مقاوم‌سازی الگوریتم‌های رمزنگاری در داخل FPGA به کمک PLL

وحید رشتچی[۱]، دانشیار؛ سید حمیدرضا موسوی[۲]، دانشجوی دکتری

۱ - دانشکده مهندسی برق و کامپیوتر - دانشگاه زنجان - زنجان - ایران – rashtchi@znu.ac.ir
۲ - دانشکده مهندسی برق و کامپیوتر - دانشگاه زنجان - زنجان - ایران – hamidreza@znu.ac.ir

چکیده: امروزه اشتراک اطلاعات در سیستم‌های مخابراتی و کامپیوترها نیازمند امنیت بسیار بالایی است. در این میان، حملات کانال جانبی همواره به‌عنوان یکی از چالش‌های امنیتی در رمزنگاری سیستم‌ها می‌باشد، که برای حمله به ادوات رمزنگاری ازجمله کارت‌های هوشمند بکار می‌رود. در این مقاله هدف ارائه طرح جدیدی برای مقاوم‌سازی الگوریتم‌های رمزنگاری است که به‌صورت سخت‌افزاری در FPGA پیاده شده‌است. اساس این طرح استفاده از حلقه فاز قفل شده PLL در الگوریتم‌های رمزنگاری AES می‌باشد که با به هم‌زدن میزان توان مصرفی و زمان‌های اجرای بخش‌های مختلف الگوریتم، مقاومت الگوریتم‌های رمزنگاری را در برابر حملات توان بالا می‌برد. این روش از دو تکنیک masking و hiding برای حفاظت کلید خصوصی رمزنگاری استفاده می‌کند، طرح پیشنهادی در تکنولوژی TSMC 65nm شبیه‌سازی شده و موفقیت قابل‌توجه نشان داده است، به‌طوری‌که توانسته است در رمزنگاری AES با هزینه سربار ۱۳٪ در فضای اشغالی CMOS و افزایش ۱۵ درصدی توان مصرفی، تنها فرکانس کاری را به اندازه ۲٪ کم کرده و امکان به دست آوردن کلید صحیح برای حمله‌کننده را بسیار سخت نماید. همچنین، روش پیشنهادی بر روی FPGA پیاده‌سازی شده‌است و نتایج رضایت‌بخشی بر روی تعداد قابل قبولی از نمودار توان به‌دست آمده‌است.

واژه‌های کلیدی: استاندارد رمزنگاری پیشرفته (AES)، پردازش توان تفاضلی، اندازه‌گیری توان، آرایه گیت‌های قابل‌برنامه‌ریزی(FPGA)

Countermeasure cryptography algorithm by PLL to FPGA

Vahid Rashtchi[1], Associate Professor; S. Hamidreza Mousavi[2], PhD Student

1- Faculty of Electrical and Computer Engineering, University of Zanjan, Zanjan, Iran, Email: rashtchi@znu.ac.ir
2- Faculty of Electrical and Computer Engineering, University of Zanjan, Zanjan, Iran, Email: hamidreza@znu.ac.ir

Abstract: Now days, sharing data in communication systems and computers require high levels of Information security. Side channel attack is one of the methods which it is applied to attack cryptographic systems such as smart cards. In this paper, a new approach for countermeasuring cryptographic algorithms has been proposed and implemented on FPGA. The scheme is based on using Phase Locked Loop in AES algorithm which by disturbing power consumption pattern and execution time of different rounds, the resistance of the algorithm against power attack has been increased. Masking and hiding technique has been used to protect the encryption key. Overall, the proposed method has been simulated within TSMC 65nm technology platform and outstanding success has been obtained; in applying the technique to AES, the overhead was 13% in CMOS area, 15% in power consumption, 2% decrease in working frequency while finding the key became difficult for attackers. In addition, the proposed method has been implemented on FPGA and satisfactory results have been obtained for an acceptable number of samples of the power trace.

Keywords: Advanced Encryption Standard (AES), Differential Power Analysis (DPA), Power Analysis (PA), power measurement, Field Programmable Gate Array (FPGA).

تاریخ ارسال مقاله: ۱۳۹۶/۰۳/۰۶
تاریخ اصلاح مقاله: ۱۳۹۶/۰۵/۰۸
تاریخ پذیرش مقاله: ۱۳۹۶/۰۷/۱۷
نام نویسنده مسئول: وحید رشتچی
نشانی نویسنده مسئول: ایران - زنجان – کیلومتر ۵ جاده تبریز - دانشگاه زنجان - دانشکده مهندسی برق و کامپیوتر.

۱- مقدمه

در کاربردهای سخت‌افزاری مبتنی بر حفظ و انتقال ایمن اطلاعات، استفاده از سیستم‌های رمزنگاری بسیار زیاد شده‌است. نتیجه پیشرفت‌های امنیتی و نیاز مبرم به آن را می‌توان به شدت در دستگاه‌های امروزی از جمله موبایل، کارت هوشمند، رایانه‌های قابل حمل و سیستم‌های کنترل صنعتی و غیره مشاهده نمود[۳،۲،۱]. با توجه به نیاز بازار به سرعت بالا، امنیت قابل قبول و توان مصرفی کم، محققین روی رمزنگاری‌های سخت‌افزاری تمرکز کرده‌اند. بعد از معرفی تحلیل توان به عنوان ابزاری برای بدست‌آوردن کلید رمزنگاری توسط کوچر در سال ۱۹۹۹ [۴]، حمله‌کنندگان به سیستم‌های رمزنگاری نیز روی حملات کانال‌های جانبی بسیار کار کرده‌اند، به‌طوری‌که در سال‌های اخیر مهم‌ترین تهدید علیه سیستم‌های رمزنگاری سخت‌افزاری، حملات مبتنی بر تحلیل توان شده‌است[۵]. تکنیک‌های SCA، DPA، CPA و تحلیل‌های مختلف توان از دست آوردهای اصلی سال‌های اخیر است[۷-۶]. سادگی و سرعت بالای این روش‌ها علت اصلی استفاده وسیع از این تکنیک‌ها بجای تحلیل‌های ریاضیاتی و تئوری است. با پیشرفت تکنولوژی، استفاده از ادوات رمزنگاری سخت‌افزاری جدید، همراه با تنوع حملات سخت‌افزاری در حال افزایش است[۱۱-۸]. در تحلیل‌های حملات کانال جانبی اساس کار مبتنی بر میزان امواج الکترومغناطیسی، امواج آکوستیک، دما و حرارت و یا توان مصرفی است که از سیستم خارج می‌شود. این پارامترها به‌نحوی وابسته به داده‌های در حال پردازش در داخل تراشه‌ها هستند[۱۳-۱۲].

اندازه‌گیری دقیق این خروجی‌ها، پیداکردن کلید صحیح را ممکن می‌سازد، یکی از مفیدترین مسیرهای نفوذ، اندازه‌گیری توان مصرفی در سخت‌افزار رمزنگاری می‌باشد[۱۴]. در اندازه‌گیری توان باید تمرکز روی توان مصرفی پویا باشد، زیرا توان مصرفی استاتیک اطلاعات چندانی در اختیار حمله‌کننده قرار نمی‌دهد. توان پویا وابستگی مستقیم به تغییر حالات ترانزیستورها دارد، که این امر نقطه قوت حملات کانال جانبی است. تغییر حالات ترانزیستورها اساس عملکرد فاصله همینگ نیز می‌باشد[۱۵] که می‌تواند منجربه یافتن کلید یا زیر کلید صحیح شود. الگوریتم AES که پس از شکسته شدن DES ارائه شد، یکی از الگوریتم‌های بسیار پرسرعت و ایمن می‌باشد که هم‌اکنون نیز بسیار مورد استفاده قرار می‌گیرد. در این الگوریتم برای امنیت بیشتر، طول کلیدها حتی به ۲۵۶ بیت نیز می‌رسد که در این‌صورت تعداد حالات ممکن برای کلید برابر با عدد 2^{256} می‌باشد که این تعداد حالات امکان پیداکردن کلید با سعی و خطا در زمان قابل‌قبول را منتفی می‌کند. بااین‌وجود الگوریتم AES هنوز هم در مقابل حملات توان آسیب‌پذیر است[۱۶]. همه روش‌های موجود به‌نحوی به دنبال به هم‌زدن رابطه میان داده‌های در حال پردازش در داخل سخت‌افزار با توان مصرفی قابل‌مشاهده و اندازه‌گیری می‌باشند. هرکدام از این روش‌ها به نوعی هزینه سرباری شامل هزینه ساخت، فضا یا توان مصرفی و کاهش فرکانس کاری سیستم را به دنبال دارند.

