(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
2018 年 5 月 31 日 (31.05.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/094566 A1

(51) 国际专利分类号:
G06F 19/00 (2011.01)

(21) 国际申请号: PCT/CN2016/106780

(22) 国际申请日: 2016 年 11 月 22 日 (22.11.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 深圳大学(SHENZHEN UNIVERSITY) [CN/CN]; 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

(72) 发明人: 张鹏 (ZHANG, Peng); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。 张晓妹 (ZHANG, Xiaomei); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。 喻建平 (YU, Jianping); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

(74) 代理人: 深圳市恒申知识产权事务所 (普通合伙) (HENSEN INTELLECTUAL PROPERTY FIRM); 中国广东省深圳市福田区南园路68号上步大厦10H, Guangdong 518000 (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, DJ, 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, KW, KZ, LA, LC, LK, LR, LS, 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) 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, ST, 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,

(54) **Title:** CONSTRUCTION METHOD FOR PARALLEL HASH FUNCTION

(54) **发明名称:** 并行哈希函数的构造方法

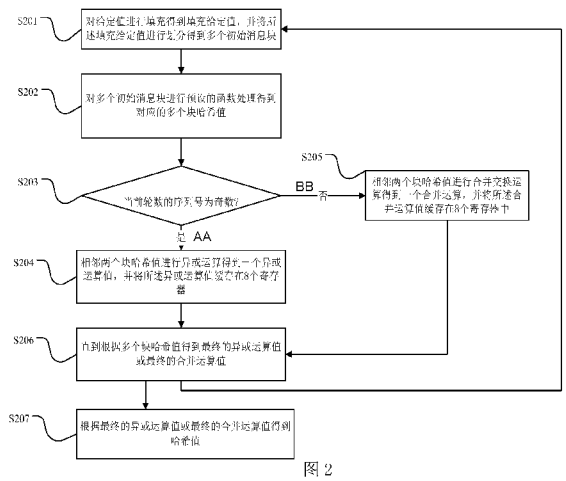

图 2

S201 Fill a set value to obtain a filled set value, and divide the filled set value to obtain multiple initial message blocks
S202 Perform preset function processing on the multiple initial message blocks to obtain corresponding multiple blocks of hash values
S203 Is the sequence number of the current round an odd number?
S204 Perform an exclusive-or operation on two adjacent blocks of hash values to obtain an exclusive-or value and cache the exclusive-or value in 8 registers
S205 Perform a merge-exchange operation on two adjacent blocks of hash values to obtain a merge value and cache the merge value in 8 registers
S206 Continue until a final exclusive-or value or a final merge value is obtained on the basis of the multiple blocks of hash values
S207 Obtain a hash value on the basis of the final exclusive-or value or merge value
AA Yes
BB No

(57) **Abstract:** The present invention provides a construction method for a parallel hash function, the construction method comprising the following steps: filling a set value to obtain a filled set value, dividing the filled set value to obtain multiple initial message blocks; performing preset function processing on the multiple initial message blocks to obtain corresponding multiple blocks of hash values; determining a sequence number of a current round to be an odd number or an even number, wherein if the sequence number of the current round is an odd number, performing an exclusive-or operation on two adjacent blocks of hash values to obtain an exclusive-or value and caching the exclusive-or operation value in 8 registers, and if the sequence number of the current round is an even number, performing a merge-exchange operation on two adjacent blocks of hash values to obtain a merge value and caching the merge operation value in 8 registers; and continuing until a final exclusive-or value or a final merge value is obtained on the basis of the multiple blocks of hash values; and obtaining a hash value on the basis of the final exclusive-or value or merge value.

WO 2018/094566 A1

[见续页]

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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本发明提供一种并行哈希函数的构造方法，所述构造方法包括以下步骤：对给定值进行填充得到填充给定值，并将所述填充给定值进行划分得到多个初始消息块；对多个初始消息块进行预设的函数处理得到对应的多个块哈希值；判断当前轮数的序列号为奇数或偶数，其中，当当前轮数的序列号为奇数时，相邻两个块哈希值进行异或运算得到一个异或运算值，并将所述异或运算值缓存在8个寄存器中，当当前轮数的序列号为偶数时，相邻两个块哈希值进行合并交换运算得到一个合并运算，并将所述合并运算值缓存在8个寄存器中；直到根据多个块哈希值得到最终的异或运算值或最终的合并运算值；根据最终的异或运算值或最终的合并运算值得到哈希值。

并行哈希函数的构造方法

技术领域

本发明涉及信息安全领域，尤其涉及一种并行哈希函数的构造方法。

背景技术

现有的哈希函数消息运算过程中重复使用一压缩函数 f，如图 1 所示，函数 f 的输入有两项，一项是上一轮（第 $i-1$ 轮）的输出 CV_{i-1}，也即是链接变量，另一项则是本轮（第 i 轮）输入的消息块 Y_i。因此只有上一个消息块的值计算结束之后才能计算下一个消息块的值，这就增加了计算时间。当消息足够长时，运算速率不可避免的会很低，使得运算的效率降低。

发明内容

本发明旨在解决现有技术中哈希函数运算效率较低的技术问题，提供一种并行哈希函数的构造方法。

本发明的实施例提供一种并行哈希函数的构造方法，所述构造方法包括以下步骤：

对给定值进行填充得到填充给定值，并将所述填充给定值进行划分得到多个初始消息块；

对多个初始消息块进行预设的函数处理得到对应的多个块哈希值；

判断当前轮数的序列号为奇数或偶数，其中，当当前轮数的序列号为奇数时，相邻两个块哈希值进行异或运算得到一个异或运算值，并将所述异或运算值缓存在 8 个寄存器中，当当前轮数的序列号为偶数时，相邻两个块哈希值进行合并交换运算得到一个合并运算，并将所述合并运算值缓存在 8 个寄存器中；

直到根据多个块哈希值得到最终的异或运算值或最终的合并运算值；

根据最终的异或运算值或最终的合并运算值得到哈希值。

本发明的技术方案与现有技术相比，有益效果在于：每个块哈希值在计算时不受其他消息块值的影响，不需要等待其他消息块值的运算结果来进行运算，

即在每轮计算中，多个消息块可以同时被处理，因此可以提高运算效率，节省运算时间。

附图说明

图 1 是现有技术中哈希函数的运算示意图；

图 2 是本发明并行哈希函数的构造方法一种实施例的流程示意图；

图 3 是本发明并行哈希函数一种实施例的结构示意图；

图 4 是本发明并行哈希函数的构造方法中初始链接变量值的处理方法一种实施例的流程示意图；

图 5 是本发明并行哈希函数的构造方法中初始链接变量值的处理方法另一种实施例的流程示意图；

图 6 是本发明并行哈希函数的仿真结果示意图。

具体实施方式

下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本发明，而不能理解为对本发明的限制。

本发明一个实施例的并行哈希函数的构造方法，如图 2 所示，所述构造方法包括以下步骤：

步骤 S201，对给定值进行填充得到填充给定值，并将所述填充给定值进行划分得到多个初始消息块；

步骤 S202，对多个初始消息块进行预设的函数处理得到对应的多个块哈希值；

步骤 S203，判断当前轮数的序列号为奇数或偶数，其中，当当前轮数的序列号为奇数时，进入步骤 S204，当当前轮数的序列号为偶数时，进入步骤 S205；

步骤 S204，相邻两个块哈希值进行异或运算得到一个异或运算值，并将所述异或运算值缓存在 8 个寄存器中；

步骤 S205，相邻两个块哈希值进行合并交换运算得到一个合并运算，并将

所述合并运算值缓存在 8 个寄存器中；

步骤 S206，直到根据多个块哈希值得到最终的异或运算值或最终的合并运算值；

步骤 S207，根据最终的异或运算值或最终的合并运算值得到哈希值。

在具体实施中，所述对给定值进行填充得到填充给定值具体为：

在给定值的后面加入一个常数 1 和多个常数 0；

加入给定值的长度值，得到长度为 512 倍数的填充给定值。

在具体实施中，所述将所述填充给定值进行划分得到多个初始消息块的步骤，具体为：

按照 512 比特，将所述填充给定值进行划分得到多个初始消息块

在具体实施中，所述预设的函数具体为：压缩函数 f 。

在具体实施中，当当前轮数的序列号为奇数时，相邻两个块哈希值进行异或运算得到一个异或运算值，具体为：

当当前轮数的序列号为奇数时，在最后一个块哈希值之后增加一个块哈希值；

相邻两个块哈希值进行异或运算得到一个异或运算值，其中，增加的块哈希值与最后一个块哈希值相同。

在具体实施中，图 3 是本发明一个实施例并行哈希函数的结构示意图。首先把给定的消息 M 进行填充，使得填充后的长度是 512 的倍数。填充的规则是在消息后加入一个 1 和若干个 0，在最后再加入消息的长度。填充之后的消息被分成若干个 512 比特的消息块 Y_0， Y_1， … ， Y_{L-1}。我们先各自计算每一个消息块的值并把它们的值记录下来表示为块哈希值。

