PATENTOVÝ SPIS

(11) Číslo dokumentu:

308 895

(13) Druh dokumentu: **B6**

(51) Int. Cl.:

G06F 21/75	(2013.01)
G06K 19/073	(2006.01)
G11C 7/24	(2006.01)
H03K 19/0185	(2006.01)
H03K 19/17768	(2020.01)
H04L 9/00	(2006.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2020-153**
(22) Přihlášeno: **19.03.2020**
(40) Zveřejněno: **11.08.2021**
(Věstník č. 32/2021)
(47) Uděleno: **30.06.2021**
(24) Oznámení o udělení ve věstníku: **11.08.2021**
(Věstník č. 32/2021)

(56) Relevantní dokumenty:
Vincent Beroulle, et al.: Laser-Induced Fault Effects in Security-Dedicated Circuits , IFIP/IEEE International Conference on Very Large Scale Integration - System on a Chip VLSI-SoC 2014: VLSI-SoC: Internet of Things Foundations , pages 220-240 , First Online: 25 November 2015 , [retrieved on 2020-07-14], Retrieved from < https://link.springer.com/chapter/10.1007/978-3-319-25279-7_12 >; Kohei Matsuda, et al.: An IC-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density , Japanese Journal of Applied Physics, Vol 59, SGGL02 (2020) , https://doi.org/10.7567/1347-4065/ab65d3 , Published online February 28, 2020 , [retrieved on 2020-07-14], Retrieved from < https://iopscience.iop.org/article/10.7567/1347-4065/ab65d3 >; Takeshi Sugawara, et al: Side-channel leakage from sensor-based countermeasures against fault injection attack, Microelectronics Journal , Volume 90, August 2019, Pages 63-71 , https://doi.org/10.1016/j.mejo.2019.05.017 , [retrieved on 2020-07-14], Retrieved from < https://www.sciencedirect.com/science/article/pii/S0026269218309534 >.
US 2002141234 A1; AU 2018101695 A4; US 2018108386 A1; US 2013200371 A1; EP EP2259487 B1.

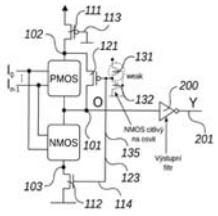
(73) Majitel patentu:
České vysoké učení technické v Praze, Praha 6, Dejvice, CZ

(72) Původce:
Ing. Jan Bělohoubek, Starý Plzenec, CZ
doc. Ing. Petr Fišer, Ph.D., Davle, Sázava, CZ
doc. Ing. Jan Schmidt, Ph.D., Praha 1, Staré Město, CZ

(74) Zástupce:
Ing. Hana Dušková, Na Kočově 180, 281 03 Chotutice

(54) Název vynálezu:
Zapojení standardní buňky CMOS se sníženou datovou závislostí statické spotřeby

(57) Anotace:
Statický CMOS obvod (100) obsahuje bloky PMOS (104) a NMOS (105). Blok PMOS (104) je připojen mezi virtuální napájecí uzel (102) připojený k napájecímu vodiči a výstup (101). Blok NMOS (105) je připojen mezi virtuální zemní uzel (103) připojený k zemnímu vodiči a výstup (101). Na výstup O (101) statického CMOS obvodu (100) je připojen vstup řetězce tvořeného alespoň jedním balančním invertorem. Výstup tohoto řetězce je výstupem celého zapojení. Velikost balančních invertorů zařazených v řetězci je optimalizovaná dle statického CMOS obvodu (100), kdy součet statické spotřeby včetně spotřeby indukované osvícením balančních invertorů (200, 300, 400) v řetězci a statického CMOS obvodu (100) je pro všechny možné kombinace vstupů statického CMOS obvodu (100) co nejbližší konstantě. Statický CMOS obvod (100) je doplněn kombinací dalších zapojení.



CZ 308895 B6

Zapojení standardní buňky CMOS se sníženou datovou závislostí statické spotřeby

Oblast techniky

Předkládaný vynález se týká nových zapojení CMOS obvodů snižujících datovou závislost mezi zpracovávanými daty a statickou spotřebou obvodu. Zapojení snižují zejména datovou závislost statické spotřeby indukované dodáním energie do oblasti se strukturami unipolárních tranzistorů, například osvícením obvodu. Řešení patří do oblasti elektroniky a číslicového návrhu.

Statickou spotřebu, a zejména spotřebu indukovanou ozářením obvodu, lze využít ke kompromitaci zařízení. Předkládané řešení slouží ke zvýšení bezpečnosti, a to zvýšením odolnosti proti útokům na zařízení, v němž je využito. Složité CMOS obvody VLSI se konstruují ze základních prvků nazývaných standardní buňka. Předkládané řešení umožňuje implementovat zabezpečenou verzi standardních buněk CMOS. Zabezpečená standardní buňka CMOS snižuje zejména závislost indukované statické spotřeby na stavu datových vstupů zabezpečené buňky a má pozitivní vliv také na datovou závislost statické spotřeby CMOS obvodu – leakage.

Dosavadní stav techniky

Současná řešení zvyšující odolnost VLSI CMOS obvodů proti fyzickým útokům tak zvaným postranním kanálem se zaměřují zejména na prevenci útoků zaměřených na závislost mezi dynamickou spotřebou obvodu a zpracovávanými daty. Jednou z možností ochrany CMOS obvodů je dosažení konstantní, datově nezávislé spotřeby. K tomuto účelu se často používá zvýšení symetrie obvodu s použitím komplementární dvoudrátové logiky, která je popsána například v dokumentu SPARSØ, Jens; FURBER, Steve. Principles of asynchronous Circuit design - A System Perspective. Kluwer Academie Publishers, 2002. Příkladem řešení využívajícího symetrie dvoudrátové logiky je WDDL, Wave Dynamic Differential Logic, viz dokument US 8947123 B2. Obdobné řešení založené na vzájemném vyvažování komplementárních hodnot v identických obvodech s komplementárními vstupy je HDRL, Homogeneous Dual-Rail Logic, US 8395408 B2.

Dynamická spotřeba sice v CMOS obvodu tvoří významnější datově závislý postranní kanál, avšak poslední výzkumy identifikovaly také zranitelnost CMOS obvodu spočívající v datové závislosti statické spotřeby, jak uvádí například publikace MOOS, Thorben; MORADI, Amir; RICHTER, Bastian. Static Power Side-Channel Analysis - An Investigation of Measurement Factors. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, a zejména statické spotřeby indukované osvitem, viz příspěvek BĚLOHOUBEK, Jan; FIŠER, Petr; SCHMIDT, Jan. CMOS Illumination Discloses Processed Data. In: 2019 22nd Euromicro Conference on Digital System Design (DSD). IEEE, 2019. p. 381-388.

