 8 pages (Ref.: 29907-0037JP1).	□
	25	Notice of Final Rejection issued in Japanese Application No. 2007-551522 on May 30, 2012; 7 pages (Ref.: 29907-0037JP1).	□
	26	Notice of Allowance issued in Japanese Application No. 2007-551522 on October 31, 2012; 3 pages (Ref.: 29907-0037JP1).	□

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number		
	Filing Date	2013-02-19	
	First Named Inventor	Daniel Richard L. Brown et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	29907-0037002	

	27	International Search Report and Written Opinion of the International Searching Authority issued in International Application No. PCT/CA2006/000065 on May 1, 2006; 11 pages (Ref.: 29907-0037WO1).	□
	28	International Preliminary Report on Patentability issued in International Application No. PCT/CA2006/000065on August 2, 2007.	□
	29		□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	
	Filing Date	2013-02-19
	First Named Inventor	Daniel Richard L. Brown et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	29907-0037002

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael K. Henry/	Date (YYYY-MM-DD)	2013-02-19
Name/Print	Michael K. Henry, Ph.D.	Registration Number	59516

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel Richard L. Brown
Filer:	Michael K. Henry/Christie Loven
Attorney Docket Number:	29907-0037002

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	390	390
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Claims in excess of 20	1202	17	62	1054
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2314**

Electronic Acknowledgement Receipt

EFS ID:	14992335
Application Number:	13770533
International Application Number:	
Confirmation Number:	5276
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel Richard L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Lisa Peterson
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	29907-0037002
Receipt Date:	19-FEB-2013
Filing Date:	
Time Stamp:	16:21:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2314
RAM confirmation Number	4426
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Transmittal of New Application	31234-0037002_AppTransmittal.pdf	42430 3cbbf7a0e43f9d0110da902a887d65e2898f02a7	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	31234-0037002_FeeTransmittal.pdf	66020 1b7819f089ed2377d97867aa046e4e35a02ff6e4	no	2
Warnings:					
Information:					
3	Power of Attorney	31234-0037002_POA.pdf	616460 4e7414bdd27cea24462eb7486db357d98c6fbebb	no	2
Warnings:					
Information:					
4	Application Data Sheet	31234-0037002_ApplicationDataSheet.pdf	1396530 ea27e088b6428b09a9a4a3678160d5e313ee9034	no	6
Warnings:					
Information:					
5		31234-0037002_Specification.pdf	14981492 46af9405d309f3bc7340be4f0d5b8dcdaabaeeb8	yes	15
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	11	
	Claims		12	14	
	Abstract		15	15	
Warnings:					
Information:					
6	Drawings-only black and white line drawings	31234-0037002_Drawings.pdf	1854717 81046d04b04120d61a7ca3995d24935c55860546	no	6
Warnings:					
Information:					
7		31234-0037002_PreliminaryAmendment.pdf	81031 0441dbe23e04d8aaf6a993a698ac5c974fc28d41	yes	8
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	

	Preliminary Amendment			1	1
	Specification			2	2
	Claims			3	7
	Applicant Arguments/Remarks Made in an Amendment			8	8
Warnings:					
Information:					
8	Information Disclosure Statement (IDS) Form (SB08)	31234-0037002_IDS.pdf	45294 0f70a540dc995174885210fa97137305b75f388c	no	10
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
9	Fee Worksheet (SB06)	fee-info.pdf	36633 5169136eed5f3bc1d94c53ad6a6c5a4e6663932e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	19120607		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B or equivalent) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5. If the Power of Attorney by Applicant form is not accompanied by this transmittal form or an equivalent, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	February 19, 2013
First Named Inventor	Daniel Richard L. Brown et al.
Title	Elliptic Curve Random Number Generation
Art Unit	
Examiner Name	
Attorney Docket Number	29907-0037002

SIGNATURE of Applicant or Patent Practitioner

Signature	/Michael K. Henry/	Date	February 19, 2013
Name	Michael K. Henry, Ph.D.	Telephone	214-747-5070
Registration Number	59516		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications.

□ *Total of ____________ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/82B (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent): 94149

OR

□ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☒ The address associated with the above-mentioned Customer Number.

OR

□ The address associated with Customer Number:

OR

□ Firm or Individual Name	Fish & Richardson
Address	
City	State	Zip
Country	
Telephone	Email

I am the Applicant:

□ Inventor or Joint Inventor

□ Legal Representative of a Deceased or Legally Incapacitated Inventor

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign

□ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	October 01, 2012
Name	James Kesh	Telephone	(519) 888-7465
Title and Company	Treasurer Certicom Corp., 4701 Tahoe Blvd, Tahoe A, 5th Floor, Mississauga, Ontario, L4W 0B5, Canada		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below*.

□ *Total of ____________ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Legal OK

RIM OK

DJM

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	29907-0037002
	Application Number	

Title of Invention	ELLIPTIC CURVE RANDOM NUMBER GENERATION

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

□ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Daniel	Richard L.	Brown	

Residence Information (Select One) ○ US Residency ● Non US Residency ○ Active US Military Service

City	Mississauga	Country of Residence i	CA

Mailing Address of Inventor:

Address 1	4701 Tahoe Blvd., Ext. 14157		
Address 2			
City	Mississauga	**State/Province**	ON
Postal Code	L4W 0B5	**Country** i	CA

Inventor 2 Remove

Legal Name

Prefix	**Given Name**	**Middle Name**	**Family Name**	**Suffix**
	Scott	Alexander	Vanstone	

Residence Information (Select One) ○ US Residency ● Non US Residency ○ Active US Military Service

City	Campbellville	Country of Residence i	CA

Mailing Address of Inventor:

Address 1	10140 Pineview Trail		
Address 2			
City	Campbellville	**State/Province**	ON
Postal Code	L0P 1B0	**Country** i	CA

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	29907-0037002
	Application Number	
Title of Invention	ELLIPTIC CURVE RANDOM NUMBER GENERATION	

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

□ **An Address is being provided for the correspondence Information of this application.**

Customer Number	94149	
Email Address		Add Email Remove Email

Application Information:

Title of the Invention	ELLIPTIC CURVE RANDOM NUMBER GENERATION		
Attorney Docket Number	29907-0037002	**Small Entity Status Claimed**	□
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	6	**Suggested Figure for Publication (if any)**	

Publication Information:

□ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

□ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	94149		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status	Pending	Remove

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	29907-0037002
	Application Number	
Title of Invention	ELLIPTIC CURVE RANDOM NUMBER GENERATION	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	11336814	2006-01-23
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11336814	non provisional of	60644982	2005-01-21
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

			Remove
Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ● No
Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.			Add

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	29907-0037002
	Application Number	
Title of Invention	ELLIPTIC CURVE RANDOM NUMBER GENERATION	

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Remove

○ Assignee ○ Legal Representative under 35 U.S.C. 117

● Person to whom the inventor is obligated to assign. ○ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Assignee is an Organization check here. ☒

Organization Name	Certicom Corp.

Mailing Address Information:

Address 1	4701 Tahoe Blvd.		
Address 2	Tahoe A, 6th Floor		
City	Mississauga	**State/Province**	ON
Country i	CA	Postal Code	L4W 0B5
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Michael K. Henry/			Date (YYYY-MM-DD)	2013-02-19
First Name	Michael K.	Last Name	Henry, Ph.D.	Registration Number	59516

Additional Signature may be generated within this form by selecting the Add button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	29907-0037002
	Application Number	
Title of Invention	ELLIPTIC CURVE RANDOM NUMBER GENERATION	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ELLIPTIC CURVE
RANDOM NUMBER GENERATION

[0001] This application claims priority from United States Provisional Patent Application No. 60/644,982 filed on January 21, 2005.

