(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
2021 年 2 月 25 日 (25.02.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/030958 A1

(51) 国际专利分类号:
G06F 21/75 (2013.01) *G06F 21/81* (2013.01)

(21) 国际申请号: PCT/CN2019/101081

(22) 国际申请日: 2019 年 8 月 16 日 (16.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 深圳市汇顶科技股份有限公司 (**SHENZHEN GOODIX TECHNOLOGY CO., LTD.**) [CN/CN]; 中国广东省深圳市福田保税区腾飞工业大厦B座13层, Guangdong 518045 (CN)。

(72) 发明人: 薛建锋 (**XUE, Jianfeng**); 中国广东省深圳市福田保税区腾飞工业大厦B座13层, Guangdong 518045 (CN)。 杨江 (**YANG, Jiang**); 中国广东省深圳市福田保税区腾飞工业大厦B座13层, Guangdong 518045 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (**LONGSUN LEAD IP LTD.**); 中国北京市海淀区北清路68号院3号楼101, 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, 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,

(54) **Title:** DETECTION CIRCUIT FOR ELECTROMAGNETIC FAULT INJECTION, SECURITY CHIP, AND ELECTRONIC DEVICE

(54) 发明名称: 电磁故障注入的检测电路、安全芯片和电子设备

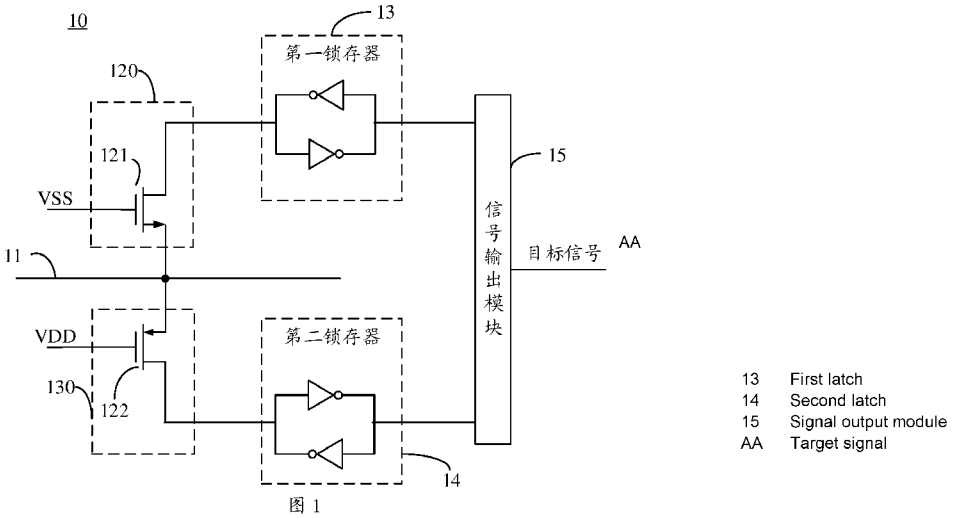

图 1

(57) **Abstract:** Provided are a detection circuit for electromagnetic fault injection, a security chip, and an electronic device. The detection circuit for the electromagnetic fault injection comprises: a shielding layer for shielding interference; at least one group of Metal-Oxide Semiconductor (MOS) transistors, sources of the at least one group of MOS transistors being connected to the shielding layer; at least one latch, drains of the at least one group of MOS transistors being connected to an input end of the at least one latch; and a signal output module, an input end of the signal output module being connected to an output end of the at least one latch. The detection circuit can detect in real time and early warn electromagnetic fault injection in time so as to ensure the robustness and security of the chip. In addition, the detection circuit for the electromagnetic fault injection is designed on the basis of the shielding layer, so that the purposes of effectively simplifying a circuit structure, saving a circuit area, avoiding static power consumption, reducing the circuit cost and the like can be achieved.

WO 2021/030958 A1

[见续页]

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)。

根据细则4.17的声明:
— 关于申请人有权申请并被授予专利(细则4.17(ii))

本国际公布:
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 提供了一种电磁故障注入的检测电路、安全芯片和电子设备，电磁故障注入的检测电路包括：屏蔽层，用于屏蔽干扰；至少一组金属氧化物半导体MOS管，所述至少一组MOS管的源端连接至所述屏蔽层；至少一个锁存器，所述至少一组MOS管的漏端连接至所述至少一个锁存器的输入端；信号输出模块，所述信号输出模块的输入端连接至所述至少一个锁存器的输出端。所述检测电路能够实时检测并及时预警电磁故障注入，以保证芯片的鲁棒性与安全性。此外，基于屏蔽层设计电磁故障注入的检测电路，能够达到有效简化电路结构、节省电路面积、避免出现静态功耗以及降低电路成本等目的。

电磁故障注入的检测电路、安全芯片和电子设备

技术领域

本申请实施例涉及电子领域，并且更具体地，涉及电磁故障注入的检测电路、安全芯片和电子设备。

背景技术

安全芯片可以用于实现用户身份识别与关键数据存储等功能，其被广泛应用于金融领域，是攻击者的重点攻击对象。攻击者通过注入故障可以使芯片工作状态发生错误，进而获取芯片机密数据。

电磁故障注入（Electromagnetic Fault Inject, EMFI）是一种新型的安全芯片攻击手段，攻击者通过将磁场探头至于芯片表面，可以在芯片局部注入电磁辐射，导致电路产生错误时序或异常翻转，进而使得系统进入异常工作状态而造成芯片关键信息泄露。