Slabiny řešení použitých jako ochrana před útoky na dynamickou spotřebu způsobené zejména nemožností odstranit variace ve výrobním procesu a dále nedostatečnou symetrií komplementárních struktur odstraňuje ve statické CMOS logice takzvaný SecLib, viz GUILLEY, Sylvain, et al. CMOS structures suitable for secured hardware. In: Proceedings Design, Automation and Test in Europe Conference and Exhibition. IEEE, 2004. p. 1414-1415, kde je pomocí maximálně symetrických struktura implicitní synchronizace dosaženo značné symetrie ve spotřebě statického CMOS obvodu. Díky maximální symetrii poskytuje toto řešení i odolnost proti útokům na statickou spotřebu CMOS obvodu, avšak za cenu značné plochy standardních buněk, což zvyšuje cenu návrhu a má to také negativní vliv na některé aspekty bezpečnosti, jak bylo prezentováno v příspěvku BĚLOHOUBEK, Jan; FIŠER, Petr; SCHMIDT, Jan. CMOS lllumination Discloses Processed Data. In: 2019 22nd Euromicro Conference on Digital System Design (DSD). IEEE, 2019. p. 381-388.

Další možností ochrany před útoky na statickou i dynamickou spotřebu je použití dynamické

logiky, například domino logiky, popsané v KRAMBECK, R. H.; LEE, Charles M.; LAW, H.-FS. High-speed compact circuits with CMOS. IEEE Journal of Solid-State Circuits, 1982, 17.3: 614-619, které lze použít ke konstrukci dvoudrátové logiky. PMOS blok v domino logice je tvořen jediným tranzistorem ovládaným hodinovým signálem a nikoliv datovými signály, což vede k výraznému snížení závislosti spotřeby buňky na zpracovávaných datech. Na druhou stranu, návrh dynamické logiky vyžaduje změnu standardního návrhového stylu. Nevýhodou může být i nutnost rozvodu hodinového signálu v kombinační logice.

Obdobně také netradiční nebo speciální návrhové postupy mohou obsahovat zapojení, která mají vliv na statickou spotřebu obvodu nebo dokonce na spotřebu indukovanou osvitem. Například zapojení sériových odpojovacích tranzistorů používaná pro minimalizaci statické spotřeby nevyužitých částí obvodu, či obecně k dočasnému vypnutí části CMOS obvodu mohou ovlivnit také datovou závislost spotřeby aktivní části CMOS obvodu, v níž jsou obsaženy, avšak tato zapojení jsou optimalizována pro minimalizaci statické spotřeby, nikoli pro zvýšení její nezávislosti na vstupních datech. Příkladem mohou být zapojení s odpojovacími tranzistory typu PMOS popsaná v US 2002141234. Dalším příkladem, popsaným taktéž například v US 2002141234 může být jakékoli sériové zapojení invertorů a jejich optimalizace za účelem zvýšení rychlosti a/nebo výstupního proudu, jejímž vedlejším efektem může být snížení datové závislosti, neboť se jedná o zapojení s komplementárními vstupními hodnotami, avšak bez speciální optimalizace velikostí struktury vzhledem ke statické spotřebě celé balancované struktury nelze snížení datové závislosti na vstupech takové struktury zaručit.

Ke snížení datové závislosti statického proudu lze použít také standardní metodu symetrizace. Symetrizace skupiny CMOS tranzistorů se provede tak, že pro každou množinu tranzistorů mezi napájecím vodičem a výstupem CMOS buňky se všechny stromy obsahující sériová propojení tranzistorů duplikují a provede se permutace bloků v sérii zachovávající funkčnost. To se provede tak, aby ve výsledném schématu byly zastoupeny všechny permutace. Velikosti tranzistorů se zároveň mohou zmenšovat až v poměru daném počtem permutací. Popsaný způsob symetrizace skupin tranzistorů odstraňuje rozdíly ve spotřebě pro permutace vstupních proměnných CMOS obvodu, například 01 a 10, tak, že spotřeba se stává nezávislou na permutaci a je závislá pouze na Hammingově váze vstupního vektoru.

K obraně proti invazivním útokům osvícením CMOS obvodu se běžně využívají detektory osvitu. Ty jsou zpravidla konstruovány za účelem vyvolání alarmu na systémové úrovni, který vede k aktivaci procedur implementovaných jako aktivní ochrana systému proti útoku. Takové senzory jsou zpravidla provedeny tak, že jeden senzor zabezpečuje rozsáhlou plochu čipu, kde detekuje osvit, na který reaguje vyvoláním alarmu. Konstrukce jednoduchého detektoru založeného na PNP tranzistoru je popsána v US 2013200371.

Popsaná existující řešení poskytují balancování statické nebo světlem indukované statické spotřeby nedostatečně, za cenu velkého nárůstu plochy a zpoždění nebo v rámci změny paradigmatu návrhu integrovaného obvodu, to je přechod na implementaci v dynamické logice. Výrazný nárůst plochy obvodu představuje nevýhodu z hlediska zvýšených nákladů na výrobu a druhotně i zvýšeného příkonu obvodu, zároveň je ale neakceptovatelný i z hlediska odolnosti proti útoku osvitem, neboť zvyšuje pravděpodobnost nerovnoměrného osvitu chráněné části obvodu a ochrany nebo kompenzační části, čímž může dojít ke snížení efektivity kompenzace a potlačení schopnosti balancování světlem indukovaného datově závislého fotoproudu.

Podstata vynálezu

Výše uvedené nevýhody odstraňuje zapojení snižující datovou závislost statické spotřeby statického CMOS obvodu podle předkládaného řešení. Toto zapojení je koncipováno tak, že chráněný statický CMOS obvod imituje funkci zdroje malého konstantního proudu a/nebo využívá komplementárních logických hodnot, které indukují komplementární proudy v různých částech

obvodu.

Chráněný statický CMOS obvod obsahuje standardně zapojené bloky PMOS a NMOS. Blok PMOS je připojen mezi virtuální napájecí uzel, který je připojen k napájecímu vodiči, a výstup. Blok NMOS je připojen mezi virtuální zemní uzel, který je připojen k zemnímu vodiči, a výstup. Na výstup statického CMOS obvodu je připojen vstup řetězce, který je tvořen alespoň jedním balančním invertorem. Výstup tohoto řetězce je výstupem celého zapojení.

Podstatou nového řešení je, že velikost balančních invertorů zařazených v řetězci je optimalizovaná podle statického CMOS obvodu, kdy součet statické spotřeby včetně spotřeby indukované osvícením balančních invertorů v řetězci a statického CMOS obvodu je pro všechny možné kombinace vstupů statického CMOS obvodu co nejbližší konstantě.

V jednom možném provedení je řetězec tvořen lineárním zřetězením lichého počtu invertorů, přičemž minimální takový řetěz je tvořen pouze prvním balančním invertorem. Výstup prvního balančního invertorů je pak výstupem celého zapojení.

V jiném možném provedení je řetězec tvořen lineárním zřetězením sudého počtu invertorů. Minimální takový řetězec je tvořen tak, že na výstup prvního balančního invertorů je připojen vstup druhého balančního invertorů, jehož výstup je negativním výstupem celého zapojení.