FIELD OF THE INVENTION:

[0002] The present invention relates to systems and methods for cryptographic random number generation.

DESCRIPTION OF THE PRIOR ART

[0003] Random numbers are utilised in many cryptographic operations to provide underlying security. In public key infrastructures, for example, the private key of a key pair is generated by a random number generator and the corresponding public key mathematically derived therefrom. A new key pair may be generated for each session and the randomness of the generator therefore is critical to the security of the cryptographic system.

[0004] To provide a secure source of random numbers, cryptographically secure pseudorandom bit generators have been developed in which the security of each generator relies on a presumed intractability of the underlying number-theoretical problem. The American National Standards Institute (ANSI) has set up an Accredited Standards Committee (ASC) X9 for the financial services industry, which is preparing a American National Standard (ANS) X9.82 for cryptographic random number generation (RNG). One of the RNG methods in the draft of X9.82, called Dual_EC_DRBG, uses elliptic curve cryptography (ECC) for its security. Dual_EC_DRBG will hereinafter be referred to as elliptic curve random number generation (ECRNG).

[0005] Elliptic curve cryptography relies on the intractability of the discrete log problem in cyclic subgroups of elliptic curve groups. An elliptic curve E is the set of points (x, y) that satisfy the defining equation of the elliptic curve. The defining equation is a cubic equation, and is nonsingular. The coordinates x and y are elements of a field, which is a set of elements that can be added, subtracted and divided, with the exception of zero. Examples of fields include rational numbers and real numbers. There are also finite fields, which are the fields most often used in cryptography. An example of a finite field is the set of integers modulo a prime q.

[0006] Without the loss of generality, the defining equation of the elliptic curve can be in the Weierstrass form, which depends on the field of the coordinates. When the field F is integers modulo a prime $q > 3$, then the Weierstrass equation takes the form $y^2 = x^3 + ax + b$, where a and b are elements of the field F.

[0007] The elliptic curve E includes the points (x, y) and one further point, namely the point O at infinity. The elliptic curve E also has a group structure, which means that the two points P and Q on the curve can be added to form a third point $P + Q$. The point O is the identity of the group, meaning $P + O = O + P = P$, for all points P. Addition is associative, so that $P + (Q + R) = (P + Q) + R$, and commutative, so that $P + Q = Q + R$, for all points P, Q and R. Each point P has a negative point $-P$, such that $P + (-P) = \mathrm{O}$. When the curve equation is the Weierstrass equation of the form $y^2 = x^3 + ax + b$, the negative of $P = (x, y)$ is determined easily as $-P = (x, -y)$. The formula for adding points P and Q in terms of their coordinates is only moderately complicated involving just a handful of field operations.

[0008] The ECRNG uses as input two elliptic curve points P and Q that are fixed. These points are not assumed to be secret. Typically, P is the standard generator of the elliptic curve domain parameters, and Q is some other point. In addition a secret seed is inserted into the ECRNG.

[0009] The ECRNG has a state, which may be considered to be an integer s. The state s is updated every time the ECRNG produces an output. The updated state is computed as $u = z(sP)$, where $z()$ is a function that converts an elliptic curve point to an integer. Generally, z consists of taking the x-coordinate of the point, and then converting the resulting field element to an integer. Thus u will typically be an integer derived from the x-coordinate of the point s.

[0010] The output of the ECRNG is computed as follows: $r = t(z(sQ))$, where t is a truncation function. Generally the truncation function removes the leftmost bits of its input. In the ECRNG, the number of bits truncated depends on the choice of elliptic curve, and typically may be in the range of 6 to 19 bits.

[0011] Although P and Q are known, it is believed that the output r is random and cannot be predicted. Therefore successive values will have no relationship that can be exploited to obtain private keys and break the cryptographic functions. The applicant has recognised that anybody who knows an integer d such that $Q = dP$, can deduce an integer e such that $ed = 1 \bmod n$, where n is the order of G, and thereby have an integer e such that $P = eQ$. Suppose $U = sP$ and $R = sQ$, which are the precursors to the updated state and the ECRNG output. With the integer e, one can compute U from R as $U = eR$. Therefore, the output $r = t(z(R))$, and possible values of R can be determined from r. The truncation function means that the truncated bits of R would have to be guessed. The z function means that only the x-coordinate is available, so that decompression would have to be applied to obtain the full point R. In the case of the ECRNG, there would be somewhere between about $2^6 = 64$ and 2^{19} (i.e. about half a million) possible points R which correspond to r, with the exact number depending on the curve and the specific value of r.

[0012] The full set of R values is easy to determine from r, and as noted above, determination of the correct value for R determines $U = eR$, if one knows e. The updated state is $u = z(U)$, so it can be determined from the correct value of R. Therefore knowledge of r and e allows one to determine the next state to within a number of possibilities somewhere between 2^6 and 2^{19}. This uncertainty will invariably be eliminated once another output is observed, whether directly or indirectly through a one-way function.

[0013] Once the next state is determined, all future states of ECRNG can be determined because the ECRNG is a deterministic function. (at least unless additional random entropy is fed into the ECRNG state) All outputs of the ECRNG are determined from the determined states of the ECRNG. Therefore knowledge of r and e, allows one to determine all future outputs of the ECRNG.

[0014] It has therefore been identified by the applicant that this method potentially possesses a trapdoor, whereby standardizers or implementers of the algorithm may possess a piece of information with which they can use a single output and an instantiation of the RNG to determine all future states and output of the RNG, thereby completely compromising its security. It is therefore an object of the present invention to obviate or mitigate the above mentioned disadvantages.

SUMMARY OF THE INVENTION

[0015] In one aspect, the present invention provides a method for computing a verifiably random point Q for use with another point P in an elliptic curve random number generator comprising computing a hash including the point P as an input, and deriving the point Q from the hash.

[0016] In another aspect, the present invention provides a method for producing an elliptic curve random number comprising generating an output using an elliptic curve random number generator, and truncating the output to generate the random number.

[0017] In yet another aspect, the present invention provides a method for producing an elliptic curve random number comprising generating an output using an elliptic curve random number generator, and applying the output to a one-way function to generate the random number.

[0018] In yet another aspect, the present invention provides a method of backup functionality for an elliptic curve random number generator, the method comprising the steps of computing an escrow key e upon determination of a point Q of the elliptic curve, whereby $P = eQ$, P being another point of the elliptic curve; instituting an administrator, and having the administrator store the escrow key e; having members with an elliptic curve random number generator send to the administrator, an output r generated before an output value of the generator; the administrator logging the output r for future determination of the state of the generator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] An embodiment of the invention will now be described by way of example only with reference to the appended drawings wherein:

[0020] Figure 1 is a schematic representation of a cryptographic random number generation scheme.

[0021] Figure 2 is a flow chart illustrating a selection process for choosing elliptic curve points.

[0022] Figure 3 is a block diagram, similar to figure 1 showing a further embodiment

[0023] Figure 4 is flow chart illustrating the process implemented by the apparatus of Figure 3.

[0024] Figure 5 is a block diagram showing a further embodiment.

[0025] Figure 6 is a flow chart illustrating yet another embodiment of the process of Figure 2.

[0026] Figure 7 is schematic representation of an administrated cryptographic random number generation scheme.

[0027] Figure 8 is a flow chart illustrating an escrow key selection process.

[0028] Figure 9 is a flow chart illustrating a method for securely utilizing an escrow key.

