مطالعه افزایش امنیت سخت افزار با استفاده از روش قفل گذاری منطقی

حسین فیروزی [۱]،کوروش منوچهری کلانتری [۲]

[۱] گروه مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)، پردیس گرمسار،ایران،

[۲]گروه مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)،پردیس گرمسار،ایران،

چکیده :

قفل‌گذاری منطقی به عنوان یکی از تکنیک‌های کلیدی در امنیت سخت‌افزار مطرح شده است که با هدف حفاظت از مدارهای مجتمع (IC) در برابر تهدیداتی مانند تولید غیرمجاز، مهندسی معکوس، و سرقت مالکیت فکری توسعه یافته است. با توجه به اهمیت روزافزون امنیت در صنعت سخت‌افزار، بررسی جامع و تحلیل دقیق کارهای پیشین در این حوزه اهمیت فراوانی دارد. این مقاله به مرور و تحلیل پژوهش‌های انجام‌شده در زمینه قفل‌گذاری منطقی می‌پردازد که بر اساس دسته‌بندی‌های مختلف این تکنیک‌ها سازماندهی شده‌اند.در این مقاله، ضمن مرور و تحلیل پژوهش‌های پیشین در هر یک از این دسته‌بندی‌ها، به‌طور ویژه به بررسی قفل‌های منطقی مبتنی بر LUT[1] پرداخته می‌شود و نتایج حاصل از این نوع قفل‌ها تحلیل می‌گردد. هدف اصلی این تحلیل، شناسایی نقاط قوت، محدودیت‌ها، و چالش‌های موجود در رویکردهای مختلف قفل‌گذاری منطقی است ، همچنین تحلیل جامعی از نتایج قفل‌های مبتنی بر LUT ارائه می‌شود.

کلمات کلیدی:

قفل‌گذاری منطقی ، امنیت سخت‌افزار ،مدارهای مجتمع ،مقاومت در برابر مهندسی معکوس

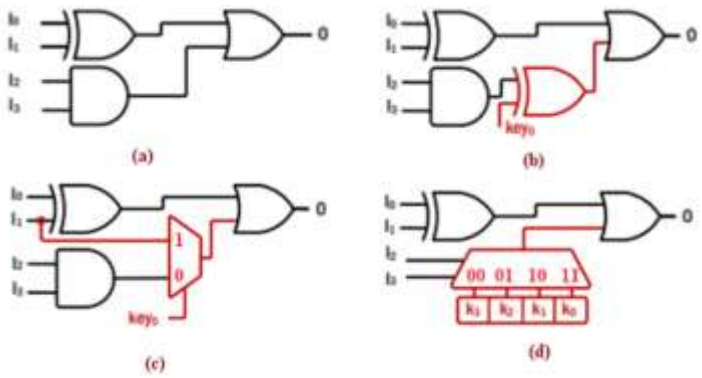
مقدمه :

امنیت سخت‌افزار به یکی از موضوعات مهم در طراحی و تولید مدارهای مجتمع (IC) تبدیل شده است، به ویژه در شرایط کنونی که زنجیره تأمین جهانی با چالش‌های امنیتی متعددی مواجه است. وابستگی به کارخانه‌های خارجی برای تولیدIC ها، نگرانی‌هایی از جمله تولید غیرمجاز، مهندسی معکوس، سرقت مالکیت معنوی (IP) و درج تروجان‌ها را به همراه داشته است.(Azar et al , 2024) این چالش‌ها نیاز به توسعه تکنیک‌های مؤثر برای حفاظت از طراحی‌ها و جلوگیری از سوءاستفاده‌های احتمالی را افزایش داده است. یکی از روش‌های مؤثر در این زمینه، قفل‌گذاری منطقی (Logic Locking) است که با افزودن یک یاچند قفل منطقی به مدار، از دسترسی غیرمجاز به طراحی اصلی جلوگیری می‌کند.قفل‌گذاری منطقی به عنوان یک رویکرد دفاعی در برابر تهدیدات امنیتی، به طور گسترده‌ای مورد توجه محققان و مهندسین قرار گرفته است. با این حال، ظهور حملات پیچیده‌ای مانند حملات مبتنی بر رضایت‌پذیری بولی (SAT[1]) نشان داده است که بسیاری از روش‌های سنتی قفل‌گذاری منطقی نسبت به این نوع حملات آسیب‌پذیر هستند. (Engels et al ,2022)در واکنش به این چالش‌ها، محققان به توسعه روش‌های جدید و مقاوم‌تری پرداخته‌اند که قادر به مقابله با حملات پیشرفته‌تر باشند. به عنوان مثال، تکنیک‌های قفل‌گذاری مبتنی بر جداول جستجو (LUT) مانند LUT-Lock معرفی شده‌اند (Kamali,et al 2018, که هدف آن‌ها افزایش امنیت بیت‌استریم‌های FPGA و سخت‌افزارهای ASIC در برابر مهندسی معکوس و سرقت مالکیت معنوی است. این روش با افزایش پیچیدگی فرآیند رفع ابهام، به طور قابل توجهی مقاومت در برابر حملات SAT را بهبود می‌بخشد.در این تحقیق، ما ابتدا یک دسته بندی جامع از قفل های منطقی ارائه می کنیم و سپس این دسته بندی ها را با هم مقایسه کرده و در ادامه به بررسی و تحلیل تکنیک‌های مختلف قفل‌گذاری منطقی بر اساس LUT ها می پردازیم .

