



- (51) **International Patent Classification:**
G09C 1/00 (2006.01) *H04L 9/06* (2006.01)
- (21) **International Application Number:**
PCT/MY2014/000160
- (22) **International Filing Date:**
4 June 2014 (04.06.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
PI 2013004371 4 December 2013 (04.12.2013) MY
- (71) **Applicant:** MIMOS BERHAD [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (72) **Inventors:** ISA, Herman Bin; c/o MIMOS BERHAD, Technology Park Malaysia, 57000 Kuala Lumpur (MY). Z'ABA, Muhammad Reza Bin; c/o MIMOS BERHAD, Technology Park Malaysia, 57000 Kuala Lumpur (MY). BAHARI, Iskandar Bin; c/o MIMOS BERHAD, Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (74) **Agent:** MIRANDAH, PATRICK; Mirandah Asia (Malaysia) sdn bhd, Suite 3B-19-3, Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

[Continued on next page]

(54) **Title:** A METHOD TO CONSTRUCT BIJECTIVE SUBSTITUTION BOX FROM NON-PERMUTATION POWER FUNCTIONS USING HEURISTIC TECHNIQUES

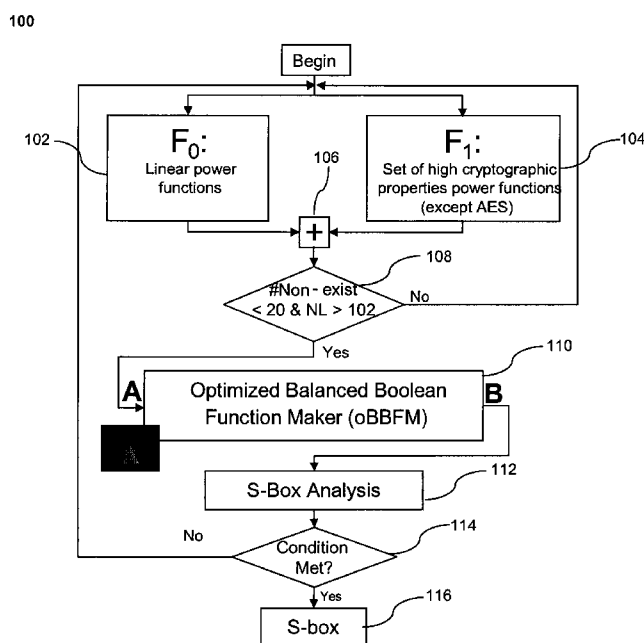


FIG. 1.0

(57) **Abstract:** Bijective substitution box is constructed from non-permutation power functions wherein said non-permutation functions are optimally converted to a permutation function by utilizing the heuristic algorithm of an Optimized Balanced Boolean Function Maker algorithm such that it has high cryptographic properties. The result is a bijective function, which provides desirable cryptographic properties such as high nonlinearity of 108 and high algebraic degree of 7. The said construction of bijective substitution boxes from non-permutation power functions using heuristic techniques comprising steps of first selecting a Boolean map from a plurality of linear power functions and high cryptographic properties power function (102, 104); extending an image of said Boolean map to generate an extended map (106, 108); obtaining a bijective function from said extended image by utilizing Optimized Balanced Boolean Function Maker algorithm (110); and performing analysis on cryptographic properties of substitution box (112). The said steps are iterated until said cryptographic properties meets the predetermined condition of a cryptographically strong bijective substitution box.



Published:

— *with international search report (Art. 21(3))*

A METHOD TO CONSTRUCT BIJECTIVE SUBSTITUTION BOX FROM NON-PERMUTATION POWER FUNCTIONS USING HEURISTIC TECHNIQUES

FIELD OF INVENTION

5

The present invention relates to a method for constructing bijective substitution box from non-permutation power functions using heuristic techniques. In particular, the present invention construct substitution box by utilizing Optimize Balanced Boolean Function Maker algorithm which includes the heuristic technique in the algorithm.

