

(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
2020 年 9 月 3 日 (03.09.2020)



(10) 国际公布号
WO 2020/173063 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01)

(21) 国际申请号: PCT/CN2019/102938

(22) 国际申请日: 2019 年 8 月 28 日 (28.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910140294.0 2019年2月26日 (26.02.2019) CN

(71) 申请人: 清华大学(TSINGHUA UNIVERSITY) [CN/
CN]; 中国北京市海淀区清华园清华大学,
Beijing 100084 (CN)。

(72) 发明人: 王小云 (WANG, Xiaoyun); 中国北京
市海淀区清华园清华大学, Beijing 100084

(CN)。 贾珂婷 (JIA, Keting); 中国北京市海
淀区清华园清华大学, Beijing 100084 (CN)。

魏淙泓 (WEI, Congming); 中国北京市海淀区
清华园清华大学, Beijing 100084 (CN)。 孙
悦 (SUN, Yue); 中国北京市海淀区清华园清
华大学, Beijing 100084 (CN)。

(74) 代理人: 北京竹辰知识产权代理事务所 (普
通合伙) (BEIJING ZHUCHEN IP FIRM); 中国北
京市北清路 68 号用友产业园北区 16A 四
层聂鹏, Beijing 100094 (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,

(54) Title: NOVEL PASSWORD-SPECIFIC 4×4 S-BOX CONSTRUCTION METHOD

(54) 发明名称: 一种新型的密码专用的4×4的S盒构造方法

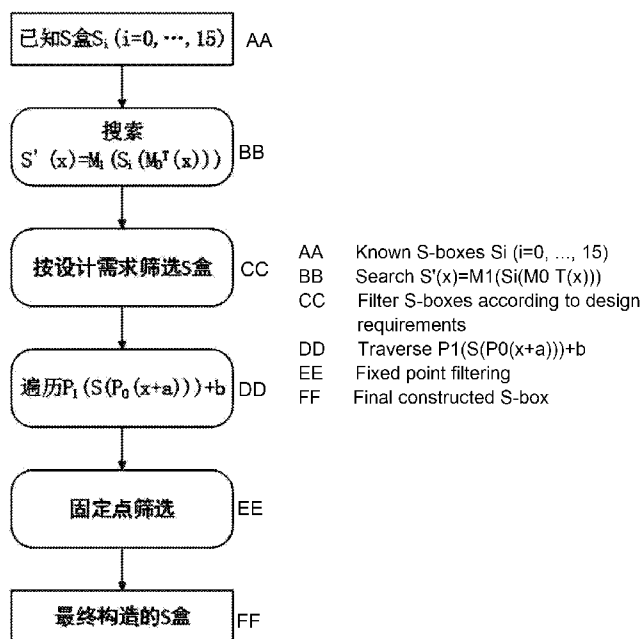


图 1

(57) Abstract: Disclosed in the present invention is a novel password-specific 4 × 4 S-box construction method, comprising: for each affine equivalence (AE) class Gi, selecting a known S-box Si and obtaining a series of new S-boxes according to a preset search method, the search method being $S'(x) = M_1(S_i(M_0^T(x)))$, wherein $i = 0, \dots, 15$, x is the input, S' is the newly obtained S-box, and M_0 and M_1 are 4 × 4 row increment reversible matrices, the values of the rows of the matrix gradually increasing from top to bottom; selecting S-boxes that meet design

JO, JP, KE, KG, KH, 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, 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))。

requirements from the obtained S-boxes; traversing $P_1(S(P_0(x+a)))+b$ for the filtered S-boxes to obtain S-boxes that entirely meet said design requirements, wherein P_0 and P_1 are 4×4 permutation matrices, and a and b are 4-bit vectors; and finally selecting an S box with a fixed point number of 0 as a final target. By means of combining AE class traversal and S-box feature filtering, the present invention can construct a large amount of 4×4 S-boxes having greater password strength.

