کاهش توان مصرفی و مقاوم سازی یک جمع کننده در برابر حمله تحلیل توان بر پایه فناوری نوظهور گرافین

حسن عبدالهی[۱]، رضا هوشمند[۲]، هادی اولیا[۳]
[۱]استادیار، دانشکده مهندسی برق، دانشگاه هوائی شهید ستاری، تهران، ایران
[۲]استادیار، دانشکده مهندسی برق، دانشگاه هوائی شهید ستاری، تهران، ایران، rhooshmand@ssau.ac.ir
[۳]استادیار، گروه مهندسی برق، دانشکده فنی و مهندسی، دانشگاه اردکان، اردکان، ایران

چکیده

در این مقاله، با کاهش توان مصرفی، برای اولین بار نقش فناوری نوظهور گرافین بر افزایش امنیت در برابر حمله تحلیل توان در مدارهای جمع کننده دیجیتالی بررسی شده است. روش‌های طراحی استاتیک (static) و منطق مد جریانی (CML) برای طراحی جمع کننده‌ها یک، چهار و هشت بیتی در فناوری‌های سیلیکون و گرافین بکار گرفته شده است. در شبیه-سازی برای ترانزیستورهای گرافینی از یک مدل سازگار با SPICE و برای ترانزیستورهای سیلیکونی FINFET از یک مدل PTM استفاده می‌شود. تحلیل نتایج نشان می‌دهد که جمع کننده‌های static مبتنی بر گرافین، کمترین مصرف انرژی را دارند. همچنین تحلیل بالازدگی‌ها و انحراف معیار در دنباله توان یک جمع کننده ۸ بیتی تایید می‌کند که جمع کننده CML مبتنی بر گرافین (G-CML) مقاوم‌ترین طرح در برابر حمله تحلیل توان در میان طراحی‌های static و CML است. نهایتا یک روش ترکیبی جدید با ارائه یک مدار پیشنهاد می‌شود که در آن امنیت با ایجاد بینظمی در دنباله توان افزایش یافته است زیرا امکان تشخیص صحیح داده با مشکل مواجه می‌شود. بر این اساس جمع کننده طراحی شده با روش پیشنهادی ضمن کاهش توان مصرفی نسبت به جمع کننده CML، امنیت بالاتری را با ایجاد الگویی متمایز در دنباله توان به همراه دارد.

کلیدواژه

جمع کننده کم-توان امن، گرافین، FET گرافینی، منطق مد جریان.

مقدمه

امروزه اینترنت اشیا (IoT) در مواجهه با مسائل متنوعی قرار دارد که ممکن است میزان دسترسی گسترده آنها را با مشکلاتی روبرو نماید [۱، ۲]. از دیدگاه امنیتی، این فناوری بایستی مقاومت قابل قبولی را در برابر حملات کانال جانبی به دست آورد و همچنان کم مصرف باقی بماند. واحدهای پردازش، مغز هر افزاره IoT است که باید از الزامات فوق تبعیت نماید. در پردازنده های دیجیتال، ALU مسئول اجرای عملیات ریاضی و منطقی است [۳]. عمل جمع در ALU ها یکی از اساسی ترین عملیات است و می‌تواند پایه ای برای سایر عملیات محاسباتی باشد. بنابراین توسعه فناورانه مدارهای جمع کننده، تأثیر قابل توجهی بر عملکرد کلی دارد. به تازگی، یک انگیزه قوی برای استفاده از روش‌های فناورانه در مدارهای دیجیتالی بوجود آمده است [۴، ۵]. قابلیت‌های فناوری‌های نوظهور جدید می‌توانند به عنوان یک راه حل ممکن برای افزایش مقاومت در برابر حملات کانال جانبی و صرفه جویی در مصرف انرژی در افزاره‌های IoT در نظر گرفته شوند.

حملات کانال جانبی از دسترسی‌های فیزیکی به اطلاعات مانند مصرف انرژی یا تابش الکترومغناطیسی برای رمزگشایی استفاده

تاریخ دریافت: ۱۳۹۷/۱۱/۰۹ تاریخ پذیرش: ۱۳۹۸/۰۹/۰۶

می‌کنند [۶، ۷]. حمله تحلیل توان یک حمله شناخته شده است که غیر فعال و غیر تهاجمی است [۷]. برای کاهش اثربخشی این حمله و مقابله با آن، انواع مختلفی از راهکارهای الگوریتمی و راهکارهای سخت افزاری ارائه شده‌اند. بعضی از متون علمی از یک تابع هش و تصادفی، و ماسک‌های تبدیل کننده و چندتایی برای مقابله با حمله الگوریتمی استفاده کرده‌اند [۸-۱۰]. از سوی دیگر، منطق آدیاباتیک، منطق دیفرانسیلی موج پویا و آرایش های منطقی دیفرانسیل در سطح سخت افزاری ارائه شده‌اند [۱۱-۱۵]. آرایش های منطقی دیفرانسیل شامل منطق تقویت‌کننده حسی (SABL) و منطق مد جریانی (CML) است [۱۶، ۱۷].

طراحی مبتنی بر CML یک روش حفاظتی شناخته شده در سطح مدار است که از مصالحه میان مصرف توان و امنیت استفاده می‌کند [۱۸]. در یک آرایش CML، از جریان به جای ولتاژ، به عنوان یک متغیر واسط که ارتباط بین منطق ورودی و خروجی را بعهده دارد، استفاده می‌شود. ساختار CML در واقع شامل زوج های دیفرانسیل است که در آن یک منبع جریان را میان شاخه هایی که منطق خروجی را در اختیار دارند، سوئیچ می‌کند. کاهش نویز خارجی و تداخل بین سیگنال‌های مجاور بعلاوه کاهش نوسانات تغذیه باعث می‌شود که CML یک نامزد مقبول در طراحی‌های میکس سیگنال و کاربردهای فرکانس بالا باشد [۱۸-۲۰].

فناوری نوظهور جدید گرافین، به دلیل خواص الکتریکی و حرارتی‌اش، توجه زیادی را در بین محققان نانو الکترونیک به خود جلب کرده است [۲۱-۲۴]. این مقاله در نظر دارد تعیین کند که چه میزان فناوری گرافین در بهره وری نقش دارد. در ابتدا، جمع کننده‌های یک، چهار و هشت بیتی در آرایش‌های منطق مکمل استاتیک (به اختصار به صورت static) و CML از نظر مصرف انرژی در فناوری های سیلیکون و گرافین مقایسه می‌شوند. قسمت دوم از این مقاله مربوط به ارزیابی امنیتی یک جمع کننده ۸ بیتی در طراحی های static و CML است. در قسمت سوم طرحی پیشنهادی برای ارتقای امنیت یک تمام جمع کننده ارائه می‌شود.

بخش های بعدی این مقاله به شرح زیر ارائه خواهند شد: بخش ۲ شرح مختصری از نقاط کلیدی مربوط به ترانزیستورهای اثر میدان گرافینی را توصیف می‌کند. مقایسه‌ای میان فناوری سیلیکونی و گرافینی در بخش ۳ ارائه می شود. در بخش ۴، مولفه‌های توان و روابط مربوطه مورد بحث قرار می‌گیرند. بخش ۵ نمایشی از یک گیت CML پایه را نشان می‌دهد. در بخش ۶، یک اینورتر به عنوان یک مطالعه موردی شبیه سازی شده است و بحث مختصری در مورد دنباله‌های توان آن نیز گنجانده شده است. بخش ۷ نتایج و بحث مربوط به جمع کننده‌های مبتنی بر گرافین و سیلیکون را در آرایش‌های static، CML و یک طرح پیشنهادی ارائه می‌شود. در انتها خلاصه‌ای از نتایج در بخش آخر ارائه شده است.