10

BACKGROUND ART

15

20

25

30

The present invention provides an improved methodology of constructing new cryptographically strong S-Boxes in which the bijective S-Boxes are obtained by utilizing Optimize Balanced Boolean Function Maker algorithm which includes the heuristic technique in the algorithm. Existing methodology in the Applicant's earlier invention is described in Malaysia Patent Application No. PI 2012005375 (hereinafter denoted as the PI '375 Application). In PI '375 Application, binomial combination is selected from a set of all power functions in $GF(2^8)$ as compared to the present invention wherein binomial combination is between power function that provide smallest number of non-existing elements but have highest cryptographic properties. Binomial operation and affine transformation between two power functions in Galois fields, i.e. $GF(2^8)$ will mostly produce new non-permutation functions (i.e. non-bijective functions). Although the resulting functions of the existing methodology includes functions with high cryptographic properties such as high nonlinearity and high algebraic degree as desired, the said resulting function of the existing methodology is non-permutation which is not suitable to be used in most block ciphers. The present invention drives to produce a method to optimally convert non-permutation functions to permutation functions with high cryptographic properties.

One example of construction of 8×8 bijective cryptographically strong S-Boxes using non-bijective power functions over finite field is disclosed in a published paper entitled "Practical Bijective S-Box Design" by Abdulrashid Mamadolimov, Herman Isa, Moesfa Soeheila Mohamad; Proceedings of the 5th Asian Mathematical Conference, Malaysia

- 2 -

2009. In the said paper, the algorithm to make a bijective Boolean function is a vectorial Boolean function which is a map from F_{2^n} to F_{2^m} ; wherein F_2 is a finite field with two elements as compared to the present invention wherein the present invention provides for binomial combination which is between the power function that provide the smallest number of non-exist elements but have highest cryptographic properties. Further, the said paper proposes several methods to generate cryptographically strong S-boxes such as random generation as compared to the present invention which utilizes Optimize Balanced Boolean Function Maker algorithm that includes the heuristic technique in the algorithm.

An example which shows how a cost function has found excellent single-output Boolean functions can be generalized to provide improved results for small S-boxes is disclosed in a paper entitled "The Design of S-boxes by Simulated Annealing" by John A. Clark, Jeremy L. Jacob, Susan Stepney; Department of Computer Science, University of York, Heslington, York, UK. In the said paper, a cost function is provided wherein excellent single-output Boolean functions can be generalized to provide improved results for small S-boxes. In contrast, the present invention provides for binomial combination which is between the power function that provides the smallest number of non-existing elements but have highest cryptographic properties. Further, the said paper discloses that s-boxes are constructed by simulated annealing as compared to the present invention which utilizes Optimize Balanced Boolean Function Maker algorithm that includes heuristic technique in the algorithm.

Preliminary theory which relates to both Boolean functions and S-boxes are disclosed in an IEEE paper entitled "Multi-objective Optimisation of Bijective S-boxes" by Joanne Fuller, William Millan and Ed Dawson; 2004 IEEE. The said paper discloses the investigation of heuristic constructions of bijective s-boxes that satisfy a wide range of cryptographic criteria including algebraic complexity, high non-linearity, and low autocorrelation. An associated Boolean function theory by designing S-boxes with a high level of security is provided wherein binomial combination with selected candidates from a set of all power functions in $GF(2^8)$ is used to define distinct 8×8 bijective S-boxes as compared to the present invention wherein binomial combination is between power function that provide smallest number of non-exist elements but have highest cryptographic properties.

- 3 -

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practiced.

SUMMARY OF INVENTION

The present invention relates to a method for constructing bijective substitution box from non-permutation power functions using heuristic techniques. In particular, the present invention construct substitution box by utilizing Optimize Balanced Boolean Function Maker algorithm which includes the heuristic technique in the algorithm.