(57) 摘要: 本发明公开了一种新型的密码专用的 4×4 的 S 盒构造方法, 其包括: 首先对每一个仿射等价(AE)类 G_i , 选用其中已知的 S 盒 S_i , 按照预设搜索方式搜索得到一系列新的 S 盒, 搜索方式为 $S'(x) = M_1(S_i(M_0^T(x)))$, 其中, $i = 0, \dots, 15$; x 为输入, S' 为新搜索到的 S 盒, M_0 和 M_1 为 4×4 的行递增可逆矩阵, 满足矩阵的行的数值从上到下逐渐递增; 然后从搜索到的 S 盒中筛选出满足设计需求的 S 盒; 再然后对筛选后的 S 盒通过遍历 $P_1(S(P_0(x+a)))+b$ 得到全部满足上述设计需求的 S 盒; 其中, P_0 和 P_1 为 4×4 置换矩阵, a 、 b 为 4 比特向量; 最后选择固定点数目为 0 的 S 盒作为最终目标。本发明通过将遍历 AE 类与 S 盒特征筛选结合, 可构造大量具有更高密码强度的 4×4 的 S 盒。

一种新型的密码专用的 4×4 的 S 盒构造方法

本申请要求于 2019 年 2 月 26 日提交中国专利局、申请号为 201910140294.0, 发明名称为“一种新型的密码专用的 4×4 的 S 盒构造方法”的中国专利申请的优先权, 其全部内容通过引用结合在本申请中。

5 技术领域

本发明涉及密码学技术领域, 尤其涉及一种新型的密码专用的 4×4 的 S 盒构造方法。

背景技术

S 盒在现代对称密码设计, 特别是分组密码和哈希函数中具有广泛的应用。在分组密码中, S 盒通常作为唯一的非线性部分提供混淆作用, 保障整个密码算法的安全性。S 盒可看作是 n 比特输入, m 比特输出的布尔函数, 称为 $n \times m$ 的 S 盒。当 n 和 m 很大时, 几乎所有的 S 盒都是非线性的, 且具有良好的密码强度, 但 n 、 m 过大会增加算法的存储量。常见的 S 盒大小是 8×8 或 4×4 。和 8×8 的 S 盒相比, 4×4 的 S 盒在资源有限的环境中更具优势, 因此常应用于轻量级密码算法。目前已知的很多算法, 如 Serpent、PRESENT、RECTANGLE 等, 均采用 4×4 的 S 盒。由于 4×4 的 S 盒的规模较小, 目前已有研究对其差分、线性等特征进行了较深入的分析, 并将其中满足差分为 4, 线性为 4 安全性要求的 S 盒划分为 16 个 AE 类, 记为 $G_0 \sim G_{15}$ 。

构造具有良好的密码强度的 S 盒是分组密码算法设计中的重要环节。目前常见的 S 盒构造方法: 1) 通过数学函数构造 S 盒, 是利用有限域上的模逆或者模幂映射; 2) 进行随机搜索, 筛选满足特定的安全特性的。

通过数学函数构造的 S 盒在差分分布、线性偏差分布和代数次数方面表现较好。但对于规模较小的 4×4 的 S 盒, 除了差分、线性和代数次数这些特征外, 还需要考虑 1 比特差分、1 比特线性等安全特征。通过数学函数构造 S 盒的方法在产生具有更高密码强度的 4×4 的 S 盒方面比较困难。

25 发明内容

针对上述现有技术中存在的不足之处, 本发明提供一种新型的密码专用的 4×4 的 S 盒构造方法, 通过将遍历仿射等价(AE)类与 S 盒特征筛选结合, 构造大量具有更高密码强度的 4×4 的 S 盒。

该新型的密码专用的 4×4 的 S 盒构造方法包括以下步骤:

30 步骤一、对每一个 AE 类 G_i , 选用其中已知的 S 盒 S_i , 按照预设搜索方式搜索得到一系列新的 S 盒, 所述预设搜索方式为 $S'(x) = M_1(S_i(M_0^T(x)))$, 其中, $i=0, \dots, 15$, x 为输入, S' 为新搜索到的 S 盒, M_0 和 M_1 为 4×4 的行递增可逆矩阵, 满足矩阵的行的数值从上到下逐渐递增;

步骤二、从步骤一所搜索到的 S 盒中筛选出满足预设设计需求的 S 盒；

步骤三、对经过步骤二筛选后的 S 盒通过遍历 $P_1(S(P_0(x+a)))+b$ 得到全部满足所述预设设计需求的 S 盒；其中， P_0 和 P_1 为 4×4 置换矩阵，a、b 为 4 比特向量；