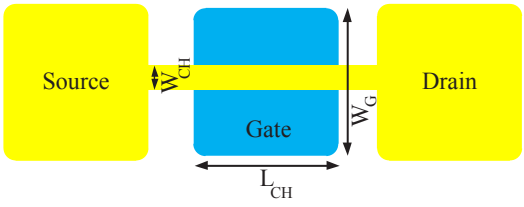
FET گرافینی

گرافین به عنوان یکی از مواد دو بعدی توجه زیادی را در میان جامعه محققین افزاره‌های الکترونیکی به خود جلب کرده است [۲۱-۲۴]. اتم‌های کربن در گرافین بصورت دو بعدی و با ساختار شبکه‌ای لانه زنبوری مرتب شده‌اند [۲۵، ۲۶]. ضخامت اتمی و مشخصات الکتریکی گرافین، این ماده را به عنوان یک جانشین بالقوه برای فناوری سیلیکون موجود مطرح کرده است که می‌تواند برخی از چالش های پیش روی فناوری سیلیکون نانو مقیاس را مرتفع نماید [۲۱، ۲۷].

گرافین در مقیاس بزرگ بدون شکاف انرژی است که این شکاف برای هر ماده ای که به عنوان یک کانال ترانزیستور بکار می رود، لازم است [۲۸، ۲۹]. هنگامی که صفحه‌های گرافین در یک جهت محدود می‌شوند، شکاف باندی به علت محصور شدن کوانتومی ظاهر می‌شود. این شکاف بطور معکوس متناسب با بعدی است که کوچک می‌شود [۲۹]. نوارهای گرافینی باریک که شکاف باند قابل قبولی را نشان می‌دهند، نانو نوار گرافینی (GNR) نامیده می‌شوند.

دو نوع GNR وجود دارد که در میان جامعه ی محققین افزاره-های الکترونیکی توجه زیادی را به خود معطوف داشته اند [۲۹، ۳۰]. این دو نوع با توجه به شکل لبه دسته بندی شده و به نام‌های زیگزاگ و آرمچیر شناخته می‌شوند. از آنجا که شکاف باند GNR های نوع آرمچیر بزرگتر هستند، کانال ترانزیستور معمولا از یک GNR آرمچیر تشکیل می‌شود [۳۰، ۳۱]. اتصالات سورس و درین گسترش‌های تغلیظ شده‌ای از کانال GNR هستند.

شماتیک FET مبتنی بر GNR آرمچیر در شکل ۱ نشان داده



شکل ۱. ساختار یک GFET

شده است که در ادامه کار به عنوان GFET نامیده می‌شود. این مدل از برخی پارامترها شامل طول کانال L_{CH}، عرض نوار W_{CH}، عرض گیت W_G و کسر تغلیظ اتصالات سورس و درین f_{dop} تشکیل شده است.

مقایسه فناوری‌های سیلیکون و گرافین

سیلیکون ماده ای با شکاف انرژی ۱/۱eV است که بصورت متداول در افزاره‌های امروزی مورد استفاده قرار می‌گیرد. کنترل گیت بر روی کانال با کوچک سازی طول کانال کاهش می‌یابد. از اینرو ساختارگیت طوری اصلاح می‌شود تا سطوح مختلف کانال توسط فلز گیت پوشش داده شود. یکی از معروفترین این روش‌ها استفاده از ترانزیستور Fin است که سطوح جانبی کانال را نیز پوشش می‌دهد. در این مقاله از این نوع پیشنهادی از ترانزیستور که در ابعاد نانومتری مطرح شده، استفاده می‌شود.

جهت شبیه‌سازی رفتار این ترانزیستور، از مدل PTM استفاده می شود [۳۲]. مدل PTM یک نسخه پیشرفته از مدل BSIM-CMG است که بطور ویژه برای طول‌های کانال زیر ۲۰nm استفاده می‌شود. در این مدل، اثراتی مانند تنزل موبلیتی، اشباع سرعت، مقاومت سری و خازن های پارازتیک لحاظ شده است.

گرافین در مقابل ماده‌ای است که با ایجاد محدودیت کوانتمی در عرض کانال دارای شکاف انرژی می‌گردد. در اینجا از گرافین با عرض ۱/۳۵nm و شکاف انرژی در حدود ۰/۶eV استفاده می‌شود. از آنجا که گرافین یک شبکه دو بعدی است، استفاده از یک گیت برروی کل سطح کانال می تواند کنترل مناسبی را به همراه داشته باشد.

در این پژوهش از مدل پیشنهادی Chen و همکاران استفاده می شود [۳۳]. محاسبه پتانسیل کانال نقش محوری را در تعیین مقادیر متغییرهای مداری ایفا می‌نماید. این پتانسیل با مدل‌سازی ارتباط ترمینال‌های اصلی ترانزیستور با کانال بدست می‌آید. چهار خازن جهت اتصال به ترمینال‌های درین، سورس، گیت و زیرلایه تعریف می‌شود که مقادیر آنها با توجه به بار الکترواستاتیک افزاره و رفتار کوانتمی در ناحیه کانال محاسبه می‌شود.

مولفه‌های توان

مصرف توان شامل دو جزء یا مولفه در مدارهای دیجیتال است [۳۴، ۳۵]. اولین مورد مربوط به یک مداری است که هیچ سیگنال سوئیچینگ به ورودی های مدار اعمال نمی‌شود. در این وضعیت، مقدار کمی از جریان از منبع تغذیه عبور می‌نماید. این مقدار به عنوان توان استاتیک شناخته شده و به صورت زیر نوشته می‌شود.

$$P_{static} = I_{DD}V_{DD} \quad (۱)$$

که در آن I_{DD} و V_{DD} به ترتیب جریان و ولتاژ منبع تغذیه هستند.

یکی دیگر از مولفه‌های توان بنام توان دینامیک، هنگامی مصرف می‌شود که سیگنال‌های سوئیچینگ به ورودی‌ها اعمال می‌شوند [۳۵]. دو مسیر وجود دارد که توان را در تغییر رخدادها تلف می‌نمایند. در اولی، مصرف توان بواسطه شارژ یا تخلیه خازن‌های پارازیتیک در هنگام تغییر مقدار ورودی (P_{chrg}) ایجاد می‌شود. در دومی، سلول‌های منطقی در طول یک فاصله زمانی کوتاه، مقدار مشخصی توان را به دلیل وقوع جریان اتصال کوتاه (P_{sc}) مصرف می‌کنند. روابط تقریبی مولفه‌های توان در زیر ارائه می‌شوند.

$$P_{dyn} = P_{chrg} + P_{sc} \quad (۲)$$

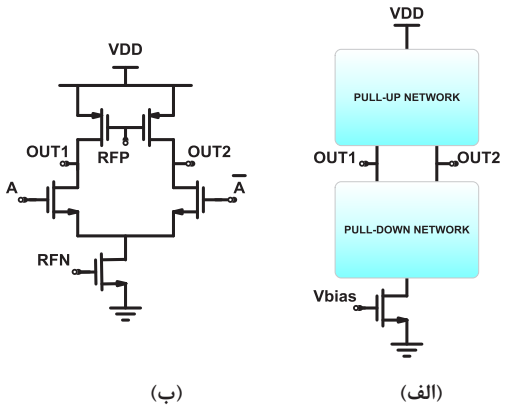
$$P_{chrg} = \alpha^* f C_L V_{DD}^2 \quad (۳)$$

$$P_{sc} = \alpha^* f V_{DD} I_{peak} t_{sc} \quad (۴)$$

پارامترهای این مؤلفه‌ها عبارتند از: ضریب فعالیت سلول α^*، فرکانس کلاک f، بار خازنی C_L، طول پایه‌ای و ارتفاع شکل موج جریان اتصال کوتاه به ترتیب با t_{sc} و I_{peak} نشان داده می‌شوند.