因此，本领域急需一种检测电路，以实时检测并及时预警电磁故障注入，进而保证芯片的鲁棒性与安全性。

发明内容

本申请实施例提供一种电磁故障注入的检测电路、安全芯片和电子设备，能够实时检测并及时预警电磁故障注入，进而保证芯片的鲁棒性与安全性。

第一方面，提供了一种电磁故障注入的检测电路，包括：

屏蔽层，用于屏蔽干扰；

至少一组金属氧化物半导体 MOS 管，所述至少一组 MOS 管的源端连接至所述屏蔽层；

至少一个锁存器，所述至少一组 MOS 管的漏端连接至所述至少一个锁存器的输入端；

信号输出模块，所述信号输出模块的输入端连接至所述至少一个锁存器的输出端，所述信号输出模块用于基于所述至少一个锁存器的输出端的电压变化生成并输出目标信号，所述目标信号用于指示所述屏蔽层是否存在电磁故障注入；

其中，所述至少一组 MOS 管中的部分或全部 MOS 导通时，所述信号

输出模块用于输出第一目标信号，所述第一目标信号用于指示所述屏蔽层存在电磁故障注入，所述至少一组 MOS 管均断开时，所述信号输出模块用于输出第二目标信号，所述第二目标信号用于指示所述屏蔽层不存在电磁故障注入。

通过所述至少一组 MOS 管能够检测出所述屏蔽层是否出现异常电压，通过所述至少一组MOS管对应的锁存器能够输出所述信号输出模块15可识别的检测信号，进而实时检测并及时预警电磁故障注入，以保证芯片的鲁棒性与安全性。

此外，基于屏蔽层设计电磁故障注入的检测电路，能够达到有效简化电路结构、节省电路面积、避免出现静态功耗以及降低电路成本等目的。

在一些可能的实现方式中，所述至少一组 MOS 管中的第一组 MOS 管的漏端连接至所述至少一个锁存器中的第一锁存器的输入端，所述第一组 MOS 管的栅端连接至地电压，所述第一锁存器的输入端连接至电源电压。

在一些可能的实现方式中，所述检测电路还包括:

第一开关，所述第一锁存器的输入端通过所述第一开关连接至所述电源电压。

在一些可能的实现方式中，所述至少一组 MOS 管中的第二组 MOS 管的漏端连接至所述至少一个锁存器中的第二锁存器的输入端，所述第二组 MOS 管的栅端连接至电源电压，所述第二锁存器的输入端连接至地电压。

在一些可能的实现方式中，所述检测电路还包括:

第二开关;

所述第二锁存器的输入端通过所述第二开关连接至所述地电压。

在一些可能的实现方式中，所述检测电路还包括:

第一反相器;

所述第二锁存器的输出端通过所述第一反相器连接至所述信号输出模块的输入端，所述信号输出模块用于基于所述第一反相器的输出端的电压变化生成并输出所述目标信号。

在一些可能的实现方式中，所述屏蔽层包括:

至少一个金属线;

所述至少一个金属线上设置有至少一个检测节点，所述至少一个检测节点通过所述至少一组 MOS 管连接至所述至少一个锁存器的输入端。

在一些可能的实现方式中，所述至少一组 MOS 管为多组 MOS 管，所述多组 MOS 管中的不同组 MOS 管的漏端连接至不同锁存器的输入端。

在一些可能的实现方式中，所述至少一组 MOS 管为多组 MOS 管，所述多组 MOS 管中的不同组 MOS 管包括不同类型的 MOS 管。

在一些可能的实现方式中，所述至少一个锁存器中的每个锁存器包括：

第二反相器和第三反相器；

所述第二反相器的输入端连接至所述第三反相器的输出端，所述第二反相器的输出端连接至所述第三反相器的输入端，所述第二反相器的输入端或所述第三反相器的输入端为锁存器的输入端。

在一些可能的实现方式中，所述信号输出模块包括第一输出端和第二输出端，所述第一输出端的输出与所述第二输出端的输出反相。

在一些可能的实现方式中，所述信号输出模块为 D 触发器。

第二方面，提供了一种安全芯片，包括：

发射器，用于生成并输出第一信号；

屏蔽层；

接收器，所述接收器通过所述屏蔽层连接至所述发射器，所述接收器用于通过所述屏蔽层接收所述发射器输出的第一信号，并基于所述第一信号输出第二信号；

数字处理器，所述数字处理器分别连接至所述发射器和所述接收器，所述数字处理器用于接收所述发射器输出的所述第一信号和所述接收器输出的所述第二信号，并基于所述第一信号和所述第二信号确定所述屏蔽层是否被破坏；

第一方面或第一方面中任一可能的实现方式中所述的检测电路；

其中，所述屏蔽层为所述的检测电路中的屏蔽层。

第三方面，提供了一种电子设备，包括第二方面所述的安全芯片。

附图说明

图 1 是本申请实施例的电磁故障注入的检测电路的示意性电路图。

图 2 是图 1 所示的检测电路的变形结构的示意性电路图。

图 3 是本申请实施例的信号输出模块的示意性结构图。

图 4 是本申请实施例的安全芯片的示意性结构图。

具体实施方式

下面将结合附图，对本申请实施例中的技术方案进行描述。

图 1 是本申请实施例的电磁故障注入的检测电路 10 的示意性电路图。

请参见图 1，所述检测电路 10 可以包括屏蔽层 11、至少一组金属氧化物半导体（Metal-Oxide Semiconductor，MOS）管、至少一个锁存器以及信号输出模块 15。

