(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 2 月 20 日 (20.02.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/026451 A1

(51) 国际专利分类号:
G06F 7/72 (2006.01)

(21) 国际申请号: PCT/CN2012/085948

(22) 国际申请日: 2012 年 12 月 5 日 (05.12.2012)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210275733.7 2012 年 8 月 3 日 (03.08.2012) CN

(71) 申请人: 华南理工大学 (SOUTH CHINA UNIVERSITY OF TECHNOLOGY) [CN/CN]; 中国广东省广州市天河区五山路 381 号, Guangdong 510640 (CN)。

(72) 发明人: 唐韶华 (TANG, Shaohua); 中国广东省广州市天河区五山路 381 号, Guangdong 510640 (CN)。
易海博 (YI, Haibo); 中国广东省广州市天河区五山路 381 号, Guangdong 510640 (CN)。

(74) 代理人: 广州市华学知识产权代理有限公司 (GUANGZHOU HUAXUE INTELLECTUAL PROPERTY AGENCY CO., LTD); 中国广东省广州市天河区五山路 381 号华南理工大学教学二区 8 号物资大楼首层, Guangdong 510640 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (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, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) Title: GALOIS FIELD INVERSION DEVICE

(54) 发明名称 : 一种有限域求逆器

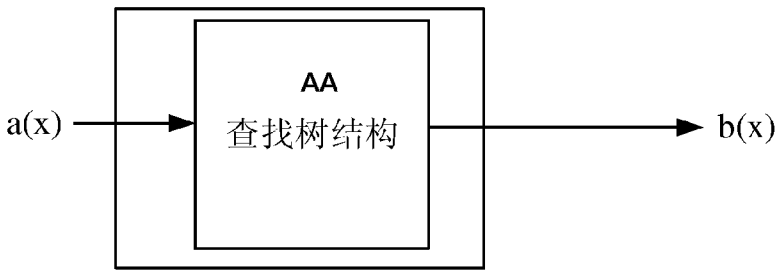

图 1 / FIG.1

AA Search tree structure

(57) Abstract: Disclosed is a Galois field inversion device, comprising an input port, an output port and a search tree inversion unit for executing inversion operation of an operation number a(x) on a Galois field GF (2^n) based on a search tree structure, the search tree inversion unit being provided with a left search tree and a right search tree. Each of the left search tree and the right search tree comprises tree nodes for processing the inversion operation of the GF (2^n) and a connecting line between the tree nodes. Each tree node comprises a root node, an inner node and a leaf node. Each path from the root node to one leaf node represents one element on the GF (2^n). The connecting line between the tree nodes represents that the path for representing the operation number a(x) is connected to a path of an inversion result b(x). According to the present invention, the inversion operation of the elements on the GF is realized by using the search tree inversion unit; compared with an existing GF inversion device, the inversion operation on the GF (2^n) is more efficient.

(57) 摘要:

[见续页]

WO 2014/026451 A1

本发明公开了一种有限域求逆器，包括输入端口、输出端口和用于执行运算数 a(x)在有限域 GF(2^n)上基于查找树结构的求逆运算的查找树求逆单元；查找树求逆单元设有左查找树和右查找树；左查找树和右查找树均包括用于处理有限域 GF(2^n)上的求逆运算的树节点和树节点之间的连线，树节点包括根节点、内部节点和叶子节点，每一条从根节点到一个叶子节点的路径表示有限域 GF(2^n)上的一个元素；所述树节点之间的连线将表示运算数 a(x)的路径与表示求逆结果 b(x)的路径连接起来。本发明通过查找树求逆单元实现了有限域上的元素的求逆运算，在计算有限域 GF(2^n)上的求逆运算时相对于现有的有限域求逆器更为高效。

一种有限域求逆器

技术领域

本发明涉及一种对有限域的元素进行求逆的装置。

背景技术

有限域是仅含有限多个元素的域，广泛地运用于各种工程领域。目前，有限域的求逆运算大致可以分为四类：基于费马定理的求逆运算，基于扩展欧几里德定理的求逆运算，基于蒙哥马利算法的求逆运算和基于查找表技术的求逆运算。

有限域的各类运算被有效地运用于各种密码应用和编码技术中。有效的有限域的求逆运算的设计，对于密码算法的实现，起着至关重要的作用。现有技术中存在的多种公知的有限域的求逆器，包括软件求逆器和硬件求逆器，均存在着不足之处，例如性能指标达不到高速度、小面积和低功耗的要求。