سلول‌های استاندارد CML

منطق مد جریانی (CML) مزایای امیدوار کننده‌ای مانند افزایش امنیت در برابر حمله توان و کاهش نویز سوئیچینگ و تداخل را نشان داده است [۱۸]. تاکنون محققان به طور گسترده ای از طرح‌های مبتنی بر CML در رمزنگاری، کاربرد-های فرکانس رادیویی، ارتباطات فیبر نوری و IC هایی با قابلیت میکس سیگنال استفاده کرده‌اند [۲۰-۱۸]. مدار CML شامل زوج‌های دیفرانسیل و ترانزیستور بایاس به عنوان یک منبع جریان می‌باشد (شکل ۲) [۱۸]. ساختار CML بر خلاف منطق مد ولتاژ (VML) که در آن مقادیر منطقی بطور کلی توسط سطوح ولتاژ نشان داده می‌شوند، از یک جریان به عنوان یک متغیر واسط استفاده می‌کند. به عبارت دیگر، جریان بایاس به ازای یک ولتاژ ورودی دیفرانسیل به یک شاخه خروجی هدایت می‌شود و منطق خروجی را تولید می‌کند. این ویژگی در شکل ۲ واضح تر است که در آن یک گیت CML اینورتر/بافر نمایش داده می‌شود.



(ب) (الف)

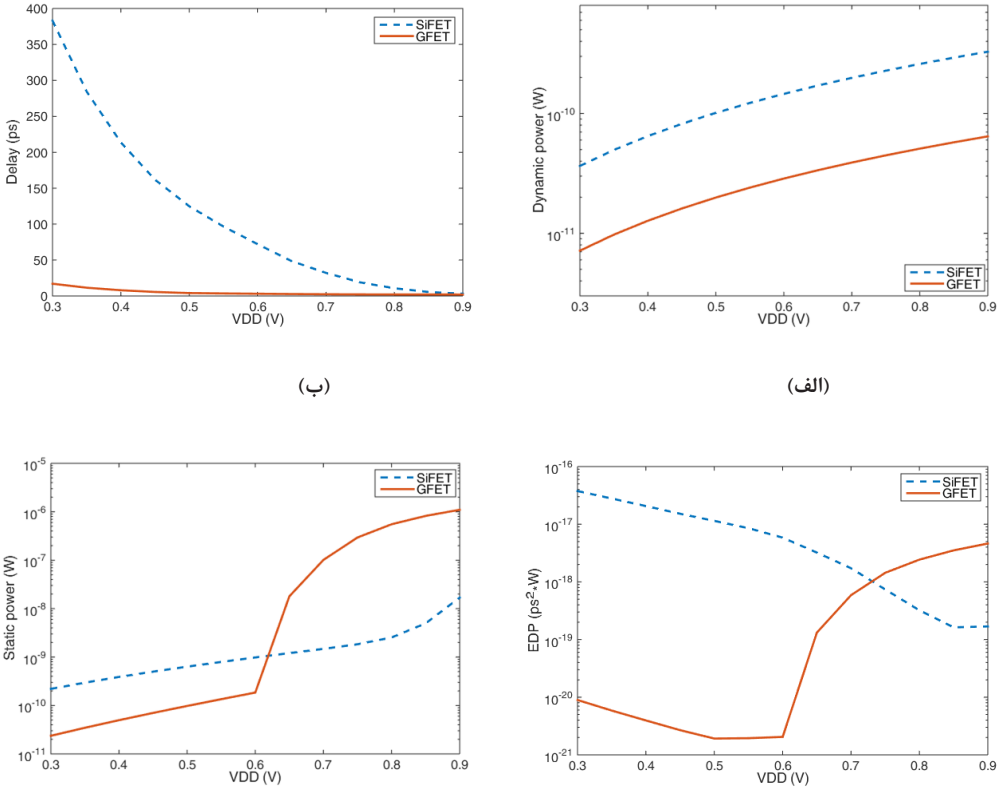
شکل۲. الف: دیاگرام یک گیت یونیورسال CML ب: اینورتر CML

در واقع، یک گیت CML دارای دو قسمت اصلی است: یک شبکه بالا-کشنده و یک شبکه پایین-کشنده. تنظیم افت ولتاژ DC در خروجی بیشتر از طریق شبکه بالا-کشنده انجام می-شود که در آن از دو مقاومت یا FET های نوع P (PFET) استفاده می‌شود. از سوی دیگر، شبکه پایین-کشنده از یک FET نوع N به عنوان منبع جریان و تعدادی از NFETها به عنوان یک واحد عملیاتی استفاده می‌کند. هر گیت CML دو پایانه خروجی یعنی OUT1 و OUT2 را دارد. این پایانه‌ها به عنوان یک جفت مکمل شناخته می‌شوند.

از آنجا که گیت‌های CML در طول زمان گذار خروجی یک مسیر با مقاومت کم ندارند، توان اتصال کوتاه در مدارهای CML در مقایسه با همتایان استاتیک حذف می‌شود. بنابراین، توان دینامیک در طراحی CML عمدتا به دلیل بارهای خازنی است. این ویژگی برای کاهش میزان تشخیص داده پردازشی در رمزنگاری استفاده می‌شود.

مطالعه موردی: اینورتر

به منظور دستیابی به مرجعی در مباحث بعدی، یک اینورتر استاتیک بصورت تفصیلی مورد مطالعه قرار می‌گیرد. در شبیه سازی‌های زیر، FINFETهای سیلیکونی (SiFETs) ۱۶ نانومتری برای کاربردهایی با کارایی بالا که از مدل PTM اقتباس شده‌اند، استفاده می‌شوند [۳۲]. به طور مشابه، ما یک مدل سازگار با SPICE را با کانال ۱۶ نانومتری برای ترانزیستورهای گرافین (GFETs) انتخاب می‌کنیم [۳۳]. پارامترهای دیگر بصورت W_G = ۱/۳۵nm ،W_{CH} = ۱۶nm و f_{dop} = ۰/۰۰۱ تعریف شده است. لازم به ذکر است که تمام شبیه سازی‌ها در فرکانس ۱۰۰ مگاهرتز انجام می‌شوند. همچنین نقش مقاومت اتصال در شبیه سازی‌ها به دلیل پیشرفت های فنی اخیر نادیده گرفته شده است [۳۶، ۳۷]. شکل ۳، تاخیر، توان دینامیکی، توان استاتیک، حاصلضرب توان تاخیر، حاصلضرب انرژی تاخیر را در اینورترهای مبتنی بر SiFET و GFET به عنوان تابع ولتاژ منبع تغذیه V_{DD} نشان می‌دهد. بر اساس حداقل حاصلضرب انرژی تاخیر، در این مقاله مقادیر ۰/۸۵V و ۰/۵V به ترتیب برای ولتاژهای تغذیه در



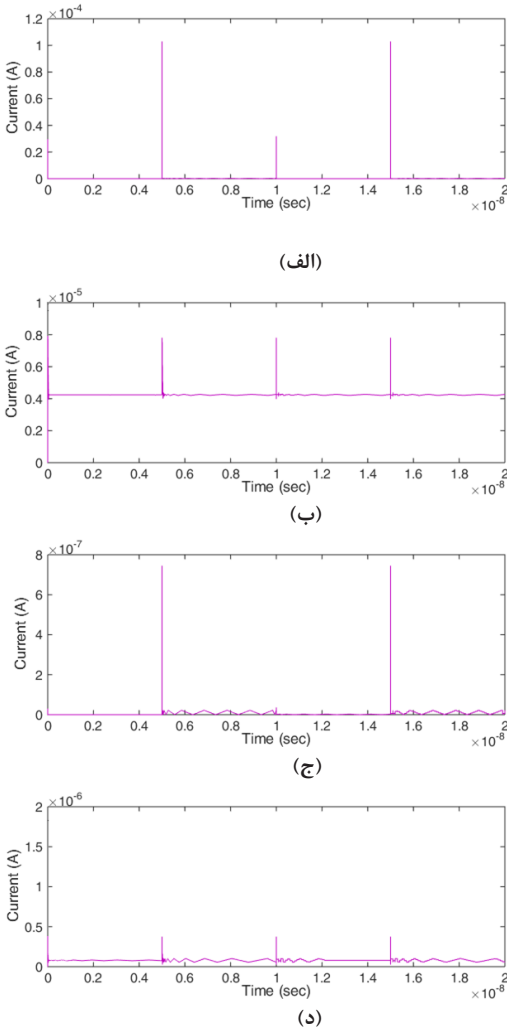
(ب) (الف)

