فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Summer 2022, 3(2), 39-50
DOR: 20.1001.1.27832570.1401.3.2.5.5

Received: 10 Apr 2022
Accepted: 01 June 2022

مقاله پژوهشی

A New Method in the Security of Encryption Systems by Unbalanced Gates

Seyyed Hamidreza Mousavi[1*], Mehdi Safaeian[2], Amir Hassan Ahmadi Ghaleh[3]

1.Assistant Professor, Faculty of Electrical and Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran. *(Corresponding Author)* hamidrezaznu@gmail.com
2. Assistant Professor, Faculty of Electrical and Computer Engineering, Hidaj Branch, Islamic Azad University, Zanjan, Iran. mehdi.safaeian@iau.ac.ir
3. MSc.Student, Department of Computer and Electrical Eng., Zanjan Branch, Islamic Azad University, Zanjan, Iran

Abstract

Introduction: Nowadays, sharing information in communication systems and computers demands high levels of security. Side channel attacks are mainly considered as a main challenge in cryptographic systems which they are used as attacking techniques to break encrypted devices such as smart cards. The purpose of this research is introducing a new plan for strengthening on-chip encryption algorithms. The proposed plan is based on using Phase-Locked Loop (PLL) and enhanced XOR gate in Advanced Encryption Standard (AES) algorithm. In this approach, by disturbing the power consumption and time of execution for each different round of the algorithm, the encryption algorithm is protected against Differential Power Attacks (DPA). The proposed method has been implemented in TSMC 65nm technology in Cadence and the results show that the algorithm becomes immune against DPA using this method. As overheads, the silicon area and power consumption increased about 33% and 25%, respectively, whereas, the clock rate has been reduced less than 3%.

Method: In modern digital systems, if the data in the systems carries classified information, data encryption is unavoidable. For example, encryption in smart cards, portable electronic devices, mobile phones and remote control devices use encryption systems to deal with unauthorized intruders [1][2]. One of the requirements of today's electronic systems is high speed, low power consumption and information security. The basis of this method is the combination of the two characteristics of delay and power noise injection into the system using gates.

Results: The comparison of the results in the simulation mode showed that the system has a good resistance against DPA attacks.One of the characteristics that exist to check the ability of retrofitting methods is the amount of hardware overhead and the imposition of additional power in the proposed retrofitting method. To check this issue, the hardware overhead and power consumption of the implemented method are presented in Table (2).

Discussion: With a reasonable number of power diagrams, so that compared to In the previous designs, the number of power diagrams has been almost doubled and the only overhead cost of the system is the increase in the volume of the occupied space by 33% and the power consumption by 20%.

Keywords: Advanced Encryption Standard (AES), Differential Power Analysis (DPA), Power Measurement, Phase Locked Loop (PLL), XOR.

فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

روش جدید در امنیّت سیستم‌های رمزنگاری توسط گیت‌های نامتوازن

تاریخ دریافت: ۱۴۰۱/۰۱/۲۱ دوره سوم، تابستان ۱۴۰۱
تاریخ پذیرش: ۱۴۰۱/۰۳/۱۱ شمارهٔ دوم ، صص: ۳۹-۵۰

سید حمیدرضا موسوی[1*]، مهدی صفائیان[2]، امیر حسن احمدی قلعه[3]

۱. استادیار، دانشکده مهندسی برق و کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران. (نویسندهٔ مسئول)
hamidrezaznu@gmail.com
۲. استادیار، دانشکده مهندسی برق و کامپیوتر، واحد هیدج، دانشگاه آزاد اسلامی، زنجان، ایران. mehdi.safaeian@iau.ac.ir
۳. دانش آموخته کارشناسی ارشد، گروه برق، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران

چکیده: امروزه اشتراک اطلاعات و انتقال ایمن آن بین سیستم‌های مختلف الکترونیکی ضروری شده‌است. یکی از چالش‌های مهم در این زمینه حملات کانال جانبی می‌باشد که با استفاده از تکنیک‌های موجود سعی در به‌دست‌آوردن کلید رمزنگاری دارند. هدف از این پژوهش ارائه طرح جدیدی برای مقاوم‌سازی الگوریتم‌های رمزنگاری می‌باشد. در این طرح با به‌هم‌زدن توان مصرفی توسط دو عامل ارتقاء گیت‌های کلیدی و تزریق تصادفی تأخیر در اجرای بخش‌های مختلف از الگوریتم استاندارد رمزنگاری پیشرفته AES، میزان مقاومت این سامانه در مقابل حملات تفاضلی توان DPA افزایش‌یافته‌است. برای اصلاح گیت XOR از مدلی استفاده شده‌است که با وجود توان متغیر در زمان‌های مختلف عملکردی ثابت و منطقی دارد. ترکیب گیت فوق با تأخیرهای تصادفی که توسط PLL در ناحیه گذرا ساخته‌می‌شود، مقاومت سیستم را بیشتر بهبوددادهاست. طرح فوق در تکنولوژی nm۶۵ پیاده‌شده و نتایج حاصل از شبیه‌سازی در مقابل حملات تفاضلی توان نتایج قابل‌قبولی را نشان‌داده‌است. این طرح تنها هزینه سربار ۳۳ در صد در فضای اشغالی و ۲۵ در صد در توان مصرفی را به‌دنبال داشته‌است، و تنها سرعت عملکرد ۳ درصد کم‌شده‌است در حالی که مقاومت تقریبا دو برابر شده‌است.

واژه‌های کلیدی: استاندارد رمزنگاری پیشرفته AES، حملات تفاضلی توان DPA، اندازه‌گیری توان، حلقه فاز قفل‌شده، گیت XOR.

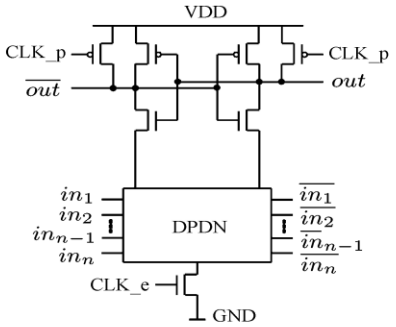
۱. مقدمه

در سیستم‌های نوین دیجیتال اگر داده‌های موجود در سامانه‌ها حامل اطلاعات طبقه‌بندی شده‌باشد، رمزنگاری داده‌ها اجتناب‌ناپذیر است. برای مثال رمزنگاری در کارت‌های هوشمند، ادوات الکترونیکی قابل‌حمل، موبایل‌ها و ادوات کنترل از راه دور، برای مقابله با متجاوزین غیرمجاز ازسامانه‌های رمزنگاری استفاده‌می‌کنند[2][1]. یکی از ملزومات سیستم‌های الکترونیکی امروزی سرعت بالا و مصرف توان پایین و امنیت اطلاعات است. برای این منظور محققین بیشتر روی رمزنگاری‌های سخت‌افزاری مطالعات گسترده‌ای انجام‌داده‌اند. از زمانی که پال کوچر در سال1999 بحث حملات مبتنی بر توان مصرفی بر روی تراشه‌ها را مطرح‌کرد[3]، رمزنگاری سخت‌افزاری نیز دچار چالشی اساسی شد، علت این امر در وابستگی مستقیم توان مصرفی تراشه‌ها به مقادیر میانی داده‌های در حال پردازش و کلید رمزنگاری در داخل سیستم بود. تکنیک‌هایی نظیر DPA،CPA وSPA در سال‌های اخیر برای حمله به سیستم‌ها مطرح‌شده‌اند که با استفاده ابزار بسیار ارزان قیمتی برای اندازه‌گیری و تحلیل توان مصرفی می‌توانند کلید رمزنگاری را کشف نمایند[7][6][5]. مزیت عمده روش‌های مبتنی بر توان مصرفی در سرعت بالای این روش ها نسبت به روش‌های مبتنی بر تحلیل محض ریاضیاتی است.