[1] Satisfiability Attack

بخش دوم : تحلیل انواع روشهای قفل سخت افزاری

قفل‌گذاری منطقی سنتی یکی از اولین روش‌های امنیتی برای حفاظت از مدارهای مجتمع (IC) در برابر تهدیداتی مانند مهندسی معکوس و سرقت مالکیت معنوی است. این روش‌ها با افزودن ورودی‌های کلید به مدار، عملکرد صحیح مدار را به کلید وابسته می‌کنند و از دسترسی غیرمجاز جلوگیری می‌کنند. از روش‌های اولیه می‌توان به(Roy, Jarrod A.et al ,2008) EPIC ، قفل‌گذاری تصادفی RLL(Engels, et al.2022) و قفل‌گذاری مبتنی بر خطا FLL(M. Yasin, et al,2016) اشاره کرد. یکی از ساده‌ترین روش‌ها استفاده از گیت‌های XOR یا XNOR است که تأثیر کمی بر عملکرد مدار دارد اما در برابر حملات SAT آسیب‌پذیر است. روش دیگری استفاده از مالتی‌پلکسرها (MUX) است که اگرچه پیچیدگی طراحی را افزایش می‌دهد، همچنان در برابر SAT ضعیف استکه این پیاده سازی ها را در شکل ۱ می توانید مشاهده کنید . قفل‌گذاری منطقی با استفاده از ماشین حالت متناهی (FSM[2]) نیز وجود دارد که در مقاله HARPOON (Chakraborty, et al ,2009) معرفی شده و مقاومت نسبی در برابر حملات دارد. با این حال، این روش‌ها در برابر حملات(Azar et al ,2021) SAT توضیح داده شده، آسیب‌پذیر هستند. تکنیک‌های دفاعی جدیدتر مانند SARLock (M. Yasin et al, 2016) و Anti-SAT برای افزایش مقاومت در برابر حملات SAT معرفی شده‌اند. این تکنیک‌ها با پیچیده کردن مدار و افزودن گیت‌های مخفی، زمان و دشواری حملات SAT را افزایش می‌دهند. روش SFLL (Yasin, Muhammad, et al, 2019) نیز بخشی از مدار را قفل‌گذاری می‌کند که بدون کلید صحیح عملکرد ناقصی دارد. همچنین، حملات AppSAT (Shamsi, Kaveh, et al, 2017) به دنبال یافتن کلید تقریبی هستند که خروجی مدار را با دقت بالایی بازتولید کند. با وجود این روش‌های دفاعی، قفل‌گذاری منطقی سنتی به عنوان پایه‌ای برای روش‌های پیچیده‌تر به کار گرفته می‌شود، اما نیاز به توسعه روش‌های جدید برای مقابله با تهدیدات نوظهور همچنان وجود دارد.



شکل ۱ : نمونه های اولیه قفل های منطقی

در ادامه به دسته بندی قفل های منطقی می پردازیم .

۱. **قفل‌گذاری منطقی نقطه‌ای(Point-Functional Logical Locking) :** روشی در قفل‌گذاری منطقی است که با هدف محدود کردن دامنه ورودی‌های ممکن که نشان‌دهنده استفاده از کلید اشتباه هستند، طراحی شده است. این تکنیک عمدتاً برای افزایش مقاومت مدارهای مجتمع در برابر حملاتی نظیر حملات SAT توسعه یافته و با خراب‌کردن خروجی‌ها در صورت استفاده از کلید نادرست به‌صورت کنترل‌شده عمل می‌کند. استراتژی‌های اولیه

[2] Finite state machine

مانند SARLock (M. Yasin et al, 2016)و AntiSAT که پیچیدگی ساختار منطقی مدار را افزایش می‌دهند، از جمله روش‌های پایه در این تکنیک هستند. با این حال، این روش‌ها دارای نقاط ضعف ساختاری هستند که می‌توانند تحت حملاتی مانند Valkyrieآسیب پذیر هستند .

۲. **قفل‌گذاری منطقی مبتنی بر چرخه(Cyclic-Oriented Logical Locking)** : این روش با افزودن چرخه‌های ترکیبی به مدار، پیچیدگی آن را افزایش داده و مقاومت مدار را در برابر حملات مانند SAT افزایش می‌دهد. (Kolhe et al ,2019),(Gandhi et al , 2023) اما ایجاد مشکلات برای ابزارهای طراحی خودکار (CAD) و چالش‌های مربوط به سنتز و ارزیابی زمانی، از معایب اصلی این روش است. این تکنیک به دلیل هزینه‌ها و پیچیدگی‌های بالا، هنوز به‌طور گسترده در صنعت پذیرفته نشده است.

۳. **قفل‌گذاری منطقی زنجیره‌ای اسکن(Scan Chaining Logical Locking)** : این روش به‌ویژه در طراحی برای تست‌پذیری (DFT) استفاده می‌شود و امکان دسترسی به رجیسترها و حالت‌های داخلی مدار را فراهم می‌کند. (Azar,et al,2021)با وجود افزایش امنیت در برابر حملات، این روش می‌تواند پیچیدگی طراحی و سربار محاسباتی را افزایش دهد و با برخی محصولات EDA ناسازگار باشد.