(د) (ج)

شکل ۳. الف: تاخیر ب: توان دینامیک ج: توان استاتیک د: حاصلضرب انرژی تاخیر (EDP) برحسب V_{DD}

اینورترهای سیلیکونی و گرافینی انتخاب شده است. این مقادیر در ادامه برای تمام مدارهای SiFET و GFET در نظر گرفته شده است.

دنباله‌های توان برای اینورترهای SiFET و GFET در هر دو طراحی static و CML در شکل ۴ نشان داده شده است. در زمان گذار منطقی، بالازدگی‌های جریان اینورتر CML مبتنی بر سیلیکون (Si-CML) حدود ده برابر کمتر از اینورتر static مبتنی بر سیلیکون است. به طور مشابه، بالازدگی‌ها دراینورترهای CML مبتنی بر گرافین (G-CML) نسبت به مقادیر همتای static مبتنی بر گرافین در حدود دو برابر کاهش یافته است. لذا اینورترهای CML به خوبی قادر به کاهش قابل توجه بالازدگی‌ها نسبت به اینورترهای static می‌باشند. دیده می شود که اینورتر G-CML نه تنها باعث کاهش بیست برابری



شکل ۴: دنباله های توان الف: اینورتر static مبتنی بر سیلیکون ب: اینورتر CML مبتنی بر سیلیکون ج: اینورتر static مبتنی بر گرافین د: اینورتر CML مبتنی بر گرافین. دنباله‌های توان در یک دوره زمانی مشخص با یک الگوی ورودی مشابه نمایش داده می شوند

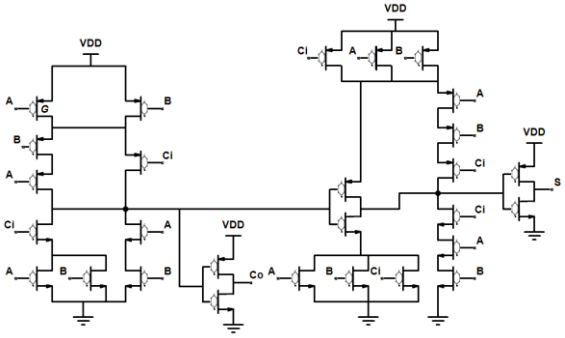
بالازدگی‌های جریان می‌شود، بلکه نود و دو برابر مصرف توان کمتری را نسبت به اینورتر Si-CML به همراه دارد.

نتایج شبیه سازی و بحث

تحلیل عملکرد جمع‌کننده‌های static و CML

عمل جمع یک عملیات پایه محاسباتی در هر واحد پردازش است [۳]. سایر عملیات محاسباتی مانند تفریق، ضرب و تقسیم از مدارهای جمع کننده بهره می‌گیرند. بنابراین، تأثیر هر گونه تغییر در مدار جمع‌کننده می‌تواند به طور قابل توجهی افزایش عملکرد واحد پردازش را به دنبال داشته باشد. یک تمام جمع کننده یک بیتی گرافینی در هر دو طراحی مدار ارائه گشته و با همتای سیلیکونی آن مقایسه می‌شود. همانطور که در شکل ۵ مشاهده می‌شود، تمام جمع‌کننده static دارای بیست و هشت ماسفت می‌باشد. ورودی‌ها A، B و Ci (کری ورودی) و خروجی‌ها S (sum) و Co (carry-out یا کری خروجی) هستند. به طور مشابه، یک تمام جمع‌کننده CML دارای سی ماسفت است که در آن مدارهای sum و carry-out از هم جدا می‌شوند (شکل ۶).

نتایج مربوط به تمام جمع‌کننده‌ها در جداول ۱ و ۲ نشان داده شده‌اند. واضح است که جمع کننده مبتنی بر گرافین در هر روش طراحی نسبت به نوع سیلیکونی برتری دارد. از آنجا که فرایند ساخت ترانزیستورهای گرافینی در مراحل مقدماتی قرار دارد و لی‌اوت استاندارد و قابل اطمینانی در حال حاضر پیشنهاد نشده است، در این مقاله، برای محاسبه سطح صرفا مساحت کانال در نظر گرفته شده است. نتایج نشان می‌دهد که مساحت و تاخیر جمع‌کننده مبتنی بر گرافین به ترتیب در حدود ۴۷ و ۵ برابر کمتر از همتای سیلیکونی در آرایش‌های static و CML است. مزیت قابل توجه مدارهای مبتنی بر GFET مربوط به راندمان توان است. به عنوان مثال، مصرف توان در جمع کننده static مبتنی بر گرافین از مرتبه ده برابر، مقدار کمتری را نسبت به همتای سیلیکونی ارائه داده است. علاوه بر این، جمع‌کننده G-CML یک سی و دوم در

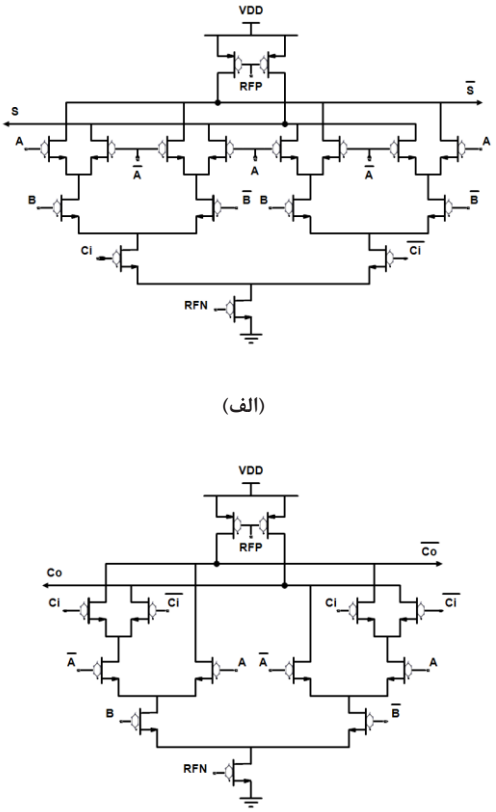


شکل ۵. تمام جمع کننده static

حاصلضرب توان تأخیر (PDP) و یک صد و پنجاه هفتم در حاصلضرب انرژی تأخیر (EDP) نسبت به جمع‌کننده CML مبتنی بر سیلیکن (Si-CML) برتری نشان می‌دهد.

برای تاکید بر اعتبار نتایج، مدارهای پیچیده‌تر از قبیل جمع کننده ۴ بیتی و ۸ بیتی در شبیه سازی‌های مداری اضافه شده است. نتایج مربوط به میزان مصرف توان و ویژگی های دیگر مانند تاخیر، PDP و EDP در جداول ۱ و ۲ خلاصه شده‌اند. از آنجا که پیاده‌سازی منطقی طرح های static بدون منبع جریان انجام می‌شود، از اینرو توان مصرفی پایین‌تری در طرح‌های static قابل دستیابی است. از سوی دیگر، به علت اینکه یک طراحی مبتنی بر CML از ساختار زوج دیفرانسیل استفاده می‌کند، تاخیر پایین‌تری را در مقایسه با همتای static آن ارائه می‌دهد.

