

dr inż. Radosław Łuczak

Wydział Elektroniki i Informatyki Politechniki Koszalińskiej
ul. Śniadeckich 2, 75–411 Koszalin
rluczak@ie.tu.koszalin.pl

Koszalin, kwiecień – czerwiec 2011.

A gdyby tak posterować prądem ...

18 kwietnia 2011 r. minęła X rocznica śmierci prof. dr hab. inż. Andrzeja Guzińskiego, pomysłodawcy, założyciela i pierwszego dziekana Wydziału Elektroniki Politechniki Koszalińskiej. Będąc studentem pierwszego naboru elektroniki w naszym Wydziale poznałem prof. A. Guzińskiego, uczestniczyłem w Jego wykładach a dzisiaj kontynuuję także pracę badawczą zapoczątkowaną przez Niego.

Niech niniejszy tekst będzie sprawozdaniem z działalności naukowej całego zespołu osób, które swoim zaangażowaniem i pracą przyczyniły się do rozwoju idei **bramki prądowej**, wymyślonej przez profesora Andrzeja Guzińskiego.

1. Wprowadzenie

Budowa systemów mieszanych, cyfrowo–analogowych MADS (Mixed Analog–Digital System), w jednej strukturze krzemowej napotyka na wiele trudności związanych z przenoszeniem zakłóceń, powstających w części cyfrowej, na część analogową. Zmiany stanu logicznego w układzie cyfrowym powodują skokowe zmiany prądu pobieranego ze źródła zasilania. Powstają tzw. szpilki prądowe przenoszone po szynie zasilającej i poprzez podłoże, do części analogowej. Widmo powstającej w chwili przełączenia stanu „szpilki” zawiera szereg częstotliwości mieszczących się w paśmie roboczym części analogowej układu. Dochodzi w ten sposób do powstawania zakłóceń, szumów o amplitudzie przekraczającej nawet poziom użytecznego sygnału analogowego [1, 2, 3, 4]. Z tego powodu podejmuje się działania w celu redukcji wpływu zakłóceń powstających w części cyfrowej na część analogową. Są to próby separacji części cyfrowej i analogowej, powodujące wzrost kosztów produkcji układów mieszanych, przy czym, należy nadmienić, że nie są do końca skuteczne. Izolowanie, ekranowanie, separowanie to działania mające na celu redukcję skutków, a nie przyczyny zakłóceń.

Na początku lat 90–tych ubiegłego wieku, prof. dr hab. inż. Andrzej Guziński, założyciel i pierwszy dziekan Wydziału Elektroniki¹ Politechniki Koszalińskiej zaproponował koncepcję budowy układów cyfrowych pracujących w trybie prądowym (bramki prądowe). Założeniem konstrukcyjnym było zbudowanie układu o stałym poborze mocy ze źródła zasilania. Dzięki temu zmiana stanu układu cyfrowego nie powoduje wystąpienia zakłócenia w postaci szpilki prądowej, a zatem wpływ części cyfrowej na analogową będzie znikomo mały [1, 3].

Przeprowadzono badania, zrealizowano kilka projektów badawczych, przypuszczenia profesora Guzińskiego co do przydatności jego **bramek prądowych** do budowy mieszanych układów cyfrowo–analogowych okazały się słuszne i dość szybko zostały potwierdzone: *Wyniki pomiarów wskazują, że proponowane układy cyfrowe pracujące w trybie prądowym stanowią odpowiedź na potrzebę poszukiwania nowych rozwiązań w zakresie minimalizacji wpływu procesów przejściowych towarzyszących pracy układów cyfrowych na pracę*

¹ dzisiejszy Wydział Elektroniki i Informatyki Politechniki Koszalińskiej, wówczas Instytut Elektroniki przy Wydziale Mechanicznym.

układów analogowych umieszczonych na tym samym podłożu układu scalonego w mieszanych analogowo-cyfrowych układach scalonych².

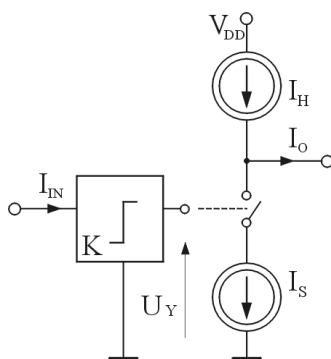
Dzisiaj, patrząc z perspektywy kilku minionych lat, poprzez pryzmat efektów uzyskanych przy pracy nad rozwojem technologii bramek prądowych, łatwiej jest nam ocenić istotę wynalazku profesora Guzińskiego, niż Jemu w czasie, kiedy ten powstawał. Wymyślając ideę bramki prądowej, profesorowi Guzińskiemu wydawało się, że otworzył furtkę do niskonakładowych konstrukcji mieszanych układów MADS. Nie mógł wówczas wiedzieć, że w rzeczywistości rozwarł wielkie wrota prowadzące do nowoczesnej elektroniki cyfrowej, do niespotykanej nigdzie prawdziwej logiki wielowartościowej (MVL – Multi Value Logic), do bezpiecznych systemów przetwarzających dane, do systemów kryptograficznych, wrota, o których istnieniu i znaczeniu nikt wówczas nie wiedział ...

2. Idea bramki prądowej

Istotą działania bramek prądowych jest wielkość fizyczna niosąca informację o stanie logicznym. W typowych układach cyfrowych ze stanem logicznym związane jest wystąpienie napięcia o określonej wartości, mieszczącej się w granicach wartości dopuszczalnych. W układach prądowych wielkością tą jest prąd wypływający z wyjścia bramki. Jest to cecha, która odróżnia bramki prądowe od innych technologii układów cyfrowych [5].

Prąd odpowiadający logicznemu poziomowi „1” ustalany jest w obwodzie polaryzacji (rys. 2.). Nazywa się go prądem jedynki i oznacza I_1 . Wartość prądu I_1 zależna jest od technologii wykonania bramki prądowej. Dla CMOS 0,6[μm] wartość tę ustala się na poziomie kilkunastu do kilkudziesięciu mikroamperów. Ponadto bramka pracuje w reżimie prądowym, tzn. niezależnie od stanu (statycznego czy dynamicznego) pobierany jest praktycznie stały prąd ze źródła zasilania. Prądowy tryb pracy układów oraz wielkość fizyczna niosąca informację o stanie logicznym zdecydowały o nazwie CMCL (Current-Mode Current Logic) dla systemów budowanych w oparciu o bramki prądowe.

Ideę działania bramki prądowej można omówić na przykładzie układu z rys. 1., przedstawiającego koncepcję budowy bramki inwertera prądowego. Zauważa się wyraźny podział na dwa moduły: moduł komparatora **K** i wyjściowy moduł inwertera **I** (I_H , klucz, I_S). Zadaniem modułu komparatora jest reakcja na prąd wejściowy, odpowiadający połowie I_1 , pojawieniem się napięcia sterującego U_Y . Napięcie to powoduje załączenie klucza i odprowadzenie prądu ze źródła I_H do masy poprzez źródło I_S (oba źródła o wydajności I_1 ³), prąd wyjściowy bramki (I_O) jest wówczas bliski 0[μA]. Jeżeli prąd wpływający do wejścia bramki ma niższą wartość od połowy I_1 , to napięcie U_Y jest bliskie 0[V] i klucz jest rozarty. Prąd wyjściowy I_O ma wartość I_1 , co wynika z wydajności źródła I_H . Z przedstawionego opisu wynika, że układ z rys. 1. dokonuje inwersji prądów.