٤. **قفل‌گذاری منطقی مبتنی بر LUT و مسیریابی(LUT/Routing-Oriented Logical Locking)** : این روش از قابلیت کامل پیکربندی جداول جستجو (LUTs) بهره می‌برد (Kolhe et al ,2019),(Gandhi et al , 2023)و مقاومت بالایی در برابر آسیب‌پذیری‌های شناخته‌شده دارد. اما پیچیدگی و هزینه‌های بالای پیاده‌سازی، استفاده از این روش را چالش‌برانگیز کرده است.

٥. **قفل‌گذاری منطقی ترتیبی(Sequential Logical Locking)** : این روش بر پایه ماشین‌های حالت متناهی (FSM) طراحی شده و با استفاده از توالی‌های پیچیده، امنیت را افزایش می‌دهد. Gandhi et al , 2023)) (Engels et al , 2022) این تکنیک در برابر حملات SAT مقاومت دارد اما با افزایش پیچیدگی طراحی و مساحت مدار روبرو است.

٦. **قفل‌گذاری تعاملی مبتنی بر زمان(Interactive Timing-Based Locking) :** قفل‌گذاری تعاملی مبتنی بر زمان با تغییر زمان‌بندی ثبت داده‌ها، مانند جایگزینی فلیپ‌فلاپ‌ها با لچ‌ها و تغییر در ساعت سیستم، تلاش می‌کند تا حملات زمان‌بندی مثل SAT را ناکارآمد کند. این روش مزایایی مانند مقاومت در برابر حملات SAT و پیچیده‌تر کردن فرآیند مهندسی معکوس دارد. اما در عین حال معایبی مانند آسیب‌پذیری در برابر حملات SMT و افزایش پیچیدگی طراحی و چالش‌های هماهنگی با ابزارهای EDA را نیز به همراه دارد.یکی از جدید ترین روش ها در این زمینه روش O'clock (Rahman, M. Sazadur et al, 2022)است که تا حد زیادی مشکلات مربوط به این دسته بندی را حل کرده است .

۷. **قفل‌گذاری منطقی در سطح بالاتر(Higher-Level Logical Locking) :** این روش به سطوح بالاتر طراحی مانند RTLو HLS پرداخته و امنیت بیشتری در برابر تهدیدات پیچیده فراهم می‌کند. اما با چالش‌هایی مانند افزایش پیچیدگی طراحی و نیاز به ابزارهای پیشرفته‌تر مواجه است که می‌تواند هزینه‌ها را افزایش دهد.

۸. **قفل های منطقی SFLL[3]:** این روش امنیتی برای مقابله با حملاتSAT ، حذف، و تقریب توسعه یافته است. (Gandhi et al , 2023) عملکرد آن بر مبنای تغییر بخشی از مدار و ایجاد خرابی کنترل‌شده در خروجی‌ها در صورت استفاده از کلید نادرست است. این کار با استفاده از ماژول "مکعب استریپر" انجام می‌شود که منطق "وارونه‌سازی و پنهان‌سازی" را در بازسازی مدار پیاده‌سازی می‌کند. مزیت این روش، مقاومت بالای آن در برابر حملات SAT است؛ اما معایب آن شامل پیچیدگی‌های پیاده‌سازی و نیاز به مدیریت دقیق الگوهای ورودی است.

۹. **قفل‌گذاری IP مبتنی برeFPGA :** این تکنیک برای محافظت از مالکیت معنوی (IP) در برابر حملات مبتنی بر یادگیری ماشین، به‌ویژه در لایه سیستم روی تراشه(SoC) ، توسعه یافته است. (Han et al , 2023). Engels) et al , 2022) این روش با استفاده از قفل‌گذاری منطقی مبتنی بر/LUT مسیریابی و طراحی متقارن بلوک‌های

[3] Stripped-Functionality Logic Locking

منطقی، حملات را دشوار می‌کند. مزیت اصلی آن، افزایش مقاومت مدار در برابر حملات I/O است، اما پیچیدگی اجرای آن نسبت به روش‌های سنتی بالاتر است.

۱۰. **فریم‌ورک‌های قفل‌گذاری منطقی :**فریم‌ورک‌هایی مانند LOTUS(Hashemi et al ,2024) به عنوان ابزارهای جامع برای پیاده‌سازی تکنیک‌های مختلف قفل‌گذاری معرفی شده‌اند. این فریم‌ورک‌ها قابلیت ترکیب و تنظیم چندین روش قفل‌گذاری را دارند و امنیت مدارها را در برابر حملات اوراکل‌محور، بدون اوراکل، و دیگر تهدیدات افزایش می‌دهند LOTUS .برای طراحی‌های بزرگ و چندماژولی مناسب است و از ویژگی‌هایی مانند قفل‌گذاری بین ماژولی و استفاده از کلیدهای نیمه‌پویا بهره می‌برد. اگرچه این فریم‌ورک‌ها امنیت و مقیاس‌پذیری بالایی دارند، اما پیچیدگی پیاده‌سازی و نیاز به دانش تخصصی از معایب آن‌هاست.

تحلیل دسته بندی های انجام شده : مقایسه‌ی دسته‌بندی‌های الگوریتم‌های قفل منطقی با توجه به معیارهایی مانند میزان امنیت، مقاومت در برابر حملات، پیچیدگی پیاده‌سازی، افزایش سخت‌افزاری، انعطاف‌پذیری، و موارد کاربرد انجام می‌شود. این مقایسه به ما کمک می‌کند تا مناسب‌ترین روش را با توجه به نیازهای خاص یک سیستم انتخاب کنیم. معیارها شامل ارزیابی سطح حفاظتی، توانایی مقابله با حملات مختلف مانند SAT و یادگیری ماشین، دشواری پیاده‌سازی، نیاز به منابع سخت‌افزاری اضافی، و قابلیت تنظیم و تطبیق هر روش با شرایط مختلف است.نتایج مرتبط با این مقایسه در جدول شماره ۱ آورده شده است .

