نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۳، پاییز ۱۳۹۸، ص ۱۰۴-۹۳

بررسی روش‌های مقابله با حملات کانال جانبی از طریق منطق تفاضلی پویا

فاطمه پویان[۱]، سیاوش بیات سرمدی[۲*]
۱- دانشجوی کارشناسی‌ارشد، ۲- استادیار، دانشگاه صنعتی شریف

(دریافت: ۹۷/۰۹/۱۲، پذیرش: ۹۷/۱۲/۱۴)

چکیده

امروزه الگوریتم‌های رمزنگاری نفوذناپذیر و کارآمدی برای حفظ امنیت اطلاعات در سامانه‌های کامپیوتری به‌کار می‌روند. این الگوریتم‌ها به شیوه‌ای طراحی شده‌اند که به‌دست آوردن کلید و دست‌یابی به داده‌های رمزشده توسط آن‌ها از طریق تحلیل الگوریتم، در زمان قابل قبول ناممکن باشد. با این وجود، امکان دست‌یابی مهاجمان به اطلاعات محرمانه از طریق تحلیل اطلاعات جانبی مدار رمزنگاری مانند توان مصرفی یا اندازه‌گیری میدان مغناطیسی، وجود دارد. استفاده از منطق تفاضلی پویا، یکی از موثرترین روش‌های مقابله با حملات توانی است. در این روش، مصرف توان تا حد امکان نسبت به داده‌های رمزنگاری ناهمبسته می‌شود و اجرای حملات کانال جانبی از نوع حملات توانی را مشکل می‌سازد. در این مقاله، تعدادی از روش‌های کاربردی و اصلی مقابله با حملات کانال جانبی بررسی شده‌اند. با وجود این‌که امکان پیاده‌سازی اغلب این روش‌ها به‌صورت مدار مجتمع خاص منظوره وجود دارد اما در این مقاله روش‌های گردآوری شده با هدف پیاده‌سازی روی تراشه‌های قابل بازپیکربندی بررسی و مقایسه شده‌اند. همچنین، کلیه این روش‌ها با استفاده از منطق تفاضلی پویا در مقابل حملات تحلیل توان، مقاوم شده‌اند. در ادامه این مقاله، این روش‌ها از جنبه‌های متفاوتی مانند آسیب‌پذیری در مقابل حملات، محدودیت‌های پیاده‌سازی و سربار تحمیل شده به مدار، با یکدیگر مقایسه شده‌اند. در پایان این مقاله با ارزیابی روش‌های شرح داده شده، نشان می‌دهد که چالش‌های پیش‌روی منطق تفاضلی پویا در ازای تحمیل سربار بالاتر کاهش می‌یابند. بررسی‌ها نشان داده که روش SDDL با ۲۰۰٪ کمترین سربار و روش DWDDL با ۱۱۶۰٪ بیشترین سربار را در پیاده‌سازی دارد. هر چند کامل‌ترین روش شرح داده شده، همچنان با محدودیت‌هایی در پیاده‌سازی مواجه است.

کلیدواژه‌ها: منطق تفاضلی پویا، حملات کانال جانبی، تراشه‌های قابل باز پیکربندی، اختفای اطلاعات

۱- مقدمه

امروزه امنیت سامانه‌های سخت‌افزاری در دنیای امروز از اهمیت ویژه‌ای برخوردار است. حملات فیزیکی تهدید اصلی برای این نوع از سامانه‌ها محسوب می‌شوند که در سه دسته قابل تقسیم‌بندی هستند [۱]. اولین دسته از این نوع حملات، حملات تهاجمی است که ابتدا پوشش محافظ تراشه را تخریب می‌کند و در ادامه با لایه‌برداری سطوح مختلف مدار مجتمع و تحلیل آنها، ساختار مدار را بازیابی می‌نماید. دسته دوم، حملات نیمه تهاجمی است که در مرحله تخریب محافظ تراشه با حملات تهاجمی مشترک است ولی مرحله لایه‌برداری بعد از آن به‌صورتی انجام می‌شود که مدار از حالت عملیاتی خارج نشود. دسته سوم، حملات غیرتهاجمی است که حالت تخریبی ندارد و بنابراین، اثری از حمله باقی نمی‌ماند و از این جهت خطر بیشتری نسبت به دو نوع حمله قبلی دارد که قربانی از حمله صورت گرفته مطلع نمی‌شود.

حمله‌های کانال جانبی امروزه از مهمترین حملات غیرتهاجمی به شمار می‌روند که سامانه‌های رمزنگاری سخت‌افزاری را تهدید می‌کنند. مهاجم در این حملات با استفاده از اطلاعات فیزیکی مدار مورد حمله نظیر توان مصرفی، تاخیر مدار یا میدان الکترومغناطیس به اطلاعاتی در مورد داده‌های مورد پردازش و یا عملیات انجام گرفته دست می‌یابد. با توجه به بسیاری از پژوهش‌های صورت گرفته در این زمینه، حمله‌های توانی از جمله قوی‌ترین و عملیاتی‌ترین تهدیداتی هستند که مدارهای رمزنگاری را تهدید می‌کنند. در این حمله‌ها می‌توان با استفاده از اطلاعات توان مصرفی و داده‌های ورودی یا خروجی، به کلید رمزنگاری دسترسی پیدا کرد. امروزه تراشه‌های قابل بازپیکربندی به‌علت دارا بودن ویژگی‌هایی از جمله تسریع پیاده‌سازی و قابلیت ایجاد تغییر و به‌روزرسانی در مدار، کاربرد گسترده‌ای یافته‌اند. با توجه به همین امر، روش‌های گردآوری

* رایانامه نویسنده مسئول: sbayat@sharif.edu

شده در این مقاله با تمرکز بر پیاده‌سازی روی بستر تراشه‌های قابل بازپیکربندی بررسی و مقایسه شده‌اند. در ادامه، ابتدا برخی از مفاهیم پرکاربرد در این حوزه معرفی می‌شود و سپس روش‌های موجود برای مقابله با حملات تحلیل توانی بر اساس منطق تفاضلی پویا مورد بررسی قرار می‌گیرد. در ادامه این مقاله، این روش‌ها از جنبه‌های متفاوتی مانند آسیب‌پذیری در مقابل حملات، محدودیت‌های پیاده‌سازی و سربار تحمیل شده به مدار، با یکدیگر مقایسه شده‌اند. در پایان، ارزیابی‌های صورت گرفته در این مقاله نشان می‌دهد که چالش‌های پیش‌روی منطق تفاضلی پویا با تحمیل سربار بیشتر، کاهش می‌یابند.لازم به ذکر است که کامل‌ترین روش شرح داده شده، همچنان با محدودیت‌هایی در پیاده‌سازی مواجه است.

ساختار ادامه این نوشتار به شرح زیر است: در بخش ۲، مفاهیم اولیه اعم از حملات توانی ساده، تفاضلی و روش‌های مقابله با آنها مطرح می‌شود. در بخش ۳، روش‌های مقابله به همراه جزئیات پیاده‌سازی ارائه می‌شود. مقایسه این روش‌ها از لحاظ نقاط آسیب‌پذیری، محدودیت‌های و سربار پیاده‌سازی در بخش ۴ انجام می‌شود. در پایان جمع‌بندی از مطالب موجود در این مقاله در بخش ۵ ارائه می‌گردد.

۲- مفاهیم اولیه

در این بخش تعدادی از تعاریف و مفاهیم مرتبط با حملات توانی و منطق‌های تفاضلی پویا شرح داده شده است. در حالت کلی، حمله‌های توانی را می‌توان به دو دسته حمله توانی ساده و تفاضلی تقسیم کرد.

۲-۱- تحلیل توانی ساده

در این مدل حمله اطلاعات توان مصرفی به صورت عینی تحلیل می‌شوند. به‌طور کلی، در این نوع حملات، هدف تشخیص فازهای مختلف برنامه‌ی در حال اجرا از روی مشاهدات توان است. به‌عنوان مثال با تشخیص نحوه اجرا دستورات شرطی وابسته به داده‌های رمزنگاری می‌توان به کلید رمزنگاری دست یافت.