DETAILED DESCRIPTION OF THE INVENTION

[0029] Referring therefore to Figure 1, a cryptographic random number generator (ECRNG) 10 includes an arithmetic unit 12 for performing elliptic curve computations. The ECRNG also includes a secure register 14 to retain a state value s and has a pair of inputs 16, 18 to receive a pair of initialisation points *P*, *Q*. The points *P*, *Q* are elliptic curve points that are assumed to be known. An output 20 is provided for communication of the random integer to a cryptographic module 22. The initial contents of the register 14 are provided by a seed input S.

[0030] This input 16 representing the point P is in a first embodiment, selected from a known value published as suitable for such use.

[0031] The input 18 is obtained from the output of a one way function in the form of a hash function 24 typically a cryptographically secure hash function such as SHA1 or SHA2 that receives as inputs the point P. The function 24 operates upon an arbitrary bit string A to produce a hashed output 26. The output 26 is applied to arithmetic unit 12 for further processing to provide the input Q.

[0032] In operation, the ECRNG receives a bit string as a seed, which is stored in the register 14. The seed is maintained secret and is selected to meet pre-established cryptographic criteria, such as randomness and Hamming weight, the criteria being chosen to suit the particular application.

[0033] In order to ensure that d is not likely to be known (e.g. such that $P = dQ$, and $ed = 1 \bmod n$); one or both of the inputs 16, 18 is chosen so as to be verifiably random. In the embodiment of Figure 1, *Q* is chosen in a way that is verifiably random by deriving it from the output of a hash-function 24 (preferably one-way) whose input includes the point *P*. As shown in Figure 2 an arbitrary string *A* is selected at step 202, a hash *H* of *A* is computed at step 204 with *P* and optionally *S* as inputs to a hash-based function $F_H()$, and the hash *H* is then converted by the arithmetic unit 12 to a field element *X* of a desired field *F* at step 206. *P* may be pre-computed or fixed, or may also be chosen to be a verifiably random chosen value. The field element *X* is regarded as the *x*-coordinate of *Q* (thus a "compressed" representation of *Q*). The *x*-coordinate is then tested for validity on the desired elliptic curve *E* at step 208, and whether or not *X* is valid, is determined at step 210. If valid, the *x*-coordinate provided by element *X* is decompressed to provide point *Q* at step 212. The choice of which of two possible values of the y co-ordinate is generally derived from the hash value.

[0034] The points P and Q are applied at respective inputs 16, 18 and the arithmetic unit 12 computes the point sQ where s is the current value stored in the register 14. The arithmetic unit 12 converts the x-coordinate of the point (in this example point sQ) to an integer and truncates the value to obtain $r = t(z(sQ))$. The truncated value r is provided to the output 20.

[0035] The arithmetic unit 12 similarly computes a value to update the register 14 by computing sP, where s is the value of the register 14, and converting the x-coordinate of the point sP to an integer u. The integer u is stored in the register to replace s for the next iteration. {ditto above}

[0036] As noted above, the point P may also be verifiably random, but may also be an established or fixed value. Therefore, the embodiment of Figure 1 may be applied or retrofitted to systems where certain base points (e.g. P) are already implemented in hardware. Typically, the base point P will be some already existing base point, such as those recommended in Federal Information Processing Standard (FIPS) 186-2. In such cases, P is not chosen to be verifiably random.

[0037] In general, inclusion of the point P in the input to the hash function ensures that P was determined before Q is determined, by virtue of the one-way property of the hash function and since Q is derived from an already determined P. Because P was determined before Q, it is clearly understood that P could not have been chosen as a multiple of Q (e.g. where $P = eQ$), and therefore finding d is generally as hard as solving a random case of the discrete logarithm problem.

[0038] Thus, having a seed value S provided and a hash-based function $F()$ provided, a verifier can determine that $Q = F(S,P)$, where P may or may not be verifiably random. Similarly, one could compute $P = F(S,Q)$ with the same effect, though it is presumed that this is not necessary given that the value of P in the early drafts of X9.82 were identical to the base points specified in FIPS 186-2.

[0039] The generation of Q from a bit string as outlined above may be performed externally of the ECRNG 10, or, preferably, internally using the arithmetic unit 12. Where both P and Q

are required to be verifiably random, a second hash function 24 shown in ghosted outline in Figure 1 is incorporated to generate the coordinate of point P from the bit string A. By providing a hash function for at least one of the inputs, a verifiably random input is obtained.

[0040] It will also be noted that the output generated is derived from the x coordinate of the point sP. Accordingly, the inputs 16, 18 may be the x coordinates of P and Q and the corresponding values of sP and sQ obtained by using Montgomery multiplication techniques thereby obviating the need for recovery of the y coordinates.

[0041] An alternative method for choosing Q is to choose Q in some canonical form, such that its bit representation contains some string that would be difficult to produce by generating $Q = dP$ for some known d and P for example a representation of a name. It will be appreciated that intermediate forms between this method and the preferred method may also exist, where Q is partly canonical and partly derived verifiably at random. Such selection of Q, whether verifiably random, canonical, or some intermediate, can be called verifiable.

[0042] Another alternative method for preventing a key escrow attack on the output of an ECRNG, shown in Figures 3 and 4 is to add a truncation function 28 to ECRNG 10 to truncate the ECRNG output to approximately half the length of a compressed elliptic curve point. Preferably, this operation is done in addition to the preferred method of Figure 1 and 2, however, it will be appreciated that it may be performed as a primary measure for preventing a key escrow attack. The benefit of truncation is that the list of R values associated with a single ECRNG output r is typically infeasible to search. For example, for a 160-bit elliptic curve group, the number of potential points R in the list is about 2^{80}, and searching the list would be about as hard as solving the discrete logarithm problem. The cost of this method is that the ECRNG is made half as efficient, because the output length is effectively halved.

[0043] Yet another alternative method shown in Figure 5 and 6 comprises filtering the output of the ECRNG through another one-way function $F_{H2,}$, identified as 34, such as a hash function to generate a new output. Again, preferably, this operation is performed in addition to the preferred method shown in Figure 2, however may be performed as a primary measure to prevent key escrow attacks. The extra hash is relatively cheap compared to the elliptic curve operations performed in the arithmetic unit 12, and does not significantly diminish the security of the ECRNG.

[0044] As discussed above, to effectively prevent the existence of escrow keys, a verifiably random Q should be accompanied with either a verifiably random P or a pre-established P. A pre-established P may be a point P that has been widely publicized and accepted to have been selected before the notion of the ECRNG 12, which consequently means that P could not have been chosen as $P = eQ$ because Q was not created at the time when P was established.

[0045] Whilst the above techniques ensure the security of the system using the ECRNG by "closing" the trap door, it is also possible to take advantage of the possible interdependence of P and Q, namely where $P = eQ$, through careful use of the existence of e.

[0046] In such a scenario, the value e may be regarded as an escrow key. If P and Q are established in a security domain controlled by an administrator, and the entity who generates Q for the domain does so with knowledge of e (or indirectly via knowledge of d). The administrator will have an escrow key for every ECRNG that follows that standard.

[0047] Escrow keys are known to have advantages in some contexts. They can provide a backup functionality. If a cryptographic key is lost, then data encrypted under that key is also lost. However, encryption keys are generally the output of random number generators. Therefore, if the ECRNG is used to generate the encryption key K, then it may be possible that the escrow key e can be used to recover the encryption key K. Escrow keys can provide other functionality, such as for use in a wiretap. In this case, trusted law enforcement agents may need to decrypt encrypted traffic of criminals, and to do this they may want to be able to use an escrow key to recover an encryption key.

