



(51) International Patent Classification:

H04L 9/28 (2006.01) **G09C 5/00** (2006.01)
H04L 9/06 (2006.01) **H04L 9/14** (2006.01)

(21) International Application Number:

PCT/MY2010/000101

(22) International Filing Date:

15 June 2010 (15.06.2010)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

PI 20092626 22 June 2009 (22.06.2009) MY

(71) Applicant (for all designated States except US): **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ABDURASHID MAMADOLIMOV** [UZ/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **HERMAN ISA** [MY/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOESFA SOEHEILA MOHAMAD** [MY/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **MIRANDAH, Patrick**; Patrick Mirandah Co. (Malaysia) Sdn Bhd, Suite 3B-19-3 Plaza Sentral, 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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

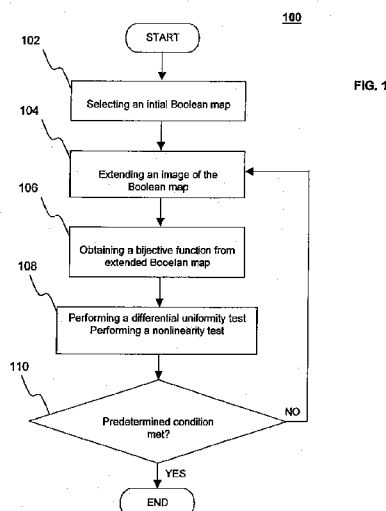
Declarations under Rule 4.17:

— as to the identity of the inventor (Rule 4.17(i))

Published:

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

(54) Title: BIJECTIVE SUBSTITUTION BOX



(57) Abstract: A method (100) for generating a bijective Substitution Box, the method (100) comprises selecting a Boolean map (102) from a plurality of non-bijective power functions and iterating extending an image of the Boolean map (104) to generate an extended Boolean map, obtaining a bijective function (106) from the extended Boolean map, performing a differential uniformity test (108) on the bijective function to obtain a differential uniformity parameter and performing a nonlinearity test (108) on the bijective function to obtain a nonlinearity parameter, until the differential uniformity parameter and the nonlinearity parameter meet a predetermined condition.

BIJECTIVE SUBSTITUTION BOX

FIELD OF INVENTION

- 5 The present invention relates to a method of generating a bijective Substitution Boxes (S-Boxes).

BACKGROUND ART

- 10 S-Boxes are vectorial Boolean functions satisfying some cryptographic criteria. S-Boxes are used as basic component of block ciphers in Cryptography. An important condition on S-Boxes is a high resistance to the differential and linear cryptanalysis, which are the main attacks on block ciphers. The functions with low differential uniformity and high nonlinearity possess a good resistance to the differential and linear attacks and they are
- 15 considered as cryptographically strong. The ciphers that are Substitution-permutation networks use bijective S-Boxes.

- For practical use, 8×8 size is optimal. S-Boxes with 8×8 size can be considered as strong if they have differential uniformity of at most 10 and nonlinearity of at least 100. It
- 20 has to be noted that the best known pair of these parameters is 4 and 112, respectively, and S-Boxes with differential uniformity below 10 and nonlinearity above 100 are very rare.

- Several methods to generate cryptographically strong S-Boxes exist, such as random
- 25 generation, the use of finite field operations, as well as heuristic algorithms.

SUMMARY OF INVENTION

In one embodiment of the present invention is a method of generating a bijective Substitution Boxes. The method comprises selecting an initial Boolean map from a plurality of non-bijective power functions over the finite field, extending image of initial map, without changing differential uniformity and nonlinearity, obtaining bijective function from extended function, with small aggravation of differential uniformity and nonlinearity and performing differential uniformity and nonlinearity tests on the bijective function, until the differential uniformity and nonlinearity parameters meet a predetermined condition.

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.

15

BRIEF DESCRIPTION OF THE 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 illustrates a flowchart of a method for generating a bijective Substitution Box (S-Box).

FIG.2 illustrates a flowchart of extending an image of a Boolean map to generate an extended Boolean map.