One aspect of the present invention provides for a method (100) to construct bijective substitution boxes from non-permutation power functions using heuristic techniques. The method (100) comprising steps of:

- i. selecting a Boolean map from a plurality of linear power functions and high cryptographic properties power function (102, 104);
- ii. extending an image of said Boolean map to generate an extended map (106, 108);
- 15 iii. obtaining a bijective function from said extended image by utilizing Optimized Balanced Boolean Function Maker algorithm (110);
- iv. performing analysis on cryptographic properties of substitution box (112); and
- 20 v. iterating steps (ii), (iii) and (iv) until said cryptographic properties meet predetermined condition of a cryptographically strong bijective substitution box

The step of obtaining a bijective function from said extended image by utilizing Optimized Balanced Boolean Function Maker algorithm (110); said bijective function is a result of heuristic technique of said Optimized Balanced Boolean Function Maker algorithm; and said bijective function provides cryptographic properties with high nonlinearity value and high algebraic value.

Another aspect of the invention provides for the step of extending an image of said Boolean map to generate an extended map (106, 108). The said step further comprising steps of:

- i. identifying a first power function from a plurality of power function which have high cryptographic properties (202);

- 5 -

- 5
- ii. generating a plurality of non-bijective power functions using a linear combination between a plurality of linear combination of power functions (204);
 - iii. identifying number of non-existence elements in the plurality of non-bijective power functions (206);
 - iv. selecting the plurality of non-bijective power functions which is less than pre-determined number of non-existence elements (208); and
 - 10 v. iterating steps (i) –(iv) for power functions of all high cryptographic properties from the plurality of power functions.

In yet another aspect of the invention is the step for obtaining a bijective function from said extended image by utilizing Optimized Balanced Boolean Function Maker algorithm (110). The said step further comprising steps of:

- 15
- i. receiving Boolean function from extended Boolean map (302);
 - ii. computing frequency table from said extended Boolean map (304);
 - iii. determining if all frequencies in frequency table = 1 (306);
If all frequencies in frequency table = 1;
 - 20 function is balanced (308) else
 - iv. identifying elements which are not outputs of extended Boolean map (310);
 - v. identifying duplicate elements in extended Boolean map using frequency table (310);
 - 25 vi. computing distance matrix of all elements in step (iv) and (v) by comparing bit error rate between said elements (312);
 - vii. locating smallest element in distance matrix (314);
 - viii. listing all corresponding header of step (vii) (316);
 - ix. listing all corresponding data of step (vii) (316)
 - 30 x. locating all corresponding location of entry of elements from step (viii) of Boolean map (318);
 - xi. replacing elements from step (ix) with corresponding element in step (viii) at location of step (x) and calculating non-linearity for temporary Boolean map (320);

- 6 -

- xii. iterating steps (ix), (x) and (xi) for all corresponding elements from step (viii) (322);
- xiii. identifying highest nonlinearity from calculations computed in step (xi) (324);
- xiv. identifying corresponding Boolean map from entry of step (xii) and replacing said original Boolean map with results obtained from step (xiii); and
- xv. iterating steps (i) to (xiv) until said frequency table is free from plurality of header and data.

5

10

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific
5 embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

10 FIG. 1.0 is a flowchart illustrating the general methodology of the present invention to construct bijective substitution boxes from non-permutation power functions using heuristic techniques

FIG. 2.0 is a flowchart illustrating the further steps for the step of extending an image of
15 said Boolean map to generate an extended map.

FIG. 3.0 is a flowchart illustrating the further steps of the step of obtaining a bijective function from said extended image by utilizing Optimized Balanced Boolean Function
20 Maker algorithm.

Table 1.0 is a classification of currently available substitution boxes and substitution boxes constructed in the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a method for constructing bijective substitution box from non-permutation power functions using heuristic techniques. In particular, the present invention constructs substitution boxes by utilizing Optimize Balanced Boolean Function Maker algorithm which includes the heuristic technique in the algorithm.

Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

A substitution box (S-box) is one of the basic components of symmetric key cryptography. In general, s-box takes m input bits and transforms the said bits into n output bits. The said transformation is known as $m \times n$ s-box and is implemented as a look up table. These s-boxes are carefully chosen to resist linear cryptanalysis by having high nonlinearity. For differential analysis, an s-box is required to have low differential uniformity while high algebraic degree will provide an s-box that is resistance against higher order differential cryptanalysis.

