مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»
سال ششم، شماره ۴، زمستان ۱۳۹۷؛ ص ۳۲-۲۳

طراحی و تحقق یک مدار مقایسه‌کننده فرکانس مبتنی بر توابع فیزیکی غیرقابل کپی برداری برای محافظت از اصالت سخت‌افزار

اقبال مددی[۱]، مسعود معصومی[۲*]، علی دهقان منشادی[۳]، ابوالفضل چمن‌مطلق[۴]

۱- کارشناس ارشد الکترونیک، ۲- استادیار، دانشکده فنی دانشگاه آزاد واحد اسلامشهر،

۳- کارشناس ارشد مخابرات، ۴- استادیار، دانشگاه ایوانکی

(دریافت: ۱۳۹۶/۰۷/۰۶، پذیرش: ۱۳۹۷/۰۳/۰۶)

چکیده

یکی از چالش‌های مهم در امنیت سخت‌افزار مقابله با کپی‌سازی و استفاده از سخت‌افزارهای جعلی به‌جای سخت‌افزارهای اصلی و واقعی است. در حقیقت هدف این نوع حمله خدشه‌دار کردن اصالت سخت‌افزار است و هدف آن کشف کلید یا پارامترهای حساس ابزار رمز نیست. از این‌رو، برای مقابله با آن باید تمهیدات ویژه و متفاوت با روش‌های متداول محافظت از امنیت الگوریتم‌ها و سامانه‌ها در نظر گرفته شود. یکی از موثرترین روش‌های مقابله با این نوع حملات و محافظت از اصالت سخت‌افزار استفاده از توابع کپی‌ناپذیر فیزیکی یا پاف است. توابع کپی‌ناپذیر فیزیکی را می‌توان برای استخراج پارامترهای مخفی از خصوصیات فیزیکی و ذاتی مدارهای مجتمع مورد استفاده قرار داد. فرآیندهای وابسته پاف‌ها می‌توانند انواع و اقسام داشته باشند اما پاف‌های سیلیکونی که بر مبنای تاخیرها و زمان‌بندی‌های خاص هر فرآیند هستند متداول‌تر هستند. در این مقاله تحقق عملی یک پاف سیلیکونی مبتنی بر نوسان‌ساز حلقوی بر روی تراشه‌های FPGA از خانواده Xilinx گزارش شده است. نتایج پیاده‌سازی نشان داد که با استفاده از پنج نوسان‌ساز حلقوی قادر به ارائه یک کد امنیتی منحصر به‌فرد ۱۰ بیتی با مصرف تقریباً یک درصد از سطح تراشه هدف هستیم ضمن آن‌که با صرف سخت‌افزار بیشتر قادر به دست‌یابی به کدهای طولانی‌تر و امنیت بیشتر هستیم. تمامی شبیه‌سازی‌های انجام شده بر روی یک رایانه قابل حمل با مشخصات پردازنده مرکزی از نوع دو هسته‌ای با فرکانس ۲ GHz و ۴ GB حافظه RAM پیاده‌سازی شده‌اند.

واژه‌های کلیدی: امنیت سخت‌افزار، توابع کپی‌ناپذیر فیزیکی، پیاده‌سازی FPGA

۱- مقدمه

یکی از چالش‌های مهم در مهندسی امنیت سخت‌افزار مقابله با مهندسی معکوس سخت‌افزارها و سامانه‌های امنیتی و اطلاعات تراشه‌ها و نیز استفاده از سخت‌افزارهای جعلی به‌جای سخت‌افزارهای اصلی و واقعی است. در حقیقت هدف این نوع حملات کشف کلید یا پارامترهای حساس ابزار رمز نیست بلکه هدف مهاجم بازیابی یا تغییر اطلاعات ذخیره شده در تراشه‌های سامانه رمز است. از این‌رو برای مقابله با آن باید تمهیدات ویژه و متفاوت با حملات رمزشکنی نرم‌افزاری و متداول در نظر گرفت. تاکنون روش‌های زیادی برای جلوگیری از به‌کارگیری غیر مجاز قطعات نیمه‌هادی ارائه شده است. این روش‌ها شامل استفاده ازسازوکارهای رمزنگاری نظیر الگوریتم‌های رمزنگاری، امضای دیجیتال[۳]، کدکردن داده‌ها و ... هستند. تمامی این روش‌ها مبتنی بر کلیدهای رمزنگاری هستند. این کلیدها دراغلب موارد در حافظه‌های غیرفرار یا فیوزها ذخیره می‌شوند که در معرض حملات مهندسی معکوس بوده و می توان توسط فناوری‌های موجود، اطلاعات درون آنها را خوانده و مورد استفاده قرار داد. از این‌رو برای تامین امنیت سامانه‌ها نمی‌توان تنها به پروتکل‌ها و الگوریتم‌های رمزنگاری متکی بود. روند مقالات و گزارش‌ها به‌روشنی نشان می‌دهد که برای تامین امنیت سازوکارهای محافظت نرم‌افزاری کافی نیستند. در عوض نیازمند روش‌ها و سازوکارهایی هستیم که به‌لحاظ فیزیکی قابل اعتماد بودن و امنیت فیزیکی ابزار امنیتی را تایید کنند. یکی از موثرترین روش‌های پیشنهاد شده برای مقابله با این نوع حملات و محافظت از اصالت سخت‌افزار و سامانه‌های رمز، استفاده از توابع کپی‌ناپذیر فیزیکی[۱] است [۴-۱]. توابع کپی‌ناپذیر فیزیکی یا

*رایانامه نویسنده مسئول: m_masoumi@iiau.ac.ir

پاف‌ها را می‌توان برای استخراج پارامترهای مخفی از خصوصیات فیزیکی مدارهای مجتمع مورد استفاده قرار داد. وقتی این خصوصیت فیزیکی تاخیر یا یک عامل زمانی باشد، این وضعیت شبیه به استخراج مقادیر تصادفی از نویز خواهد بود. یکی از مناسب‌ترین ویژگی‌ها برای شناسایی منحصر به‌فرد مدارهای مجتمع می تواند تغییرات پارامترهای وابسته به فرآیندهای ساخت آنها باشد. در واقع پاف تابعی است که پاسخ آن به هر ورودی، به صورت تکرار ناپذیری به فرآیند ساخت آن وابسته است. فرآیندهای وابسته پاف‌ها می توانند انواع و اقسام داشته باشند که پاف‌های موسوم به پافهای غیر الکترونیکی مانند نوری، اکوستیکی یا صوتی و مغناطیسی از آن جمله هستند اما پاف‌های الکترونیکی و بخصوص پاف‌های سیلیکونی که بر مبنای تاخیرها و زمان‌بندی‌های[1] خاص هر فرآیند هستند متداول‌تر هستند. اکنون کاملا مشخص شده است که زمان‌بندی‌ها و تاخیرهای یک مدار مجتمع از یک بستر[2] بر روی یک ویفر تا یک بستر دیگر بر روی همان ویفر به‌دلیل تغییرات فرایندهای ساخت مانند تأخیر سیم‌ها، سیگنال‌ها و ولتاژ آستانه که در فرآیند ساخت اتفاق می افتد، انحنای ویفر و تغییر می‌کند. از این رو پاف‌ها به‌سادگی قابل ارزیابی[3] ولی به‌سختی قابل پیش‌بینی هستند. علاوه بر آن پاف‌ها به‌سادگی قابل ساخت ولی به‌لحاظ عملی حتی با داشتن دقیق تمام پارامترهای ساخت، غیرقابل کپی‌سازی هستند. اکنون این مساله نیز به‌خوبی مشخص شده است که ولتاژ آستانه و نیز ضخامت اکسیدگیت ترانزیستورها حتی در یک فرآیند ساخت و بر روی یک بستر یکسان نیستند که این به این مفهوم است که چنانچه دو تراشه حتی با شرایط کاملاً یکسان ساخته شوند از نظر تاخیر و توان مصرفی یکسان نخواهند بود. با کوچکتر شدن ابعاد فناوری و اندازه نمای ترانزیستورها این تغییرات به‌مراتب بیشتر نیز می شود. عمده پاف‌ها مجموعه‌ای از چالش‌ها را به مجموعه منحصربه‌فردی از پاسخ ها در قالب زوج‌های چالش- پاسخ[4] می‌نگارند به‌شکلی که این پاسخ‌ها وابسته به خصوصیت فیزیکی آن ابزار خاص است و قابل کپی‌سازی در ابزار دیگری نیست [۶-۵]. در واقع این مجموعه چالش- پاسخ باید دارای ویژگی‌هایی از جمله غیرقابل پیش‌بینی بودن به‌مفهوم وجود تناظر یک به یک بین هر چالش و پاسخ متناظر آن، منحصربه‌فرد و غیرقابل پیش‌بینی بودن آنها، غیرقابل شکست بودن به‌مفهوم غیرممکن بودن به‌دست آوردن زوج چالش- پاسخ بدون در اختیار داشتن فیزیکی پاف و غیرقابل تکرار بودن خروجی حتی با وجود اطلاع از تمام پارامترهای ساخت و قابل تشخیص بودن رخنه به‌مفهوم تخریب پاف و مشخص شدن حمله به‌آن در صورت انجام حملات مهاجم می‌باشد.