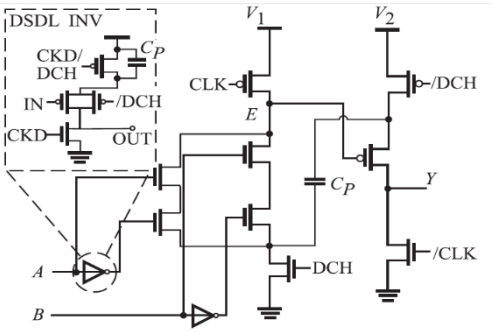
اطلاعاتی که به‌واسطه توان مصرفی از تراشه به بیرون نشت‌می‌کنند مستقیماً به داده‌های در حال پردازش وابسته است، اندازه‌گیری دقیق و به‌موقع این اطلاعات در پیداکردن کلید به حمله‌کنندگان برای کشف کلید، بسیار کمک‌می‌کند. البته در اندازه‌گیری توان لازم است حمله‌کننده توان دینامیکی سیستم را اندازه‌بگیرد زیرا اطلاعات چندانی در توان استاتیکی وجودندارد. توان دینامیکی به شدت به میزان و تعداد جهش‌های صفر به یک و یک به صفر در خروجی ترانزیستورها وابسته است. این پدیده تحت عنوان فاصله همینگ به عنوان یکی از پایه‌های حملات تفاضلی توان می‌باشد[10]. در روش رمزنگاری AES با این که بیش از ۱۵ سال از ارائه آن می‌گذرد همچنان توسط اکثر سیستم‌های نظامی و غیرنظامی استفاده می شود و در مقابل تمام حملات عمومی مقاوم می‌باشد، یکی از دلایل این مقاومت تعداد بالای بیت‌های کلید در این روش است. در نوعی از AES اندازه کلید ۲۵۶ بیت می‌باشد که برای شکست آن به روش سعی و خطا نیاز به بررسی 2^{256} حالت می‌باشد که چنین کاری در زمان معقول غیرممکن است. با این وجود این الگوریتم در مقابل حملات مبتنی بر توان مصرفی همچنان آسیب‌پذیر است. به همین منظور تعداد زیادی روش برای مقاوم‌سازی این الگوریتم در مقابل حملات توان ارائه شده‌است. در همه روش‌ها هدف سامانه مقاوم‌سازی، به‌هم‌زدن وابستگی توان مصرفی با مقدار داده‌های در حال پردازش در سیستم است[11]. در روش‌های مقاوم سازی پارامترهایی نظیر تعداد نمونه لازم برای شکست، فضای اشغالی، توان مصرفی و کاهش سرعت عملکرد سیستم به عنوان هزینه سربار در نظرگرفته شده و معیار مقایسه قرارمی‌گیرد.

از سال۱۹۹۹ که طرح حملات تفاضلی مطرح‌شد بلافاصله روش‌های متعددی برای حل این معضل توسط محققین مطرح‌شد که هرکدام دارای مزایا و معایب خاص خود بودند. از جمله طرح‌های مطرح‌شده طرح (SABL) [13][12] مبتنی برسیستم اندازه‌گیری توان دینامیکی، روش تفاضلی کردن توان دینامیکی [14] (DDL) روش‌های مبتنی بر تفاضل ساده و پیشرفته [15](WDDL) مبتنی بر تکنیک شارژ و دشارژ خازن است. در این بین بعضی از روش‌ها به‌دنبال ثابت نگه‌داشتن توان و جریان مصرفی بودند که این طرح‌ها نیز به‌خاطر سربار هزینه بالا کمتر مورد استقبال قرارگرفتند، که برای مثال می‌توان به طرح‌های مبتنی بر مدارهای دوگان اشاره‌کرد[15]. تعدادی از روش‌ها نیز مبتنی بر اضافه‌کردن نویز به مدار اصلی می‌باشد که این طرح‌ها نیز دو مشکل اساسی دارند. اولین عیب این روش مصرف توان بالا و دومین مشکل این روش کارایی پایین این روش‌ها در اندازه‌گیری‌های متعدد است، زیرا در روش DPA چنانچه تعداد نمونه‌ها زیاد باشد میزان نویز تزریقی قابل حذف است[18][17]. مدارهای مبتنی بر رینگ اسیلاتورها در این حوزه برای تولید نویز مطرح‌شده‌اند[20]. از بین روش‌های مختلف روش جابجایی توان مصرفی یکی از روش‌های کارا و در عین حال کم هزینه برای مقاوم‌سازی می‌باشد که در این مورد روش‌های تزریق تصادفی زمان و طرح PLL در ناحیه گذرا مؤثر واقع‌شده‌اند [27][19].

با وجود طرح‌های مختلف برای مقاوم سازی به‌نظرمی‌رسد در زمینه مقاوم سازی کمتر به بحث به‌هم‌ریختن رابطه توان مصرفی با داده‌های درحال پردازش توسط تزریق تصادفی تأخیر و تزریق نویز مصرفی پرداخته شده‌است. به‌ویژه در روش رمزنگاری AES به‌خاطر نیاز به سرعت و دقت بالا روش فوق بیشتر می‌تواند مؤثر باشد. برای تزریق تأخیر تصادفی استفاده از روش PLL در ناحیه گذار می‌تواند تاحدود زیادی امنیت سیستم را بالا ببرد، این بهبود امنیت در صورت استفاده از طرح PSPLL کیفیت مطلوب خود را ثابت‌کرده‌است.[۲۷]. همچنین با وجود ارائه روش‌های مقاوم سازی قبلی در سیستم‌های رمزنگاری مبتنی بر سخت‌افزار گیت XOR همواره یکی از نقاط آسیب‌پذیر سامانه‌ها می باشد. علت این امر در کاربرد این گیت در لحظه ورود کلید به سامانه‌های رمزنگاری است. اگرچه برای بهبود گیت XOR روش‌های متعددی پیشنهاد شده‌است ولی کمتر به صورت کامل مقاوم سازی مطلوب حاصل شده‌است. از جمله روش‌هایی که تاکنون در زمینه ارتقاء این گیت ارائه شده‌است می‌توان به مدارات شکل شماره ۱ و ۲ اشاره‌کرد. در مدار شکل ۱ گیت XOR توسط ساختار SABL با دو فاز ساخته‌شده‌است، که این فازها توسط کلاک از هم تمییز داده‌می شوند. روش دوم که در شکل ۲ آمده است، برای بهبود امنیت گیت از دو منبع ولتاژ متفاوت استفاده‌کرده‌است که این امر نیز در مدارات دیجیتال با یک منبع تغذیه امکان‌پذیر نیست.