Referring first to FIG. 1.0, the method to construct bijective substitution boxes from non-permutation power functions using heuristic techniques according to an embodiment of the invention is illustrated. The method (100) to construct bijective substitution boxes from non-permutation power functions using heuristic techniques comprising of first selecting a Boolean map from a plurality of linear power functions and high cryptographic properties power function (102, 104). Thereafter, an image of said Boolean map is extended to generate an extended map (106, 108) and a bijective function is obtained from said extended image by utilizing Optimized Balanced Boolean Function Maker algorithm (110). Cryptographic properties of substitution box are analyzed (112) by obtaining substitution box with highest nonlinearity and high algebraic degree by utilizing heuristic technique of Optimized Balanced Boolean Function Maker algorithm. The said steps are iterated until said cryptographic properties meets the predetermined condition of a cryptographically strong bijective substitution box. A set of high cryptographic properties power function is identified from finite field of $GF(2^8)$. The

said s-box construction in obtaining a bijective function from said extended image utilizes Optimized Balanced Boolean Function Maker algorithm wherein said bijective function is a result of the heuristic technique of said Optimized Balanced Boolean Function Maker algorithm. The said bijective function provides cryptographic properties with high
5 nonlinearity value and high algebraic value with highest nonlinearity value of 108 and highest algebraic degree of 7.

Turning to FIG. 2.0 which illustrates further steps of the step of extending an image of said Boolean map to generate an extended map (106, 108), a first power function is
10 identified from a plurality of power function which have high cryptographic properties (202). Thereafter, a plurality of non-bijective power functions is generated using a linear combination between a plurality of linear combination of power functions (204) and the number of non-existence elements in the plurality of non-bijective power functions (206) is identified. Subsequently, the plurality of non-bijective power functions which is less
15 than the pre-determined number of non-existence elements is selected (208). The said steps are iterated for all power functions which have high cryptographic properties from the plurality of power functions.

Turning to FIG. 3.0 which illustrates the further steps of obtaining a bijective function
20 from said extended image by utilizing Optimized Balanced Boolean Function Maker algorithm (110), Boolean function is first received from the extended Boolean map (302) and a frequency table is computed from said extended Boolean map (304) to determine if all frequencies in frequency table = 1 (306). It is confirmed that the Boolean function is balanced (308) if all frequencies in frequency table = 1. Otherwise, if it is confirmed that
25 all frequencies in said frequency table of Boolean function does not equate to 1, the process continues with further steps wherein elements which are not outputs of said extended Boolean map are identified (310) and further duplicate elements in extended Boolean map are identified using frequency table (310). Subsequently, distance matrix of all elements in step (304) and (310) are computed by comparing the bit error rate
30 between said elements (312). Upon computing the distance matrix, the smallest element in the said distance matrix is located (314) and all corresponding header and corresponding data of step (314) is listed (316). Further, all corresponding location of entry of elements from step (316) of Boolean map is located (318). Elements from step (316) are replaced with corresponding element in step (316) at location of step (318) to

- 10 -

calculate the non-linearity for temporary Boolean map (320). The said steps of (316), (318) and (320) are iterated for all corresponding elements from step (316) (322). The highest nonlinearity is identified from calculations computed in step (xi) (320) and the corresponding Boolean map is identified from the entry of step (322) and replacing said
5 original Boolean map with results obtained from step (324). All steps are iterated until said frequency table is free from plurality of header and data.

Table 1.0 provides a classification of currently available substitution boxes and substitution boxes constructed in the present invention

10

The present invention provides construct s-box which provide cryptographic properties with high nonlinearity value and high algebraic value with highest nonlinearity value of 108 and highest algebraic degree of 7 by utilizing heuristic technique in the algorithm of an Optimize Balanced Boolean Function Maker.

15

Throughout this specification, unless the context requires otherwise, the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated step or element or integer or group of steps or elements or integers, but not the exclusion of any other step or element or integer or group of steps,
20 elements or integers. Thus, in the context of this specification, the term "comprising" is used in an inclusive sense and thus should be understood as meaning "including principally, but not necessarily solely".