۲-۲- تحلیل توانی تفاضلی

در این نوع حمله برخلاف دسته قبل داده‌های مربوط به توان مصرفی بر اساس فرضیاتی در مورد کلید، مقدار ورودی‌ها یا خروجی‌هایی با توزیع یکنواخت به‌دست می‌آید و سپس بر اساس تحلیل‌های آماری روابط حاکم بین داده‌های به‌دست‌آمده، محتمل‌ترین حدس برای کلید مشخص می‌شود. در واقع روش پیاده‌سازی حمله تحلیل توان تفاضلی براساس تفاضل‌گیری از میانگین مصرف توان مدار به ازای دو دسته از ردیابی توانی است. به این صورت که با حدس مقدار کلید و براساس ورودی‌های مدار می‌توان مقدار یک سیگنال خاص در زمان t را به‌دست آورد (dt). بر همین اساس داده‌های ردیابی توانی به‌دست‌آمده را به دو دسته تقسیم کرده (dt=0, dt=1) و پس از میانگین‌گیری از هر دسته تفاضل مصرف توان را به‌دست می‌آورند. در واقع، هدف روش‌های مقابله با این نوع از حملات، کاهش همبستگی بین میزان مصرف توان و داده‌های میانی مورد پردازش در مدار است. این روش‌ها به دو دسته اختفای اطلاعات و پوشاندن آنها تقسیم می‌شوند.

- **اختفای اطلاعات**

در روش‌های اختفا اطلاعات، تمرکز بر روی یکسان‌سازی مصرف توان بدون توجه به داده‌های میانی و یا افزودن اختلال است. این کار باید به‌گونه‌ای انجام شود که وابستگی توان مصرفی به کلید را از بین ببرد. در حال حاضر روش‌های موجود در سطح سلول به تصحیح مدار می‌پردازند. در این سطح تلاش می‌شود که در سلول طراحی شده وابستگی بین داده مورد پردازش و توان مصرفی به حداقل برسد [۸-۲].

- **پوشاندن اطلاعات**

در روش‌های پوشاندن اطلاعات نیز تلاش می‌شود تا با افزودن یک عامل تصادفی، توان مصرفی مدار به یک مقدار تصادفی تبدیل شود و به این ترتیب وابستگس داده مورد پردازش و میزان توان مصرفی مدار کاهش یابد. این روش‌ها تاکنون در سطوح مختلفی مثل سطح دروازه و سطح الگوریتم پیاده‌سازی شده‌اند [۱۱-۹].

۲-۳- اختلالک[1]

اختلالک به تغییرات کوتاه مدت یک سیگنال پیش از ثابت شدن مقدار نهایی آن گفته می‌شود که به صورت ناخواسته در آن ایجاد می‌شود که مهاجمان با استفاده از این اختلالک‌ها می‌توانند به برخی اطلاعات محرمانه دست یابند.

۲-۴- منطق مثبت

منظور از منطق مثبت، پیاده‌سازی توابع منطقی مدار فقط با دروازه‌های AND و OR است. در این پیاده‌سازی امکان استفاده از تابع نقیض وجود ندارد. به همین علت، با پیاده‌سازی دوگان هر تابع، به‌ازای هر سیگنال مقدار نقیض آن نیز در اختیار خواهد بود. یکی از ویژگی های توابع در منطق مثبت، صفر بودن خروجی در صورت صفر بودن تمامی ورودی‌ها است.

[1] Glitch

۳- مروری بر کارهای پیشین

یکی از روش های اصلی مقابله با حملات کانال جانبی پیاده‌سازی مدار با منطق تفاضلی پویا است. در این روش مدار به صورت دو واحد موازی پیاده می‌شود که نسبت به هم به صورت تفاضلی عمل می‌کنند. عملکرد تفاضلی این دو واحد به معنای وجود مقادیر نقیض متناظر در آن‌ها است. به‌علاوه، به‌منظور همگام‌سازی مصرف توان و مسطح کردن شکل موج توان مصرفی مدار در طول زمان این پیاده‌سازی به‌صورت پویا عمل می‌کند.

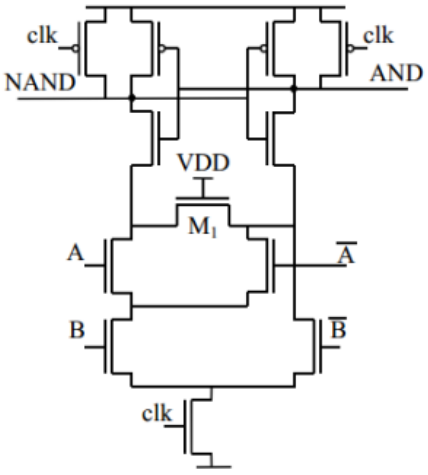
۳-۱- SABL[1]

SABL یکی از اولین روش‌های پیشنهادی به‌منظور مقابله با حمله‌های کانال جانبی است که در سطح دروازه به ارائه راه مقابله‌ای برای این نوع حملات می‌پردازد. این روش مختص مدارهای پیاده‌سازی شده به‌صورت مدارهای مجتمع خاص منظوره است. نمونه‌ای از آن در مقاله [۱۲] ارائه شده است.

دروازه‌های طراحی شده در این منطق، مانند منطق CMOS[2] با دریافت ورودی‌ها و معکوس آن‌ها خروجی و معکوس آن را تولید می‌کنند. دروازه‌های طراحی شده در این روش مانند سایر روش‌های منطق تفاضلی پویا در دو فاز فعالیت می‌کنند. خروجی اصلی و تفاضلی مدار در فاز پیش شارژ توسط مسیری به منطق مثبت متصل می‌شوند. در این فاز تعدادی از خازن‌های موجود در مدار، مستقل از مقدار ورودی‌ها شارژ خواهند شد. در فاز ارزیابی بسته به مقدار ورودی‌ها، یکی از خروجی‌های اصلی یا تفاضلی، مسیری به سمت پتانسیل صفر (GND) خواهند داشت که تمامی خازن‌های شارژ شده در فاز پیش شارژ از طریق این مسیر تخلیه می‌شوند. دروازه‌های طراحی‌شده با این روش، در هر سیکل کلاک ظرفیت ثابتی از خازن‌های بار را شارژ می‌کنند. بنابراین، مصرف توان در این دسته دروازه‌ها مستقل از ورودی یکنواخت خواهد بود.

۳-۱-۱- جزئیات پیاده‌سازی

در شکل (۱) پیاده‌سازی یک دروازه تفاضلی AND/NAND نشان داده شده است. هر دروازه در منطق SABL را می‌توان شامل دو بخش در نظر گرفت. یکی از این بخش‌ها شبکه اتصال به زمین تفاضلی است. این بخش از دروازه نقش پیاده‌سازی مسیر اتصال به زمین و تخلیه خازن‌های بار را بر حسب مقادیر ورودی و تابع پیاده‌سازی شده بر عهده دارد. در پیاده‌سازی موجود در شکل (۱)، این بخش در نیمه پائینی شکل و با ورودی‌های A,B و نقیض آن‌ها نمایش داده شده‌اند. قسمت دوم دروازه بخشی است که در فاز پیش شارژ وظیفه تغییر مقدار خروجی‌های تفاضلی و اتصال هر دوی آنها به مقدار VCC را بر عهده دارد. هر یک از دو بخش مدار به شیوه‌ای طراحی شده‌اند که در هر سیکل کلاک، مقدار یکسانی از خازن بار شارژ و تخلیه می‌شود. در شکل (۱)، این بخش نیمه بالایی مدار و خروجی‌های AND و NAND را شامل می‌شود. با فرض این‌که سیگنال‌های تفاضلی مسیر مشابهی را تا ورودی دروازه بعدی طی می‌کنند، می‌توان ادعا کرد که در این منطق مصرف توان و مقادیر داده‌های مورد پردازش مستقل از یکدیگر هستند.



شکل (۱): پیاده‌سازی تابع NAND در منطق SABL [۲]

۳-۱-۲- معایب

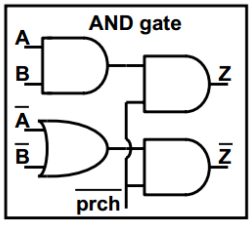
در این روش نیاز است که مسیریابی سیگنال‌های اصلی و نقیض آنها کاملاً یکسان باشد تا خازن‌های بار ناشی از مسیریابی نیز یکسان گردد. به علاوه زمان ورود مدار به فاز ارزیابی بسته به مقدار ورودی‌ها و زمان ورود آنها به این فاز، متغیر خواهد بود که این خود عاملی برای آسیب‌پذیری روش SABL در مقابل حمله‌های کانال جانبی خواهد بود. یک مشکل اساسی در پیاده‌سازی این منطق به روش مطرح شده در مقاله [۱۲]، یک بودن مقدار سیگنال‌ها در طول فاز پیش شارژ است. در صورتی که تغییر ورودی‌ها با تاخیر نسبت به هم انجام شود، ممکن است که خروجی مدار ابتدا به صفر تغییر یابد و با ثابت شدن مقدار ورودی‌ها و دشارژ خازن‌های بار، دیگر امکان برگشت به مقدار یک وجود نخواهد داشت و مدار مقدار نادرستی را تولید خواهد کرد. همچنین این منطق کماکان با مشکل رخداد اختلالک همراه است.