شکل ۱: گیت XOR با ساختار SABL با دو فاز



شکل 2: گیت XOR با دو منبع ولتاژ

در این مقاله دو روش مقاوم سازی مبتنی بر تزریق تصادفی تأخیر در مراحل مختلف الگوریتم AES و ارتقاء گیت XOR با تئوری RPFL تلفیق شده است. این طرح دو روش ماسک‌گذاری و پنهان‌نگاری را به‌صورت توأم انجام‌داده‌است. در نهایت وابستگی بین توان مصرفی و داده‌های میانی نسبت به کارهای قبلی ارتقاء یافته‌است. نقطه قوت این مقاله ارتقاء امنیت گیت XNOR و پنهان‌کردن زمان عملکرد آن از دید ناظر بیرونی می‌باشد. نتایج حاصل از شبیه سازی‌ها در تکنولوژی 65nm افزایش امنیت و هزینه حمله‌گر تا نزدیک به دو برابر را نشان‌می‌دهد. مقایسه این نتایج با کارهای قبلی بهبود فوق را تائیدکرده‌است. ادامه مقاله به صورت زیر سازماندهی شده‌است: در بخش دو ساختار سیستم رمزنگاری و روش حمله توان برای سامانه AES ارائه‌شده‌است. روش ساخت PLL و گیت ارتقاءیافته در بخش سه و چهار ارائه شده و نتایج نهایی در بخش ۵ گزارش‌شده‌است.

۲. ساختار سیستم رمزنگاری و مقاوم‌سازی

۲/۱. آنالیز رمزنگاری و حملات کانال جانبی

در دو دهه اخیر محققین با بررسی توان مصرفی تراشه رمزنگاری توانسته‌اند بسیار سریعتر از روش‌های تحلیلی ریاضی و تئوری به کلید رمزنگاری دسترسی یابند. برای آنالیز توان باید ابتدا توان مصرفی تراشه اندازه‌گیری‌شود. اساس این حمله مبتنی بر میزان توان مصرفی طبق معادله شماره ۱ می‌باشد.

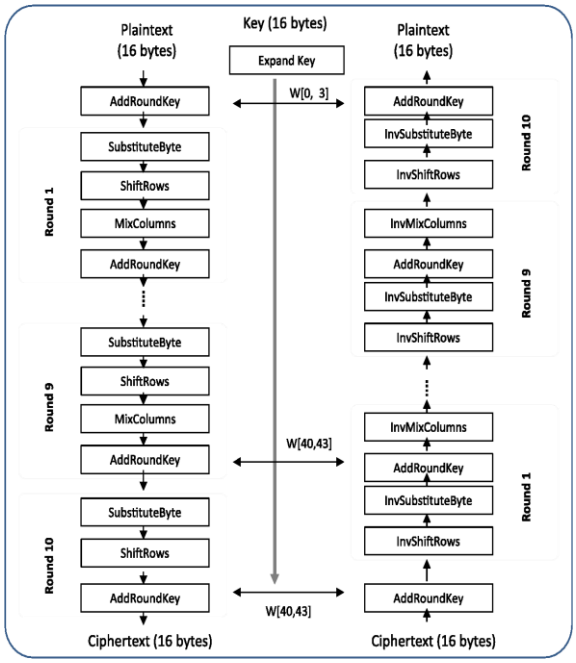
$$P_D = C_L(V_{PP})^2 P_{0\to1} f \quad (1)$$

در معادله فوق PD توان مصرفی دینامیکی، CL مقدار خازن خروجی، f فرکانس کاری و P(0→1) احتمال تغییر مقدار خروجی از ۰ به ۱ است. مهمترین ابزار مورد نیاز روش حمله DPA، ادوات مربوط به اندازه‌گیری توان می‌باشد، که در این ادوات دقت اندازه‌گیری و سرعت آن بسیار حائز اهمیت است[27]. در روش DPA حمله‌گر نیازی به دانستن جزئیات زیاد از نحوه پیاده‌سازی سامانه ندارد و فقط داشتن تعدادی نمونه تصادفی توان و متن داده خروجی متناسب با توان مصرفی کافی است[3]. این ویژگی مهمترین مزیت روش DPA در به‌دست‌آوردن کلید رمزنگاری نسبت به سایر روش‌های موجود می‌باشد.

۲. ۲. رمزنگاری استاندارد پیشرفته

الگوریتم AES یکی از ایمن‌ترین الگوریتم‌های رمزنگاری متقارن است، طبق فلوچارت کلی این الگوریتم در شکل شماره ۳، برای هر دو حالت رمزنگاری و رمزگشایی در این الگوریتم چهار بخش اصلی که هرکدام به‌مثابه یک تابع تبدیل عمل‌می‌کند، وجوددارد. برای همه سایزهای ممکن برای کلید، چهار تبدیل اصلی (SubByte, ShiftRows, MixColumns, AddRoundKey) حتماً به داده‌ها اعمال‌می شود و تفاوت اصلی در تعداد دفعات اعمال این چهار تابع تبدیل است.

هر چهار بخش مورد اشاره پشت‌سرهم و به‌ترتیب به داده ورودی اعمال‌می‌شوند. در ادامه هریک از این تبدیل‌ها و نحوه ساخت آن توضیح داده‌شده‌اند.



شکل ۳: بلوک دیاگرام کلی رمزنگاری و رمزگشایی در AES [۱۹]

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 نسبت‌داده و مشابه یک جدول جایگشت عمل‌می‌کند، و همین تغییردادن به اندازه زیادی عملکرد الگوریتم را غیرخطی و پیچیده‌می‌کند، لازم به ذکر است که همین پیچیدگی به اندازه زیادی مصرف توان در این الگوریتم را نیز افزایش‌داده‌است. 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 جداکرده و توان مصرفی در این بخش را مستقلاً تحلیل‌نمود. روش پیاده‌سازی این بخش چنانچه پیچیده‌تر شود به‌شدت روی سرعت رمزنگاری و رمزگشایی تأثیرگذاشته و سرعت آن را کم‌می‌کند، لذا نمی‌توان هر طرحی را پیاده‌کرد.

۲. ۲. ۲. تابع تبدیل ShiftRows

در این بخش هرکدام از سطرهای جدول داده به سمت چپ شیفت داده‌می‌شوند، ولی مقدار داده‌ها تغییرنکرده و فقط محل قرارگیری آن‌ها تغییرمی‌یابد. چنانچه در این بخش از مدارات ترتیبی استفاده‌شود، دوباره حمله‌گر می‌تواند از وابستگی توان مصرفی به این تغییرات استفاده‌کند. روش مرسوم پیاده سازی 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 می شوند. مزیت این روش کاهش فضای مصرفی در تراشه است، ولی در طرح پیشنهادی این مقاله با قبول هزینه سربار، این بخش با استفاده از مدارات ترتیبی ساخته شده است. وجود مدارات ترتیبی به سامانه مقاوم کننده اجازه جابجایی مکان توان مصرفی را می‌دهد.