حملاتی همچون SCA، DPA و CPA برای شکست الگوریتم AES در مقالات مختلف بررسی شده‌است[۱۸-۱۷]، که از میان آن‌ها روش DPA و CPA بیشتر از بقیه روش‌ها مورد استفاده قرار گرفته و بررسی شده‌اند که دلیل آن، قدرت بالای این دو روش در شکست الگوریتم‌ها می‌باشد، تاکنون روش‌های بسیار زیادی برای مقابله با این حمله‌گرها توسط متخصصین ارائه شده‌اند، که اکثراً از مقاوم‌سازی‌های مبتنی بر سخت‌افزار هستند. از بین روشهای ارائه‌شده مهم‌ترین آن‌ها در موارد زیر خلاصه شده‌است. روش‌های مقاوم سازی SABL، WDDL، Dual-Rail Logic [۲۱-۱۹] که برای پیاده‌سازی نیاز به سلول کتابخانه جدید دارند. روش‌های مبتنی بر ولتاژ [۲۲] و فرکانس پویا [۲۳] که پیاده‌سازی آنها با استفاده از مدارات جانبی امکان‌پذیر است. روش RSL مبتنی بر استفاده از گیت‌های تصادفی [۲۴] و روش موازی‌کردن و به اشتراک گذاشتن حافظه که پیاده‌سازی آن به‌صورت نرم‌افزاری [۲۵] قابل انجام است. رمزکردن و موازی‌نمودن حافظه[۲۶]، تصادفی‌کردن توان مصرفی با اضافه‌کردن مصرف‌کننده‌های مختلف، منطق مکمل و منطق غیرهم‌زمان [۲۸-۲۷] و روش‌های glitch، hazard[۲۹]، Ring Oscillators [۳۰]، روش‌های مبتنی بر تأخیرهای تصادفی در زمان‌های اجرا[۳۱]، روش 1-of-n مبتنی بر کدکردن داده[۳۲] از دیگر روش‌های ارائه‌شده می‌باشند. متأسفانه اکثر این تکنیک‌ها برای محافظت FPGA ها در عمل ناکارآمد هستند. برای مثال طرح SABL یا Ring Oscillators در FPGA غیر قابل پیاده‌سازی است، یا طرح Dual-Rail Logic درصورت ساخته‌شدن، دو برابر حجم خود الگوریتم اصلی فضا اشغال کرده و توان مصرف می‌کند[۳۳].

اکثر روش‌های فوق به‌جز طرحهای مبتنی بر مقاوم سازی نرم افزاری و ایجاد تأخیر، به‌نحوی نیاز به تغییر در ساختار سخت‌افزاری در لایه CMOS دارند. این کار علاوه بر هزینه بالا گاهی اوقات امکان‌پذیر نمی‌باشد، زیرا ایجاد تغییر در سطح CMOS صرفاً در اختیار شرکت تولیدکننده می‌باشد. همان‌طور که قبلاً نیز گفته شد، امکان پیاده‌سازی اکثر این روش‌ها در FPGA وجود ندارد. برای مثال در FPGA توانایی استفاده از مدارات ترکیبی فیدبک دار وجود ندارد تا پیاده‌سازی رینگ اسیلاتور مبتنی بر گیت NOT با فیدبک مقدور گردد. برای پیاده‌سازی روش RSL حتماً نیاز به تحریک ترانزیستورها می‌باشد که این عمل در تعارض مستقیم با خواص ذاتی FPGA مبنی بر دیجیتال بودن آن است.

اگرچه بر هم‌ریختن رابطه میان توان مصرفی و داده‌ها با استفاده از تزریق نویز در مقالات متعددی[۳۵،۳۴،۲۸،۲۷] مورد بررسی قرار گرفته‌است. ولی استفاده از تغییرات توان مصرفی PLL در ناحیه گذرا به عنوان نویز توان توام با اعمال تاخیرهای تصادفی با استفاده از خروجی PLL در ناحیه گذرا کمتر بررسی شده‌است.

برای پیاده‌سازی PLL در داخل FPGA دو راه کار وجود دارد، یکی استفاده از IP core های قرارگرفته از قبل در تراشه‌های امروزی است، و روش دوم ساخت یک PLL دیجیتال توسط گیتهای منطقی یا کدهای ترتیبی در داخل FPGA است[۳۶]. در این مقاله هر دو تکنیک بررسی شده‌است و طرحی برای پیاده‌سازی PLL با استفاده از گیت‌های ترکیبی و مدارات ترتیبی ارائه شده‌است که می‌تواند مقاومت سیستم در مقابل حملات توان را افزایش دهد. همان‌طور که گفته شد، اساس کلی حملات توان، اندازه‌گیری توان مصرفی و پردازش آن برای کشف ارتباط این توان با مقادیر داخل تراشه در حال پردازش می‌باشد. اصولاً برای اندازه‌گیری توان در حملات توان روشهای مختلفی بکار می‌رود[۳۸-۳۷]. که از بین روشهای موجود دو روش CAD و FPGA Board انتخاب شده‌است.

بخش‌های باقی مانده به‌صورت زیر مرتب شده‌است. رمزنگاری و حملات کانال جانبی در FPGA و الگوریتم AES در بخش ۲ مرور شده‌است، در بخش ۳ روش‌های پیاده‌سازی PLL پیشنهادی و انطباق آن با FPGA بررسی شده‌است و در بخش ۴ طرح کلی مورد آزمایش مطرح و پیاده‌سازی شده‌است. درنهایت در بخش ۵ نتایج حاصل از طرح فوق گزارش گردیده‌است.

۲- تاریخچه

۲-۱- آنالیز رمزنگاری و حملات کانال جانبی

محققین در دو دهه گذشته با بررسی توان مصرفی تراشه‌های در حال رمزنگاری توانستند کلیدهای خصوصی قرارگرفته در تراشه‌های رمز نگاری را خیلی سریعتر از روشهای تئوری به دست بیاورند. در روش تحلیل توان میزان توان مصرفی در زمان پردازش رمزنگاری به دفعات متعدد ذخیره‌شده و از این اصل که در مدارات CMOS وابستگی میزان توان مصرفی را می‌توان طبق رابطه (۱) به داده‌های میانی در حال پردازش مدل کرد، استفاده می‌شود.

$$P_{} \quad (۱)$$

اگر در رابطه فوق P_D توان مصرفی پویا فرض شده‌باشد و C_L ظرفیت خازنی گیت‌ها یا ترانزیستورها و f فرکانس کاری تراشه و V_{PP} ولتاژ تغذیه باشد، می‌توان $P_{(0\to1)}$ را احتمال تغییرات خروجی گیت از ۰ به ۱ در نظر گرفت[39]. یکی از ملزومات اصلی حملاتDPA اندازه‌گیری دقیق توان پویا در تراشه‌ها، هنگام پردازش داده‌ها می‌باشد. در روش DPA برخلاف سایر روش‌ها نیاز چندانی به دانستن جزییات زیاد از نحوه پیاده‌سازی الگوریتم در تراشه نیست، که این امر از نقاط قوت این روش نسبت به سایر روشهای تئوری است.

در سال ۲۰۰۴ اولین حمله کاملاً موفق براساس پردازش تشعشعات الکترومغناطیسی توسط ارس ارائه شد[۱۴]. با گذشت بیش از یک دهه از آن تاریخ و پیشرفت‌های بسیار زیاد در ساخت و استفاده از FPGA ها، استفاده از این قطعه قابل برنامه ریزی بسیار زیاد شده‌است. مهم‌ترین دلیل استفاده از FPGA ها ارزان‌بودن قیمت، قابلیت انعطاف و تغییرپذیری آن در سطح سخت‌افزار می‌باشد، همچنین نحوه استفاده از FPGA نیز به خاطر پیشرفت زبانهای توصیف سخت‌افزار HDL بسیار آسان‌تر شده‌است، به موارد فوق اگر سادگی شبیه‌سازی و سنتز در FPGA اضافه گردد، مشاهده خواهدشد که یکی از بهترین انتخاب‌ها برای ساخت تجهیزات جدید، FPGA ها هستند. امروزه FPGA به‌عنوان یکی از بهترین انتخاب‌ها برای پیاده‌سازی الگوریتم رمزنگاری با سرعت بالا می‌باشد[۴۰] علی‌الخصوص قبل از ساخت تراشه ASIC ، استفاده از FPGA یک کار کاملاً بهینه می‌باشد.

از جمله ویژگی‌های جالب توجه در FPGA برای محققین رمزنگاری، قابلیت به‌روزکردن و تغییردادن برنامه داخل آن به دفعات متعدد و قابلیت اجرای همزمان چند برنامه در FPGA می‌باشد که این امر موجب افزایش سرعت در این ساختار شده‌است. از این قابلیت ذاتی عملکرد موازی چند برنامه در FPGA، علاوه برعاملی برای افزایش سرعت می‌توان به عنوان عامل مقاوم‌سازی در برابر حملات کانال جانبی نیز استفاده کرد به این‌نحو که با موازی‌کردن یک منبع نویز در کنار برنامه اصلی، میزان وابستگی توان پویا به داده‌های در حال رمزنگاری کاهش پیدا می‌کند[۴۱]. از کارهای موفقی که در حمله به FPGA ها صورت گرفته است، می‌توان به گزارشات مختلفی اشاره کرد که در سال‌های اخیر ارائه شده‌است[۴۳-۴۲].

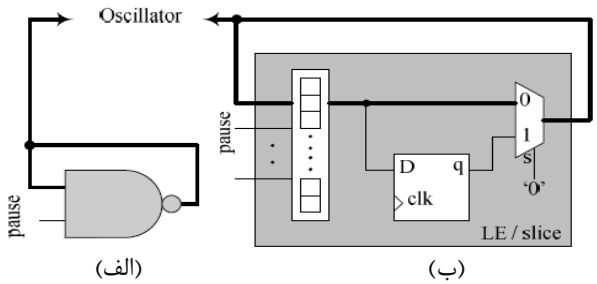
در FPGA ها تغییرات در لایه ترانزیستورها در دسترس کاربران عادی نمی‌باشد، لذا نمی‌توان به‌سادگی روش‌های مقاوم‌سازی در حد CMOS را در آن پیاده کرد[۴۴] مگر شرکت‌های سازنده این FPGA ها همکاری کنند، که این امر درصورت موافقت شرکت سازنده مستلزم هزینه‌های بالا و صرف زمان زیاد است. لذا در FPGA ها روش‌هایی از مقاوم‌سازی موردقبول است که قابلیت پیاده‌سازی توسط کاربران عادی را داشته باشند.