在接下来的每一轮里，每两个相邻的消息块的值被一起进行运算。当每一轮里消息块的个数是奇数时，我们添加一个块哈希值，该块哈希值和本轮最后一个消息块的值是相同的。在这个阶段，使用 256 比特长的缓冲区以存储中间结果和最后的哈希值，缓冲区可表示为 8 个 32 比特长的寄存器 A，B，C，D，E，F，G，H。

假设 i 是轮数的序列号，当 $i \bmod 2 = 1$ （ $i = 1,2,\cdots$ ）时，让该轮里相邻的两个消息块进行异或运算，获得的值分别存放在八个寄存器 A，B，C，D，E，F，G，H

中。比如在第一轮中，Y_0对应的消息块值和 Y_1对应的消息块值进行异或运算得到运算值 h1，Y_2对应的消息块值和 Y_2对应的消息块值进行异或运算得到运算值 h2,在第一轮中，最后一个 Y_i对应的消息块值没有可以进行运算的对象，因此增加一个 Y_i 对应的消息块值与最后一个 Y_i 对应的消息块值进行异或运算。当 $i \bmod 2 = 0$ （$i = 1,2,\ldots$）时，我们把这两个消息块中前一个消息块的E, F, G, H中的值依次赋给新的寄存器A, B, C, D，把后一个消息块的A, B, C, D中的值依次赋给新的寄存器E, F, G, H，这样就得到新的值。比如相邻两个消息块需要合并，记第一消息块为 MB1 和第二消息块 MB2。第一消息块 MB1 需要 ABCDEFGH 八个寄存器存放，第二消息块 MB2 也需要 ABCDEFGH 八个寄存器存放。当 imod2=0 时，第一消息块为 MB1 和第二消息块 MB2 的合并结果记为 NMB。其中，NMB 的 ABCD 四个寄存器存放第一消息块 MB1 的 EFGH 四个寄存器的值，NMB 的四个寄存器 EFGH 存放第二消息块 MB2 的 ABCD 四个寄存器的值。

根据本发明中并行哈希函数的构造方法， 每个块哈希值在计算时不受其他消息块值的影响，不需要等待其他消息块值的运算结果来进行运算，即在每轮计算中，多个消息块可以同时被处理，因此可以提高运算效率，节省运算时间。

在具体实施中，由于现有哈希函数的初始链接变量值是常量，这就使得攻击者可以采用穷举攻击的方法找到碰撞，使得哈希函数变得不安全，通过对初始链接变量值进行处理改进，可以增强哈希函数的不可确定性和不可预测性。本发明还提供一种实施例的并行哈希函数的构造方法，如图 4 所述，在步骤 S203 之前以下步骤:

步骤 S401，将多个块哈希值一一对应存放在对应的 8 个寄存器中；

步骤 S402，在每个块哈希值对应的 8 个寄存器中进行第一次计算，根据函数 $f_1, f_2, \sigma_1, \sigma_2$ 对每相邻两个寄存器中的值进行结合运算，得到第一次结合运算结果；

步骤 S403，进行第二次计算，根据函数 $f_3, f_4, \sigma_3, \sigma_4$ 和第一轮结合运算结果对第一寄存器中的值和第四寄存器中的值、第二寄存器中的值和第三寄存器中的值、第五寄存器中的值和第八寄存器中的值以及第六寄存器中的值和第七寄存器中的值分别进行结合运算，得到第二次结合运算结果；

步骤 S404，进行第三次计算，根据函数 $f_5, f_6, \sigma_5, \sigma_6$ 和第二次结合运算结果对

第一寄存器中的值和第六寄存器中的值、第二寄存器中的值和第五寄存器中的值、第三寄存器中的值和第八寄存器中的值以及第四寄存器中的值和第七寄存器中的值分别进行结合运算，得到每个块哈希值对应的 8 个寄存器中的更新值。

也就是说，上述步骤具体为图 3 中 block hash 的细化步骤，在当 i=1 时，先对初始链接变量值进行处理改进之后，再根据每相邻两个块哈希值对应的 8 个寄存器中的更新值进行异或运算。

在具体实施中，步骤 S402 具体为：

根据函数 s_1 对第一寄存器 A 中的值进行运算得到函数 s_1 的第一计算结果，并将函数 s_1 的第一计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第二寄存器 B 中的值、函数 s_1 的第一计算结果和第一预设值 n_1 进行运算得到函数 f1 的第一计算结果，并将函数 f1 的第一计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第一计算结果进行运算得到函数 s_2 的第一计算结果并更新至第二寄存器 B，并将函数 s_2 的第一计算结果输出至函数 f2 和第二次计算中；

根据函数 f2 对函数 s_1 的第一计算结果、函数 s_2 的第一计算结果和第二预设值 n_2 进行运算得到函数 f2 的第一计算结果更新至第一寄存器 A，并将函数 f2 的第一计算结果输出至第二次计算中；

根据函数 s_1 对第三寄存器 C 中的值进行运算得到函数 s_1 的第二计算结果，并函数 s_1 的第二计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第四寄存器 D 中的值、函数 s_1 的第二计算结果和第一预设值 n_1 进行运算得到函数 f1 的第二计算结果，并将函数 f1 的第一计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第二计算结果进行运算得到函数 s_2 的第二计算结果更新至第四寄存器 D，并将函数 s_2 的第二计算结果输出至函数 f2 和第二次计算中；

根据函数 f2 对函数 s_1 的第二计算结果、函数 s_2 的第二计算结果和第二预设值 n_2 进行运算得到函数 f2 的第二计算结果更新至第三寄存器 C，并将函数 f2 的第二计算结果输出至第二次计算中；

根据函数 s_1 对第五寄存器 E 中的值进行运算得到函数 s_1 的第三计算结果，并将函数 s_1 的第三计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第六寄存器 F 中的值、函数 s_1 的第三计算结果和第一预设值 n_1 进行运算得到函数 f1 的第三计算结果，并将函数 f1 的第三计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第三计算结果进行运算得到函数 s_2 的第三计算结果更新至第六寄存器 F，并将函数 s_2 的第三计算结果输出至函数 f2 和第二次计算中；

根据函数 f2 对函数 s_1 的第三计算结果、函数 s_2 的第三计算结果和第二预设值 n_2 进行运算得到函数 f2 的第三计算结果更新至第五寄存器 E，并将函数 f2 的第三计算结果输出至第二次计算中；

根据函数 s_1 对第七寄存器 G 中的值进行运算得到函数 s_1 的第四计算结果，并将函数 s_1 的第四计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第八寄存器 H 中的值、函数 s_1 的第四计算结果和第一预设值 n_1 进行运算得到函数 f1 的第四计算结果，并将函数 f1 的第四计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第四计算结果进行运算得到函数 s_2 的第四计算结果更新至第八寄存器 H，并将函数 s_2 的第四计算结果输出至函数 f2 和第二次计算中；

根据函数 f2 对函数 s_1 的第四计算结果、函数 s_2 的第四计算结果和第二预设值 n_2 进行运算得到函数 f2 的第四计算结果更新至第七寄存器 G，并将函数 f2 的第四计算结果输出至第二次计算中。

在具体实施中，步骤 S403 具体为：

根据函数 s_3 对函数 f2 的第一计算结果进行运算得到函数 s_3 的第一计算结果，并将函数 s_3 的第一计算结果输出至函数 f3 和函数 f4 中；

根据函数 s_3 对函数 f2 的第二计算结果进行运算得到函数 s_3 的第二计算结果，并将函数 s_3 的第二计算结果输出至函数 f3 和函数 f4 中；

根据函数 f3 对函数 s_2 的第一计算结果、函数 s_3 的第二计算结果和第三预设值 n_3 进行运算得到函数 f3 的第一计算结果，并将函数 f3 的第一计算结果输