۲. ۲. ۳. تابع تبدیل Mix Columns

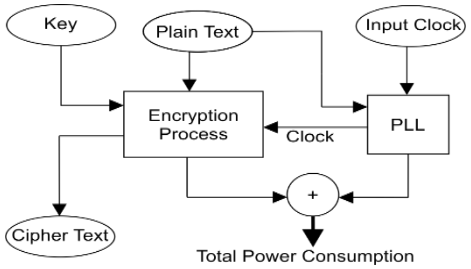
در مرحله Mix Columns، چهار بایت از هر ستون جدول state با استفاده از تبدیل خطی معکوس ترکیب‌می‌شوند. این تابع چهار بایت را به عنوان ورودی درنظرمی‌گیرد و چهار بایت را به خروجی تحویل‌می‌دهد، که با استفاده از ضرب در حوزه گالیوس هر بایت ورودی بر هر چهار بایت خروجی تأثیر می‌گذارد. الین بخش نیز اگرچه خطی است ولی تأثیر به‌سزایی در مصرف توان و شکل ظاهری آن دارد. با اضافه‌شدن این بخش به مرحله ShiftRows آشفتگی زیادی در رمزنگاری فراهم‌می‌شود این مرحله را نیز با دو روش ترکیبی و ترتیبی می‌توان‌ساخت که به‌خاطر ایجاد تأخیرهای تصادفی در زمان اجرا روش ترتیبی استفاده شده‌است.

۲. ۲. ۴. مرحله AddRoundKey

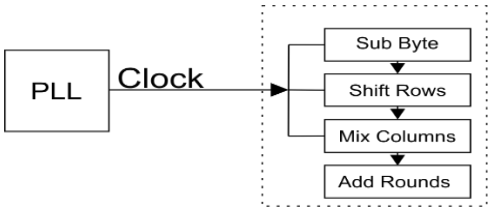
آخرین بخش از مراحل چهارگانه AES بخش AddRounKey می‌باشد که با اضافه‌کردن زیرکلیدی از کلید اصلی از دو جهت حائز اهمیت است. اولا این بخش لحظه ورود کلید به پروسه رمزنگاری می‌باشد، از طرفی عملیات انجام‌شده بسیار ساده بوده و فقط ترکیب داده با کلید توسط یک گیت XOR انجام‌می‌شود. لذا معلوم‌نبودن زمان شروع این بخش میزان مقاوم‌سازی را تا حد بسیار زیادی بالامی‌برد. ذکر این نکته لازم است که مکان عملکرد این بخش را به‌صورت کامل نمی‌توان پنهان‌کرد زیرا اگر حمله‌گر عرض پنجره نمونه‌گی را خیلی بزرگ نماید می‌تواند به زمان اجرای این بخش پی‌ببرد لذا علاوه بر پنهان‌کردن زمان اجرای XOR میزان توان مصرفی آن نیز باید تغییرکند.

۳.استفاده از PLL در به‌هم‌ریختن توان AES

در طرح پیاده‌شده برای مقاوم‌سازی الگوریتم رمزنگاری AES مدار مقاوم‌شده مشابه شکل ۳ پیاده شده است . همان‌طور که در این شکل دیده‌می شود از PLL به عنوان منبع پالس سیستم استفاده‌گردیده‌است خروجی PLL در ناحیه گذرا طبق شکل ۴ به تک‌تک بخش‌های اصلی از هر مرحله(روند) متصل شده‌است.

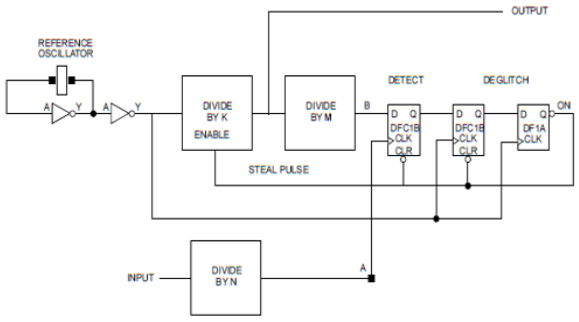


شکل ۴: بلوک دیاگرام سیستم کلی



شکل ۵: بلوک دیاگرام سیستم کلی ایمن‌شده با PLL

با بر سی مدار های متنوع تولید PLL طرحی که در تحقیق برگزیده شد به صورت شکل ۶ می با شد. در این طرح که مبتنی PSPLL می‌با شد میزان تغییرات در ناحیه گذرا کاملاً غیرخطی ا ست و برعکس PLL های معمولی با گذر زمان فاصله از فرکانس مرجع کم نمی‌شود و به صورت غیرخطی به فرکانس مرجع می‌رسد.



شکل ۶: بلوک دیاگرام سیستم PSPLL

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 ۶ فرکانس پالس ورودی بعد از تقسیم‌شدن به N به عنوان فرکانس مرجع استفاده‌می‌شود و رابطه بین ورودی و فرکانس اسیلاتور برابر با رابطه (۲) است.

$$\frac{OSC}{k*M}=\frac{Inpout}{N}=comparison\ ferquancy \qquad (2)$$

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

$$\frac{1}{comparison\ ferquancy}-\frac{k*M}{\text{osc}+}=0.5*(1/OSC) \qquad (3)$$

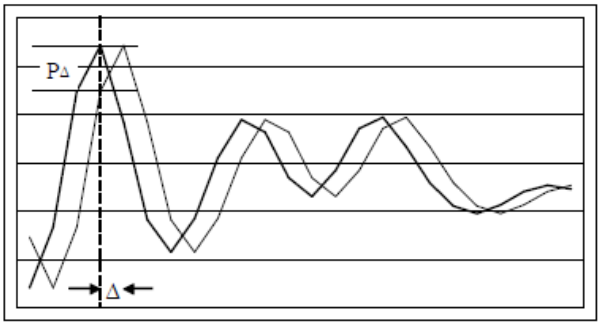
در این مدار به‌سادگی با تغییر مقدار K و M می‌توان فرکانس خروجی را تغییرداد. این تغییرات به‌صورت آنی نمی‌تواند فرکانس خروجی را تغییردهد، و خروجی بسته به فرکانس فعلی و مقدار تغییر K و M تأخیرکرده و سپس به ناحیه پایدار می‌رسد. در PLL چنانچه گین حلقه باز بزرگ باشد، سیستم سریع‌تر به پایداری می‌رسد که این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

$$Lock\ Range = \pm\ (osc+/OSC)/input \qquad (۴)$$

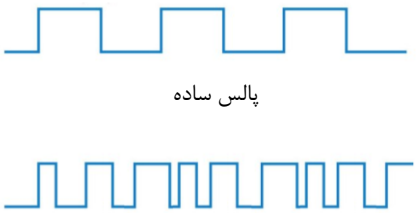
در طرح این مقاله فرکانس ورودی به داده‌های در حال رمزنگاری وابسته شده‌است، به‌این‌صورت که مقدار N با توجه به یکی از بایت‌های ورودی به‌صورت تصادفی انتخاب‌می‌شود. در نتیجه نویز شدیدی از جهت مصرف توان به سیستم در ناحیه گذرا تزریق‌می‌شود و با تغییر مداوم داده‌های در حال رمزنگاری میزان نویز نیز متفاوت‌می‌شود،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