[1] Sense Amplifier Based Logic
[2] Complementary Metal–Oxide–Semiconductor

۳-۲- SDDL[1]

روش SDDL یکی از اولین روش‌های منطق تفاضلی پویا است. این روش قابل پیاده‌سازی روی تراشه‌های قابل باز پیکربندی و مدارهای مجتمع خاص منظوره است. در ادامه این بخش به بررسی این روش پرداخته خواهد شد که در مقاله [۱] ارائه شده است.

برای پیاده‌سازی مدار به روش SDDL، به‌ازای هر دروازه با استفاده از قانون دمورگان، دروازه دوگان آن به شکلی انتخاب می‌شود که با اعمال ورودی‌های نقیض، نقیض خروجی تولید شود. مزیت این کار همپوشانی مصرف توان این دو مسیر برای ایجاد رد توانی ثابت و مستقل از ورودی است. در نتیجه، بین هر دروازه اصلی و دوگان همواره فقط یکی از خروجی‌ها می‌تواند دارای مقدار یک باشد. در ادامه، این دو خروجی (جداگانه) توسط سیگنال سراسری پیش شارژ کنترل می‌شوند. در هنگام ورود به فاز پیش شارژ، مقدار این سیگنال برابر یک (یا صفر بسته به پیاده‌سازی) خواهد بود و بنابراین، خروجی‌های دروازه‌ها و فلیپ‌فلاپ‌ها به حالت NULL (هر دو مقداری یکسان) منتقل می‌شوند. با ورود به فاز ارزیابی مقدار سیگنال پیش شارژ برابر یک (یا صفر) خواهد بود و بنابراین، مقدار خروجی دروازه‌ها و فلیپ‌فلاپ‌ها در مدار انتشار می‌یابد. در این روش، در هر سیکل کلاک مصرف توان (با فرض یکسان بودن مسیریابی در مدار اصلی و دوگان) نسبتاً یکنواخت خواهد بود؛ چون برای هر سیگنال یک تغییر مقدار به‌ازای هر سیکل کلاک مورد انتظار است. شکل (۲) نمایی از پیاده‌سازی دروازه AND را در منطق SDDL را نشان می‌دهد.



شکل (۲): پیاده‌سازی تابع AND در منطق SDDL [۱۳]

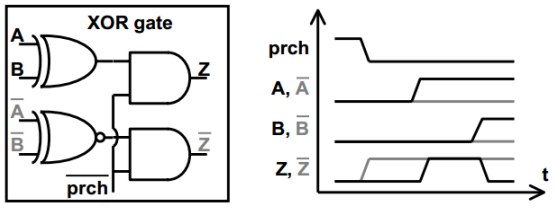
۳-۲-۱- جزئیات پیاده‌سازی

برای پیاده‌سازی این منطق به صورت مدارهای مجتمع خاص منظوره باید خازن‌های بار مربوط به دروازه‌ها و به علاوه، در اتصالات بین دروازه‌ها یکسان باشد. با این حال، می‌توان به علت بزرگتر بودن خازن‌های بار در مسیر ورودی‌های دروازه نسبت به خازن‌های داخل دروازه، از یکسان‌سازی خازن‌های داخل دروازه‌ها صرف نظر کرد. بنابراین مسئله با یکسان کردن مسیریابی بین دو مدار دوگان قابل حل است.

در پیاده‌سازی روی تراشه‌های قابل بازپیکربندی، مسئله تفاوت تاخیر داخلی دروازه‌ها وجود نخواهد داشت، زیرا معمولاً تاخیر جداول جستجو به تابع پیاده‌سازی شده بستگی ندارد. مسئله مهم در اینجا نیز یکسان‌سازی مسیریابی‌ها است. حل این مسئله در تراشه‌های قابل بازپیکربندی نسبت به مدارهای خاص منظوره مشکل‌تر است، چون برای مسیریابی در تراشه‌های قابل بازپیکربندی محدود به استفاده از منابع مسیریابی مشخص و ثابت هستیم. طراحی مسیریاب بهینه و بررسی تاثیرگذاری مسیریابی دو چالش اساسی پیش روی این منطق است [۱۴-۱۵].

۳-۲-۲- معایب

بزرگترین مشکل این روش بروز اختلالک در آن است که اساساً کارایی آن را در برابر حمله‌های کانال جانبی کاهش می‌دهد. این روش ممکن است که به دلیل عدم محدودیت در منطق طراحی، با بروز اختلالک در خروجی همراه باشد. در این‌صورت در فاز ارزیابی، خروجی می‌تواند بیش از یکبار تغییر کند. به علت وجود ارتباط بین مصرف توان و الگوی ورودی‌های مدار در رخداد اختلالک، آسیب‌پذیری در مقابل حمله‌های کانال جانبی در این منطق افزایش می‌یابد. در شکل (۳)، وقوع اختلالک در خروجی Z مدار قابل مشاهده است. به علت تفاوت در تاخیر ورودی‌های A و B مقدار این سیگنال ابتدا برابر یک و سپس صفر خواهد شد و در نتیجه ، دقیقاً یک گذار به‌ازای هر سیگنال نقض رخ خواهد داد.



شکل (۳): رخداد اختلالک در تابع XOR در منطق SDDL [۱۳]

به‌علاوه، مشکل ارزیابی زودهنگام نیز در این مدار رخ می‌دهد. ارزیابی زودهنگام به معنای وجود ارتباط بین الگوی ورودی‌های یک دروازه و زمان ورود آن به فاز ارزیابی است. یک دروازه OR را در این منطق در نظر بگیرید. پس از ورود سیگنال پیش شارژ به فاز ارزیابی، خروجی دروازه در مدار اجازه‌ی انتشار می‌یابد. در این حالت، در صورت یک شدن هر ورودی دروازه، خروجی آن نیز یک خواهد شد. با توجه به این‌که ورودی‌های دروازه می‌توانند با تاخیرهای متفاوتی تغییر کنند، بنابراین، زمان

[1] Separated Dynamic and Differential Logic

ورودِ خروجی دروازه به فاز ارزیابی نیز بسته به الگوی ورودی‌های آن متفاوت خواهد بود.

یکی دیگر از مشکلات این طرح استفاده از سیگنال سراسری پیش شارژ است. با استفاده از یک سیگنال سراسری برای ورود به فاز پیش شارژ تفاوت قابل مشاهده‌ای بین قله مصرف توان در هنگام ورود به فاز پیش شارژ و فاز ارزیابی به‌وجود می‌آید. این تفاوت خود می‌تواند یکی از عوامل آسیب‌پذیری این منطق باشد. همان‌طور که پیش‌تر مطرح شد، این روش نیازمند روشی برای یکسان‌سازی جایابی و مسیریابی دو مدار اصلی و دوگان است. در مرجع [۱۶] امنیت منطق SDDL به‌وسیله طراحی روشی برای جایابی و مسیریابی ارتقا یافته است.

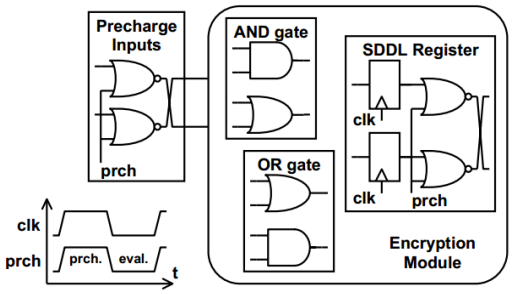
۳-۳- WDDL[1]

برای پیاده‌سازی هر تابع منطقی حداقل به سه تابع OR، AND و INVERTER نیاز است. در این روش، با محدود کردن پیاده‌سازی مدار به استفاده از منطق مثبت، ورود به فاز پیش شارژ به‌صورت یک موج در مدار منتشر می‌شود و در صورت نیاز به نقیض یک سیگنال، از سیگنال متناظر در مدار دوگان استفاده می‌شود.