步骤四、在步骤三的基础上进一步对遍历到的 S 盒进行筛选，选择固定点数目为 5 0 的 S 盒作为最终目标。

进一步地，每个 AE 类的可选的已知 S 盒的十六进制表示如下：

G0:0123468A5BCF7E9D	G1:0123468A5BCFED97
G2:0123468A5BCF79DE	G3:0123468B5CD7F9EA
G4:0123468B5C9DEA7F	G5:0123468B5CD7AF9E
G6:0123468B5CD79FAE	G7:0123468C59BDEA7F
G8:0123468A5BCFDE79	G9:0123468B59CED7AF
G10:0123468C59BDE7AF	G11:0123468C59DFA7BE
G12:0123468B5C9DE7AF	G13:0123468B59CEDA7F
G14:0123468B59CF7DAE	G15:0123468A5BCF7D9E

进一步地，所述预设设计需求包括差分概率、线性逼近概率、输入输出 1 比特差分个数、输入输出 1 比特线性掩码个数，以及代数次数。

进一步地，所述步骤三中是根据所述步骤二中筛选出的满足所述预设设计需求的每类 S 盒的最小代表元，通过遍历 $P_1(S(P_0(x+a)))+b$ 得到全部满足所述预设设计需求的 S 盒。

相比于现有的数学函数构造 S 盒的方法，本发明提供的新型的密码专用的 4×4 的 S 盒构造方法通过将遍历 AE 类与 S 盒特征筛选结合，可以构造大量具有更高密码强度的 4×4 的 S 盒。

附图说明

图 1 为本发明实施例提供的新型的密码专用的 4×4 的 S 盒构造方法的流程示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本

发明保护的范围。

请参阅图 1, 本实施例提供一种新型的密码专用的 4×4 的 S 盒构造方法, 该新型的密码专用的 4×4 的 S 盒构造方法包括以下步骤:

步骤一、对每一个 AE 类 G_i , 选用其中已知的 S 盒 S_i ($i=0, \dots, 15$), 搜索得到一系列新的 S 盒, 搜索方式为 $S'(x) = M_1(S_i(M_0^T(x)))$, 其中 x 为输入, S' 为新搜索的 S 盒, M_0 和 M_1 为 4×4 的行递增可逆矩阵, 满足矩阵的行的数值从上到下逐渐递增。

每个 AE 类的可选的已知 S 盒的十六进制表示如下:

G0:0123468A5BCF7E9D	G1:0123468A5BCFED97
G2:0123468A5BCF79DE	G3:0123468B5CD7F9EA
G4:0123468B5C9DEA7F	G5:0123468B5CD7AF9E
G6:0123468B5CD79FAE	G7:0123468C59BDEA7F
G8:0123468A5BCFDE79	G9:0123468B59CED7AF
G10:0123468C59BDE7AF	G11:0123468C59DFA7BE
G12:0123468B5C9DE7AF	G13:0123468B59CEDA7F
G14:0123468B59CF7DAE	G15:0123468A5BCF7D9E

步骤二、从步骤一搜索到的 S 盒中筛选出满足设计所要求的安全性(差分概率不小于 2^{-2} 、线性逼近概率不小于 2^{-2} 、输入输出 1 比特差分个数、输入输出 1 比特线性掩码个数、代数次数为 3)的 S 盒, 如满足 1 比特输入输出差分值为 0, 1 比特线性掩码输入输出个数为 4, 代数次数为 3 的 S 盒有两类, 最小代表元分别为 03589CE7ADF46B12 和 03586CB7DAE41F29(类中其它 S 盒可通过代表元经步骤三的遍历公式得到)。

步骤三、对步骤二筛选后的 S 盒通过遍历 $P_1(S(P_0(x+a))) + b$ 得到全部满足上述设计要求的 S 盒。其中 P_0 和 P_1 为 4×4 置换矩阵, a 、 b 为 4 比特向量。