屏蔽层 11 用于屏蔽干扰，其可以是现有的安全芯片的的屏蔽层，也可以是其他任意器件或部件的屏蔽层，所述至少一组 MOS 管的源端连接至所述至少一个锁存器的输入端；所述信号输出模块 15 的输入端连接至所述至少一个锁存器的输出端，所述信号输出模块 15 用于基于所述至少一个锁存器的输出端的电压变化生成并输出目标信号，所述目标信号用于指示所述屏蔽层 11 是否存在电磁故障注入；其中，所述至少一组 MOS 管中的部分或全部 MOS 导通时，所述信号输出模块 15 用于输出第一目标信号，所述第一目标信号用于指示所述屏蔽层 11 存在电磁故障注入，所述至少一组 MOS 管均断开时，所述信号输出模块 15 用于输出第二目标信号，所述第二目标信号用于指示所述屏蔽层 11 不存在电磁故障注入。

换言之，所述信号输出模块 15 可以配置为在所述至少一组 MOS 管中的部分或全部 MOS 导通的情况下输出第一目标信号以及在所述至少一组 MOS 管均断开的情况下输出第二目标信号，所述第一目标信号用于指示所述屏蔽层 11 存在电磁故障注入，所述第二目标信号用于指示所述屏蔽层 11 不存在电磁故障注入。

通过所述至少一组 MOS 管能够检测出所述屏蔽层是否出现异常电压，通过所述至少一组 MOS 管对应的锁存器能够输出所述信号输出模块 15 可识别的检测信号，进而实时检测并及时预警电磁故障注入，以保证芯片的鲁棒性与安全性。

此外，基于屏蔽层设计电磁故障注入的检测电路，能够达到有效简化电路结构、节省电路面积、避免出现静态功耗以及降低电路成本等目的。

在本申请的一些实施例中，所述至少一组 MOS 管中的第一组 MOS 管 120 的漏端可连接至所述至少一个锁存器中的第一锁存器的输入端，所述第一组 MOS 管 120 的栅端可连接至地电压，所述第一锁存器的输入端可连接

至电源电压。所述第一组 MOS 管 120 可用于检测所述屏蔽层 11 是否出现电压值低于地电压的异常现象。

请继续参见图 1，以所述第一组 MOS 管 120 包括第一 NMOS 管 121 为例，所述第一 NMOS 管 121 的栅极连接至地电压，所述第一 NMOS 管 121 的源极连接至屏蔽层 11，所述第一 NMOS 管 121 的漏端连接至第一锁存器 13。

假设所述屏蔽层 11 存在电磁故障注入，所述屏蔽层 11 会产生感应电流，使得所述屏蔽层 11 的电压发生变化，进而导致所述屏蔽层 11 的电压范围超出 VSS~VDD，此时，若 VSS 与所述屏蔽层 11 的电压的差值大于或等于所述第一 NMOS 管 121 的阈值电压，则所述第一 NMOS 管 121 导通，进而导致所述第一锁存器 13 的输入端的电压下降，所述第一锁存器 13 的输入端的电压下降导致所述第一锁存器 13 的输出端的电压上升，所述信号输出模块 15 根据所述第一锁存器 13 的输出端的电压变化，输出用于指示所述第一目标信号，以指示所述屏蔽层 11 存在电磁故障注入。

图 2 是图 1 所示的检测电路的具体实现方式的示意性电路图。

请参见图 2，所述检测电路 10 还可包括第一开关 16。

例如，所述第一锁存器 13 的输入端通过所述第一开关 16 连接至所述电源电压 VDD，以保证所述第一锁存器的输入端处于高电压状态，例如在所述第一 NMOS 管 121 导通前，通过导通所述第一开关 16 使得所述第一锁存器 13 的输入端的电压等于电源电压。

在本申请的另一些实施例中，所述至少一组 MOS 管中的第二组 MOS 管 130 的漏端连接至所述至少一个锁存器中的第二锁存器的输入端，所述第二组 MOS 管 130 的栅端连接至电源电压，所述第二锁存器的输入端连接至地电压。所述第二组 MOS 管 130 可用于检测所述屏蔽层 11 是否出现电压值高于电源电压的异常现象。

请继续参见图 1，以所述第二组 MOS 管 130 包括第一 PMOS 管 122 为例，所述第一 PMOS 管 122 的栅极连接至电源电压，所述第一 PMOS 管 122 的源极连接至屏蔽层 11，所述第一 PMOS 管 122 的漏端连接至第二锁存器 14。

假设所述屏蔽层 11 存在电磁故障注入，所述屏蔽层 11 会产生感应电流，使得所述屏蔽层 11 的电压发生变化，进而导致所述屏蔽层 11 的电压范围超

出 VSS~VDD，此时，若所述屏蔽层 11 的电压与所述 VDD 的差值大于或等于所述第一 PMOS 管 122 的阈值电压，则所述第一 PMOS 管 122 导通，进而导致所述第二锁存器 14 的输入端的电压上升，所述第二锁存器 14 的输入端的电压上升导致所述第二锁存器 14 的输出端的电压下降，所述信号输出模块 15 了根据所述第二锁存器 14 的输出端的电压变化，输出用于指示所述第一目标信号，以指示所述屏蔽层 11 存在电磁故障注入。

请继续参见图 2，所述检测电路 10 还可包括第二开关 17。

例如，所述第二锁存器 14 的输入端通过所述第二开关 17 连接至所述地电压，以保证所述第二锁存器 14 的输入端在所述第一 PMOS 管 122 导通前处于地电压状态，例如在所述第一 PMOS 管 122 导通前，通过导通所述第二开关 17 使得所述所述第二锁存器 14 的输入端的电压等于地电压。