出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第一计算结果进行运算得到函数 s_4 的第一计算结果更新至第二寄存器 B，并将函数 s_4 的第一计算结果输出至函数 f4 和第三次运算中；

根据函数 f4 对函数 s_4 的第一计算结果、函数 s_3 的第二计算结果和第四预设值 n_4 进行运算得到函数 f4 的第一计算结果更新至第三寄存器 C，并将函数 f4 的第一计算结果输出至第三次运算中；

根据函数 f3 对函数 s_3 的第一计算结果、函数 s_2 的第二计算结果和第三预设值 n_3 进行运算得到函数 f3 的第二计算结果，并将函数 f3 的第二计算结果输出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第二计算结果进行运算得到函数 s_4 的第二计算结果更新至第四寄存器 D，并将函数 s_4 的第二计算结果输出至函数 f4；

根据函数 f4 对函数 s_4 的第二计算结果、函数 s_3 的第一计算结果和第四预设值 n_4 进行运算得到函数 f4 的第二计算结果更新至第一寄存器 A，并将函数 f4 的第二计算结果输出至第三次运算中；

根据函数 s_3 对函数 f2 的第三计算结果进行运算得到函数 s_3 的第三计算结果，并将函数 s_3 的第三计算结果输出至函数 f3 和函数 f4 中；

根据函数 s_3 对函数 f2 的第四计算结果进行运算得到函数 s_3 的第四计算结果，并将函数 s_3 的第四计算结果输出至函数 f3 和函数 f4 中；

根据函数 f3 对函数 s_2 的第三计算结果、函数 s_3 的第四计算结果和第三预设值 n_3 进行运算得到函数 f3 的第三计算结果，并将函数 f3 的第三计算结果输出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第三计算结果进行运算得到函数 s_4 的第三计算结果更新至第六寄存器 F，并将函数 s_4 的第三计算结果输出至函数 f4 和第三次运算中；

根据函数 f4 对函数 s_4 的第三计算结果、函数 s_3 的第四计算结果和第四预设值 n_4 进行运算得到函数 f4 的第三计算结果更新至第七寄存器 G，并将函数 f4 的第三计算结果输出至第三次运算中；

根据函数 f3 对函数 s_3 的第三计算结果、函数 s_2 的第四计算结果和第三预

设值 n_3 进行运算得到函数 f3 的第四计算结果，并将函数 f3 的第四计算结果输出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第四计算结果进行运算得到函数 s_4 的第四计算结果更新至第八寄存器 H，并将函数 s_4 的第四计算结果输出至函数 f4；

根据函数 f4 对函数 s_4 的第四计算结果、函数 s_3 的第三计算结果和第四预设值 n_4 进行运算得到函数 f4 的第四计算结果更新至第五寄存器 E，并将函数 f4 的第四计算结果输出至第三次运算中。

在具体实施中，步骤 S404 具体为：

根据函数 s_5 对函数 f4 的第二计算结果进行运算得到函数 s_5 的第一计算结果，并将函数 s_5 的第一计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第一计算结果、函数 s_4 的第三计算结果和第五预设值 n_5 进行运算得到函数 f5 的第一计算结果，并将函数 f5 的第一计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第一计算结果进行运算得到函数 s_6 的第一计算结果更新至第六寄存器 F，并将函数 s_6 的第一计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第一计算结果、函数 s_5 的第一计算结果和第六预设值 n_6 进行运算得到函数 f6 的第一计算结果更新至第一寄存器 A 中；

根据函数 s_5 对函数 f4 的第四计算结果进行运算得到函数 s_5 的第二计算结果，并将函数 s_5 的第二计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第二计算结果、函数 s_4 的第一计算结果和第五预设值 n_5 进行运算得到函数 f5 的第二计算结果，并将函数 f5 的第二计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第二计算结果进行运算得到函数 s_6 的第二计算结果更新至第二寄存器 B，并将函数 s_6 的第二计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第二计算结果、函数 s_5 的第二计算结果和第六预设值 n_6 进行运算得到函数 f6 的第二计算结果更新至第五寄存器 E 中；

根据函数 s_5 对函数 f4 的第一计算结果进行运算得到函数 s_5 的第三计算结果，并将函数 s_5 的第三计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第三计算结果、函数 s_4 的第四计算结果和第五预

设值 n_5 进行运算得到函数 f5 的第三计算结果，并将函数 f5 的第三计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第三计算结果进行运算得到函数 s_6 的第三计算结果更新至第八寄存器 H 中，并将函数 s_6 的第三计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第三计算结果、函数 s_5 的第三计算结果和第六预设值 n_6 进行运算得到函数 f6 的第三计算结果更新至第三寄存器 C 中；

根据函数 s_5 对函数 f4 的第三计算结果进行运算得到函数 s_5 的第四计算结果，并将函数 s_5 的第四计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第四计算结果、函数 s_4 的第二计算结果和第五预设值 n_5 进行运算得到函数 f5 的第四计算结果，并将函数 f5 的第四计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第四计算结果进行运算得到函数 s_6 的第四计算结果更新至第四寄存器中，并将函数 s_6 的第四计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第四计算结果、函数 s_5 的第四计算结果和第六预设值 n_6 进行运算得到函数 f6 的第四计算结果更新至第七寄存器 G 中。

在具体实施中，如图 5 所示，在初始链接变量值的处理过程中，采用一个 32 比特输入 x_i 的函数 σ_i 和有三个 32 比特的输入 k_i, m_i, n_i 的函数 f_i，$i=1,2,...,6$。$ROTR^{s_i}(x_i)$ 表示把 x_i 循环右移 s_i 位。在不同轮选择了不同的 s_i 值。σ_i 和 f_i 的计算公式如下所示：

$$\sigma_1=ROTR^{3}(x_1)\oplus ROTR^{7}(x_1)\oplus ROTR^{18}(x_1);$$

$$\sigma_2=ROTR^{3}(x_2)\oplus ROTR^{14}(x_2)\oplus ROTR^{25}(x_2);$$

$$\sigma_3=ROTR^{10}(x_3)\oplus ROTR^{13}(x_3)\oplus ROTR^{17}(x_3);$$

$$\sigma_4=ROTR^{10}(x_4)\oplus ROTR^{15}(x_4)\oplus ROTR^{19}(x_4);$$

$$\sigma_5=ROTR^{8}(x_5)\oplus ROTR^{13}(x_5)\oplus ROTR^{15}(x_5);$$

$$\sigma_6=ROTR^{8}(x_6)\oplus ROTR^{17}(x_6)\oplus ROTR^{19}(x_6);$$

$$f_i=(k_i\wedge m_i)\oplus(\neg k_i\wedge n_i)(i=1,3,5);$$

$$f_i=(k_i\wedge m_i)\oplus(k_i\wedge n_i)\oplus(m_i\wedge n_i)(i=2,4,6);$$

其中，x1，x2，x3，x4，x5，x6 为输入值，k_i 表示函数 σ_i 的输出，m_i 表述函数 σ_{i-1} 的输出，当 i=1 时，σ_0 是寄存器中的值。

原先已知的初始值存放在寄存器A，B，C，D，E，F，G，H中，这些值将经过三轮处理来获得更新后的初始值。在第一轮中，相邻寄存器中的值通过函数$f_1, f_2, \sigma_1, \sigma_2$进行运算，也即是$A$和$B$进行结合运算，$C$和$D$进行运算，$E$和$F$进行运算，$G$和$H$进行结合运算，得到新的值。接下来两轮中值的计算方法和第一轮中是类似的，只是采用的函数和值结合的次序不同。第二轮中，采用的函数是$f_3, f_4, \sigma_3, \sigma_4$，前四个值中，$A$和$D$，$B$和$C$分别进行进行结合运算，后四个值中，$E$和$H$，$F$和$G$分别进行结合运算。在第三轮中，函数$f_5, f_6, \sigma_5, \sigma_6$被采用，其中$A$和$F$进行结合运算，$B$和$E$进行运算，$C$和$H$进行运算，$D$和$G$进行运算。经过这三轮运算，最终得出更新后初始值。对于任意函数f_i有三个输入，其中一个输入k_i来自函数σ_i的输出，另一个输入m_i来自函数σ_{i-1}的输出，最后一个输入n_i的值是常数，在不同轮的取值情况分别列在表一和表二中。在表一中，n_1的值分别取自$SHA256(t)(t = 0,1,2,3)$得到的哈希值的前 32 比特，n_2的值来源于t $(t = 2,3,5,7)$的平方根的十进制部分的二进制表示的前 32 位。通过表二可以看出，对于n_3，n_4，n_5，n_6，同样的值被使用。

