

## 逻辑运算电路、差分放大电路及电子设备

### 技术领域

本申请涉及集成电路领域，具体涉及一种逻辑运算电路、差分放大电路及电子设备。

### 背景技术

近年来随着半导体集成电路的迅速发展，集成电路的漏洞带来的安全问题也愈加显著。边信道攻击，又称侧信道攻击，其核心思想是通过获取硬件运行时产生的各种泄漏信息分析出明文信息或密钥信息。硬件运行时产生的各种泄漏信息主要包括芯片内部电平翻转时的功耗、电磁辐射或者温度等变量，通过分析这些变量，可以捕获芯片内部的数据信息。随着移动支付的发展，越来越多的机密数据构建在芯片底层之上，尽管这些机密数据已经利用了加密算法进行保护，但是攻击者依然可以对芯片进行边信道分析从而获取内部明文、密钥等信息。另外，边信道攻击还会给各类电子设备带来重大安全隐患，尤其是 AES（高级加密标准）加解密电子设备。

现有技术中使用单根信号线进行信号传输，信号在 0/1 之间变化，此时信号线上传输的电压在高电平和低电平之间切换，电平的翻转需要吸收或者释放大电荷，从而使得电路功耗、电磁辐射或者温度等物理信息表现出不同特征，通过对该特征的分析，能够获得芯片内部的数据信息，容易发生边信道攻击。

### 技术问题

本申请提供一种逻辑运算电路、差分放大电路及电子设备，以解决现有的单根信号线进行信号传输，容易发生边信道攻击的问题。

### 技术方案

本申请提供的逻辑运算电路，包括至少一差分逻辑运算电路，所述差分逻辑运算电路包括：逻辑网络模块，包括逻辑功能互补的第一逻辑网络单元和第

二逻辑网络单元，所述第一逻辑网络单元和所述第二逻辑网络单元的输入信号构成差分信号，用于根据输入信号实现预设逻辑功能，并输出运算结果；差分放大模块，包括第一输入端、第二输入端、第一输出端和第二输出端，所述第一输入端和所述第二输入端分别与所述第一逻辑网络单元和所述第二逻辑网络单元的输出端连接，所述第一输出端和所述第二输出端构成差分输出端，用于对所述运算结果进行放大并输出逻辑运算结果。

可选的，所述差分放大模块包括：差分放大单元，连接于所述逻辑网络模块的输出端，用于放大所述运算结果后输出所述逻辑运算结果；预充电单元，与所述差分放大单元连接，用于在预充电周期时控制所述第一输出端和所述第二输出端预充电至电源电压；电流源单元，与所述差分放大单元连接，用于在求值周期时给所述差分放大单元提供电流通路。

可选的，所述差分放大模块还包括：存储单元，连接于所述第一逻辑网络单元和所述第二逻辑网络单元的输出端，用于进行信息存储。

可选的，所述差分放大模块还包括：吸收单元，与所述存储单元连接，用于吸收所述存储单元在开关切换时产生的多余电荷。

可选的，所述存储单元包括：第一晶体管和第二晶体管；所述第一晶体管和所述第二晶体管的栅极均连接时钟信号，漏极分别与所述第一逻辑网络单元和所述第二逻辑网络单元的输出端连接，源极分别连接所述第一输入端和第二输入端。

可选的，所述吸收单元包括：第三晶体管和第四晶体管；所述第三晶体管和第四晶体管为 N 沟道型晶体管时，第三晶体管的栅极与所述第四晶体管的源极连接，漏极接电源电压，源极与所述第一输入端连接；所述第四晶体管的栅极与所述第三晶体管的源极连接，漏极接电源电压，源极与所述第二输入端连接。所述第三晶体管和第四晶体管为 P 沟道型晶体管时，第三晶体管的栅极与所述第四晶体管的漏极连接，源极接电源电压，漏极与所述第一输入端连接；所述第四晶体管的栅极与所述第三晶体管的漏极连接，源极接电源电压，漏极与所述第二输入端连接。N 沟道型晶体管比如 N 沟道 MOS（场效应管）管，P

沟道型晶体管比如 P 沟道 MOS 管。

可选的，所述差分放大模块还包括：至少一开关电容单元，与所述电流源单元连接，用于增加输出驱动电压的范围。

可选的，包括两个以上所述差分逻辑运算电路；相邻所述差分逻辑运算电路中，其中一所述差分逻辑运算电路的输出端连接至另一所述差分逻辑运算电路的输入端以实现级联。

可选的，还包括：时钟缓冲模块，连接于所述差分逻辑运算电路之间，用于控制不同的所述差分逻辑运算电路之间的时序关系。

一种差分放大电路，包括至少一差分模块，所述差分模块包括存储子模块、差分放大子模块、预充电子模块和电流源子模块：存储子模块，包括差分输入端，用于在预充电周期时存储输入的差分信号，并将所述差分信号输入至所述差分放大子模块；差分放大子模块，包括差分输出端，与所述存储子模块连接，用于根据所述差分信号输出差分结果；预充电子模块，与所述差分放大子模块连接，用于在预充电周期时控制所述差分输出端预充电至电源电压；电流源子模块，与所述差分放大子模块连接，用于在求值周期时给所述差分放大单元提供电流通路。

可选的，还包括：吸收子模块，与所述存储子模块连接，用于吸收所述存储子模块在开关切换时产生的多余电荷。

可选的，还包括第一差分模块和第二差分模块，所述第一差分模块的第一输入端与所述第二差分模块的第二输出端连接，第二输入端与所述第二差分模块的第一输出端连接，第一输出端与所述第二差分模块的第二输入端连接，第二输出端与所述第二差分模块的第一输入端连接。