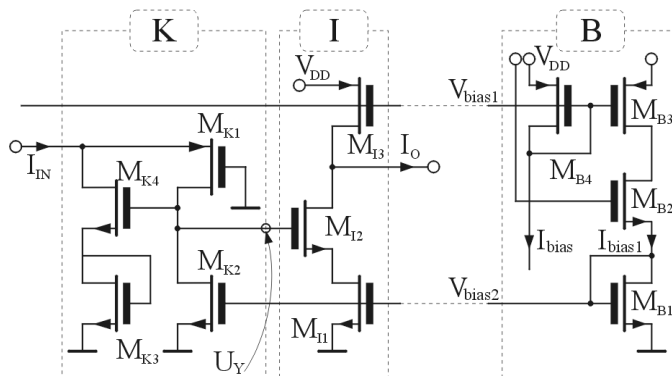


Rys. 1. Idea inwertera prądowego.

² za prof. dr. hab. inż. Andrzejem Guzińskim.

³ W brankach 3. generacji wydajność źródła I_S jest o ok. 6% większa od I_H . Stanowi to problem występujący przy próbie budowy bramki MVL, gdyż każdy inwerter w stanie „0” odbiera ok. 6% prądu I_1 od połączonego z nim inwertera w stanie „1”.

Na rys. 2. przedstawiono przykład realizacji bramki typu inwerter w technologii CMOS wraz z układem polaryzacji. Jest to już trzecia generacja bramek prądowych. Inwerter wymyślony przez prof. Guzińskiego miał nieco inną, prostszą budowę. Od chwili wynalezienia, bramki prądowe przeszły kilka znaczących modyfikacji w celu poprawy ich właściwości, co pokazuje, że idea jest wciąż żywa i rozwijana.



Rys. 2. Przykład implementacji inwertera prądowego w technologii CMOS, wraz z układem polaryzacji.

Modyfikacje bramek prądowych wcześniejszych generacji dotyczyły przede wszystkim modułu komparatora **K**, który na początku realizowany był na pojedynczym tranzystorze w połączeniu diodowym. W bramkach trzeciej generacji komparator **K** zbudowany jest ze źródła prądowego, zrealizowanego na M_{K2} , o wydajności $\frac{1}{2} I_1$ oraz układu klucz – obciążenie (M_{K4} , M_{K3}) odbierającego nadwyżkę prądu. W trzeciej generacji, do syntezy układów cyfrowych wykorzystuje się bramki prądowe zbudowane z udziałem 4 istniejących modułów: **K** – komparator, **I** – moduł inwertera, **AI** – moduł anti-inwertera, **SI** – prosty moduł inwersji napięć.

W tab. 1. podano nazwy i oznaczenia znanych bramek prądowych, ich budowę, realizowane operacje logiczne (różne rodzaje negacji charakterystyczne dla algebry prądowej) oraz tablice prawdy i prądy pobierane ze źródła zasilania.

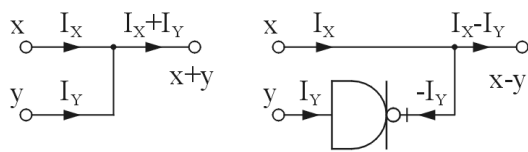
Tab. 1. Podstawowe typy bramek CMCL, ich budowa z dostępnych modułów, realizowane funkcje logiczne, tablice prawdy i pobór prądu ze źródła zasilania.

<p>Inwerter</p> <p>$y = \bar{x}$</p> <p>$I = 1 \cdot I_1$</p>		<p>podwójny inwerter</p> <p>$y = \bar{\bar{x}}$</p> <p>$I = 2 \cdot I_1$</p>															
<table border="0"> <tr><td>x</td><td>y</td></tr> <tr><td>-n</td><td>1</td></tr> <tr><td>0</td><td>1</td></tr> <tr><td>n</td><td>0</td></tr> </table>	x	y	-n	1	0	1	n	0	<table border="0"> <tr><td>x</td><td>y</td></tr> <tr><td>-n</td><td>0</td></tr> <tr><td>0</td><td>0</td></tr> <tr><td>n</td><td>1</td></tr> </table>	x	y	-n	0	0	0	n	1
x	y																
-n	1																
0	1																
n	0																
x	y																
-n	0																
0	0																
n	1																
<p>anti-inwerter</p> <p>$y = \hat{x}$</p> <p>$I = 0 \cdot I_1$</p>		<p>podwójny anti-inwerter</p> <p>$y = \hat{\hat{x}}$</p> <p>$I = 1 \cdot I_1$</p>															
<table border="0"> <tr><td>x</td><td>y</td></tr> <tr><td>-n</td><td>0</td></tr> <tr><td>0</td><td>0</td></tr> <tr><td>n</td><td>-1</td></tr> </table>	x	y	-n	0	0	0	n	-1	<table border="0"> <tr><td>x</td><td>y</td></tr> <tr><td>-n</td><td>-1</td></tr> <tr><td>0</td><td>-1</td></tr> <tr><td>n</td><td>0</td></tr> </table>	x	y	-n	-1	0	-1	n	0
x	y																
-n	0																
0	0																
n	-1																
x	y																
-n	-1																
0	-1																
n	0																

Bramki prądowe mają budowę modułową. Każda posiada jedno wejście. Na wejściu znajduje się komparator **K**. Do komparatora podłącza się do 8 wyjść jednego z 4 typów. Wyjścia realizują 4 różne inwersje prądowe. Realizacja wyjść typu podwójny inwerter oraz podwójny anti-inwerter wymaga zastosowania prostego modułu inwersji (**SI**) dołączonego do komparatora, co zwiększa liczbę wykorzystanych tranzystorów. Do syntezy układów logicznych bardzo atrakcyjne wydają się wyjścia inwertera i anti-inwertera zbudowane odpowiednio z 3 i 2 tranzystorów ze względu na najmniejszą liczbę tranzystorów występujących w bramce. W układach syntezowanych z bramek prądowych występują trzy podstawowe stany logiczne: „-1”, „0”, „1”, oraz ich wielokrotności. Z tego względu „logika prądowa” różni się od typowej logiki Boolowskiej.

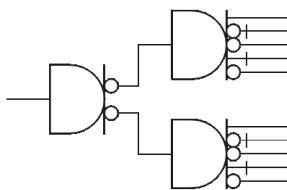
2.1. Elementy algebry prądowej

Logika prądowa pozwala na prostą realizację sumy arytmetycznej bez ponoszenia żadnego nakładu sprzętowego. Aby ją otrzymać, wystarczy połączyć ze sobą wyjścia bramek, prąd wypływający z takiego węzła będzie sumą prądów doprowadzonych (rys. 3). Ta cecha układów prądowych wydaje się bardzo atrakcyjna do syntezy układów cyfrowych gdyż realizacja funkcji logicznych odbywa się przy niewielkim nakładzie sprzętowym [5, 6, 7].



Rys. 3. Realizacja operacji dodawania i odejmowania arytmetycznego w układach prądowych.

Niestety, aby zrealizować jednocześnie kilka funkcji z udziałem sygnału prądowego x , należy wcześniej go powielić. Jak już wspomniano, w systemach CMCL wielkością fizyczną niosącą informację o stanie logicznym jest prąd i nie można powielić sygnału cyfrowego poprzez rozgałęzienie ścieżki. Spowodowałoby to rozdzielenie prądu o wartości zdeterminowanej stanem logicznym na części, z których żadna nie niosła by właściwej informacji. Uzyskanie powielenia odbywa się poprzez zastosowanie powielającej bramki wielowyjściowej, co powoduje wzrost nakładu sprzętowego.



Rys. 4. Powielanie sygnału –kaskadowe połączenie bramek prądowych.

Opisane powielanie logicznych sygnałów prądowych za pomocą bramek powielających wydają się być głównym powodem dużej złożoności sprzętowej i nadmiernego poboru mocy ze źródła zasilania w systemach CMCL [8, 9].