[0048] Figure 7 shows a domain 40 having a number of ECRNG's 10 each associated with a respective member of the domain 40. The domain 40 communicates with other domains 40a, 40b, 40c through a network 42, such as the internet. Each ECRNG of a domain has a pair of identical inputs P,Q. The domain 40 includes an administrator 44 who maintains in a secure manner an escrow key e.

[0049] The administrator 44 chooses the values of P and Q such that he knows an escrow key e such that $Q = eP$. Other members of the domain 40 use the values of P and Q, thereby giving the administrator 44 an escrow key e that works for all the members of the organization.

[0050] This is most useful in its backup functionality for protecting against the loss of encryption keys. Escrow keys e could also be made member-specific so that each member has its own escrow e' from points selected by the administrator 44.

[0051] As generally denoted as numeral 400 in Figure 8, the administrator initially selects a point P which will generally be chosen as the standard generator P for the desired elliptic curve 402. The administrator then selects a value d and the point Q will be determined as $Q = dP$ 404, for some random integer d of appropriate size. The escrow key e is computed as $e = d^{-1} \bmod n$ 406, where n is the order of the generator P and stored by the administrator.

[0052] The secure use of such an escrow key 34e is generally denoted by numeral 500 and illustrated in Figure 9. The administrator 44 is first instituted 502 and an escrow keys e would be chosen and stored 504 by the administrator44

[0053] In order for the escrow key to function with full effectiveness, the escrow administrator 44 needs direct access to an ECRNG output value r that was generated before the ECRNG output value k (i.e. 16) which is to be recovered. It is not sufficient to have indirect access to r via a one-way function or an encryption algorithm. A formalized way to achieve this is to have each member with an ECRNG 12 communicate with the administrator 44 as indicated at 46 in figure 7. and step 506 in figure 9. This may be most useful for encrypted file storage systems or encrypted email accounts. A more seamless method may be applied for cryptographic applications. For example, in the SSL and TLS protocols, which are used for securing web (HTTP) traffic, a client and server perform a handshake in which their first actions are to exchange random values sent in the clear.

[0054] Many other protocols exchange such random values, often called nonces. If the escrow administrator observes these nonces, and keeps a log of them 508, then later it may be able to determine the necessary r value. This allows the administrator to determine the subsequent state of the ECRNG 12 of the client or server 510 (whoever is a member of the domain), and thereby recover the subsequent ECRNG 12 values. In particular, for the client who generally generates a random pre-master secret from which is derived the encryption key for the SSL or TLS session, the escrow key may allow recovery of the session key. Recovery of the session key allows recovery of the whole SSL or TLS session.

[0055] If the session was logged, then it may be recovered. This does not compromise long-term private keys, just session keys obtained from the output of the ECRNG, which should alleviate any concern regarding general suspicions related to escrows.

[0056] Whilst escrow keys are also known to have disadvantages in other contexts, their control within specific security domains may alleviate some of those concerns. For example, with digital signatures for non-repudiation, it is crucial that nobody but the signer has the signing key, otherwise the signer may legitimately argue the repudiation of signatures. The existence of escrow keys means the some other entity has access to the signing key, which enables signers to argue that the escrow key was used to obtain their signing key and subsequently generate their signatures. However, where the domain is limited to a particular organisation or part of an organisation it may be sufficient that the organisation cannot repudiate the signature. Lost signing keys do not imply lost data, unlike encryption keys, so there is little need to backup signing keys.

[0057] Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

What is claimed is:

1. A method of computing a random number for use in a cryptographic operation comprising the steps of providing a pair of inputs to an elliptic curve random number generator with each input representative of at least one coordinate of an elliptic curve point and with at least one of said inputs being verifiably random.

2. A method according to claim 1 wherein said at least one input is obtained from an output of a hash function.

3. A method according to claim 2 wherein the other of said inputs is utilized as an input to said hash function.

4. A method according to claim 1 wherein said random number generator has a secret value and said secret value is used to compute scalar multiples of said points represented by said inputs.

5. A method according to claim 4 wherein one of said scalar multiples is used to derive said random number and the other of said scalar multiples is used to change said secret value for subsequent use.

6. A method according to claim 2 wherein said output of said hash function is validated as a coordinate of a point on an elliptic curve prior to utilization as said input.

7. A method according to claim 6 wherein another coordinate of said point is obtained from said one coordinate for inclusion as said input.

8. A method according to claim 7 wherein said other input is a representation of an elliptic curve point.

9. A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and truncating said coordinate to a bit string for use as said random number.

10. A method according to claim 9 wherein said one coordinate is truncated in the order of one half the length of a representation of an elliptic curve point representation.

11. A method according to claim 5 wherein said random number is derived from said scalar multiple by selecting one coordinate of said point represented by said scalar multiple and hashing said one coordinate to provide a bit string for use as said random number.

12. A method according to claim 1 wherein said verifiably random input is chosen to be of a canonical form whereby a predetermined relationship between said inputs is difficult to maintain.

13. A method of computing a random number for use in a cryptographic operation, said method comprising the steps of providing a pair of inputs, each representative of at least one coordinate of a pair of elliptic curve points to an elliptic curve random number generator, obtaining an output representative of at least one coordinate of a scalar multiple of an elliptic curve point and passing said output through a one way function to obtain a bit string for use as a random number.

14. A method according to claim 13 wherein said one way function is a hash function.

15. An elliptic curve random number generator having a pair of inputs each representative of at least one coordinate of a pair of elliptic curve points and an output for use as a random number in a cryptographic operation, at least one of said inputs being verifiably random.

16. An elliptic curve random number generator according to claim 15 wherein said one input is derived from an output of a one way function.

17. An elliptic curve random number generator according to claim 16 wherein said one way function is a hash function.

18. An elliptic curve random number generator according to claim 17 wherein the other of said inputs is provided as an input to said hash function.

19. A method of establishing an escrow key for a security domain within a network, said method comprising the steps of establishing a pair of points PQ as respective inputs to an elliptic curve random number generator with a relationship between said point such that $P = eQ$, storing said relationship e as an escrow key with an administrator and generating from said elliptic curve random number generator a random number for use in cryptographic operations within said domain.

ABSTRACT

An elliptic curve random number generator avoids escrow keys by choosing a point Q on the elliptic curve as verifiably random. An arbitrary string is chosen and a hash of that string computed. The hash is then converted to a field element of the desired field, the field element regarded as the x-coordinate of a point Q on the elliptic curve and the x-coordinate is tested for validity on the desired elliptic curve. If valid, the x-coordinate is decompressed to the point Q, wherein the choice of which is the two points is also derived from the hash value. Intentional use of escrow keys can provide for back up functionality. The relationship between P and Q is used as an escrow key and stored by for a security domain. The administrator logs the output of the generator to reconstruct the random number with the escrow key.