一种用于抵抗边信道攻击的电路，包括上述所述的逻辑运算电路。

一种电子设备，包括上述所述的逻辑运算电路。

可选的，还包括上述所述的差分放大电路。

**有益效果**

本发明的逻辑运算电路，包括至少一差分逻辑运算电路，所述差分逻辑运算电路包括：逻辑网络模块和差分放大模块，将逻辑网络模块包括逻辑功能互补的第一逻辑网络单元和第二逻辑网络单元，第一逻辑网络单元和所述第二逻辑网络单元的输入信号构成差分信号，通过逻辑网络模块可以实现各种预设的逻辑功能，由于逻辑网络模块输出的信号较弱，还需要将逻辑网络模块的输出结果连接到一差分放大模块进行信号放大，并输出差分形式的逻辑运算结果，由于将逻辑网络模块使用差分信号进行信号传输，差分信号采用电平之间的正负电压差来表征 0 和 1，电平变化幅度小，从而使得电路功耗、电磁辐射或者温度等物理信息变化不明显，即无论传输的信息是 0 或者是 1，对于外界能捕获的物理量均相同，不容易获得芯片内部的数据信息，防止了边信道攻击，提高了数据的安全性。另外，使用逻辑网络模块可实现各种逻辑功能，提高了电路的逻辑复杂性，由于逻辑网络模块可以使用较低的电源电压供电，降低了电路功耗；另外，相比于使用分立器件实现逻辑功能，使用专用的逻辑网络模块可以减少元器件数量，优化了芯片面积。

#### 附图说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明一实施例的逻辑运算电路的结构示意图；

图 2 为本发明一实施例的差分逻辑运算电路的结构示意图；

图 3 为本发明一实施例的逻辑运算电路的电路结构示意图；

图 4 为本发明一实施例的逻辑运算电路的电路结构示意图；

图 5 为本发明一实施例的二输入异或门传输计算电路；

图 6 为本发明一实施例的带开关电容单元的逻辑运算电路；

图 7 为本发明一实施例的差分逻辑运算电路级联的电路图；

图 8 为本发明一实施例的时钟缓冲模块的电路图；

图 9 为本发明一实施例的 16bit 超前进位加法器组合的结构示意图；

图 10 为本发明一实施例的差分放大电路的结构示意图；

图 11 为本发明一实施例的差分放大电路的电路结构示意图；

图 12 为本发明一实施例的利用差分放大电路生成差分时钟信号的电路图。

## 本发明的实施方式

下面结合附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本申请一部分实施例，而非全部实施例。基于本申请中的实施例，本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。在不冲突的情况下，下述各个实施例及其技术特征可以相互组合。

请参考图 1，为本发明一个实施例的逻辑运算电路的结构示意图。

本实施例的逻辑运算电路 200，包括至少一差分逻辑运算电路 100。如图 2 所示，差分逻辑运算电路 100 包括：逻辑网络模块 1 和差分放大模块 2。

逻辑网络模块 1 包括逻辑功能互补的第一逻辑网络单元 11 和第二逻辑网络单元 12，所述第一逻辑网络单元 11 的输入信号 IN 和所述第二逻辑网络单元 12 的输入信号  $\overline{IN}$  构成差分信号，第一逻辑网络单元 11 和第二逻辑网络单元 12 内部优选为晶体管的组合，可以采用晶体管不同排列来实现不同逻辑功能，比如异或计算、与非计算、1 位全加器、1 位半加器等任意逻辑计算以实现不同的预设逻辑功能。第一逻辑网络单元 11 和第二逻辑网络单元 12 设置在差分放大模块 2 的两侧，该电路连接方式不同于 DYCML（动态电流模式逻辑）电路将逻辑电路包含在充放电单元之内，可以提高电路的复杂程度。

差分放大模块 2 包括第一输入端、第二输入端、第一输出端 OUT 和第二输出端  $\overline{OUT}$ ，所述差分放大模块 2 的第一输入端和所述差分放大模块 2 的第二输入端分别与所述第一逻辑网络单元 11 和所述第二逻辑网络单元 12 的输出端连接，所述第一输出端 OUT 和所述第二输出端  $\overline{OUT}$  构成差分输出端，差分放大模