步骤四、在步骤三的基础上进一步对 S 盒进行筛选, 选择固定点数目为 0 的 S 盒作为最终目标。

值得一提的是, 本实施例的上述方案采用的是先搜索 $S'(x) = M_1(S_i(M_0^T(x)))$ 筛选出满足设计所要求的安全性的 S 盒, 再遍历 $P_1(S(P_0(x+a))) + b$ 的方式得到全部 S 盒; 当然也可以直接对 AE 类进行穷搜筛选, 其原理与本实施例的上述方案的原理相同, 但效率较低。

相比于现有的数学函数构造 S 盒的方法, 本实施例提供的新型的密码专用的 4×4 的 S 盒构造方法通过将遍历 AE 类与 S 盒特征筛选结合, 可以构造大量具有更高密码

强度的 4×4 的 S 盒。

此外，需要说明的是，本发明实施例中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域技术人员来说，本发明可有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1.一种新型的密码专用的 4×4 的 S 盒构造方法，其特征在于，所述构造方法包括以下步骤：

步骤一、对每一个仿射等价(AE)类 G_i ，选用其中已知的 S 盒 S_i ，按照预设搜索方式搜索得到一系列新的 S 盒，所述预设搜索方式为 $S'(x) = M_1(S_i(M_0^T(x)))$ ，其中， $i = 0, \dots, 15$ ； x 为输入， S' 为新搜索到的 S 盒， M_0 和 M_1 为 4×4 的行递增可逆矩阵，满足矩阵的行的数值从上到下逐渐递增；

步骤二、从步骤一所搜索到的 S 盒中筛选出满足预设设计需求的 S 盒；

步骤三、对经过步骤二筛选后的 S 盒通过遍历 $P_1(S(P_0(x+a))) + b$ 得到全部满足所述预设设计需求的 S 盒；其中， P_0 和 P_1 为 4×4 置换矩阵， a 、 b 为 4 比特向量；

步骤四、在步骤三的基础上进一步对遍历到的 S 盒进行筛选，选择固定点数目为 0 的 S 盒作为最终目标。

2.如权利要求 1 所述的新型的密码专用的 4×4 的 S 盒构造方法，其特征在于，每个 AE 类的可选的已知 S 盒的十六进制表示如下：

G0:0123468A5BCF7E9D G1:0123468A5BCFED97
G2:0123468A5BCF79DE G3:0123468B5CD7F9EA
G4:0123468B5C9DEA7F G5:0123468B5CD7AF9E
G6:0123468B5CD79FAE G7:0123468C59BDEA7F
G8:0123468A5BCFDE79 G9:0123468B59CED7AF
G10:0123468C59BDE7AF G11:0123468C59DFA7BE
G12:0123468B5C9DE7AF G13:0123468B59CEDA7F
G14:0123468B59CF7DAE G15:0123468A5BCF7D9E。

3.如权利要求 1 所述的新型的密码专用的 4×4 的 S 盒构造方法，其特征在于，所述预设设计需求包括差分概率、线性逼近概率、输入输出 1 比特差分个数、输入输出 1 比特线性掩码个数，以及代数次数。

4.如权利要求 1 所述的新型的密码专用的 4×4 的 S 盒构造方法，其特征在于，所述

步骤三中是根据所述步骤二中筛选出的满足所述预设设计需求的每类 S 盒的最小代表元，通过遍历 $P_1(S(P_0(x+a))) + b$ 得到全部满足所述预设设计需求的 S 盒。

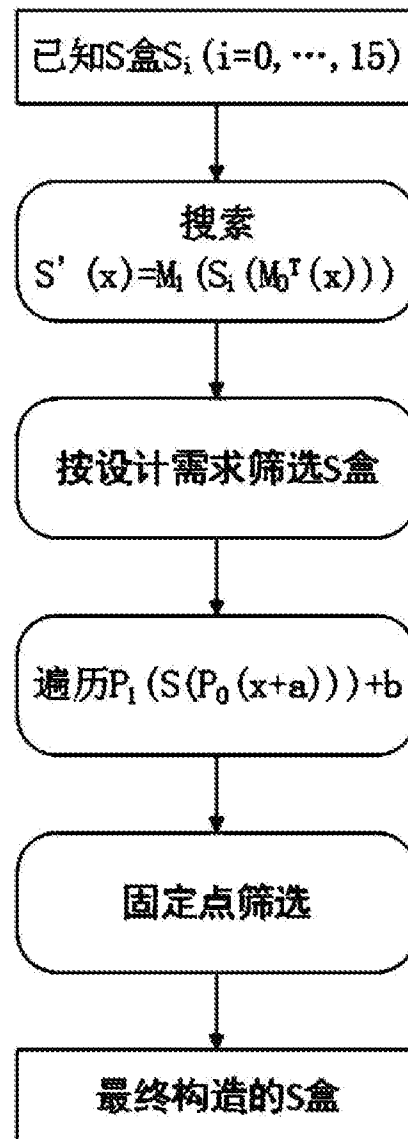


图 1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/102938

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/06(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)