جدول۱: تحلیل دسته بندی های قفل های منطقی

دسته‌بندی	میزان امنیت	مقاومت در برابر حملات	پیچیدگی پیاده‌سازی	سربار مکانی	موارد کاربردی
Primitive Logical Locking	پایین تا متوسط	ضعیف در برابر حملات SAT	پایین	کم	سیستم های ساده
Point-Functional Logical Locking	متوسط	مقاوم در برابر حملات SAT اولیه	پایین تا متوسط	کم تا متوسط	کاربرد های عمومی
Cyclic-Oriented Logical Locking	بالا	مقاوم در برابر انواع حملات	متوسط تا بالا	متوسط	سیستم هایی با نیاز امنیتی بالا
LUT/Routing-Oriented Logical Locking	بالا	بسیار مقاوم	بالا	بالا	طراحی های پیچیده و حساس
Scan Chaining Logical Locking	متوسط	وابسته به نوع پیاده سازی و تکنیک استفاده شده	متوسط	کم تا متوسط	سیستم با نیاز به تست پذیری بالا
Sequential Logical Locking	بالا	مقاوم در برابر حملات مبتنی بر حالت	بالا	متوسط	مدار های ترتیبی پیچیده
Interactive Timing-Based Locking	بالا	مقاوم در برابر حملات زمانی	بالا	متوسط تا بالا	سیستم های حساس به زمان

طراحی در سطوح انتزاعی بالاتر	کم تا متوسط	متوسط	متغیر بر اساس پیاده سازی	متوسط	**Higher-Level Logical Locking**
IP های حساس و قابل پیکربندی	بسیار بالا	بالا	بسیار مقاوم در برابر انواع حملات	بالا	**eFPGA-Oriented IP Locking**

بخش چهارم : قفل های منطقی مبتنی بر LUT :

در ادامه از بین دسته بندی بخش قبلی به صورت تخصصی تر فقط قفل های مبتنی بر LUT را بررسی می کنیم فلذا ابتدا یک توضیح کامل تر در مورد مبهم سازی قفل های منطقی می دهیم .مبهم‌سازی مبتنی بر LUT (LUT-Based Obfuscation) یکی از روش‌های نوین در زمینه امنیت سخت‌افزار است که به ویژه برای حفاظت ازFPGA ها و سخت‌افزارهای ASIC در برابر تهدیدات امنیتی همچون مهندسی معکوس، سرقت مالکیت معنوی(IP) ، و حملات SAT توسعه یافته است. این روش بر استفاده از جداول جستجو (LUT) برای مبهم‌سازی نت‌لیست‌ها و ایجاد ابهام در عملکرد مدار متمرکز است.

۴,۱-مبانی مبهم‌سازی مبتنی برLUT : مبهم‌سازی مبتنی بر LUT یک تکنیک مهم در افزایش امنیت طراحی‌های سخت‌افزاری است که در آن ازLUT ها به عنوان واحدهای پایه‌ای برای پیاده‌سازی منطق مدار استفاده می‌شود. هر LUT توانایی پیاده‌سازی یک تابع منطقی با چند ورودی را دارد، اما در مبهم‌سازی، اینLUT ها به گونه‌ای پیکربندی می‌شوند که عملکرد دقیق مدار برای مهاجمان مشخص نباشد. درFPGA ها پس از پیاده‌سازی یک مدار، تعدادی ازLUT ها ممکن است بلااستفاده باقی بمانند. اینLUT های بلااستفاده می‌توانند برای مبهم‌سازی منطق مدار به کار گرفته شوند و این کار باعث می‌شود که تحلیل و مهندسی معکوس مدار برای مهاجمان دشوارتر شود. یکی از چالش‌های اصلی در مبهم‌سازی مبتنی برLUT ، مقابله با حملات پیشرفته مانند حملات SAT است. استفاده ازLUT های بزرگ‌تر می‌تواند امنیت بالاتری را در برابر این حملات فراهم کند، اما این کار هزینه‌های طراحی را از نظر فضا و مصرف توان افزایش می‌دهد. کاهش اندازهLUT ها ممکن است هزینه‌های طراحی را کاهش دهد، اما به طور همزمان امنیت مدار را نیز به خطر می‌اندازد. درASIC ها ،استفاده ازLUT ها برای مبهم‌سازی منجر به افزایش سربار ناحیه و تأخیر می‌شود. به عنوان مثال، در فناوریCMOS ، سربار ناحیه‌ای که توسط عناصر حافظه یک LUTایجاد می‌شود، به صورت نمایی با افزایش تعداد ورودی‌ها افزایش می‌یابد. این موضوع تعدادLUT هایی را که می‌توانند به جای گیت‌های معمولی استفاده شوند، محدود می‌کند و ممکن است عملکرد مدار را تحت تأثیر قرار دهد. برای کاهش این چالش‌ها، پژوهش‌ها به سمت توسعه فناوری‌های جدیدی مانند STT و MTJ پیش می‌روند. این فناوری‌ها امکان ادغام بهتر LUTها با فناوری CMOS را فراهم می‌کنند و باعث کاهش قابل توجه سربار ناحیه می‌شوند. با ادغام این فناوری‌ها، می‌توان تعداد بیشتری ازLUT ها را بدون افزایش زیاد در ناحیه یا تأخیر مدار پیاده‌سازی کرد.