مقاوم‌سازی‌های معمول که روی FPGA انجام شده‌است اصولاً مبتنی بر اضافه‌کردن نویز، تصادفی‌کردن داده‌ها، masking، hiding، ایجاد تأخیر زمانی، تصادفی‌کردن کلاک، پیاده‌سازی پویا و تفاضلی و HDRL، قرار دادن Ring Oscillator ترتیبی در تراشه و ... می‌باشد. هدف اکثر این روش‌ها پیچیده‌کردن توان مصرفی می‌باشد، که این پیچیدگی عامل مقاومت می‌باشد.

روش دیگر برای مقاوم‌سازی در FPGA ها مبتنی بر تولید فرکانس به روش SIRO می‌باشد که در این روش اساس کار استفاده از رینگ اسیلاتور ساخته شده با گیت NAND است.

پیاده‌سازی SIRO در FPGA بسیار ساده است، کافی است از خروجی یک گیت NAND به یکی از ورودیهای آن گیت فیدبک وصل شود، با توجه به این که در مدارات پیاده‌سازی شده در FPGA امکان ساخت حلقه‌های ترکیبی، ساده نمی‌باشد، لذا از مدارات ترتیبی استفاده می‌شود. شکل (۱) هر دو حالت را نشان می‌دهد، لذا می‌توان SIRO را در عمل به‌صورت شکل (۱ب) مشاهده کرد[۴۵].

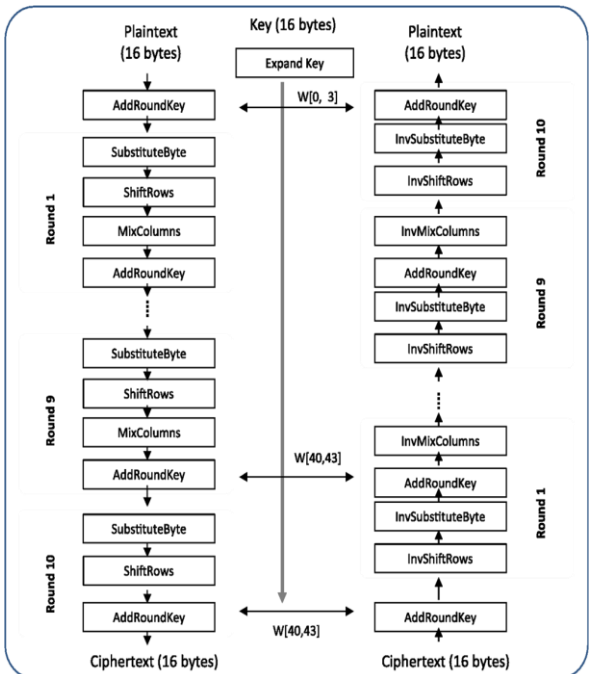
در این ساختار از کلاک خروجی SIRO به عنوان منبع کلاک برای پردازشهای FPGA استفاده شده‌است، با توجه به تصادفی‌بودن فرکانس کلاک سرعت پردازش و تأخیرهای آن، زمان پردازشهای مختلف جابجا شده و در نهایت توان مصرفی وابستگی خود به داده‌های اصلی را تا حدودی از دست می‌دهد.



شکل ۱: رینگ اسیلاتور ساخته شده با گیت NAND : الف)مدارترکیبی مبتنی بر NAND دو پایه. ب) مدار پیاده سازی شده در FPGA

۲-۲- روش عملکرد الگوریتم AES

الگوریتم AES یکی از ایمن‌ترین الگوریتم‌های رمزنگاری متقارن است، طبق فلوچارت کلی این الگوریتم در شکل(۲)، برای هر دو حالت رمزنگاری و رمزگشایی در این الگوریتم چهار بخش اصلی که هرکدام به مشابه یک تابع تبدیل عمل می‌کند، وجود دارد. برای همه سایزهای ممکن برای کلید، چهار تبدیل اصلی (SubByte, ShiftRows, MixColumns, AddRoundKey) حتماً به داده‌ها اعمال می‌شود.



شکل ۲: بلوک دیاگرام کلی رمزنگاری و رمزگشایی در AES [۴۶]

هر چهار بخش مورد اشاره پشت‌سرهم و به‌ترتیب به داده ورودی اعمال می‌شوند. در ادامه هریک از این تبدیل‌ها و نحوه ساخت آن به اختصار توضیح داده شده‌اند.

۲-۲-۱-تابع تبدیل SubByte

این واحد اولین بخش از الگوریتم AES است که با عملکرد غیرخطی خود هر بایت از داده ورودی را به ۸ بیت جدید نسبت داده و مشابه یک جدول جایگشت عمل می‌کند، و همین تغییردادن به اندازه زیادی عملکرد الگوریتم را غیرخطی و پیچیده می‌کند، لازم به ذکر است که همین پیچیدگی به اندازه زیادی مصرف توان در این الگوریتم را نیز افزایش داده‌است. در سایر بخش‌ها (روندها)، اساس کار خطی می‌باشد. یکی از تکنیک‌های حمله‌کنندگان توان برای حملات موفق، جداکردن توان‌های مصرفی در بازه‌های مختلف زمانی می‌باشدکه مختص بخش خاصی از عملکرد الگوریتم باشد. چنانچه کلاک عملکرد سیستم همیشه ثابت باشد به‌سادگی می‌توان بخش SubByte را از سایر بخشها جدا کرده و توان مصرفی در این بخش را مستقلاً تحلیل نمود. روش پیاده‌سازی این بخش چنانچه پیچیده‌تر شود به‌شدت روی سرعت رمزنگاری و رمزگشایی تأثیر گذاشته و سرعت آن را کم می‌کند، لذا نمی‌توان هر طرحی را پیاده کرد.

۲-۲-۲-تابع تبدیل ShiftRows

در این بخش هرکدام از سطرهای جدول داده به سمت چپ شیفت داده می‌شوند، ولی مقدار داده‌ها تغییرنکرده و فقط محل قرارگیری آنها تغییر می‌یابد. چنانچه در این بخش از مدارات ترتیبی استفاده شود، دوباره حمله‌گر می‌تواند از وابستگی توان مصرفی به این تغییرات استفاده کند. روش مرسوم پیاده‌سازی این بخش مبتنی بر آرایش مسیرها می‌باشد به‌طوری که بدون استفاده از هیچ‌گونه گیت منطقی و فقط با استفاده از مسیرهای مبتنی بر سیم(wire) مناسب از محل بیت ورودی به محل بیت خروجی داده‌ها انتقال داده می‌شوند. مزیت این روش کاهش فضای مصرفی در تراشه است، ولی در طرح پیشنهادی این مقاله با قبول هزینه سربار این بخش از مدارات ترتیبی برای پیاده سازی ShiftRows استفاده شده‌است.

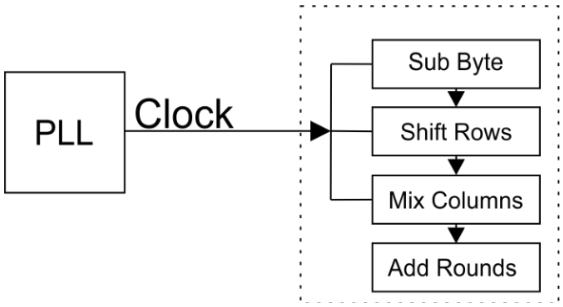
۲-۲-۳- تابع تبدیل MixColumns

در مرحلهMixColumns، چهار بایت از هر ستون جدول state با استفاده از تبدیل خطی معکوس ترکیب می‌شوند. این تابع چهار بایت را به عنوان ورودی در نظر می‌گیرد و چهار بایت را به خروجی تحویل می‌دهد، که با استفاده از ضرب در حوزه گالیوس هر بایت ورودی بر هر چهار بایت خروجی تأثیر می‌گذارد. با اضافه‌شدن این بخش به مرحله ShiftRows آشفتگی زیادی در رمزنگاری فراهم می‌شود این مرحله را نیز با دو روش ترکیبی و ترتیبی می‌توان ساخت که به‌خاطر ایجاد تاخیرهای تصادفی در زمان اجرا روش ترتیبی استفاده شده‌است.

AddRoundKey -۴-۲-۲

آخرین بخش از مراحل چهارگانه AES بخش AddRounKey می‌باشد که با اضافه‌کردن زیرکلیدی از کلید اصلی از دو جهت حائز اهمیت است. اولاً این بخش لحظه ورود کلید به پروسه رمزنگاری می‌باشد، از طرفی عملیات انجام‌شده بسیار ساده بوده و فقط ترکیب داده با کلید توسط یک گیت XOR انجام می‌شود. لذا معلوم‌نبودن زمان شروع این بخش میزان مقاوم‌سازی را تا حد بسیار زیادی بالا می‌برد.

در طرح پیاده‌شده برای مقاوم‌سازی الگوریتم رمزنگاری خروجی PLL در ناحیه گذرا طبق شکل(۳) به تک‌تک بخش‌های اصلی از هر مرحله(روند) متصل شده‌است.