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, CNPAT, CNKI: S盒, 搜索, 遍历, 密码, 筛选, 仿射, S box, affine equivalent, AE, search, password

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109905231 A (TSINGHUA UNIVERSITY) 18 June 2019 (2019-06-18) claims 1-4	1-4
A	CN 105681026 A (INSTITUTE OF COMPUTING TECHNOLOGY, CHINESE ACADEMY OF SCIENCES) 15 June 2016 (2016-06-15) description, paragraphs [0070]-[0107]	1-4
A	CN 106330429 A (CHINA INFORMATION TECHNOLOGY SECURITY EVALUATION CENTER) 11 January 2017 (2017-01-11) entire document	1-4
A	CN 103378968 A (INSTITUTE OF SOFTWARE, CHINESE ACADEMY OF SCIENCES) 30 October 2013 (2013-10-30) entire document	1-4
A	US 2010138462 A1 (EADS SECURE NETWORKS) 03 June 2010 (2010-06-03) entire document	1-4
A	陈基昕 等 (CHEN, Jixin et al.). "CAN总线通信中的改进AES加密算法设计 (Design of Improved AES Encryption Algorithm in CAN Bus Communication)" 单片机与嵌入式系统应用 (Microcontrollers & Embedded Systems), No. 7, 01 July 2018 (2018-07-01), entire document	1-4



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

22 October 2019

Date of mailing of the international search report

29 November 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/102938

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109905231	A	18 June 2019	None			
CN	105681026	A	15 June 2016	None			
CN	106330429	A	11 January 2017	None			
CN	103378968	A	30 October 2013	None			
US	2010138462	A1	03 June 2010	WO	2009004235	A2	08 January 2009
				EP	2168245	A2	31 March 2010
				FR	2917549	A1	19 December 2008

国际检索报告

国际申请号

PCT/CN2019/102938

A. 主题的分类 H04L 9/06 (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) 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, EPDOC, CNPAT, CNKI: S盒, 搜索, 遍历, 密码, 筛选, 仿射, S box, affine equivalent, AE, search, password		
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
PX	CN 109905231 A (清华大学) 2019年 6月 18日 (2019 - 06 - 18) 权利要求1-4	1-4
A	CN 105681026 A (中国科学院计算技术研究所) 2016年 6月 15日 (2016 - 06 - 15) 说明书第[0070]-[0107]段	1-4
A	CN 106330429 A (中国信息安全测评中心) 2017年 1月 11日 (2017 - 01 - 11) 全文	1-4
A	CN 103378968 A (中国科学院软件研究所) 2013年 10月 30日 (2013 - 10 - 30) 全文	1-4
A	US 2010138462 A1 (EADS SECURE NETWORKS) 2010年 6月 3日 (2010 - 06 - 03) 全文	1-4
A	陈基昕 等. "CAN总线通信中的改进AES加密算法设计" 单片机与嵌入式系统应用, 第7期, 2018年 7月 1日 (2018 - 07 - 01), 全文	1-4
☐ 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
2019年 10月 22日		2019年 11月 29日
ISA/CN的名称和邮寄地址		受权官员
中国国家知识产权局 (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		黄欣欣 电话号码 (86-10)53961641

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/102938

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)
CN	109905231	A	2019年 6月 18日	无			
CN	105681026	A	2016年 6月 15日	无			
CN	106330429	A	2017年 1月 11日	无			
CN	103378968	A	2013年 10月 30日	无			
US	2010138462	A1	2010年 6月 3日	W0	2009004235	A2	2009年 1月 8日
				EP	2168245	A2	2010年 3月 31日
				FR	2917549	A1	2008年 12月 19日