Řetězec může být tvořen lineárním zřetězením sudého počtu invertorů a zpětnovazebními invertory, jejichž počet je vždy nižší než počet invertorů v lineární části řetězce. Minimální takový řetězec je tvořen tak, že na výstup prvního balančního invertorů je připojen vstup druhého balančního invertorů, jehož výstup je negativním výstupem zapojení. Druhý balanční invertor je zároveň propojen se zpětnovazebním invertorem, jehož výstup je spojen s výstupem prvního balančního invertorů. Tento zpětnovazební invertor je realizován vzhledem k prvnímu balančnímu invertorů jako slabý invertor. Výstup druhého balančního invertorů je zároveň výstupem celého zapojení.

Výše uvedená provedení mohou být doplněna dvěma způsoby, a to vždy alespoň jednou z dále uvedených variant daného způsobu nebo jejich libovolnou kombinací, a to v závislosti na požadovaném stupni ochrany a struktuře původní CMOS buňky.

Při použití prvního způsobu je v jedné variantě virtuální napájecí uzel k napájecímu vodiči připojen přes sériový tranzistor typu P, jehož drain je připojen k virtuálnímu napájecímu uzlu, source je připojen k napájecímu vodiči, a vývod gate je připojen k zemnímu vodiči.

Další variantou je, že virtuální zemní uzel je k zemnímu vodiči připojen přes sériový tranzistor typu N, jehož drain je připojen k virtuálnímu zemnímu uzlu, source je připojen k zemnímu vodiči a vývod gate je připojen k napájecímu vodiči.

V jiné variantě je k virtuálnímu napájecímu uzlu připojen source doplňkového tranzistoru typu P, jehož drain je připojen k výstupu O a vývod gate je připojen k napájecímu vodiči.

Existuje i další varianta, kdy je k virtuálnímu zemnímu uzlu připojen source doplňkového tranzistoru typu N, jehož drain je připojen k výstupu O a vývod gate je připojen k zemnímu vodiči.

Při použití druhého způsobu zapojení obsahuje invertor citlivý na osvit. Ten je tvořený tranzistorem typu P, jehož source je propojen s napájecím vodičem, drain je přes společný uzel propojen s drain tranzistoru typu N, jehož source je propojen se zemním vodičem. Gate tranzistoru typu P a tranzistoru typu N je spojen se zemním vodičem. K výstupu prvního řídicího signálu z invertorů citlivého na osvit je připojen vstup invertorů s výstupem, který je současně výstupem druhého řídicího signálu.

V jedné variantě je virtuální napájecí uzel k napájecímu vodiči připojen přes sériový tranzistor typu P, jehož drain je připojen k virtuálnímu napájecímu uzlu, source je připojen k napájecímu vodiči, a vývod gate je připojen k výstupu druhého řídicího signálu.

V další variantě je virtuální zemní uzel k zemnímu vodiči připojen přes sériový tranzistor typu N, jehož drain je připojen k virtuálnímu zemnímu uzlu, source je připojen k zemnímu vodiči a vývod gate je připojen k výstupu prvního řídicího signálu.

Jinou variantou je, že k virtuálnímu napájecímu uzlu je připojen source doplňkového tranzistoru typu P, jehož drain je připojen k výstupu O a vývod gate je připojen k výstupu prvního řídicího signálu.

Rovněž je možné zapojení, kdy k virtuálnímu zemnímu uzlu je připojen source doplňkového tranzistoru typu N, jehož drain je připojen k výstupu O a vývod gate je připojen k výstupu druhého řídicího signálu.

Jak již bylo uvedeno, lze použít kteroukoli z uvedených variant a jakékoli jejich kombinace.

Výhodou navrženého řešení je, že přináší snížení datové závislosti mezi zpracovávanými daty a statickou spotřebou obvodu a zejména statickou spotřebou obvodu indukovanou dodáním energie do oblasti se strukturami unipolárních tranzistorů, například osvícením obvodu ve statické CMOS logice s využitím značné menší plochy než nejbližší známé řešení SecLib. Předkládané řešení slouží ke zvýšení bezpečnosti zařízení, v němž je využito.

Objasnění výkresů

Provedení zabezpečené standardní buňky CMOS se sníženou datovou závislostí indukované statické spotřeby a neutrálním vlivem na statickou spotřebu, leakage, je pro lepší přehlednost popsáno hierarchicky. Na obr. 1 je znázorněna logická struktura zabezpečené standardní CMOS buňky s pozitivním výstupem, na obr. 2a, 2b a 2c jsou pak znázorněny možnosti vnitřního provedení základního CMOS obvodu. Možnost balancování lichým počtem invertorů je uvedena na obr. 3. obr. 4 ilustruje princip předkládaného řešení, kde nové struktury imitují chování zdroje malého proudu. Na obr. 5 je schéma CMOS buňky AND obsahující některá z předkládaných řešení tvořící tak zabezpečenou standardní buňku. Obr. 6a, 6b a 6c znázorňují průběh odběru statického, světlem indukovaného proudu v závislosti na vstupních datech, intenzitě osvitu a různém stupni zabezpečení CMOS buňky.

Příklady uskutečnění vynálezu

Zabezpečená standardní buňka CMOS se skládá ze sériově zapojeného statického CMOS obvodu 100 a prvního balančního invertorů 200, obr. 1. Celý obvod realizuje logickou funkci n vstupů označených I_0 až I_{n-1}, kde n je přirozené číslo. Výstup 201 zabezpečené standardní buňky, označený jako Y je pozitivní. Statický CMOS obvod 100 je obvod realizující logickou funkci s negativním výstupem 101, vyznačeným na výkrese pro lepší orientaci jako output O, a s n vstupy I_0 až I_{n-1}. Výstup 101 statického CMOS obvodu 100 je připojen na jediný vstup prvního balančního invertorů 200, jehož výstup 201 je zároveň výstupem celé standardní buňky.

První balanční invertor 200 je proveden jako standardní CMOS invertor, jehož velikost je optimalizovaná dle statického CMOS obvodu 100 tak, aby součet statické spotřeby, včetně spotřeby indukované osvícením prvního balančního invertorů 200 a statického CMOS obvodu 100 byl pro všechny možné kombinace vstupu statického CMOS obvodu 100 co nejbližší konstantě.

První balanční invertor 200 je možno vynechat, postačuje-li částečná balance statické spotřeby a

je-li požadován negativní výstup standardní buňky. Je-li první balanční invertor 200 vynechán, je výstupem celé standardní buňky negativní výstup O 101.

Je-li požadována plná balance statické spotřeby a zároveň negativní výstup celé CMOS buňky, je možno využít prostého zapojení lichého počtu invertorů nebo zapojení z obr. 3, kde výstup 201 prvního balančního invertorů 200 je přiveden na vstup druhého balančního invertorů 300, jehož výstup 301, označený jako Y2, pak představuje negativní výstup zabezpečené buňky. Zároveň je výstup 301 vstupem zpětnovazebního invertorů 400, jehož výstup je spojen s výstupem 201 prvního balančního invertorů 200.

Zpětnovazební invertor 400 je standardním způsobem, například modifikací šířky P a N kanálů, zkonstruován jako slabý (weak), oproti prvnímu balančnímu invertorů 200.