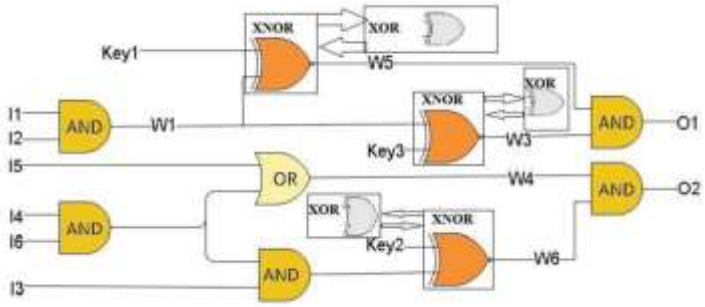
۴/۲-مرور منابع و روش ها قفل های مبتنی بر LUT :

۱. **بررسی روش STT و منطق قابل پیکربندی مجدد برای امنیت :** یکی از روش‌های نوین در حوزه امنیت سخت‌افزار، استفاده از منطق قابل پیکربندی مجدد مبتنی بر STT[4] است(Winograd et al ,2016) . این روش به عنوان یک راهکار برای افزایش امنیت در طراحی‌های مدارهای مجتمع خاص کاربردی (ASIC) مطرح شده و مزایای متعددی نسبت به روش‌های مبتنی بر SRAM و CMOS دارد. در این مقاله، نویسندگان با معرفی جدول جستجوی (LUT) مبتنی بر STT غیر فرّار و ادغام آن با گیت‌های سفارشیCMOS ، موفق به ایجاد یک طراحی مقاوم‌تر در برابر تهدیدات امنیتی مختلف، به ویژه حملات کانال جانبی شده‌اند.این روش علاوه بر ارائه توان نشتی کمتر و پایداری حرارتی بالاتر، مشکلات امنیتی مرتبط با حافظه‌های غیر فرّار خارجی را که در تکنولوژی‌های مبتنی بر CMOS و SRAMمشاهده می‌شود، برطرف می‌کند. نویسندگان همچنین یک جریان طراحی ترکیبی STT-CMOS با تمرکز بر

[4] Spin-Transfer Torque

امنیت پیشنهاد داده‌اند که نه تنها امنیت مدار را تضمین می‌کند، بلکه عملکرد و کارایی آن را نیز بهبود می‌بخشد.این رویکرد نشان‌دهنده‌ی پیشرفت‌های قابل توجهی در استفاده از فناوری STT برای افزایش امنیت در سیستم‌های نهفته است که دارای محدودیت‌های شدید در زمینه توان و عملکرد هستند.

۲. **پیکربندی جزئی پویا و به‌روزرسانی کلیدهای دینامیک در قفل‌گذاریLUT** :یکی از روش‌های پیشرفته در زمینه قفل‌گذاری منطقی که در مقالات اخیر مورد بررسی قرار گرفته است، استفاده از پیکربندی جزئی پویا برای به‌روزرسانی دینامیک کلیدهای قفل‌گذاری در طراحی‌های مبتنی بر LUT است. (Slowik et al ,2022) ، نویسندگان یک جریان طراحی امن برای ادغام مالکیت فکری شخص ثالث (3PIP[5]) در پلتفرم‌های FPGA پیشنهاد کرده‌اند که امکان به‌روزرسانی کلیدهای قفل را در طول چرخه حیات ۳ PIPفراهم می‌کند.در این روش، جداول جستجو (LUT) به عنوان بخش‌های قابل برنامه‌ریزی در FPGA مورد استفاده قرار می‌گیرند و با بهره‌گیری از پیکربندی جزئی پویا، امکان تغییر و به‌روزرسانی کلیدهای قفل‌گذاری در زمان اجرای برنامه فراهم می‌شود که می توانید نحوه نگاشت گیت های کلید را در شکل ۲ مشاهده کنید. در شکل ۲ مشاهده می کنید که مدار به دو بخش استاتیک و داینامیک تبدیل شده است و گیت هایی که خاصیت داینامیک دارند(.../XOR/XNOR/MUX) به آن ها کلید اعمال شده شده است . حال اگر این گیت ها با LUT جایگذاری شوند هم میتوانند خاصیت کلیدی داشته و مبهم سازی را ایجاد کنند . این روش علاوه بر بهبود امنیت مدارهای مجتمع در برابر حملاتSAT ، به دلیل نیاز به پیکربندی مجدد تنها در بخش‌های خاصی از مدار، کمترین اختلال را در عملکرد کلی سیستم ایجاد می‌کند.این رویکرد، همچنین امکان انعطاف‌پذیری بالاتری در مدیریت کلیدهای امنیتی فراهم می‌آورد و از آنجا که تنها بخش‌های مشخصی از FPGA به‌روزرسانی می‌شوند، سربار سخت‌افزاری و تأخیر ناشی از این فرآیند به حداقل می‌رسد. به‌روزرسانی دینامیک کلیدها با استفاده از این تکنیک، مقاومت مدار در برابر تهدیدات امنیتی را به طور چشمگیری افزایش می‌دهد و از سرقت مالکیت فکری و دسترسی غیرمجاز به مدارهای مجتمع جلوگیری می‌کند.