表一

第一轮	*A*&B	*C*&*D*	*E*&*F*	*G*&*H*
n_1的值	5feceb66	6b86b273	d4735e3a	4e074085
n_2的值	428a2f98	71374491	b5c0fbcf	e9b5dba5

表二

第二轮	*B*&C	*A*&*D*	*F*&G	*E*&H
第三轮	*B*&E	*A*&*F*	*D*&G	*C*&H
n_3, n_5的值	71374491	6b86b273	e9b5dba5	4e074085
n_4, n_6的值	5feceb66	428a2f98	d4735e3a	b5c0fbcf

通过把最终得到的值作为新的初始链接变量值。通过对于初始值的改进，增强了函数的不可确定性和不可预测性。

在具体实施中，测试哈希值对初始链接变量的敏感性，即为了评估初始值改变对于最终哈希值的影响，任意选择了一个文本“Hash function is one of the major tools in cryptography, which is usually used for data integrity

in conjunction with digital signature schemes.”并对其在六种不同的情况下进行测试。

情形 1：计算这个给定的消息的哈希值；

情形 2：第一个字符‘H’换成‘A’；

情形 3：把单词“data”变成“date”；

情形 4：句子末尾的句号换成分号；

情形 5：把句子中的第二个单词“function”改成“Function”；

情形 6：在单词“Hash”之前添加一个数字 6。

得出的相对应的哈希值用十六进制表示如下：

情形 1：

107CC9225AD8BB6D15D51992C3AE6386321F150D5320716C71F9BF7C47783920 ；

情形 2：

B81788A2CF98DE7AD4CB770459046C9104E7F46953563302FEFDA941A46C1D08 ；

情形 3：

8AC84B4DAD82294541B27C1207C0D90ACF9CD89A541871AC9BFA6D2A9E7A2849 ；

情形 4：

63DFE552EDACCB56E73225BE335FBE7FD4947C2BEE2697DF0D5346A422001A38 ；

情形 5：

5BC213F16560D60784E6815039E9677C80F5129EA7D5920AE57A70B30D93ADB0 ；

情形 6：

AB20F763C0E7093C10011597572D0E828118662FA28C57E0A8DE4C651D051CC0 。

如图 6 所示，得出的不同情况下的测试值即仿真结果。根据仿真结果可以看出，不管消息有多么极小的改变，哈希值都将会有很大的变化。结果表明并行哈希函数的敏感性很好。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示

例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

权 利 要 求 书

1、一种并行哈希函数的构造方法，其特征在于：所述构造方法包括以下步骤：

对给定值进行填充得到填充给定值，并将所述填充给定值进行划分得到多个初始消息块；

对多个初始消息块进行预设的函数处理得到对应的多个块哈希值；

判断当前轮数的序列号为奇数或偶数，其中，当当前轮数的序列号为奇数时，相邻两个块哈希值进行异或运算得到一个异或运算值，并将所述异或运算值缓存在 8 个寄存器中，当当前轮数的序列号为偶数时，相邻两个块哈希值进行合并交换运算得到一个合并运算，并将所述合并运算值缓存在 8 个寄存器中；

直到根据多个块哈希值得到最终的异或运算值或最终的合并运算值；

根据最终的异或运算值或最终的合并运算值得到哈希值。

2、如权利要求 1 所述的构造方法，其特征在于：所述对给定值进行填充的步骤，具体为：

在给定值的后面加入一个常数 1 和多个常数 0；

加入给定值的长度值，得到长度为 512 倍数的填充给定值。

3、如权利要求 2 所述的构造方法，其特征在于：所述将所述填充给定值进行划分得到多个初始消息块的步骤，具体为：

按照 512 比特，将所述填充给定值进行划分得到多个初始消息块。

4、如权利要求 1-3 任意一项所述的构造方法，其特征在于：当当前轮数的序列号为奇数时，相邻两个块哈希值进行异或运算得到一个异或运算值，具体为：

当当前轮数的序列号为奇数时，在最后一个块哈希值之后增加一个块哈希值；

相邻两个块哈希值进行异或运算得到一个异或运算值。

5、如权利要求 4 所述的构造方法，其特征在于：增加的块哈希值与最后一个块哈希值相同。

6、如权利要求 1 所述的构造方法，其特征在于：在判断当前轮数的序列号为奇数或偶数之前，还包括以下步骤：

将多个块哈希值一一对应存放在对应的 8 个寄存器中；

在每个块哈希值对应的 8 个寄存器中进行第一次计算，根据函数 $f_1, f_2, \sigma_1, \sigma_2$ 对每相邻两个寄存器中的值进行结合运算，得到第一次结合运算结果；

进行第二次计算，根据函数 $f_3, f_4, \sigma_3, \sigma_4$ 和第一轮结合运算结果对第一寄存器中的值和第四寄存器中的值、第二寄存器中的值和第三寄存器中的值、第五寄存器中的值和第八寄存器中的值以及第六寄存器中的值和第七寄存器中的值分别进行结合运算，得到第二次结合运算结果；

进行第三次计算，根据函数 $f_5, f_6, \sigma_5, \sigma_6$ 和第二次结合运算结果对第一寄存器中的值和第六寄存器中的值、第二寄存器中的值和第五寄存器中的值、第三寄存器中的值和第八寄存器中的值以及第四寄存器中的值和第七寄存器中的值分别进行结合运算，得到每个块哈希值对应的 8 个寄存器中的更新值。

7、如权利要求 6 所述的构造方法，其特征在于：所述根据函数 $f_1, f_2, \sigma_1, \sigma_2$ 对每相邻两个寄存器中的值进行结合运算，得到第一次结合运算结果，具体为：

根据函数 s_1 对第一寄存器中的值进行运算得到函数 s_1 的第一计算结果，并将函数 s_1 的第一计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第二寄存器中的值、函数 s_1 的第一计算结果和第一预设值 n_1 进行运算得到函数 f1 的第一计算结果，并将函数 f1 的第一计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第一计算结果进行运算得到函数 s_2 的第一计算结果并更新至第二寄存器，并将函数 s_2 的第一计算结果输出至函数 f2 和第二

次计算中；

根据函数 f2 对函数 s_1 的第一计算结果、函数 s_2 的第一计算结果和第二预设值 n_2 进行运算得到函数 f2 的第一计算结果更新至第一寄存器，并将函数 f2 的第一计算结果输出至第二次计算中；

根据函数 s_1 对第三寄存器中的值进行运算得到函数 s_1 的第二计算结果，并函数 s_1 的第二计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第四寄存器中的值、函数 s_1 的第二计算结果和第一预设值 n_1 进行运算得到函数 f1 的第二计算结果，并将函数 f1 的第一计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第二计算结果进行运算得到函数 s_2 的第二计算结果更新至第四寄存器，并将函数 s_2 的第二计算结果输出至函数 f2 和第二次计算中；

根据函数 f2 对函数 s_1 的第二计算结果、函数 s_2 的第二计算结果和第二预设值 n_2 进行运算得到函数 f2 的第二计算结果更新至第三寄存器，并将函数 f2 的第二计算结果输出至第二次计算中；

根据函数 s_1 对第五寄存器中的值进行运算得到函数 s_1 的第三计算结果，并将函数 s_1 的第三计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第六寄存器中的值、函数 s_1 的第三计算结果和第一预设值 n_1 进行运算得到函数 f1 的第三计算结果，并将函数 f1 的第三计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第三计算结果进行运算得到函数 s_2 的第三计算结果更新至第六寄存器，并将函数 s_2 的第三计算结果输出至函数 f2 和第二次计算中；