15

FIG. 3 illustrates a flowchart of obtaining a bijective function from an extended Boolean map.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a method for generating a bijective Substitution Box (S-Box). Hereinafter, this specification will describe the present invention according to the preferred embodiments of the present invention. However, 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 that those skilled in the art may devise various modifications and equivalents without departing from the scope of the appended claims.

10

The method for generating the bijective S-Box according to the embodiments of the present invention relates to generating a cryptographically strong S-Box. The method of generating cryptographically strong S-Boxes of the present invention comprises generating bijective $n \times n$ size S-Boxes using non-bijective power functions in the finite field. The $n \times n$ size S-Boxes of the present invention have good differential uniformity and nonlinearity parameters and are not equivalent to any known S-Boxes.

15

Reference is being made to FIG. 1. FIG. 1 illustrates a flowchart of the method (100) for generating the bijective S-Box. The method (100) for generating the bijective S-Box comprises selecting an initial Boolean map (102) from a plurality of non-bijective power functions over the finite field; extending image of initial Boolean map (104), without changing differential uniformity and nonlinearity, obtaining bijective function (106) from extended function, with small aggravation of differential uniformity and nonlinearity and performing differential uniformity and nonlinearity tests (108) on the bijective function, until the differential uniformity and nonlinearity parameters meet a predetermined condition.

20
25

The method (100) of generating the bijective S-Boxes according to the present invention begins with selecting the Boolean map (102) from a plurality of non-bijective power functions over the finite field. In one embodiment of the present invention, where F_{2^n} is a finite field of 2^n elements, $x \rightarrow x^d$ power functions are considered, where $x \in F_{2^n}$ and d is a positive integer.

It is well known some power functions with lowest DU or highest NL. For practical use we limit oneself the case $n=8$. S-Boxes with 8×8 size can be considered as strong if they have $DU \leq 10$ and $NL \geq 100$. The only 8 bijective power functions (permutations) satisfy above mentioned condition. They are $x^{127}, x^{254}, x^{253}, x^{251}, x^{247}, x^{239}, x^{223}, x^{191}$. All these functions are cyclomatic cosets, i.e., they are equivalent functions. Therefore there is only one strong bijective power function up to equivalence.

It is considered strong non-bijective power functions. There are 24 non-bijective power functions with best parameters $(DU, NL)=(2,112)$. They include 3 non-equivalence classes: (3, 6, 12, 24, 48, 96, 192, 129), (9, 18, 36, 72, 144, 33, 66, 132) and (39, 78, 156, 57, 114, 228, 201, 147). It can be chosen any representative of these functions for next using. It is chosen first function of first class, i.e., the function x^3 .

Upon selecting the Boolean map, the image of the selected Boolean map is extended (104) to generate an extended Boolean map

Reference is now being made to FIG. 2. FIG. 2 illustrates a flowchart of extending the image of the Boolean map to generate the extended Boolean map.

According to the embodiments of the present invention, the Boolean map is extended by identifying a first linear power function (202) from a plurality of linear power functions, generating binomial function (204) by adding initial Boolean map multiplied a constant alpha to a chosen linear power function multiplied by a constant beta and identifying
 5 binomial function (206) with a maximum number of image elements.

The steps generating binomial function (204) by adding initial Boolean map multiplied a constant alpha to a chosen linear power function multiplied by a constant beta and identifying binomial function (206) with a maximum number of image elements are
 10 iterated for all linear combinations from the plurality of linear combinations.

The steps identifying a first linear power function (202) from a plurality of linear power functions, generating binomial function (204) by adding initial Boolean map multiplied a constant alpha to a chosen linear power function multiplied by a constant beta and
 15 identifying binomial function (206) with a maximum number of image elements are iterated for all linear power functions from the plurality of linear power functions.