در طرح فوق توسط PLL دیجیتال دو عامل ایجاد تأخیر و تزریق نویز توان را توأم انجام‌می‌شود. 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 ۷ این تغییر را نشان‌می‌دهد، با این جابجایی حمله‌گر به تعداد بیشتری نمونه برای حمله موفق نیاز دارد. برای انجام این پروسه پالس ساده به پالس PWM طبق شکل ۸ تغییریافته‌است. روش فوق تحت عنوان، تأخیر تصادفی RDI [۳۱][27] برای جابجاکردن محل اجرای عملکرد های

رمزنگاری اســـت. با ترکیب مدار Digital PLL با مدار رمزنگاری‌کننده، علاوه بر به‌هم‌خوردن میزان مصـــرف توان، میزان تأخیرها نیز تغییرمی‌کند جابجا شده‌است. در این حالت زمان آماده‌شدن داده خروجی کاملاً متفاوت از حالت بدون محافظت می‌باشـــد. این امر کار حمله‌گر برای پیداکردن محل دقیق عملکردها را ســـخت‌تر می‌کند[۴۳]. در طرح فوق یک بایت از ورودی به صورت تصادفی انتخاب شده و به‌عنوان ضریب به PLL اعمال‌می شود. لذا در PLL طراحی شده دو عامل تصادفی‌بودن انتخاب ضریب با توجه به مقدار ورودی و عملکرد ناهمزمانی در خروجی PLL در ناحیه گذرا، که به مراحل مختلف الگوریتم اعمال‌می‌شـود، به‌شـدت میزان وابســتگی توان مصـرفی به داده‌های در حال رمزنگاری را کم‌می‌کند.



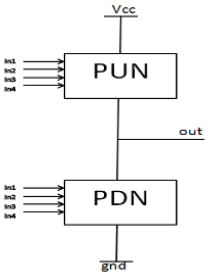
شکل ۷: جابجایی توان به اندازه Δ در ساختار RDI [19]



شکل ۸: پالس خروجی PLL درناحیه گذرا

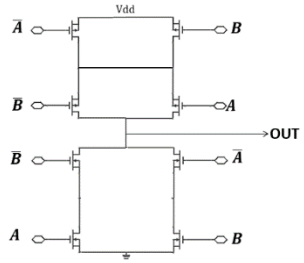
۴. استفاده از گیت ارتقاءیافته

در دنیای CMOS یکی از روش‌های ساخت مدارات به‌صورت شکل ۹ است. در این ساختار که از دو قسمت PUN و PDN تشکیل‌شده‌است، گیت ج در قســـمت بالایی مدار و ترانزیســـتورهای nmos در قســـمت پایینی مدار قرارمی‌گیرند.

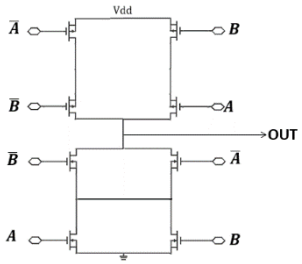


شکل ۹: نمای کلی مدار cmos

برای عملکرد صحیح مدار باید ساختار ترانزیستورهای PUN به‌صورت دوگان PDN باشند. برای مثال ساختار استاندارد گیت XNOR به‌صورت ۹ است. با توجه به ســـاختار اســـتاندارد ابعاد ترانزیســـتورها و نســـبت W/L در آن‌ها تعیین می‌شوند. ساختار دیگری که برای گیت XOR پیشنهاددادهایم شکل 10 می‌باشد که این ساختار را وارون و ساختار استاندارد را ساختار مستقیم می‌نامیم.



شکل۱۰: گیت XNOR در توپولوژی مستقیم



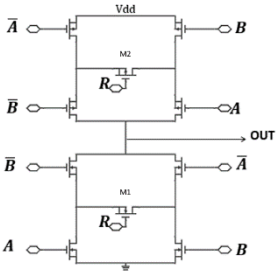
شکل۱۱: گیت XNOR در توپولوژی وارون

تابع بولین هر دو مدار گیت XNOR را تشریح‌می‌کند، که این روابط برای هر دو ساختار مستقیم و وارون به‌ترتیب به‌صورت معادلات ۵ و ۶ است.

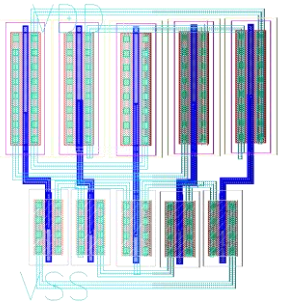
$$OUT = \overline{A\bar{B} + \bar{A}B} \qquad (۵)$$

$$OUT = \overline{(A+B).(\bar{A}+\bar{B})} \qquad (۶)$$
$$= A\bar{B} + \bar{A}B$$

با توجه به برابری دو معادله و طراحی ابعاد ترانزیستور بر پایه مدل استاندارد(مستقیم) اگر از مدل مستقیم به مدل وارن تغییر حالت دهیم به شدت مقدار مقاومت‌ها تغییرمی‌کنند به‌طوری که مقاومت ناشی از بخش PDN که حاصل سری شدن دو مقاومت موازی بودند به حاصل موازی شدن دو مقاومت سری تغییر حالت می‌دهد. مدار شکل ۱۲ برای تغییر حالت بین دو مدل مستقیم و وارون پیشنهاد شده‌است. در این ساختار با قرار گرفتن دو ترانزیستور به عنوان کلید در بخش بالایی و پایینی، مدار اصلاح شده‌است. با تغییر حالت ترازیستور اضافه شده هر دو قسمت مدار تغییر حالت می‌دهند و ساختار ترانزیستورهای اصلی از سری به موازی و از موازی به سری تبدیل‌می‌شوند. حال اگر کنترل ترانزیستور به‌صورت تصادفی باشد تغییر حالات نیز به‌صورت تصادفی می‌شود. برای بررسی بیشتر عملکرد صحیح مدار فوق، لیویت این طرح در تکنولوژی 65nm پیاده‌شده‌است. هزینه سربار ۲۵ در صدی برای فضای اشغالی در شکل ۱۳ مشهود است ولی این هزینه در مقابل بهبود مقاومت کل مدار در مقایسه با سایر روش‌ها قابل صرف‌نظر است.