Výše popsané zapojení vede ke snížení datové závislosti statické spotřeby, zejména světlem indukovaného datově závislého fotoproudu u CMOS obvodu, neboť výsledná zřetězení invertorů a CMOS obvodů s negativním výstupem obsahují vždy páry CMOS obvodů pracující s komplementárními výstupy. V základním CMOS obvodu platí, že výstup obvodu je ve statickém stavu a pro libovolnou kombinaci vstupů vždy připojen k napájecímu nebo zemnímu vodiči. Díky tomuto faktu existuje v řetězci ke každé konfiguraci tranzistorů, tvořících CMOS obvod, její komplement vzhledem k propojení výstupu a napájecího, respektive zemního vodiče, který je využit k vzájemnému balancování statické spotřeby. Balancování se v principu provádí tak, že velikost balanční struktury se zvětší tak, aby odpovídala mohutnosti balancované struktury.

Balancování lichým počtem invertorů, a tedy vytváření komplementárních logických funkcí s negativním výstupem, například AND -> NAND, je možné s použitím zpětné vazby nebo výrazným posílením vybraných invertorů v lineárním řetězu. Použití lichého počtu invertorů většího než 1 v sériovém zapojení je nutné vzhledem k nutnosti zachování vysoké vstupní impedance balancovaného celku. Využití zpětnovazebního invertorů umožňuje rovnoměrněji balancovat zátěž invertorů v řetězci.

V obou případech balancování invertorem má výstupní invertor, tedy první balanční invertor 200, respektive druhý balanční invertor 300 zároveň roli filtru výstupního napětí a budiče následující úrovně hradel. Výstupní invertor nesmí být tedy výrazně zmenšen. Redukci velikosti, případně optimalizaci zpoždění lze provést modifikací velikostí tranzistorů uvnitř řetězu invertorů.

Vnitřní struktura statického CMOS obvodu 100 obsahuje prvky znázorněné na obr. 2a a/nebo 2b a/nebo 2c, tedy buď všechny, nebo jejich různé kombinace podle stupně požadované ochrany a struktury bloků NMOS a PMOS. Statický CMOS obvod 100 sestává vždy z bloku PMOS 104 připojeného mezi virtuální napájecí uzel 102 a výstupní uzel 101 a z bloku NMOS 105 připojeného mezi virtuální zemní uzel 103 a výstupní uzel 101. Výstupní uzel 101 je výstupem statického CMOS obvodu 100.

Snížení datové závislosti světlem indukovaného datově závislého fotoproudu bez zvýšení datové závislosti statické spotřeby je u CMOS obvodu 100 dosaženo napodobením chování zdroje malého konstantního proudu - viz obr. 4.

Napodobení chování zdroje malého konstantního proudu je dosaženo ve dvou krocích. Prvním je zvýšení datově nezávislé složky odporu, to je zapojení statického sériového odporu, a druhým krokem je snížení datově závislé složky odporu, to je zapojení statického malého odporu paralelně s datově závislým potenciometrem. V technologii CMOS je toho dosaženo sériovým, respektive paralelním zapojením tranzistorů vzhledem k blokům PMOS, respektive NMOS.

Sériové tranzistory, zde tedy sériový tranzistor 111 typu P a sériový tranzistor 112 typu N, viz obr. 2a, jsou použity k imitaci chování statické části odporu. Paralelní tranzistory, zde doplňkový tranzistor 121 typu P a doplňkový tranzistor 122 typu N, viz obr. 2b, se uplatní v případě osvícení

chráněného obvodu, na něž reagují výrazným zvýšením vodivosti.

Řídicí elektrody přidaných sériových, respektive paralelních doplňkových tranzistorů mohou být s výhodou řízeny na základě intenzity osvitu, což umožňuje dosažení lepšího chování pro velký rozsah intenzity osvitu chráněného obvodu.

Virtuální napájecí uzel 102 je připojen k napájecímu vodiči buď přímo, jak je znázorněno na obr. 2b, nebo přes sériový tranzistor 111 typu P způsobem znázorněným na obr. 2a. Virtuální zemní uzel 103 je připojen k zemnímu vodiči buď přímo, jak je znázorněno na obr. 2b, nebo přes sériový tranzistor 112 typu N způsobem znázorněným na obr. 2a.

Na obr. 2a je znázorněno možné zapojení sériových tranzistorů 111 a 112. Sériový tranzistor 111 typu P, jehož source S je připojen k napájecímu vodiči, drain D k virtuálnímu napájecímu uzlu 102 a vývod 113 gate G je připojen buď k zemnímu vodiči, nebo je připojen k výstupu 134 druhého řídicího signálu C2. Sériový tranzistor 112 typu N, jehož source S je připojen k zemnímu vodiči, drain D k virtuálnímu zemnímu uzlu 103 a vývod 114 gate G je připojen k napájecímu vodiči neboje připojen k výstupu 135 prvního řídicího signálu C1.

Na obr. 2b je znázorněno možné zapojení paralelních doplňkových tranzistorů 121 a 122. První doplňkový tranzistor 121 je tranzistor typu P, jehož source S je připojen k virtuálnímu napájecímu uzlu 102, drain D k výstupu O 101 a vývod 123 gate G je připojen k napájecímu vodiči nebo ke společnému uzlu 135, který je výstupem prvního řídicího signálu C1. Druhý doplňkový tranzistor 122 je tranzistor typu N, jehož source S je připojen k virtuálnímu zemnímu uzlu 103, drain D k výstupu O 101 a vývod 124 gate G je připojen k zemnímu vodiči nebo k výstupu 134 druhého řídicího signálu C2.

Na obr. 2c je znázorněno možné zapojení řídicích obvodů, jejichž výstupem jsou první řídicí signál C1 a druhý řídicí signál C2. Tranzistory 131 a 132 tvoří invertor citlivý na osvit s výstupem 135 prvního řídicího signálu C1. První tranzistor je tranzistor 131 typu P, jehož source S je připojen k napájecímu vodiči, drain D budí první výstupní řídicí signál C1 a gate G je připojen k zemnímu vodiči. Druhý tranzistor je tranzistor 132 typu N, jehož source S je připojen k zemnímu vodiči, drain D budí první výstupní řídicí signál C1 a gate G je připojen k zemnímu vodiči. Standardní CMOS invertor 133, na jehož jediný vstup je připojen výstup 135 prvního řídicího signálu C1, budí na výstupu 134 druhý řídicí signál C2. Tranzistor 131 typu P je standardním způsobem, například modifikací šířky kanálu, zkonstruován jako slabý (weak), oproti tranzistoru 132 typu N.

Protože tranzistory typu N mají výrazně vyšší citlivost na osvit, je požadovaného chování struktur reagujících na intenzitu osvitu docíleno samostatným zapojením tranzistorů typu N s bází trvale připojenou k zemi, případně zapojením tranzistorů typu N proti tranzistorům typu P s výrazně sníženou vodivostí. U struktur, kde není žádoucí, aby reagovaly na změnu intenzity ozáření, se komplementární tranzistory typu N, a typu P dimenzují standardním způsobem tak, aby bylo dosaženo obdobné vodivosti N i P tranzistorů.