块 2 用于对第一逻辑网络单元 11 和所述第二逻辑网络单元 12 的输出运算结果进行放大并输出逻辑运算电路 200 的逻辑运算结果。

请参考图 3, 实施例的逻辑运算电路的电路结构示意图, 差分放大模块 2 优选包括: 电流源单元 21、预充电单元 22 和差分放大单元 23, 差分放大单元 23 连接于所述第一逻辑网络单元 11 和第二逻辑网络单元 12 的输出端, 用于放大所述运算结果后输出所述逻辑运算结果; 预充电单元 22, 与所述差分放大单元 23 连接, 用于在预充电周期时控制所述第一输出端 OUT 和所述第二输出端  $\overline{OUT}$  预充电至电源电压 VDD; 电流源单元 21, 与所述差分放大单元 23 连接, 用于在求值周期时给所述差分放大单元 23 提供电流通路。具体的, 晶体管 M1、晶体管 M2 和电容 C 构成电流源单元 21, 晶体管 M1 和晶体管 M2 为 N 沟道 MOS 管, 晶体管 M1 的栅极连接时钟信号 CLK, 源极连接晶体管 M2 的漏极和电容 C 的一端, 晶体管 M2 的栅极连接时钟信号  $\overline{CLK}$ , 时钟信号  $\overline{CLK}$  与 CLK 的相位相反, 晶体管 M2 的源极和电容 C 的另一端接地 GND。晶体管 M3 和晶体管 M4 构成预充电单元 22, 晶体管 M3 和晶体管 M4 为 P 沟道 MOS 管, 时钟信号 CLK 输入到晶体管 M3 的栅极, 晶体管 M3 的源极连接电源电压 VDD, 漏极与第一输出端 OUT 连接; 时钟信号 CLK 输入到晶体管 M4 的栅极, 晶体管 M4 的源极连接电源电压 VDD, 漏极与第二输出端  $\overline{OUT}$  连接, 预充电单元 22 用于控制第一输出端 OUT 和第二输出端  $\overline{OUT}$  在预充电周期时输出电源电压 VDD。晶体管 M7 和晶体管 M8 构成差分放大单元 23, 用于放大第一逻辑网络单元 11 和第二逻辑网络单元 12 输出的运算结果并输出放大后的逻辑运算结果。晶体管 M7 和晶体管 M8 为 N 沟道 MOS 管, 晶体管 M7 的栅极连接第一逻辑网络单元 11 的输出端, 漏极连接晶体管 M3 的漏极, 源极连接晶体管 M1 的漏极, 晶体管 M8 的栅极连接第二逻辑网络单元 12 的输出端, 漏极连接晶体管 M4 的漏极, 源极连接晶体管 M1 的漏极。同时, 晶体管 M7 和晶体管 M8 也构成了 PDN (下拉网络), 用于对第一输出端 OUT 和第二输出端  $\overline{OUT}$  电压进行传输和放大。

本实施例的逻辑运算电路, 包括至少一差分逻辑运算电路, 所述差分逻辑运算电路包括: 逻辑网络模块和差分放大模块, 将逻辑网络模块包括逻辑功能

互补的第一逻辑网络单元和第二逻辑网络单元，第一逻辑网络单元和所述第二逻辑网络单元的输入信号构成差分信号，通过逻辑网络模块可以实现各种预设的逻辑功能，由于逻辑网络模块输出的信号较弱，还需要将逻辑网络模块的输出结果连接到一差分放大模块进行信号放大，并输出差分形式的逻辑运算结果，由于将逻辑网络模块使用差分信号进行信号传输，差分信号采用电平之间的正负电压差来表征 0 和 1，电平变化幅度小，从而使得电路功耗、电磁辐射或者温度等物理信息变化不明显，不容易获得芯片内部的数据信息，防止了边信道攻击，提高了数据的安全性。另外，相比于现有技术中，在差分电路内部使用实现简单逻辑功能的电路，本实施例的差分逻辑运算电路将逻辑网络模块设置在差分放大模块的外部，将各种复杂逻辑功能的逻辑网络模块单独分离出来，并通过与差分放大模块的差分输入端连接以实现逻辑网络模块的逻辑功能，可以进行更复杂的逻辑运算。由于传统差分电路内部逻辑运算网络与 PDN 构成的共源共栅结构要求更高的电源电压才能工作，提高了电路的功耗，而本实施例中的逻辑网络模块与差分放大模块是分离的，逻辑网络模块使用低于电源电压摆幅，降低了电路的功耗。

上述实施例中的逻辑运算电路中逻辑网络模块的计算结果直接输出，无法进行存储。由于逻辑运算电路需要存储中间信息才能形成流水线用以提高计算能力，为了解决信息存储问题，在上述实施例的基础上，本实施例的差分放大模块 2 进一步包括存储单元，该存储单元连接于所述第一逻辑网络单元 11 和所述第二逻辑网络单元 12 的输出端，用于进行信息存储。又为了进一步优化沟道电荷注入效应，提高电路速度和降低电路功耗，本实施例的差分放大模块 2 进一步包括吸收单元，该吸收单元与所述存储单元连接，用于吸收所述存储单元在开关切换时产生的多余电荷。又为了使逻辑运算电路的输出稳定的差分电压，本实施例的差分放大模块 2 进一步包括锁存单元。