发明内容

为了克服现有技术的不足，本发明的目的在于提供一种有限域求逆器，利用查找树结构对有限域的元素进行求逆，在计算有限域 $GF(2^n)$ 上的求逆运算时相对于现有的有限域求逆器更为高效，具有高速度、小面积和低功耗的特点。

本发明的目的通过以下技术方案实现：一种有限域求逆器，包括：

输入端口，用于输入运算数 $a(x)$；

查找树求逆单元，用于执行运算数 $a(x)$ 在有限域 $GF(2^n)$ 上基于查找树结构的求逆运算；

输出端口，用于输出运算数 $a(x)$ 的求逆结果 $b(x)$；

所述查找树求逆单元设有左查找树和右查找树；左查找树和右查找树均包括用于处理有限域 $GF(2^n)$ 上的求逆运算的树节点和树节点之间的连线，树节点包括根节点、内部节点和叶子节点，每一条从根

节点到一个叶子节点的路径表示有限域$GF(2^n)$上的一个元素；所述树节点之间的连线将表示运算数$a(x)$的路径与表示求逆结果$b(x)$的路径连接起来。

所述查找树求逆单元中，运算数$a(x)$由根节点到一个叶子节点n_1的路径表示，求逆结果$b(x)$由根节点到一个叶子节点n_2的路径表示，所述连线设置在叶子节点n_1和叶子节点n_2之间。

所述查找树求逆单元中，树节点包括*NXOR*逻辑门、*AND*逻辑门以及数据选择器MUX；*NXOR*逻辑门的一个输入为运算数$a(x)$的比特数值，另一个输入为i_2； *AND*逻辑门的一个输入为i_0，另外一个输入为*NXOR*逻辑门的输出；数据选择器MUX设有数据输入i_2、来自其孩子节点的选通输入i_3、求逆输出o_2及传输给其父节点的输出o_3；当树节点为根节点时，i_0为 1；当树节点为内部节点或叶子节点，且为左孩子节点时，$i_2=0$；当树节点为内部节点或叶子节点，且为右孩子节点时，$i_2=1$；当树节点为根节点或内部节点时，*AND*逻辑门将逻辑与运算结果输出给其孩子节点；当树节点为叶子节点时，*AND*逻辑门将逻辑与运算结果输出给与其连接的叶子节点；左查找树的根节点$i_2=0$，右查找树的根节点$i_2=1$。

所述运算数$a(x)$和求逆结果$b(x)$具有如下形式：

$a(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+...+a_0$；

$b(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+...+b_0$。

与现有技术相比，本发明具有以下优点和技术效果：

本发明通过查找树的结构实现了有限域的求逆运算，在计算$GF(2^n)$上的求逆运算上相对于现有的有限域求逆器有着明显的高速度、小面积及低功耗的优势，并可以广泛运用于各种工程领域，特别是密码算法的硬件实现和各种数学问题的求解中。