در این روش در مقاله [۱۳] ارائه شده است که برخلاف روش SDDL برای ورود به فاز پیش شارژ تنها نیاز است تا ورودی‌های اصلی مدار و خروجی فلیپ‌فلاپ ها با استفاده از سیگنال سراسری پیش شارژ کنترل شوند (مشابه SDDL). با ورود به فاز پیش شارژ، مقادیر ورودی‌های تمامی دروازه‌ها در سطح اول (دروازه‌هایی که از ورودی‌های اصلی مدار یا فلیپ فلاپ‌ها ورودی می‌گیرند) صفر می‌شوند، در نتیجه خروجی آن‌ها نیز برابر صفر خواهد شد. این روند به صورت یک موج تمامی مدار را وارد فاز پیش شارژ خواهد کرد. برای ورود به فاز ارزیابی نیز کافی است تا با تغییر مقدار سیگنال سراسری پیش شارژ، مقادیر واقعی فلیپ‌فلاپ‌ها و ورودی‌ها به مدار اعمال شوند. یکی از مهم‌ترین مزایای این روش نسبت به SDDL عدم رخداد اختلالک در آن است. با توجه به این‌که که در هر دو تابع AND و OR در صورت یک شدن ورودی‌ها با تاخیرهای متفاوت، نوسانی در خروجی رخ نخواهد داد، بنابراین، WDDL تضمین می‌کند که هر سیگنال در هر سیکل کلاک دقیقاً یک بار تغییر مقدار داشته باشد.

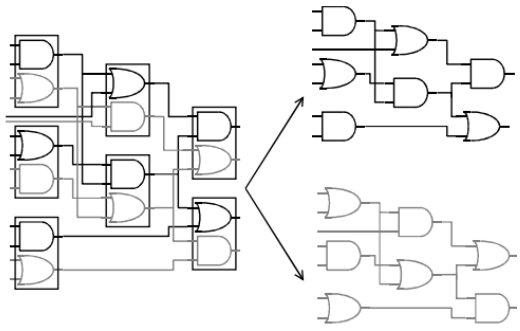
۳-۳-۱- جزئیات پیاده‌سازی

در شکل (۴) دروازه‌های AND و OR پیاده‌سازی شده در منطق WDDL نشان داده شده‌اند. همان‌طور که پیشتر مطرح شد، سیگنال پیش شارژ فقط در ورودی‌ها و خروجی ثبات‌ها به کار می‌رود. در روش‌های منطق تفاضلی پویا یکی از مهم‌ترین مسائل، پیاده‌سازی طراحی به‌گونه‌ای است که مسیریابی مدارهای اصلی و دوگان کمترین اختلاف ممکن را داشته باشند. زیرا در صورت مسیریابی متفاوت سیگنال‌های متناظر، مسطح‌سازی توان مصرفی میسر نخواهد شد که هدف اصلی طراحی است.



شکل (۴): پیاده‌سازی توابع AND و OR در منطق WDDL [۱۳]

برای پیاده‌سازی WDDL با مسیریابی‌های نسبتاً یکسان، یکی از روش‌های پیشنهادی، حذف کردن وابستگی قسمت‌های اصلی و دوگان از یکدیگر به منظور دستیابی به دو مدار کاملاً مجزا است. در این روش ابتدا مدار داده شده به گونه‌ای تغییر داده می‌شود که به جز در ورودی‌های مدار به استفاده از معکوس‌کننده نیازی وجود نداشته باشد. این هدف در صورتی قابل دست‌یابی است که به ازای ورودی‌های مدار، معکوس آن‌ها نیز در اختیار باشد.



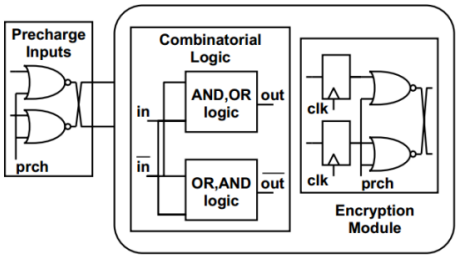
شکل (۵): تولید دو بخش مجزا پس از پیاده‌سازی در منطق WDDL [۱۳]

در مرحله بعد مدار با منطق WDDL تولید می‌شود. همان‌طور که در بخش قبل گفته شد، در پیاده‌سازی WDDL قسمت‌های اصلی و دوگان مدار برای تولید معکوس سیگنال‌ها به هم مرتبط هستند (Cross Coupling). با توجه به این‌که پیاده‌سازی مدار بدون نیاز به معکوس‌کننده در مرحله اول انجام شده است، بنابراین، در پیاده‌سازی، WDDL قسمت‌های اصلی و

[1] Wave Dynamic Differential Logic

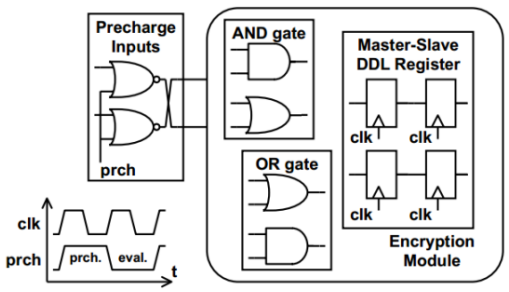
دوگان از هم مجزا هستند. شکل (۵) مثالی از نحوه جداسازی دو مدار برای حذف وابستگی آن ها به یکدیگر را نشان می‌دهد.

در این حالت می‌توان مدار اصلی را جایابی و مسیریابی کرد. برای ساختن مدار دوگان از روی آن نیز تنها به تعویض توابع به کمک قانون دمورگان نیاز است. در این‌صورت می‌توان مسیریابی این دو مدار را مشابه دانست. هر چند که به‌علت جایابی‌های متفاوت همچنان با مسئله اختلاف فرآیند در فناوری‌های با ابعاد نانومتری روبه‌رو خواهیم بود.



شکل (۶): پیاده‌سازی توابع در منطق DWDDL [۱۳]

به این منطق که با تغییر جزئی از WDDL به‌دست‌آمده است، Divided WDDL گفته می‌شود. شکل (۶) نمایی سطح بالا از منطق DWDDL[1] را نشان می‌دهد. همان‌طور که در شکل مشاهده می‌شود، مدارهای اصلی و دوگان آن به‌طور کامل از یکدیگر مجزا هستند و با توابع دوگان پیاده‌سازی شده‌اند. همچنین با ایجاد تغییراتی در پیاده‌سازی فلیپ‌فلاپ در این منطق می‌توان موج پیش شارژ را بدون نیاز به توابع XOR نشان داده شده در خروجی فلیپ‌فلاپ‌ها، بر روی خروجی آن‌ها اعمال کرد.



شکل (۷): پیاده‌سازی فلیپ‌فلاپ حاکم-تابع در منطق WDDL [۱۳]

در این منطق برای پیاده‌سازی فلیپ‌فلاپ‌ها، از دو فلیپ‌فلاپ استفاده می‌شود که به‌صورت تابع- حاکم به هم متصل شده‌اند. هر چند در این حالت برای دست‌یابی به نرخ داده معادل با حالت قبل، باید فرکانس کاری مدار را دو برابر نمود ولی در این وضعیت کل مجموعه هر فلیپ‌فلاپ در هر سیکل کلاک یک بار صفر می‌شوند. شکل (۷)، منطق WDDL را با استفاده از فلیپ‌فلاپ‌های تابع- حاکم نمایش می‌دهد.

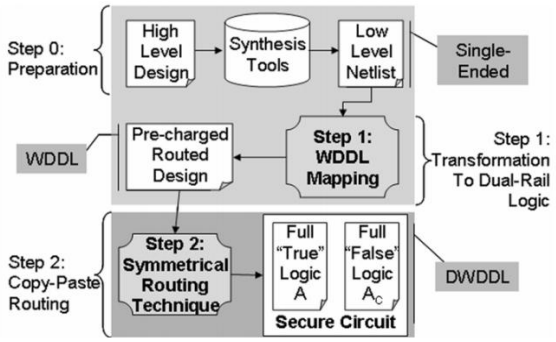
۳-۳-۲- معایب

یکی از معایب این روش محدود بودن به پیاده‌سازی مدار تنها با استفاده از دورازه‌های منطق مثبت است. این محدودیت ممکن است، منجر به افزایش مصرف منابع شود. به‌علاوه، به‌علت این محدودیت در قسمت‌هایی از مدار که به تابع نقیض نیاز است، باید از جابه‌جایی سیگنال‌های دو مدار اصلی و دوگان (Cross Coupling) استفاده شود. این مسئله تا حد زیادی یکسان‌سازی جایابی و مسیریابی این دو مدار را تحت تاثیر قرار می‌دهد. روش WDDL همچنین با مشکل ارزیابی زودهنگام رو به رو است. همان طور که در بخش پیش توضیح داده شد، در این روش نیز زمان ورود به فاز ارزیابی به الگوی ورودی‌ها بستگی دارد. بنابراین، امکان حمله موفق به این پیاده‌سازی وجود دارد.