The power function x^3 has $(DU, NL) = (2, 112)$ and is a non-bijective function. If I is image of the power function x^3 , then $|I| = 86$. When power function x^3 is considered
 20 as a mapping of $F_{2^s}^* \rightarrow F_{2^s}^*$, wherein $F_{2^s}^* = F_{2^s} \setminus \{(0,0,\dots,0)\}$, then the power function x^3 appears as a three to one function. In order to obtain strong bijective functions from the power function x^3 , function $\alpha \cdot x^3 + \beta \cdot x^4$ is considered, wherein $\alpha, \beta \in F_{2^s}$. Due to the fact that power function x^4 is linear, hence $DU(x^3) = DU(\alpha \cdot x^3 + \beta \cdot x^4)$ and $NL(x^3) = NL(\alpha \cdot x^3 + \beta \cdot x^4)$. If J is image of $\alpha \cdot x^3 + \beta \cdot x^4$, then $I \subset J$ and $|J| = 192$.

With this, the power function x^3 almost resembles a bijective function without compromising the differential uniformity parameter and the nonlinearity parameter.

Upon extending the image of the Boolean map, the bijective function is obtained from
5 the extended Boolean map. Reference is now being made to FIG. 3. FIG. 3 illustrates a flowchart of obtaining the bijective function from the extended Boolean map.

According to the embodiments of the present invention, obtaining the bijective function comprises identifying a first duplicate output element (302) of the output list of function,
10 selecting a first element (304) which is not in the output list of the function and has least distance from the identified duplicate output element and replacing the first duplicate output element with the selected first element (306). The steps of identifying the first duplicate output element (302), selecting the first element (304) and replacing the first duplicate output element with the selected first element (306) are iterated until the
15 Boolean map is free from a plurality duplicate output elements.

According to the embodiments of the present invention, the bijective function obtained is subjected to differential uniformity test (108) to obtain the differential uniformity parameter and nonlinearity test (108) to obtain the nonlinearity parameter. The steps of
20 extending the image of the Boolean map (104), obtaining a bijective function (106) and performing the uniformity test and nonlinearity test (108) are iterated until the differential uniformity parameter and the nonlinearity parameter meet the predetermined condition of DU less than or equal to 10 and NL more than or equal to 100.

According to the embodiments of the present invention, performing the differential uniformity test on the bijective function comprises introducing all possible changes to an input and comparing an output to an original output, counting a number of the inputs which produce the same output difference for any given input change and identifying a maximum number of the counts to determine the differential uniformity parameter of the bijective function.

According to the embodiments of the present invention, performing the nonlinearity test on the bijective function comprises generating all non-trivial linear combinations of a plurality of component functions, generating all affine functions with the same number variables as a given function, counting a Hamming distance between pairs of linear combination and affine functions and identifying a minimum number of the counts to determine the nonlinearity parameter of the bijective function.

CLAIMS

1. A method (100) for generating a bijective Substitution Box, the method (100) comprises
 - 5 (i) selecting a Boolean map (102) from a plurality of non-bijective power functions;
 - (ii) extending an image of the Boolean map (104) to generate an extended Boolean map;
 - (iii) obtaining a bijective function (106) from the extended Boolean map;
 - 10 (iv) performing a differential uniformity test (108) on the bijective function to obtain a differential uniformity parameter;
 - (v) performing a nonlinearity test (108) on the bijective function to obtain a nonlinearity parameter; and
 - (vi) iterating steps (ii), (iii), (iv) and (v) until the differential uniformity
15 parameter and the nonlinearity parameter meet a predetermined condition.
2. The method (100) according to claim 1, wherein extending the image of the Boolean map to generate the extended Boolean map further comprises
 - 20 (i) identifying a first linear power function (202) from a plurality of linear power functions;
 - (ii) generating the plurality of non-bijective power functions (204) using a linear combination from a plurality of linear combinations of the power function and the plurality of linear power functions;