附图说明

图 1 为本发明的实施例的有限域求逆器的结构示意图。

图 2 为本发明的实施例的查找树求逆单元的结构示意图。

图 3 为本发明的实施例的各类树节点的结构示意图。

图 4 为本发明的实施例的查找树求逆单元用于查找所需求逆的

有限域元素的结构示意图。

图 5 为本发明的实施例的查找树求逆单元用于查找有限域元素的逆的结构示意图。

具体实施方式

下面结合实施例及附图，对本发明作进一步地详细说明，但本发明的实施方式不限于此。

实施例

如图 1 所示，本发明的有限域求逆器包括输入端口、输出端口和查找树单元。

下面分别对本发明的求逆器的各组成部分做详细介绍：

（1）输入端口：如图 1 所示，本发明的实施例的求逆器的输入端口用于输入运算数 $a(x)$ 。

$a(x)$ 可以表示为以下形式：

$a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_0$ 。

其中 $a_{n-1}, a_{n-2}, ..., a_0$ 均是 $GF(2)$ 上的元素。

（2）输出端口：如图 1 所示，输出端口用于输出求解有限域元素 $a(x)$ 的逆 $b(x)$ 。

$b(x)$ 可以表示为以下形式：

$b(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_0$ 。

其中 $b_{n-1}, b_{n-2}, ..., b_0$ 均是 $GF(2)$ 上的元素。

（3）查找树单元：查找树单元作为求逆器的主要的部件，是本发明的核心部件，包括多个树节点以及节点之间的连线等。

如图 2 所示，所有树节点除了叶子节点均有左孩子节点和右孩子节点，左孩子节点的数值为 0，右孩子节点的数值为 1。每一条从根节点到一个叶子节点的路径代表一个有限域 $GF(2^n)$ 上的元素。如果一个有限域 $GF(2^n)$ 上的元素 $a(x)$ 是由根节点到一个叶子节点 n_1 的路径表示，并且 $a(x)$ 的逆是由根节点到一个叶子节点 n_2 的路径表示，那么叶子节点 n_1 和叶子节点 n_2 之间有一条连线。

如图 3 所示，查找树结构的树节点包括三类树节点，图 3（1）、

图 3（2）、图 3（3）分别是根节点、内部节点和叶子节点。三类树节点的内部电路都是一样的，均包括两个逻辑门，即 *NXOR* 和 *AND* 逻辑门，以及数据选择器 MUX。

i_1 和 i_2 是 *NXOR* 的两个输入，$i_1 = a_i, i_2 = 0/1$；*AND* 的一个输入 i_0 是来自其父亲节点的输出，另一个输入是 *NXOR* 的输出；$o_1 = o_2$ 是 *AND* 的输出，直接输出到此节点的左右孩子节点。如果树节点是左孩子节点，那么 *NXOR* 的两个输入分别是 a_i 和 0；否则，*NXOR* 的两个输入分别是 a_i 和 1。根据如图 3 所示，有如下逻辑表示，$o_0 = (NOT(i_1\ XOR\ i_2))\ AND\ i_0$，$o_1 = (NOT(i_1\ XOR\ i_2))\ AND\ i_0$。

三类树节点所不同的是输入输出端口。例如，在根节点中，$i_0 = 1, i_1 = a_{n-1}, i_2 = 0/1$，$a_{n-1}$ 是有限域元素 $a(x)$ 的第 $n-1$ 个比特的数值，*NXOR* 逻辑门将 $a(x)$ 的第 $n-1$ 个比特的数值 a_{n-1} 与另一输入 i_2 进行逻辑运算后，将运算结果输入到 *AND* 逻辑门的一个输入端，*AND* 逻辑门将所述运算结果与 1 进行逻辑与运算后，将逻辑与运算结果分别输出给根节点的左孩子和右孩子；在内部节点中，$i_1 = a_i, i_2 = 0/1$，a_i 是有限域元素 $a(x)$ 的第 i 个比特的数值，*NXOR* 逻辑门将 $a(x)$ 的第 i 个比特的数值 a_i 与另一输入 i_2 进行逻辑运算后，将运算结果输入到 *AND* 逻辑门的一个输入端，*AND* 逻辑门将所述运算结果与来自该内部节点的父节点的输出 i_0 进行逻辑与运算后，将逻辑与运算结果分别输出给该内部节点的左孩子和右孩子；在叶子节点中，$i_1 = a_0, i_2 = 0/1$，a_0 是有限域元素 $a(x)$ 的第 0 个比特的数值，*NXOR* 逻辑门将 $a(x)$ 的第 0 个比特的数值 a_0 与另一输入 i_2 进行逻辑运算后，将运算结果输入到 *AND* 逻辑门的一个输入端，*AND* 逻辑门将所述运算结果与来自该叶子节点的父节点的输出 i_0 进行逻辑与运算后，将逻辑与运算结果输出给与其相连接的叶子节点。当树节点是左孩子节点时，$i_2 = 0$；当树节点是右孩子节点时，$i_2 = 1$。本发明包括左查找树和右查找树两棵查找树，左查找树的根节点 $i_2 = 0$，右查找树的根节点 $i_2 = 1$。

数据选择器 MUX 定义如下：i_2 是数据输入和 i_3 是选通输入，i_3 是来自此节点的孩子节点的输入；o_2 和 o_3 是输出，o_2 是输出到求逆器的