Należy nadmienić, że na skutek sumowania, oprócz podstawowych stanów logicznych: „-1”, „0”, „1”, w logice prądowej występują także wielokrotności tych stanów. Na wejściu bramki może pojawić się prąd o wartości ze zbioru $(-n, \dots, 0, \dots, n)$ [10]. Daje to możliwość realizacji systemów pracujących w logice wielowartościowej. Aksjomaty i tożsamości algebry bramek prądowych zostały dokładnie opisane w [6, 7, 11, 12, 13, 14].

2.2. Pobór mocy w cyfrowych układach prądowych

Wspomniano, że bramki prądowe pobierają stałą moc ze źródła zasilania. Dzieje się tak dlatego, że prąd jedynek pobierany jest przez pewne obwody w bramce (konkretnie przez prosty układ inwersji **SI** i układ wyjścia typu inwerter **I**) nieustannie, zmienia się jedynie ścieżka przepływu prądu przy przełączaniu klucza sterującego źródłem I_s . Najmniej korzystną bramką prądową pod kątem konsumpcji mocy jest bramka podwójnego inwertera gdyż zbudowana jest z układu **SI** i modułu wyjściowego **I**, które pobierają prąd odpowiadający logicznej jedynce. Pobór prądu ze źródła zasilania dla wszystkich bramek z jednym wyjściem przedstawiono w tab. 1.

W cyfrowych układach prądowych występuje problem dużego poboru mocy. Całkowity pobór mocy systemu CMCL zależy od sumy układów **SI** i sumy wyjść typu inwerter. Redukcję poboru mocy można uzyskać zmniejszając wartość prądu jedynek, jednakże powoduje to zwiększenie czasu propagacji bramki, który zależy od szybkości przeładowania pasozytniczych pojemności bramki tranzystora (klucza) sterowanego komparatorem. Pojemności te przeładowywane są w czasie przełączania stanu logicznego co najwyżej prądem jedynek. Obniżenie wartości tego prądu redukuje jednocześnie szybkość pracy układu cyfrowego. W praktyce więc redukcji poboru mocy nie da się uzyskać przez zmniejszenie prądu jedynek, należy raczej dążyć do zwiększania tej wartości ze względu na szybkość pracy układu. Znaczące rozwiązanie problemu poboru mocy przedstawione zostanie w kolejnych rozdziałach, przy omawianiu najnowszych wyników związanych z bramkami 4. generacji.

Rozważania na temat mocy pobieranej przez bramki prądowe należy zakończyć przedstawieniem pewnego aspektu związanego ze stałym prądem pobieranym ze źródła. O ile w układzie prądowym nie występują

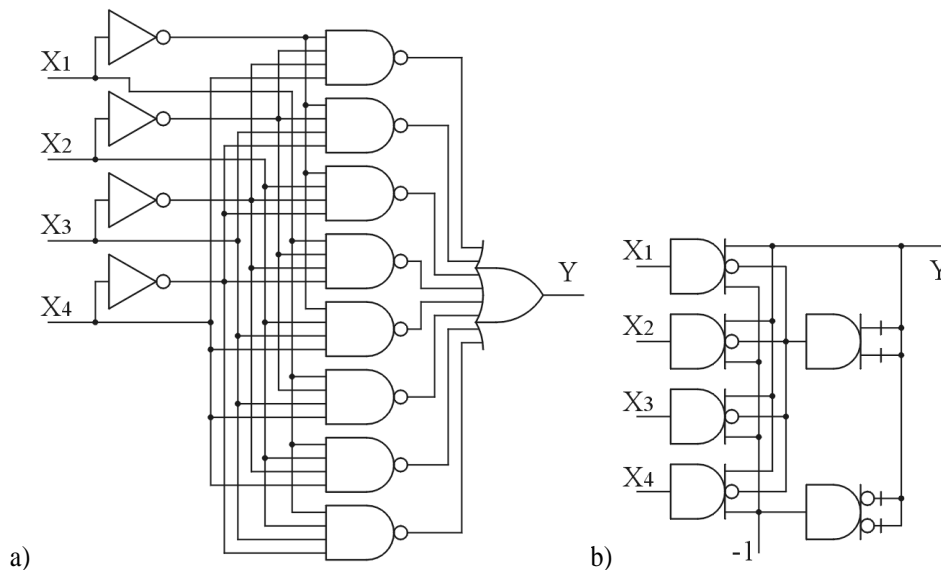
skokowe zmiany mocy przy przełączaniu stanu logicznego, to jednocześnie nie zachodzą znaczące zmiany poziomu pola elektromagnetycznego, generowanego przez układ cyfrowy, co zostanie szerzej przedstawione w rozdziale 3. przy wykorzystaniu CMCL dla celów bezpieczeństwa emisji elektromagnetycznej systemów przetwarzających dane.

3. Potencjał bramek prądowych

Bramki prądowe mają dwie charakterystyczne cechy dające potencjalne możliwości wykorzystania ich w takich sytuacjach, gdzie zastosowanie klasycznych bramek stwarza poważne problemy lub jest zwyczajnie niemożliwe. Pierwszą z cech jest praca w trybie prądowym, z czego wynika praktycznie stały pobór mocy, drugą jest reprezentacja stanu logicznego za pomocą prądu. W niniejszym rozdziale przedstawiono potencjalne zastosowania CMCL wynikające z przedstawionych cech tych układów i płynące z tego korzyści [10].

3.1. Prosta realizacja funkcji logicznych

W 2.1. pokazany został sposób realizacji funkcji logicznych w algebrze bramek prądowych. Istotą jest możliwość zrealizowania sumy arytmetycznej prądów poprzez połączenie wyjść bramek, czyli bez udziału funktora logicznego. Wiąże się z tym redukcja nakładu sprzętowego w układzie cyfrowym. Jednocześnie przykład pokazuje, że funkcje logiczne w algebrze bramek prądowych realizowane są zupełnie inaczej niż w przypadku klasycznych bramek cyfrowych. Algebra „prądowa” jest inna od algebry Boolowskiej. Okazało się niezbędne wprowadzenie podstawowych tożsamości oraz opracowanie metod minimalizacji [12, 13, 14].



Rys. 5. Przykład układu kombinacyjnego a) zbudowanego z klasycznych bramek b) realizujący tą samą funkcję logiczną układ z bramek prądowych.

Opracowanie odpowiednich, automatycznych technik minimalizacji funkcji logicznych w algebrze bramek prądowych okazało się problemem niezwykle trudnym. Prace badawcze trwały kilka lat. W pierwszym etapie synteza układów prądowych była heurystyczna. Struktura systemu cyfrowego zależała od doświadczenia osoby projektującej układ. W efekcie wypracowano jednak metody pozwalające na uzyskanie bardzo prostych (w porównaniu z bramkami napięciowymi) struktur logicznych, realizujących te same funkcje [5, 6, 7, 10, 11]. Przedstawiony na rys. 5. przykład pokazuje, że stosowanie bramek cyfrowych pracujących w trybie prądowym umożliwia skorzystanie z rozszerzonych reguł charakterystycznych wyłącznie dla tych układów. Reguły te wykraczają poza stosowane w klasycznych układach cyfrowych, pracujących według logiki boolowskiej, prawa deMorgana. Korzyścią jest możliwość wydajnej minimalizacji funkcji logicznych, a w rezultacie: prosta postać

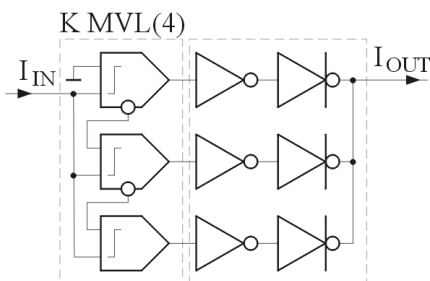
układów kombinacyjnych; szybko działające układy; redukcja nakładu sprzętowego oraz radykalne zmniejszenie liczby i całkowitej długości połączeń występujących w układzie cyfrowym.