请继续参见图 2，所述检测电路 10 还可包括第一反相器 18。

例如，所述第二锁存器 14 的输出端通过所述第一反相器 18 连接至所述信号输出模块 15 的输入端，所述信号输出模块 15 用于基于所述第一反相器 18 的输出端的电压变化生成并输出所述目标信号。由此，所述信号检测电路 10 同时包括所述第一组 MOS 管 120 和所述第二组 MOS 管 130 时，通过检测所述第一锁存器 13 的上升沿和所述第一反相器 18 的上升沿生成所述目标信号，避免了同时检测所述第一锁存器 13 上升沿和所述第二锁存器 14 的下降沿，进而可以降低所述信号输出模块 15 的复杂度。

请继续参见图 2，所述第二锁存器 14 可包括第二反相器 181 和第三反相器 182，所述第二反相器 181 的输入端连接至所述第三反相器 182 的输出端，所述第二反相器 181 的输出端连接至所述第三反相器 182 的输入端，所述第二组 MOS 管 130 的漏端可以连接至所述第二反相器 181 的输入端，所述第二反相器 181 的输出端连接至所述信号输出模块 15。

需要说明的是，所述至少一组 MOS 管中每组 MOS 管可以仅包括一个 MOS 管，也可以包括多个 MOS 管，本申请实施例对此不做具体限定。例如，请继续参见图 1，所述第一组 MOS 管 120 可以仅第一 NMOS 管 121，所述第二组 MOS 管 130 可以仅包括所述第一 PMOS 管 122。又例如，请继续参见图 2，所述第一组 MOS 管 120 还可以包括第二 NMOS 管 131 和第三 NMOS 管 141，所述第二组 MOS 管 130 还可以包括第二 PMOS 管 132 和第三 PMOS 管 142。当然，图 1 和图 2 仅为本申请的示例，不应理解为对本申请的限制，

在其他可替代实施例中，所述第一组 MOS 管 120 和所述第二组 MOS 管 130 可以分别包括其它数量的 MOS 管。

在本申请的一些实施例中，所述屏蔽层 11 可包括至少一个金属线；所述至少一个金属线上设置有至少一个检测节点，所述至少一个检测节点通过所述至少一组 MOS 管连接至所述至少一个锁存器的输入端。

以所述至少一个金属线中的第一金属线为例，所述第一金属线可以设置有至少一个第一检测节点和/或至少一个第二检测节点，所述至少一组 MOS 管中的第一组 MOS 管 120 通过所述至少一个第一检测节点连接至所述至少一个锁存器中的第一锁存器，所述至少一组 MOS 管中的第二组 MOS 管 130 可通过所述至少一个第二检测节点连接至所述至少一个锁存器中的第二锁存器。

在本申请的一些实施例中，所述至少一组 MOS 管中同一组 MOS 管中的所有 MOS 管的漏端均连接至同一锁存器的输入端。

例如，所述至少一组 MOS 管中的不同组 MOS 管的漏端连接至不同的锁存器的输入端。结合图 2 来说，所述第一组 MOS 管 120 的漏端可连接至所述第一锁存器 13 的输入端，所述第二组 MOS 管的漏端可连接至所述第二锁存器 14 的输入端。

又例如，所述至少一组 MOS 管中的一部分组 MOS 管连接至所述第一第一锁存器 13，所述至少一组 MOS 管中的另一部分组 MOS 管连接至所述第二锁存器 14。其中，所述一部分组 MOS 管可包括 MOS 管类型相同的至少一组 MOS 管，所述另一部分组 MOS 管可包括 MOS 管类型相同的至少一组 MOS 管。所述一部分组 MOS 管中的 MOS 管的 MOS 管类型和所述另一部分组 MOS 管中的 MOS 管的 MOS 管类型可以相同，也可以不同，本申请对此不做具体限定。

在本申请的一些实施例中，所述至少一组 MOS 管为多组 MOS 管，所述多组 MOS 管中的不同组 MOS 管包括不同类型的 MOS 管。

应理解，所述不同类型的 MOS 管包括但不限于“N 型”MOS 管（NMOSFET）与“P 型”MOS 管（PMOSFET）。其中，“N 型”MOS 管和“P 型”MOS 管当作开关使用时，“N 型”MOS 管（衬底 PN 结指向内的 MOS 管或电流流出的 MOS 管）的栅端接高电平时导通，接低电平时关断；“P 型”MOS 管（PN 结指向外的 MOS 管或电流流入的 MOS 管）的栅端接高电平时关断，

接低电平时导通。

在本申请的一些实施例中，所述至少一组 MOS 管包括多个不同类型的 MOS 管。

例如，所述至少一组 MOS 管中不同类型的 MOS 管连接至不同锁存器的输入端。结合图 2 来说，所述至少一组 MOS 管中的 NMOS 管可连接至所述第一锁存器 13 的输入端，所述至少一组 MOS 管中的 PMOS 管的漏端可连接至所述第二锁存器 14 的输入端。

图 3 是本申请实施例的信号输出模块的示意性结构图。

请参见图 3，所述信号输出模块 15 可为 D 触发器。

例如，所述 D 触发器的重置（RESET）端 B 连接至重置信号 W，例如所述重置信号 W 可以是与所述第一开关 16 的控制信号或第二开关 17 的控制信号；所述 D 触发器的 D 端连接至 VDD；所述 D 触发器的检测端 A 连接至所述第一锁存器 13 的输出端或第一反相器 18 的输出端，用于接收检测信号，所述 D 触发器的输出端 Q 输出目标信号（即预警（ALARM）信号）。当然，所述信号生成电路 13 还可以是其他器件，例如比较器。