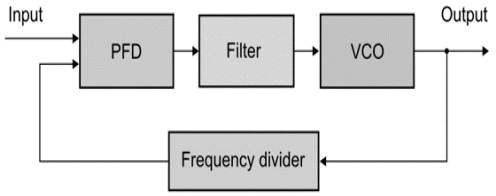
شکل ۳: کنترل زمان اجرای توابع تبدیل با PLL

در طرح فوق دو عامل تاخیرهای تصادفی در آماده شدن خروجی بلوک‌های چهارگانه و مصرف توان توسط بلوک PLL به‌صورت توام اتفاق افتاده است. همان‌طور که در شکل (۳) دیده می‌شود، خروجی PLL به سه بخش اول هر روند اعمال می‌شود، زیرا در بخش AddRounKey عملیات ترکیبی بوده و این بخش با بخش قبلی قابل ترکیب می‌باشد. بدین منظور دو بخش آخر از این چهار بخش با هم دیگر ترکیب می‌شوند.

نتایج حاصل از پیاده‌سازی الگوریتم AES، به‌صورت سخت‌افزاری با زبان توصیف سخت‌افزار (VHDL) در ISE پیاده شده و نتایج حاصل آن توسط ModelSim شبیه‌سازی شده‌است.

۳- ساختار PLL پیشنهادی و انطباق آن با FPGA

یک سیستم حلقه فاز قفل‌شده (PLL) یک سیستم فیدبک‌دار برای تولید کلاک در خروجی می‌باشد، که فاز خروجی می‌بایست منطبق با فاز ورودی باشد. در شکل(۴) نمای ساده‌ای از یک مدار PLL قرار دارد.



شکل ۴: دیاگرام کلی مدار PLL با۴ بخش اصلی

اصولاً در PLL ها چهار بخش عمده وجود دارد:

۱- PFD: مدار تشخیص فاز فرکانس که عملکرد آن تشخیص اختلاف فاز فرکانس خروجی با فاز و فرکانس مرجع است.

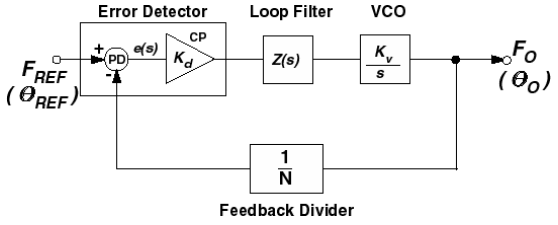
۲- LF: بخشی از مدار که کار آن حذف فرکانس‌های بالای خروجی برای رسیدن به حالت پایداری است.

۳- VCO: یک منبع ولتاژ متناوب متناسب با ولتاژ ورودی است، که قلب PLL نیز می‌باشد.

۴- Divider: نقش آن مقسم فرکانس خروجی برای انتقال و مقایسه با ورودی است.

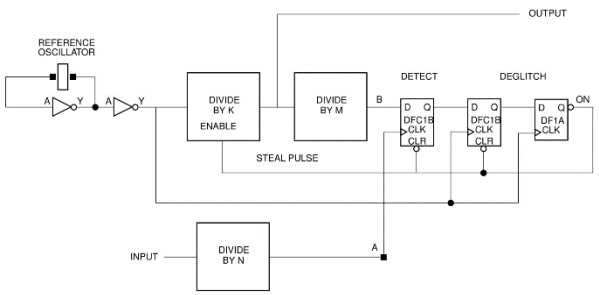
فرکانس خروجی VCO تا زمانی که ولتاژ ورودی آن ثابت است، تغییر نمی‌کند. ولی چنانچه ضریب مقسم یا مرجع مقایسه ورودی تغییر کند، بلافاصله PFD اختلاف را تشخیص داده و VCO را به دنبال خود به تغییر می‌اندازد،که درنهایت پس از گذشت زمان کوتاهی (ناحیه گذرا) دوباره VCO به حالت پایدار می‌رسد، هدف ما در این مقاله استفاده‌کردن از ناحیه گذرا در PLL تا رسیدن به زمان پایداری، برای ایجاد نویز می‌باشد.

PLL ها به صورت عمده در دستگاه‌هایی که نیاز به فرکانس و سرعت بالا با دقت خوب باشد، استفاده می‌شوند که از جمله آن می‌توان به سیستم‌های مخابراتی اشاره کرد، مدار PLL در حالت آنالوگ به‌صورت شکل(۵) می‌باشد که امکان پیاده‌سازی مستقیم آن در FPGA امکان‌پذیر نیست.



شکل ۵: بلوک دیاگرام حالت مدار PLL در مد آنالوگ

در FPGA های امروزی در خانواده Spartan6 تراشه مدل Xilinx-XC6SLX45-2FGG484I چهار عدد CMT وجود دارد و هر کدام شامل یک عدد IP core آماده برای ایجاد PLL است که فرکانس آن تا یک گیگاهرتز می‌تواند افزایش پیدا کند. علاوه بر PLL موجود در FPGA ها می‌توان PLL را به‌صورت نرم‌افزاری و دیجیتال نیز تحت شرایطی پیاده کرد، طرح مورد استفاده در این طرح برای PLL دیجیتال تحت عنوان Pulse Steal PLL به‌صورت بلوک دیاگرام شکل(۶) است.



شکل ۶: دیاگرام مدار[۴۴] Pulse Steal PLL

مدل فوق در مدارات فرکانس بالای دیجیتال در کاربردهای مخابراتی نیز بسیار پرکاربرد است، زیرا در آنجا نیاز ما سنکرون‌شدن با ورودی است[۳۰]، در مدار شکل (۴) فرکانس پالس ورودی بعد از تقسیم‌شدن به N به عنوان فرکانس مرجع استفاده می‌شود و رابطه بین ورودی و فرکانس اسیلاتور برابر با رابطه (۲) است.

$$\frac{(}{k} \quad (۲)$$

با این روش می‌توان فرکانس مرجع را کمی بزرگتر از فرکانس OSC در نظر گرفت. لذا OSC+ باید به‌صورت رابطه (۳) انتخاب شود.

$$\overline{c(} \quad (۳)$$

در این مدار به‌سادگی با تغییر مقدار K و M می‌توان فرکانس خروجی را تغییر داد. این تغییرات به‌صورت آنی نمی‌تواند فرکانس خروجی را تغییر دهد، و خروجی بسته به فرکانس فعلی و مقدار تغییر K و M تأخیر کرده و سپس به ناحیه پایدار می‌رسد. در PLL چنانچه گین حلقه باز بزرگ باشد، سیستم سریع‌تر به پایداری می‌رسد که این امر فقط در حالت آنالوگ امکان‌پذیر است. این روش ساخت PLL در FPGA ها دارای دامنه قفل شدن طبق رابطه (۴) است.

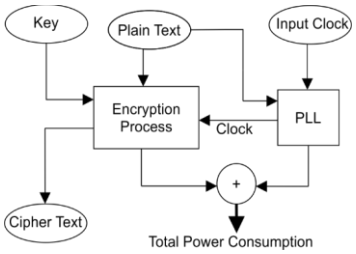
$$L(\quad (۴)$$

در طرح این مقاله فرکانس ورودی به داده‌های در حال رمزنگاری وابسته شده‌است، به‌این‌صورت که مقدار N با توجه به یکی از بایت‌های ورودی به‌صورت تصادفی انتخاب می‌شود. در نتیجه نویز شدیدی از جهت مصرف توان به سیستم در ناحیه گذرا تزریق می‌شود و با تغییر مداوم داده‌های در حال رمزنگاری میزان نویز نیز متفاوت می‌شود، حال از فرکانس خروجی به عنوان فرکانس کاری سیستم استفاده می‌شود، این امر نیز میزان تاخیرهای محاسباتی را تصادفی کرده است. در نهایت این طرح به‌صورت سخت‌افزاری سیستم را در مقابل حملات DPA ایمن کرده‌است.

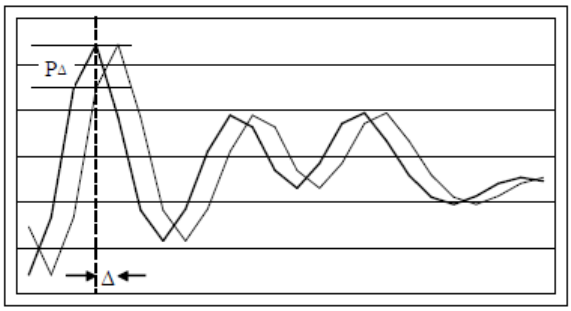
۴ – طرح پیشنهادی

در سیستم‌های رمزنگاری حملات مبتنی بر توان استاتیک کاملاً دفع شده‌اند درحالی که حملات مبتنی بر توان پویا همچنان به عنوان یک چالش برای محققین مطرح می‌شود، در شبیه‌سازی توان، نرم افزار HSPICE و Synopsis- SYSPTPX به‌عنوان دو ابزار قوی، برای تحلیل توان‌های شبیه‌سازی شده در تحلیل حملات تفاضل توان DPA مورد استفاده است[۴۲]. در شکل (۷) طرح کلی مدار پیاده‌سازی‌شده قرار دارد.

در طرح فوق توسط PLL دیجیتال دو عامل ایجاد تأخیر و تزریق نویز توان را توأم انجام می‌شود. ایجاد تأخیر در زمان نشست کلاک‌ها ، اگر محل کلاک‌کاری تراشه را به اندازه Δ جابجا کند(تأخیر دهد) میزان توان مصرفی ناشی از آن کلاک در گیت یا بلوک موردنظر نیز به اندازه Δ جابجا خواهدشد. حال اگر این تغییرات تصادفی باشد، میزان آشفتگی در توان مصرفی بیشتر می‌شود. شکل (۸) این تغییر را نشان می‌دهد، با این جابجایی حمله‌گر به تعداد بیشتری نمونه برای حمله موفق نیاز دارد. روش فوق تحت عنوان، تأخیر تصادفیRDI [۳۱] برای جابجاکردن محل اجرای عملکردهای رمزنگاری است.