请参考图 4，本发明的另一实施例的逻辑运算电路的电路结构示意图。

在图 3 的基础上，本实施例的差分放大模块 2 还包括：锁存单元、存储单元和吸收单元。

如图4所示,晶体管M5和晶体管M6为P沟道MOS管,第一晶体管M9、第二晶体管M10、第三晶体管M11与第四晶体管M12为N沟道MOS管,晶体管M5和晶体管M6构成锁存单元,第一晶体管M9和第二晶体管M10构成存储单元,第三晶体管M11和第四晶体管M12构成吸收单元。晶体管M5和晶体管M6构成一组latch(锁存器),晶体管M5的栅极与晶体管M4和晶体管M6的漏极连接,源极连接电源电压VDD,漏极与晶体管M3的漏极和晶体管M6的栅极连接,晶体管M6的源极连接电源电压VDD。锁存单元用于在求值周期时控制第一输出端OUT和第二输出端 $\overline{OUT}$ 形成差分电压。此时,晶体管M7的栅极连接晶体管M9的源极,漏极连接晶体管M5的漏极,源极连接晶体管M1的漏极,晶体管M8的栅极连接晶体管M10的源极,漏极连接晶体管M6的漏极,源极连接晶体管M1的漏极。第一晶体管M9和第二晶体管M10的栅极连接时钟信号 $\overline{CLK}$ ,漏极分别与所述第一逻辑网络单元11和所述第二逻辑网络单元12的输出端连接,源极分别与晶体管M7和晶体管M8的栅极连接。第一晶体管M9和第二晶体管M10对于存储于晶体管M7和晶体管M8栅极的电荷进行控制,实现了将信息存储在晶体管M7和晶体管M8的栅极。第三晶体管M11的栅极与第四晶体管M12的源极和第二晶体管M10的源极连接,漏极接电源电压VDD;第四晶体管M12的栅极与第三晶体管M11的源极和第一晶体管M9的源极连接,漏极接电源电压VDD,第三晶体管M11和第四晶体管M12分别用于吸收由第一晶体管M9,第二晶体管M10在开关切换时产生的多余电荷。利用第三晶体管M11和第四晶体管M12构成latch连接以实现第一晶体管M9和第二晶体管M10沟道电荷注入效应的优化。沟道电荷注入指的是在MOS(金属-氧化物-半导体)器件导通或关断的瞬间,沟道区内的电荷流入或流出MOS开关,改变对应节点的电压,引入误差的现象。第一晶体管M9和第二晶体管M10沟道电荷注入效应的优化可以提高电路速度和降低电路功耗。第三晶体管M11和第四晶体管M12可以是N型晶体管或者P型晶体管。当第三晶体管M11和第四晶体管M12为P型晶体管时,第三晶体管M11的栅极与第四晶体管M12的漏极连接,源极接电源电压,漏极与晶体管M7的栅极连接;第四晶体管M12

的栅极与第三晶体管 M11 的漏极连接，源极接电源电压，漏极与晶体管 M8 的栅极连接。

图 4 中的逻辑运算电路的工作分成预充电周期和求值周期，过程如下：在预充电周期，时钟信号 CLK 为低电平，时钟信号  $\overline{CLK}$  为高电平，预充电单元中晶体管 M3 和晶体管 M4 导通，第一输出端 OUT 和第二输出端  $\overline{OUT}$  输出电源电压 VDD，第一晶体管 M9 和第二晶体管 M10 导通，第一逻辑网络单元 11 和第二逻辑网络单元 12 的输出结果分别存储在晶体管 M7 和晶体管 M8 的栅极，第三晶体管 M11 或第四晶体管 M12 导通，吸收第一晶体管 M9 或第二晶体管 M10 开关产生的多余电荷。此时，晶体管 M2 导通，使得电容 C 上的电荷释放到地 GND。同时，晶体管 M1 是关闭的，电源电压 VDD 到地 GND 之间电流通路关闭。在求值周期，时钟信号 CLK 为高电平，时钟信号  $\overline{CLK}$  为低电平，预充电单元中晶体管 M3 和晶体管 M4、第一晶体管 M9、第二晶体管 M10、第三晶体管 M11、第四晶体管 M12 是关闭的，电流源单元中晶体管 M1 导通，电容 C 构成虚拟地，晶体管 M7 或者晶体管 M8 也导通，第一输出端 OUT 和第二输出端  $\overline{OUT}$  到地 GND 形成了电流通路。由于第一输出端 OUT 和第二输出端  $\overline{OUT}$  的电流通路有不同的阻抗，因此，会出现一个输出电压比另一个输出电压下降较快的情况。此时，锁存单元中晶体管 M5 和晶体管 M6 会帮助电路平衡，当输出电压下降到一定程度时，晶体管 M5 或晶体管 M6 会导通以使得输出电压再次回到电源电压 VDD。

可见，本实施例的逻辑运算电路，工作分成预充电周期和求值周期，第一晶体管 M9、第二晶体管 M10 作用是控制信息的存储至晶体管 M7 和 M8 的栅极。在求值周期中，第三晶体管 M11、第四晶体管 M12 的作用是消除第一晶体管 M9、第二 M10 晶体管的沟道电荷注入效应的有害影响，利用有益影响。由于第一晶体管 M9 的沟道电荷注入影响被第三晶体管 M11 所消除，第二晶体管 M10 的沟道电荷注入影响被第四晶体管 M12 所消除，因此第一晶体管 M9、第二晶体管 M10 晶体管有一只需要存储低电平，另一只存储高电平，沟道电荷注入效应所带来的益处被保留在低电平栅极，沟道电荷注入效应的缺陷被第三晶体管

M11 或者第四晶体管 M12 所消除, 因此 PDN 网络的跨导差值被保留, 从而影响输出结果。晶体管 M3, 晶体管 M4 的作用是在预充电周期控制输出电平回到 VDD, 晶体管 M1, 晶体管 M2 的作用是在求值周期, 通过将电容 C 的电子流入逻辑网络模块, 从而进行逻辑运算, 在预充电周期对电容 C 进行放电, 使得电子释放到地。晶体管 M5, 晶体管 M6 的主要作用是使得输出状态在求值周期得到保持。另外, 本实施例的逻辑运算电路的第一输出端 OUT 和第二输出端  $\overline{OUT}$  不会满摆幅, 使得电路功耗更低, 适用范围更广。

图 4 中的晶体管可以部分或全部为 P 型晶体管也可以为 N 型晶体管。另外, 电流源单元 21 为电荷泵或任意可实现电荷搬运功能的电路。由于晶体管 M1, 晶体管 M2, 电容 C 用于提供电荷搬运通路, 集成电路领域电荷泵能够实现相同功能, 因此电容 C 本身可以用集成电路领域常见的 MOS 代替实现, 或者利用 MIM (金属电容) 实现, 或者特殊工艺在芯片内部来实现电容, 或是通过另一颗芯片专门放置电容, 通过芯片上的通孔或者其他 bonding (键合) 线连接至电流源单元 21 以替代电容 C。