输出端口，即$b(x)$的一部分，o_3输出到此节点的父亲节点。有$o_3=i_3$；而且仅当$i_3=1$时，$o_2=i_2$，即当来自该节点的孩子节点的输出为 1 时，求逆器在该节点的输出结果为*NXOR*逻辑门的输入i_2。

下面以$n=4$为例说明本发明的求逆器的工作过程。

首先，如图 4 所示，找出哪一条路径代表需要求逆的有限域元素$a(x)$。

假设需要求逆的元素$a(x)=x$，二进制表示形式即$(0010)_2$。由于$a_{n-1}=n_1=1$，所以n_1节点在正确的路径上，*AND*逻辑门输出的值为 1 并送到左、右孩子节点中。在n_2节点中，由于$i_1=0,i_2=0,i_0=1$，所以*AND*逻辑门输出为 1，并送到左、右孩子节点中，即n_2节点也在正确的路径上。用同样的方法可以得到n_3节点和n_4节点均在正确的路径上，所以路径n_1到n_4即代表$(0010)_2$，也就是$a(x)$。由于n_4节点连着n_5节点，所以n_4节点的*AND*逻辑门输出送到n_5节点。即$a(x)$存在有限域上的逆。

其次，如图 5 所示，找出哪一条路径代表需要求逆的有限域元素$a(x)$的逆$b(x)$。

由于n_4节点连着n_5节点，所以n_4节点的输出数值 1，送到n_5节点。n_5节点可以直接把数值 1 传输到其父亲节点n_6节点，以及祖先节点n_7节点和n_8节点。同时，n_5节点、n_6节点、n_7节点和n_8节点把内部的数值（即*NXOR*逻辑门的输入i_2）输出到输出端口，即$b(x)$。所以，$b(x)$即是$a(x)$的逆。

上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受所述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，均应为等效的置换方式，都包含在本发明的保护范围之内。

权 利 要 求 书

1、一种有限域求逆器，其特征在于，包括：

输入端口，用于输入运算数$a(x)$；

查找树求逆单元，用于执行运算数$a(x)$在有限域$GF(2^n)$上基于查找树结构的求逆运算；

输出端口，用于输出运算数$a(x)$的求逆结果$b(x)$；

所述查找树求逆单元设有左查找树和右查找树；左查找树和右查找树均包括用于处理有限域$GF(2^n)$上的求逆运算的树节点和树节点之间的连线，树节点包括根节点、内部节点和叶子节点，每一条从根节点到一个叶子节点的路径表示有限域$GF(2^n)$上的一个元素；所述树节点之间的连线将表示运算数$a(x)$的路径与表示求逆结果$b(x)$的路径连接起来。

2、根据权利要求 1 所述的有限域求逆器，其特征在于，所述查找树求逆单元中，运算数$a(x)$由根节点到一个叶子节点n_1的路径表示，求逆结果$b(x)$由根节点到一个叶子节点n_2的路径表示，所述连线设置在叶子节点n_1和叶子节点n_2之间。

3、根据权利要求 1 所述的有限域求逆器，其特征在于，所述根节点和内部节点均有左孩子节点和右孩子节点，左孩子节点的数值为 0，右孩子节点的数值为 1。

4、根据权利要求 2 所述的有限域求逆器，其特征在于，所述查找树求逆单元的树节点采用逻辑门电路实现。

5、根据权利要求 4 所述的有限域求逆器，其特征在于，所述查找树求逆单元中，树节点包括 *NXOR* 逻辑门、*AND* 逻辑门以及数据选择器 MUX；*NXOR* 逻辑门的一个输入为运算数$a(x)$的比特数值，另一个输入为i_2；*AND* 逻辑门的一个输入为i_0，另外一个输入为 *NXOR* 逻辑门的输出；数据选择器 MUX 设有数据输入i_2、来自其孩子节点的选通输入i_3、求逆输出o_2及传输给其父节点的输出o_3；当树节点为根节点时，i_0为 1；当树节点为内部节点或叶子节点，且为左孩子节点时，$i_2=0$；当树节点为内部节点或叶子节点，且为右孩子节点时，$i_2=1$；

当树节点为根节点或内部节点时，*AND*逻辑门将逻辑与运算结果输出给其孩子节点；当树节点为叶子节点时，*AND*逻辑门将逻辑与运算结果输出给与其连接的叶子节点；左查找树的根节点$i_2=0$，右查找树的根节点$i_2=1$。