مساحت جمع کننده‌های ۸ بیتی مبتنی بر گرافین حدود ۴۸ برابر کوچکتر از همتایان مبتنی بر سیلیکون است. همچنین، تأخیر در جمع کننده‌های مبتنی بر گرافین نسبت به انواع سیلیکونی، کمی بیشتر از ۵۵ درصد کاهش را نشان می‌دهد. تفاوت مصرف انرژی در دو فناوری معنی‌دار است و نشان دهنده آنست که اگرچه فناوری مدار دارای تأثیر غالب در مساحت و تاخیر است، اما مصرف توان بوضوح تابعی از هر دوی فناوری و روش طراحی است. مشاهده می‌شود که جمع کننده static مبتنی بر گرافین در مقایسه با همتای سیلیکونی، ۲۶/۶ برابر



(الف)

(ب)

شکل ۶. تمام جمع کننده CML

جدول ۱. مساحت، تاخیر و توان مدارات محاسباتی static و CML مبتنی بر سیلیکون

روش طراحی	سلول	تعداد ترانزیستورها	مساحت (μm^2)	تاخیر (ps)	توان (nW)	PDP (nW × ps)	EDP ($nW \times ps^2$)
Static	جمع کننده ۱ بیتی	۲۸	۰/۰۲۸۸۶۷۲	۱۱	۷۷/۶۹۲۳	۸۵۴/۶۱۵۳	۹۴۰۰/۷۶۸
	جمع کننده ۴ بیتی	۱۱۲	۰/۱۱۴۶۸۸	۶۹/۵	۲۵۱/۹۶۲	۱۷۵۱۱/۳۶	۱۲۱۷۰۳۹
	جمع کننده ۸ بیتی	۲۲۴	۰/۲۲۹۳۷۶	۹۳	۳۴۸/۸۵۵	۳۲۴۴۳/۵۲	۳۰۱۷۲۴۷
	میانگین	۱۲۱/۳۳۳	۰/۱۲۴۲۴۵	۵۷/۸۳۳۳	۲۲۶/۱۷	۱۳۰۸۰/۱۶	۷۵۶۴۶۸/۷
CML	جمع کننده ۱ بیتی	۳۰	۰/۰۳۰۷۲	۵/۲۵	۷۰۴۹/۸	۳۷۰۱۱/۴۵	۱۹۴۳۱۰/۱
	جمع کننده ۴ بیتی	۱۲۰	۰/۱۲۲۸۸	۲۹	۲۸۱۵۶/۷	۸۱۶۵۴۴/۳	۲۳۶۷۹۷۸۵
	جمع کننده ۸ بیتی	۲۴۰	۰/۲۴۵۷۶	۵۱	۵۶۳۱۹/۵	۲۸۷۲۲۹۵	۱۴۶۴۸۷۰۲۰
	میانگین	۱۳۰	۰/۱۳۳۱۲	۲۸/۴۱۶۷	۳۰۵۰۸/۷	۸۶۶۹۵۶/۶	۲۴۶۳۶۰۴۵

جدول ۲. مساحت، تاخیر و توان مدارات محاسباتی static و CML مبتنی بر گرافین

روش طراحی	سلول	تعداد ترانزیستورها	مساحت (μm^2)	تاخیر (ps)	توان (nW)	PDP (nW × ps)	EDP ($nW \times ps^2$)
Static	جمع کننده ۱ بیتی	۲۸	۰/۰۰۰۶۰۵	۵/۲۵	۵/۴۷۱۱	۲۸/۷۲۳۲۸	۱۵۰/۷۹۷۲
	جمع کننده ۴ بیتی	۱۱۲	۰/۰۰۲۴۱۹	۲۹	۸/۸	۲۵۵/۲	۷۴۰۰/۸
	جمع کننده ۸ بیتی	۲۲۴	۰/۰۰۴۸۳۸	۵۴	۱۳/۰۵۶	۷۰۵/۰۲۴	۳۸۰۷۱/۳
	میانگین	۱۲۱/۳۳۳	۰/۰۰۲۶۲۱	۲۹/۴۱۶۷	۹/۱۰۸۹	۲۶۷/۹۵۳۸	۷۸۸۲/۳۱۶
CML	جمع کننده ۱ بیتی	۳۰	۰/۰۰۰۶۴۸	۱/۰۷۵	۱۰۷۴/۳۶	۱۱۵۴/۹۳۷	۱۲۴۱/۵۵۷
	جمع کننده ۴ بیتی	۱۲۰	۰/۰۰۲۵۹۲	۱۷/۳	۳۱۶۳/۲	۵۴۷۲۳/۳۶	۹۴۶۷۱۴/۱
	جمع کننده ۸ بیتی	۲۴۰	۰/۰۰۵۱۸۴	۲۸	۴۵۰۸/۱	۱۲۶۲۲۶/۸	۳۵۳۴۳۵۰
	میانگین	۱۳۰	۰/۰۰۲۸۰۸	۱۵/۴۵۸۳	۲۹۱۵/۲	۴۵۰۶۴/۰۴	۶۹۶۶۱۳/۴

توان را مصرف می‌کند در حالیکه این مقدار در زمان مقایسه با طرح های CML ۱۲۴/۹ است. علاوه بر این، شاخصه های PDP و EDP در حدود بیست تا صد برابر مقادیر کمتری را برای فناوری گرافین نشان می‌دهند.

مشاهده می‌شود که با استفاده از مدارهای CML مبتنی بر گرافین، مزیت موجود در طرح‌های CML با هزینه کمتری قابل دستیابی است. برای مثال، میزان مصرف انرژی در مدارهای استاتیک و CML با فناوری گرافین بهبود می‌یابد. این رابطه بین مدارهای static و CML مبتنی بر سیلیکون حدود ۱ به ۱۳۵ است در حالیکه این نسبت بین یک مدار static نوعی مبتنی بر سیلیکون و یک مدار مشابه CML مبتنی بر گرافین تقریبا برابر با ۱ به ۱۳ است. از این رو با استفاده از فناوری گرافین، مصرف انرژی از مرتبه ده در یک جمع کننده CML کاهش می‌یابد.

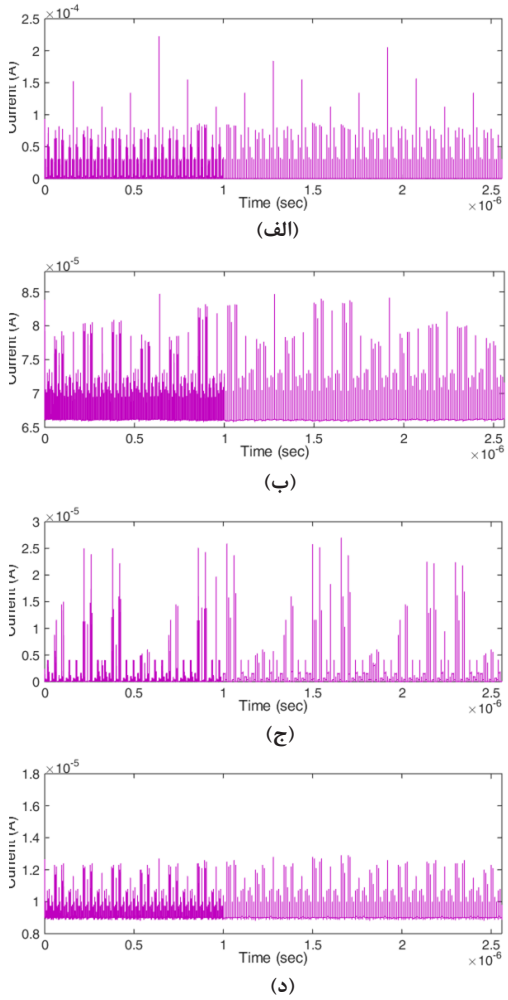
تحلیل امنیتی جمع‌کننده‌های static و CML: اقدام متقابل در برابر حمله تحلیل توان

جمع کننده ۸ بیتی شامل هشت جمع کننده یک بیتی است که مصرف توان کلی را افزایش می‌دهد. همانطور که انتظار می‌رود، عناصر پارازیتیکی در برخی از گره های داخلی نیز بزرگتر می‌شوند و منجر به کشیدن جریان های بیشتر از منبع تغذیه می‌شوند. این وضعیت برای یک جمع کننده ۸ بیتی در شکل ۷ نشان داده شده است. واضح است که مصرف توان در مدارهای CML در سطح غیر صفر آغاز می‌شود، زیرا همیشه حداقل یک منبع جریان در مدار های CML وجود دارد که توان استاتیک را افزایش می‌دهد.