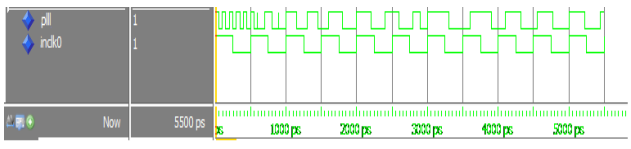


شکل ۷: بلوک دیاگرام کلی سیستم مقاوم شده توسط Digital PLL از نوع Pulse Steal PLL



شکل ۸: جابجایی نمودار توان به اندازه Δ به خاطر RDI [۳۱]

نمودار شبیه‌سازی در شکل(۹) مربوط به خروجی منبع کلاک برای رمز نگاری AES در دوحالت منبع کلاک ساده و منبع کلاک از نوع PLL می‌باشد.



شکل ۹: خروجی منبع کلاک ، نمودار بالا برای حالت PLL در ناحیه گذرا

با ترکیب مدار Digital PLL با مدار رمزنگاری‌کننده، علاوه بر به‌هم‌خوردن میزان مصرف توان، میزان تاخیرها نیز جابجا شده‌است. در این حالت زمان آماده‌شدن داده خروجی کاملاً متفاوت از حالت بدون محافظت می‌باشد. این امر کار حمله‌گر برای پیداکردن محل دقیق پرش‌ها را سخت‌تر می‌کند[۴۳]. در طرح فوق یک بایت از ورودی به‌صورت تصادفی انتخاب‌شده و به‌عنوان ضریب به PLL اعمال می‌شود. لذا در PLL طراحی‌شده دو عامل تصادفی بودن انتخاب ضریب با توجه

به مقدار ورودی و عملکرد ناهمزمانی در خروجی PLL در ناحیه گذرا، که به مراحل مختلف الگوریتم اعمال می‌شود، به شدت میزان وابستگی توان مصرفی به داده‌های در حال رمزنگاری را کم می‌کند.

۵- نتایج شبیه‌سازی و پیاده‌سازی سخت‌افزاری

در این بخش نتایج شبیه‌سازی و پیاده‌سازی سخت‌افزاری طرح پیشنهادی برای مقاوم‌سازی الگوریتم AES در مقابل حملات کانال جانبی به روش DPA ارائه می‌گردد. شبیه‌سازی و پیاده‌سازی‌های سخت‌افزاری برای دوحالت به‌کارگیری PLL آنالوگ بر مبنای IP core و نیز به‌کارگیری PLL دیجیتال پیشنهادی به روش Pulse Steal PLL ارائه خواهدگردید. معیار کلی برای بررسی مقاومت مدارها در برابر حمله DPA میزان جهش نمودار خروجی DPA می‌باشد. اعداد این نمودار میزان همبستگی توانهای دسته‌بندی‌شده روی کلید حدس‌زده‌شده می‌باشد.

۵-۱- نتایج شبیه‌سازی

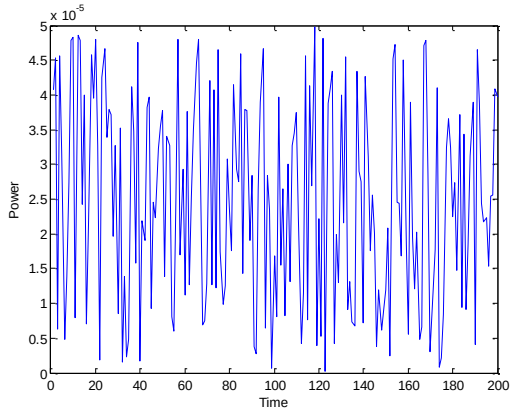
در شبیه‌سازی توان، نرم‌افزار HSPICE و Synopsis- SYSPTPX به عنوان دو ابزار قوی، برای تحلیل توانهای شبیه‌سازی‌شده در تحلیل حملات تفاضل توان DPA مورد استفاده است. برای تائید عملکرد صحیح مدار، طرح در تکنولوژی استاندارد 65nm شبیه‌سازی شده است. دلیل انتخاب این تکنولوژی نزدیکی آن به تکنولوژی ساخت Xilinx XC6SLX45-2FGG484I با 45nm می‌باشد. تعداد نمونه‌ها در حالت شبیه‌سازی ۲۵۰۰۰ نمونه است.

شبیه‌سازی حمله به روش DPA برای بدست‌آوردن یک زیرکلید، برای دوحالت به‌کارگیری طرح PLL آنالوگ و نیز به‌کارگیری PLL دیجیتال پیشنهادی به روش Pulse Steal PLL ارائه‌شده در شکل (۶) انجام شده‌است. نتایج شبیه‌سازی حاصل در شکل‌های (۱۰) و (۱۱) ارائه شده‌است.

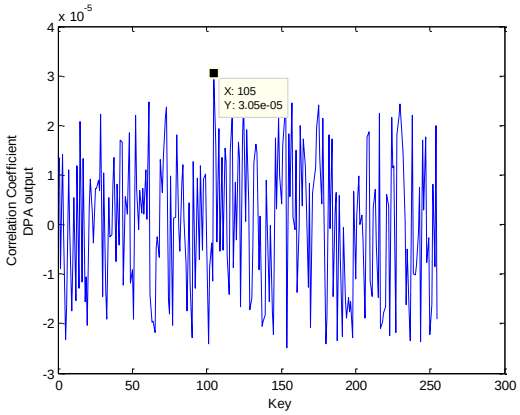
شکل (۱۰) برای شبیه‌سازی حالتی است که طرح PLL آنالوگ مورد استفاده قرار گرفته است. نمودار توان در حال پردازش، در شکل (۱۰ الف) و نمودار خروجی حمله DPA که همان همبستگی نمودارهای توان نمونه گرفته‌شده برای هر کلید حدس‌زده‌شده می‌باشد، در شکل (۱۰ ب) نشان داده شده‌است. با توجه به این که زیرکلید موردنظر برای حدس‌زدن، دارای ۸ بیت می‌باشد لذا در حالت کلی ۲۵۶ حالت برای این زیر کلید متصور است که یکی از آنها صحیح بوده و مابقی اشتباه هستند. نمودار خروجی DPA روی کلید صحیح بیشترین همبستگی را نشان می‌دهد. همان‌گونه که در شکل (۱۰ ب) نشان داده شده‌است حمله‌گر در حالت آنالوگ، موفق عمل کرده و پیک خروجی تحلیل DPA در زیرکلید صحیح 0x6A (عدد ۱۰۵) اتفاق افتاده است.

شکل (۱۱) برای حالتی است که PLL دیجیتال به روش Pulse Steal PLL مورد استفاده قرار گرفته‌است. نمودار توان مصرفی در حال پردازش در شکل (۱۱ الف) و نمودار خروجی حمله DPA در شکل (۱۱ ب) نشان داده شده‌است. همانگونه‌که در این شکل نشان داده شده‌است، سیستم در مقابل حمله با تعداد نمونه‌های موجود کاملاً مقاوم شده است، که دلیل اصلی آن به‌هم‌ریختن رابطه توان و داده‌های میانی به دو دلیل توان مصرفی اضافی و RDI است.

در نمودار (۱۱ ب) بیشترین همبستگی روی کلید ۴۷ می‌باشد که این کلید حدس‌زده‌شده اشتباه می‌باشد.

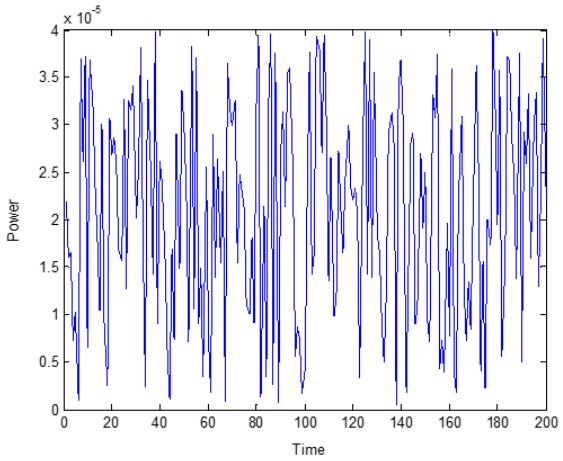


الف) نمودار توان در حال پردازش

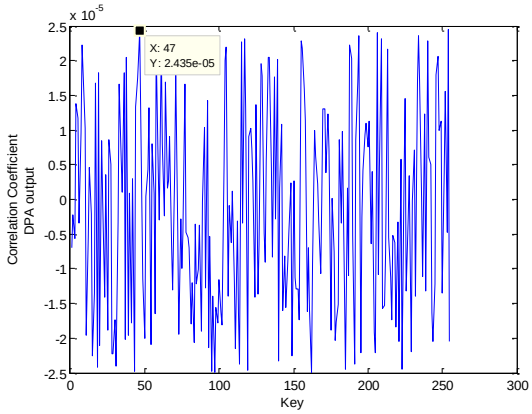


ب) نمودار خروجی حمله DPA

شکل ۱۰: نتایج شبیه‌سازی توان و نمودار خروجی حمله DPA با به‌کارگیری PLL آنالوگ



الف) نمودار توان در حال پردازش

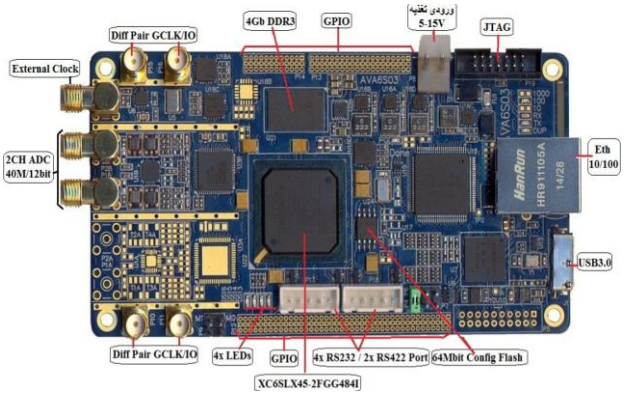


ب) نمودار خروجی حمله DPA

شکل ۱۱: نتایج شبیه‌سازی توان و نمودار خروجی حمله DPA با به‌کارگیری Pulse Steal PLL