It will be appreciated that the foregoing description has been given by way of illustrative
25 example of the invention and that all such modifications and variations thereto as would be apparent to persons of skill in the art are deemed to fall within the broad scope and ambit of the invention as herein set forth.

CLAIMS

1. A method (100) to construct bijective substitution boxes from non-permutation power functions using heuristic techniques comprising steps of:

- 5 i. selecting a Boolean map from a plurality of linear power functions and high cryptographic properties power function (102, 104);
- ii. extending an image of said Boolean map to generate an extended map (106, 108);
- iii. obtaining a bijective function from said extended image by utilizing
10 Optimized Balanced Boolean Function Maker algorithm (110);
- iv. performing analysis on cryptographic properties of substitution box to obtain highest nonlinearity and high algebraic degree (112); and
- v. iterating steps (ii), (iii) and (iv) until said cryptographic properties meet predetermined condition of a cryptographically strong
15 bijective substitution box
 characterized in that
 obtaining a bijective function from said extended image by utilizing
 Optimized Balanced Boolean Function Maker algorithm (110);
 said bijective function is a result of heuristic technique of said
20 Optimized Balanced Boolean Function Maker algorithm; and said
 bijective function provides cryptographic properties with high
 nonlinearity value and high algebraic degree value.

2. A method (200) according to Claim 1, wherein extending an image of said
25 Boolean map to generate an extended map (106, 108) further comprising steps
 of:

- i. identifying a first power function from a plurality of power functions
 which have high cryptographic properties of power function (202);
- ii. generating a plurality of non-bijective power functions using a
30 linear combination between a plurality of linear combination of
 power functions (204);
- iii. identifying number of non-existence elements in the plurality of
 non-bijective power functions (206);

- 12 -

- iv. selecting the plurality of non-bijective power functions which is less than pre-determined number of non-existence elements (208); and
- v. iterating steps (i) –(iv) for all power functions which have high cryptographic properties from the plurality of power functions.

3. A method (300) according to Claim 1, wherein obtaining a bijective function from said extended image by utilizing Optimized Balanced Boolean Function Maker algorithm (110) further comprising steps of:

- i. receiving Boolean function from extended Boolean map (302);
- ii. computing frequency table from said extended Boolean map (304);
- iii. determining if all frequencies in frequency table = 1 (306);
If all frequencies in frequency table =1;
function is balanced (308) else
- iv. identifying elements which are not outputs of extended Boolean map (310);
- v. identifying duplicate elements in extended Boolean map using frequency table (310);
- vi. computing distance matrix of all elements in step (iv) and (v) by comparing bit error rate between said elements (312);
- vii. locating smallest element in distance matrix (314);
- viii. listing all corresponding header of step (vii) (316);
- ix. listing all corresponding data of step (vii) (316)
- x. locating all corresponding location of entry of elements from step (viii) of Boolean map (318);
- xi. replacing elements from step (ix) with corresponding element in step (viii) at location of step (x) and calculating non-linearity for temporary Boolean map (320);
- xii. iterating steps (ix), (x) and (xi) for all corresponding elements from step (viii) (322);
- xiii. identifying highest nonlinearity from calculations computed in step (xi) (324);

- 13 -

- xiv. identifying corresponding Boolean map from entry of step (xii) and replacing said original Boolean map with results obtained from step (xiii); and
- xv. iterating steps (i) to (xiv) until said frequency table is free from plurality of header and data.

5

4. A method (100) according to Claim 1, wherein a set of high cryptographic properties power function is identified from finite field of $GF(2^8)$.