Invertor 133 se vynechá v případě, kdy výstup 134 druhého řídicího signálu C2 není připojen ani k sériovému tranzistoru 111 typu P, ani k doplňkovému tranzistoru 122 typu N. V případě, že výstup 135 prvního řídicího signálu C1 není připojen ani k sériovému tranzistoru 112 typu N, ani k doplňkovému tranzistoru 121 typu P a není připojen ani na vstup invertorů 133, vynechají se také tranzistory 131 a 132 tvořící invertor citlivý na osvit.

Tranzistor 132 typu N funguje jako světelný senzor, k jehož otevření dojde v případě osvícení zabezpečeného obvodu. Hodnota prvního řídicího signálu C1 překročí rozhodovací úroveň při dodání alespoň prahové energie, jejíž velikost je dána technologií výroby, poměrem velikostí a vodivostí kanálů a ploch drain D a source S tranzistoru 131 typu P a tranzistoru 132 typu N. V případě připojení vývodu 124 gate G doplňkového tranzistoru 122 typu N k zemnímu vodiči

funguje obdobně, tedy jako samostatný světelný senzor, také tento doplňkový tranzistor 122 typu N.

V případě, že je vývod 113 gate G připojen k zemnímu vodiči, musí být vodivost P kanálu a plochy vývodů drain D a source S sériového tranzistoru 111 typu P nastaveny tak, aby tento sériový tranzistor 111 typu P efektivně omezoval proud procházející mezi napájecím vodičem a výstupem 101 pro co nejširší spektrum energie dodané do oblasti CMOS obvodu například jeho ozářením.

V případě, že vývod 114 gate G sériového tranzistoru 112 typu N je připojen k napájecímu vodiči, musí být vodivost jeho N kanálu a plochy vývodů drain D a source S nastaveny tak, aby tento sériový tranzistor 112 typu N efektivně omezoval proud procházející mezi zemním vodičem a výstupem 101 pro co nejširší spektrum energie dodané do oblasti CMOS obvodu například jeho ozářením.

V případě, že vývod 124 gate G je připojen k zemnímu vodiči, musí být vodivost N kanálu a plochy drain D a source S doplňkového tranzistoru 122 typu N nastaveny tak, aby přes něj procházela co největší část indukovaného proudu mezi virtuálním zemním uzlem 103 a výstupem 101 pro co nejširší spektrum energie dodané do oblasti CMOS obvodu například jeho ozářením.

Příklad zabezpečené standardní buňky CMOS implementované s použitím některých výše představených mechanismů je na obr. 5. Bloky PMOS a NMOS mohou být vnitřně symetrické.

Na obr. 6a, 6b a 6c je uveden průběh odběru statického, světlem indukovaného proudu v závislosti na různém stupni zabezpečení CMOS buňky. Obr. 6a znázorňuje závislost statického, světlem indukovaného proudu ve struktuře dvouvstupové CMOS buňky NAND s prvním balančním invertorem 200 na výstupu a symetrickými bloky PMOS a NMOS, na hustotě energie dodávané do oblasti CMOS buňky, která odpovídá zobrazenému výkonu laseru na normalizované ploše. Obr. 6b znázorňuje tutéž závislost totožné CMOS buňky obohacené navíc o sériový tranzistor 111 typu P. Obr. 6c znázorňuje tutéž závislost totožné CMOS buňky jako obrázek 6b, kde tato CMOS buňka je vybavena navíc řídicím obvodem reagujícím na osvit tvořeným tranzistorem 131 typu P a tranzistorem 132 typu N, a jím řízeným sériovým tranzistorem 121 typu N a paralelním tranzistorem 121 typu P. Tato struktura je znázorněna na obr. 5.

Průmyslová využitelnost

Předkládané řešení je dobře průmyslové využitelné například při tvorbě zákaznických obvodů se zvýšenými nároky na bezpečnost. Řešení je vhodné zejména pro tvorbu zabezpečených knihoven standardních buněk v technologii CMOS, které slouží jako základní bloky pro implementaci CMOS obvodu. Balancovaná CMOS knihovna přináší zvýšení bezpečnosti libovolného návrhu implementovaného s jejím použitím.

PATENTOVÉ NÁROKY

1. Zapojení standardní buňky CMOS se sníženou datovou závislostí statické spotřeby, kde statický CMOS obvod (100) obsahuje standardně zapojené bloky PMOS (104) a NMOS (105), kde blok PMOS (104) je připojen mezi virtuální napájecí uzel (102), který je připojen k napájecímu vodiči, a výstup (101), a blok NMOS (105) je připojen mezi virtuální zemní uzel (103), který je připojen k zemnímu vodiči, a výstup (101), kde na výstup O (101) statického CMOS obvodu (100) je připojen vstup řetězce tvořeného alespoň jedním balančním invertorem, kde výstup tohoto řetězce je výstupem celého zapojení, **vyznačující se tím**, že velikost balančních invertorů zařazených v řetězci je optimalizovaná dle statického CMOS obvodu (100), kdy součet statické spotřeby včetně spotřeby indukované osvícením balančních invertorů (200, 300, 400) v řetězci a statického CMOS obvodu (100) je pro všechny možné kombinace vstupů statického CMOS obvodu (100) co nejbližší konstantě.

2. Zapojení podle nároku 1, **vyznačující se tím**, že řetězec je tvořen lineárním zřetězením lichého počtu invertorů, přičemž minimální takový řetěz je tvořen pouze prvním balančním invertorem (200), jehož výstup (201) je výstupem (Y) celého zapojení.

3. Zapojení podle nároku 1, **vyznačující se tím**, že řetězec je tvořen lineárním zřetězením sudého počtu invertorů, přičemž minimální takový řetězec je tvořen tak, že na výstup (201) prvního balančního invertoru (200) je připojen vstup druhého balančního invertoru (300), jehož výstup (301) je negativním výstupem (Y2) celého zapojení.

4. Zapojení podle nároku 1, **vyznačující se tím**, že řetězec je tvořen lineárním zřetězením sudého počtu invertorů a zpětnovazebními invertory, jejichž počet je vždy nižší než počet invertorů v lineární části řetězce, přičemž minimální takový řetězec je tvořen tak, že na výstup (201) prvního balančního invertoru (200) je připojen vstup druhého balančního invertoru (300), jehož výstup (301) je negativním výstupem (Y2) zapojení a je zároveň propojen se zpětnovazebním invertorem (400), jehož výstup je spojen s výstupem (201) prvního balančního invertoru (200), přičemž tento zpětnovazební invertor (400) je realizován vzhledem k prvnímu balančnímu invertoru (200) jako slabý invertor, přičemž výstup (301) je zároveň výstupem (Y) celého zapojení.