۵-۲- نتایج پیاده‌سازی سخت‌افزاری

در طرح فوق سیستم سخت‌افزاری پیاده‌شده، شامل یکی از FPGAهای خانواده‌ی spatran6 تحت عنوان Xilinx XC6SLX45-2FGG484I می‌باشد و پروتکل ارتباطی آن با کامپیوتر usart است. ابتدا الگوریتم AES را با معماری Unrolled – Loop روی FPGA با استفاده از برد شکل (۱۲) پیاده‌سازی شده‌است. هدف این پیاده‌سازی قابلیت تفکیک بخش‌های اجرایی الگوریتم با تقسیم‌بندی زمان می‌باشد. برای اندازه‌گیری توان یک مقاومت ۱۰ اهمی در مسیر تغذیه FPGA قرار داده شده‌است. با توجه به این که در این سیسم، سرعت نمونه‌گیری توان می‌بایستی بیش از فرکانس کاری FPGA باشد لذا سرعت عملکرد FPGA با مقسم فرکانسی کم شده‌است. فرکانس کاری FPGA در طول الگوریتم ۱۵۰KHz می‌باشد. در طول پروسه نمونه‌برداری نمونه‌هایی از توان مصرفی که به خاطر نویزهای غیر قابل پیش‌بینی، جهش بالایی داشته‌اند و مقدار متوسط آنها از متوسط کل نمونه‌ها بیشتر بوده از جدول نمونه‌ها حذف شده‌اند.



شکل ۱۲: برد سخت افزاری شامل Xilinx XC6SLX45-2FGG484I

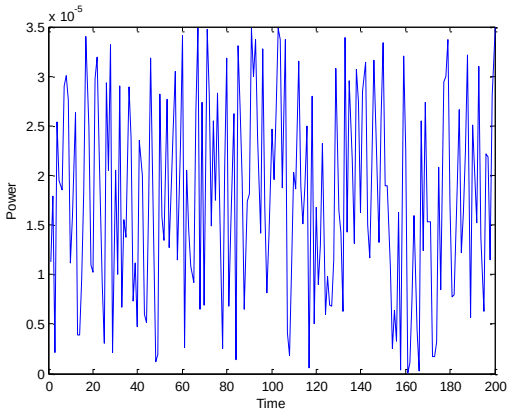
در این مقاله ابتدا الگوریتم بدون هیچ حفاظتی آزمایش شد، سپس برای محافظت از PLL بر مبنای IP core در داخل FPGA استفاده شد و در نهایت طرح PLL نوع دیجیتال پیشنهادی پیاده شده‌است. لازم به ذکر است که برای حمله DPA نمونه‌ها بعد از ضبط و ذخیره به کامپیوتر انتقال داده‌شده و برای تحلیل همبستگی داده‌ها از نرم افزار متلب استفاده گردیده‌است.

در طول زمان حمله سخت‌افزاری، تعداد زیادی نمونه تصادفی برای رمزنگاری و اندازه‌گیری توان نیاز است. با توجه به این که ابزار اندازه‌گیری و ثبت داده‌ها ایده‌آل نیستند، به اجبار تعداد نمونه‌ها را نسبت به حالت شبیه‌سازی، افزایش داده شده‌است. در این‌جا ۳۵۰۰۰ نمونه برای آزمایش حمله تفاضلی، اندازه‌گیری و ضبط می‌شود تا در پردازش بعدی مورد استفاده قرارگیرد. فرکانس نمونه‌برداری ۴۰MHz است. منحنی‌های توان در حال پردازش و خروجی حمله DPA بر روی برد سخت‌افزاری و برای حالتی‌که هیچگونه مقاوم‌سازی صورت نگرفته است در شکل (۱۳) نشان داده شده‌است. طبق شکل (۱۳ الف) میزان توان مصرفی با وجود قابلیت تشخیص محل روندها، الگوی مشخصی ندارد، با این وجود اگر مقاوم‌سازی انجام نشود DPA موفق می‌شود با ۳۵۰۰۰ نمونه به زیرکلید اصلی طبق شکل (۱۳ ب) دسترسی پیدا کند. در حالت اندازه‌گیری توان، میزان نمونه‌ها در هر دوره اندازه‌گیری ۲۰۰ نقطه می‌باشد. همان‌طور که در شکل (۱۳ ب) دیده می‌شود، مقداری جهش حول عدد ۱۰۵ ایجاد شده‌است که نشان از همبستگی بالا در این نقطه نسبت به سایر نقاط دارد. اگرچه دامنه این جهش به نسبت حالت شبیه سازی در مقایسه با نقاط دیگر کمتر است ولی وجود این جهش و همبستگی روی زیرکلید صحیح آسیب‌پذیری الگوریتم محافظت‌نشده را آشکار می‌کند.

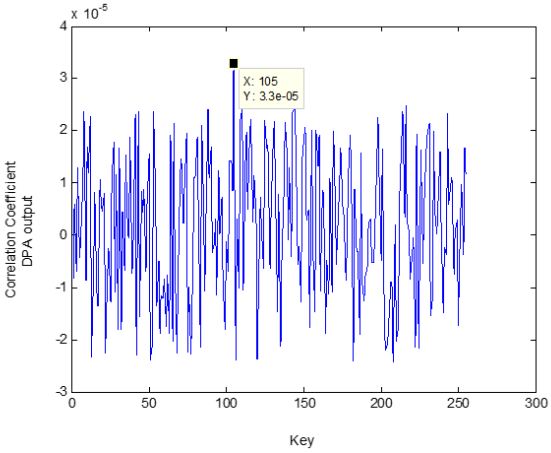
منحنی‌های توان در حال پردازش و نمودار خروجی حمله DPA بر روی برد سخت‌افزاری و برای حالتی‌که مقاوم‌سازی با استفاده از PLL های برمبنای IP core صورت گرفته است در شکل (۱۴) نشان داده شده‌است. در این‌حالت نیز DPA با کمی افزایش تعداد نمونه موفق می‌شود به زیرکلید صحیح دسترسی پیدا کند. طبق شکل (۱۴ الف) میزان توان مصرفی دوباره مشابه حالت قبل الگوی مشخصی ندارد،

هرچند در اینجا نیز دامنه جهش در خروجی DPA به نسبت حالت بدون مقاوم‌سازی، کمتر است ولی دوباره وجود این جهش کم نیز همبستگی بالا در زیرکلید صحیح و آسیب‌پذیری الگوریتم محافظت‌شده با PLL آماده در داخل FPGA را تائید می‌کند.

نتایج پیاده‌سازی برمبنای مقاوم‌سازی با استفاده از Pulse Steal PLL در شکل (۱۵) نشان داده شده‌است. در این‌حالت همانطور که در شکل (۱۵ ب) نشان داده شده‌است، مدار با تعداد نمونه مشابه دو حالت قبل به قدری مقاومت کرده‌است، که حمله‌گر با روش DPA در بدست‌آوردن زیرکلید صحیح با استفاده از نمودار خروجی تحلیل توان موفق نشده‌است. لذا حمله‌گر نتوانسته است به کلید اصلی دسترسی پیدا کند. در نمودار (۱۵ ب) بیشترین همبستگی روی کلید ۱۴۰ می‌باشد که این کلید حدس زده‌شده، اشتباه می‌باشد لذا مقاومت سیستم در برابر حمله DPA مشاهده می‌گردد.