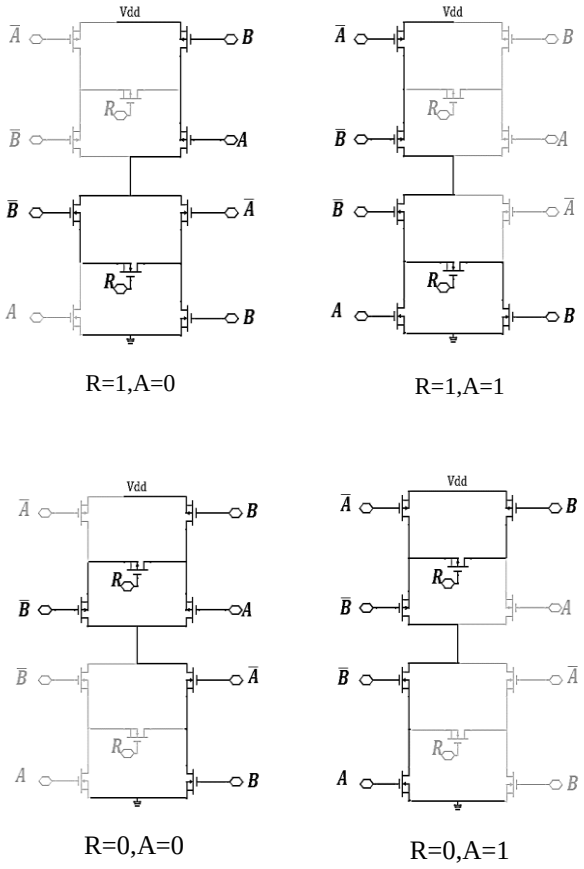


شکل ۱۲: گیت XNOR در توپولوژی وارون و مستقیم با قابلیت انتخاب



شکل ۱۳: گیت XNOR در توپولوژی وارون و مستقیم با قابلیت انتخاب

با توجه به مقدار R برای ترانزیستور اضافه‌شده و مقدار ورودی A می‌توان ۴ حالت مختلف برای توپولوژی فوق را در شکل ۱۳ مشاهده‌کرد، در این اش‌کال ترانزیستورهای کم رنگ با توجه به مقدار R,A در عملکرد مدار شرکت‌نکرده و با کمی تقریب توان چندانی مصرف‌نمی‌کنند. میزان توان مصرفی دینامیک با توجه به تغییر ورودی B از یک به صفر و صفر به یک در شکل ۱۴ آمده‌است.



شکل ۱۴: حالت گیت XNOR با مقادیر مختلف R , A

جدول ۱: مقدار مقاومت کل در گیت XNOR با مقادیر مختلف R , A

	New mode	AOI	OAI
State1 R=0 A=0	2Rnon+2Rntr	3Rnon+2Rntr	3Ron+2Rntr
State2 R=0 A=1	2Rnon+2Rntr	3Rnon+2Rntr	3Rnon+2Rntr
state3 R=1 A=0	2.5Rnon+2Rntr	3Rnon+2Rntr	3Rnon+2Rntr
State4 R=1 A=1	2.5Rnon+2Rntr	3Rnon+2Rntr	3Rnon+2Rntr

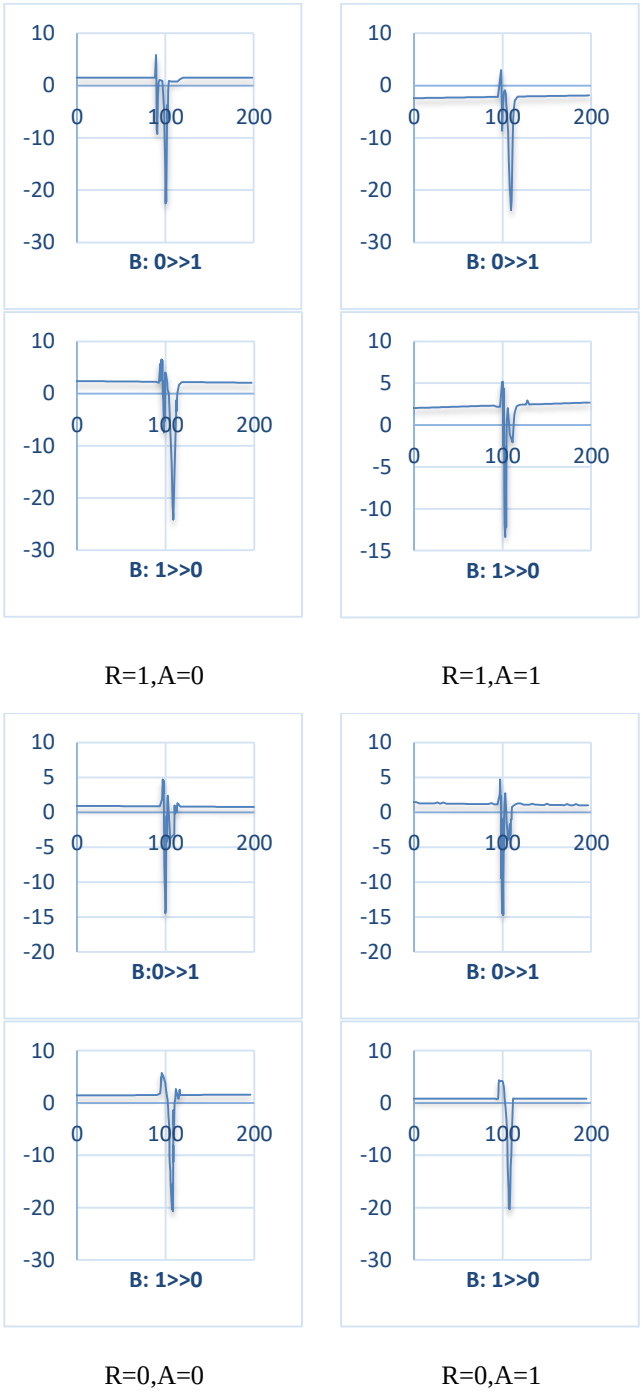
این اختلاف در مقدار مقاومت کل منشأ اصلی اختلاف توان مصرفی در چهار حالت فوق است.

۵. نتایج حاصل از ترکیب PSPLL با گیت ارتقایافته

برای مقاوم سازی نهایی دو عامل PLL و گیت XNOR ارتقاء یافته ترکیب شده است. علت استفاده از PLL به‌هم‌زدن و پنهان‌کردن زمان اجرای بخش‌های مختلف است. اگر این عامل به‌تنهایی استفاده‌شود با بزرگ‌کردن پنجره نمونه‌برداری تاحدودی قابل شکست است، البته هزینه‌های بزرگ کردن پنجره نمونه‌برداری کاملاً رابطه مستقیم با میزان به هم ریخته‌شدن فاصله‌های زمانی دارد. طرح گیت ارتقاءیافته نیز با به‌هم‌زدن توان مصرفی سعی در کم‌کردن رابطه توان مصرفی با داده‌های در حال پردازش را دارد، به‌خصوص مقاوم‌کردن گیت XOR خود گام مثبتی برای بهبود عملکرد کل سیستم است زیرا این گیت دروازه ورود کلید به پرو سه رمزنگاری است. با ترکیب این دو توپولوژی طبق شکل ۳ مقاومت کل در مقابل حملات تفاضلی توان با ۶۰۰۰۰ نمونه مقاوم مانده‌است.