به‌دلیل ویژگی‌های منحصربه‌فرد پاف‌ها، از آنها در کاربردهای مختلفی از جمله محافظت از مالکیت معنوی، نگهداری امن کلید، تایید ابزار[5] که به‌نوعی مقابله با کپی‌سازی و مهندسی معکوس به‌شمار می‌رود، برقراری اعتماد در ارتباطات راه دور ... استفاده می‌شود [۱۰-۷].

براساس بررسی‌های به‌عمل‌آمده و با وجود این‌که محافظت سامانه‌های رمزنگاری در برابر سخت‌افزارهای جعلی و نیز مهندسی معکوس از موضوعات بسیار مهم و غیرقابل چشم پوشی در حوزه امنیت سخت‌افزاری سامانه‌ها محسوب می‌گردد و با وجود مقالات متعدد در این خصوص از دانشگاه‌ها و مراکز تحقیقاتی بین المللی، تاکنون تحقیقات کمی در این خصوص در داخل کشور صورت گرفته است.

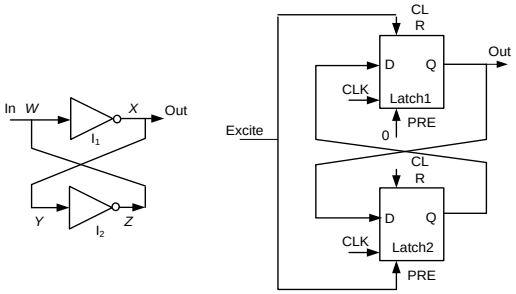
دراین مقاله ضمن بررسی مختصر انواع توابع فیزیکی کپی‌ناپذیر موجود و به‌خصوص توابع قابل پیاده‌سازی بر روی تراشه‌های سیلیکونی و تراشه‌های FPGA، یک نمونه از این نوع از انواع توابع کاربردی و قابل پیاده‌سازی بر روی تراشه FPGA که مبتنی بر نوسان‌سازهای حلقوی است [۱۴-۱۱] به‌صورت عملی پیاده‌سازی شده و نتایج آن مورد بررسی قرار گرفته است. با توجه به تنوع بالای تراشه‌های برنامه‌پذیر، آزمایشات لازم بر روی چند تراشهٔ نمونه از تراشه‌های خانواده Xilinx انجام گرفته است. از نتایج این کار می‌توان برای ارائه و پیاده‌سازی راه‌کار مناسب برای محافظت از تراشه‌ها در مقابل جعل، کپی‌سازی و آسیب‌پذیری‌های مختلف از ناحیه ارتباط سامانه امنیتی با سامانه‌های غیرخودی، تولید اعداد تصادفی، شناسایی ابزار و استفاده نمود. در ادامه مقاله ابتدا در بخش ۲ به‌طور مختصر ساختار پاف‌های سیلیکونی و کاربردهای آنها، در بخش ۳، شمای طرح پیشنهادی و نحوه پیاده‌سازی آن بر روی تراشه‌های هدف و سپس در بخش ۴ به ارائه نتایج خواهیم پرداخت. در انتها جمع‌بندی نتایج نهایی را ارائه خواهیم داد.

۲- برخی از انواع پاف‌های سیلیکونی

با توجه به متداول‌تر بودن استفاده از پاف‌های سیلیکونی برای آشنا شدن بهتر با موضوع چند نوع پاف سیلیکونی متداول را به‌صورت مختصر تشریح می‌کنیم و سایر موارد را به خواننده علاقمند واگذار می‌کنیم.

1-Physically Unclonable Function
2- Die
3- Evaluate
4- Challenge-Response Pair
5- Device Authentication

پاف‌های مبتنی بر حافظه[1]: پاف‌های مبتنی‌بر SRAM و پاف‌های پروانه‌ای[2] از جمله پاف‌های متداول مبتنی بر حافظه هستند [۱]. یک پاف SRAM شامل تعداد زیادی از واحدهای حافظه است. وجود تفاوت جزیی در ولتاژها ترانزیستورها به‌دلیل تفاوت در فرآیندهای ساخت، توسط معکوس کننده های موجود در ساختار تقویت‌شده و باعث ایجاد '1' یا '0' تصادفی در خروجی خواهد شد. در واقع چالش، مجموعه‌ای از واحدهای حافظه پس از روشن شدن مدار و پاسخ، مجموعه‌ای از این مقادیر خروجی خواهد بود. از آنجا که همه FPGA ها شامل حافظه‌هایی که نیاز به فرانشانی نداشته باشند نیستند این نوع پاف‌ها برای همه FPGAها مناسب نیستند. راه‌کار پیشنهاد شده از سوی گواردو[3] [۱۵، ۷] جایگزینی معکوس‌کننده‌های ساختار با فلیپ فلاپ‌های متقاطع است. این مدارها که می‌توانند اطلاعات را در خود ذخیره کنند پس از باز نشانی اطلاعاتشان پاک می‌شود و نیاز به فرانشانی ندارند. از این‌رو این ساختار می‌تواند بر روی FPGA پیاده‌سازی شود. شکل (۱) نشان‌دهنده نمونه‌ای از این ساختارهاست که یکی معکوس‌کننده متقاطع و یکی فلیپ- فلاپ متقاطع موسوم به پاف پروانه را نشان می‌دهد.



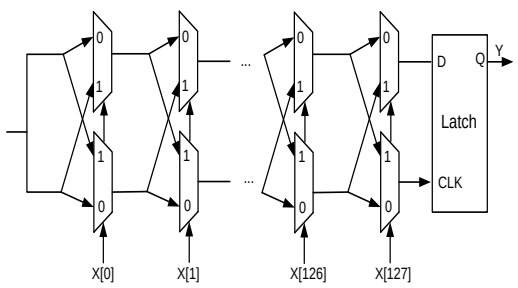
شکل (۱): دو فلیپ فلاپ متقاطع موسوم به پاف پروانه (راست) و معکوس‌کننده متقاطع (چپ) [۱].

پاف‌های مبتنی بر تاخیر[4]: این گونه پاف نیز انواع و اقسام دارند اما پاف‌های داور[5] و پاف‌های مبتنی بر نوسان‌ساز از جمله پرکاربردترین آنها هستند.

پاف های داور برای اولین بار در [۱۷-۱۶] معرفی شد و در خانواده پاف‌های قوی قرار می گیرند [۵]، بدین مفهوم که می‌توانند تعداد بسیار زیادی زوج چالش- پاسخ[6] را فراهم آورند و ازاین حیث برای شناسایی ابزارهای کم قیمت مناسب هستند. ساختار پایه چنین مداراتی در شکل (۸-۲) نشان داده شده است. این ساختار یک زنجیره ۱۲۸ تایی از مالتی پلکسرهای با ورودی مشترک است که یکی از خروجی های آخرین طبقه به ورودی D یک فلیپ- فلاپ و خروجی دیگر به پالس ساعت آن وصل می‌شود. ورودی مدار سیگنال‌های پله است. ایده اصلی پس این نوع پاف بر مبنای برقراری یک شرط مسابقه[7] بین دو مسیر دیجیتال درون یک تراشه است. بیت‌های چالش ورودی X[0]~X[127] است که به ورودی‌های انتخاب مالتی‌پلکسرها وارد می شود. سیگنال X[i] نشان دهنده آن است که سیگنال ورودی در طبقه i ام به کدام مالتی پلکسر وارد می‌شود. سیگنال‌های‌چالش مختلف ورودی و تاخیرهای مختلف بین زنجیره مالتی‌پلکسرهای موازی تعیین‌کننده آن است که آیا سیگنال پله به ورودی D فلیپ- فلاپ یا به پایه پالس ساعت می‌رسد. در حالت اول منطق '1' و در حالت دوم منطق '0' در خروجی فلیپ- فلاپ‌لچ خواهد شد. هر بیت خروجی به‌عنوان یک بیت امضا در پاسخ به چالش ورودی در نظر گرفته می‌شود.