- (iii) identifying at least one non-bijective power function from the plurality of non-bijective power functions with a maximum number of image elements (206);
 - (iv) iterating steps (ii) and (iii) for all linear combinations from the plurality of linear combinations; and
 - (v) iterating steps (i), (ii) and (iii) for all linear power functions from the plurality of linear power functions.
3. The method (100) according to claim 1, wherein obtaining the bijective function from the extended Boolean map further comprises
- (i) identifying a first duplicate output element (302) in the Boolean map;
 - (ii) selecting a first element (304) which is not an output in the Boolean map and has a least distance from the first duplicate output element;
 - (iii) replacing the first duplicate output element with the first element (306);
 - (iv) iterating steps (i), (ii) and (iii) until the Boolean map is free from a plurality duplicate output elements.
4. The method according to claim 1, wherein the performing the differential uniformity test on the bijective function further comprises
- introducing all possible changes to an input and comparing an output to an original output;
 - counting a number of the inputs which produce the same output difference for any given input change; and
 - identifying a maximum number of the counts to determine the differential uniformity parameter of the bijective function.

5. The method according to claim 1, wherein the performing the nonlinearity test on the bijective function further comprises

generating all non-trivial linear combinations of a plurality of component functions;

5 generating all affine functions with the same number variables as a given function;

counting a Hamming distance between pairs of linear combination and affine functions; and

10 identifying a minimum number of the counts to determine the nonlinearity parameter of the bijective function.