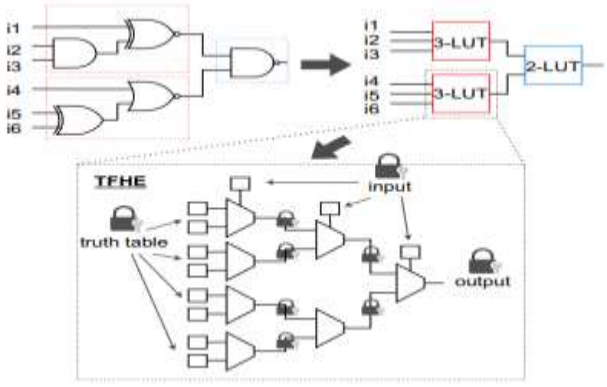
شکل ۲ :گیت های کلید نگاشت شده به بخش های قابل بازپیکربندی

۳. **LUT-Lockیک الگوریتم نوآورانه برای مبهم‌سازی منطق در FPGA وASIC** :یکی از روش‌های پیشرفته و نوآورانه در حوزه امنیت سخت‌افزار که در این مقاله معرفی شده است، LUT-Lockاست(Kamali et al , 2018). این الگوریتم به منظور افزایش امنیت بیت‌استریم‌های FPGA و سخت‌افزارهای ASIC در برابر تهدیداتی همچون مهندسی معکوس و سرقت مالکیت معنوی (IP) توسعه داده شده است LUT-Lock .با استفاده از جداول جستجوی (LUT) خاص، فرآیند مبهم‌سازی منطق را پیچیده‌تر کرده و مقاومت در برابر حملات SAT را به طور قابل توجهی افزایش می‌دهد.در این روش، الگوریتم پیشنهادی با استفاده استراتژیک ازLUT ها در طراحی مدار، به گونه‌ای عمل می‌کند که کمترین تأثیر را بر خروجی‌های اصلی مدار داشته باشد و در عین حال زمان لازم برای شکستن قفل‌های امنیتی توسط حملات SAT را به طور نمایی افزایش دهد. این افزایش مقاومت به لطف ترکیب چند ویژگی

[5] Third-Party Intellectual Property

کلیدی در الگوریتم، از جمله تمرکز بر مخروط فن-این(Fan-In Cones) ، گیت‌های با Skew بالاتر (High Skew Candidates)، گیت‌هایی با حداقل Fan-Out و اجتناب از قرار گرفتنLUT ها به صورت پشت‌سرهم(Non-Back-to-Back LUT placement)، به دست آمده است. LUT-Lock.در مقایسه با روش‌های قبلی، نه تنها توانسته است زمان اجرای حل‌کننده‌های SAT را برای شکستن مبهم‌سازی به شدت افزایش دهد، بلکه با کاهش سربار مساحت و بهبود عملکرد، یک راه‌حل قوی و کارآمد برای حفاظت از طراحی‌های حساس سخت‌افزار ارائه می‌دهد.

۴. **قفل‌گذاری منطقی مبتنی برTFHE : امنیت داده‌ها و الگوریتم‌ها در محیط‌های توزیع‌شده**:یکی از روش‌های نوین و پیشرفته در حوزه امنیت داده‌ها و الگوریتم‌ها که در این مقاله مورد بررسی قرار گرفته است (Suemitsu, et al (2024، استفاده از قفل‌گذاری منطقی مبتنی بر TFHE[6] برای حفاظت از داده‌ها و الگوریتم‌ها در محیط‌های توزیع‌شده است. این روش به طور خاص برای حفاظت از داده‌های کاربر و الگوریتم‌های یادگیری ماشین در برابر حملات امنیتی طراحی شده است و از ترکیب تکنیک‌های رمزنگاری هومومورفیک و مبهم‌سازی مبتنی بر LUT استفاده می‌کند.در این پروتکل، الگوریتم‌ها و داده‌های کاربر از طریق یک فرآیند قفل‌گذاری منطقی پیچیده محافظت می‌شوند که از TFHE برای رمزگذاری کلیدهای قفل‌گذاری استفاده می‌کند. این رویکرد به گونه‌ای طراحی شده که ارزیابی الگوریتم‌ها در محیط‌های توزیع‌شده بدون نیاز به افشای داده‌ها یا الگوریتم‌ها ممکن شود. به علاوه، این روش مقاومت بالایی در برابر حملات SAT و سایر حملات تحلیل زمانی دارد که به دلیل استفاده از ساختارهای مبتنی بر LUTو ترکیب آن‌ها با تکنیک‌های رمزنگاری پیشرفته TFHE است.که یک شکل مفهومی از روش ارائه شده را در شکل ۵ می توانید مشاهده کنید . در این شکل ورودی‌ها(i_1 تاi_6)و کلیدهای قفل‌گذاری منطقی که مقادیر جدول درستی هستند، رمزگذاری می‌شوند. مقدار خروجی رمزگذاری‌شده بدون نیاز به رمزگشایی به دست می‌آید. پروتکل پیشنهادی شامل چندین مرحله کلیدی است که از تولید کلید، انتقال کلید عمومی، مبهم‌سازی تابع، رمزگذاری مقادیرLUT ، ارزیابی و رمزگشایی نتایج رمزگذاری‌شده تشکیل شده است. هر یک از این مراحل به‌طور دقیق طراحی شده‌اند تا امنیت داده‌ها و الگوریتم‌ها را در برابر دسترسی‌های غیرمجاز تضمین کنند. این روش با حفظ حریم خصوصی و امنیت داده‌ها، امکان انجام محاسبات امن در محیط‌های توزیع‌شده را فراهم می‌کند و از آنجایی که امنیت کلیدهای قفل‌گذاری با استفاده از TFHE تضمین می‌شود، حتی در صورت دسترسی فیزیکی به سیستم، امکان استخراج کلید و دستیابی به اطلاعات محافظت‌شده وجود ندارد. علاوه بر این، این پروتکل به دلیل استفاده از ساختارهای مبتنی بر LUT و مقاومت بالا در برابر حملاتSAT ، به عنوان یک راهکار قوی برای حفاظت از الگوریتم‌ها در برابر تهدیدات امنیتی شناخته می‌شود.