为了实现二输入异或门传输计算, 在上述实施例的基础上, 本发明提出了一种新的技术方案。

请参考图 5, 本发明的另一实施例的二输入异或门传输计算电路。

本实施例的二输入异或门传输计算电路是将图 4 中的第一逻辑网络单元 11 和第二逻辑网络单元 12 替换成了预设的异或逻辑功能之后形成的实例化, 能够完成二输入异或功能。图 5 中晶体管 M13 和晶体管 M15 构成第一异或单元 110, 晶体管 M14 和晶体管 M16 构成第二异或单元 120, 晶体管 M13、晶体管 M14、晶体管 M15 和晶体管 M16 均为 N 沟道 MOS 管, 晶体管 M13 的栅极接输入信号  $\overline{A}$ , 漏极接输入信号 B, 源极接第一晶体管 M9 的漏极, 晶体管 M14 的栅极接输入信号 A, 漏极接输入信号  $\overline{B}$ , 源极接第一晶体管 M9 的漏极, 晶体管 M15 的栅极接输入信号  $\overline{A}$ , 漏极接输入信号  $\overline{B}$ , 源极接第二晶体管 M10 的漏极, 晶体管 M16 的栅极接输入信号 A, 漏极接输入信号 B, 源极接第二晶体管 M10 的漏极, 输入信号 A 和 B 是异或门的两输入信号, 本实施例可以实现 A 异或 B 的

运算功能，且能够存储运算一起完成。逻辑运算电路优选地可以省去第一晶体管 M9 和第二晶体管 M10 以实现没有存储功能的差分计算电路。需要说明的是，通过将逻辑网络模块替换成任意能够完成计算的电路，从而实现不同的逻辑计算功能。

上述实施例的逻辑运算电路可以实现逻辑功能的计算及信息存储，但是与其他电路级联时，电流源单元提供的驱动电压的范围较窄。为了在逻辑运算电路级联时增加下一级电路的驱动电压的范围，本发明提供了一种新的技术方案。

请参看图 6，本发明的另一实施例的带开关电容单元的逻辑运算电路。

本实施例的带开关电容单元的逻辑运算电路中差分放大模块进一步包括至少一开关电容单元，与所述电流源单元连接，用于增加输出驱动电压的范围。如图 6 所示，开关电容单元包括：晶体管 M17 和晶体管 M18，晶体管 M17 和晶体管 M18 为 N 沟道型晶体管。此时，电流源单元中的电容 C 的一端与晶体管 M2 的漏极连接，电容 C 的另一端与晶体管 M18 的漏极连接，晶体管 M17 的栅极连接时钟信号  $\overline{CLK}$ ，漏极连接电源电压 VDD，源极与晶体管 M18 的漏极连接，晶体管 M18 的栅极连接时钟信号 CLK，源极连接地 GND。通过增加开关电容单元可以减小电容 C 的容量，减少电容 C 的面积，晶体管 M1 的源极输出驱动电压的范围更大。

上述实施例的逻辑运算电路仅是单独的电路，电路实现的逻辑功能相对简单，为了实现更为复杂的电路逻辑功能，在上述实施例的基础上进一步提出了新的技术方案，新的技术方案可以解决逻辑运算电路的级联问题，增加电路的复杂度，同时满足各电路之间的时序要求。

请参看图 7，本发明的另一实施例的差分逻辑运算电路级联的电路图。

本实施例的逻辑运算电路包括两个以上差分逻辑运算电路；相邻所述差分逻辑运算电路中，其中一所述差分逻辑运算电路的输出端连接至另一所述差分逻辑运算电路的输入端以实现级联，增加电路的复杂度。又由于逻辑电路之间对时序的要求很高，为了使级联的逻辑运算电路之间的时序满足要求，本实施例中逻辑运算电路还包括：时钟缓冲模块，连接于所述差分逻辑运算电路之间，

用于控制不同的所述差分逻辑运算电路之间的时序关系。

具体的，如图 7 所示，逻辑运算电路包括两个差分逻辑运算电路，差分逻辑运算电路 101 和差分逻辑运算电路 102，差分逻辑运算电路 101 的第一输出端 OUT 和第二输出端  $\overline{OUT}$  分别与差分逻辑运算电路 102 的输入端 IN 和  $\overline{IN}$  对应连接，以实现差分逻辑运算电路 101 和差分逻辑运算电路 102 级联。其中逻辑网络模块之间根据前后级的计算关系进行连接，根据时序需求，可以通过时钟缓冲模块 103 与下一级相连接。

图 7 中的时钟缓冲模块 103 如图 8 所示，晶体管 M21、晶体管 M24 为 P 沟道型晶体管、晶体管 M22、晶体管 M23 和晶体管 M25 均为 N 沟道 MOS 管，晶体管 M21 的栅极连接时钟信号 CLK，源极接电源电压 VDD，漏极连接晶体管 M22 的漏极，晶体管 M22 的栅极连接信号 EOE（求值结束信号），源极连接晶体管 M23 的漏极，晶体管 M23 的栅极连接时钟信号 CLK，源极接地，晶体管 M24 的栅极连接晶体管 M21 的漏极，源极接电源电压 VDD，漏极连接晶体管 M25 的漏极，晶体管 25 的栅极连接时钟信号  $\overline{CLK}$ ，源极接地，晶体管 M25 的漏极输出信号 SE（开始求值），SE 与差分逻辑运算电路 102 中的晶体管 M19 的栅极连接。在预充电周期，时钟缓冲模块 103 的 EOE 节点电压为 0，在求值周期开始，电容 C 开始充电，EOE 输出高电平以给差分逻辑运算电路 102 提供驱动。