根据函数 f2 对函数 s_1 的第三计算结果、函数 s_2 的第三计算结果和第二预设值 n_2 进行运算得到函数 f2 的第三计算结果更新至第五寄存器，并将函数 f2 的第三计算结果输出至第二次计算中；

根据函数 s_1 对第七寄存器中的值进行运算得到函数 s_1 的第四计算结果，并将函数 s_1 的第四计算结果输出至函数 f1 和函数 f2 中；

根据函数 f1 对第八寄存器中的值、函数 s_1 的第四计算结果和第一预设值 n_1 进行运算得到函数 f1 的第四计算结果，并将函数 f1 的第四计算结果输出至函数 s_2 中；

根据函数 s_2 对函数 f1 的第四计算结果进行运算得到函数 s_2 的第四计算结果更新至第八寄存器，并将函数 s_2 的第四计算结果输出至函数 f2 和第二次计算中；

根据函数 f2 对函数 s_1 的第四计算结果、函数 s_2 的第四计算结果和第二预设值 n_2 进行运算得到函数 f2 的第四计算结果更新至第七寄存器，并将函数 f2 的第四计算结果输出至第二次计算中。

8、如权利要求 6 所述的构造方法，其特征在于：所述进行第二次计算，根据函数 $f_3, f_4, \sigma_3, \sigma_4$ 和第一轮结合运算结果对第一寄存器中的值和第四寄存器中的值、第二寄存器中的值和第三寄存器中的值、第五寄存器中的值和第八寄存器中的值以及第六寄存器中的值和第七寄存器中的值分别进行结合运算，得到第二次结合运算结果的步骤，具体为：

根据函数 s_3 对函数 f2 的第一计算结果进行运算得到函数 s_3 的第一计算结果，并将函数 s_3 的第一计算结果输出至函数 f3 和函数 f4 中；

根据函数 s_3 对函数 f2 的第二计算结果进行运算得到函数 s_3 的第二计算结果，并将函数 s_3 的第二计算结果输出至函数 f3 和函数 f4 中；

根据函数 f3 对函数 s_2 的第一计算结果、函数 s_3 的第二计算结果和第三预设值 n_3 进行运算得到函数 f3 的第一计算结果，并将函数 f3 的第一计算结果输出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第一计算结果进行运算得到函数 s_4 的第一计算结果更新至第二寄存器，并将函数 s_4 的第一计算结果输出至函数 f4 和第三次运算中；

根据函数 f4 对函数 s_4 的第一计算结果、函数 s_3 的第二计算结果和第四预设值 n_4 进行运算得到函数 f4 的第一计算结果更新至第三寄存器，并将函数 f4 的第一计算结果输出至第三次运算中；

根据函数 f3 对函数 s_3 的第一计算结果、函数 s_2 的第二计算结果和第三预设值 n_3 进行运算得到函数 f3 的第二计算结果，并将函数 f3 的第二计算结果输出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第二计算结果进行运算得到函数 s_4 的第二计算结果更新至第四寄存器，并将函数 s_4 的第二计算结果输出至函数 f4；

根据函数 f4 对函数 s_4 的第二计算结果、函数 s_3 的第一计算结果和第四预设值 n_4 进行运算得到函数 f4 的第二计算结果更新至第一寄存器，并将函数 f4 的第二计算结果输出至第三次运算中；

根据函数 s_3 对函数 f2 的第三计算结果进行运算得到函数 s_3 的第三计算结果，并将函数 s_3 的第三计算结果输出至函数 f3 和函数 f4 中；

根据函数 s_3 对函数 f2 的第四计算结果进行运算得到函数 s_3 的第四计算结果，并将函数 s_3 的第四计算结果输出至函数 f3 和函数 f4 中；

根据函数 f3 对函数 s_2 的第三计算结果、函数 s_3 的第四计算结果和第三预设值 n_3 进行运算得到函数 f3 的第三计算结果，并将函数 f3 的第三计算结果输出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第三计算结果进行运算得到函数 s_4 的第三计算结果更新至第六寄存器，并将函数 s_4 的第三计算结果输出至函数 f4 和第三次运算中；

根据函数 f4 对函数 s_4 的第三计算结果、函数 s_3 的第四计算结果和第四预设值 n_4 进行运算得到函数 f4 的第三计算结果更新至第七寄存器，并将函数 f4 的第三计算结果输出至第三次运算中；

根据函数 f3 对函数 s_3 的第三计算结果、函数 s_2 的第四计算结果和第三预设值 n_3 进行运算得到函数 f3 的第四计算结果，并将函数 f3 的第四计算结果输出至函数 s_4 中；

根据函数 s_4 对函数 f3 的第四计算结果进行运算得到函数 s_4 的第四计算结果更新至第八寄存器，并将函数 s_4 的第四计算结果输出至函数 f4；

根据函数 f4 对函数 s_4 的第四计算结果、函数 s_3 的第三计算结果和第四预设值 n_4 进行运算得到函数 f4 的第四计算结果更新至第五寄存器，并将函数

f4 的第四计算结果输出至第三次运算中。

9、如权利要求 6 所述的构造方法，其特征在于：所述进行第三次计算，根据函数 $f_5, f_6, \sigma_5, \sigma_6$ 和第二次结合运算结果对第一寄存器中的值和第六寄存器中的值、第二寄存器中的值和第五寄存器中的值、第三寄存器中的值和第八寄存器中的值以及第四寄存器中的值和第七寄存器中的值分别进行结合运算，得到每个块哈希值对应的 8 个寄存器中的更新值的步骤，具体为：

根据函数 s_5 对函数 f4 的第二计算结果进行运算得到函数 s_5 的第一计算结果，并将函数 s_5 的第一计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第一计算结果、函数 s_4 的第三计算结果和第五预设值 n_5 进行运算得到函数 f5 的第一计算结果，并将函数 f5 的第一计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第一计算结果进行运算得到函数 s_6 的第一计算结果更新至第六寄存器，并将函数 s_6 的第一计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第一计算结果、函数 s_5 的第一计算结果和第六预设值 n_6 进行运算得到函数 f6 的第一计算结果更新至第一寄存器中；

根据函数 s_5 对函数 f4 的第四计算结果进行运算得到函数 s_5 的第二计算结果，并将函数 s_5 的第二计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第二计算结果、函数 s_4 的第一计算结果和第五预设值 n_5 进行运算得到函数 f5 的第二计算结果，并将函数 f5 的第二计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第二计算结果进行运算得到函数 s_6 的第二计算结果更新至第二寄存器，并将函数 s_6 的第二计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第二计算结果、函数 s_5 的第二计算结果和第六预设值 n_6 进行运算得到函数 f6 的第二计算结果更新至第五寄存器中；

根据函数 s_5 对函数 f4 的第一计算结果进行运算得到函数 s_5 的第三计算结果，并将函数 s_5 的第三计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第三计算结果、函数 s_4 的第四计算结果和第五

预设值 n_5 进行运算得到函数 f5 的第三计算结果，并将函数 f5 的第三计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第三计算结果进行运算得到函数 s_6 的第三计算结果更新至第八寄存器中，并将函数 s_6 的第三计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第三计算结果、函数 s_5 的第三计算结果和第六预设值 n_6 进行运算得到函数 f6 的第三计算结果更新至第三寄存器中；

根据函数 s_5 对函数 f4 的第三计算结果进行运算得到函数 s_5 的第四计算结果，并将函数 s_5 的第四计算结果输出至函数 f5 和函数 f6 中；

根据函数 f5 对函数 s_5 的第四计算结果、函数 s_4 的第二计算结果和第五预设值 n_5 进行运算得到函数 f5 的第四计算结果，并将函数 f5 的第四计算结果输出至函数 s_6 中；