6、根据权利要求 1 所述的有限域求逆器，其特征在于，所述运算数$a(x)$和运算数$b(x)$具有如下形式：

$a(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+...+a_0$；

$b(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+...+b_0$。

WO 2014/026451 PCT/CN2012/085948

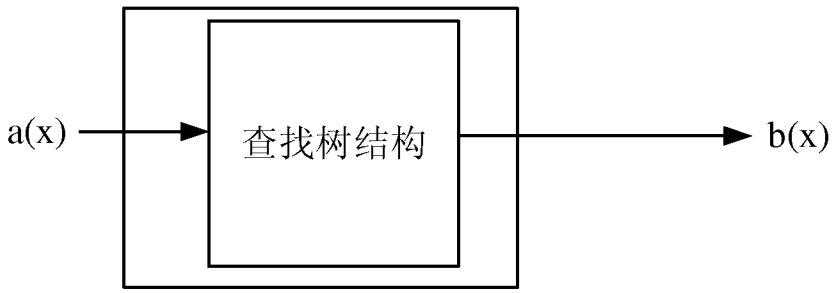

图 1

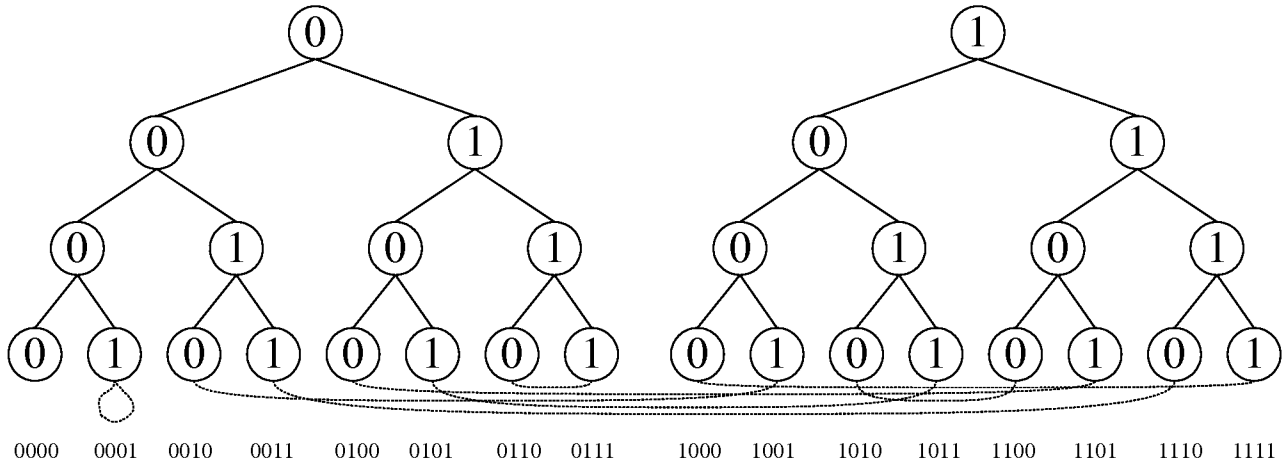