图 7 中的差分逻辑运算电路的连接方法，其核心技术要点在于 N 型晶体管形成的逻辑计算模块，该逻辑网络模块用于计算时，所有晶体管使用 N 型会带来功耗延迟积的改善，比常见 CMOS 或者互补逻辑更有优势。在其他实施方式中，逻辑网络模块也可使用 P 型晶体管或传输门逻辑。逻辑网络模块可根据具体需要的计算进行分割，排列和组合以实现多种功能。需要说明的是，图 7 中的各差分逻辑运算电路之间需要 CLK 信号来控制时间序列关系，通过确定的时钟信号到来的早晚，来决定何时进行求值、何时进行预充电。如果 CLK 之间的相位差能够保证时序满足设计要求，图 7 中的时钟缓冲模块 103 可以省略，若上下两级之间的差分逻辑运算电路之间需要紧密的时序配合，逻辑之间有紧密

时序关系,则需要使用图 8 中的时钟缓冲模块 103,以满足时序要求。差分逻辑运算电路 101 也可直接从时钟源连接至差分逻辑运算电路 102。在其他可选的实施方式中,可通过控制不同的所述差分逻辑运算电路之间的时序关系,并在差分逻辑运算电路 101 和差分逻辑运算电路 102 连接不同相位差的时钟,以实现差分逻辑运算电路 101 和差分逻辑运算电路 102 之间时序正确,差分逻辑运算电路 101 和差分逻辑运算电路 102 能够相互配合产生正确的计算结果,提高了计算结果的准确性。

上述实施例可以实现逻辑运算电路的级联,提高电路的逻辑复杂度。本发明提供了一利用上述实施例实现加法器的实施例。

请参见图 9,本发明的另一实施例的 16bit (比特)超前进位加法器组合。

本实施例的 16bit (比特)超前进位加法器组合,由四组 4bit 超前进位加法器构成,4bit 超前进位加法器使用差分逻辑运算电路实现,其内部逻辑网络模块由具体进位产生信号 G 和进位传输信号 P 的逻辑决定,具体计算逻辑是:

$$G=G_3+P_3G_2+P_3P_2G_1+P_3P_2P_1G_0$$

其中,  $G_0$ 、 $G_1$ 、 $G_2$ 、 $G_3$  分别为由低位到高位 4bit 超前进位加法器的进位产生信号,  $P_0$ 、 $P_1$ 、 $P_2$ 、 $P_3$  分别为由低位到高位 4bit 超前进位加法器的进位传输信号, G 为组合后的 16bit 超前进位加法器的进位产生信号。

本实施例可以使用多个差分逻辑运算电路实现更多比特位的加法器,不限于以上举例内容。

本发明还提供一种差分放大电路,差分放大电路包括至少一差分模块。本实施例的差分放大电路包括一个差分模块,请参见图 10,差分模块包括存储子模块 31、差分放大子模块 32、预充电子模块 33 和电流源子模块 34。

存储子模块 31,包括差分输入端,用于在预充电周期时存储输入的差分信号,并将所述差分信号输入至所述差分放大子模块 32;差分放大子模块 32,包括差分输出端,与所述存储子模块 31 连接,用于根据所述差分信号输出差分结果;预充电子模块 33,与所述差分放大子模块 32 连接,用于在预充电周期时控制所述差分输出端预充电至电源电压;电流源子模块 34,与所述差分放大子模

块 32 连接, 用于在求值周期时给所述差分放大单元提供电流通路。

本实施例的差分放大电路, 通过增加存储子模块 31, 可实现信息存储。该差分模块与其他电路模块连接, 可以实现信号的差分形式传输, 从而使得电路功耗、电磁辐射或者温度等物理信息变化不明显, 不容易获得芯片内部的数据信息, 防止了边信道攻击, 提高了数据的安全性。另外, 随着集成电路的功能越来越复杂, 模块集成度越来越高, 通过增加存储功能方便与其他模块进行连接, 实现各种复杂逻辑功能。

上述实施例的差分放大电路可以实现信息存储, 为了进一步提高电路速度和降低电路功耗, 本发明提供了一种新的技术方案对存储子模块 31 进行优化。

请参见图 11, 本发明另一实施例的差分放大电路的电路结构示意图。

本实施例的差分放大电路还包括吸收子模块, 吸收子模块与所述存储子模块 31 连接, 用于吸收所述存储子模块 31 在开关切换时产生的多余电荷, 以提高电路的速度, 降低电路功耗。

具体的, 如图 11 所示, 本实施例的差分放大电路, 包括: 电容 C1、晶体管 M41、晶体管 M42、晶体管 M43、晶体管 M44、晶体管 M45、晶体管 M46、晶体管 M47、晶体管 M48、晶体管 M49、晶体管 M50、晶体管 M51、晶体管 M52、电源电压 VDD 和接地 GND。其中, 晶体管 M41、晶体管 M42、晶体管 M47、晶体管 M48、晶体管 M49、晶体管 M50、晶体管 M51、晶体管 M52 为 N 沟道 MOS 管, 晶体管 M43、晶体管 M44、晶体管 M45、晶体管 M46 为 P 沟道 MOS 管, 晶体管 M49 和晶体管 M50 构成存储子模块, 晶体管 M49 和晶体管 M50 的栅极连接时钟信号  $\overline{CLK}$ , 漏极分别与差分输入信号 IN 和  $\overline{IN}$  连接, 源极分别与晶体管 M47 和晶体管 M48 的栅极连接。晶体管 M49 和晶体管 M50 对于存储于晶体管 M47 和晶体管 M48 栅极的电荷进行控制, 实现了将信息存储在晶体管 M47 和晶体管 M48 的栅极。