۳-۴- DWDDL[2]

این منطق برگرفته از روش WDDL است. در این روش تمرکز بر یکسان‌سازی حداکثری جایابی و مسیریابی با هدف دست‌یابی به سطح مطلوبی از مسطح شدن توان مصرفی است [۲]. در این روش برای مدار هدف دو بار با استفاده از منطق WDDL دو مدار مجزا تولید می‌شود. این دو مدار باید دوگان هم باشند. در این صورت می‌توان ادعا کرد که به‌علت یکسان بودن جایابی و مسیریابی بین دو مدار WDDL تولید شده، به سطح قابل قبولی از مسطح‌سازی توان مصرفی و تاخیر مسیرها دست یافته است.

در شکل (۸) روش کلی تولید این منطق نمایش داده شده است. در این روش، تمامی جزئیات پیاده‌سازی با پیاده‌سازی مربوط به منطق WDDL که در بخش قبل به آن پرداخته شده، مشابه می‌باشد.



شکل (۸): فرایند پیاده‌سازی مدار با منطق DWDDL [۲]

[1] Divided Wave Dynamic Differential Logic

[2] Double Wave Dynamic Differential Logic

۳-۴-۱- معایب

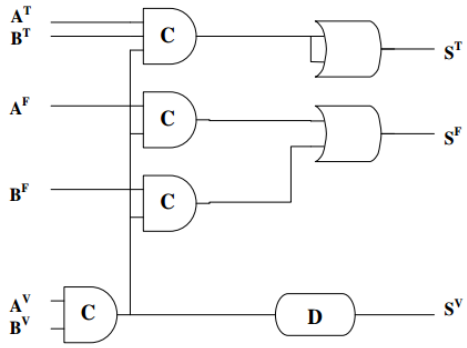
در این روش با وجود دست‌یابی به امنیت بالاتر و مقاومت بهتر در مقابل حمله‌های توانی، دو برابر شدن سربار مساحت نسبت به منطق WDDL مسئله قابل توجهی می‌باشد که استفاده عملی از این روش را با محدودیت‌ها و چالش‌هایی رو به رو می‌سازد.

۳-۵- STTL[1]

در این بخش به بررسی روش STTL پرداخته می‌شود که در منابع [۹ و ۱۷] ارائه شده است. در این منطق، سعی شده است تا مشکل رخداد ارزیابی زودهنگام، به‌وسیله افزودن یک سیگنال کمکی حل شود. به‌ازای سیگنال فرضی XT و دوگان آن، XF، $(XF \ \& \ XT)' = XV$ برقرار است. بنابراین، مقدار XV در صورتی برابر یک خواهد بود که مقادیر اصلی و دوگان سیگنال معتبر باشند و در غیر این‌صورت مقدار سیگنال برابر صفر خواهد بود (به دلیل استفاده از سیگنال اعتبار در این روش، امکان صفر شدن همزمان یک وروی معتبر و دوگان آن وجود ندارد). به‌ازای هر ورودی X یک ورودی XV نیز به هر دروازه وارد می‌شود که معتبر بودن مقدار سیگنال X را نشان می‌دهد. مقدار خروجی دروازه درصورتی تولید می‌شود که سیگنال اعتبار برای تمامی ورودی‌ها معتبر باشد. به‌علاوه، به‌ازای خروجی دروازه (Y) نیز سیگنال YV تولید می‌شود. نکته مهم در این منطق لزوم وجود تاخیر بین زمان تولید هر سیگنال و سیگنال اعتبار متناظر با آن است. در حقیقت وجود تاخیر باعث می‌شود تا در هر دروازه مدار، ابتدا مقدار خروجی با توجه به ورودی‌ها تعیین شود. این مقدار فقط وقتی در سطح بعد استفاده می‌شود که سیگنال اعتبار متناظر خروجی، پس از پس از سپری شدن تاخیر معینی، برابر یک شود. بنابراین، نشان می‌دهد که مستقل از وجود تفاوت در مسیریابی و جایابی مدار، می‌توان تاخیر انتشار را در این منطق کنترل کرد.

۳-۵-۱- جزئیات پیاده‌سازی

در شکل (۹) پیاده‌سازی منطقی تابع AND دو ورودی در این منطق نشان داده شده است. همان طور که مشاهده می‌شود، مقدار خروجی فقط در هنگام یک بودن مقدار سیگنال اعتبار برای ورودی‌های مورد نظر می‌تواند برابر یک شود. به‌علاوه، مقدار بیت اعتبار برای خروجی با تاخیر مشخصی نسبت به یک شدن این سیگنال برای ورودی‌ها تولید می‌شود. ماژول تاخیر می‌تواند تضمین کند که زمان تولید خروجی و سیگنال اعتبار مربوط به آن نسبت به هم تاخیر دارند.



شکل (۹): پیاده‌سازی تابع AND مدار با منطق STTL [۹]

۳-۵-۲- معایب

مسئله اساسی که در این طراحی به آن توجه نشده است، عدم استفاده از منطق پویا به‌منظور مسطح‌سازی مصرف توان در تمامی سیکل‌های کلاک و مستقل از تغییرات ورودی است. در حقیقت در این مدار درصورت رخداد تغییری در ورودی، مستقل از مقدار ورودی‌ها با تاخیر ثابتی این تغییر در مدار منتشر می‌شود اما بین مقدار مصرف توان و اصل رخ دادن تغییر در مقدار ورودی‌ها و انتشار آنها همبستگی وجود دارد. از طرف دیگر، در نحوه پیاده‌سازی دروازه‌های پایه‌ای (دروازه پایه‌ای، دروازه‌ای است که برای پیاده‌سازی هر تابع دیگر محدود و ملزم به استفاده از آن هستیم) این منطق در مدارهای خاص منظوره یا تراشه‌های قابل بازپیکربندی، به یکسان بودن مقدار توان مصرفی برای مدارهای مثبت و منفی توجهی نشده است که این مسئله نیز می‌تواند عامل مهمی برای آسیب‌پذیر بودن روش STTL نسبت به حملات کانال جانبی به‌شمار رود.

۳-۶- BCDL[2]

در این منطق به‌طور همزمان به حل مشکل پیش شارژ زودهنگام و ارزیابی زودهنگام در مدارهای تفاضلی پویا می‌پردازد که در مقاله [۱۸] ارائه شده است.

۳-۶-۱- مقدمه‌ای بر سیگنال‌های کنترل فاز

در این منطق برای کنترل فازهای هر مدار برای ورود به‌فازهای پیش شارژ و ارزیابی دو سیگنال کمکی تولید می‌شوند. سیگنال U_0 مطابق با شرط زیر تولید می‌شود:

[1] Secure Triple Track Logic

[2] Balanced Cell-based Dual-rail Logic

$$U_0(x.y\ldots) = \begin{cases} 1 & if\ x = y = \cdots = (0.0) \\ 0 & others \end{cases}$$

در حقیقت این سیگنال در صورت صفر بودن تمام ورودی‌های مدار، مقدار یک و در غیر این‌صورت مقدار صفر را خواهد داشت. بنابراین، می‌توان از این سیگنال به‌عنوان مجوز ورود به فاز پیش شارژ استفاده کرد.

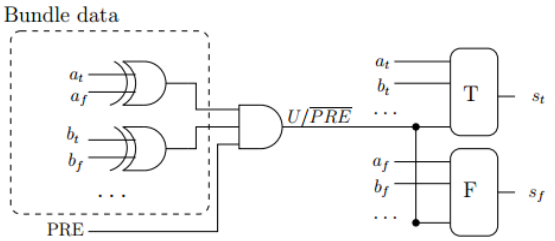
سیگنال U_1 نیز درصورت معتبر بودن ورودی‌های تابع (تمام ورودی‌ها و سیگنال دوگان متناظر آن‌ها مقدار متفاوتی داشته باشند) مقدار یک و در غیر این‌صورت مقدار صفر را خواهد داشت. بنابراین، از این سیگنال می‌توان به‌منظور صدور مجوز برای ورود به فاز ارزیابی استفاده کرد. چون این سیگنال تنها درصورتی برابر یک خواهد شد که تمام ورودی‌های تابع وارد فاز ارزیابی شده باشند. با توجه به توضیحات بالا، می‌توان دریافت که با تولید دو سیگنال U_0 و U_1 برای هر تابع پیاده‌سازی‌شده در جدول جستجو می‌توان ورود به فازهای ارزیابی و پیش شارژ را طوری کنترل کرد که ارزیابی زودهنگام و پیش‌شارژ زودهنگام در مدار رخ ندهد.

$$U_1(x.y\ldots) = \begin{cases} 1 & if\quad x \neq (0.0) \text{ and } y \neq (0.0) \\ 0 & others \end{cases}$$

با توجه به امکان استفاده از خطوط منتقل‌کننده پرسرعتی که برای سیگنال‌های سراسری در تراشه‌های قابل بازپیکربندی در نظر گرفته شده است، در طراحی BCDL به‌منظور کاهش پیچیدگی مدار از یک سیگنال سراسری پیش‌شارژ استفاده شده است. این سیگنال همان‌گونه که در بالا اشاره شد، به جای سیگنال U_0 در کمترین زمان ممکن تمام مدار را وارد فاز پیش‌شارژ می‌کند. در این طرح سیگنال سراسری پیش‌شارژ نسبت به سایر سیگنال‌ها سریع‌تر منتشر می‌شود. بنابراین، مقدار خروجی جداول جستجو سریع‌تر از سایر سیگنال‌های مدار صفر می‌شود. در مورد فاز ارزیابی نیز مجوز ورود به این فاز برای خروجی جداول جستجو، پس از ورود تمامی سیگنال‌های ورودی به فاز ارزیابی، صادر می‌شود. با توجه به این نکات می‌توان گفت که در این مدار اختلالک رخ نمی‌دهد. به‌علاوه، توابع پیاده‌سازی شده در جدول‌های جستجو در این طراحی می‌توانند تمام حالت‌های ممکن را داشته باشند.