在本申请的一些实施例中，所述信号输出模块 15 可包括第一输出端和第二输出端，所述第一输出端的输出与所述第二输出端的输出反相。即所述信号输出模块 15 输出的目标信号可以是差分信号。

图 4 是本申请实施例的安全芯片 20 的示意性结构图。

请参见图 4，所述安全芯片 20 可包括发射器 21、屏蔽层 22、接收器 23 以及数字处理器 24。

其中，所述屏蔽层 22 可以是图 1 或图 2 所示的屏蔽层 11，所述发射器 21 用于生成并输出第一信号；所述接收器 23 可通过所述屏蔽层 11 连接至所述发射器 21，所述接收器 23 可用于通过所述屏蔽层 11 接收所述发射器 21 输出的第一信号，并基于所述第一信号输出第二信号；所述数字处理器 24 分别连接至所述发射器 21 和所述接收器 23，所述数字处理器 24 可用于接收所述发射器 21 输出的所述第一信号和所述接收器 23 输出的所述第二信号，并基于所述第一信号和所述第二信号确定所述屏蔽层 11 是否被破坏（例如，物理损坏）。

换言之，所述安全芯片 20 可以包括被保护的芯片主体电路、所述芯片主体电路的屏蔽层 22、用于检测所述屏蔽层 22 是否被破坏的电路以及用于

检测所述屏蔽层 22 是否存在电磁故障注入的电测电路 10。其中，所述屏蔽层 11 可用作用于检测所述屏蔽层 22 是否被破坏的电路和所述检测电路 10 中的器件或元件。

本申请还提供了一种电子设备，其可包括图 4 所示的安全芯片 20。所述电子设备可以包括上文所述的安全芯片。例如，例如，智能手机、笔记本电脑、平板电脑、游戏设备等便携式或移动计算设备，以及电子数据库、汽车、银行自动柜员机（Automated Teller Machine，ATM）等其他电子设备。但本申请实施例对此并不限定。

应理解，图 1 至图 4 仅为本申请的示例，不应理解为对本申请的限制。

例如，检测电路 10 还可以包括阈值判决模块。

例如，所述至少一个锁存器的输出端通过所述阈值判决模块连接至所述信号输出模块 15，所述阈值判决模块用于放大所述至少一个锁存器输出的信号，并将放大后的信号发送至所述信号输出模块 15。例如所述阈值判决模块可包括第四反相器和第五反相器，所述至少一个锁存器的输出端通过第四反相器连接至所述第五反相器的一端，所述第五反相器的另一端连接至所述信号输出模块 15。其中所述第四反相器的翻转阈值可小于所述第五反相器的翻转阈值。例如所述第四反相器的翻转阈值为 0.3，所述第五反相器的翻转阈值为 0.8，即通过降低所述第四反相器的翻转阈值提升所述检测电路 10 的灵敏度，并通过增大所述第五反相器的翻转阈值，保证所述检测电路 10 的稳定性。应理解，上述 0.3 和 0.8 仅为示例，本申请对所述第四反相器的翻转阈值和所述第五反相器的翻转阈值不做具体限定。通过所述阈值判决模块的配合，可以提高电磁故障注入的检测精度，进一步提升所述检测电路 10 的灵敏度。

在本申请所提供的几个实施例中，应该理解到，所揭露的电路、支路和模块，可以通过其它的方式实现。例如，以上所描述的支路是示意性的，例如，该模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个模块可以结合或者可以集成到一个支路，或一些特征可以忽略，或不执行。

所述集成的模块如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方

案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以该权利要求的保护范围为准。

权利要求

1. 一种电磁故障注入的检测电路，其特征在于，包括:

屏蔽层，用于屏蔽干扰;

至少一组金属氧化物半导体 MOS 管，所述至少一组 MOS 管的源端连接至所述屏蔽层;

至少一个锁存器，所述至少一组 MOS 管的漏端连接至所述至少一个锁存器的输入端;

信号输出模块，所述信号输出模块的输入端连接至所述至少一个锁存器的输出端，所述信号输出模块用于基于所述至少一个锁存器的输出端的电压变化生成并输出目标信号，所述目标信号用于指示所述屏蔽层是否存在电磁故障注入;

其中，所述至少一组 MOS 管中的部分或全部 MOS 导通时，所述信号输出模块用于输出第一目标信号，所述第一目标信号用于指示所述屏蔽层存在电磁故障注入，所述至少一组 MOS 管均断开时，所述信号输出模块用于输出第二目标信号，所述第二目标信号用于指示所述屏蔽层不存在电磁故障注入。

2. 根据权利要求 1 所述的检测电路，其特征在于，所述至少一组 MOS 管中的第一组 MOS 管的漏端连接至所述至少一个锁存器中的第一锁存器的输入端，所述第一组 MOS 管的栅端连接至地电压，所述第一锁存器的输入端连接至电源电压。

3. 根据权利要求 2 所述的检测电路，其特征在于，所述检测电路还包括:

第一开关，所述第一锁存器的输入端通过所述第一开关连接至所述电源电压。

4. 根据权利要求 1 至 3 中任一项所述的检测电路，其特征在于，所述至少一组 MOS 管中的第二组 MOS 管的漏端连接至所述至少一个锁存器中的第二锁存器的输入端，所述第二组 MOS 管的栅端连接至电源电压，所述第二锁存器的输入端连接至地电压。

5. 根据权利要求 4 所述的检测电路，其特征在于，所述检测电路还包括:

第二开关;