1/3

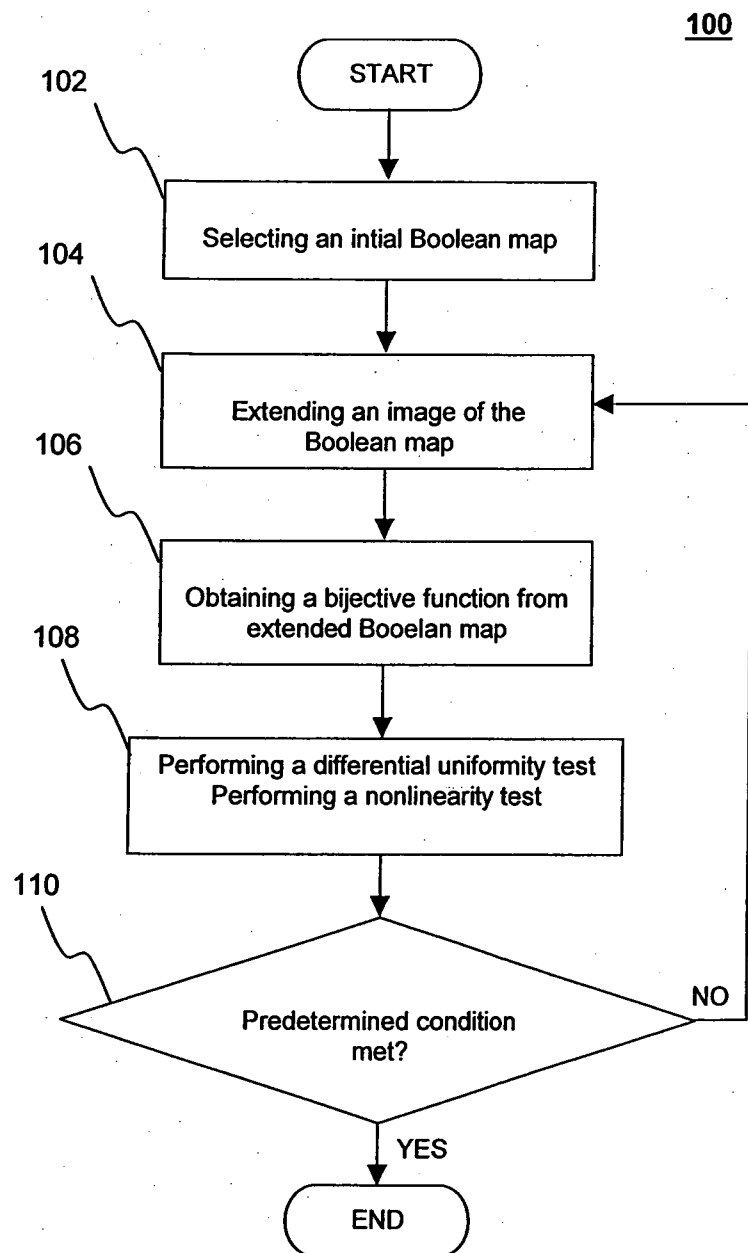


FIG. 1

2/3

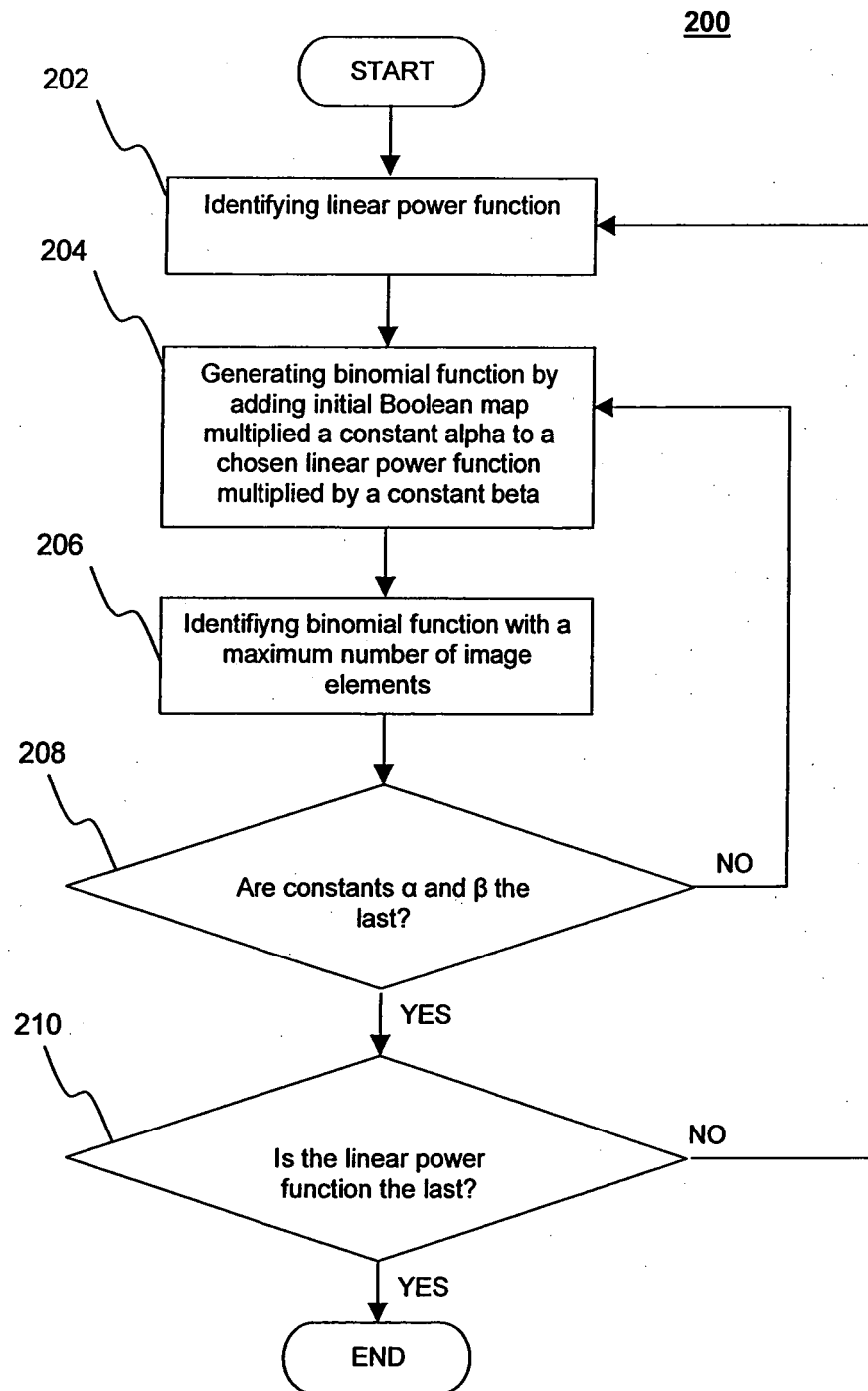


FIG. 2

3/3

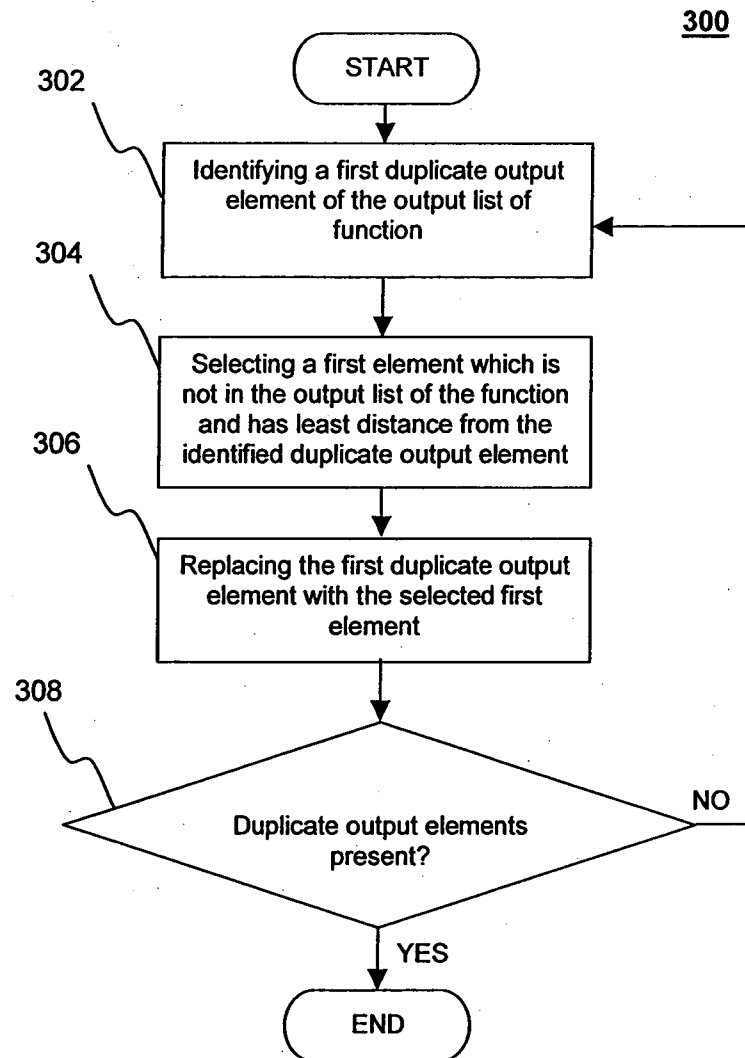


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/MY2010/000101

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/28 (2006.01)

H04L 9/06 (2006.01)

G09C 5/00 (2006.01)

H04L 9/14 (2006.01)

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)

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)

EPODOC, WPI, INSPEC, ESPACE, TXTEN, GOOGLE PATENTS and SCHOLAR with Cryptography, Substitution Box, Non-linearity, Differential, Bijective, Power Function and similar keywords.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KIM, K. et al., "A Recursive Construction Method of S-boxes Satisfying Strict Avalanche Criterion", Advances in Cryptology - CRYPTO '90, Lecture Notes in Computer Science, Edited by: Menezes, A. J. et al., Volume 537, 1991. See Whole Document	
A	Burnett, Linda, "Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography", Thesis Submitted for Degree of Doctor of Philosophy, Queensland University of Technology, 2005 [retrieved on 2 September 2010]. Retrieved from the Internet <URL: http://eprints.qut.edu.au/16023/ > See Whole Document	
A	US 6 804 355 B1 (GRAUNKE) 12 October 2004 See Whole Document	
A	US 6 064 738 A (FRIDRICH) 16 May 2000 See Whole Document	

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

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
06 September 2010Date of mailing of the international search report
13 SEP 2010Name and mailing address of the ISA/AU
AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No. +61 2 6283 7999Authorized officer
PRASHANT SURYANARAYANAN
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : +61 2 6225 6144

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2010/000101

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member
US	6804355	NONE
US	6064738	NONE
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.		
END OF ANNEX		