۳-۶-۲- جزئیات پیاده‌سازی

در شکل (۱۰) نمایی از پیاده‌سازی یک مدار در منطق BCDL نشان داده شده است.



شکل (۱۰): پیاده‌سازی توابع در منطق BCDL [۱۸]

برای تولید سیگنال U_1 از XOR کردن هر ورودی و مقدار دوگان آن استفاده شده است. سپس مقدار خروجی این توابع XOR با سیگنال پیش شارژ، AND شده است. در نهایت خروجی این AND به یکی از ورودی‌های جدول جستجو، داده شده است. تابع پیاده‌سازی‌شده در جدول جستجو، به‌صورتی تغییر داده می‌شود تا درصورت صفر بودن سیگنال U=PRE خروجی نیز مقدار صفر داشته باشد. در صورت یک بودن این سیگنال خروجی مقدار اصلی تابع را با توجه به ورودی‌ها تولید خواهد کرد.

۳-۶-۳- معایب

طبق نکته گفته شده در مقاله [۱۸] با وجود حذف مشکل ارزیابی زودهنگام و پیش شارژ زودهنگام، به‌علت استفاده از سیگنال سراسری پیش‌شارژ در این طرح و ورود سریع و همزمان خروجی‌های جدول‌های جستجوی مدار به این فاز، قله مصرف توان در هنگام ورود به این فاز در مقایسه با فاز ارزیابی متفاوت خواهد بود. بنابراین، این تفاوت دیده‌شده در مصرف توان، می‌تواند باعث آسیب‌پذیری این منطق در مقابل حمله‌های کانال جانبی شود.

۳-۷- DPL-noEE[1]

همان‌طور که از نام روش ارائه‌شده در مقاله [۱۹] برداشت می‌شود، مشکل ارزیابی زودهنگام در این روش برطرف شده است. در این روش، برای پیاده‌سازی هر تابع از شکل جمع مینترم‌ها استفاده شده است. لازم به ذکر است که برای پیاده‌سازی یک تابع به شکل مجموع مینترم‌ها به تمام ورودی‌ها و نقیض آن‌ها نیاز است. به‌علاوه در این پیاده‌سازی فقط از دروازه‌های AND و OR استفاده می‌شود. در این روش نیز مانند بسیاری از روش‌های دیگر DPL فرض بر یکسان بودن مسیریابی مدار اصلی و دوگان می‌باشد. در پیاده‌سازی توابع به روش مجموع مینترم‌ها، در ورودی هر دروازه AND هر سیگنال ورودی یا نقیض آن وجود دارد. در هنگام ورود به فاز ارزیابی، تا هنگامی که تمامی ورودی‌های یک تابع وارد این فاز نشده باشند، خروجی در فاز پیش‌شارژ باقی می‌ماند؛ زیرا خروجی مجموع مینترم‌هایی است

[1] DPL without Early Evaluation

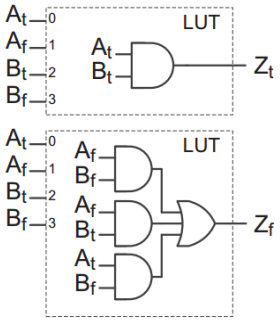
که در ورودی هر کدام از آنها خود یا نقیض سیگنالی وجود دارد که هنوز در فاز پیش شارژ مانده است. بنابراین، آخرین سیگنال خارج شده از فاز پیش شارژ، اجازه ورود خروجی به فاز ارزیابی را صادر می‌کند. زمان ورود هر تابع به فاز ارزیابی، مطابق با زمان خروج آخرین ورودی آن از فاز پیش شارژ تنظیم می‌شود و بنابراین، زمان این تغییر فاز، علاوه‌بر مقدار ورودی‌ها، پس از اعمال آخرین تغییر روی آنها نیز رخ می‌دهد.

۳-۷-۱- جزئیات پیاده‌سازی

در شکل (۱۱)، پیاده‌سازی دروازه‌های AND و NAND در این منطق نشان داده شده است. در هر دو دروازه نشان داده شده، تمامی ورودی‌ها و نقیض آن‌ها در ورودی وجود دارند. همان‌طور که نشان داده شده است، در ورودی تمام دروازه‌های AND استفاده شده حداقل یکی از سیگنال‌های A_t یا A_f و B_t یا B_f وجود دارند.

۳-۷-۲- معایب

در این روش مسئله پیش‌شارژ زودهنگام حل نشده است. به این دلیل که با ورود اولین سیگنال ورودی هر تابع به فاز پیش شارژ، خروجی تابع نیز وارد این فاز خواهد شد. به‌علاوه، مسئله یکسان‌سازی مسیریابی در دو مدار دوگان نیز همچنان وجود دارد.



شکل (۱۱): پیاده‌سازی توابع AND و NAND در منطق DPL-noEE [۱۹]

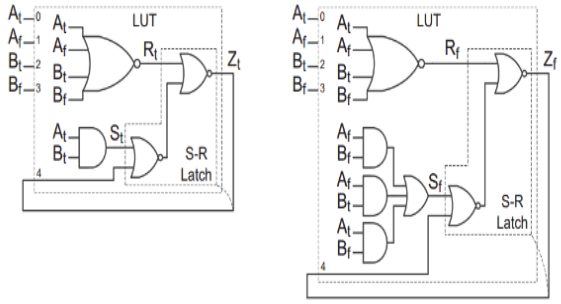
۳-۸- AWDDL[1]

این روش که در مقاله [۱۹] ارائه‌شده تا حدودی به روش DPL-noEE شباهت دارد و در آن علاوه‌بر مسئله ارزیابی زودهنگام، مشکل پیش‌شارژ زودهنگام نیز حل شده است. این روش نیز همچنان با محدودیت یکسان‌سازی مسیریابی رو به رو است. در این روش، توابع مانند روش DPL-noEE به شکل مجموع مینترم‌ها پیاده‌سازی می‌شوند. با این تفاوت که در داخل هر جدول جستجو، یک S-R latch پیاده‌سازی می‌شود که ورودی Set آن به خروجی پیاده‌سازی تابع مورد نظر به شکل مجموع مینترم‌های تابع و ورودی Reset آن به خروجی یک دروازه NOR متصل می‌شود. تمامی ورودی‌های تابع و نقیض‌های آن‌ها به ورودی این دروازه NOR داده می‌شوند.

در هنگام ورود به فاز پیش شارژ در صورتی خروجی جدول جستجو صفر خواهد شد که ورودی Reset یک شده باشد. ورودی Reset از خروجی تابع NOR برای تمام ورودی‌ها و نقیض آن‌ها ساخته می‌شود. بنابراین، درصورتی که تمامی ورودی‌ها وارد فاز پیش شارژ شده باشند، خروجی نیز وارد این فاز خواهد شد. برای ورود به فاز ارزیابی نیز مشابه روش DPL-noEE ابتدا باید تمام ورودی‌ها وارد این فاز شوند تا در نتیجه ورودی Set نیز مقدار معتبر تابع را داشته باشد. به علت صفر بودن مقدار Reset، مقدار نهایی تابع روی خروجی جدول جستجو قرار خواهد گرفت.