所述第二锁存器的输入端通过所述第二开关连接至所述地电压。

6. 根据权利要求 5 所述的检测电路，其特征在于，所述检测电路还包括：

第一反相器；

所述第二锁存器的输出端通过所述第一反相器连接至所述信号输出模块的输入端，所述信号输出模块用于基于所述第一反相器的输出端的电压变化生成并输出所述目标信号。

7. 根据权利要求 1 至 6 中任一项所述的检测电路，其特征在于，所述屏蔽层包括：

至少一个金属线；

所述至少一个金属线上设置有至少一个检测节点，所述至少一个检测节点通过所述至少一组 MOS 管连接至所述至少一个锁存器的输入端。

8. 根据权利要求 1 至 7 中任一项所述的检测电路，其特征在于，所述至少一组 MOS 管为多组 MOS 管，所述多组 MOS 管中的不同组 MOS 管的漏端连接至不同锁存器的输入端。

9. 根据权利要求 1 至 8 中任一项所述的检测电路，其特征在于，所述至少一组 MOS 管为多组 MOS 管，所述多组 MOS 管中的不同组 MOS 管包括不同类型的 MOS 管。

10.根据权利要求 1 至 9 中任一项所述的检测电路，其特征在于，所述至少一个锁存器中的每个锁存器包括：

第二反相器和第三反相器；

所述第二反相器的输入端连接至所述第三反相器的输出端，所述第二反相器的输出端连接至所述第三反相器的输入端，所述第二反相器的输入端或所述第三反相器的输入端为锁存器的输入端。

11. 根据权利要求 1 至 10 中任一项所述的检测电路，其特征在于，所述信号输出模块包括第一输出端和第二输出端，所述第一输出端的输出与所述第二输出端的输出反相。

12. 根据权利要求 1 至 11 中任一项所述的检测电路，其特征在于，所述信号输出模块为 D 触发器。

13. 一种安全芯片，其特征在于，包括：

发射器，用于生成并输出第一信号；

屏蔽层；

接收器，所述接收器通过所述屏蔽层连接至所述发射器，所述接收器用

于通过所述屏蔽层接收所述发射器输出的第一信号，并基于所述第一信号输出第二信号；

数字处理器，所述数字处理器分别连接至所述发射器和所述接收器，所述数字处理器用于接收所述发射器输出的所述第一信号和所述接收器输出的所述第二信号，并基于所述第一信号和所述第二信号确定所述屏蔽层是否被破坏；