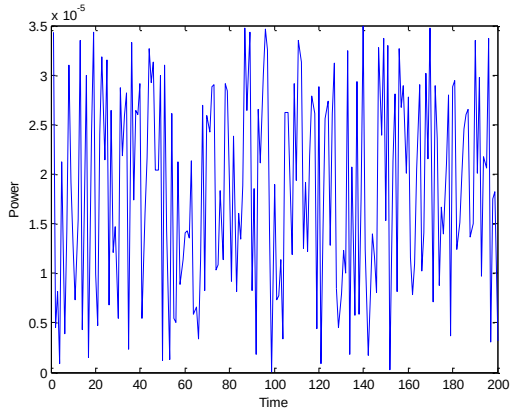


الف) نمودار توان در حال پردازش

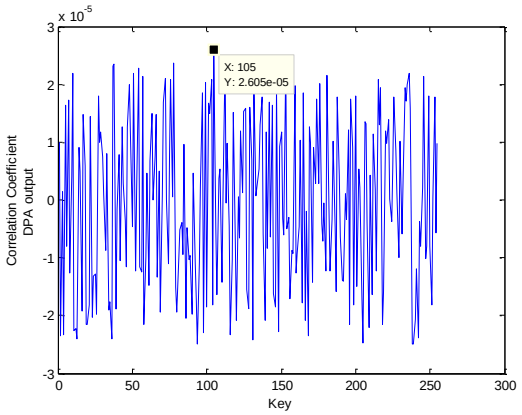


ب) نمودار خروجی حمله DPA

شکل ۱۳: نتایج پیاده‌سازی توان و نمودار خروجی حمله DPA بدون مقاوم‌سازی

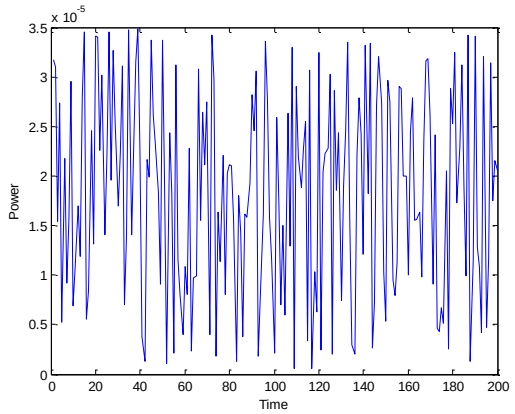


الف) نمودار توان در حال پردازش

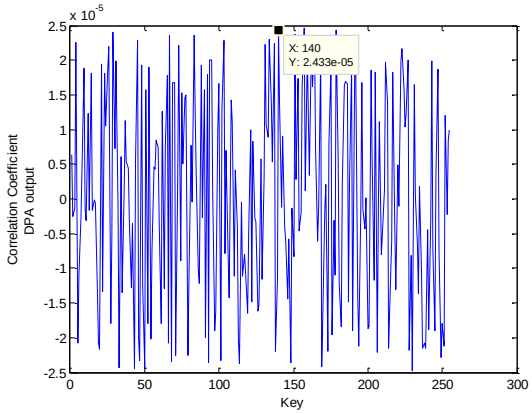


ب) نمودار خروجی حمله DPA

شکل ۱۴: نتایج پیاده‌سازی توان و نمودار خروجی حمله DPA برای مقاوم‌سازی با PLL بر مبنای IP core



الف) نمودار توان در حال پردازش



ب) نمودار خروجی حمله DPA

شکل ۱۵: نتایج پیاده سازی توان و نمودار خروجی حمله DPA برای مقاوم سازی با Pulse Steal PLL

۵-۳- مقایسه با کارهای قبلی

یکی از معیارهایی که برای بررسی توانمندی روشهای مقاوم‌سازی وجود دارد میزان سربار سخت‌افزاری و تحمیل توان اضافی در روش مقاوم‌سازی پیشنهادی می‌باشد. برای بررسی این موضوع سربار سخت‌افزاری و توان مصرفی سه روش پیاده‌سازی شده بر روی برد FPGA در جدول (۱) ارائه گردیده است.

جدول ۱: هزینه سربارشده به سیستم مقاوم و مقایسه با حالت ساده

ردیف	هزینه سربار	حالت ساده بدون مقاوم‌سازی	مقاوم‌سازی با استفاده از PLL داخل FPGA	مقاوم‌سازی با استفاده از طرح PLL دیجیتال با RDI
۱	سلول مصرفی	۱۰۴,۳۲۰	PLL+۱۰۴,۴۸۰	۱۱۸,۳۴۰
۲	توان مصرفی	mw۱۷	mw۱۷,۳	mw۱۹,۳

بر اساس جدول فوق ملاحظه می‌گردد که روش مقاوم‌سازی پیشنهادی که در FPGA پیاده شده‌است، دارای سربار سخت‌افزاری ۱۳ درصد و سربار توان ۱۵ درصد می‌باشد.

جدول ۲: مقایسه و هزینه سربار شده به سیستم با روشهای قبلی

روش پیشنهادی	[۵۲]	[۵۱]	[۵۰]	[۴۹]	[۳۰]	[۴۸]	
65 nm	130 nm	130 nm	65 nm	180 nm	90 nm	40 nm	**تکنولوژی**
Pulse Steal PLL	Duplicated complement	Current equalizer	CP-PLL	WDDL	CBRO	RMTL	**روش**
٪۱۳	٪۱۰۴	٪۲۵	٪۳.۵	٪۲۱۰	٪۱۹	٪۱۰	**هزینه سربار فضای اشغالی**
17mW 19.7mW	گزارش نشده	33.2 mW 44.34 mW	14.5 mW 15.5 mW	54 mW 200 mW	گزارش نشده	گزارش نشده	**توان مصرفی محافظت‌نشده محافظت شده**
٪۱۵	-	٪۳۳	٪۳.۵	٪۲۷۰	-	٪۲۰	**هزینه سربار توان مصرفی**

نتایج مشابه برای دیگر روش‌های مقاوم‌سازی ارائه‌شده براساس تعدادی از کارهای قبلی در جدول (۲) ارائه شده‌است. طرح معروف WDDL [۴۹] با اینکه مقاومت خوبی در مقابل حملات تفاضلی توان دارد ولی به خاطر هزینه بالا در فضای اشغالی از سطح CMOS و توان مصرفی بالا نمی‌تواند روش مورد قبولی در ابزار هوشمند قابل حمل باشد، روش RMTL [۴۸] با اینکه از لحاظ هزینه و توان مصرفی درسطح قابل قبولی قرار دارد ولی به خاطر نوع طراحی نمی‌تواند در FPGA ها بدون تغییر در لایه CMOS کارائی داشته باشد. طرح مشابه دیگر هم اگرچه ازلحاظ توان مصرفی و فضای اشغالی نیاز سیستم را برطرف می‌کند، از لحاظ پیاده‌سازی به خاطر محدودیت‌های ذاتی FPGA قابل استفاده نمی‌باشد. لذا با مقایسه طرح فوق با طرح‌های قبلی در حالت شبیه‌سازی از نظر فضای اشغال‌شده CMOS و توان مصرفی و مقاومتی که در این روش حاصل شده است، این روش می‌تواند روش مقاوم‌سازی قابل قبولی باشد.

۶- نتایج

در این مقاله روش جدیدی برای مقابله با حملات DPA در الگوریتم AES ارائه شد. اساس این روش ترکیب دو ویژگی تغییر در تاخیرها و تزریق نویز توان به سیستم با استفاده از PLL طرح دیجیتال است، که به‌صورت سخت‌افزاری در FPGA پیاده‌سازی شده‌است، مقایسه نتایج در حالت شبیه‌سازی و پیاده‌سازی نشان داد که سیستم در مقابل حملات DPA با تعداد معقولی از نمودار توان، مقاومت خوبی دارد، تنها هزینه سربار سیستم به اندازه افزایش حجم فضای اشغالی به اندازه ۱۳درصد و توان مصرفی ۱۵ درصد است، که نهایتاً فرکانس‌کاری سیستم را به اندازه کمتر از ۲ درصد کم کرده‌است.

قدردانی

برخود واجب می‌دانیم از آقای دکتر معین کیانپور به خاطر کمک‌هایشان در آماده‌سازی بستر پیاده‌سازی و اندازه توان تقدیر و تشکر نماییم.

مراجع

[1] M. Lazzaroni, V. Piuri, and C. Maziero, *Computer security aspects in industrial instrumentation and measurements*, in Proc. IEEE Instrum. Meas. Technol. Conf. (I2MTC), Austin, TX, USA, pp. 1216–1221, 2010.

[2] P. Bilski and W. Winiecki, *Multi-core implementation of the symmetric cryptography algorithms in the measurement system*, Measurement, vol.43, no. 8, pp. 1049–1060, 2010.

[3] P. Bilski, W. Winiecki, and T. Adamski, *Implementation of symmetric cryptography in embedded systems for secure measurement systems*, in Proc. IEEE Instrum. Meas. Technol. Conf. (I2MTC), Warsaw, Poland, pp. 1–6, 2011.

[4] P. Kocher, J. Jaffe, and B. Jun, *Differential power analysis*, in Proc.19th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, pp.388–397, 1999.

[5] Lee, J.W., Chung, S.C., Chang, H.C. and Lee, C.Y., *Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture*, IEEE Transactions on very large scale integration (vlsi) systems, 22(1), pp.49-61, 2014.

[6] E. Brier, C. Clavier, and F. Olivier, *Correlation power analysis with a leakage model*, in Proc. Cryptographic Hardware Embedded Syst.,Cambridge, MA, USA, pp. 16–29, 2004.

[7] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks*, New York,NY, USA: Springer Science Business Media, LLC, 2007.

[8] R. Modugu, Y.-B. Kim, and M. Choi, *Design and performance measurement of efficient IDEA (International Data Encryption Algorithm) crypto-hardware using novel Modular arithmetic*, in Proc. IEEE Instrum. Meas. Technol. Conf. (I2MTC), Austin, TX , USA, pp.1222–1227, 2010.

[9] S. B. Ors, E. Oswald, and B. Preneel, *Power-analysis attacks on an FPGA—First experimental results*, in Proc. Workshop Cryptographic Hardware Embedded Syst., LNCS 2779, pp. 35–50, 2003.

[10] J. Wu, Y. Shi, and M. Choi, *Measurement and evaluation of power analysis attacks on asynchronous S-box*, IEEE Trans. Instrum. Meas.,vol. 61, no. 10, pp.2765–2775, 2012.

[11] K. Tiri and I. Verbauwhede, *A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation*, in Proc. Des., Autom. Test Eur. Conf. Exhib., vol. 1. pp. 246–251, 2004.