10

5. A method (100) according to Claim 1, wherein highest nonlinearity value obtained using heuristic technique is 108.

6. A method (100) according to Claim 1, wherein highest algebraic degree obtained using heuristic technique is 7.

100

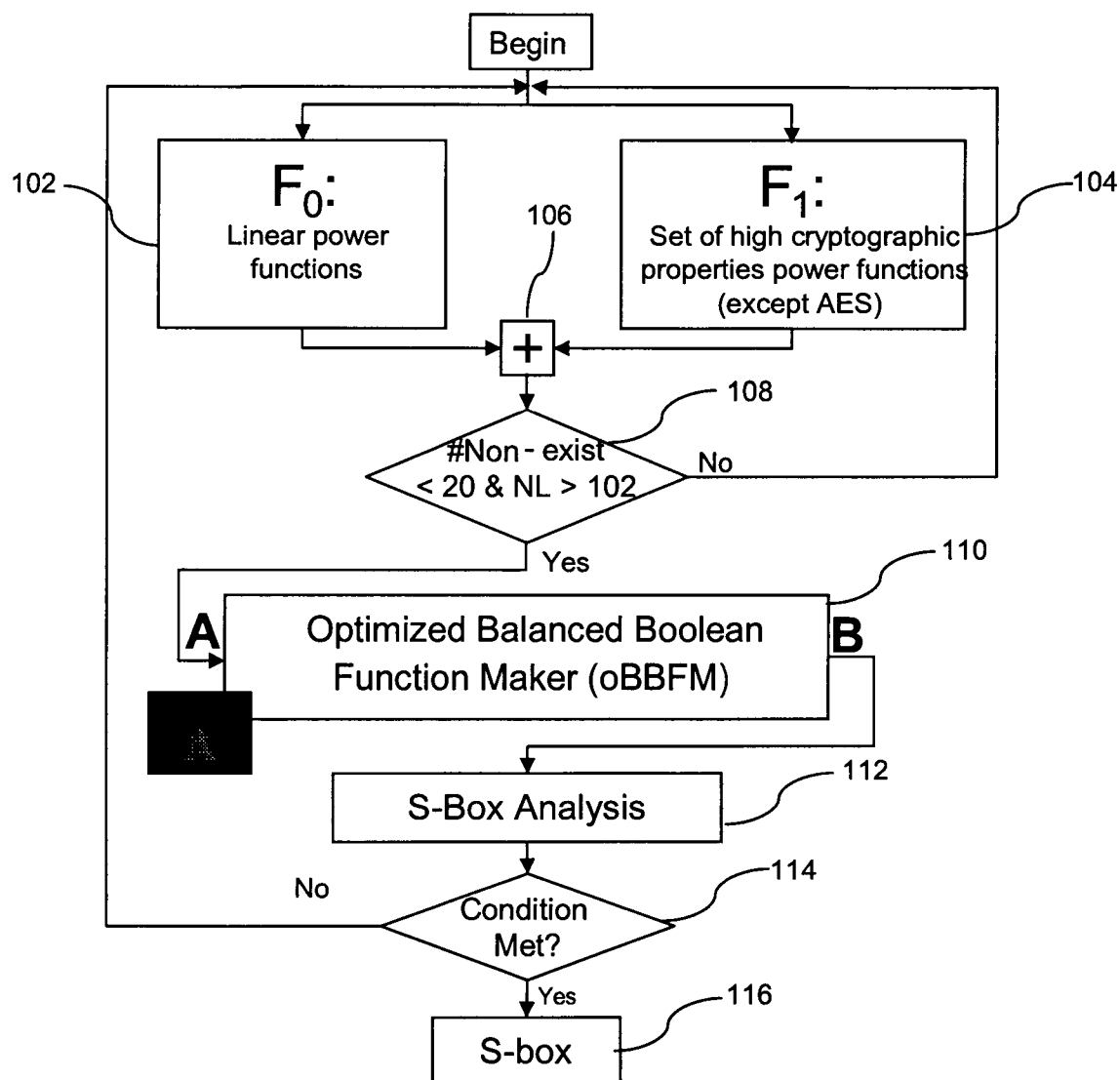


FIG. 1.0

200

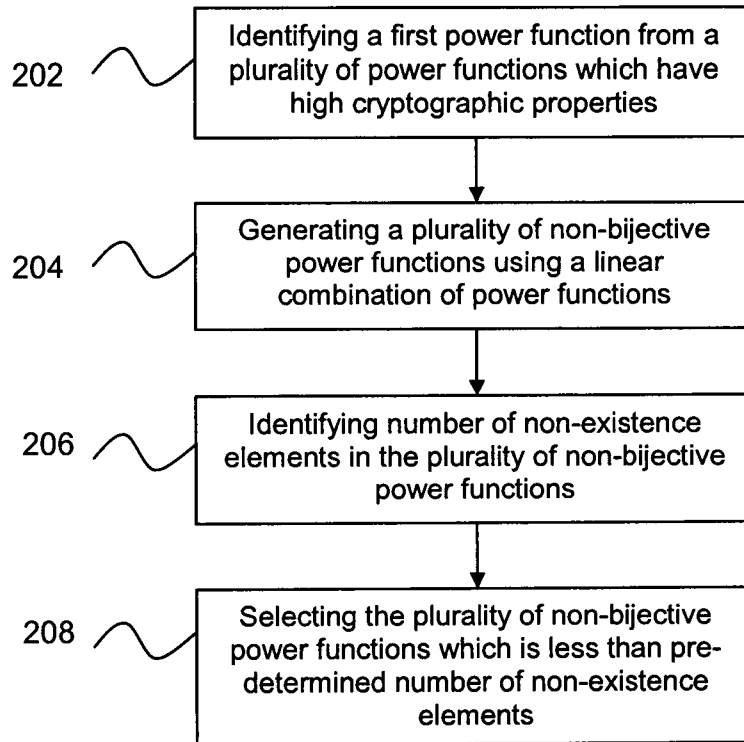


FIG. 2.0

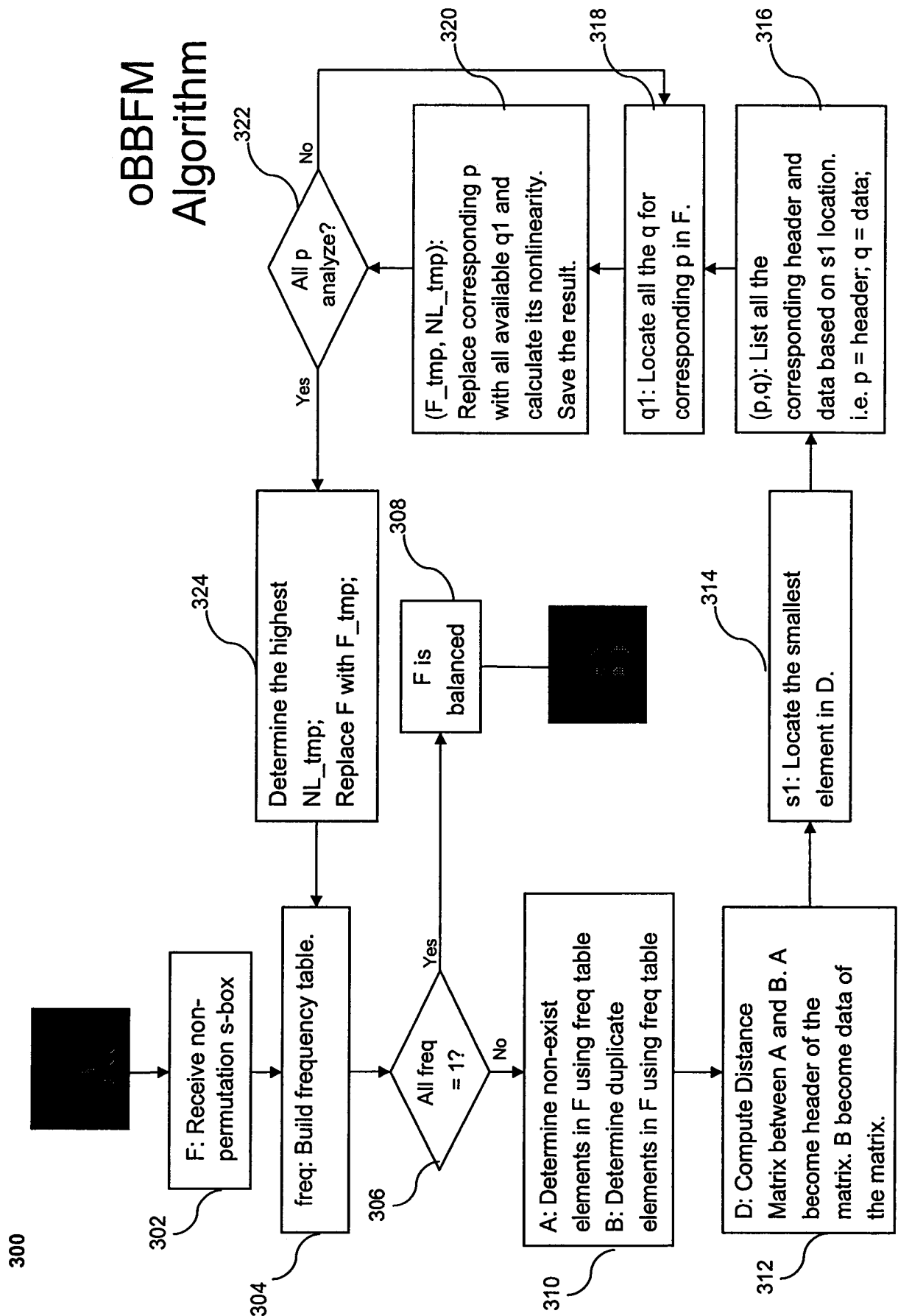


FIG. 3.0

Block Cipher	NL	DU	AD	LA	Fp	OFp	Design Techniques
AES	112	4	7	16	0	0	x^{-1} power functions
Camellia	112	4	7	16	0	0	
Aria	112	4	7	16	0	0	
Aria-2	112	4	7	16	0	1	
HyRAL	112	4	7	16	0	0	
Hierocrypt-HL	112	4	7	16	1	2	x^{-1} power functions
Hierocrypt-LL	106	6	7	22	0	0	Bit permutation
Clelia-S 0	100	10	6	28	0	2	Random
Clelia-S 1	112	4	7	16	0	1	x^{-1} power functions
Skipjack	100	12	7	28	0	0	Unknown
Khazad	96	8	7	32	0	0	Recursive Structure
Iceberg	96	8	7	32	0	4	Pseudo-Random Involution