5. Zapojení podle kteréhokoliv z nároků 1 až 4, **vyznačující se tím**, že virtuální napájecí uzel (102) je k napájecímu vodiči připojen přes sériový tranzistor (111) typu P, jehož drain (D) je připojen k virtuálnímu napájecímu uzlu (102), source (S) je připojen k napájecímu vodiči, a vývod (113) gate (G) je připojen k zemnímu vodiči,

a/nebo

virtuální zemní uzel (103) je k zemnímu vodiči připojen přes sériový tranzistor (112) typu N, jehož drain (D) je připojen k virtuálnímu zemnímu uzlu (103), source (S) je připojen k zemnímu vodiči a vývod (114) gate (G) je připojen k napájecímu vodiči,

a/nebo

k virtuálnímu napájecímu uzlu (102) je připojen source (S) doplňkového tranzistoru (121) typu P, jehož drain (D) je připojen k výstupu O (101) a vývod (123) gate (G) je připojen k napájecímu vodiči,

a/nebo

k virtuálnímu zemnímu uzlu (103) je připojen source (S) doplňkového tranzistoru (122) typu N, jehož drain (D) je připojen k výstupu O (101) a vývod (124) gate (G) je připojen k zemnímu vodiči.

6. Zapojení podle kteréhokoliv nároku 1 až 4, **vyznačující se tím**, že obsahuje invertor citlivý na osvit tvořený tranzistorem (131) typu P, jehož source (S) je propojen s napájecím vodičem, drain (D) je přes společný uzel (135) propojen s drain (D) tranzistoru (132) typu N, jehož source (S) je propojen se zemním vodičem a kde gate (G) tranzistoru (131) typu P a tranzistoru (132) typu N je spojen se zemním vodičem, a dále je k výstupu (C1) prvního řídicího signálu z invertoru citlivého na osvit připojen vstup invertoru (133) s výstupem (134), který je současně výstupem druhého řídicího signálu (C2), přičemž

virtuální napájecí uzel (102) je k napájecímu vodiči připojen přes sériový tranzistor (111) typu P, jehož drain (D) je připojen k virtuálnímu napájecímu uzlu (102), source (S) je připojen k napájecímu vodiči, a vývod (113) gate (G) je připojen k výstupu druhého řídicího signálu (C2), a/nebo

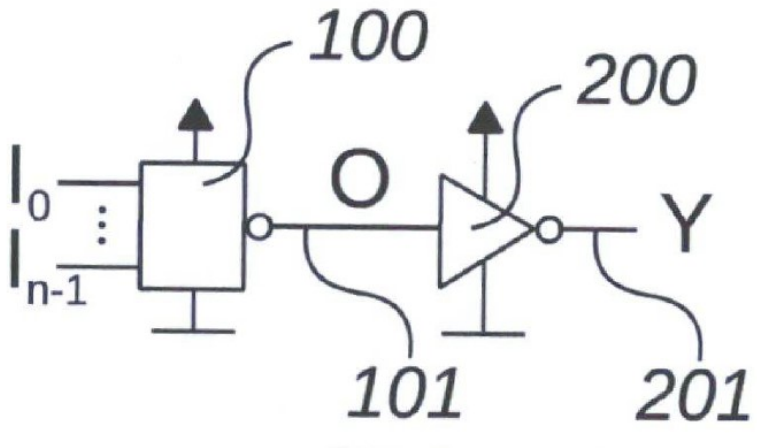
virtuální zemní uzel (103) je k zemnímu vodiči připojen přes sériový tranzistor (112) typu N, jehož drain (D) je připojen k virtuálnímu zemnímu uzlu (103), source (S) je připojen k zemnímu vodiči a vývod (114) gate (G) je připojen k výstupu prvního řídicího signálu (C1), a/nebo

k virtuálnímu napájecímu uzlu (102) je připojen source (S) doplňkového tranzistoru (121) typu P, jehož drain (D) je připojen k výstupu O (101) a vývod (123) gate (G) je připojen k výstupu prvního řídicího signálu (C1),

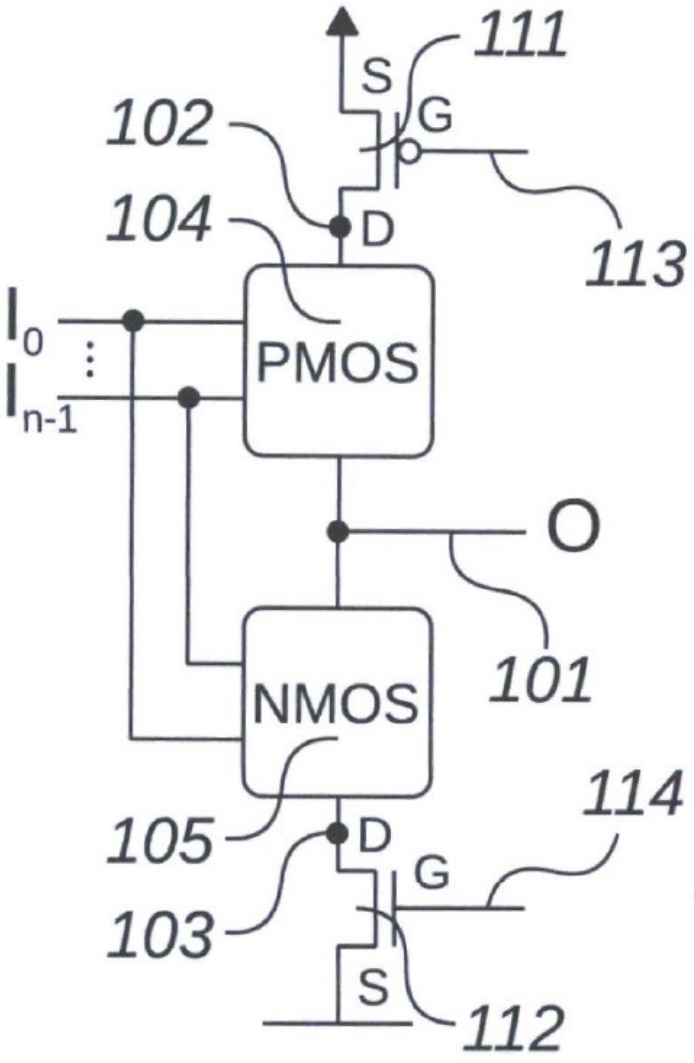
a/nebo

k virtuálnímu zemnímu uzlu (103) je připojen source (S) doplňkového tranzistoru (122) typu N, jehož drain (D) je připojen k výstupu O (101) a vývod (124) gate (G) je připojen k výstupu druhého řídicího signálu (C2).