۳-۸-۱- جزئیات پیاده‌سازی

در شکل (۱۲)، پیاده‌سازی توابع AND و NAND نشان داده شده است. همان‌طور که مشاهده می‌شود، ورودی‌هایSET از پیاده‌سازی تابع خروجی به شکل مجموع مینترم‌ها و ورودی Reset از NOR شدن ورودی‌ها تولید شده است. ارائه دهندگان این روش، همچنین پیشنهادی به‌منظور یکسان‌سازی مسیریابی‌ها در دو مدار داده شده است. به این‌صورت که مسئله مسیریابی را به‌صورت یک مسئله ارضای محدودیت در می‌آورند. در این مسئله عوامل مهمی در حل مسئله در نظر گرفته می‌شود که در ایجاد اختلاف تاخیر و توان مصرفی دو مسیر تاثیرگذار هستند. در نهایت مسیریابی به‌دست‌آمده در مقایسه با مسیریاب معمولی بهبود قابل ملاحظه‌ای خواهد داشت [۱۹].



شکل (۱۲): پیاده‌سازی توابع AND و NAND در منطق AWDDL [۱۹]

۳-۸-۲- معایب

این روش همچنان محدود به یکسان‌سازی جایابی و مسیریابی دو مدار برای امکان کارکرد صحیح می‌باشد ولی سایر مسائل مطرح

[1] Asynchronous WDDL

برای سایر روش‌ها نظیر ارزیابی زودهنگام، پیش‌شارژ زودهنگام و اختلالک، در این روش حل شده‌اند.

۴- مقایسه و بررسی نتایج

در این بخش روش‌های شرح داده شده، از سه دیدگاه آسیب‌پذیری، سربار تحمیل شده به مدار، جزئیات و محدودیت‌های پیاده‌سازی مورد بررسی قرار گرفته‌اند.

۴-۱- مقایسه نقاط آسیب‌پذیری روش‌ها

در جدول (۱) سه مورد از مهم‌ترین موانع پیش روی منطق‌های تفاضلی پویا مورد بررسی قرار گرفته‌اند. در ستون اول مسئله ارزیابی زودهنگام درج شده است که به معنای وابستگی ورود به فاز ارزیابی، به تغییرات داده‌ها و مقادیر آن‌ها است. روش‌های DPL-noEE، BCDL، STTL و AWDDL، روش‌هایی هستند که در آن‌ها این مسئله رفع شده است.

جدول (۱): مقایسه نقاط آسیب‌پذیری روش‌ها

منطق	ارزیابی زودهنگام	پیش شارژ زودهنگام	رخداد اختلالک
SDDL	✓	✓	✓
WDDL	✓	✓	×
DWDDL	✓	✓	×
STTL	×	×	×
BCDL	×	×	×
DPL-noEE	×	✓	×
AWDDL	×	×	×

در ستون بعدی مسئله پیش‌شارژ زودهنگام بررسی شده است که مشابه قسمت قبل در فاز پیش‌شارژ رخ می‌دهد. همان طور که مشاهده می‌شود، روش DPL-noEE تنها روشی است که فقط در فاز ارزیابی موفق به حل این مسئله شده است ولی همچنان در فاز پیش‌شارژ آسیب‌پذیر است. در پایان آسیب‌پذیری از طریق رخداد اختلالک در هر یک از روش‌ها بررسی شده است. همان‌طور که مشاهده می‌شود، تنها در روش SDDL با این مسئله رو به رو هستیم و در سایر روش‌ها با دو شیوه زیر از رخداد اختلالک جلوگیری شده است:

۱) محدود بودن به استفاده از توابع پایه‌ای یکنوا (DWDDL، WDDL)

۲) مقید کردن ورود به فاز ارزیابی، به ورود تمامی سیگنال‌های ورودی به این فاز (AWDDL، DPL-noEE، BCDL، STTL)

۴-۲- مقایسه جزئیات پیاده‌سازی روش‌ها

در جدول (۲) سه ویژگی پیاده‌سازی روش‌ها بررسی شده‌اند. در ستون اول، در صورت وجود، تابع پایه‌ای پیاده‌سازی هر منطق درج شده است. به‌عنوان مثال، پیاده‌سازی منطق WDDL و DWDDL ملزم به استفاده از منطق مثبت (توابع AND و OR) است. لازم به‌ذکر است که در منطق‌های DWDDL و WDDL محدود بودن به استفاده از توابع پایه‌ای خاص خود می‌تواند دلیلی برای سربار مساحت بیشتر نسبت به سایر روش‌ها باشد.

در ستون بعد، محدودیت‌های و پیش‌فرض‌های پیاده‌سازی روش‌ها مقایسه شده‌اند. همان‌طور که مشاهده می‌شود، تمامی روش‌ها نیازمند یکسان‌سازی جایابی و مسیریابی در دو مدار می‌باشند. این یکسان‌سازی به مسطح‌سازی مصرف توان در دو مدار و افزایش مقاومت در برابر حمله‌های کانال جانبی می‌انجامد. در روش STTL علاوه‌بر مورد قبل، برای تضمین کارکرد صحیح مدار باید بتوان به نحوی تاخیر مورد نیاز در انتشار سیگنال اعتبار را ایجاد نمود. بنابراین، روش ایجاد این تاخیر نیز یکی از مواردی است که در پیاده‌سازی این روش مورد توجه قرار می‌گیرد.

جدول (۲): مقایسه محدودیت‌های پیاده‌سازی در روش‌های معرفی‌شده

منطق	اجزای سازنده	محدودیت‌های پیاده‌سازی
SDDL	–	جایابی و مسیریابی
WDDL	منطق مثبت	جایابی و مسیریابی
DWDDL	منطق مثبت	جایابی و مسیریابی
STTL	–	ایجاد تاخیر برای سیگنال اعتبار، جایابی و مسیریابی
BCDL	–	جایابی و مسیریابی
DPL-noEE	–	جایابی و مسیریابی
AWDDL	–	جایابی و مسیریابی

۴-۳- مقایسه سربار

در این بخش به تحلیل سربار مساحت و همچنین نرخ داده در روش‌ها پرداخته خواهد شد. در این قسمت منظور از سربار مساحت، مجموع مساحت فلیپ فلاپ‌ها و جدول‌های جستجوی مورد نیاز در پیاده‌سازی است.

در جدول (۳) منطق‌های مختلف از لحاظ سربار مساحت و نرخ داده، مقایسه شده‌اند. در ستون اول، سربار مساحت مدار AES-128[1] یا DES[2] (لگوریتم‌های رمزنگاری که در بسیاری از پژوهش‌ها به‌عنوان الگوریتم هدف پیاده‌سازی می‌شوند) در

[1] Advanced Encryption Standard
[2] Data Encryption Standard

مقایسه با پیاده‌سازی آن در حالت غیر حفاظت‌شده اصلی بر حسب درصد بیان شده است. همان‌طور که در جدول (۳) مشاهده می‌شود، بیشترین سربار مساحت مربوط به منطق DWDDL است. این نتیجه با توجه به استفاده از دو مدار در منطق WDDL، مورد انتظار است. کمترین سربار مساحت نیز مربوط به منطق SDDL می‌باشد. این منطق ساده‌ترین روش مقابله با حملات کانال جانبی است که با مسئله اختلالک و انتشار زودهنگام رو به رو می‌باشد.

جدول (۳): مقایسه روش‌ها بر اساس سربار مساحت و نرخ داده

منطق	مدار کامل	دروازه دو ورودی در جدول جستجوی *Kintex-7*		فلیپ فلاپ	نرخ داده
		AND, NAND, OR, NOR	XOR, XNOR		
SDDL [۱۶]	Spartan-3 AES ۲۰۰٪	۲×		×۲	> ۵۰٪
WDDL [۲۰]	Spartan-3 AES ۵۸۰ ٪	×۲	×۲	×۲	> ۵۰٪
DWDDL [۲۰]	Spartan-3 AES ۱۱۶۰ ٪	×۴	×۲۱	×۴	< ۵۰٪
STTL [۹]	Spartan-3 DES ۵۶۰ ٪	×۶		×۲	> ۲۵٪
BCDL [۲۰]	Startix-II AES ۳۰۰ ٪	×۴		×۲	< ۵۰٪
DPL-noEE [۲۱]	Spartan-6 AES ۲۷۰ ٪	×۲		×۲	> ۵۰٪
AWDDL [۲۱]	Spartan-6 AES ۵۰۰ ٪	×۴		×۲	> ۵۰٪

ستون دوم، به منظور ممکن ساختن مقایسه‌ی این منطق‌ها از لحاظ میزان سربار مساحت، به بررسی تعداد جداول جستجوی لازم برای پیاده‌سازی یک تابع دو ورودی در بورد Kintex-7متعلق به شرکت Xilinx پرداخته است. در این مدار، جداول جستجو دارای ۶ ورودی و ۲ خروجی می‌باشند که از آنها می‌توان برای پیاده‌سازی یک تابع ۶ ورودی و یا دو تابع ۵ ورودی با ورودی‌های مشترک استفاده کرد. همان طور که مشاهده می‌شود، بیشترین سربار مساحت در این قسمت برای مدار DWDDL می‌باشد.