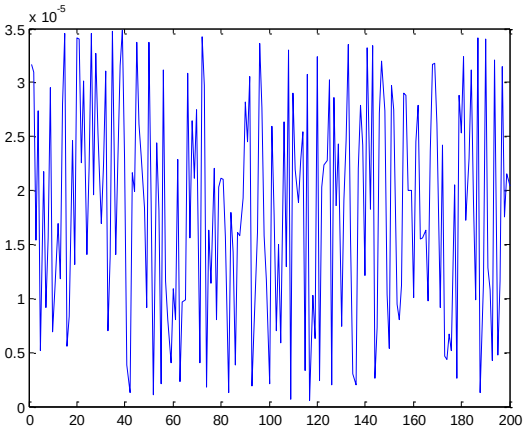
۵. ۱. نتایج شبیه‌سازی

برای شبیه‌سازی توان مصرفی دینامیکی و حملات DPA از ابزار cadence در تکنولوژی 65nm استفاده شده است. ابتدا طرح بدون مقاوم سازی مورد آنالیز قرارگرفت. شکل 16a میزان توان مصرفی یک سامانه غیرایمن را نشان‌می‌دهد تعداد نمونه‌ها ۲۰۰ عدد برای هر نمودار توان است. با اجرای چندین باره الگوریتم به تعداد ۲۰۰۰۰ عدد نمونه توان ذخیره‌می‌کنیم با اجرای حمله DPA بر روی این ۲۰۰۰۰ نمونه آسیب‌پذیری سیستم طبق شکل 16b مشخص‌می شود. زیر کلید رمزنگاری در این آزمایش عدد ۱۰۵ است.

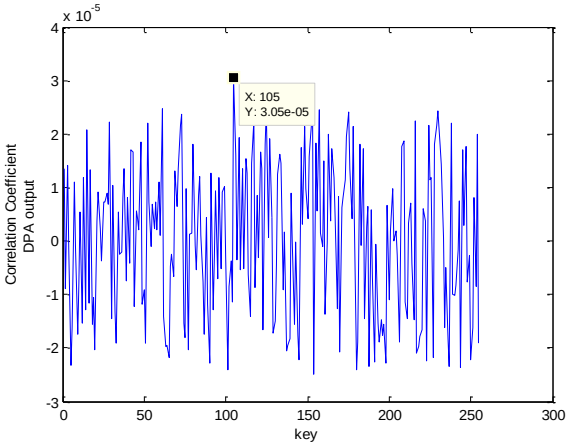


شکل ۱۵: مقادیر مصرف جریان برای حالات گیت XNOR با مقادیر مختلف R , A با تغییر B

یکی از دلایل اختلاف بین توان‌ها مصرفی در اختلاف بین مقاومت‌های موجود در ساختار مختلف ایجادشده‌است. برای ساختارهای شکل ۱۳ میزان مقاومت از VCC تا GND مطابق جدول شماره ۲ است.



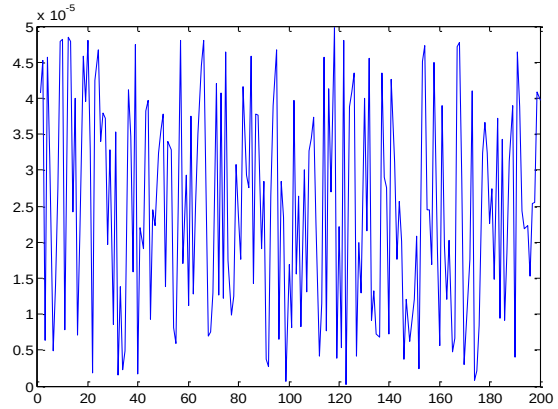
(a):: نمودار توان مصرفی در یک دوره رمزنگاری



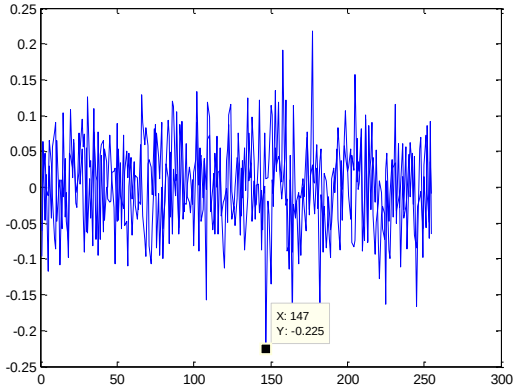
(b):نمودار خروجی DPA برای ۸ بیت اول کلید با ۲۰۰۰۰ نمونه

شکل ۱۶: توان مصرفی و خروجی DPA برای سیستم بدون مقاوم سازی

حال سامانه را توسط دو عامل PLL و گیت ارتقاءیافته به‌صورت توأم مقاوم-می‌کنیم. شکل 17a میزان توان مصرفی در این حالت و شکل 17b نمودار خروجی حمله DPA را نشان‌می‌دهد. همان‌طور که در شکل دیده‌می‌شود سامانه در مقابل حمله توان با تعداد 60000 عدد نمودار هنوز مقاوم است.



(a):نمودار توان مصرفی در یک دوروه رمزنگاری



(b):نمودار خروجی DPA برای ۸ بیت اول کلید با ۶۰۰۰۰ نمونه

شکل ۱۷: توان مصرفی و خروجی DPA برای سیستم با مقاوم سازی

۵. ۲. مقایسه با کارهای قبلی

یکی از معیارهایی که برای بررسی توانمندی روش‌های مقاوم‌سازی وجوددارد میزان سربار سخت‌افزاری و تحمیل توان اضافی در روش مقاوم‌سازی پیشنهادی می‌باشد. برای بررسی این موضوع سربار سخت‌افزاری و توان مصرفی روش پیاده‌سازی‌شده در جدول ۲ ارائه‌گردیده است.

۶. نتیجه‌گیری

در این مقاله روش جدیدی مبتنی بر پنهان‌کاری و ماسک‌گذاری برای مقابله با حملات DPA در الگوریتم AES ارائه‌شد. اساس این روش ترکیب دو ویژگی تغییر در تأخیرها و تزریق نویز توان به سیستم با استفاده گیت ارتقاء یافته‌است، مقایسه نتایج در حالت شبیه‌سازی نشان‌داد که سیستم در مقابل حملات DPA با تعداد معقولی از نمودار توان، مقاومت خوبی دارد به‌طوری که نسبت به طرح‌های قبلی تعداد نمودارهای توان تقریباً دو برابر شده و تنها هزینه سربار سیستم به اندازه افزایش حجم فضای اشغالی به اندازه ۳۳٪ و توان مصرفی ۲۰٪ است.