اساس یک حمله تحلیل توان مبتنی بر تشخیص مصرف توان گذرا در عملیات است [۱۷، ۳۴]. بنابراین، هر چه دنباله توان هموارتر باشد، تشخیص لحظه تغییر داده دشوارتر خواهد بود. بالازدگی‌ها در لحظه گذار منطقی در مدارهای CML به شکل مناسبی در دنباله توان کاهش داده می‌شوند (شکل ۷). علاوه بر این، مشاهده می‌شود که فناوری گرافین باعث کاهش بالازدگی‌های جریان در هر دو روش طراحی می‌شود.

با بررسی دنباله های توان مشاهده می‌شود که ارتفاع بالازدگی‌های جریان در جمع کننده‌های CML کاهش یافته است. انتظار می رود که در این جمع کننده‌ها توان دینامیک کوچکتر شود و در این حال توان استاتیک به علت جریان ثابت موجود افزایش یابد. از دیدگاه فناورانه، هر دو توان استاتیک و دینامیک در یک جمع کننده مبتنی بر گرافین پایین‌تر از این مقادیر در جمع کننده مبتنی بر سیلیکون است.

جدول ۳ نتایج استخراج شده از دنباله‌های توان جمع کننده ۸ بیتی را خلاصه می‌کند. ستون های سه تا پنج حداقل توان



شکل ۷. دنباله های توان الف: جمع کننده ۸ بیتی static مبتنی بر سیلیکون ب: جمع کننده ۸ بیتی CML مبتنی بر سیلیکون ج: جمع کننده ۸ بیتی static مبتنی بر گرافین د: جمع کننده ۸ بیتی CML مبتنی بر گرافین. دنباله‌های توان در یک دوره زمانی مشخص با یک الگوی ورودی مشابه نمایش داده می شوند

P_{min}، حداکثر توان P_{max} و اختلاف بین آنها را نشان می‌دهند. بیشترین مقدار در حداکثر توان متعلق به جمع کننده static مبتنی بر سیلیکون است. اختلاف بین حداقل توان و حداکثر توان می‌تواند یک معیار مناسب برای میزان حساسیت مدار به تغییرات ورودی باشد [۳۸]. از آنجا که کمترین مقدار به جمع کننده G-CML اختصاص دارد، می‌توان نتیجه گرفت که جمع‌کننده مبتنی بر فناوری گرافین می‌تواند به طور موثری نشت اطلاعات را به حداقل برساند.

معیارهای دیگری برای ارزیابی دقیق تر مدارهای جمع کننده وجود دارد [۴۰-۳۸]. اولین مورد انحراف معیار σ است. نتایج نشان می‌دهد که جمع کننده G-CML کمترین انحراف معیار را دارد. به عبارت دیگر، کمترین تغییرات در مصرف توان در جمع کننده G-CML برای ورودی های مختلف قابل دستیابی است. لازم به ذکر است که جمع کننده Si-CML نیز نقش

جدول ۳. مقایسه نتایج بر روی جمع کننده ۸ بیتی

فناوری	روش طراحی	P_{min} (nW)	P_{max} (nW)	P_{max}-P_{min} (nW)	P_{av} (nW)	σ (nW)	NED	NSD
سیلیکون	Static	۷۲/۶۶	۱۸۹۳۰۰	۱۸۹۲۲۷/۳۴	۳۴۷/۱۹	۲۶۶۰/۶	۰/۹۹۹۶	۷/۶۶
	CML	۵۵۹۱۳	۷۲۰۰۴	۱۶۰۹۱	۵۶۳۱۸	۸۷۶/۵۷	۰/۲۲۳	۰/۰۲
گرافین	Static	۰/۰۰۰۱۶	۱۳۴۹۵	۱۳۴۹۴/۹۹۹۸۴	۱۳/۰۵۶	۴۰۱/۱	۱	۲/۱
	CML	۴۴۱۰	۸۸۸۰	۴۴۷۰	۴۵۱۰	۸۲/۵	۰/۵۰۴	۰/۰۲

موثری در کاهش اختلاف توان و انحراف معیار دارد و این زمانیست که تنها فناوری سیلیکون متعارف در نظر گرفته شود. دو معیار دیگر برای ارزیابی چنین مدارهایی به نام‌های انحراف انرژی نرمالیزه شده (NED) و انحراف معیار نرمالیزه شده (NSD) ارائه شده‌اند. روابط آنها به صورت زیر است [۳۸-۴۰]:

$$NED = \frac{P_{max} - P_{min}}{P_{max}} \quad (۵)$$

$$NSD = \frac{\sigma}{P_{av}} \quad (۶)$$

که در آن، P_{av} نشان دهنده توان متوسط دنباله مربوطه است. پایین‌ترین مقدار برای NED متعلق به جمع کننده Si-CML است که ممکن است گمراه کننده باشد. بطور کلی می‌توان نتیجه گرفت که هرچند NED در جمع کننده Si-CML کمترین را دارد، اما اختلاف توان، توان متوسط و انحراف معیار، تایید می‌کنند که جمع کننده G-CML بهترین گزینه می‌باشد. تفاوت بزرگ میان توان مصرفی متوسط جمع کننده‌های Si-CML و G-CML منشا چنین مشاهداتی در مقادیر NED است. مقادیر NSD در جمع کننده‌های CML تقریبا برابر با یکدیگر هستند و مقادیر حداقلی را نشان می‌دهند. می‌توان نتیجه گرفت که مقادیر NSD بخوبی قادرند نقش روش طراحی را آشکار سازند، اما برای تعیین سهم فناوری مفید نیستند.

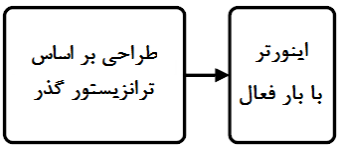
نتایج امیدوار کننده فوق تایید می‌کند که جمع کننده G-CML بهترین عملکرد را در برابر حمله تحلیل توان نشان می‌دهد. هرچند که این جمع کننده در مقایسه با جمع کننده static مبتنی بر گرافین توان بیشتری مصرف می‌کند.