البته از آنجا که پاسخ یک پاف سیلیکونی مبتنی‌بر تاخیر را می‌توان توسط یک تابع خطی چالش‌ها نشان داد، چنانچه مهاجم تاخیر هر طبقه را بداند ممکن است به‌تواند با جمع کردن تاخیر مسیرها خروجی را حدس بزند. از این‌رو استفاده از چند مسیر برای تعیین پاسخ خروجی کار مهاجم را به‌مراتب سخت‌تر خواهد کرد.

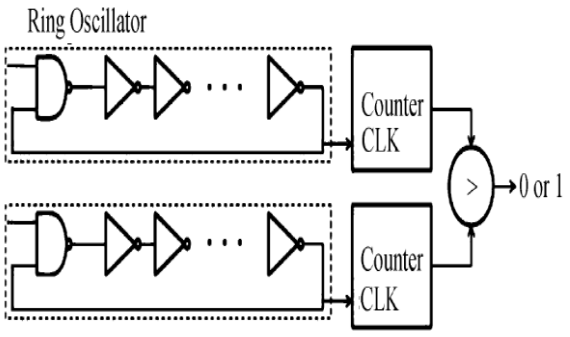
در سناریوهای مرسوم کاربردی، از پاف در دو مرحله استفاده می‌شود. در مرحله اول، که نام نویسی[8] نام دارد، تعدادی زوج ورودی- خروجی با استفاده از پاف مورد نظر جمع‌آوری شده و درون یک پایگاه داده که پایگاه داده زوج ورودی- خروجی نام دارد، ذخیره می شود. در فاز دوم که فاز شناسایی نام دارد، یک ورودی از پایگاه داده انتخاب شده و به پاف اعمال می شود. خروجی تولید شده توسط پاف با خروجی مربوطه ذخیره شده در پایگاه داده مقایسه می‌شود. در صورتی‌که شباهت پاسخ پاف به ازای ورودی مشخص، با پاسخ ذخیره‌شده در پایگاه داده از حد معینی بیشتر بود، عمل شناسایی مثبت بوده و این پاف، همان پاف مورد نظر تشخیص داده می‌شود [۱۸].



شکل (۲): ساختار یک پاف داور [۱].

1- Memory-Based PUFs
2- Butterfly
3 -Guajardo
4-Delay-Based PUFs
5 -Arbiter PUF
6 -Challenge-Response Pair
7 -Race Condition
8 -Enrollment

پاف‌های مبتنی بر نوسان‌سازهای حلقوی اولین بار توسط سوه[1] و همکارانش استفاده از پاف‌های مبتنی بر نوسان‌سازهای حلقوی که خود آنها بر مبنای تفاوت تاخیر بین این نوسان‌سازها برای تولید رشته بیت‌های تصادفی است را پیشنهاد دادند. یک نوسان‌ساز حلقوی یک مدار ساده متشکل از تعدادی معکوس‌کننده است که به‌صورت حلقوی به یکدیگر متصل شده‌اند و با فرکانس مشخصی نوسان می‌کند. فرکانس نوسان نوسان‌ساز بستگی به تعداد و تاخیر معکوس‌کننده‌ها و نیز سیم‌های بین آنها دارد. از آنجا که این تاخیرها به پارامترهای ساخت و نیز برخی فاکتورهای غیرقطعی بستگی دارد فرکانس نوسان نوسان‌ساز به‌طور قطعی قابل پیش‌بینی نیست. ساده‌ترین فرم این پاف‌ها رشته‌ای از بیت‌های ’0‘ و ’1‘ را در خروجی با مقایسه فرکانس یک زوج یا چند نوسان‌ساز تولید می‌کند. از آنجا که پاف‌های مبتنی‌بر نوسان‌سازهای حلقوی نیاز به تقارن ندارند پیاده‌سازی آنها در FPGA نسبتا ساده است. شکل (۸-۳) ساختار یک پاف مبتنی‌بر نوسان‌ساز حلقوی و شکل (۳) ساختار یک پاف مبتنی‌بر N نوسان‌ساز حلقوی را نشان می‌دهد. نشان داده شده که یک پاف دارای N نوسان‌ساز حلقوی دارای آنتروپی $N \times log_2^N$ بیت اطلاعات است [۵]. این توابع، در مقایسه با پاف‌هایی که براساس تاخیر گیت‌ها و داوری طراحی شده‌اند از لحاظ پیاده‌سازی ساده‌تر هستند اما از لحاظ منابع و توان مصرفی نیاز به منابع سخت‌افزاری و توان مصرفی بیشتری نسبت به روش تاخیر و داوری دارند و سرعت آنها نیز پایین‌تر است.



شکل (۳): ساختار پایه یک پاف مبتنی‌بر نوسان‌ساز حلقوی.

مطابق با آنچه در منابع مربوطه گزارش شده است پاف‌های مبتنی‌بر SRAM دارای بالاترین امنیت (آنتروپی)، پس از آن پاف‌های پروانه و پس از آن پاف‌های مبتنی بر تاخیر قرار دارند. جدول (۱) آنتروپی سه طرح مختلف پاف را به‌ازاء ۱۰۰۰ بیت خروجی نشان می‌دهد [۱۹].

جدول (۱): مقایسه آنتروپی سه طرح مختلف پاف [۱۹].

نوع پاف	آنتروپی در ۱۰۰۰ بیت
پاف SRAM	۹۵۰
پاف پروانه	۶۰۰
پاف تاخیر	۱۵۰

۳- پیاده‌سازی طرح پاف مورد نظر

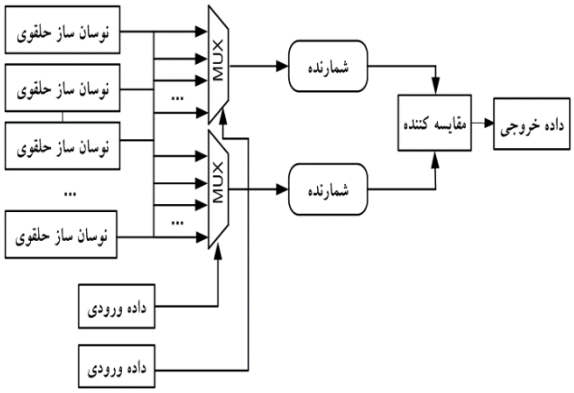
همان‌طور که ذکر شد از بین تمام شماهای پیشنهاد شده برای تحقق پاف‌ها، طرح‌های پروانه و نوسان‌ساز حلقوی مناسب تر از بقیه برای پیاده‌سازی بر روی FPGA هستند که در این تحقیق طرح نوسان‌ساز حلقوی پیاده‌سازی شد. در ادامه نحوه پیاده‌سازی و نتایج به‌دست‌آمده را تشریح می‌کنیم.