根据函数 s_6 对函数 f5 的第四计算结果进行运算得到函数 s_6 的第四计算结果更新至第四寄存器中，并将函数 s_6 的第四计算结果输出至函数 f6 中；

根据函数 f6 对函数 s_6 的第四计算结果、函数 s_5 的第四计算结果和第六预设值 n_6 进行运算得到函数 f6 的第四计算结果更新至第七寄存器中。

10、如权利要求 6 所述的构造方法，其特征在于：函数 σ_i 和 f_i 计算公式如下所示：

$\sigma_1=ROTR^3(x_1)\oplus ROTR^7(x_1)\oplus ROTR^{18}(x_1)$；

$\sigma_2=ROTR^3(x_2)\oplus ROTR^{14}(x_2)\oplus ROTR^{25}(x_2)$；

$\sigma_3=ROTR^{10}(x_3)\oplus ROTR^{13}(x_3)\oplus ROTR^{17}(x_3)$；

$\sigma_4=ROTR^{10}(x_4)\oplus ROTR^{15}(x_4)\oplus ROTR^{19}(x_4)$；

$\sigma_5=ROTR^8(x_5)\oplus ROTR^{13}(x_5)\oplus ROTR^{15}(x_5)$；

$\sigma_6=ROTR^8(x_6)\oplus ROTR^{17}(x_6)\oplus ROTR^{19}(x_6)$；

$f_i=(k_i\wedge m_i)\oplus(\neg k_i\wedge n_i)(i=1,3,5)$；

$f_i=(k_i\wedge m_i)\oplus(k_i\wedge n_i)\oplus(m_i\wedge n_i)(i=2,4,6)$；

其中，x1，x2，x3，x4，x5，x6 为输入值，k_i 表示函数 σ_i 的输出，m_i 表示函数 σ_{i-1} 的输出，当 i=1 时，σ_0 是寄存器中的值。

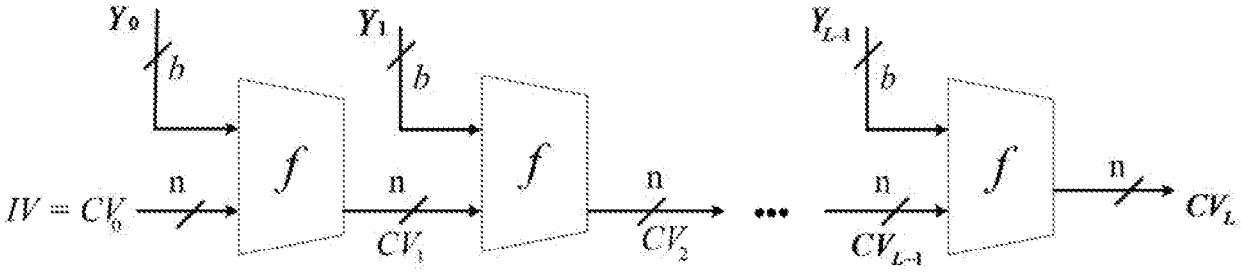
Y_0
Y_1
Y_{L-1}
b
b
b
$IV = CV_0$
n
f
n
CV_1
f
n
CV_2
...
n
CV_{L-1}
f
n
CV_L

图 1

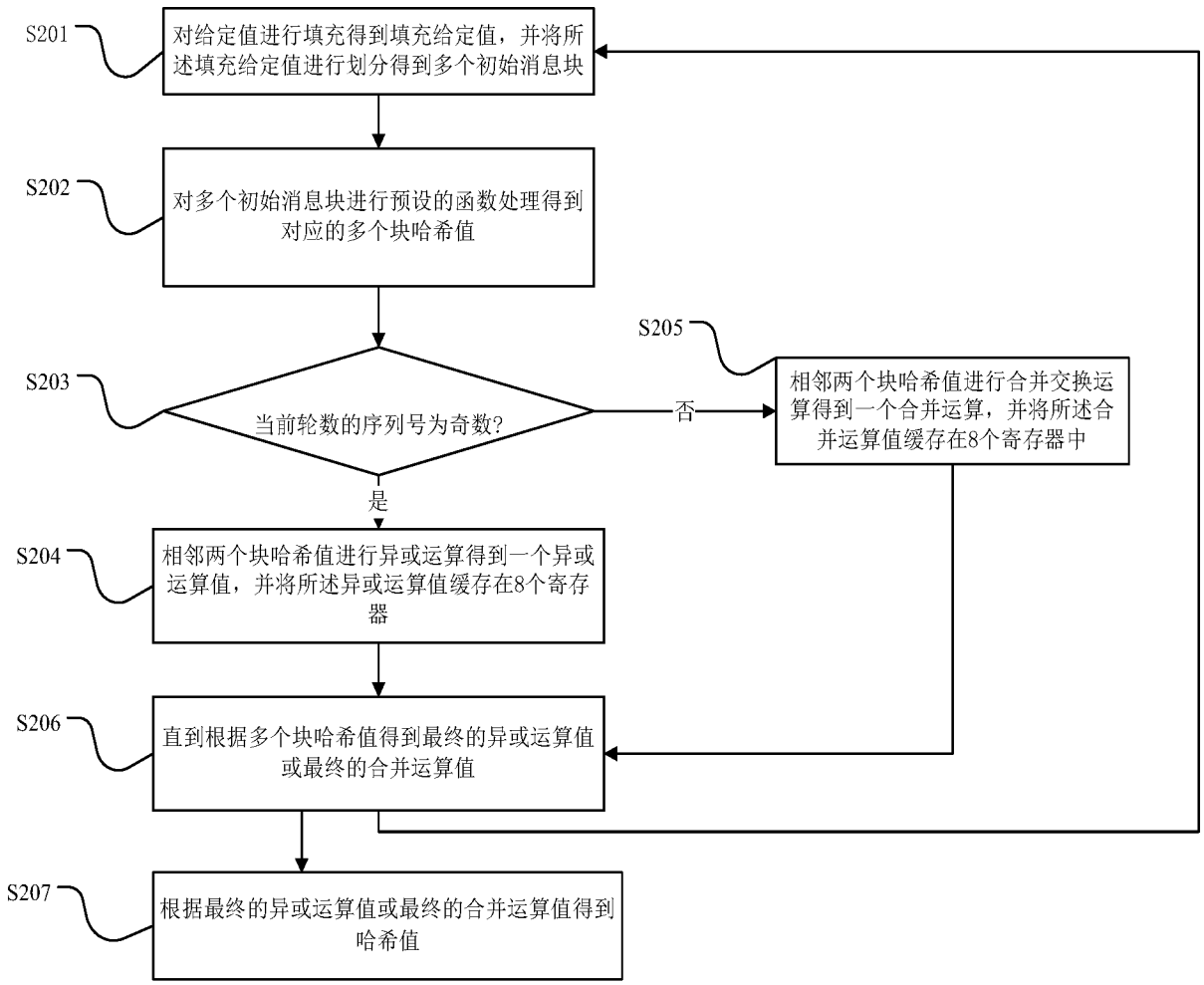
S201
对给定值进行填充得到填充给定值，并将所述填充给定值进行划分得到多个初始消息块
S202
对多个初始消息块进行预设的函数处理得到对应的多个块哈希值
S203
当前轮数的序列号为奇数?
否
S205
相邻两个块哈希值进行合并交换运算得到一个合并运算，并将所述合并运算值缓存在8个寄存器中
是
S204
相邻两个块哈希值进行异或运算得到一个异或运算值，并将所述异或运算值缓存在8个寄存器
S206
直到根据多个块哈希值得到最终的异或运算值或最终的合并运算值
S207
根据最终的异或运算值或最终的合并运算值得到哈希值