[12] S. Mangard, *A simple power-analysis (SPA) attack on implementations of the AES key expansion*, Fifth Int. Conf. Information Security and Cryptology, pp. 343358, November 2002.

[13] R. Bevan and E. Knudsen, *Ways to enhance differential power analysis*,LCNS 2587, pp. 327342, 2003.

[14] Siddika Berna, Ors, Frank K. G, urkaynak, Elisabeth Oswald, and Bart Preneel. *Power-Analysis Attack on an ASIC AES Implementation*. In Proccedings International Conference on Information Technology - ITCC 2004, Las Vegas, USA, Proceedings, 2004.

[15] J. Li, W. Shan, and C. Tian, *Hamming distance model based power analysis for cryptographic algorithms*, in Proc. Int. Conf. Front. Manuf. Des. Sci., Chonqqing, China, pp. 867–871, 2011.

[16] Masoumi, M., Habibi, P., Dehghan, A., Jadidi, M. and Yousefi, L., *Efficient implementation of power analysis attack resistant advanced encryption standard algorithm on side-channel attack standard evaluation board*. International Journal of Internet Technology and Secured Transactions, 6(3), pp.203-218, 2016.

[17] E. Brier, C. Clavier, F. Olivier, "Correlation Power Analysis with a Leakage Model", *Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '04)*, pp. 16-29, 2004.

[18] T.S. Messerges. *Using second-order power analysis to attack DPA resistant software*. In Cryptographic Hardware and Embedded Systems — CHES 2000 LNCS 1965, pp. 238–252, Springer-Verlag, 2000.

[19] D. Sokolov, J. P. Murphy, A. Bystrov, and A. Yakovlev, *Improving the security of dual-rail circuits*, in Proc. Workshop CHES, Cambridge,MA, USA, pp. 282–297, 2004.

[20] S. Guiley, S. L. Sauvage, P. Hoogvorst, R. Pacalet, G. M. Bertoni, and S.Chaudhuri, *Security evaluation of WDDL and seclib countermeasures against power attacks*, IEEE Trans. Comput., vol. 57, pp. 1482–1497, 2008.

[21] D. Hwang, K. Tiri, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, *AES-based security coprocessor IC in 0.18μm CMOS with resistance to differential power analysis side-channel attacks*, IEEE J. Solid-State Circuits, vol. 41, no. 4, pp. 781-792, Apr. 2006.

[22] T.S. Messerges, E. Dabbish, and R. Sloan, Investigations of Power Analysis Attacks on Smartcards, Proc. USENIX Workshop Smartcard Technology, pp. 151-161, 1999.

[23] S. Yang, W. Wolf, N. Vijaykrishnan, D.N. Serpanos, Y. Xie, *Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach*, in Design, Automation and Test in Europe DATE 2005 (IEEE Computer Society, Los Alamitos), pp. 64–69, 2005.

[24] Daisuke Suzuki, Minoru Saeki, and Tetsuya Ichikawa. *Random Switching Logic: A Countermeasure against DPA based on Transition robability*. Cryptology ePrint Archive (http://eprint.iacr.org), Report 2004/346, 2004.

[25] Gülmezoğlu B, Inci MS, Irazoqui G, Eisenbarth T, Sunar B. *A faster and more realistic flush+ reload attack on AES*. InInternational Workshop on Constructive Side-Channel Analysis and Secure Design, pp.111-126, Springer International Publishing, 2015.

[26] Gülmezoğlu, B., Inci, M.S., Irazoqui, G., Eisenbarth, T. and Sunar, B., *A faster and more realistic flush+ reload attack on AES*. In International Workshop on Constructive Side-Channel Analysis and Secure Design (pp. 111-126). Springer International Publishing, 2015.

[27] J. J. A. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor, *Security Evaluation of Asynchronous Circuits*, Proc. International Workshop on Cryptographic Hardware and Embedded Systems, pp. 125-136, 2003.

[28] K. Tiri, D. Hwang, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, *Prototype IC with WDDL and differential routing-DPA sesistance assessment*, Proc. International Workshop on Cryptographic Hardware and Embedded Systems, pp. 354-365, 2005.

[29] Mangard, S., Oswald, E., Popp, T.: *Power analysis attacks: revealing the secrets of smart cards*. Springer, New York . ISBN: 978-0-387-30857-9, 2007.

[30] Liu PC, Chang HC, Lee CY. *A low overhead DPA countermeasure circuit based on ring oscillators.* IEEE Transactions on Circuits and Systems II: Express Briefs. Jul;57(7):546-50, 2010.

[31] Lu, Y., O'Neill, M.P. and McCanny, J.V., 2008, December. F*PGA implementation and analysis of random delay insertion countermeasure against DPA.* In ICECE Technology, 2008. FPT. International Conference on (pp. 201-208). IEEE, 2008.

[32] Moore, S., Anderson, R., Cunningham, P., Mullins, R. and Taylor, G., *Improving smart card security using self-timed circuits*. In Asynchronous Circuits and Systems, 2002. Proceedings. Eighth International Symposium on (pp. 211-218). IEEE, 2002.

[33] K. Tiri, and I. Verbauwhede, *Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology*, Proc. International Workshop on Cryptographic Hardware and Embedded Systems, pp.125-136, 2003.

[34] Standaert, F.X., Rouvroy, G. and Quisquater, J.J., 2006, August. *FPGA implementations of the DES and Triple-DES masked against power analysis attacks*. In Field Programmable Logic and Applications, FPL'06. International Conference on (pp. 1-4). IEEE, 2006.

[35] Johnson, A.P., Chakraborty, R.S. and Mukhopadhyay, D., October. *A Novel Attack on a FPGA based True Random Number Generator*. In Proceedings of the WESS'15: Workshop on Embedded Systems Security (p. 6). ACM, 2015.

[36] Trimberger SM, editor. *Field-programmable gate array technology*. Springer Science & Business Media; 2012 Dec 6.

[37] Synopsys. Inc., PrimeTime®PX User Guide Version E-2010.12, Mar. 2011.

[38] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Tri filetti, *Effectiveness of leakage power an alysis attacks on DPA resistant logic styles under process variations*, IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 61, no. 2, pp. 429–442, Feb. 2014.

[۳۹] محمد آسیایی، « دومینو مبتنی بر مقایسه جریان ارتقاءیافته برای طراحی گیت‌های عریض توان پایین،» مجله مهندسی برق دانشگاه تبریز، دوره ۴۷، شماره ۱ ،صفحه ۱-۱۰ ،۱۳۹۶

[۴۰] پرهام درّی، علی قیاسیان، حسین سعیدی، « طراحی و پیاده‌سازی رمزنگار AES در بستر FPGA برای خطوط پرسرعت،» مجله مهندسی برق دانشگاه تبریز، دوره ۴۶، شماره ۱ ،صفحه ۱۵۳-۱۶۷، ۱۳۹۵

[41] S. Bongiovanni, F. Centurelli, G. Scotti, and A. Trifiletti. *Design and vali-dation through a frequency-based metric of a new countermeasure to pro-tect nanometer ICs from Side-Channel Attacks*. Journal of CryptographicEngineering, 5(4):269–288, 2015.

[42] U. R¨uhrmair, X. Xu, J. S¨olter, A. Mahmoud, M. Majzoobi, F. Koushanfar, and W. P. Burleson. *Efficient power and timing side channels for physical unclonable functions*. In 16th

[48] Avital M, Dagan H, Keren O, Fish A. *Randomized multitopology logic against differential power analysis*. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. Apr;23(4):702-11, 2015.

[49] D. Hwang, et al., *AES-based Security Coprocessor IC in 0.18 µm CMOS with Resistance to Differential Power Analysis Side-Channel Attacks*, J. Solid State Circuits, vol. 41, pp. 781-792, Apr. 2006.

[50] Attaran, A. and Mirhassani, M., 2015, July. *An embedded low-overhead PLL-based countermeasure against DPA side channel attack. In Signals*, Circuits and Systems (ISSCS), International Symposium on (pp. 1-4). IEEE, 2015.

[51] C. Tokunaga, D. Blaauw, *Secure AES engine with a local switched-capacitor current equalizer*, In Proceedings of ISSCC Dig. Tech. Papers, pp. 274-275, Feb. 2009.

[52] M. Doulcier-Verdier, et al., *A side-channel and fault-attack resistant AES circuit working on duplicated complemented values*, In Proceedings of ISSCC Dig. Tech. Papers, pp. 274-275, Feb. 2011.

International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2014) , pages 476–492, 2014.

[43] A. Moradi, D. Oswald, C. Paar, andP. Swierczynski, *Side channel attacks on thebitstream encryption mechanism of AlteraStratix II*, inProc. ACM/SIGDA Int. Symp.Field-Programm. Gate Arrays, pp. 91–100, 2013.

[44] D. Suzuki et al., *Fabrication of a 3000-6-input-LUTs embedded and block-level power-gated nonvolatile FPGA chip using p-MTJ-based logic-in-memory structure*, Proc. Symp. VLSI Circuits, pp. C172-C173, 2015.

[45] Y. Zafar and A. Ahmed, *A Novel FPGA Compliant Micropipeline*, IEEE Transactions on Circuits and Systems -II: Express Briefs, vol. 52, no. 9, pp. 611-615, September 2005.

[46] M. Khalil, and M. Hani, *Verilog Design of a 256-Bit AES Crypto Processor Core*, Universiti Teknologi Malaysia, Faculty of Electrical Engineering, 2007.

[47] Trimberger SM, editor. *Field-programmable gate array technology*. Springer Science & Business Media; 2012 Dec 6.