Największy wkład w opracowanie technik minimalizacji wniósł Śp. prof. dr. hab. inż. Oleg Maslennikow, który przez wiele lat kierował zespołem badawczym, zajmującym się rozwojem idei prof. A. Guzińskiego. Prace prof. O. Maslennikowa zaowocowały istniejącymi dzisiaj technikami minimalizacji, pozwalającymi na syntezę układów CMCL, charakteryzującymi się minimalną strukturą.

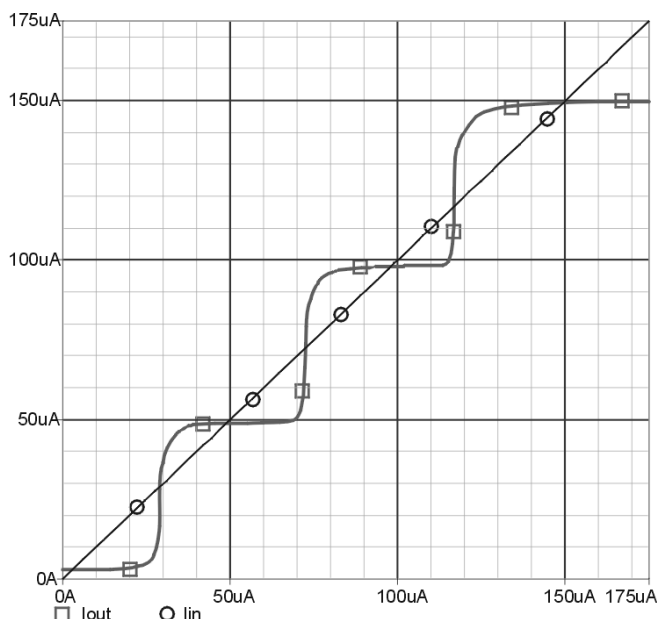
3.2. Budowa systemów pracujących w logice wielowartościowej

W praktyce układów cyfrowych spotyka się jedynie systemy binarne. Istnieją próby realizacji układów pracujących w tzw. logice „wielowartościowej”, jednakże występują tam tylko trzy poziomy: niski, wysoki i stan wysokiej impedancji (czyli brak konkretnego poziomu logicznego, stan wysokiej impedancji można traktować jak odłączenie bramki od układu). Wynika to stąd, że w przypadku bramek napięciowych nie można zrealizować prawdziwej logiki wielowartościowej, gdyż zazwyczaj poziom niski reprezentowany jest przez napięcie bliskie V_{SS} , a wysoki przez napięcie bliskie V_{DD} . Z tego wynika, że w przedziale $V_{SS} .. V_{DD}$ (co odpowiada napięciu zasilania) nie ma miejsca na dodatkowe poziomy logiczne. Obniżenie poziomu napięcia związanego ze stanem „1” do poziomu odpowiadającego $U_1=(V_{DD}-V_{SS})/(N-1)$, gdzie N —podstawa systemu, spowodowałaby, po pierwsze, zmniejszenie stosunku sygnał/szum, a ponadto wymusiłaby redukcję tolerancji napięć odpowiadających za stany logiczne i spowodowałaby wzrost nakładu sprzętowego wynikający z konieczności dyskryminacji tych stanów.

W przypadku bramek prądowych implementacja MVL odbywa się w sposób naturalny. Dzięki temu, że poziom logiczny reprezentowany jest przez prąd wypływający z bramki, możliwe jest uzyskanie sumy arytmetycznej kilku prądów I_1 . W CMCL jest to zjawisko powszechne, gdyż w taki właśnie sposób realizowane są funkcje logiczne. Do prawdziwej logiki wielowartościowej konieczne jest jedynie zrealizowanie komparatora MVL(N), który dokona interpretacji prądu wejściowego, reagując na wejściowy prąd o wartości $n \cdot I_1$ wygenerowaniem n napięć sterujących U_Y . Dołączając do komparatora $N-1$ połączonych modułów wyjściowych jednakowego typu uzyskuje się bramkę prądową MVL(N).



Rys. 6. Bramka prądowa MVL(4) typu podwójny inwerter.



Rys. 7. Charakterystyka przejściowa bramki MVL(4) typu podwójny inwerter.[†]

W chwili obecnej, powstała czwarta generacja bramek prądowych, która umożliwia budowanie systemów CMCL pracujących w logice wielowartościowej z podstawą do $N=8$ włącznie, której poświęcono czwarty rozdział [14].

Zastosowanie MVL w systemach cyfrowych niesie ze sobą kolejną możliwość redukcji całkowitej długości połączeń występujących w układzie scalonym poprzez redukcję szerokości magistrali danych. Przykładowo, dla MVL(4) szerokość magistrali maleje dwukrotnie w stosunku do systemu binarnego. Wiadomo, że szybkość działania współczesnych układów cyfrowych nie zależy tak bardzo od czasu propagacji bramki, jak od opóźnień sygnału cyfrowego w torze logicznym. Decydujący wpływ na te opóźnienia ma długość połączeń występujących między bramkami cyfrowymi. Nie bez znaczenia jest także powierzchnia zajmowana przez szyny sygnałowe w układzie scalonym. Logika wielowartościowa daje możliwość redukcji powierzchni układu scalonego poprzez redukcję całkowitej długości i ilości połączeń, co wpływa pośrednio na wzrost szybkości przetwarzania układu.

3.3. Kryptografia

Obecnie obserwuje się gwałtowny rozwój tzw. inżynierii zabezpieczeń – stosunkowo nowej dyscypliny naukowej, zajmującej się różnymi aspektami ochrony informacji. W ostatnich latach liczba aspektów bezpieczeństwa danych szybko wzrasta. Obecnie dotyczy, oprócz kryptografii i kontroli dostępu do informacji, m.in. problemów odporności sprzętu na penetrowanie fizyczne oraz zapewnienia bezpieczeństwa emisji elektromagnetycznej systemów komputerowych (Emsec – emission security), a w szczególności bezpieczeństwa emisji systemów kryptograficznych. Pojawia się problem ochrony systemów kryptograficznych przed atakami SCA (Side Channel Attack) polegającymi na tzw. „podśluchiwaniu”, tj. na analizie zmian poboru mocy (Power Analysis Attacks – PAA) lub pola elektromagnetycznego (ElectroMagnetic Attack – EMA).