图 2

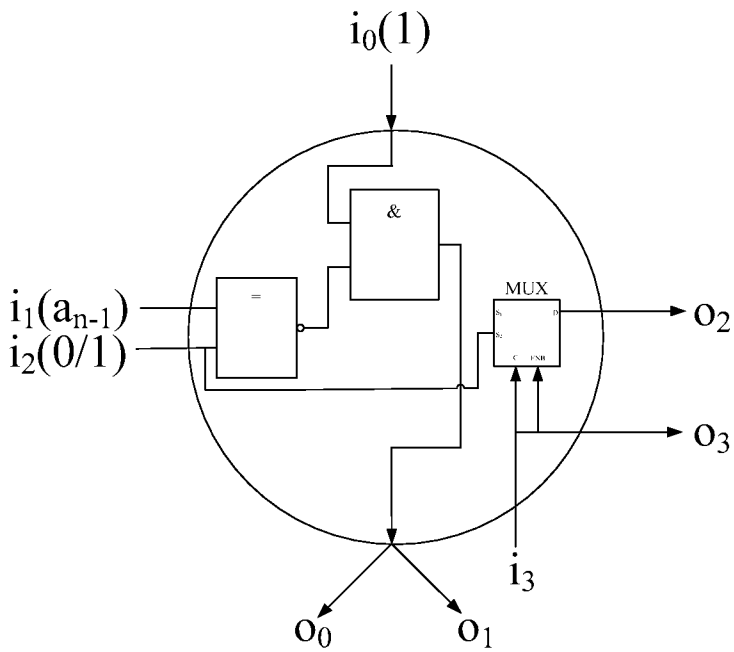

图 3（1）

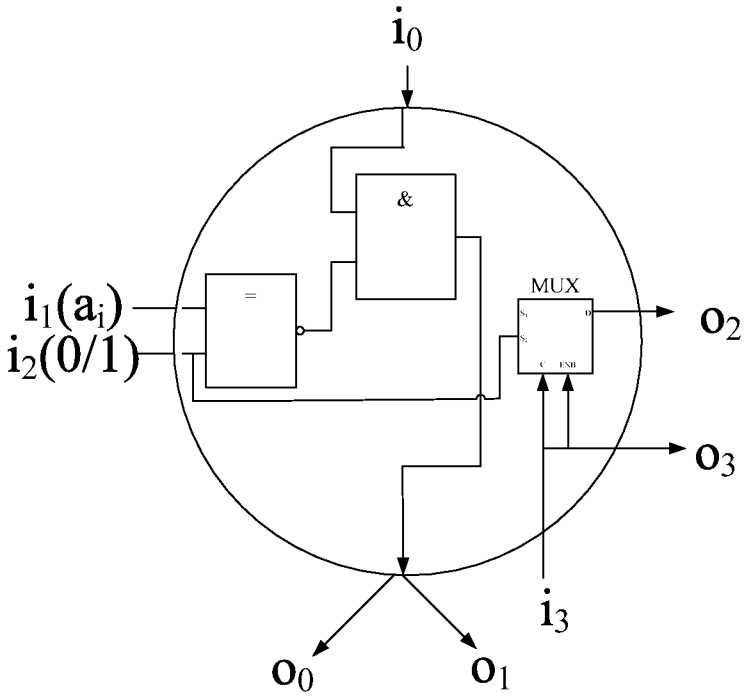

图 3（2）

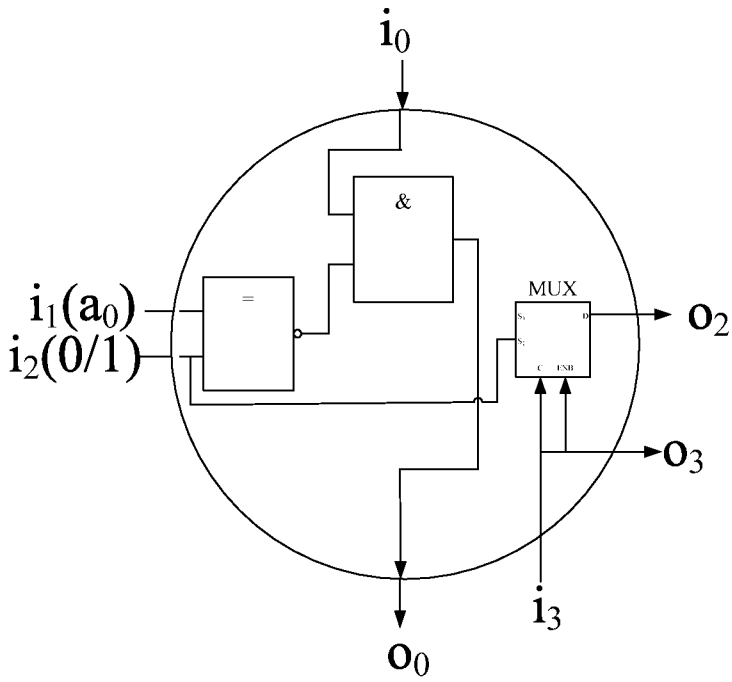

图 3（3）

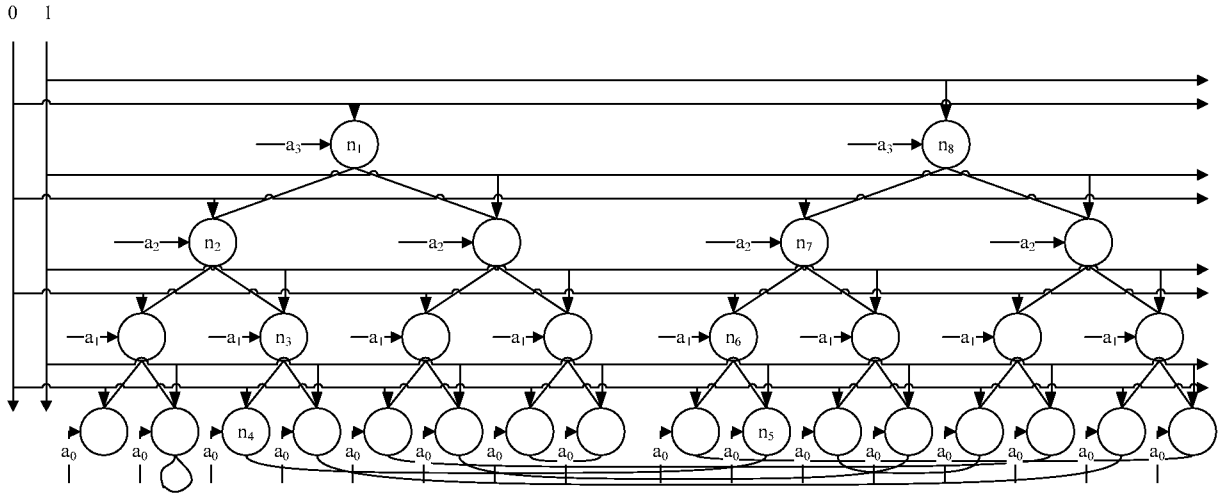
0
1
a3
n1
n8
a2
n2
n7
a1
n3
n6
a0
n4
n5

图 4

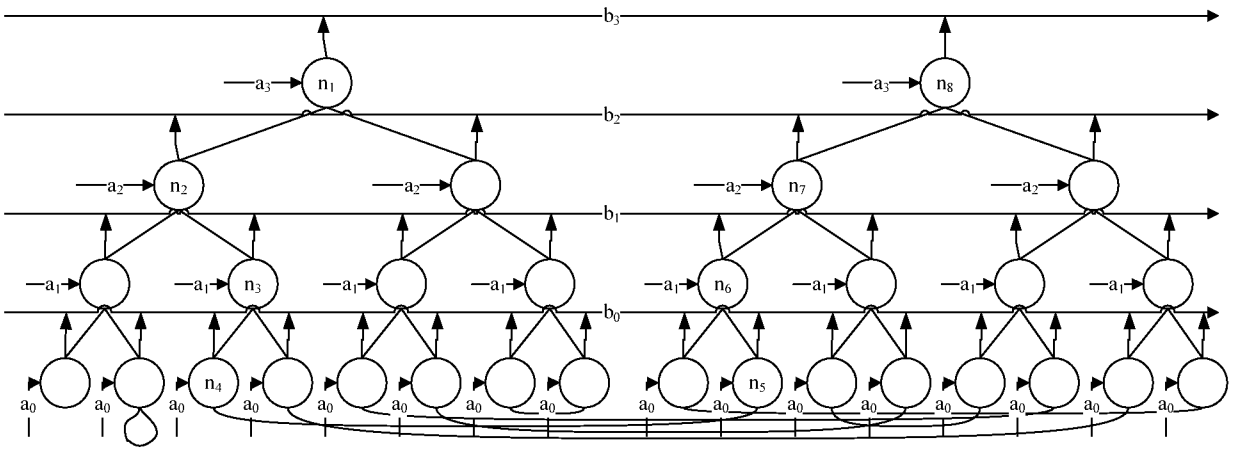
b3
b2
b1
b0
a3
n1
n8
a2
n2
n7
a1
n3
n6
a0
n4
n5

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/085948

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/72 (2006.01) i

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)

IPC: G06F /-; G09G /-; 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)