根据权利要求 1 至 12 中任一项所述的检测电路；

其中，所述屏蔽层为所述的检测电路中的屏蔽层。

14. 一种电子设备，其特征在于，包括：

根据权利要求 13 所述的安全芯片。

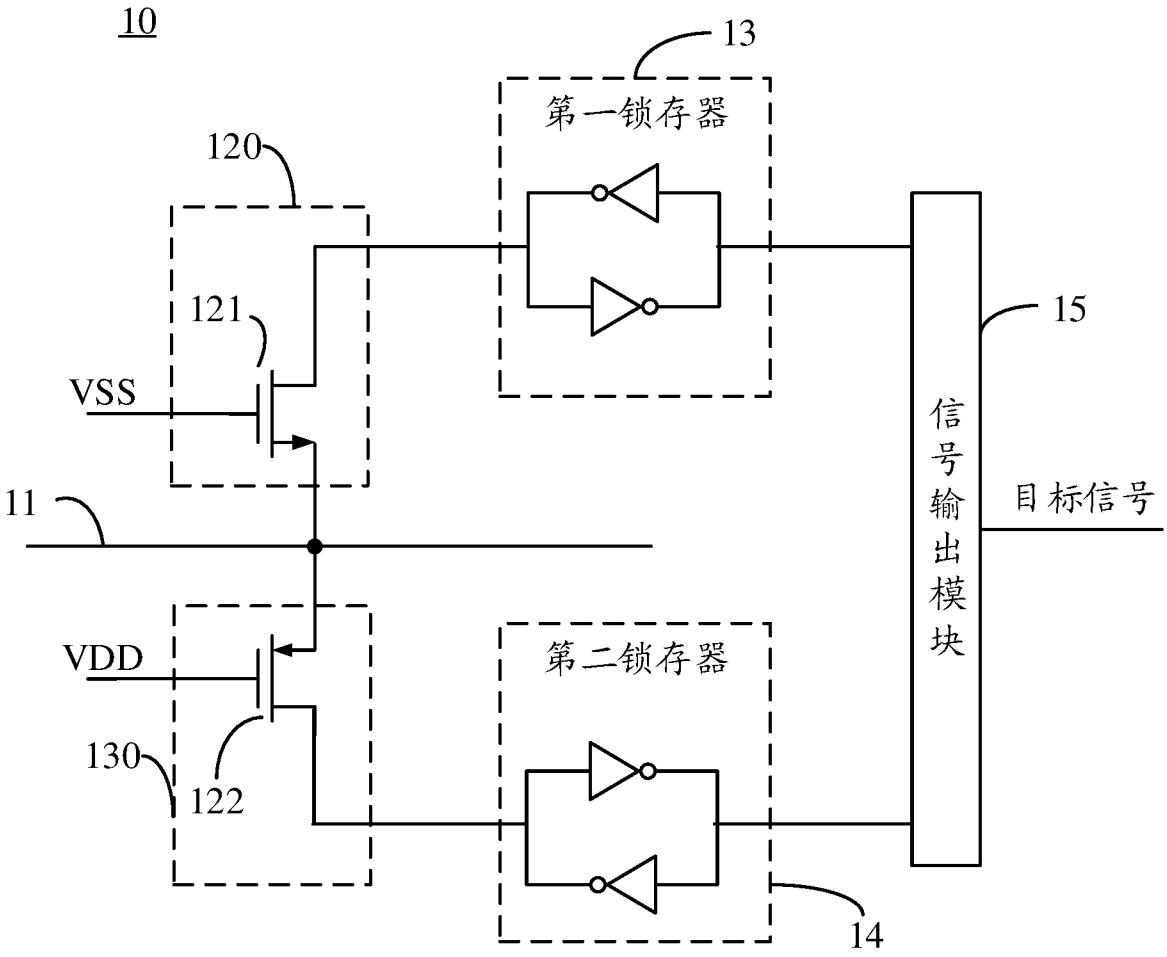

图 1

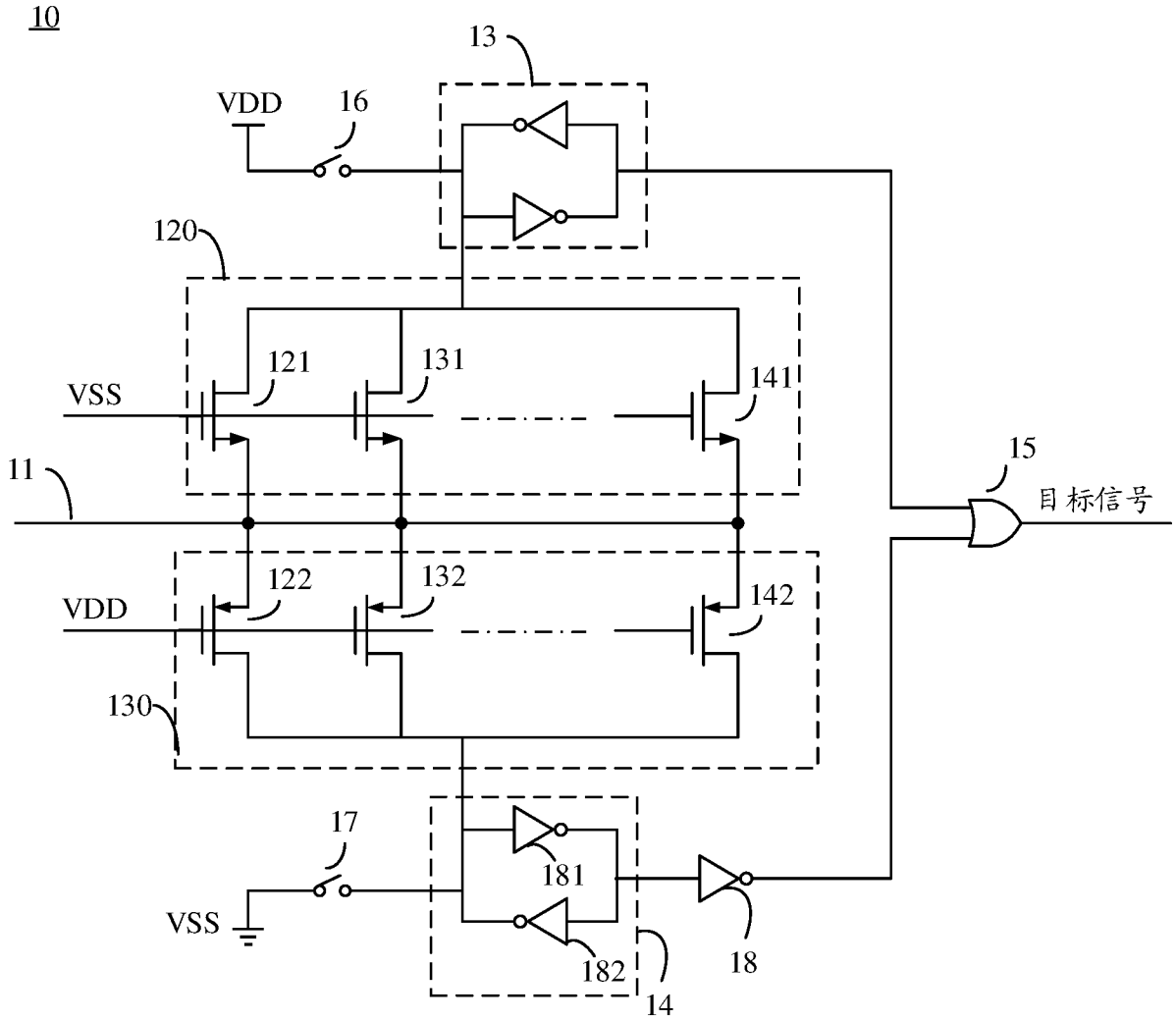
10
13
VDD
16
120
121
131
141
VSS
11
15
目标信号
122
132
142
VDD
130
17
181
VSS
182
18
14