۳-۱- شمای طرح پیاده‌سازی شده

شکل (۵) شمایی از طرح پیشنهادی برای تحقق پاف مورد نظر را نشان می‌دهد. در هر نوسان‌ساز تاخیر گیت‌ها و مسیر بیش از دویست گیت منطقی در نظر گرفته شده است. اختلاف فرکانس نوسان‌سازها از اختلاف تاخیر سیم‌ها و گیت‌ها ناشی می‌شود. با استفاده از این طرح، تراشه دارای کد منحصربه‌فردی می‌شود که این کد باعث تمایز این تراشه از تراشه‌های دیگر می‌شود. و از این کد منحصربه‌فرد می‌توان، برای شناسه، احراز اصالت و یا در برچسب‌های RFID استفاده نمود [۱۸و ۹]. ما طرح خود را بر روی سه تراشه FPGA مختلف پیاده‌سازی نموده و مشاهده نمودیم که کد ایجادشده که براساس خواص فیزیکی پدیدارشده منحصربه‌فرد بوده و باعث به‌وجود آمدن یک شناسه منحصربه‌فرد برای آن تراشه خواهد شد. نوع نوسان‌های ایجاد شده و فرکانس نوسان طرح پیاده‌سازی شده منحصربه‌فرد بوده که این فرکانس توسط شمارنده[2]، شمرده‌شده و سپس فرکانس‌های شمرده‌شده برای احراز اصالت بر اساس خصوصیّات فیزیکی باهم مقایسه می‌شوند و یک کد منحصربه‌فرد به‌عنوان شناسه تراشه استخراج می‌گردد. لازم به‌ذکر است که آزمایشات ما نشان داد که چنانچه همین طرح برروی همان تراشه و در قسمت دیگری از آن پیاده‌سازی شود کد به‌دست‌آمده با کد قبلی متفاوت خواهدبود که این امر موید مواردی است که در قسمت‌های قبل در مورد منحصربه‌فرد بودن کد استخراج شده ذکر شد.

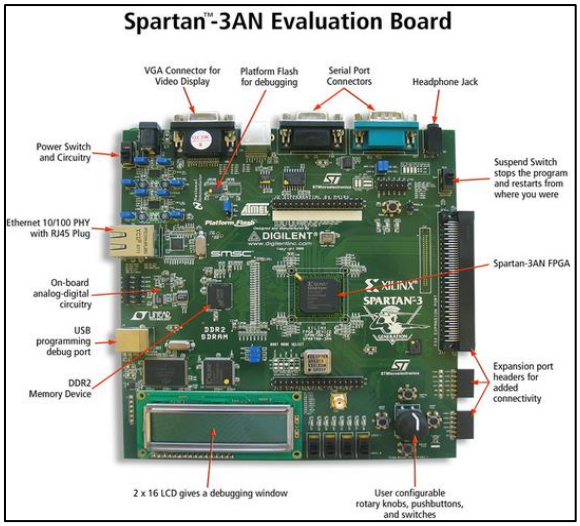
1- Suh

2- Counter



شکل (۴): شمای طرح پیاده‌سازی شده بر روی تراشه FPGA شامل تعدادی نوسان‌ساز حلقوی، شمارنده و مقایسه‌گر

بعد از بررسی اجمالی پاف و کاربردهای آن، نوبت به نحوه پیاده‌سازی و نتایج به‌دست‌آمده از اجرای طرح‌ها بر روی تراشه FPGA می‌رسد. ما در این تحقیق از سه بورد FPGA با مشخصات Virtex 5 ML506 Evaluation Platform و Spartan3 XC3S400 و Spartan3AN XC3S700AN برای پیاده‌سازی طرح استفاده نمودیم. شکل (۶) شمای بورد Spartan3A XC3S700AN را نشان می‌دهد که دارای تراشه XC3S700AN و دارای حافظه XCF02/04S برای برنامه‌ریزی FPGA است. ضمن این‌که این بورد مجهز به نوسان‌ساز، کانکتورها و سوئیچ‌های مختلف برای برنامه‌ریزی عملکرد آن در کاربردهای مختلف است.



شکل (۵): تصویر بورد Spartan3A XC3S700AN از شرکت Xilinx.

۳-۲- پیاده‌سازی نوسان‌ساز حلقوی با استفاده از زبان توصیف سخت‌افزار وریلاگ

یکی از چالش‌های مهم در تحقق عملی نوسان‌سازهای حلقوی پیاده‌سازی آن با زبان توصیف سخت‌افزار است. مشکل اصلی در استفاده از گیت‌های معکوس‌کننده سری است که ابزار ساخت آنها را به‌عنوان یک منطق بی اثر در نظر گرفته و حذف می‌کند زیرا ترکیب سری دو معکوس‌کننده از نظر منطقی یک ترکیب بی اثر است. استفاده از دستور 'KEEP' در زبان توصیف سخت‌افزار باعث می‌شود تا ابزار سنتز از حذف گیت‌هایی که در ادامه این دستور قرار می‌گیرند خودداری کند و از این‌رو، برای پیاده‌سازی ساختار نوسان‌ساز حلقوی استفاده از این دستور حتماً لازم است. شکل (۶) کد پیاده‌سازی یک نوسان‌ساز حلقوی با استفاده از این دستور را نشان می‌دهد که در آن از ۷۵ گیت معکوس‌کننده در یک ساختار حلقوی استفاده شده است. علاوه بر آن از یک گیت AND برای کنترل شروع نوسانات استفاده شده است. نتایج به‌دست‌آمده پس از سنتز مدار بر روی تراشه نشان داد که چنین نوسان‌سازی موج مربعی با پریود تقریبی ۱۰۰ ns تولید خواهد کرد.

```
module oscillator(
input enable,
output osc
);

(*KEEP=”TRUE”*) wire [0:74] im;
and g1(im[0], im[74], enable);
not g2(im[1], im[0]);
.....
not g73(im[74], im[73]);
not g74(osc, im[74]);
endmodule
```

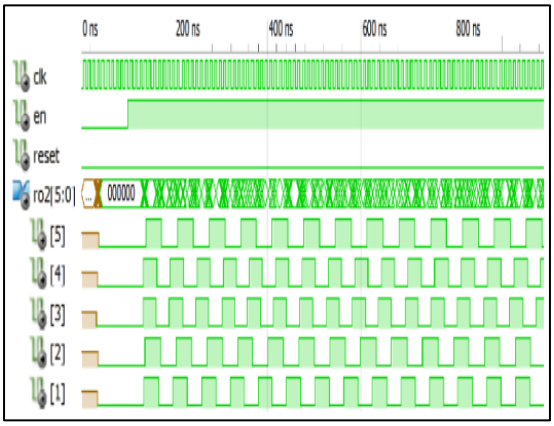
شکل (۶): پیاده‌سازی نوسان‌ساز حلقوی متشکل از ۷۵ گیت معکوس‌کننده با استفاده از زبان توصیف سخت‌افزار ویلاگ.

۳-۳- نتایج به‌دست‌آمده از شبیه‌سازی و پیاده‌سازی

برای شبیه‌سازی و سنتز طرح از کدهای قابل سنتز زبان توصیف سخت‌افزار وریلاگ و نرم‌افزار ISE 14.4 استفاده شد. شکل (۷) شبیه‌سازی طرح نوسان‌ساز حلقوی بعد از مرحله جایابی و مسیریابی[1] بر روی یک بورد FPGA با مشخصات Virtex 5 ML506 Evaluation Platform را نشان می‌دهد. این شبیه‌سازی در محیط ISIM در نرم‌افزار ISE 14.4 و با استفاده از یک رایانه قابل حمل دوهسته‌ای انجام شده است. شبیه‌سازی نشان داد که نوسان‌کننده‌ها دارای نوسان متمایز از یکدیگر می‌باشند. همان‌طور که ملاحظه می‌شود، هر کدام از نوسان‌کننده‌ها دارای اختلاف زمانی برای شروع نوسان از نوسان‌کننده‌های دیگر دارا می‌باشد و این به خاطر تأخیرهای متفاوت گیت و مسیر در

1- Place&Route

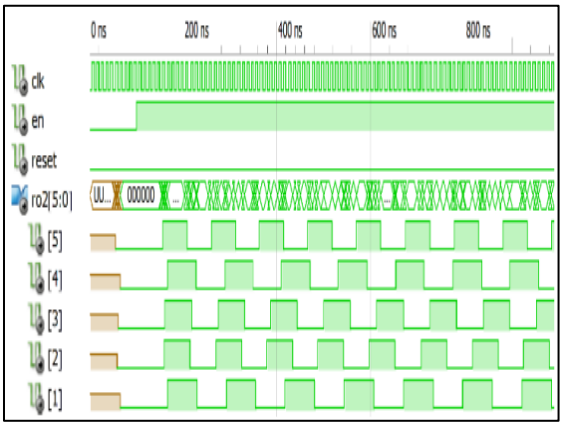
FPGA می‌باشد. با افزایش تعداد گیت‌ها و طول مسیر فرکانس نوسان‌کننده‌ها کاهش می‌یابد.