Kamkar	96	10	7	32	0	1	Key-Dependent RNG
Fox	96	16	6	32	1	1	Pseudo-Random
Anubis	94	8	7	26	0	2	Pseudo-Random Involution
Our1	100	10	7	28	0	0	Fix Column + Random
Our2	102	8	7	26	0	0	NP Power Func. + BBFM
Our3	104	6	5	24	0	0	Binomial Power Functions
This Invention	108	10	7	20	0	0	Heuristic

Table 1.0

INTERNATIONAL SEARCH REPORT

International application No

PCT/MY2014/000160

A. CLASSIFICATION OF SUBJECT MATTER
 INV. G09C1/00 H04L9/06
 ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 G09C H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HERMAN ISA ET AL: "S-box construction from non-permutation power functions", SECURITY OF INFORMATION AND NETWORKS, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA, 26 November 2013 (2013-11-26), pages 46-53, XP058035918, DOI: 10.1145/2523514.2523525 ISBN: 978-1-4503-2498-4 sections 1, 3.1, 3.2.1 ----- -/--	1-3



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

8 December 2014

Date of mailing of the international search report

15/12/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Manet, Pascal

INTERNATIONAL SEARCH REPORT

International application No

PCT/MY2014/000160

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ABDURASHID MAMADOLIMOV ET AL: "PRACTICAL BIJECTIVE S-BOX DESIGN", PROCEEDINGS OF THE 5TH ASIAN MATHEMATICAL CONFERENCE,, 1 January 2009 (2009-01-01), pages 584-587, XP007922592, cited in the application section 5	1
X	----- WO 2010/151103 A1 (MIMOS BERHAD [MY]; ABDURASHID MAMADOLIMOV [MY]; HERMAN ISA [MY]; MOESF) 29 December 2010 (2010-12-29) page 4 - page 7; claims 1,2 -----	1,2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/MY2014/000160

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010151103 A1	29-12-2010	MY 144134 A WO 2010151103 A1	10-08-2011 29-12-2010