Klasyczne cyfrowe bramki CMOS, które są powszechnie stosowane w systemach komputerowych, w tym kryptograficznych, prawie nie pobierają prądu ze źródła zasilania w stanach ustalonych (stan „0” lub „1”), natomiast pobierają od kilku do kilkunastu tysięcy razy większy prąd w trakcie zmiany stanu. Zmiana stanu logicznego wiąże się ze zmianą polaryzacji sieci podciągającej i ściągającej w bramce. W obszarze przejściowym obie sieci przewodzą, a tranzystory są w nasyceniu. Umożliwia to swobodny przepływ prądu od zasilania do masy, ograniczony jedynie chwilową rezystancją tranzystorów MOS (w nasyceniu). Te względnie duże impulsy prądu (tzw. szpilki prądowe) powodują powstanie charakterystycznych zakłóceń (szumu cyfrowego) na szynach zasilania systemu. Można wykazać, że różne rozkazy mikroprocesora mają różne profile poboru mocy. Atakujący, analizując szum (fluktuacje napięcia i/lub prądu) na szynie zasilania mikroprocesora, może określić, jaka

instrukcja jest wykonywana, a nawet na jakich danych!. Okazuje się, że mając informacje o tym, jaki mikroprocesor działa w systemie kryptograficznym i jaki algorytm szyfrowania jest zaimplementowany, mierząc prąd pobierany przez mikroprocesor w trakcie szyfrowania, można rekonstruować klucz szyfrujący (deszyfrujący). Do przeprowadzenia ataku PAA (pomiar, rejestracja i analiza prądu/napięcia zasilania) konieczny jest fizyczny dostęp do systemu, co nie zawsze jest możliwe. Istnieje bardziej wyrafinowany typ ataku – nie wymagający bezpośredniej ingerencji bądź kontaktu z systemem cyfrowym, polegający na analizie zmian emitowanego przez system pola elektromagnetycznego (EMA). W celu pomiaru tych zmian konieczne jest dysponowanie zaawansowanym sprzętem – specjalną anteną i odbiornikiem pomiarowym. Oba rodzaje ataków należą do jednej rodziny SCA, gdyż przyczyna zmian emisji pola jest ta sama – szpilki prądowe powstające w obwodach układu podczas przełączania bramek cyfrowych.

Rozwijane są różne metody skierowane na zapewnienie bezpieczeństwa emisji oraz przeciwdziałania atakom SCA. Metody te działają głównie na poziomie oprogramowania systemu (np. poprzez ujednoczenie czasu trwania operacji; wprowadzenie operacji nadmiarowych; itd.) lub na poziomie sprzętu (np. wprowadzenie generatorów szumu i/lub układów uśredniających pobór mocy; wprowadzenie osobnego, wewnętrznego zegara systemowego zmieniającego swoją częstotliwość, stosowanie układów samosynchronizujących się, itd.). Innym sposobem jest ekranowanie urządzeń. Wymienione metody (choć niezwykle kosztowne) nie zabezpieczają systemów kryptograficznych przed „podsluchaniem”, a tylko utrudniają jego przeprowadzenie.

Innym kierunkiem zapewnienia bezpieczeństwa emisji oraz przeciwdziałania atakom SCA może być wykorzystanie w systemie bramek CMCL. Ponieważ w/w bramki pobierają prawie stały prąd ze źródła zasilania zarówno w stanach ustalonych, jak i podczas przełączania się, atak polegający na analizie zmian poboru mocy lub pola elektromagnetycznego układu podczas jego działania jest skazany na niepowodzenie w znacznie większym stopniu, niż w przypadku układów i systemów cyfrowych zbudowanych z klasycznych bramek CMOS. Wstępne badania opracowanego układu ASIC, zrealizowanego w technologii 0,35[μm], wykazały, że układ prądowy cechuje się znacznie mniejszym poziomem emisji elektromagnetycznej niż jego odpowiednik klasyczny. Ponadto, zapis dynamiki emisji układu CMCL (tzw. profil emisji) nie zawiera fragmentów charakterystycznych, pozwalających na wykonanie analizy różnicowej. Układy prądowe są odporne na różnicową analizę mocy oraz na analizę emisji elektromagnetycznej (ataki SCA). Pozwoli to na znaczące obniżenie kosztów produkcji systemów kryptograficznych, odpornych na ataki SCA.

3.4. Problemy w technologii CMCL

Oprócz wielu zalet i wynikających z nich potencjalnych możliwości układów CMCL istnieją też cechy niepożądane. W układach cyfrowych realizowanych w oparciu o bramki prądowe występują dwa podstawowe problemy: problem dużego poboru mocy i problem dużego czasu propagacji bramki. O poborze mocy pisano już w rozdziale 2.2. W rozdziale 2.1. wspomniano o konieczności powielania sygnałów prądowych, co powoduje wzrost nakładu sprzętowego. Wraz ze wzrostem złożoności układu dochodzi do wzrostu opóźnień w torze sygnału logicznego. Jak się okazuje oba występujące problemy mają wspólne źródło jakim jest złożoność układu cyfrowego. Częściowe rozwiązanie obu występujących problemów zostanie przedstawione w kolejnym rozdziale, który poświęcono kolejnej generacji bramek prądowych, w której uzyskano znaczącą redukcję nakładu sprzętowego, pobieranej mocy i opóźnień w torze sygnału.

4. Bramki 4. generacji

Najnowsze badania związane z rozwojem koncepcji prof. A. Guzińskiego dotyczącej bramek prądowych, przeprowadzone w latach 2009 – 2011 zaowocowały powstaniem bramek 4. generacji. Wprowadzono dwie znaczące modyfikacje w stosunku do poprzednich realizacji bramek.

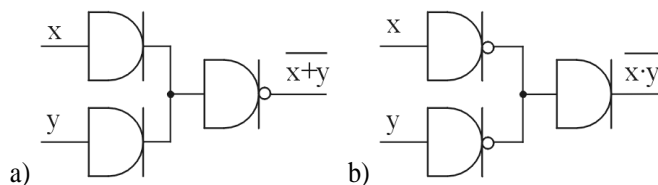
Modyfikacja pierwsza – liczba wejść: Bramki prądowe do 3. generacji włącznie posiadały jedno wejście, mogły natomiast mieć więcej niż jedno wyjście. W czasie badań nad minimalizacją funkcji logicznych w algebrze prądowej zauważono możliwość redukcji nakładu sprzętowego poprzez zaprojektowanie bramki dwuwejściowej dla realizacji jednej z funkcji charakterystycznych (funkcja wzorcowa typu T), opisujących układ kombinacyjny

[9]. Zastosowanie bramek wielowejsiowych okazało się wyjątkowo eleganckie. Modyfikacja druga – tolerancja prądów: Ze względu na konieczność ograniczenia prądu wypływającego z bramki w stanie „0” (tzw. prąd szczytkowy I_R) w module wyjściowym typu inwerter, w bramkach 3. generacji przyjęto zwiększoną wydajność źródła I_S , poprzez zwiększenie szerokości kanału tranzystora M_{11} (rys. 2.). Takie działanie pozwoliło na polepszenie parametrów bramek dla systemów binarnych, ale uniemożliwiło zarazem budowanie bramek wielowartościowych. W czasie prac związanych z projektem badawczym, którego celem jest wykorzystanie bramek prądowych w kryptografii, wykorzystanie logiki wielowartościowej okazało się niezwykle przydatne. Dokonano więc zmniejszenia wydajności źródła I_S do wartości dokładnie I_1 , co poskutkowało wzrostem prądu szczytkowego. Zmodyfikowano zatem moduł wyjściowy typu inwerter poprzez implementację klucza przełączającego n-p w celu redukcji prądu szczytkowego, co zmieniło nieco ideę działania bramki. Uzyskano w ten sposób znaczącą redukcję prądu szczytkowego oraz możliwość budowy układów w logice wielowartościowej [14].

4.1. Bramki wielowejsiowe [9]

Przy minimalizacji funkcji logicznych dla CMCL, chętnie wykorzystywaną bramką jest bramka typu anti-inwerter ze względu na najmniejszą liczbę tranzystorów. Zastosowanie anti-inwertera powoduje częste występowanie stanu logicznego „-1” w systemie cyfrowym. Poziom „-1” jest specyficzny, gdyż traktowany jest, z punktu widzenia logiki prądowej, jak stan „0”. W związku z tym operacja logiczna „-1” + „1” powinna mieć wartość „1”, tymczasem suma algebraiczna prądów wynosi 0.