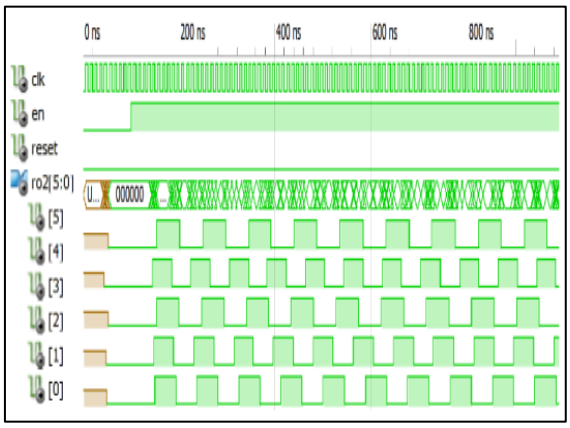
شکل (۷): شبیه‌سازی نوسان‌ساز حلقوی بعد از مرحله جایابی و مسیریابی بر روی بورد Virtex 5 ML506 Evaluation Platform تعداد پنج نوسان‌ساز به‌صورت همزمان با یکدیگر شروع به‌کار می‌کنند. که به‌دلیل تفاوت فرآیندهای ساخت با فرکانس‌های متفاوتی بایکدیگر نوسان می‌کنند.

در تمام شبیه‌سازی‌های انجام شده پایه enable تعریف شده است. با یک شدن پایه enable، نوسان‌کننده‌های طراحی شده همزمان باهم شروع به نوسان می‌کنند که این کار برای همزمانی شروع نوسان‌کننده‌ها بسیار مهم می‌باشد. در مرحله بعدی طرح را بر روی یک بورد دیگر FPGA که از خانواده Spartan3 مدل XC3S400 شبیه‌سازی و پیاده‌سازی نمودیم. همان‌طور که در شکل (۸) مشاهده می‌شود، نوسان‌کننده‌ها دارای نوسان متمایز از یکدیگر می‌باشند. چنانکه گفته شد، با توجه به تفاوت ویژگی‌های فیزیکی تراشه که در موقع ساخت اتّفاق می‌افتد، فرکانس نوسان‌کننده‌ها نیز متمایز از یکدیگر خواهد بود.

باید در نظر داشت که اصول پایه‌ای نوسان‌کننده‌ها که باید بر اساس تأخیر مسیر و گیت می‌باشد، در هر حلقه باید این تأخیرها باید در نظر گرفته شود. دستور 'KEEP' را باید تحت شرایط نحوه نوسان حلقه‌ها برای هر حلقه منظور نمود. این کار باعث می‌شود، تأخیر گیت و مسیر بخوبی در شبیه‌سازی و پیاده‌سازی مورد استفاده قرار گیرد. در مرحله سوم طرح خود را بر روی یک بورد دیگر FPGA ساخت شرکت Xilinx و از خانواده Spartan3A مدل XC3S700AN شبیه‌سازی و پیاده سازی نمودیم. با توجه به شکل (۹) و نتایج به‌دست‌آمده از ابزار سنتز مشخص شد که براساس خصوصیّاتی که در فرآیند ساخت اتفاق افتاده، فرکانس نوسان‌کننده‌ها و نوسان آنها متمایز از یکدیگر می‌باشند.



شکل (۸): شبیه‌سازی نوسان‌ساز حلقوی بعد از مرحله جایابی و مسیریابی بر روی بورد Spartan3 XC3S400



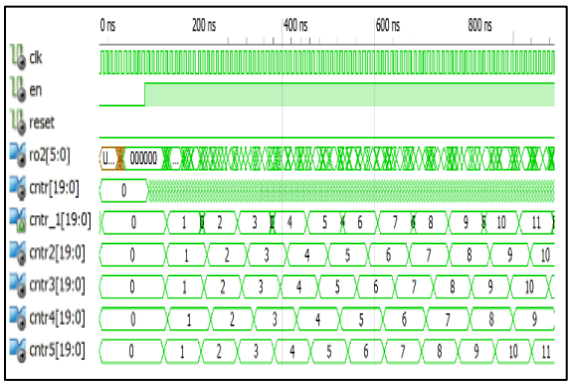
شکل (۹): اجرای نوسان‌ساز حلقوی در Spartan3AN XC3S700AN

۳-۴- شبیه‌سازی شمارنده

شمارنده[1] در منطق دیجیتال و محاسبات، مداری است که تعداد دفعاتی که یک رویداد یا فرایند خاص رخ داده است را شمارش کرده و نمایش می‌دهد. معمولاً مبنای عمل شمارش به پایین‌رونده یا بالارونده بودن پالس ساعت آن می‌باشد. در طراحی شمارنده از دستور لبه بالارونده[2] استفاده نمودیم. در شکل (۱۰) تعداد ۵ شمارنده را مشاهده می‌نماییم که این شمارنده‌ها نوسانی که ایجاد شده را بر اساس برنامه نوشته شده لبه بالا رونده، در حال شمارش هستند. در قسمت آخر باید برای تولید رشته بیت احراز اصالت، مقادیر شمارنده‌ها با یکدیگر مقایسه می‌شوند که از مقایسه دوبه‌دو مقادیر این شمارنده‌ها یک کد ده رقمی حاصل خواهد شد زیر $\binom{5}{2}=10$ می‌باشد. بدیهی است که برای دست‌یابی به کدهای طولانی‌تر لازم است تا تعداد بیشتری از نوسان‌سازهای حلقوی مورد استفاده قرار به‌گیرند. در شبیه‌سازی در یک زمان

1- Counter
2- Rising edge

خاص برای هر پنج نوسان‌کننده، دستور شمارش داده شده است. با این کار اختلاف فرکانس نوسان‌کننده‌ها به خوبی قابل مشاهده می‌باشد. همان‌طور که در شکل زیر مشاهده می‌شود، با یک شدن پایه enable شمارنده‌های طراحی شده شروع به عمل شمارش می‌کنند تا در یک زمان خاص تعیین شده مورد مقایسه قرار گیرند.



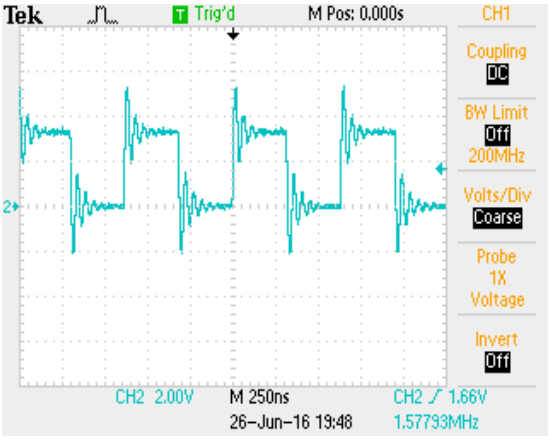
شکل (۱۰): شبیه‌سازی شمارنده‌های طراحی‌شده در این پروژه که با لبه بالا رونده پالس ساعت کار می‌کنند. اختلاف شمارنده‌ها با یکدیگر موید تفاوت فرکانس نوسان‌سازهای حلقوی است.

شکل (۱۱) نوسان یکی از نوسان‌سازهای حلقوی بر روی تراشه Virtex-5 را نشان می دهد که نوسان‌ساز، یک موج مربعی با فرکانس ۱/۵۷ MHz تولید کرده است.