晶体管 M47 和晶体管 M48 构成差分放大子模块 32, 用于放大输入的差分信号 IN 和  $\overline{IN}$ , 晶体管 M47 的栅极连接晶体管 M49 的源极, 漏极连接晶体管 M45 的漏极, 源极连接晶体管 M41 的漏极, 晶体管 M48 的栅极连接晶体管 M50

的源极,漏极连接晶体管 M46 的漏极,源极连接晶体管 M41 的漏极。同时,晶体管 M47 和晶体管 M48 也构成了 PDN,分别用于对输出节点电压进行传输和放大。

晶体管 M43 和晶体管 M44 构成预充电电子模块 33,时钟信号 CLK 输入到晶体管 M43 的栅极,晶体管 M43 的源极连接电源电压 VDD,漏极与第一输出端 OUT 连接;时钟信号 CLK 输入到晶体管 M44 的栅极,晶体管 M44 的源极连接电源电压 VDD,漏极与第二输出端  $\overline{OUT}$  连接,预充电单元用于控制第一输出端 OUT 和第二输出端  $\overline{OUT}$  在预充电周期时输出电源电压。

晶体管 M41、晶体管 M42 和电容 C1 构成电流源子模块 34,晶体管 M41 的栅极连接时钟信号 CLK,源极连接晶体管 M42 的漏极和电容 C1 的一端,晶体管 M42 的栅极连接时钟信号  $\overline{CLK}$ ,时钟信号  $\overline{CLK}$  与 CLK 构成相反信号,晶体管 M42 的源极和电容 C1 的另一端接地 GND。

晶体管 M45 和晶体管 M46 构成一组 latch,构成锁存子模块 35,晶体管 M45 的栅极与晶体管 M44 和晶体管 M46 的漏极连接,源极连接电源电压 VDD,漏极与晶体管 M43 的漏极和晶体管 M46 的栅极连接,晶体管 M46 的源极连接电源电压 VDD。锁存子模块用于在求值周期时控制第一输出端 OUT 和第二输出端  $\overline{OUT}$  形成差分电压。

晶体管 M51 和晶体管 M52 构成吸收子模块,晶体管 M51 的栅极与晶体管 M52 的源极和晶体管 M50 的源极连接,漏极接电源电压 VDD;晶体管 M52 的栅极与晶体管 M51 的源极和晶体管 M49 的源极连接,漏极接电源电压 VDD,晶体管 M51 和晶体管 M52 分别用于吸收由晶体管 M49,晶体管 M50 在开关切换时产生的多余电荷。利用晶体管 M51 和晶体管 M52 构成 latch 连接以实现晶体管 M49 和晶体管 M50 沟道电荷注入效应的优化。沟道电荷注入指的是在 MOS 器件导通或关断的瞬间,沟道区内的电荷流入或流出 MOS 开关,改变对应节点的电压,引入误差的现象。晶体管 M49 和晶体管 M50 沟道电荷注入效应的优化可以提高电路速度和降低电路功耗。晶体管 M51 和晶体管 M52 包括 N 型晶体管和 P 型晶体管。当晶体管 M51 和晶体管 M52 为 P 型晶体管时,晶体管 M51

的栅极与晶体管 M52 的漏极连接，源极接电源电压，漏极与晶体管 M47 的栅极连接；晶体管 M52 的栅极与晶体管 M51 的漏极连接，源极接电源电压，漏极与晶体管 M48 的栅极连接。

图 11 中的差分放大电路的工作分成预充电周期和求值周期，原理与工作过程与图 4 中的差分逻辑运算电路类似，此处不再赘述。

为了实现差分放大电路之间的级联，在上述实施例的基础上，本发明提供了下面的实施例。

请参见图 12，本发明另一实施例的利用差分放大电路生成差分时钟信号的电路图。

本实施例的利用差分放大电路生成差分时钟信号的电路图，包括第一差分模块 321 和第二差分模块 322，所述第一差分模块 321 的第一输入端 IN1 与所述第二差分模块 322 的第二输出端  $\overline{OUT2}$  连接，第二输入端  $\overline{IN1}$  与所述第二差分模块 322 的第一输出端 OUT2 连接，第一输出端 OUT1 与所述第二差分模块 322 的第二输入端  $\overline{IN2}$  连接，第二输出端  $\overline{OUT1}$  与所述第二差分模块 322 的第一输入端 IN2 连接，该差分模块用于实现差分时钟信号。

本发明还提供一种包括上述的逻辑运算电路的用于抵抗边信道攻击的电路。通过上述逻辑运算电路使得电路功耗、电磁辐射或者温度等物理信息变化不明显，不容易获得芯片内部的数据信息，防止了边信道攻击，提高了数据的安全性。另外，使用逻辑网络模块可实现各种逻辑功能，提高了电路的逻辑复杂性，由于逻辑网络模块可以使用较低的电源电压供电，降低了电路功耗。