Jeżeli chociaż jeden z sygnałów może przyjmować wartość „-1”, to sumy logicznej nie da się zrealizować poprzez sumowanie prądów w węźle. Konieczne jest zastosowanie wówczas bramek typu podwójny inwerter (lub inwerter) na wejściach, w celu normalizacji sygnałów prądowych i sprowadzenia ich z zakresu (-n .. n) do jednego ze stanów („0”, „1”). Z tego samego powodu, na wyjściu dołącza się dodatkową bramkę, jak na rys. 8.

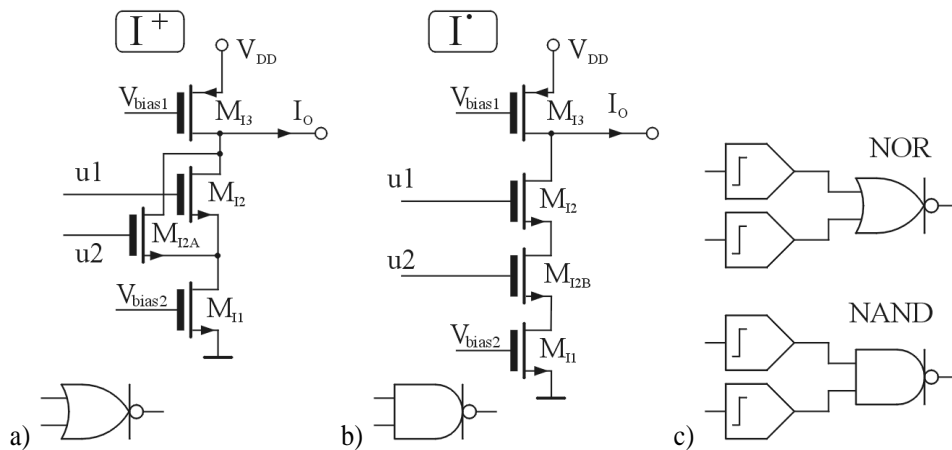


Rys. 8. Realizacja operacji logicznych a) NOR b) NAND na bramkach prądowych.

Należy wyjaśnić, że bramki potrzebne są tylko na tych wejściach, na których może wystąpić stan „-n”. Okazuje się, że takie sytuacje występują w praktyce dość często [8, 9].

Struktura z rys. 8.a, realizująca prądową funkcję NOR, zbudowana jest z trzech bramek. Do jej realizacji sprzętowej w technologii CMOS, wykorzystano 27 tranzystorów, a pobór prądu wynosi $5 \cdot I_1$. Realizacja funkcji NAND wymaga wykorzystania 24 tranzystorów przy poborze prądu $4 \cdot I_1$. Możliwa jest redukcja zarówno ilości tranzystorów, jak i mocy, poprzez zastosowanie dwuwejściowego modułu inwertera.

Do modułu inwertera (**I**) można dołączyć dodatkowy tranzystor-klucz. Stosuje się równoległe bądź szeregowe połączenie kluczy, oznaczonych na rys. 9. jako M_{12} i $M_{12A/B}$. Uzyskuje się w ten sposób moduł wyjściowy typu inwerter, sterowany sygnałami napięciowymi u_1 i u_2 , który nie realizuje już jedynie negacji (ale sumę lub iloczyn logiczny), gdyż stan wyjścia zależy od stanu obu wejść.



Rys. 9. Dwuwęściowe moduły inwertera i ich symbole a) z kluczami równoległymi b) z kluczami połączonymi szeregowo c) nowa realizacja NOR i NAND.

Dołączając komparatory do wejść tak zbudowanych modułów, buduje się dwuwęściowe bramki prądowe realizujące operacje NOR i NAND w algebrze prądowej. Do budowy każdej z nich wykorzystuje się 12 tranzystorów, a prąd pobierany ze źródła jest równy I_1 . W porównaniu z układami z rys. 8., realizującymi te same funkcje logiczne, następuje **dwukrotna** redukcja złożoności sprzętowej i **czterokrotna** redukcja pobieranego prądu. Wykorzystanie wielowęściowego modułu inwertera do konstrukcji bramek wielowęściowych daje znaczący zysk związany z mniejszym nakładem sprzętowym i redukcją mocy pobieranej przez prądowy system cyfrowy.

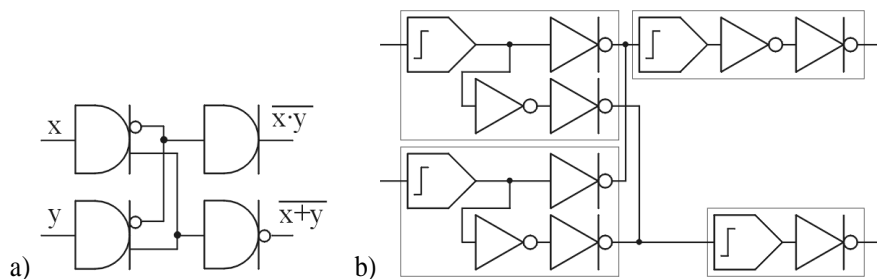
Podobnie można postąpić z modułem anti-inwertera (**AI**) i modułem inwersji napięciowej (**SI**), uzyskując możliwość tworzenia całej gamy nowych, wielowęściowych bramek prądowych, obok czterech, do tej pory stosowanych bramek realizujących jedynie negacje [9].

Tab. 2. Wykorzystywane dotychczas i nowo opracowane moduły do syntezy bramek prądowych.

	komparator	inwerter	anti-inwerter	inw. napięcia
znane moduły	4	3	2	3
nowe moduły	7	4	3	4
		4	3	4

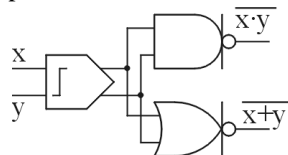
W tab. 2. podano oznaczenia znanych i nowych modułów do syntezy bramek CMCL. Kształt symbolu wiąże się z operacją logiczną, wykonywaną na sygnałach wejściowych, symbol na wyjściu modułów inwertera i anti-inwertera oznacza realizowaną negację prądową. Obok symboli zamieszczono liczby mówiące o ilości tranzystorów.

Jako ilustrację zysku jaki niesie zastosowanie bramek wielowęściowych zaprezentowany zostanie prosty przykład jednoczesnej realizacji funkcji NOR i NAND na sygnałach x i y , pokazany na rys. 10. Należy zwrócić uwagę, że 2 bramki wejściowe służą nie tylko normalizacji wejściowych sygnałów x i y , ale także powieleniu tych sygnałów prądowych w celu jednoczesnego wykonywania wielu funkcji logicznych.



Rys. 10. Jednoczesna realizacja funkcji logicznych NOR i NAND a) na bramkach prądowych b) z pokazaniem wewnętrznej, modułowej struktury bramek.

Do jednoczesnej realizacji funkcji NAND i NOR wykorzystano 4 bramki prądowe. Pobór mocy tego układu jest równy $9 \cdot I_1$, a na jego budowę składają się 43 tranzystory. Wykorzystanie dwuwęściowego modułu inwertera i dwuwęściowego komparatora pozwala na zbudowanie struktury pokazanej na rys. 11. Układ składa się z 15 tranzystorów, a prąd pobierany ze źródła wynosi $2 \cdot I_1$. Nastąpiła **trzykrotna** redukcja złożoności sprzętowej i ponad **czterokrotna** redukcja pobieranej mocy.



Rys. 11. Dwuwęściowa bramka prądowa NOR/NAND z wykorzystaniem modułów wielowęściowych (budowa modułowa, por. rys. 10.b).