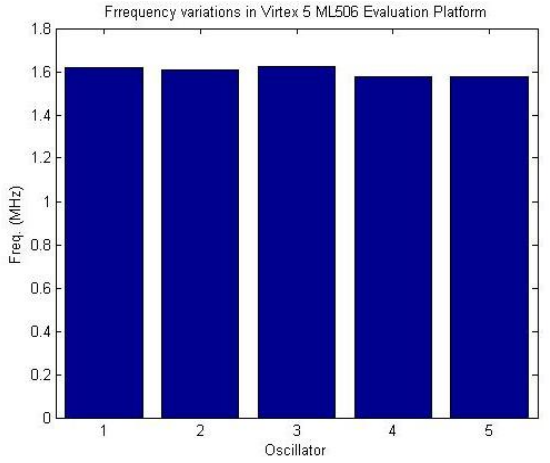
در شکل (۱۲) فرکانس‌های اندازه‌گیری شده برای پنج نوسان‌ساز حلقوی پیاده‌سازی‌شده بر روی بورد Virtex 5 FPGA ML506 Evaluation Platform را مشاهده می‌نماییم. اختلاف فرکانس ایجاد شده در پنج نوسان‌کننده، بر اساس خصوصیّات فیزیکی تراشه بوده و این خصوصیّات فیزیکی تراشه باعث شده، تأخیرهای گیت و مسیر تراشه، آثار خود را در اختلاف فرکانس نوسان‌سازها نشان دهد.

در شکل (۱۳) فرکانس‌های نوسان‌ساز حلقوی پیاده‌سازی شده بر روی بورد FPGA با تراشه Spartan3 XC3S400 را مشاهده می‌نماییم. همان‌طور که ذکر شد این اختلاف فرکانس نیز ناشی از خصوصیّات فیزیکی و ذاتی تراشه می‌باشد، که در موقع فرآیند ساخت اتفاق افتاده است.

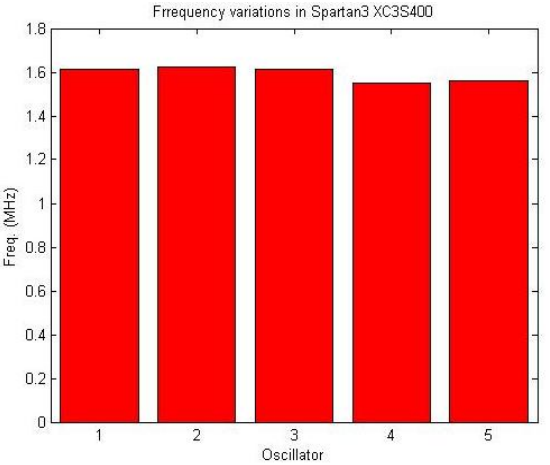
در مرحله سوم طرح نوسان‌ساز حلقوی ایجاد شده بر روی سومین FPGA با تراشه Spartan3AN XC3S700AN پیاده‌سازی شده است. فرکانس این ۵ نوسان‌کننده در شکل (۱۴) به نمایش گذاشته شده است. همان‌گونه که از شکل پیداست فرکانس هیچ‌یک از نوسان سازها با یکدیگر برابر نیست و این امر تایید کننده انتظارات ما از طراحی مورد نظر است.



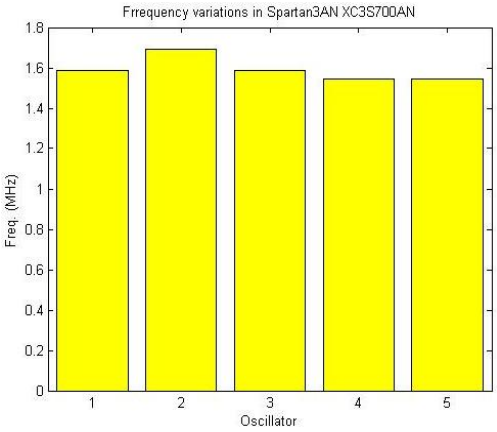
شکل (۱۱): نوسان یکی از نوسان‌سازهای پیاده‌سازی شده با فرکانس ۱/۵۷ MHz بر روی تراشه Virtex-5.



شکل (۱۲): فرکانس نوسان‌سازهای پیاده‌سازی شده بر روی بورد Virtex 5 ML506 Evaluation Platform. همان‌گونه که از شکل پیداست با وجود اینکه مدارها بر روی یک تراشه پیاده‌سازی شده‌اند فرکانس نوسان آنها با یکدیگر متفاوت است.



شکل (۱۳): فرکانس نوسان‌سازهای پیاده‌سازی شده بر روی بورد Spartan3 XC3S400 و اختلاف آن‌ها با یکدیگر.



شکل (۱۴): فرکانس نوسان‌سازهای پیاده‌سازی شده بر روی بورد Spartan3AN XC3S700AN و اختلاف آنها با یکدیگر.

۴- نتایج پیاده‌سازی سخت‌افزاری

جدول (۲) نتایج پیاده‌سازی طرح مورد نظر بر روی تراشه‌های مورد نظر از حیث مساحت اشغالی و منابع سخت‌افزاری مورد استفاده را نشان می‌دهد. منابع سخت‌افزاری بر حسب تعداد LUTهای چهار ورودی و نیز تعداد بلوک‌های منطقی آرایش‌پذیر[1] بیان شده‌اند. از آنجا که در جستجوهای انجام شده موردی دقیقاً مشابه با طرح پیشهادی یافت نشد لذا نتوانستیم طرح خود را به‌طور مستقیم با سایر کارها مقایسه کنیم اما خوشبختانه گزارش ابزار سنتز نشان داد که طرح مورد نظر مساحت معقول و قابل قبولی را روی تراشه‌ها اشغال می‌کند که از این حیث پیاده‌سازی آن کاملاً منطقی و معقول بنظر می‌رسد.

جدول (۲): منابع سخت‌افزاری استفاده شده در پیاده‌سازی سخت‌افزاری طرح پاف مورد نظر بر روی FPGAهای مختلف از خانواده Xilinx.

Device Utilization Summary for Spartan3-xc3s400		
Logic Utilization	Used	Available
No. of Slices	۵۵	۳۵۸۴
No. of 4-input LUTs	۱۴۵	۷۱۶۸
Device Utilization Summary for Virtex-5 xc5vsx50t		
Logic Utilization	Used	Available
No. of Slices	۷۵	۳۲۶۴۰
No. of fully used LUT-FF pairs	۰	۶۰
Device Utilization Summary for Soartan3- xc3s700AN		
Logic Utilization	Used	Available
No. of Slices	۵۵	۵۵۸۸
No. of 4-input LUTs	۱۴۵	۱۱۷۷۶

1- CLB Slices

۵- مشخصات شناسه و اثر دما بر عملکرد پاف

همان‌طور که گفته شد در مرحله آخر فرکانس پنج نوسان‌کننده هر کدام از FPGA ها برای احراز هویّت مورد مقایسه قرار گرفت. شناسه ایجاد شده در هر کدام از تراشه‌های مورد آزمایش با تراشه دیگر متفاوت بوده و این تفاوت بر اساس خصوصیّات فیزیکی تراشه می‌باشد. آزمایشات ما نشان داد که چنانچه همین طرح بر روی یک تراشه با شماره دقیقاً یکسان و از همان کارخانه سازنده پیاده‌سازی شود باز هم کد شناسه بدست آمده متفاوت و منحصر به‌فرد خواهد بود. در واقع با این طرح می‌توان برای هر تراشه یک کد شناسه منحصربه‌فرد تعریف کرده و آنرا از سایر تراشه‌ها متمایز نمود. از این مفهوم می‌توان برای ایجاد اعتماد در محاسبات راه دور، محاسبات مطمئن[2]، کنترل دسترسی، احراز اصالت تراشه‌ها و یا تولید کلید خصوصی منحصربه‌فرد برای هر تراشه در محاسبات کلید عمومی و تسهیم راز استفاده کرد. در واقع شناسه تعریف شده، اثر انگشت هر تراشه است که در کاربردهای احراز هویت تراشه‌ها مورد استفاده قرار می‌گیرد. لازم به‌ذکر است که آنچه در این تحقیق پیاده‌سازی شد یک نمونه آزمایشگاهی است که هنوز تا کاربردهای عملی قدری فاصله دارد اما نتایج به‌دست آمده کاملاً امیدوارکننده و منطقی است بشکلی که توسعه طرح برای دست‌یابی به کدهای بلندتر کاملاً امکان‌پذیر است.