本发明还提供一种包括上述的逻辑运算电路或差分放大电路的电子设备，例如手机、平板电脑、功放等。通过上述逻辑运算电路或差分放大电路，使得电路功耗、电磁辐射或者温度等物理信息变化不明显，不容易获得芯片内部的数据信息，防止了边信道攻击，提高了数据的安全性。另外，使用逻辑网络模块可实现各种逻辑功能，可用于实现更复杂的逻辑运算，由于逻辑网络模块可以使用较低的电压驱动，降低了电路功耗。

即，以上所述仅为本申请的实施例，并非因此限制本申请的专利范围，凡

是利用本申请说明书及附图内容所作的等效结构或等效流程变换，例如各实施例之间技术特征的相互结合，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

## 权利要求书

1.一种逻辑运算电路,其特征在于,包括至少一差分逻辑运算电路,所述差分逻辑运算电路包括:

逻辑网络模块,包括逻辑功能互补的第一逻辑网络单元和第二逻辑网络单元,所述第一逻辑网络单元和所述第二逻辑网络单元的输入信号构成差分信号,用于根据输入信号实现预设逻辑功能,并输出运算结果;

差分放大模块,包括第一输入端、第二输入端、第一输出端和第二输出端,所述第一输入端和所述第二输入端分别与所述第一逻辑网络单元和所述第二逻辑网络单元的输出端连接,所述第一输出端和所述第二输出端构成差分输出端,用于对所述运算结果进行放大并输出逻辑运算结果。

2.如权利要求1所述的逻辑运算电路,其特征在于,所述差分放大模块包括:

差分放大单元,连接于所述逻辑网络模块的输出端,用于放大所述运算结果后输出所述逻辑运算结果;

预充电单元,与所述差分放大单元连接,用于在预充电周期时控制所述第一输出端和所述第二输出端预充电至电源电压;

电流源单元,与所述差分放大单元连接,用于在求值周期时给所述差分放大单元提供电流通路。

3.如权利要求2所述的逻辑运算电路,其特征在于,所述差分放大模块还包括:

存储单元,连接于所述第一逻辑网络单元和所述第二逻辑网络单元的输出端,用于进行信息存储。

4.如权利要求3所述的逻辑运算电路,其特征在于,所述差分放大模块还包括:

吸收单元,与所述存储单元连接,用于吸收所述存储单元在开关切换时产生的多余电荷。

5.如权利要求3所述的逻辑运算电路,其特征在于,所述存储单元包括:

第一晶体管和第二晶体管；

所述第一晶体管和所述第二晶体管的栅极均连接时钟信号，漏极分别与所述第一逻辑网络单元和所述第二逻辑网络单元的输出端连接，源极分别连接所述第一输入端和所述第二输入端。

6.如权利要求4所述的逻辑运算电路，其特征在于，所述吸收单元包括：

第三晶体管和第四晶体管；

当所述第三晶体管和所述第四晶体管为N沟道型晶体管时，所述第三晶体管的栅极与所述第四晶体管的源极连接，漏极接电源电压，源极与所述第一输入端连接，所述第四晶体管的栅极与所述第三晶体管的源极连接，漏极接电源电压，源极与所述第二输入端连接；

当所述第三晶体管和所述第四晶体管为P沟道型晶体管时，所述第三晶体管的栅极与所述第四晶体管的漏极连接，源极接电源电压，漏极与所述第一输入端连接；所述第四晶体管的栅极与所述第三晶体管的漏极连接，源极接电源电压，漏极与所述第二输入端连接。

7.如权利要求2所述的逻辑运算电路，其特征在于，所述差分放大模块还包括：

至少一开关电容单元，与所述电流源单元连接，用于增加输出驱动电压的范围。

8.如权利要求1所述的逻辑运算电路，其特征在于，包括两个以上所述差分逻辑运算电路；

相邻所述差分逻辑运算电路中，其中一所述差分逻辑运算电路的输出端连接至另一所述差分逻辑运算电路的输入端以实现级联。

9.如权利要求8所述的逻辑运算电路，其特征在于，还包括：

时钟缓冲模块，连接于所述差分逻辑运算电路之间，用于控制不同的所述差分逻辑运算电路之间的时序关系。

10.一种差分放大电路，其特征在于，包括至少一差分模块，所述差分模块包括存储子模块、差分放大子模块、预充电子模块和电流源子模块：

存储子模块,包括差分输入端,用于在预充电周期时存储输入的差分信号,并将所述差分信号输入至所述差分放大子模块;

差分放大子模块,包括差分输出端,与所述存储子模块连接,用于根据所述差分信号输出差分结果;

预充电电子模块,与所述差分放大子模块连接,用于在预充电周期时控制所述差分输出端预充电至电源电压;

电流源子模块,与所述差分放大子模块连接,用于在求值周期时给所述差分放大单元提供电流通路。

11.根据权利要求 10 所述的差分放大电路,其特征在于,还包括:

吸收子模块,与所述存储子模块连接,用于吸收所述存储子模块在开关切换时产生的多余电荷。

12.根据权利要求 10 所述的差分放大电路,其特征在于,还包括:第一差分模块和第二差分模块,所述第一差分模块的第一输入端与所述第二差分模块的第二输出端连接,第二输入端与所述第二差分模块的第一输出端连接,第一输出端与所述第二差分模块的第二输入端连接,第二输出端与所述第二差分模块的第一输入端连接。

13.一种电子设备,其特征在于,包括权利要求 6 所述的逻辑运算电路。

14.如权利要求 13 所述的电子设备,其特征在于,还包括权利要求 11 所述的差分放大电路。