图 2

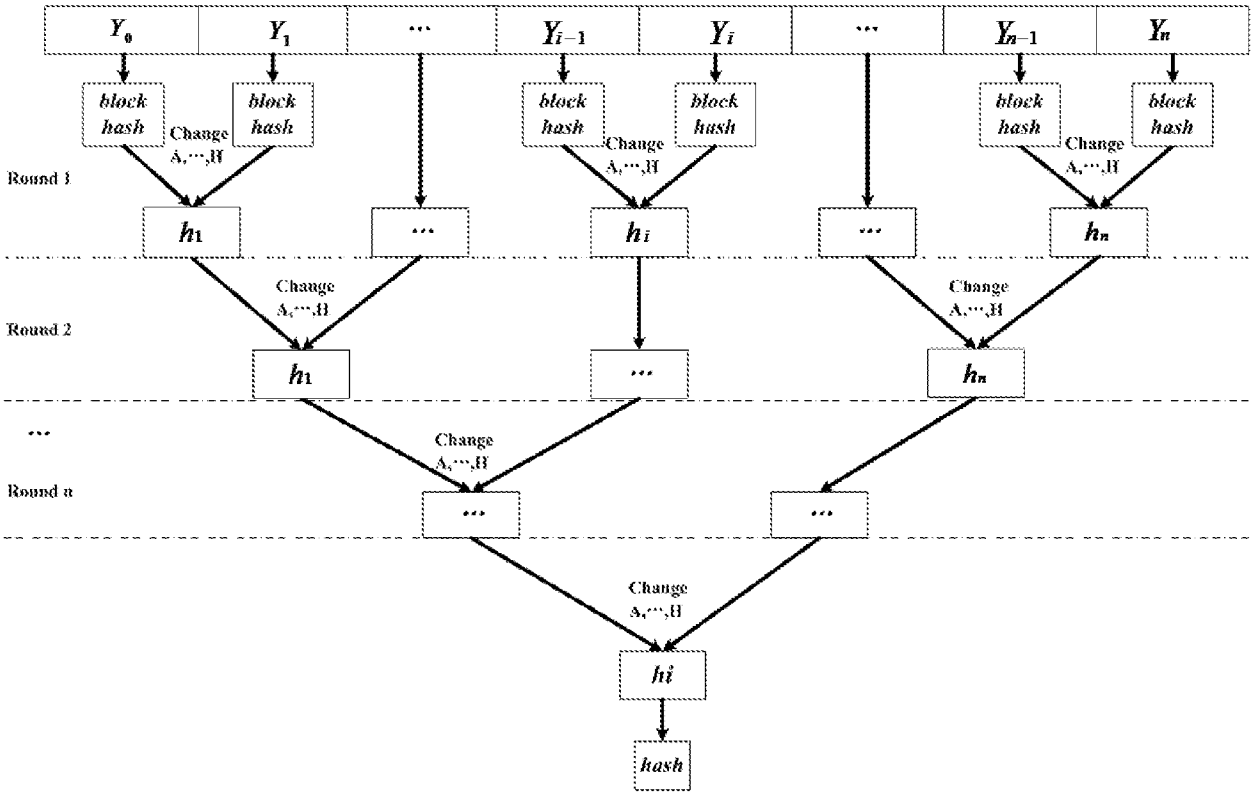
Y0
Y1
…
Yi−1
Yi
…
Yn−1
Yn
block hash
Change A,…,H
Round 1
h1
hi
hn
Round 2
Round n
hi'
hash

图 3

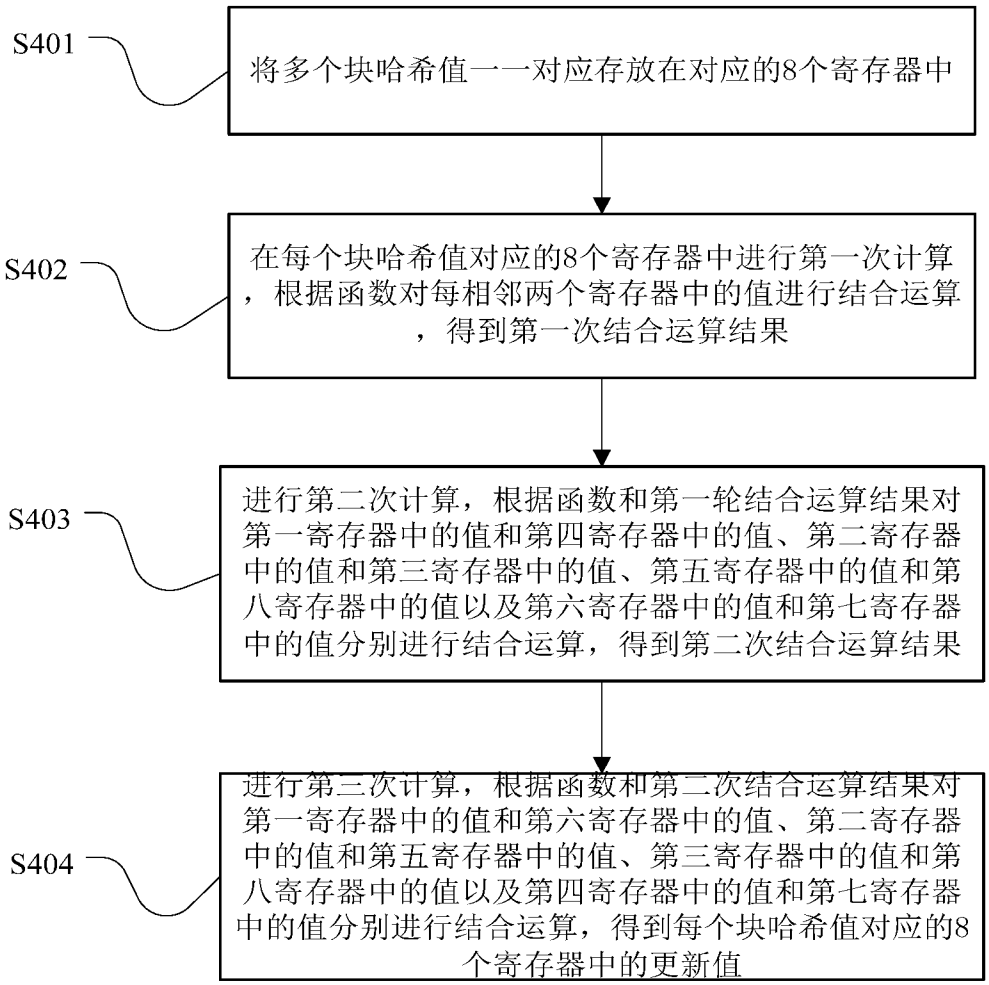
S401
将多个块哈希值一一对应存放在对应的8个寄存器中
S402
在每个块哈希值对应的8个寄存器中进行第一次计算，根据函数对每相邻两个寄存器中的值进行结合运算，得到第一次结合运算结果
S403
进行第二次计算，根据函数和第一轮结合运算结果对第一寄存器中的值和第四寄存器中的值、第二寄存器中的值和第三寄存器中的值、第五寄存器中的值和第八寄存器中的值以及第六寄存器中的值和第七寄存器中的值分别进行结合运算，得到第二次结合运算结果
S404
进行第三次计算，根据函数和第二次结合运算结果对第一寄存器中的值和第六寄存器中的值、第二寄存器中的值和第五寄存器中的值、第三寄存器中的值和第八寄存器中的值以及第四寄存器中的值和第七寄存器中的值分别进行结合运算，得到每个块哈希值对应的8个寄存器中的更新值