افزایش عملکرد و امنیت با پیشنهاد یک مدار ترکیبی

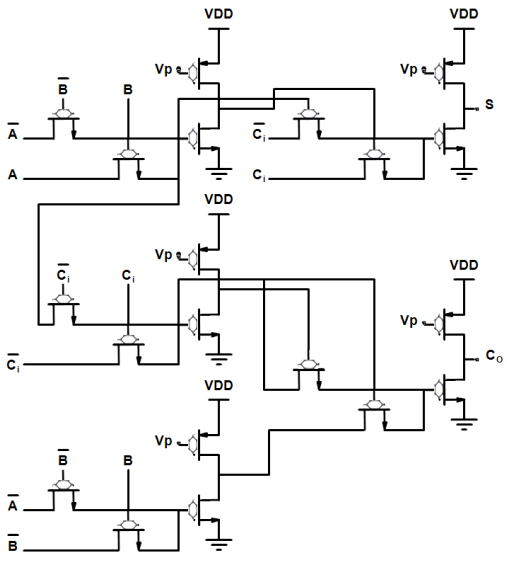
ارزیابی امنیت سخت‌افزاری تاکنون عمدتا برمحور کاهش ارتفاع و واریانس بالازدگی‌ها استوار بوده است [۱۷، ۳۸-۴۰]. رویکرد دیگر می‌تواند در اثر ایجاد بینظمی در دنباله باشد تا امکان تشخیص صحیح داده هنگام مشاهده تغییر در دنباله توان کاهش یابد.

دنباله‌های توان ساختارهای static و CML توان مصرفی استاتیک ثابتی را در طی تغییرات ورودی نشان می‌دهند. در این مقاله پیشنهاد می شود که از یک ساختار ترکیبی استفاده شود. این ساختار از دو طبقه تشکیل می‌شود که در شکل ۸ نمایش داده می شود. در طبقه اول از ترانزیستورهای گذر و در طبقه دوم از یک اینورتور با بار فعال استفاده می شود. علت بکارگیری ترانزیستورهای گذر انتقال بخشی از توان کل مصرفی در اثر تغییرات ورودی به توان استاتیک است. طبقه اینورتر با بار فعال جهت تقویت سیگنال خروجی گیت‌های انتقال بکار گرفته شده است. استفاده از اینورتر با بار فعال بجای اینورتر static جهت کاهش ارتفاع بالازدگی‌های بزرگ مشاهده شده در آرایش static می‌باشد. خروجی دنباله توان در ساختار پیشنهادی نسبت به انواع دیگر طراحی ذکر شده یک نوع بی-نظمی بیشتری را با توجه به تغییرات هر دو توان استاتیک و دینامیک نمایش می‌دهد. از اینرو این شیوه از طراحی مقاومت مدار را در حمله تحلیل توان افزایش می‌دهد.

مدار تمام جمع کننده یک بیتی بصورت نمونه‌ای در شکل ۸ نشان داده شده است. نتایج ارزیابی برای فناوری‌های سیلیکونی و گرافینی در جدول ۴ خلاصه شده است. بر اساس این



(الف)



(ب)

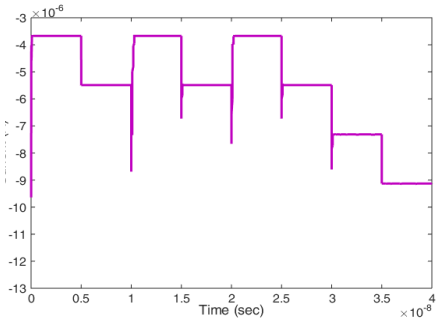
شکل ۸. الف: بلوک دیاگرام و ب: تمام جمع کننده با روش طراحی پیشنهادی

جدول ۴. ارزیابی مدار تمام جمع کننده با روش طراحی پیشنهادی

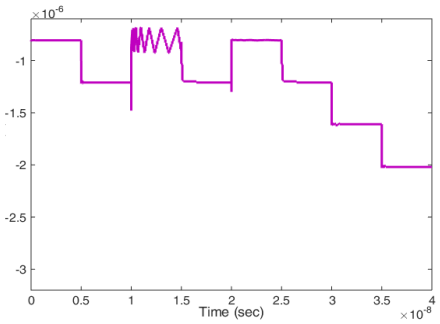
فناوری	تعداد ترانزیستورها	مساحت (μm^2)	تاخیر (ps)	توان (nW)	PDP (nW × ps)	EDP ($nW \times ps^2$)
سیلیکون	۲۰	۰/۰۲۰۶۱۹	۶۲	۴۶۸۸/۱۸	۲۹۰۶۷۷	۱۸۰۲۱۳۵۱
گرافین	۲۰	۰/۰۰۰۴۳۲۱	۱۷	۶۰۳/۴۹	۱۰۲۵۹/۳۹	۱۷۴۴۰۹/۷

طراحی، میزان توان مصرفی مدار مابین طراحی static و CML واقع شده است. درصورتیکه دنباله توان این مدار در فناوری‌های سیلیکونی و گرافینی رفتار متفاوت با دو طراحی قبل را ارائه می دهد (شکل ۹). اثر تغییرات منطق در این مدار در هر دو بخش توان استاتیک و دینامیک منعکس شده است که با ایجاد بینظمی در دنباله توان باعث می‌شود مقاومت مدار در برابر حمله توان افزایش یابد. این رفتار با کاهش ارتفاع بالازدگی‌ها در دنباله توان جمع کننده گرافینی بطور مطلوب‌تری نمایان است. بنابراین انتخاب آگاهانه طراحی مدار می‌تواند نقش بسزایی در ارتقای امنیت مدار ایفا نماید.

در تمامی طراحی‌های فوق، فناوری گرافین اثر قابل توجهی در ارتقا امنیت پردازش داده و همچنین کاهش مصرف انرژی نسبت به همتای سیلیکونی خود را نشان داده است. از این رو، به نظر می‌رسد که توسعه افزاره‌های IoT مبتنی بر گرافین قابلیت رشد بالاتری دارند بطوریکه که نیازمندی‌های آنها به طور موثرتری برآورده می‌شوند.



(الف)



(ب)

شکل ۹. دنباله‌های توان تمام جمع کننده الف: سیلیکون ب: گرافین

نتیجه‌گیری

این مقاله نشان می‌دهد که افزاره‌های نوظهوری، مانند GFET ها، چگونه فرصت‌های جدیدی را برای طرح‌های کم توان و امن ارائه می‌دهند. یک جمع کننده نوعی با تعداد مختلف ورودی مورد ارزیابی واقع شده است. نتایج نشان می‌دهد که جمع کننده‌های static توان کمتری را مصرف می‌کنند و کمترین میزان توان مصرفی به جمع کننده static مبتنی بر گرافین تعلق دارد. دنباله توان جمع کننده‌های CML بالازدگی‌های کوچکتری را در جریان کشیده شده از منبع تغذیه نشان می‌دهند. دنباله توان یکنواخت‌تر در جمع کننده‌های CML باعث کاهش احتمال کشف داده‌ها می‌گردد. این امر با هزینه مصرف انرژی بالاتر محقق می‌شود. براساس یافته‌های بدست آمده از طراحی‌های static و CML، این مقاله یک طرح را پیشنهاد داده است. این طرح ضمن کاهش توان مصرفی نسبت به همتای CML آن، امنیت بالاتری را در اثر ایجاد الگوی متمایز در دنباله توان ارائه می‌دهد. بکارگیری فناوری گرافین تاثیر مثبتی را برروی شاخصه‌های اصلی (مانند تاخیر، توان و امنیت) طراحی‌های مذکور دارد و می‌تواند توسعه بستر سخت‌افزاری IoT را بیش از پیش فراهم نماید.

مراجع

[1] H. Sun, M. Yin, W. Wei, J. Li, H. Wang, and X. Jin, “MEMS based energy harvesting for the Internet of Things: a survey,” Microsystem Technologies, vol. 24, no. 7, pp. 2853–2869, Jul. 2018.

[2] K. Yang, D. Blaauw, and D. Sylvester, “Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey,” IEEE Micro, vol. 37, no. 6, pp. 72–89, 2017.

[3] M. M. Mano, Digital design. Upper Saddle River, NJ: Pearson Prentice Hall, 2002.