Powstanie wielowęściowych modułów bramki prądowej pozwoliło na utworzenie całego zestawu nowych bramek dwuwęściowych (wielowęściowych), które uzupełniają zbiór znanych bramek prądowych, realizujących jedynie negacje. Daje to większą swobodę przy projektowaniu systemów CMCL. Dzięki nowym modułom możliwa jest realizacja funkcji logicznych OR, NOR, AND ... przy dużo mniejszym nakładzie sprzętowym, dzięki możliwości pominięcia powielania i normalizacji sygnałów prądowych. Uzyskuje się także redukcję mocy pobieranej przez system cyfrowy.

4.2. Zastosowanie klucza n-p w module wyjściowym typu inwerter – Koncepcja przełączania prądu w obwodzie bramki prądowej. [14]

Wspomniano wcześniej, że bramki prądowe dają potencjalną możliwość realizacji logiki MVL. W praktycznej implementacji układów MVL napotyka się trudności wynikające z tolerancji poziomów prądów odpowiadającym stanom logicznym. W układach binarnych ich wpływ na poprawne działanie układu jest znikomy. Budowa układów MVL wymaga jednak, aby tolerancje te były możliwie małe, gdyż sumowanie prądów łączy się z sumowaniem błędów. Realizacja bramki MVL wymaga połączenia wyjść $N-1$ modułów inwertera.

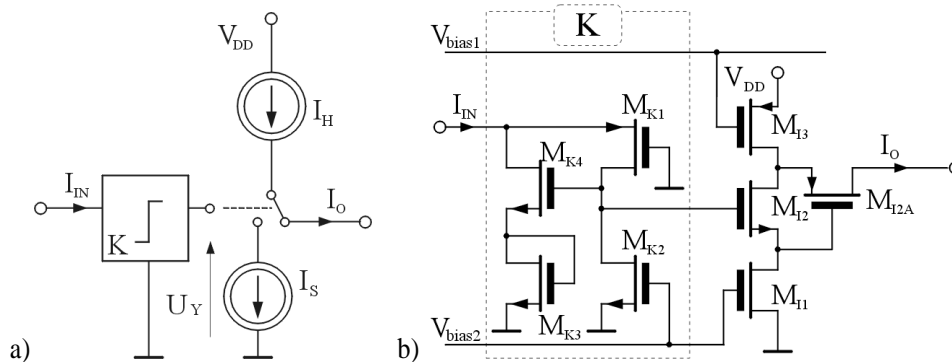
Niestety na wyjściu prądowego inwertera nawet w stanie logicznego zera występuje szczątkowa wartość prądu I_R (residual current). Cecha ta nie pozwala na łączenie dowolnej ilości wyjść bramek prądowych. Suma tych prądów w węzle może przekroczyć wartość graniczną $\frac{1}{2}$ prądu jedynek logicznej I_1 i zostanie „zinterpretowana” jako „1” przez układ wejściowy kolejnej bramki (komparator).

W praktycznej realizacji układów binarnych za pomocą bramek 3. generacji, ze względu na konieczność zapewnienia poprawnego działania prądowych układów cyfrowych zwiększono o ok. 6% wydajność źródła I_S poprzez zwiększenie szerokości kanału tranzystora M_{11} . Spowodowało to redukcję I_R , jednakże spowodowało, że każdy inwerter w stanie „0” odbiera $6\%I_1$ od połączonego z nim inwertera w stanie „1”. Prąd wypadkowy jest zatem pomniejszony o nadwyżkę wydajności źródła I_S . Z tego powodu przyjęto ograniczenie w ilości jednocześnie połączonych wyjść bramek do 8. Wprowadzone zmiany i ograniczenia w praktyce uniemożliwiają budowanie układów pracujących w systemach wielowartościowych.

W wyniku badań symulacyjnych określono, że prąd szczątkowy inwertera 3. generacji wynosi ok. 7% prądu I_1 . Dla przyjętego poziomu $I_1=50[\mu A]$, wartość prądu szczątkowego I_R wyniosła ok. $3,6[\mu A]$.

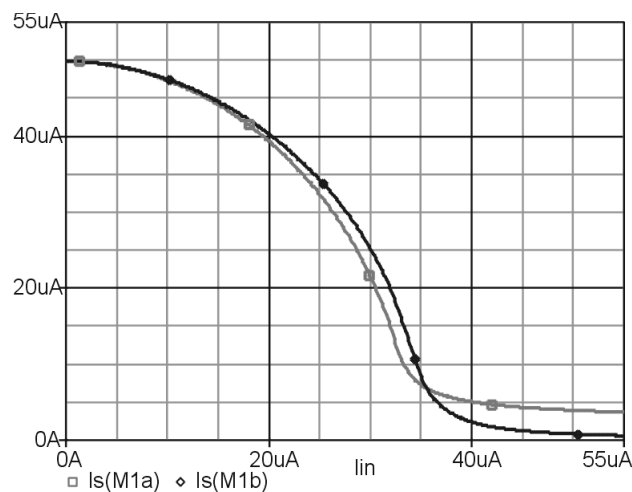
Przeprowadzono także badanie inwertera z ze źródłem I_S o takiej samej wydajności jak I_H (nie powiększonej) i zaobserwowano wówczas wzrost prądu I_R do ok. 11% I_1 .

Wyniki przeprowadzonych badań sugerują, że do praktycznej realizacji układów MVL konieczna jest zmiana idei bramki prądowej. Zaproponowano przełączanie prądu ze źródła I_H między gałęzią zawierającą I_S a wyjściem bramki, jak na rys. 12.a. za pomocą klucza przełączającego **n-p**. Spowodowało to redukcję prądu szczytkowego I_R wypływającego z inwertera w stanie 0 i umożliwiło zastosowanie źródła I_S o dokładnie takiej wydajności jak I_H (nie powiększonej).



Rys. 12. a) Nowa koncepcja bramki prądowej – zastosowanie klucza przełączającego; b) jednowęściowa bramka typu inwerter z kluczem n-p (czwartej generacji).

Wykonano symulację porównawczą starej i nowej realizacji inwertera [15]. Rozbieżności kształtu charakterystyki wynikają z różnicy w wydajności źródła I_S , oraz z wartości prądu szczytkowego I_R .



Rys. 13. Charakterystyka przejściowa bramki typu inwerter trzeciej generacji (IsM1a) i czwartej generacji (IsM1b).

W bramce 4. generacji dokonano redukcji prądu szczytkowego do poziomu $I_R=0,6[\mu A]$, co stanowi zaledwie 0,83% I_1 . Pozwala to na połączenie do 30 modułów wyjściowych. Stosując klucz **n-p** w miejsce klucza M_{I2} , kosztem dodania jednego tranzystora, uzyskano ponad czterokrotne zwiększenie dopuszczalnej ilości wyjść bramek łączonych w węzle przy jednakowej wydajności źródeł I_S i I_H . W praktyce oznacza to, że można łączyć wyjścia nawet 4 bramek MVL o podstawie $N=8$ $\{4 \cdot 7=28 < 30\}$. Dzięki temu umożliwiono praktyczną realizację bramek MVL. Charakterystykę bramki MVL(4) 4. generacji pokazano wcześniej na rys. 7.

5. Podsumowanie

W pracy przedstawiono genezę i rozwój idei budowy cyfrowych systemów prądowych, której autorem był Śp. prof. dr hab. inż. Andrzej Guziński. Pokazano złożoność problemów, które napotyka praktyczna implementacja CMCL, jak choćby opracowanie od podstaw praw „algebry prądowej”, czy metod minimalizacji, niezbędnych do realizacji złożonych systemów cyfrowych. Trzeba nadmienić, że przed całym zespołem stoi trudne zadanie opracowania automatycznych metod minimalizacji właściwych dla bramek 4. generacji. Metody te będą inne od metod opracowanych wcześniej, gdyż należy uwzględnić możliwość wykorzystania bramek wielowarstwowych. Zadanie dodatkowo utrudnia brak Śp. prof. dr hab. inż. O. Maslennikowa, który w zagadnieniach logiki i minimalizacji był i długo pozostanie niezastąpiony.