图 4

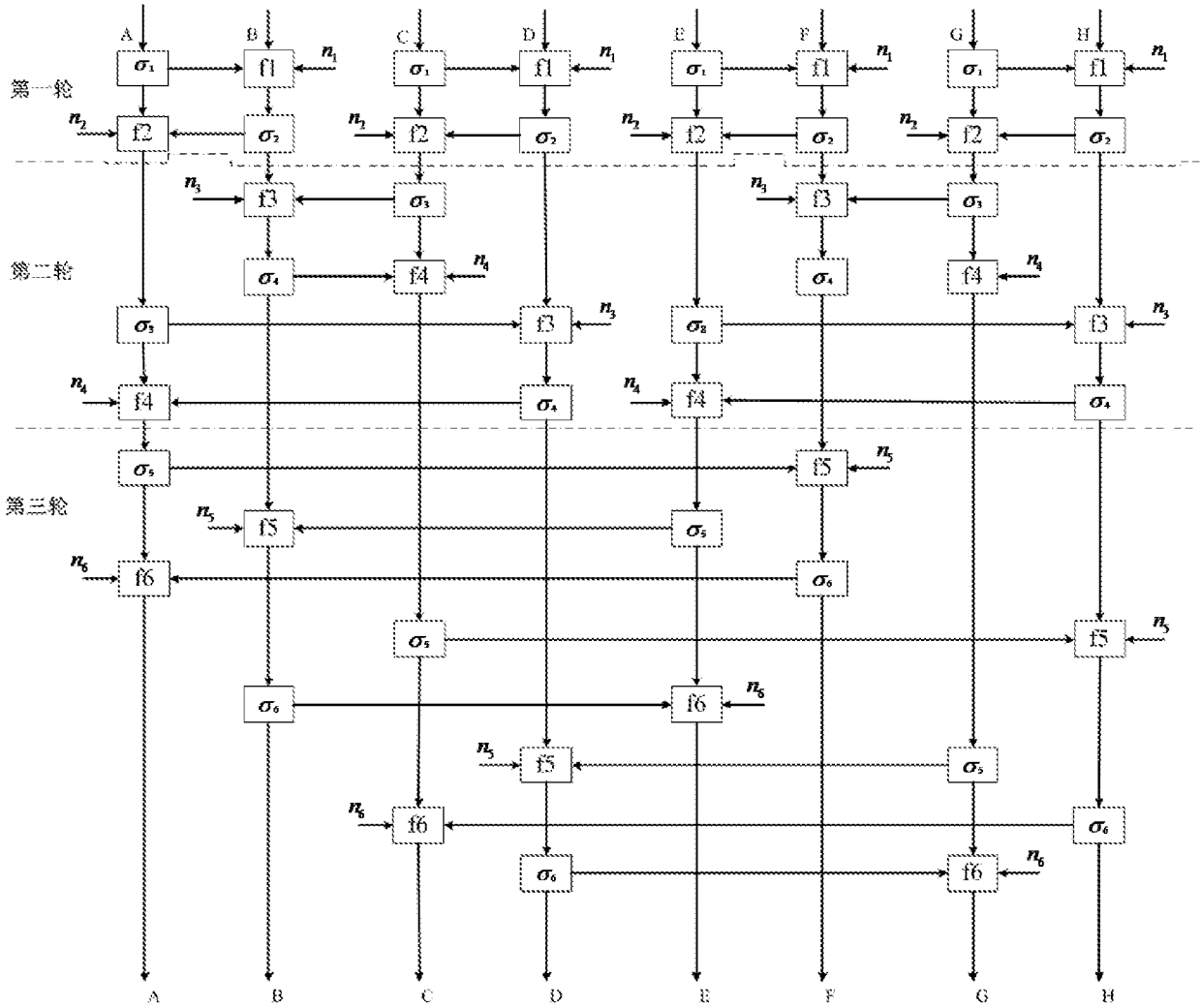
第一轮
第二轮
第三轮
A
B
C
D
E
F
G
H
f1
f2
f3
f4
f5
f6

图 5

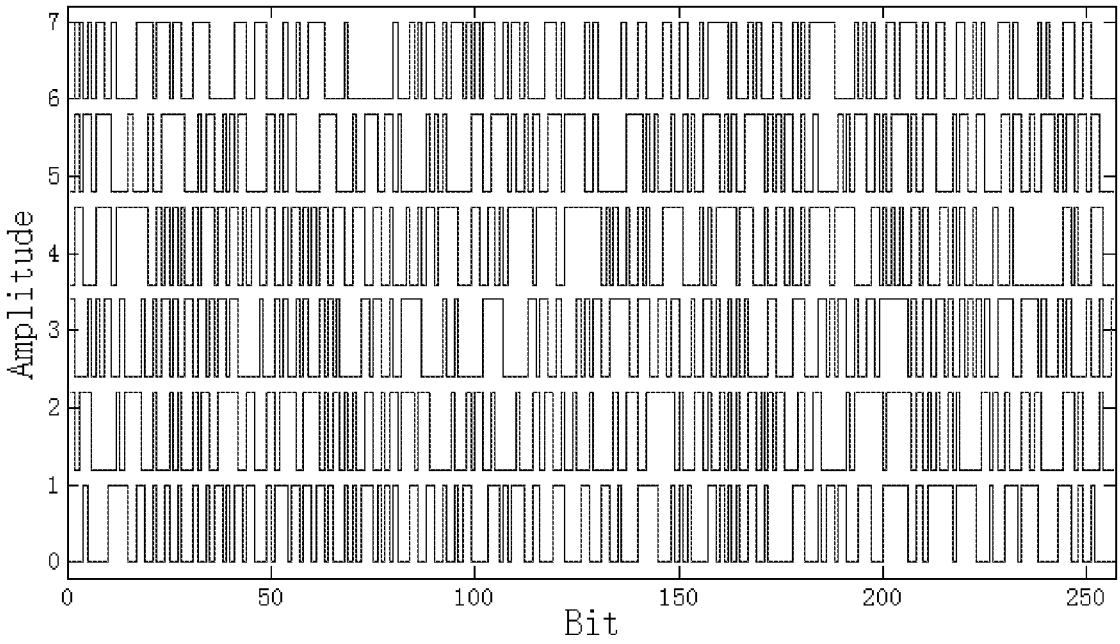
Amplitude
Bit
0
1
2
3
4
5
6
7
0
50
100
150
200
250

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/106780

A. CLASSIFICATION OF SUBJECT MATTER

G06F 19/00 (2011.01) 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)

G06F 19; H04

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)

CNABS, CNTXT, DWPI, SIPOABS, CNKI, IEEE: 哈希, 并行, 块, 奇数, 偶数, 迭代, 轮, 异或, 合并, 交换, hash, block, odd, even, iteration, round, XOR, merge, switch

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	CN 106650240 A (SHENZHEN UNIVERSITY), 10 May 2017 (10.05.2017), claims 1-10	1-10
A	CN 103258035 A (HUAWEI TECHNOLOGIES CO., LTD.), 21 August 2013 (21.08.2013), the whole document	1-10
A	CN 103477341 A (CERTICOM CORP.), 25 December 2013 (25.12.2013), the whole document	1-10
A	US 2008063187 A1 (YOSHIDA, H. et al.), 13 March 2008 (13.03.2008), the whole document	1-10
A	US 2009080646 A1 (YEN, C.H.), 26 March 2009 (26.03.2009), the whole document	1-10

☐ 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
28 July 2017	09 August 2017

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	XU, Feifei Telephone No. (86-10) 62411752

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/106780

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 2008063187 A1	13 March 2008	JP 2007316614 A	06 December 2007
		JP 5000365 B2	15 August 2012
CN 103258035 A	21 August 2013	CN 103258035 B	08 February 2017
CN 103477341 A	25 December 2013	WO 2012135958	11 October 2012
		US 8712039 B2	29 April 2014
		CA 2830779 C	07 March 2017
		CN 103477341 B	18 May 2016
		US 2012257742 A1	11 October 2012
		EP 2601613 A1	12 June 2013
		CA 2830779 A1	11 October 2012
US 2009080646 A1	26 March 2009	TW 200933475 A	01 August 2009

国际检索报告

国际申请号
PCT/CN2016/106780

A. 主题的分类

G06F 19/00(2011.01)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)

G06F19; H04

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））

CNABS,CNTXT,DWPI,SIPOABS,CNKI,IEEE:哈希，并行，块，奇数，偶数，迭代，轮，异或，合并，交换，hash,block,odd,even,iteration,round,XOR，merge,switch

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
E	CN 106650240 A (深圳大学) 2017年 5月 10日 (2017-05-10) 权利要求1-10	1-10
A	CN 103258035 A (华为技术有限公司) 2013年 8月 21日 (2013-08-21) 全文	1-10
A	CN 103477341 A (塞尔蒂卡姆公司) 2013年 12月 25日 (2013-12-25) 全文	1-10
A	US 2008063187 A1 (YOSHIDA HIROTAKA等) 2008年 3月 13日 (2008-03-13) 全文	1-10
A	US 2009080646 A1 (YEN CHIH-HSU) 2009年 3月 26日 (2009-03-26) 全文	1-10

☐ 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
2017年 7月 28日	2017年 8月 9日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 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 许菲菲 电话号码 (86-10)62411752

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/106780

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
US	2008063187	A1	2008年 3月 13日	JP	2007316614	A	2007年 12月 6日
				JP	5000365	B2	2012年 8月 15日
CN	103258035	A	2013年 8月 21日	CN	103258035	B	2017年 2月 8日
CN	103477341	A	2013年 12月 25日	WO	2012135958		2012年 10月 11日
				US	8712039	B2	2014年 4月 29日
					CA2830779	C	2017年 3月 7日
				CN	103477341	B	2016年 5月 18日
				US	2012257742	A1	2012年 10月 11日
				EP	2601613	A1	2013年 6月 12日
					CA2830779	A1	2012年 10月 11日
US	2009080646	A1	2009年 3月 26日		TW200933475	A	2009年 8月 1日