جدول۲: مقایسه و هزینه سربار شده به سیستم با روش‌های قبلی

compare	Technology	method	design	Area/ Overhead	Power sample need /Improve	Power / Overhead
[28]	130nm	Switched Capacitor	protected	0.44 mm^2 27%	-	44.3 mW / 33%
			Un protected	0.35 mm^2	-	33.3 mW
[20]	90nm	Digital Ring Oscillator	protected	0.10 mm^2 6%	-	7.10 mW / 18.5%
			Un protected	0.09 mm^2	-	5.99 mW
[29]	180nm	WDDL	protected	02.4 mm^2 210%	-	200 mW / 270%
			Un protected	0.79 mm^2	-	54 mW
[30]	65nm	CP-PLL	protected	0.24 mm^2 3.5%	-	15.0 mW / 3.5%
			Un protected	0.24 mm^2	-	14.5 mW
[27]	**65nm**	**Pulse Steal PLL**	**protected**	**0.2 mm^2 25%**	**35000 - 10%**	**19.7 mW / 15%**
			Un protected	**0.24 mm^2**	**32000**	**17 mW**
[25]	**65nm**	**RPFL**	**protected**	**0.25 mm^2 1%**	**40000 - 25%**	**18 mW / 1%**
			Un protected	**0.24 mm^2**	**32000**	**17 mW**
new method	**65nm**	**PSPLL+RPFL**	**protected**	**0.31 mm^2 33%**	**60000 - 95%**	**20 mW / 20%**
			Un protected	**0.24 mm^2**	**32000**	**17 mW**

References

[1] P. Bilski and W. Winiecki, “Multi-core implementation of the symmetric cryptography algorithms in the measurement system,” Meas. J. Int. Meas. Confed., vol. 43, no. 8, pp. 1049–1060, 2010.

[2] I. Hammad, K. El-Sankary, and E. El-Masry, “High-speed AES encryptor with efficient merging techniques,” IEEE Embed. Syst. Lett., vol. 2, no. 3, pp. 67–71, 2010.

[3] P. C. Kocher et al., “Differential Power Analysis,” Journal of Cryptographic Engineering. pp. 1–10, 1999.

[4] J. W. Lee, S. C. Chung, H. C. Chang, and C. Y. Lee, “Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture,” IEEE Trans. Very Large Scale Integr. Syst., vol. 22, no. 1, pp. 49–61, 2014.

[5] Randolph M, Diehl W. Power side-channel attack analysis: A review of 20 years of study for the layman. Cryptography. 2020 Jun;4(2):15.

[6] T. Popp, E. Oswald, and S. Mangard, “Power Analysis Attacks and Countermeasures,” Des. Test Comput. IEEE, vol. 24, no. 6, pp. 535–543, 2007.

[7] U. Rührmair et al., “Efficient Power and Timing Side Channels for Physical Unclonable Functions.” pp. 476–492, 2014.

[8] R. Bevan, E. Knudsen, and B. Bp, “Ways to Enhance Differential Power Analysis,” Icisc 2002, vol. 1, pp. 327–342, 2002.

[9] S. Mangard, “A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion,” Society, vol. 2587, pp. 343–358, 2002.

[10] X. Cui, R. Li, W. Wei, J. Gu, and X. Cui, “AHardware implementation of des with combined countermeasure against DPA,” in Proceedings of International Conference on ASIC, 2013.

[11] M. Masoumi, P. Habibi, A. Dehghan, M. Jadidi, and L. Yousefi, “Efficient implementation of power analysis attack resistant advanced encryption standard algorithm on side-

channel attack standard evaluation board," Int. J. Internet Technol. Secur. Trans., vol. 6, no. 3, p. 203, 2016.
[12] I. Verbauwhede and K. Tiri, "A Dynamic and Differential CMOS Logic with Signal-Independent Power Consumption to Withstand Differential Power Analysis," 2008.
[13] Z. Y. and Z. X. WANG Pengjun, "Design of Two-phase SABL Flip-flop for Resistant DPA Attacks," Chinese J. Electron., vol. 22, no. 4, pp. 833–837, 2013.
[14] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," Proc. - Des. Autom. Test Eur. Conf. Exhib., vol. 1, pp. 246–251, 2004.
[15] K. Tiri, D. Hwang, A. Hodjat, and B.-C. Lai, "Prototype IC with WDDL and differential routing–DPA resistance assessment," Cryptogr. Hardw. Embed. Syst. – CHES 2005, vol. 3659/2005, pp. 354–365, 2005.
[16] T. Popp and S. Mangard, "Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints," pp. 172–186, 2005.
[17] Sim BY, Kwon J, Choi KY, Cho J, Park A, Han DG. Novel side-channel attacks on quasi-cyclic code-based cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems. 2019 Aug 9:180-212.
[18] J. J. A. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor, "Security Evaluation of Asynchronous Circuits," Cryptogr. Hardw. Embed. Syst. - CHES 2003, 2003.
[19] Y. Lu, M. P. O'Neill, and J. V. McCanny, "FPGA implementation and analysis of random delay insertion countermeasure against DPA," Proc. 2008 Int. Conf. Field-Programmable Technol. ICFPT 2008, pp. 201–208, 2008.
[20] C. Y. Liu, P.C., Chang, H.C. and Lee, "A low overhead DPA countermeasure circuit based on ring oscillators," IEEE Trans. Circuits Syst. II, vol. 57, no. 7, pp. 546–550, 2010.
[21] S. M. Trimberger, Field-Programmable Gate Array Technology. 2012.
[22] J. S. and W. Y. TANG Wenyi, "Dual-Voltage Single-Rail Dynamic DPA-Resistant Logic Based on Charge Sharing Mechanism," Chinese J. Electron., vol. 26, no. 5, pp. 899–905, 2017.
[23] Lou X, Zhang T, Jiang J, Zhang Y. A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography. ACM Computing Surveys (CSUR). 2021 Jul 13;54(6):1-37.
[24] U.~Meyer-Bäse, "Coherent Demodulation with {FPGA}s," Lect. Notes Comput. Sci., vol. 1142, pp. 166–175, 1996.
[25] V. Rashtchi and H. Mousavi, "Countermeasure cryptography algorithm by PLL to FPGA," tjee, vol. 3, no. 2, 2017.
[26] Kumar R, Liu X, Suresh V, Krishnamurthy HK, Satpathy S, Anders MA, Kaul H, Ravichandran K, De V, Mathew SK. A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4K crypto-processor in 14-nm CMOS. IEEE Journal of Solid-State Circuits. 2021 Jan 28;56(4):1141-51.
[27] V. Rashtchi and H. Mousavi, "Strengthening AES Encryption Algorithms with an Improved Logic Topology," Majlesi J. Electr. Eng., vol. 6, no. 3, 2018.
[28] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," Dig. Tech. Pap. - IEEE Int. Solid-State Circuits Conf., 2009.
[29] H. Wang, "AES-based security coprocessor IC in 0.18 µm CMOS with resistance to differential power analysis side channel attack," Ieee Jssc, vol. 41, no. 4, pp. 781–791, 2006.
[30] A. Attaran and M. Mirhassani, "An embedded low-overhead PLL-based countermeasure against DPA side channel attack," ISSCS 2015 - Int. Symp. Signals, Circuits Syst., 2015.