W rozdziałach 2.2 i 3.4 pokazano problemy wynikające z konieczności powielania sygnałów prądowych, których skutkiem jest stosunkowo duży pobór mocy i czas propagacji układów. Przedstawiono częściowe rozwiązania niektórych problemów dzięki nowej koncepcji bramek 4. generacji.

Nie trudności stanowią jednak o potencjale bramek prądowych. To możliwości niespotykane w innych rodzinach układów cyfrowych. Zamysłem autora było przedstawienie atutów układów prądowych. Wynikiem pracy w **trybie prądowym** jest praktycznie stała moc pobierana przez bramki ze źródła zasilania, a co ważniejsze bardzo niski poziom zakłóceń występujących przy przełączaniu stanu logicznego, przenoszonych przez podłoże i szyny zasilające. W wyniku tego bramki CMCL:

- nadają się do budowy systemów cyfrowo–analogowych, w których nie jest konieczne wykonywanie drogich, dodatkowych procesów technologicznych służących ekranowaniu, separacji części analogowej i cyfrowej;
- nadają się do budowy jednostek przetwarzających w systemach przetwarzania danych zapewniając duże bezpieczeństwo emisji elektromagnetycznej (Emsec), wynikiem czego jest odporność na ataki SCA, przy braku konieczności ponoszenia dodatkowych kosztów na zabezpieczenia.

Ponieważ **poziom logiczny** reprezentowany jest poprzez prąd na wyjściu bramki, możliwa jest prosta realizacja funkcji logicznych w algebrze prądowej. Niesie to za sobą możliwość realizacji układów cyfrowych, których budowa jest mniej złożona niż ich odpowiedników wykonanych w innej technologii. Mniejsza liczba bramek skutkuje mniejszą liczbą połączeń oraz mniejszą sumaryczną długością połączeń w układzie scalonym. Bramki prądowe umożliwiają ponadto budowę systemów opartych o logikę wielowartościową o podstawie $N > 2$. Także w tym przypadku zysk wynika z redukcji ilości połączeń, co dodatkowo wpływa na całkowitą powierzchnię struktury krzemowej.

Przedstawione aspekty zastosowania bramek prądowych to przysłowiowy czubek góry lodowej. Mówiąc o potencjale CMCL w niniejszej pracy, autorowi udało się ledwie wspomnieć o kilku charakterystycznych cechach układów z tej rodziny. Możliwości ich są z pewnością większe, prawdopodobnie niebawem zaistnieją kolejne potrzeby (aspekt Emsec jeszcze niedawno nie istniał), gdzie możliwe będzie zastosowanie układów CMCL. Istotne jest, że bramki prądowe już dziś stanowią alternatywę dla klasycznych bramek CMOS. Zastosowanie ich w wielu przypadkach daje wymierne korzyści w postaci redukcji kosztów produkcji systemów cyfrowych i analogowo–cyfrowych lub umożliwia budowę systemów, których zrealizowanie z klasycznych bramek cyfrowych jest niemożliwe.

Rozdziały 3. i 4. zawierają wyniki prac wykonanych w ramach Projektu Badawczego **O N515086737**

Bibliografia

1. A. Guziński, A. Kielbasiński, “Current–Mode Digital Circuits Operating in Mixed Analog–Digital Systems”, Proc. of the XVIII-th National Conference on Circuit Theory and Electronic Networks, pp. 317–322, Kołobrzeg 1995.
2. G. Blakiewicz, Porównanie właściwości układów tłumienia zakłóceń podłożowych, VI Krajowa konferencja Elektroniki : materiały konferencji, Darłówko wschodnie, 11-13 czerwca 2007, T. ½, Darłówko wschodnie, 11-13 czerwca 2007, s. 149-154.
3. Guziński A., Pawłowski P. “Current-mode digital circuits for low-voltage mixed analog-digital systems”, Proc. 6-th Int. Conf. Mixed design of integrated circuits systems, MIXDES’99 , Kraków, Poland, 1999, pp.369-372.

4. P. Pawłowski, „Ocena przydatności bramek cyfrowych pracujących w trybie prądowym w mieszanych systemach analogowo–cyfrowych”, rozprawa doktorska, Politechnika Koszalińska Wydział Elektroniki, Koszalin 2004.
5. A. Guziński, P. Pawłowski, D. Czwyrów, J. Kaniewski, O. Maslennikow, N. Maslennikowa, D. Rataj, „Design of Digital Circuits with Current-Mode Gates”, Bulletin of the Polish Academy of Sciences, Technical Sciences, Vol. 48, No. 1, pp. 73-91, 2000.
6. O. Maslennikow, A. Guziński, J. Kaniewski, R. Berezowski, “Rules of Current-mode Digital Circuit Design and Analysis”, Proc. of the XXII Nat.Conf. on Circuit Theory and Electronic Networks - KKTOiUE, pp. 149-154, Stare Jabłonki 1999.
7. O. Maslennikow, „Minimalizacja funkcji logicznych w algebrze bramek prądowych”, Prace IV Krajowej Konferencji Elektroniki, KKE'2005, pp., Kołobrzeg 2005.
8. O. Maslennikow, N. Maslennikowa, P. Pawłowski, M. Rajewska, R. Berezowski, “Hardware realization of the modular Exponentiation operation in cryptographic systems based on binary and multivalued logic”, 16th Internation Conference Mixdes 2009, pp. 210–214, June 2009, Łódź.
9. Łuczak R., Rajewska M. „Wielowejściowe bramki prądowe”, [Elelektronika - Konstrukcje, Technologie, Zastosowania 2011/9](#), Sigma–NOT Warszawa, 2011.
10. M. Białko, O. Maslennikow, N. Maslennikowa, P. Pawłowski, „Układy cyfrowe zbudowane z bramek prądowych: stan obecny, perspektywy rozwoju i zastosowania”, Elektronika - konstrukcje, technologie, zastosowania, nr 12, str. 38-43, 2004r.
11. O. Maslennikow, “Approaches to Designing and Examples of Digital Circuits Based on the Current-Mode Gates”, Data Recording, Storage & Processing, Vol.3, No.2, pp. 84-98, 2001.
12. O. Maslennikow, M. Rajewska, R. Berezowski, “Hardware Realization of the AES Algorithm S-Block Functions in the Current-Mode Gate Technology”, Proc. 9-th Int. Conf. Experience of Designing and Application of CAD Systems in Microelectronics, CADSM'2007, IEEE Catalog Number 07EX1594, pp.211-217, Lwów-Polyana, 2007.
13. M. Rajewska, R. Berezowski, O. Maslennikow, „Realizacja S-bloków systemu kryptograficznego DES na bramkach prądowych”, Prace XII Konferencji Krajowej „Komputerowe wspomaganie badań naukowych”, KOWBAN'2005, pp. 121-126, Polanica-Zdrój.
14. R. Łuczak, „An application of a N-P switch for a construction of current-mode gates”, Proc. of 18-th Int. Conf. Mixed Design of Integrated Circuits and Systems, Mixdes 16–18 June 2011, Gliwice, p.p.243–247.
15. Weidong Liu, Xiaodong Jin, James Chen, Min-Chie Jeng, Zhihong Liu, Yuhua Cheng, Kai Chen, Mansun Chan, Kelvin Hui, Jianhui Huang, Robert Tu, Ping K. Ko and Chenming Hu „BSIM3v3.2.2 MOSFET Model, Users' Manual”, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720, 1999.