WPI; EPODOC; CNKI; IEEE; CNPAT

finite w field?, Galois w field, invers+, lookup w table, lookup w tree, search w tree, node?, root, leaf, logic w gate, LUT, NXOR, AND, MUX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6138133 A (SAMSUNG ELECTRONICS CO., LTD.) 24 October 2000 (24.10.2000) see the whole document	1-6
A	US 20100306299 A1 (ITT MANUFACTURING ENTERPRISE INC) 02 December 2010 (02.12.2010) see the whole document	1-6
A	CN 1032595 A (DIGITAL EQUIPMENT CORPORATION) 26 April 1989 (26.04.1989) see the whole document	1-6
A	US 6779011 B2 (MAXTOR CORPORATION) 17 August 2004 (17.08.2004) see the whole document	1-6
A	US 20030219118 A1 (BEVERLY, HARIAN T.) 27 November 2003 (27.11.2003) see the whole document	1-6

☐ 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	Date of mailing of the international search report
23 April 2013 (23.04.2013)	16 May 2013 (16.05.2013)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Le Telephone No. (86-10) 62411827

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/085948

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 6138133 A	24.10.2000	JP 11317676 A	16.11.1999
		KR 19990069340 A	06.09.1999
		KR 100304193 B	22.11.2001
		JP 3913921 B2	09.05.2007
US 20100306299 A1	02.12.2010	EP 2261795 A1	15.12.2010
		EP 2261795 B1	23.11.2011
		EP 2261795 B9	09.05.2012
		AT 534950 T	15.12.2011
CN 1032595 A	26.04.1989	WO 8901660 A	23.02.1989
		AU 2906588 A	09.03.1989
		EP 0328637 A	23.08.1989
		JPH 02503855 A	08.11.1990
		US 4975867 A	04.12.1990
		CA 1312954 C	19.01.1993
		KR 930006519 B1	16.07.1993
		EP 0328637 A4	08.01.1992
		EP 0328637 B1	27.11.1996
		DE 3855684 G	09.01.1997
		CN 1013715 B	28.08.1991
		AU 613701 B	08.08.1991
		MX 164418 B	12.08.1992
		DE 3855684 T	15.05.1997
		JP 7112162 B	29.11.1995
US 6779011 B2	17.08.2004	US 20020156823 A1	24.10.2002
US 20030219118 A1	27.11.2003	None	

国际检索报告

国际申请号
PCT/CN2012/085948

A. 主题的分类

G06F 7/72 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC： G06F /-; G09G/-; H04L/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI;EPODOC;CNKI;IEEE;CNPAT

有限域，伽罗华，伽罗瓦，逆运算，模逆，查找树，查找表，搜索树，节点，根节点，叶子，逻辑门； finite w field?, Galois w field, invers+, lookup w table, lookup w tree, search w tree, node?, root, leaf, logic w gate, LUT, NXOR, AND, MUX

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US6138133A (三星电子株式会社) 24.10 月 2000 (24.10.2000) 参见全文	1-6
A	US20100306299A1 (ITT 制造企业公司) 02.12 月 2010 (02.12.2010) 参见全文	1-6
A	CN1032595A (数字设备公司) 26.4 月 1989 (26.04.1989) 参见全文	1-6
A	US6779011B2 (迈拓公司) 17.8 月 2004 (17.08.2004) 参见全文	1-6
A	US20030219118A1 (BEVERLY, Harian T.) 27.11 月 2003 (27.11.2003) 参见全文	1-6

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
23.4 月 2013 (23.04.2013)	**16.5 月 2013 (16.05.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 李乐 电话号码：(86-10) **62411827**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2012/085948

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US6138133A	24.10.2000	JP11317676A	16.11.1999
		KR19990069340A	06.09.1999
		KR100304193B	22.11.2001
		JP3913921B2	09.05.2007
US20100306299 A1	02.12.2010	EP2261795A1	15.12.2010
		EP2261795B1	23.11.2011
		EP2261795B9	09.05.2012
		AT534950T	15.12.2011
CN1032595A	26.04.1989	WO8901660A	23.02.1989
		AU2906588A	09.03.1989
		EP0328637A	23.08.1989
		JPH02503855A	08.11.1990
		US4975867A	04.12.1990
		CA1312954C	19.01.1993
		KR930006519B1	16.07.1993
		EP0328637A4	08.01.1992
		EP0328637B1	27.11.1996
		DE3855684G	09.01.1997
		CN1013715B	28.08.1991
		AU613701B	08.08.1991
		MX164418B	12.08.1992
		DE3855684T	15.05.1997
		JP7112162B	29.11.1995
US6779011B2	17.08.2004	US20020156823A1	24.10.2002
US20030219118A1	27.11.2003	无	