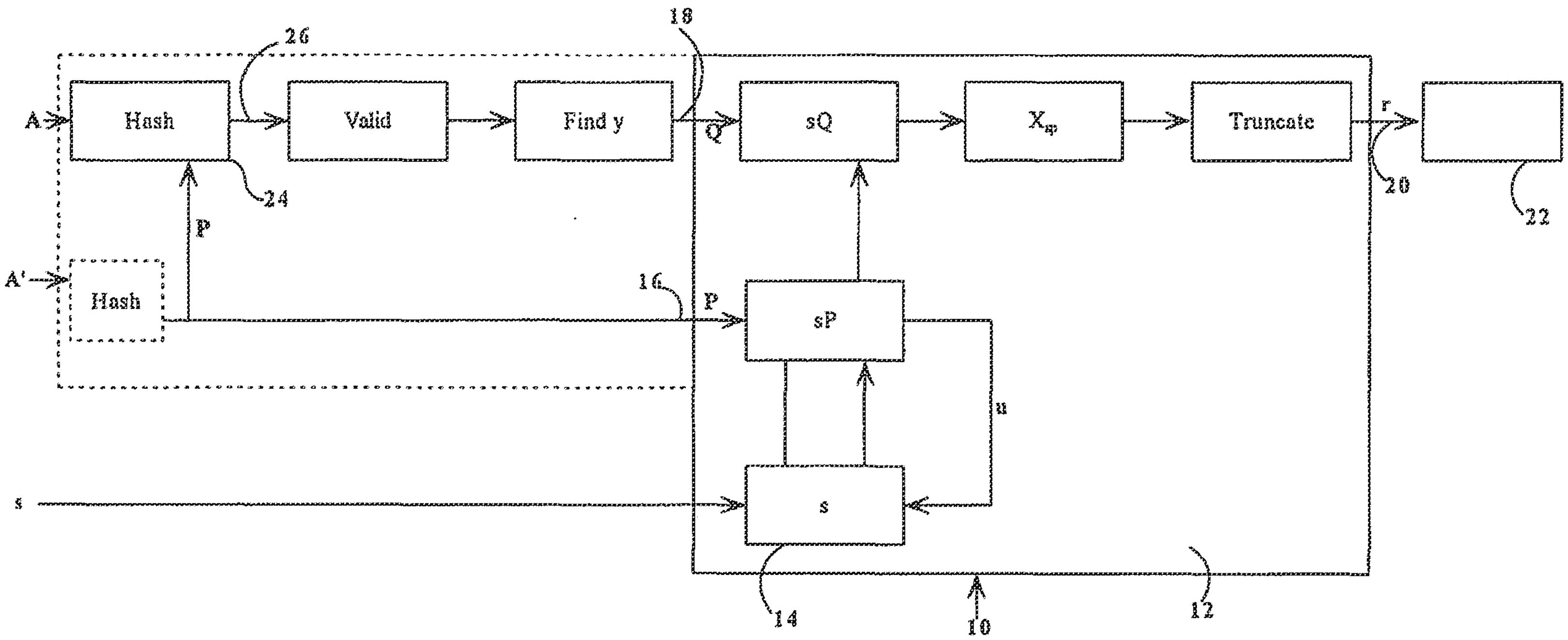
A
A'
s
Hash
Hash
P
P
Valid
Find y
Q
sQ
X_{sp}
Truncate
r
sP
s
u
26
24
18
16
20
22
14
10
12

FIGURE 1

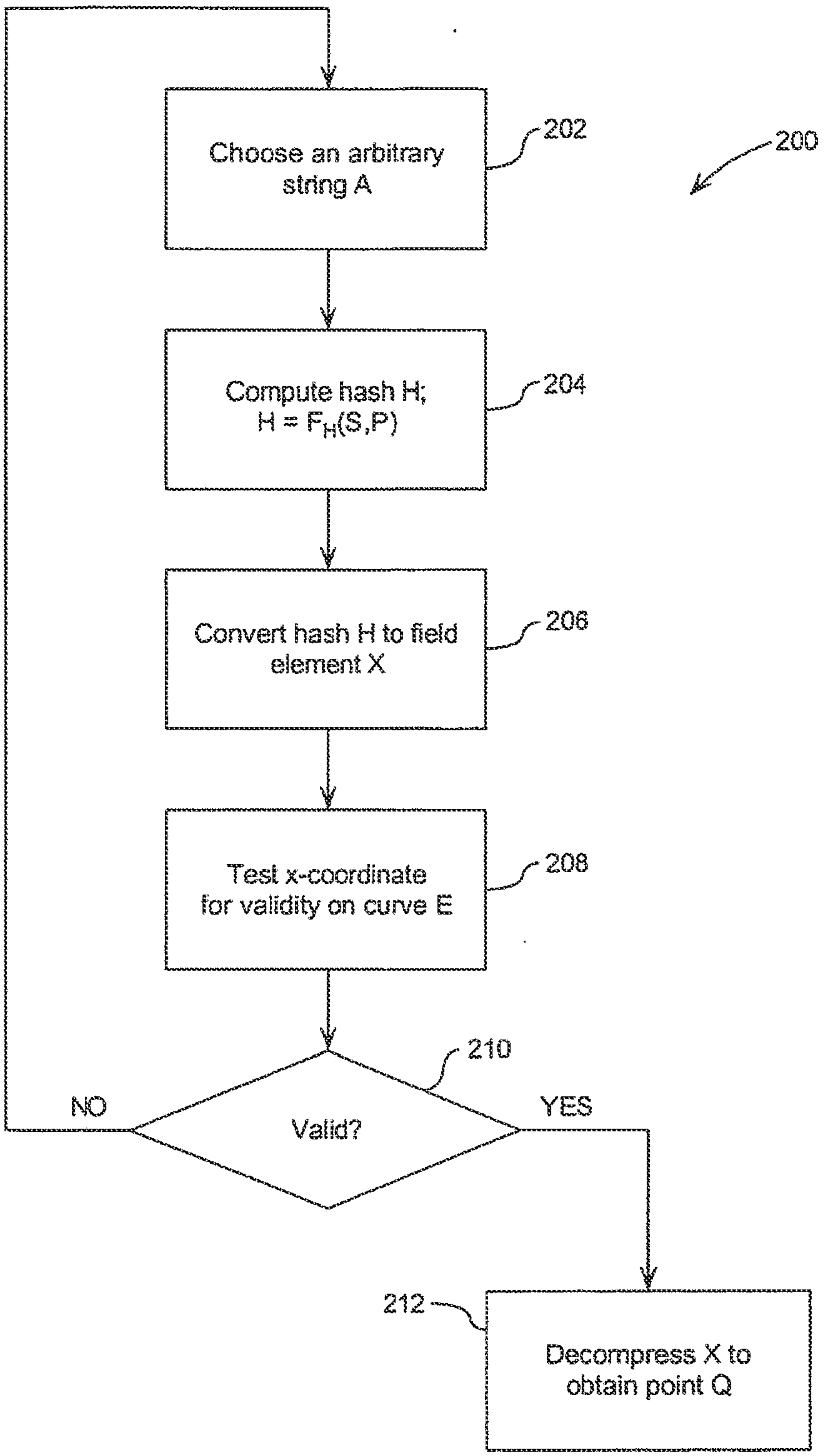
200
Choose an arbitrary string A
202
Compute hash H;
$H = F_H(S,P)$
204
Convert hash H to field element X
206
Test x-coordinate for validity on curve E
208
Valid?
210
NO
YES
212
Decompress X to obtain point Q