۵-۱- تاثیر دما بر عملکرد طرح پیشنهادی

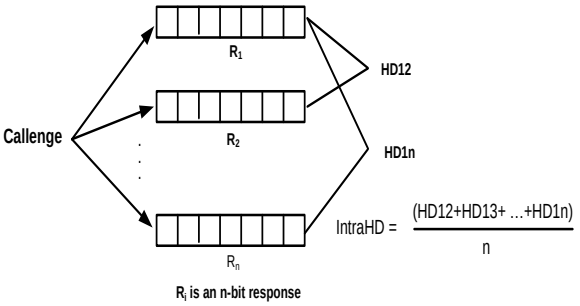
همان‌طور که ذکر شد مانند سایر مدارها قابلیت اطمینان و امنیت از جمله مهم‌ترین معیارهای ارزیابی کیفیت پاف‌ها هستند. دما و تشعشعات الکترومغناطیسی از جمله تاثیرگذارترین عوامل بر عملکرد پاف هستند [۲۴-۲۳]. در صورت در اختیار داشتن فضای لازم روی تراشه استفاده از کدهای تصحیح خطا می تواند به کاهش احتمال خطا در شرایط مختلف دمایی یا عملکردی پاف کمک کند زیرا در کاربردهایی که نیاز به بازتولید شناسه وجود دارد پایداری و قابلیت اطمینان پاف امر مهمی است که نمی‌تواند نادیده گرفته شود حال آن‌که ممکن است این مساله در تولید اعداد تصادفی مساله چندان مهمی نباشد. معمولاً برای اندازه‌گیری میزان قابلیت اطمینان پاف از معیار وزن همینگ درون تراشه[3] استفاده می‌شود. بدین مفهوم که از تراشه i پاسخ n بیتی R_i در دما و شرایط متعارف استخراج می‌شود. سپس S نمونه $R_{i,q\in\{1,2,...,s\}}$ پاسخ همان پاف در شرایط کاری متفاوت مانند دما یا ولتاژهای مختلف استخراج می‌شود. سپس از

2- Trusted Computing
3- Intra-chip Hamming distance

رابطه (۵) برای ارزیابی اختلاف امضای به‌دست‌آمده از پاف به‌ازای دو چالش یکسان در دو آزمایش متوالی استفاده می‌شود.

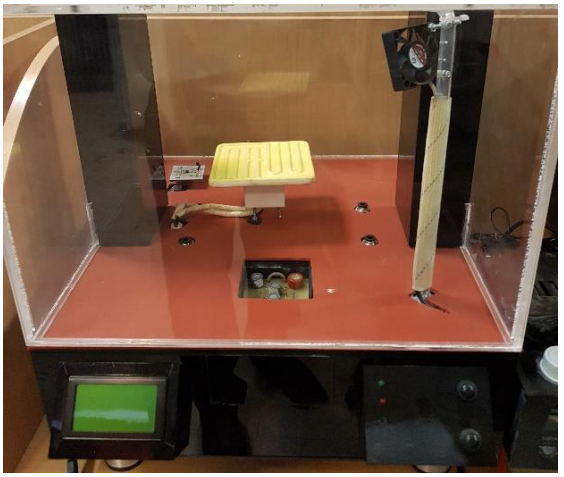
$$r = \frac{1}{s}\sum_{q=1}^{s}\frac{HD(R_i, R_{i,q})}{n} \times 100\% \qquad (۵)$$

در رابطه (۱) s نشان‌دهنده تعداد نمونه‌ها، n نشان‌دهنده تعداد بیت‌ها در هر امضا و $HD(R_i, R_{i,q})$ نشان‌دهنده فاصله همینگ بین پاسخ R_i و q امین تکرار همان آزمایش است. شکل (۱۵) به‌سادگی نشان می‌دهد که چگونه می‌توان وزن همینگ درون تراشه را برای یک پاف مشخص در آزمایش‌های مختلف محاسبه کرد.



شکل (۱۵): محاسبه وزن همینگ درون تراشه‌ای برای اندازه‌گیری میزان قابلیت اطمینان یک پاف نوعی.

برای محاسبه قابلیت اطمینان طرح مورد نظر، بورد FPGA شامل مدار پاف پیاده‌سازی شده را در محفظه نشان داده شده در شکل (۱۶) که مجهز به یک دستگاه تولید گرما با قابلیت کنترل دما به‌صورت دیجیتال است قرار دادیم. این محفظه به‌طور کامل در داخل کشور توسط دانشجویان طراحی و ساخته شده است.



شکل (۱۶): محفظه حرارتی با قابلیت کنترل دما به‌صورت دیجیتال با حساسیت یک درجه سانتی‌گراد.

تغییر دما از ۲۰ تا ۶۰ درجه سانتی‌گراد تنها یک بیت خطا در خروجی پاف اتفاق افتاد و از این‌رو، قابلیت اطمینان طرح حدود ۹۰ درصد به‌دست می‌آید. لازم به‌ذکر است که مطابق با آنچه در منابع مرتبط ذکرشده پاف نوسان‌ساز حلقوی معمولاً از قابلیت اطمینان کاملاً قابل قبولی برخوردار است و در برابر تغییر دما مقاوم است اما برای استفاده از یک پاف در شرایط عملیاتی لازم است تا آزمایش مورد نظر به‌شکلی که توضیح داده شد برای پاف با کد خروجی بلندتر تکرار شود [۲۴-۲۳].

۶- نتیجه‌گیری

وقایع و گزارشات اخیر در حوزه امنیت به‌روشنی نشان می‌دهد که تراشه‌ها و ابزارهای محاسباتی به‌صورت عمده، بدون نظارت و در معرض انواع حملات فیزیکی و سایر انواع حملات هستند. کامپیوترها در شبکه اینترنت، تراشه‌های تعبیه‌شده در انواع ابزارهای ارتباطی و الکترونیکی نمونه‌ای از این ابزارها هستند که مهاجمین می‌توانند از طریق حملات فیزیکی امنیت آنها را مورد تهدید قرار دهند. حملات تهاجمی و نیمه تهاجمی، نصب نرم‌افزارهای مخرب و ... همه از تهدیداتی هستند که به‌روشنی نشان می‌دهند سازوکارهای محافظت نرم‌افزاری به‌تنهایی کافی نیستند. ذخیره اطلاعات دیجیتال به‌شکل مطمئن در یک ابزار کار ساده‌ای نیست و از این‌رو، توابع کپی‌ناپذیر فیزیکی و سازوکارهای مشابه مهم هستند. پاف‌ها از جمله راه‌کارهای پیشنهادی مناسب برای مقابله با جعل، کپی‌سازی، مهندسی معکوس، تزریق کلید غیرمجاز یا تغییر دادن برنامه ذخیره‌شده در ابزار رمز یا سایر حملات فیزیکی، مقابله با سرقت مالکیت معنوی، تولید کلید و اعداد تصادفی به‌صورت سخت‌افزاری از یک سیستم فیزیکی غیرقابل پیش‌بینی بدون نیاز به ذخیره‌سازی به‌صورت سخت‌افزاری در حافظه‌های غیرفرار و بدون نیاز به حافظه زیاد هستند. در این تحقیق یکی از انواع کاربردی پاف‌های سیلیکونی مبتنی‌بر نوسان‌ساز حلقوی به‌طور موفقیت‌آمیز بر روی تراشه FPGA پیاده‌سازی و آزمایش شد. با پیاده‌سازی پنج نوسان‌ساز حلقوی و با استفاده از اختلاف فرکانس آن‌ها یک کد یکتای ۱۰ بیتی به‌دست آمد که برای حصول کدهای بلندتر نیاز به افزایش تعداد نوسان‌سازها خواهد بود. نتیجه پیاده‌سازی بر روی چند تراشه مختلف نشان داد که با توسعه طرح مزبور می‌توان از آن برای محافظت از تراشه در مقابل جعل یا مهندسی‌معکوس به‌خوبی استفاده کرد. با اندازه‌گیری تغییر دما بر روی طرح پیاده‌سازی شده مشخص شد که با تغییر ۴۰ درجه سانتی‌گراد دما ضریب اطمینان پاف در حدود ۹۰٪ و بالاتر است. ضمن این‌که پیاده‌سازی عملی سایر طرح‌های پاف

برای استفاده در سایر کاربردها از جمله تولید اعداد تصادفی و یا تولید کلید رمز و نیز بررسی حملات مختلف به آن‌ها می‌تواند از موضوعات جذاب تحقیقاتی برای محققین حوزه امنیت و سایر رشته‌های مرتبط باشد [۲۸-۲۵].