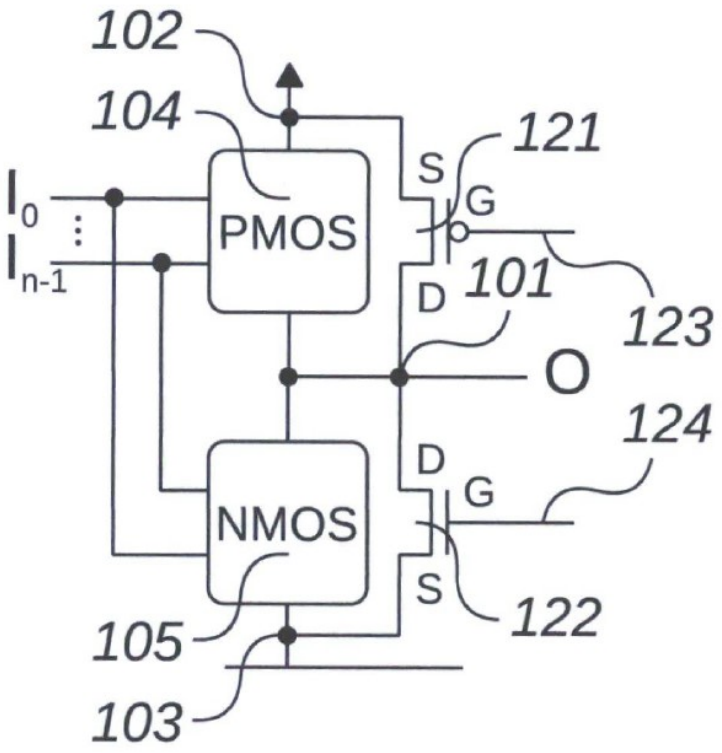
7 výkresů


100
200
O
Y
I_0
I_{n-1}
101
201

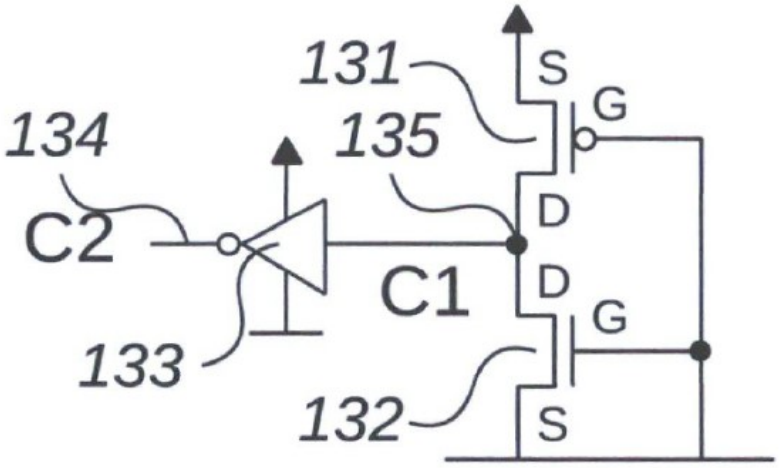
Obr. 1


S
111
G
102
D
104
113
I_0
I_{n-1}
PMOS
O
101
NMOS
114
105
D
G
103
S
112

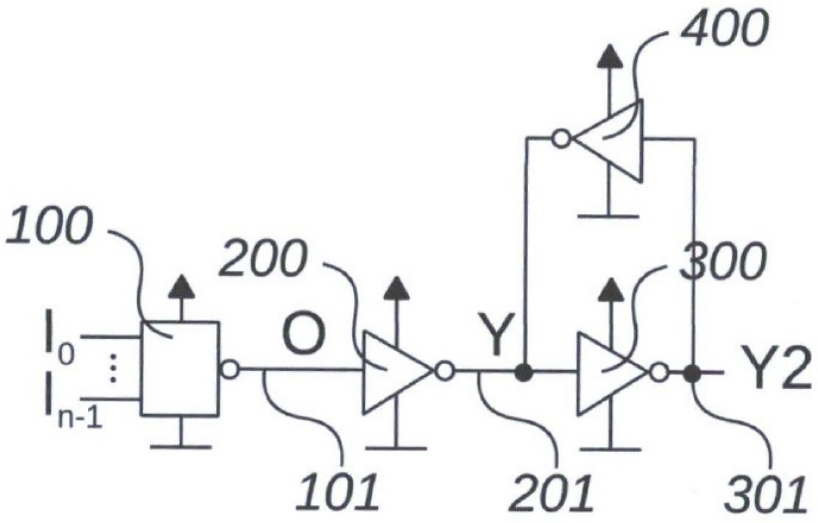
Obr. 2a


102
104
121
S
G
I_0
I_{n-1}
PMOS
D
101
123
O
124
D
G
NMOS
S
122
105
103

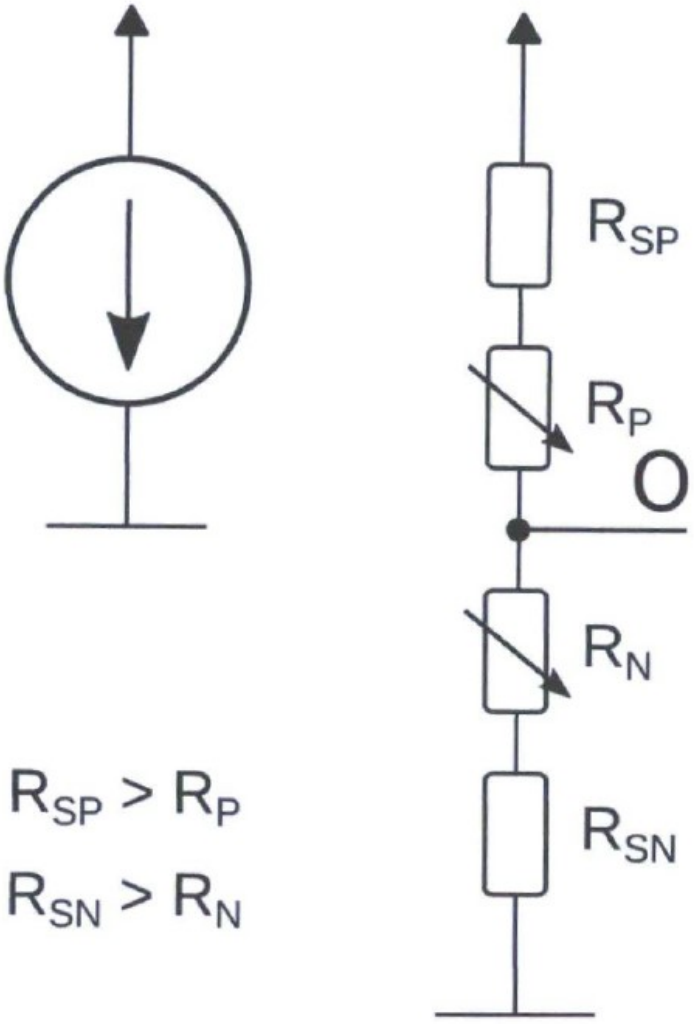
Obr. 2b


131
S
G
134
135
C2
D
C1
D
G
133
132
S

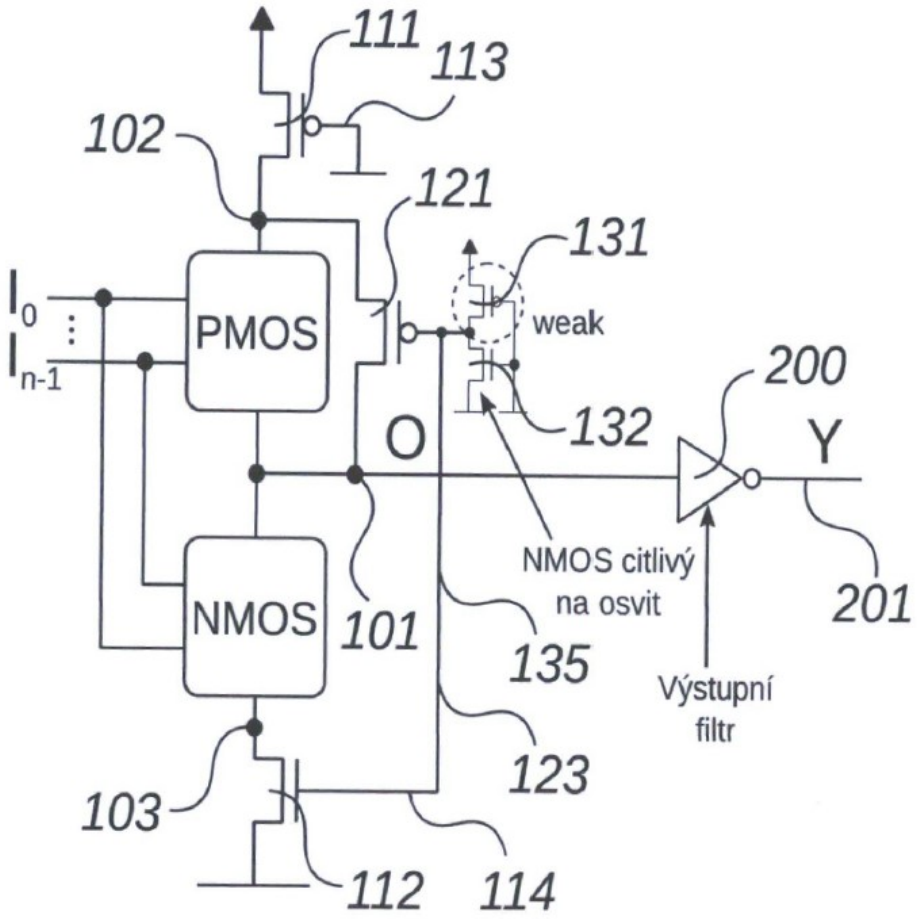
Obr. 2c



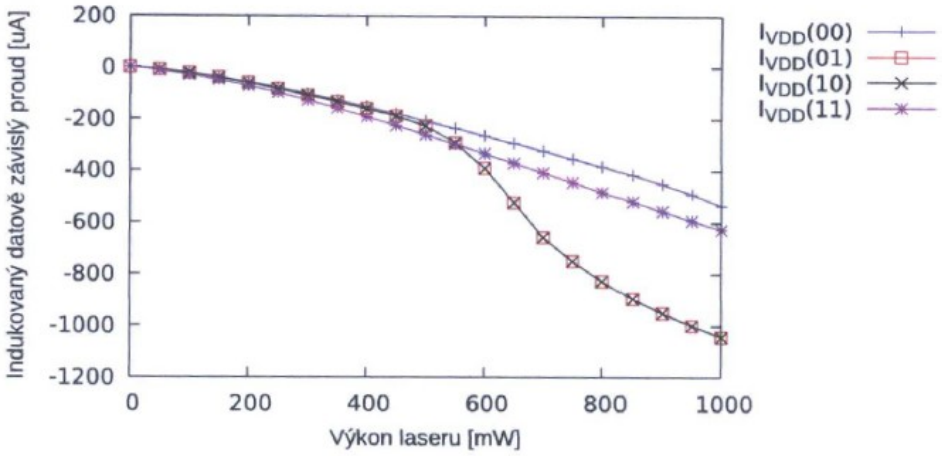
Obr. 3



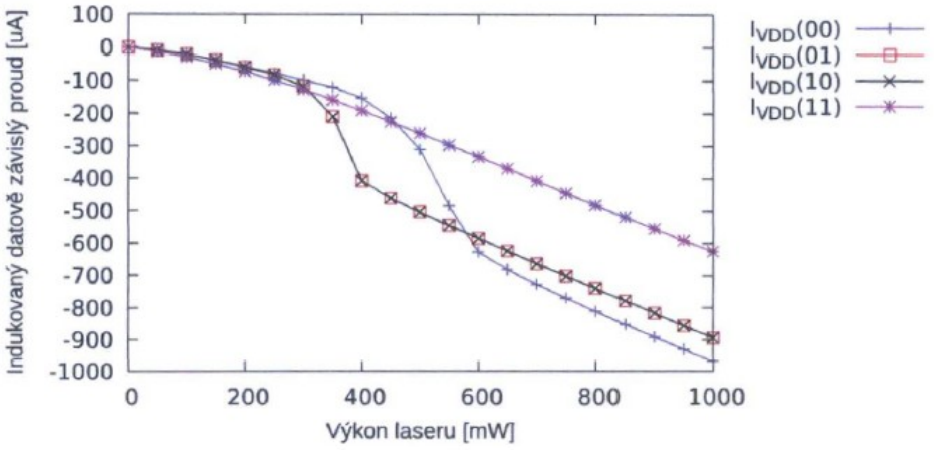
Obr. 4


111
113
102
121
131
I_0
I_{n-1}
PMOS
weak
200
132
O