در ستون سوم، تعداد فلیپ‌فلاپ‌های لازم برای پیاده‌سازی یک فلیپ‌فلاپ در هر یک از روش‌ها مورد بررسی قرار گرفته است. باید به این نکته توجه کرد که در تعدادی از این منطق‌ها، برای پیاده‌سازی صحیح فلیپ‌فلاپ نیازمند استفاده از مدارهای ترکیبی نیز می‌باشند که در این ستون از گزارش سربار آنها صرف نظر شده است. همان طور که مشاهده می‌شود، به جز روش DWDDL سایر روش‌ها به دو برابر فلیپ‌فلاپ نیاز دارند که علت این امر، استفاده از دو مدار اصلی و دوگان است. در DWDDL نیز به علت پیاده‌سازی دو مدار به روش WDDL تعداد ۴ برابری فلیپ‌فلاپ‌ها قابل توجیه است.

در آخرین ستون نرخ داده در این روش‌ها مورد بررسی قرار گرفته است. با توجه به منطق دو فازی تمام این روش‌ها، کاهش نرخ داده به نصف در آنها، کاملاً مورد انتظار است. روش STTL به علت نیاز به تاخیر انتشار سیگنال اعتبار نسبت به سایر سیگنال‌ها، با کاهش حدود یک چهارمی در نرخ داده رو به رو است. لازم به‌ذکر است که منطق SABL به‌علت عدم امکان پیاده‌سازی روی تراشه‌های قابل بازپیکربندی و در نتیجه عدم امکان مقایسه با سایر روش‌ها، در این جدول بررسی نشده است.

۵- نتیجه‌گیری

در این مقاله به بررسی روش‌های مقابله با حملات کانال جانبی پرداخته شده است. در بین انواع مختلف حملات کانال جانبی، حملات توانی از اهمیت ویژه‌ای برخوردار هستند. روش‌های موجود در این حوزه با استفاده از اختفا و یا پوشاندن اطلاعات در تلاش هستند که امکان حملات موفق را کاهش دهند. برای اختفای یا پوشاندن اطلاعات به صورت موثرتر، مسطح کردن توان مصرفی مدار و کاهش وابستگی توان مصرفی مدار به داده‌ی ورودی و یا پردازش‌های میانی ضروری است. روش‌های منطق پویا سعی در کاهش این وابستگی و مسطح کردن توان مصرفی مدار دارند که این روش‌ها در این مقاله مورد بررسی قرار گرفته‌اند. مزایا، معایب و محدودیت‌های هر کدام از این روش‌ها بررسی و با هم مقایسه شده است. بررسی‌ها نشان داده که روش SDDL با ۲۰۰٪ کمترین سربار و روش DWDDL با ۱۱۶۰٪ بیشترین سربار را در پیاده‌سازی دارد.

۶- منابع

[1] M. Tehranipoor and C. eds. Wang, "Introduction to hardware security and trust," Springer Science & Business Media, 2011.

[2] P. Yu and P. Schaumont, "Secure FPGA circuits using controlled placement and routing," in Proceedings of the 5th IEEE/ACM international conference on Hardware/software codesign and system synthesis (ACM), 2007.

[3] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: Dparesistance without routing constraints," in International Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2005.

[4] A. Wild, A. Moradi, and T. Guneysu, "Glifred: Glitch-free duplicationtowards power-equalized circuits on FPGAs," IEEE Transactions on Computers, no. 1, pp. 1–1, 2017.

[5] Z. Chen and Y. Zhou, "Dual-rail random switching logic: a countermeasure to reduce side channel leakage," in International Workshop on Cryptographic Hardware and Embedded Systems, 2006.

[6] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dualrail pre-charge logic," in International Workshop on Cryptographic Hardware and Embedded Systems, pp. 232–241, 2006.

[7] W. He, E. de la Torre, and T. Riesgo, "An interleaved epe-immune PA-DPL structure for resisting concentrated em side channel attacks on FPGA implementation," in International Workshop on Constructive SideChannel Analysis and Secure Design, 2012.

[8] S. Guilley, S. Chaudhuri, L. Sauvage, T. Graba, J.-L. Danger, P. Hoogvorst, V.-N. Vong, and M. Nassar, "Place-and-route impact on the security of DPL designs in FPGAs," in Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust (HOST), 2008.

[9] R. Soares, N. Calazans, V. Lomne, P. Maurine, L. Torres, and M. Robert, "Evaluating the robustness of secure triple track logic through prototyping," in Proceedings of the 21st annual symposium on Integrated circuits and system design (ACM), 2008.

[10] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style mdpl on a prototype chip," in International Workshop on Cryptographic Hardware and Embedded Systems, 2007.

[11] M. Masoumi, A. Dehghan Menshadi, E. Madadi, S. Saee Moghadam, "A New and Efficient Method of Mass Masking and its Resistance Assessment to Power Analysis," Journal of Electronical & Cyber Defence, vol. 6, no. 2, 2018.

[12] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards," in Proceedings of the 28th IEEE European Conference on Solid-State Circuits (ESSCIRC), 2002.

[13] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant asic or FPGA implementation," in Proceedings of IEEE Europe Conference and Exhibition on Design, Automation and Test, vol. 1, pp. 246–251, 2004.

[14] A. Moradi and A. Poschmann, "Lightweight Cryptography and DPA Countermeasures: A Survey," Financial Cryptography and Data Security Lecture Notes in Computer Science, pp. 68–79, 2010.

[15] W. He, A. Otero, E. de la Torre, and T. Riesgo, "Customized and automated routing repair toolset towards side-channel analysis resistant dual rail logic," Microprocessors and Microsystems, vol. 38, no. 8, pp. 899–910, 2014.

[16] R. Velegalati and J.-P. Kaps, "Improving security of SDDL designs through interleaved placement on Xilinx FPGAs," in Proceedings of IEEE International Conference on Field Programmable Logic and Applications (FPL), 2011.

[17] A. Razafindraibe, M. Robert, and P. Maurine, "Improvement of dual rail logic as a countermeasure against DPA," in Proceedings of IEEE IFIP International Conference on Very Large Scale Integration (VLSI-SoC), 2007.

[18] M. Nassar, S. Bhasin, J.-L. Danger, G. Duc, and S. Guilley, "BCDL: a high speed balanced DPL for FPGA with global precharge and no early evaluation," in Proceedings of the Conference on Design, Automation and Test in Europe, 2010.

[19] A. Moradi and V. Immler, "Early propagation and imbalanced routing, how to diminish in FPGAs," in International Workshop on Cryptographic Hardware and Embedded Systems, 2014.

[20] D. Jayasinghe, A. Ignjatovic, J. A. Ambrose, R. Ragel, and S. Parameswaran, "Quadseal: Quadruple algorithmic symmetrizing countermeasure against power based side-channel attacks," in Proceedings of IEEE International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2015.

[21] A. Wild, A. Moradi, and T. Guneysu, "Evaluating the duplication of dual-rail precharge logics on FPGAs," in International Workshop on Constructive Side-Channel Analysis and Secure Design, 2015.

Journal of Electronical & Cyber Defence
Vol. 7, No. 3, 2019, Serial No. 27

Side-Channel Attack Resistance Approaches Through Dynamic Differential Logic

F. Pooyan, S. Bayat-Sarmadi

*Sharif University of Technology

(Received: 03/12/2018, Accepted: 05/03/2019)

ABSTRACT

Cryptographic algorithms have improved in a way that algorithm-level analysis is no longer capable of obtaining their secret key. However, these systems are still vulnerable to side-channel attacks which focus on side-channel information including power consumption and electromagnetic field radiations to achieve the secret key. Dynamic differential logic is one of the most effective countermeasures against power analysis attacks. In this approach, circuit power consumption is made flattened and uncorrelated to the secret data. This paper concentrates on several dynamic differential logic approaches most of which are implemented on reconfigurable circuits, and are claimed to be resistant against side-channel attacks. The methods are explained and compared based on vulnerabilities, overheads and implementation details and limitations. Finally, it is concluded that less vulnerable approaches are designed at the expense of more imposed overhead. Research results show that the SDDL method with %200 and the DWDDL method with %1160 have the lowest and highest overheads respectively. However, the most resistant approach explained here, still faces some limitations in placement and routing which hinder its implementations.

Keywords: Dynamic Differential Logic, Side Channel Attack, Reconfigurable Chips, Information Hiding

* Corresponding Author Email: sbayat@sharif.edu