[4] S. Moysidis, I. G. Karafyllidis, and P. Dimitrakis, “Graphene Logic Gates,” IEEE Transactions on Nanotechnology, vol. 17, no. 4, pp. 852–859, 2018.

[5] S. Tabrizchi, A. Panahi, F. Sharifi, K. Navi, and N. Bagherzadeh, “Method for designing

ternary adder cells based on CNFETs," IET Circuits, Devices & Systems, vol. 11, no. 5, pp. 465–470, Jan. 2017.

[6] F. X. Standaert, "Introduction to side-channel attacks," in Secure Integrated Circuits and Systems, I. M. R. Verbauwhede, Ed. Boston, USA: Springer, 2010, pp. 27–42.

[7] A. J. Acosta, T. Addabbo, and E. Tena-Sánchez, "Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview," International Journal of Circuit Theory and Applications, vol. 45, no. 2, pp. 145–169, 2017.

[8] P. Kocher, "Design and validation strategies for obtaining assurance in countermeasures to power analysis and related," in the proceedings of the NIST physical security workshop, San Francisco, 2005, pp. 1–11.

[9] M. L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in International workshop on cryptographic hardware and embedded systems, Berlin, 2001, pp. 309–318.

[10] S. Yang, W. Wolf, N. Vijaykrishnan, D. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in Design, Automation and Test in Europe, Munich, 2005, pp. 64–69.

[11] B.-D. Choi, K. E. Kim, K.-S. Chung, and D. K. Kim, "Symmetric Adiabatic Logic Circuits against Differential Power Analysis," ETRI Journal, vol. 32, no. 1, pp. 166–168, May 2010.

[12] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in Proceedings Design, Automation and Test in Europe Conference and Exhibition, Paris, 2004, pp. 246–251.

[13] P. Yu and P. Schaumont, "Secure FPGA circuits using controlled placement and routing," in IEEE/ACM international conference on Hardware/software codesign and system synthesis, Salzburg, 2007, pp. 45–50.

[14] Y. Bi, P. E. Gaillardon, X. S. Hu, M. Niemier, J. S. Yuan, and Y. Jin, "Leveraging emerging technology for hardware security - case study on silicon nanowire FETs and graphene Symfets," in IEEE 23rd asian test symposium, Hangzhou, 2014, pp. 342–347.

[15] B.-D. Choi, K. E. Kim, K.-S. Chung, and D. K. Kim, "Symmetric Adiabatic Logic Circuits against Differential Power Analysis," ETRI Journal, vol. 32, no. 1, pp. 166–168, May 2010.

[16] E. Tena-Sanchez, J. Castro, and A. J. Acosta, "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 4, no. 2, pp. 203–215, 2014.

[17] Y. Bi, K. Shamsi, J.-S. Yuan, Y. Jin, M. Niemier, and X. S. Hu, "Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 3, pp. 340–352, Jan. 2017.

[18] M. Alioto and G. Palumbo, Model and design of bipolar and MOS current-mode logic: CML, ECL and SCL digital circuits. Dordrecht: Springer, 2006.

[19] O. Lozada and G. Espinosa, "An improved high speed, and low voltage CMOS current mode logic latch," Analog Integrated Circuits and Signal Processing, vol. 90, no. 1, pp. 247–252, 2016.

[20] Y. Bai, Y. Song, M. N. Bojnordi, A. Shapiro, E. G. Friedman, and E. Ipek, "Back to the Future: Current-Mode Processor in the Era of Deeply Scaled CMOS," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 4, pp. 1266–1279, 2016.

[21] S. Sato, "Graphene for nanoelectronics," Japanese Journal of Applied Physics, vol. 54, no. 4, p.040102, 2015.

[22] H. Owlia and P. Keshavarzi, "Investigation of the novel attributes of a double-gate graphene nanoribbon FET with AlN high-κ dielectrics," Superlattices and Microstructures, vol. 75, pp. 613–620, 2014.

[23] H. Owlia and P. Keshavarzi, "A bilayer graphene nanoribbon field-effect transistor with a dual-material gate," Materials Science in Semiconductor Processing, vol. 39, pp. 636–640, 2015.

[24] Z. Yan, D. L. Nika, and A. A. Balandin, "Thermal properties of graphene and few-layer graphene: applications in electronics," IET Circuits, Devices & Systems, vol. 9, no. 1, pp. 4–12, Jan. 2015.

[25] K. S. Novoselov, "Electric Field Effect in Atomically Thin Carbon Films," Science, vol. 306, no. 5696, pp. 666–669, 2004.

[26] A. K. Geim and K. S. Novoselov, "The rise of graphene," Nature Materials, vol. 6, no. 3, pp. 183–191, 2007.

[27] H. Owlia and P. Keshavarzi, "Locally Defect-Engineered Graphene Nanoribbon Field-Effect Transistor," IEEE Transactions on Electron Devices, vol. 63, no. 9, pp. 3769–3775, 2016.

[28] F. Schwierz, "Graphene transistors," Nature nanotechnology, vol. 5, no. 7, p. 487, 2010.

[29] Y.-W. Son, M. L. Cohen, and S. G. Louie, "Energy Gaps in Graphene Nanoribbons," Physical Review Letters, vol. 97, no. 21, 2006.

[30] F. Schwierz, "Graphene Transistors: Status, Prospects, and Problems," Proceedings of the IEEE, vol. 101, no. 7, pp. 1567–1584, 2013.

[31] Y. Yoon, G. Fiori, S. Hong, G. Iannaccone, and J. Guo, "Performance Comparison of Graphene Nanoribbon FETs With Schottky Contacts and Doped Reservoirs," IEEE Transactions on Electron Devices, vol. 55, no. 9, pp. 2314–2323, 2008.

[32] "Predictive Technology Model (PTM)," Predictive Technology Model (PTM). [Online]. Available: http://ptm.asu.edu/. [Accessed: 15-Nov-2018].

[33] Y.-Y. Chen, A. Sangai, A. Rogachev, M. Gholipour, G. Iannaccone, G. Fiori, and D. Chen, "A SPICE-Compatible Model of MOS-Type Graphene Nano-Ribbon Field-Effect Transistors Enabling Gate- and Circuit-Level Delay and Power Analysis Under Process Variation," IEEE Transactions on Nanotechnology, vol. 14, no. 6, pp. 1068–1082, 2015.

[34] J. M. Rabaey, M. Pedram, Low Power Design Methodologies. Springer Verlag, 2012.

[35] S. Mangard, E. Oswald, and T. Popp, Power analysis attacks: revealing the secrets of smart cards. New York, NY: Springer, 2008.

[36] C. Liang, Y. Wang, and T. Li, "Studies on contact resistance in graphene based devices," Microsystem Technologies, vol. 22, no. 8, pp. 1943–1947, Nov. 2015.

[37] Q. Kong, X. Wang, L. Xia, C. Wu, Z. Feng, M. Wang, and J. Zhao, "Achieving Low Contact Resistance by Engineering a Metal–Graphene Interface Simply with Optical Lithography," ACS Applied Materials & Interfaces, vol. 9, no. 25, pp. 21573–21578, 2017.

[38] K. Zhou, P. Wang, and L. Wen, "Design of power balance SRAM for DPA-resistance," Journal of Semiconductors, vol. 37, no. 4, p. 045002, 2016.

[39] I. Hassoune, F. Mace, D. Flandre, and J.-D. Legat, "Low-swing current mode logic (LSCML): A new logic style for secure and robust smart cards against power analysis attacks," Microelectronics Journal, vol. 37, no. 9, pp. 997–1006, 2006.

[40] C. Monteiro, Y. Takahashi, and T. Sekine, "Low-power secure S-box circuit using charge-sharing symmetric adiabatic logic for advanced encryption standard hardware design," IET Circuits, Devices & Systems, vol. 9, no. 5, pp. 362–369, Jan. 2015.