Y
NMOS citlivý
na osvit
NMOS
101
201
135
Výstupní
filtr
123
103
112
114

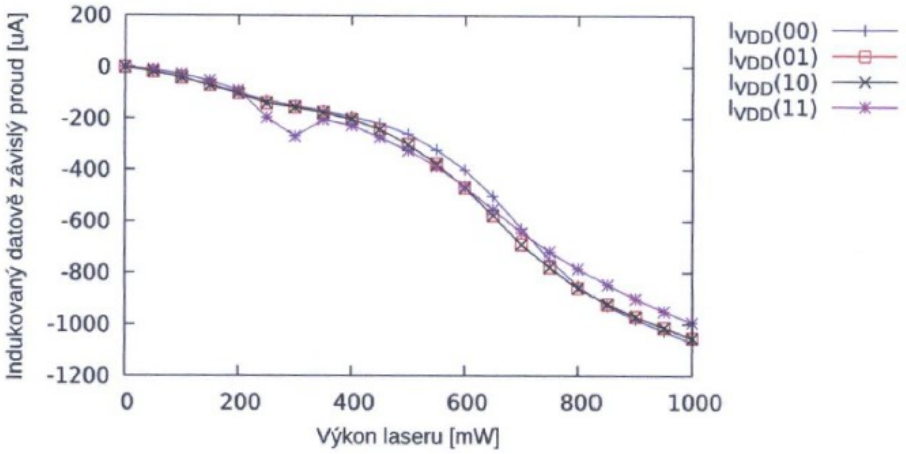
Obr. 5


Indukovaný datově závislý proud [uA]
200
0
-200
-400
-600
-800
-1000
-1200
0
200
400
600
800
1000
Výkon laseru [mW]
IVDD(00)
IVDD(01)
IVDD(10)
IVDD(11)

Obr. 6a


Indukovaný datově závislý proud [uA]
100
0
-100
-200
-300
-400
-500
-600
-700
-800
-900
-1000
0
200
400
600
800
1000
Výkon laseru [mW]
IVDD(00)
IVDD(01)
IVDD(10)
IVDD(11)

Obr. 6b


200
0
-200
-400
-600
-800
-1000
-1200
0
200
400
600
800
1000
Indukovaný datově závislý proud [uA]
Výkon laseru [mW]
IVDD(00)
IVDD(01)
IVDD(10)
IVDD(11)

Obr. 6c