Figure 2

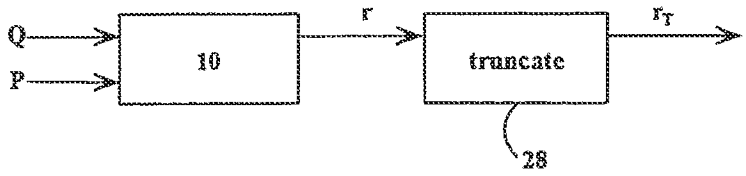

FIGURE 3

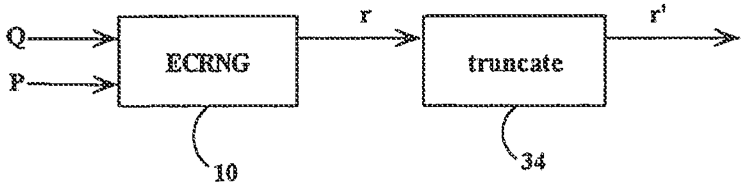

FIGURE 5

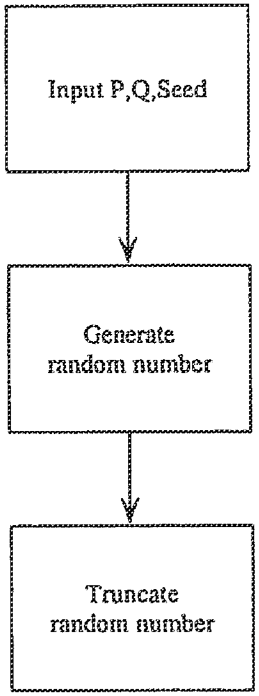

Figure 4

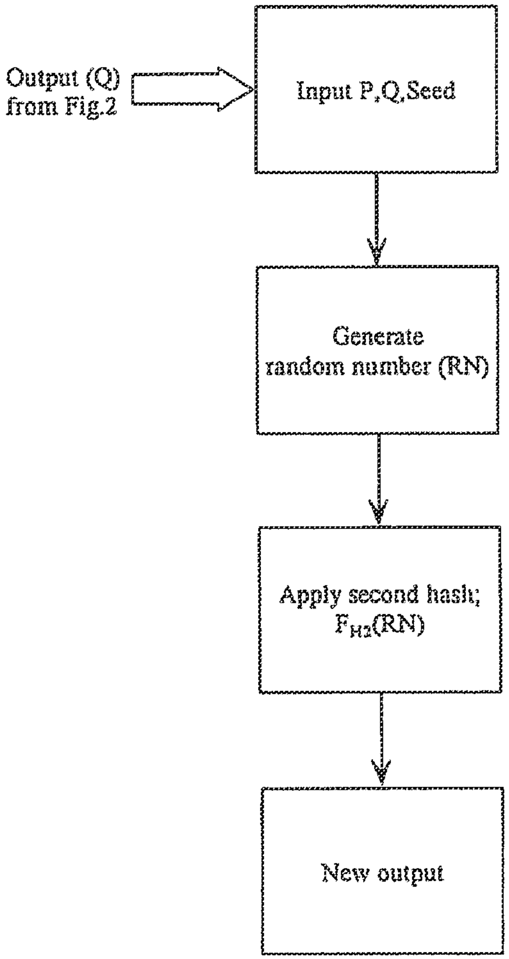

Figure 6

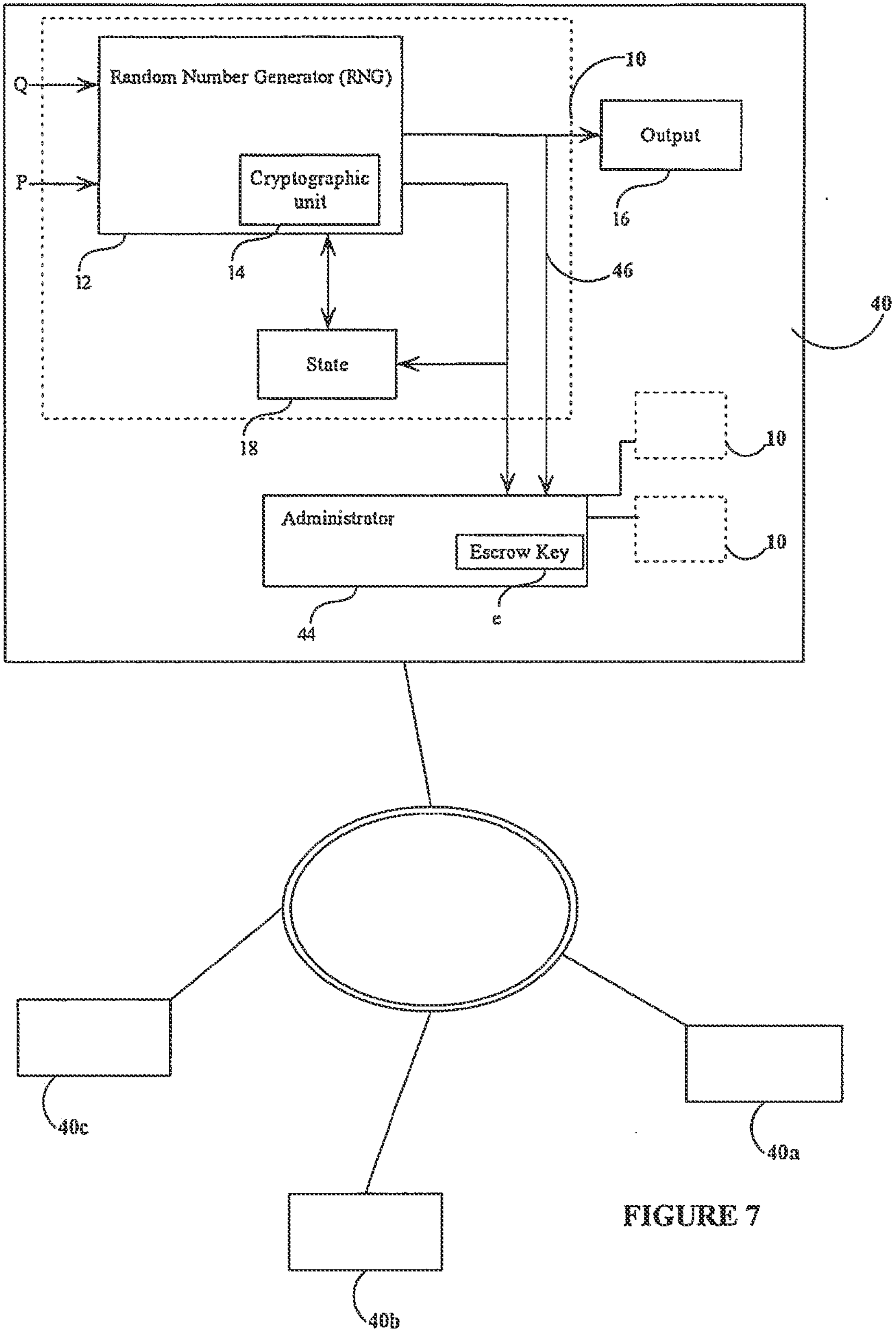
Q
P
Random Number Generator (RNG)
Cryptographic unit
10
Output
16
12
14
46
40
State
18
10
10
Administrator
Escrow Key
44
e
40c
40a
40b