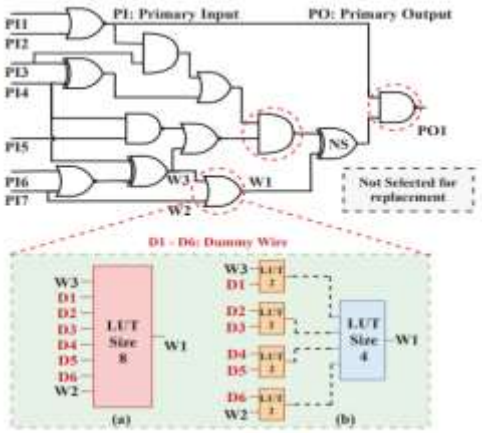
شکل ۳: مرور مفهومی از قفل‌گذاری منطقی مبتنی بر LUT پیشنهادی بر روی TFHE

[6] Fully Homomorphic Encryption over the Torus

۵. **روش ELBO[7] و HLRO[8] :**در مقاله(Chowdhury,,2021)، دو روش نوآورانه برای بهبود مبهم‌سازی مدارهای منطقی بر اساس بلوک‌های قابل پیکربندی مجدد) مانندLUT ها (معرفی شده است که هدف آن‌ها افزایش مقاومت در برابر حملات SAT و کاهش هزینه‌های طراحی است. این دو روش شامل Enhanced 2-Stage LUT-Based Obfuscation (ELBO)و Hybrid Logic-Routing Obfuscation (HLRO)هستند.روش ELBOبا به کارگیری معیارهای تست‌پذیری مدارات دیجیتال، به انتخاب بهینه مکان‌های جایگزینیLUT ها و ورودی‌های جایگزین پرداخته و از الگوریتم‌های مرتبط با تحلیل مشاهده‌پذیری و کنترل‌پذیری برای افزایش مقاومت در برابر حملات SATاستفاده می‌کند. در این روش، مکان جایگزینیLUT ها به نحوی انتخاب می‌شود که حداکثر فاصله همینگ بین خروجی صحیح و خروجی به دست آمده با کلید نادرست ایجاد شود، و همچنین ورودی‌های جایگزین به گونه‌ای انتخاب می‌شوند که تعداد تکرارهای حمله SAT افزایش یابد.در مقابل، روش HLROبا ترکیب بلوک‌های LUT با شبکه‌های کلیدپذیر (Switch Boxes) و مسیریابی(CLNs) ، به ایجاد فرم‌های SAT-hard می‌پردازد که نه تنها مقاومت در برابر حملات SAT را افزایش می‌دهد، بلکه هزینه‌های طراحی را نیز کاهش می‌دهد. این روش با کاهش تعدادLUT های مورد نیاز و ایجاد فرم‌های پیچیده‌تر، می‌تواند همان سطح مقاومت در برابر حملات SAT را با هزینه‌های کمتری نسبت به روش‌های پیشین فراهم کند.این مقاله نشان می‌دهد که با استفاده از روش‌های ELBO وHLRO ، می‌توان به طور قابل توجهی زمان اجرای حملات SAT را افزایش داد و در عین حال، سربار مساحت طراحی را به نصف کاهش داد. این روش‌ها به طور گسترده‌ای در طراحی‌های مداری با امنیت بالا و کاربردهای حساس مورد استفاده قرار می‌گیرند.

٦. **مبهم‌سازی ترکیبی مبتنی بر LUT سفارشی :**مقاله (Kolhe et al , 2019)با هدف بهبود تکنیک‌های مبهم‌سازی مبتنی بر LUT و افزایش امنیت در برابر حملاتSAT ، یک روش طراحی LUT سفارشی را پیشنهاد می‌دهد که شامل مراحلی است.ابتدا، یک LUT دو ورودی در کنار یک LUT بزرگ‌تر قرار داده می‌شود. این ترکیب به گونه‌ای طراحی شده که LUT کوچک‌تر مسئولیت مبهم‌سازی مسیریابی را بر عهده دارد و LUT بزرگ‌تر مسئولیت مبهم‌سازی منطق را ایفا می‌کندکه این اقدام را در شکل ٤ میتوانید مشاهده کنید . این تنظیمات منجر به افزایش امنیت مدار می‌شود، زیرا فضای جستجوی کلید برای حملات SAT به طور قابل توجهی بزرگ‌تر می‌شود.در مرحله بعد، برای نمایش LUTها در فرآیند مبهم‌سازی، از مالتی‌پلکسرها (MUX) استفاده می‌شود. هر LUT به صورت یک MUX مدل‌سازی می‌شود که این امر باعث افزایش پیچیدگی محاسباتی مورد نیاز برای حل مسئله SAT می‌شود. این کار به افزایش مقاومت مدار در برابر حملات کمک می‌کند.در نهایت، این ساختار سفارشی به گونه‌ای طراحی شده که بدون کاهش امنیت، هزینه‌های طراحی را کاهش دهد. این روش با افزایش فضای جستجوی کلید و کاهش سربارهای طراحی (از جمله مساحت و توان)، به عنوان یک راه‌حل عملی و موثر برای امنیت سخت‌افزار ارائه شده است.نمای کلی پیاده سازی این ایده را می توانید در شکل شماره ۴ ببینید

[7] Enhanced 2-Stage LUT-Based Obfuscation
[8] Hybrid Logic-Routing Obfuscation



شکل ۴ : جایگزینی گیت با استفاده از LUT (a) سنتی با اندازه ۸،(b). LUT سفارشی‌شده با اندازه ٤ و ٤ عدد LUT دو ورودی.