۷- منابع

[1] M. Roel, "Physically Unclonable Functions: Constructions," Properties and Applications, Ph. D. thesis, Dissertation, University of KU Leuven, 2012.

[2] H. Handschuh, S. Geert-Jan, and P. Tuyls, "Hardware Intrinsic Security from Physically Unclonable Functions," Parts of Towards Hardware-Intrinsic Security, Springer Berlin Heidelberg, pp. 39-53, 2010.

[3] M. Platonov, "SRAM-Based Physical Unclonable Function on an Atmel ATmega Microcontroller," Master's thesis, Czech Technical University in Prague, Faculty of Information Technology, 2013.

[4] V. Van der Leest, G.-J. Schrijen, H. Handschuh, and P. Tuyls, "Hardware Intrinsic Security from D Flip-Flops," In ACM workshop on scalable trusted computing-STC 2010, New York: ACM, pp. 53–62, 2010.

[5] J.-L. Zhang, "A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs, Journal Of Computer Science and Technology," vol. 29, no. 4, pp. 664–678, July 2014. DOI 10.1007/s11390-014-1458-1.

[6] Y. Lao and K. Parhi, "Reconfigurable architectures for silicon physical unclonable functions," In IEEE international conference on electro/information technology-EIT 2011, New York: IEEE, pp. 1–7, 2011.

[7] J. Guajardo, S. S. Kumar, G. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," CHES 2007, LNCS 4727, pp. 63–80, 2007.

[8] N. Beckmann and M. Potkonjak, "Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions," In Lecture notes in computer science (LNCS), vol. 5806, International workshop on information hiding-IH 2009, Berlin: Springer, pp. 206–220, 2009.

[9] L. Bolotny and G. Robins, "Physically Unclonable Function-Based Security and Privacy in RFID Systems," In IEEE international conference on pervasive computing and communications-PERCOM 2007, New York: IEEE, pp. 211–220, 2007.

[10] F. Armknecht, R. Maes, A.-R. Sadeghi, B. Sunar and P. Tuyls, "Memory leakage resilient encryption based on physically unclonable functions," In Lecture notes in computer science (LNCS), vol. 5912, Advances in cryptology-ASIACRYPT 2009, Berlin: Springer, pp. 685–702, 2009.

[11] Q. Chen, G. Csaba, and P. Lugli, U. Schlichtmann, and U. Ruhrmair, "The bistable ring PUF: a new architecture for strong physical unclonable functions," In IEEE international symposium on hardware-oriented security and trust-HOST 2011, New York: IEEE, pp. 134–141, 2011.

[12] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: an FPGA-friendly secure primitive," Journal of Cryptology, vol. 24, pp. 375–397, 2011.

[13] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," In International conference on field programmable logic and applications-FPL 2009, New York: IEEE, pp. 703–707, 2009.

[14] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," In IEEE international symposium on hardware-oriented security and trust-HOST 2010, New York: IEEE, pp. 94–99, 2010.

[15] J. Guajardo, et al, "Brand and IP protection with physical unclonable functions," 2008 IEEE International Symposium on Circuits and Systems, IEEE, 2008.

[16] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," In Proc. Symposium on VLSI Circuits, Digest of Technical Papers, pp.176-179, Jun. 2004.

[17] D. Lim, J. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. Syst., vol. 13, no. 10, pp.1200-1205, 2005.

[18] S. Kardas, M. Akgun, M. S. Kiraz, and H. Demirci, "Cryptanalysis of lightweight mutual authentication and ownership transfer for RFID systems," In Workshop on lightweight security and privacy: devices, protocols, and applications-LightSec 2011, NewYork: IEEE, pp. 20-25 2011.

[19] H. Handschuh, G.-J. Schrijen, and P.Tuyls, "Hardware Intrinsic Security from Physically Unclonable Functions," A.-R. Sadeghi, D. Naccache (eds.), Towards Hardware-Intrinsic Security, Information Security and Cryptography, DOI 10.1007/978-3-642-14452-3_2, pp. 39-53, 2011.

[20] R. Maes, A.Van Herrewege, and I. Verbauwhede, " PUFKY: a fully functional PUF-based cryptographic key generator," In Lecture notes in computer science (LNCS):, Workshop on cryptographic hardware and embedded systems-CHES 2012, Berlin: Springer, vol. 7428, 2012.

[21] C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, "Physically uncloneable functions in the universal composition framework," In Lecture notes in computer science (LNCS), Advances in cryptology-CRYPTO 2011, Berlin: Springer, vol. 6841, pp. 51–70, 2011.

[22] E. Barker and J. Kelsey, "Recommendation for random number generation using deterministic random bit generators," NIST special publication 800-90A, 2012. http://csrc.nist.gov/publications/nistpubs/800-0A/SP800-90A.pdf.

[23] G. Swetha, "Temperature variation effects on asynchronous PUF design using FPGAs," Phd Thesis, University of Toledo, 2014. http://utdr-toledo.edu/theses-dissersions.

[24] R. Tauhidur, et al., "ARO-PUF: An aging-resistant ring oscillator PUF design," Proceedings of the conference on Design, Automation & Test in Europe, European Design and Automation Association, 2014.

[25] S. Mueelich and M. Bossert, "A New Error Correction Scheme for Physical Unclonable Functions," IEEE SCC 2017, Hamburg, Germany, 6-9 Feb. 2017.

[26] F. Ganji, S. Tajik, and J.-P. Seifert, "Fourier Analysis Based Attack against Physically Unclonable Functions," https://eprint.iacr.org/2017/551.pdf

[27] T. A. Soroceanu, "Security Analysis of Strong Physical Unclonable Functions," MSc Thesis, Berlin, 2017.

[28] S. Tajik, "On the physical security of physically unclonable functions," MSc thesis, TU Berlin, 2017.

Journal of Electronical & Cyber Defence
Vol. 6, No. 4, 2019, Serial No. 24

Design and Implementation of a Physically Unclonable Function on FPGA

E. Madadi, M. Masoumi*, A. Dehghan, A. Chamanmotlagh

*Islamic Azad University Islamshahr Branch

(Received: 28/09/2017 , Accepted: 27/05/2018)

ABSTRACT

One of the challenges in the hardware security is withstanding cloning and hardware duplication. In fact this attack aims hardware originality so the defense mechanism should be different from common system security and algorithm protection. Applying Physically Unclonable Functions (PUFs) is one of the most effective protection methods.

Physically Unclonable Functions (PUFs) are functions that generate a set of random responses when stimulated by a set of pre-defined requests or challenges. Since these challenge-response schemes extract hidden parameters of complex physical unpredictable properties of substrate materials, such as delay of interconnections and wiring in the CMOS process and devices, they are called physically unclonable functions. They are mainly used for electronic security purposes such as hardware verification and/or device authentication mechanisms, protection of sensitive intellectual property (IP) on devices and protection against insecure hardware connections and communications. PUF-based security mechanisms have some obvious advantages compared to traditional cryptography-based techniques, including more resistance against physical and side channel attacks and suitability for lightweight devices such as RFIDs.

In FPGA devices, PUFs are instantiated by exploiting the propagation delay differences of signals caused by manufacturing process variations. However, real implementation of PUFs on FPGAs is a big challenge given the fact that the resources inside FPGAs are limited, and that it is not easy to simulate the behavior of PUF using existing software tools. In addition, there are a few articles that explain details of the implementation of PUFs on FPGAs. In practice, it usually takes a long time to get a simple PUF to work both in simulations and on board.

In this work, we describe a practical realization of a ring-oscillator based PUF on Xilinx FPGAs and illustrate how such architecture is mapped into some FPGAs from this device family. Using this architecture, we obtain a unique 10-bit code which can be used to identify a chip between many similar devices of the same family in order to provide a reliable access control and authentication mechanism. Simulations are carried out using a dual core computer with 2 GHz clock frequency and 4 GBytes RAM memory.

Keywords: Hardware Security, Physically Unclonable Function, FPGA Implementation

* Corresponding Author Email: masoumi@iiau.ac.ir