图 2

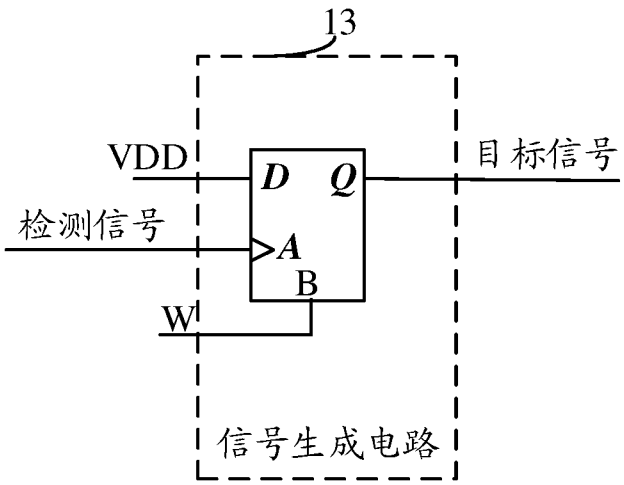
13
VDD
D
Q
目标信号
检测信号
A
B
W
信号生成电路

图 3

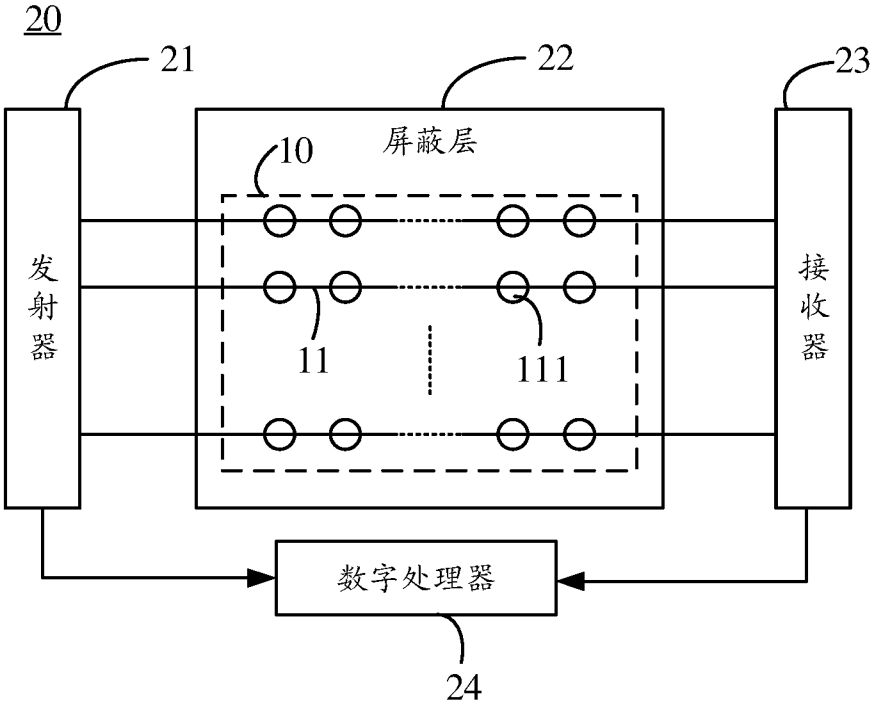

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/101081

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/75(2013.01)i; G06F 21/81(2013.01)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)

G06F21; G01R19

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; VEN; USTXT; WOTXT; EPTXT; CNKI; IEEE: 电磁故障注入, 屏蔽, 芯片, 电路, 电压, 阈值, 参考, 锁存, 场效应管, 功率管, 晶体管, 栅极, 漏极, Electromagnetic Fault Inject, EMFI, shield, MOS, FET, chip, IC, circuit, voltage, threshold, reference, latch, gate, drain

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 107563191 A (STMICROELECTRONICS (ROUSSET) SAS) 09 January 2018 (2018-01-09) description, paragraphs [0031]-[0088], and figure 3	1-14
Y	CN 103034804 A (SHENZHEN STATE MICRO TECHNOLOGY CO., LTD.) 10 April 2013 (2013-04-10) description, paragraphs [0012]-[0016], and figure 1	1-14
Y	CN 102565514 A (HONGFUJIN PRECISION INDUSTRY (SHENZHEN) CO., LTD. et al.) 11 July 2012 (2012-07-11) description, paragraphs [0004]-[0010], and figure 1	1-14

☐ 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
31 March 2020	**29 April 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/101081

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107563191	A	09 January 2018	FR	3053503	A1	05 January 2018
				EP	3264460	A1	03 January 2018
				US	2018005964	A1	04 January 2018
				FR	3053503	B1	29 March 2019
				CN	207182284	U	03 April 2018
				US	10361164	B2	23 July 2019
CN	103034804	A	10 April 2013	CN	103034804	B	23 December 2015
CN	102565514	A	11 July 2012	None			

国际检索报告

国际申请号
PCT/CN2019/101081

A. 主题的分类

G06F 21/75(2013.01)i; G06F 21/81(2013.01)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)

G06F21; G01R19

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;VEN;USTXT;WOTXT;EPTXT;CNKI;IEEE：电磁故障注入，屏蔽，芯片，电路，电压，阈值，参考，锁存，场效应管，功率管，晶体管，栅极，漏极，Electromagnetic Fault Inject，EMFI，shield，MOS，FET，chip，IC，circuit，voltage，threshold，reference，latch，gate，drain

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
Y	CN 107563191 A (意法半导体鲁塞公司) 2018年 1月 9日 (2018-01-09) 说明书第[0031]-[0088]段，附图3	1-14
Y	CN 103034804 A (深圳国微技术有限公司) 2013年 4月 10日 (2013-04-10) 说明书第[0012]-[0016]段，附图1	1-14
Y	CN 102565514 A (鸿富锦精密工业深圳有限公司 等) 2012年 7月 11日 (2012-07-11) 说明书第[0004]-[0010]段，附图1	1-14

☐ 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
2020年 3月 31日	2020年 4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	王莹
传真号 (86-10)62019451	电话号码 86-（0512）-88997264

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/101081

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	107563191	A	2018年 1月 9日	FR	3053503	A1	2018年 1月 5日
				EP	3264460	A1	2018年 1月 3日
				US	2018005964	A1	2018年 1月 4日
				FR	3053503	B1	2019年 3月 29日
				CN	207182284	U	2018年 4月 3日
				US	10361164	B2	2019年 7月 23日
CN	103034804	A	2013年 4月 10日	CN	103034804	B	2015年 12月 23日
CN	102565514	A	2012年 7月 11日		无		