FIGURE 7

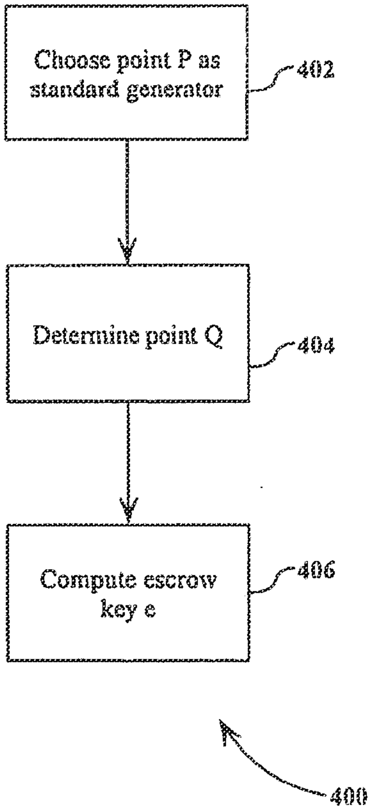

Figure 8

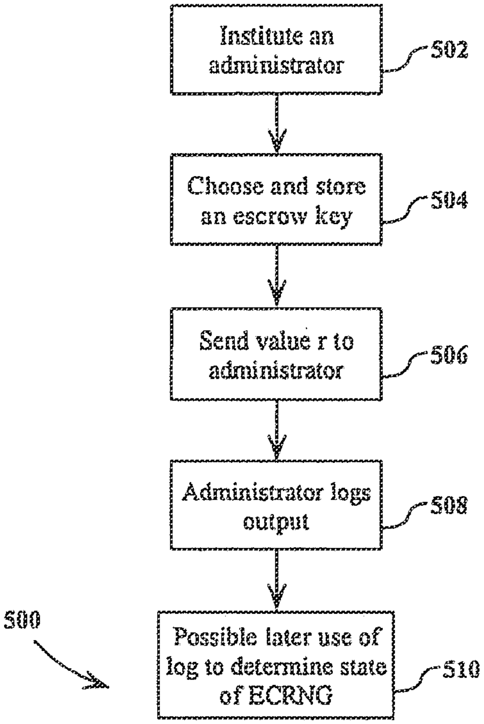
Institute an administrator
502
Choose and store an escrow key
504
Send value r to administrator
506
Administrator logs output
508
Possible later use of log to determine state of ECRNG
510
500

Figure 9

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Daniel Richard L. Brown et al.   Art Unit : Unknown
Serial No. : Unknown   Examiner : Unknown
Filed : February 19, 2013
Title : ELLIPTIC CURVE RANDOM NUMBER GENERATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination, please amend the application as indicated on the following pages.

Amendments to the Specification:

Please replace paragraph [0001] found on page 1 with the following amended paragraph:

This application is a continuation of and claims priority from United States Patent Application No. 11/336,814, filed on January 23, 2006, which is hereby incorporated by reference and which claims priority from United States Provisional Patent Application No. 60/644,982 filed on January 21, 2005.

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-19. (Cancelled)

20. (New) A computer-implemented method of generating a random number for use in a cryptographic operation, the method comprising:

generating a random number by operating one or more processors on a pair of inputs, each input representing at least one coordinate of a respective one of a pair of elliptic curve points, at least one input of the pair of inputs being generated in a manner to ensure that one point of the pair of elliptic curve points is not a multiple of the other point of the pair of elliptic curve points.

21. (New) The method of claim 20, wherein the at least one of the pair of inputs is obtained from an output of a hash function.

22. (New) The method of claim 21, wherein the other input of the pair of inputs is obtained from an output of a hash function.

23. (New) The method of claim 21, wherein the other input of the pair of inputs is used as an input to the hash function.

24. (New) The method of claim 23, wherein the other input of the pair of inputs represents an elliptic curve point.

25. (New) The method of claim 21, further comprising:

testing the output of the hash function to determine whether the output is a valid coordinate of a point on an elliptic curve before using the output as one of the inputs.

26. (New) The method of claim 25, wherein the output is a valid coordinate of a first elliptic curve point, and the method comprises obtaining another coordinate of the first elliptic curve point before using the first elliptic curve point as one of the inputs.

27. (New) The method of claim 20, further comprising using a secret value to compute scalar multiples of each of the points represented by the pair of inputs.

28. (New) The method of claim 27, further comprising using one of the scalar multiples to derive the random number and using the other of the scalar multiples to change the secret value for subsequent use.

29. (New) The method of claim 27, further comprising deriving the random number from one of the scalar multiples by selecting one coordinate of the point represented by the one of the scalar multiples and truncating the coordinate to a bit string for use as the random number.

30. (New) The method of claim 29, wherein truncating the coordinate includes removing the highest order half of the bits in an elliptic curve point representation.

31. (New) The method of claim 27, further comprising deriving the random number from one of the scalar multiples by selecting one coordinate of the point represented by the one of the scalar multiples and hashing the one coordinate to provide a bit string for use as the random number.

32. (New) The method of claim 20, comprising generating the pair of inputs in a manner to ensure that one point of the pair of elliptic curve points is not a multiple of the other point of the pair of elliptic curve points.

33. (New) A non-transitory computer-readable medium comprising instructions that are operable when executed by one or more processors to perform operations comprising:

generating a random number from a pair of inputs, each input representing at least one coordinate of a respective one of a pair of elliptic curve points, at least one input of the pair of inputs being generated in a manner to ensure that one point of the pair of elliptic curve points is not a multiple of the other point of the pair of elliptic curve points.

34. (New) The computer-readable medium of claim 33, wherein the at least one of the pair of inputs is obtained from an output of a hash function.

35. (New) The computer-readable medium of claim 34, wherein the other input of the pair of inputs is obtained from an output of a hash function.

36. (New) The computer-readable medium of claim 34, wherein the other input of the pair of inputs is used as an input to the hash function.

37. (New) The computer-readable medium of claim 36, wherein the other input of the pair of inputs represents an elliptic curve point.

38. (New) The computer-readable medium of claim 34, the operations further comprising:

testing the output of the hash function to determine whether the output is a valid coordinate of a point on an elliptic curve before using the output as one of the inputs.

39. (New) The computer-readable medium of claim 38, wherein the output is a valid coordinate of a first elliptic curve point, and the operations comprise obtaining another coordinate of the first elliptic curve point before using the first elliptic curve point as one of the inputs.

40. (New) The computer-readable medium of claim 33, the operations further comprising using a secret value to compute scalar multiples of each of the points represented by the pair of inputs.

41. (New) The computer-readable medium of claim 40, the operations further comprising using one of the scalar multiples to derive the random number and using the other of the scalar multiples to change the secret value for subsequent use.

42. (New) The computer-readable medium of claim 40, the operations further comprising deriving the random number from one of the scalar multiples by selecting one coordinate of the point represented by the one of the scalar multiples and truncating the coordinate to a bit string for use as the random number.

43. (New) The computer-readable medium of claim 42, wherein truncating the coordinate includes removing the highest order half of the bits in an elliptic curve point representation.

44. (New) The computer-readable medium of claim 40, the operations further comprising deriving the random number from one of the scalar multiples by selecting one coordinate of the point represented by the one of the scalar multiples and hashing the one coordinate to provide a bit string for use as the random number.

45. (New) A random number generator system comprising one or more processors configured to:

generate a random number from a pair of inputs, each input representing at least one coordinate of a respective one of a pair of elliptic curve points, at least one input of the pair of inputs being generated in a manner to ensure that one point of the pair of elliptic curve points is not a multiple of the other point of the pair of elliptic curve points.

46. (New) The elliptic curve random number generator system of claim 45, wherein the at least one of the pair of inputs is obtained from an output of a hash function.

47. (New) The elliptic curve random number generator system of claim 46, wherein the other input of the pair of inputs is obtained from an output of a hash function.

48. (New) The elliptic curve random number generator system of claim 46, wherein the other input of the pair of inputs is used as an input to the hash function.

49. (New) The elliptic curve random number generator system of claim 46, wherein the other input of the pair of inputs represents an elliptic curve point.

50. (New) The elliptic curve random number generator system of claim 46, the one or more processors configured to:

test the output of the hash function to determine whether the output is a valid coordinate of a point on an elliptic curve before using the output as one of the inputs.

51. (New) The elliptic curve random number generator system of claim 50, wherein the output is a valid coordinate of a first elliptic curve point, and the one or more processors are

configured to obtain another coordinate of the first elliptic curve point before using the first elliptic curve point as one of the inputs.

52. (New) The elliptic curve random number generator system of claim 45, the one or more processors configured to use a secret value to compute scalar multiples of each of the points represented by the pair of inputs.

53. (New) The elliptic curve random number generator system of claim 52, the one or more processors configured to use one of the scalar multiples to derive the random number and using the other of the scalar multiples to change the secret value for subsequent use.

54. (New) The elliptic curve random number generator system of claim 52, the one or more processors configured to derive the random number from one of the scalar multiples by selecting one coordinate of the point represented by the one of the scalar multiples and truncating the coordinate to a bit string for use as the random number.

55. (New) The elliptic curve random number generator system of claim 54, wherein truncating the coordinate includes removing the highest order half of the bits in an elliptic curve point representation.

56. (New) The elliptic curve random number generator system of claim 52, the one or more processors configured to derive the random number from one of the scalar multiples by selecting one coordinate of the point represented by the one of the scalar multiples and hashing the one coordinate to provide a bit string for use as the random number.

REMARKS

This Preliminary Amendment is being filed concurrently with the application. The specification is currently amended to refer to the parent application. Claims 1-19 are currently canceled, and claims 20-56 are currently added. It is respectfully requested that all claims be examined in view of the amendments set forth above.

No fees are believed to be due. However, please apply any deficiencies or any other required fees or any credits to Deposit Account 06-1050, referencing the above attorney docket number.

Respectfully submitted,

Date: February 19, 2013

/Michael K. Henry/
Michael K. Henry, Ph.D.
Reg. No. 59,516

Customer Number 94149
Fish & Richardson P.C.
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/770,533	Filing Date 02/19/2013	□ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY □		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
□ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**02/19/2013**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 37	Minus	** 37	= 0	X $ =		OR	X $62=	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $ =		OR	X $250=	0
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/JULIET MCMILLAN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/17 (10-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if known	
Application Number	
Filing Date	February 19, 2013
First Named Inventor	Daniel Richard L. Brown et al.
Examiner Name	
Art Unit	
Practitioner Docket No.	29907-0037002

□ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 2314.00

METHOD OF PAYMENT (check all that apply)

□ Check □ Credit Card □ Money Order □ None □ Other (please identify): ____________

☒ Deposit Account Deposit Account Number: 06-1050 Deposit Account Name: Fish & Richardson P.C.

For the above-identified deposit account, the Director is hereby authorized to (check all that apply):

☒ Charge fee(s) indicated below □ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayment of fee(s)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	390	195	620	310	250	125	1260
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	390	195	620	310	760	380	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	62	31
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	460	230

Total Claims		Extra Claims		Fee ($)		Fee Paid ($)
37	-20 or HP =	17	x	62	=	1054

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		Extra Claims		Fee ($)		Fee Paid ($)
3	-3 or HP =		x	250 .	=	

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims
Fee ($) ________ Fee Paid ($) ________

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $320 ($160 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof		Fee ($)		Fee Paid ($)
21	- 100 =		/ 50 =	(round up to a whole number)	x		=	

4. OTHER FEE(S) Fees Paid ($)

Non-English specification, $130 fee (no small entity discount) ________

Non-electronic filing fee under 37 CFR 1.16(t) for a utility application, $400 fee ($200 small entity) ________

Other (e.g., late filing surcharge): ____________ ________

SUBMITTED BY

Signature	/Michael K. Henry/	Registration No. (Attorney/Agent) 59516	Telephone 214-747-5070
Name (Print/Type)	Michael K. Henry, Ph.D.		Date February 19, 2013

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	14992335
Application Number:	13770533
International Application Number:	
Confirmation Number:	5276
Title of Invention:	ELLIPTIC CURVE RANDOM NUMBER GENERATION
First Named Inventor/Applicant Name:	Daniel Richard L. Brown
Customer Number:	94149
Filer:	Michael K. Henry/Lisa Peterson
Filer Authorized By:	Michael K. Henry
Attorney Docket Number:	29907-0037002
Receipt Date:	19-FEB-2013
Filing Date:	
Time Stamp:	16:21:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2314
RAM confirmation Number	4426
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/770,533	02/19/2013	Daniel Richard L. Brown	29907-0037002

CONFIRMATION NO. 5276

94149
Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

NOTICE

OC000000059768443

Date Mailed: 03/15/2013

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  All
  Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/770,533	02/19/2013		2444	29907-0037002	37	3

CONFIRMATION NO. 5276

94149
Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

FILING RECEIPT

OC000000059768442

Date Mailed: 03/15/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Daniel Richard L. Brown, Mississauga, CANADA;
Scott Alexander Vanstone, Campbellville, CANADA;

Applicant(s)

CERTICOM CORP., Mississauga, CANADA

Assignment For Published Patent Application

CERTICOM CORP., Mississauga, CANADA

Power of Attorney: The patent practitioners associated with Customer Number 94149

Domestic Priority data as claimed by applicant

This application is a CON of 11/336,814 01/23/2006 PAT 8396213
which claims benefit of 60/644,982 01/21/2005

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

Projected Publication Date: To Be Determined - pending completion of Security Review

Non-Publication Request: No

Early Publication Request: No

Title

ELLIPTIC CURVE RANDOM NUMBER GENERATION

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
13/770,533

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY			OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE($)	FEE($)	OR	RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	390
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	37 minus 20 =	* 17			OR	x 62 =	1054
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2314

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/770,533	02/19/2013	Daniel Richard L. Brown	29907-0037002

CONFIRMATION NO. 5276

94149
Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

POA ACCEPTANCE LETTER

OC000000059766986

Date Mailed: 03/15/2013

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/19/2013.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/jchery/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

3/21/13

DEPARTMENT OF DEFENSE
ACCESS ACKNOWLEDGEMENT / SECRECY ORDER RECOMMENDATION
FOR PATENT APPLICATION

Application Serial No: DP13770533 Date Referred: 03/01/2013

I hereby acknowledge that the Department of Defense reviewers have inspected this application in administration of 35 USC 181 on behalf of the Agencies/Commands specified below. DoD reviewers will not divulge any information from this application for any purpose other than administration of 35 USC 181.

Defense Agency	**Recommendation**	**Reviewer Name**	**Date Reviewed**
NSA	Secrecy Not Recommended	Robert Morelli	04 Mar 2013

Defense Agency	**Reviewer Name**	**Date Viewed PDF**
DTSA	Tim Hamilton	04 Mar 2013 13:57

Instructions to Reviewers:

1. All DoD personnel reviewing this application will be listed on this form regardless of whether they are making a secrecy order recommendation.
2. This form will be forwarded to USPTO once all assigned DoD entities have provided their secrecy order recommendation.

DoD Completion of Review: Final
Forwarded to USPTO: 03/07/2013

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/770,533	02/19/2013	Daniel Richard L. Brown	29907-0037002

CONFIRMATION NO. 5276

94149
Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

NEW OR REVISED PPD NOTICE

OC000000060123758

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 07/04/2013. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Data Management, Application Assistance Unit at (571) 272-4000, or (571) 272-4200, or 1-888-786-0101.

PART 1 - ATTORNEY/APPLICANT COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/770,533	02/19/2013	Daniel Richard L. Brown	29907-0037002

CONFIRMATION NO. 5276

PUBLICATION NOTICE

OC000000062382593

94149
Fish & Richardson PC
P.O.Box 1022
Minneapolis, MN 55440

Title:ELLIPTIC CURVE RANDOM NUMBER GENERATION

Publication No.US-2013-0170642-A1
Publication Date:07/04/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101