تحلیل متد های مبتنی بر LUT:روش استفاده از واحدهای LUT مبتنی بر STT باعث کاهش چشمگیر تأثیر بر عملکرد، توان و مساحت مدارها شده و امنیت طراحی در برابر حملات مهندسی معکوس را به میزان زیادی افزایش می‌دهد. اما از معایب این روش می‌توان به پیچیدگی بیشتر در طراحی و پیاده‌سازی اشاره کرد که ممکن است نیازمند منابع و زمان بیشتری باشد. این روش ممکن است در مدارهای کوچک‌تر و با منابع محدود، عملکرد بهینه‌ای نداشته و باعث افزایش سربار هزینه‌ها و پیچیدگی‌ها شود.در روش کلیدهای دینامیک در قفل‌گذاریLUT نتایج نشان می‌دهد که این روش با استفاده از LFSR و جریان‌های جزئی، امنیت قفل‌گذاری را بهبود می‌بخشد. همچنین، فاصله همینگ ۵۰ درصدی بین خروجی‌های درست و نادرست نشان می‌دهد که طراحی قفل‌گذاری شده قادر است حملات مبتنی بر کلید نادرست را دفع کند.

از معایب این روش می‌توان به پیچیدگی بیشتر در مدیریت کلیدها و نیاز به زیرساخت‌های امنیتی مناسب برای انتقال ایمن کلیدها اشاره کرد. علاوه بر این، فرآیند به‌روزرسانی دینامیک کلیدها می‌تواند منجر به افزایش پیچیدگی طراحی و مشکلات در زمان اجرای واقعی شود.روش LUT-lock در مقایسه با روش‌های قبلی، مقاومت بسیار بالاتری در برابر حملات SAT دارد و زمان اجرای حمله به صورت نمایی افزایش می‌یابد. با این حال، افزایش سربار مساحت و توان در طراحی‌های پیچیده از معایب اصلی این روش است.همچنین نیاز به انتخاب دقیق جایگزینی‌هایLUT ها نیز می‌تواند طراحی را پیچیده‌تر و زمان‌بر کند، که این امر ممکن است عرضه محصول را به تعویق بیندازد

روش Logic Locking over TFHE برای حفاظت از داده‌ها و الگوریتم‌ها در محیط‌های توزیع‌شده به کار می‌رود. آزمایش‌ها نشان داد که این روش در برابر حملات SAT بسیار مقاوم است و زمان اجرای حمله را به شدت افزایش می‌دهد. همچنین، سربار عملکرد ایجاد شده توسط قفل‌گذاری منطقی TFHE حداقل بوده و تأثیر قابل توجهی بر عملکرد کلی ندارد. با این حال، یکی از معایب اصلی این روش، پیچیدگی محاسباتی بالای TFHE است که می‌تواند زمان اجرای محاسبات را در کاربردهای بزرگ‌تر و پیچیده‌تر افزایش دهد. همچنین، نیاز به منابع محاسباتی قابل توجهی دارد که ممکن است در سیستم‌هایی با محدودیت منابع چالش‌برانگیز باشد.در روش مبهم‌سازی ترکیبی مبتنی بر LUT سفارشی ،نتایج نشان می‌دهد که استفاده از LUTهای سفارشی با اندازه‌های مختلف می‌تواند امنیت را افزایش داده و در عین حال سربارهای طراحی را کاهش دهد. با این حال، استفاده ازLUT های بزرگ‌تر باعث افزایش پیچیدگی و هزینه‌های طراحی می‌شود.

نیاز به تنظیم دقیق اندازه و تعدادLUT ها برای بهینه‌سازی امنیت و سربار، ممکن است زمان‌بر و پیچیده باشد که این موضوع می‌تواند در پروژه‌های با زمان محدود چالش ایجاد کند.دو تکنیک ELBO وHLRO توانسته‌اند با کاهش تعداد گیت‌های جایگزین شده، هزینه‌های طراحی را به طور قابل توجهی کاهش دهند. با این حال، با وجود بهبودهای امنیتی، همچنان نیاز به منابع محاسباتی و زمان بیشتری برای پیاده‌سازی و اجرای تکنیک‌های ELBO و HLRO وجود دارد. همچنین، این روش‌ها ممکن است برای مدارهای کوچک و با منابع محدود کمتر مناسب باشند و پیچیدگی‌های بیشتری را به طراحی اضافه کنند.برای

تحلیل بهتر و دقیق‌تر روش‌ها و متدها، به مقایسه آن‌ها بر اساس معیارهای مشترکی که در نظر گرفته‌ایم می‌پردازیم. این معیارها شامل مقاومت در برابر حملاتSAT ، که یکی از معیارهای اصلی برای سنجش امنیت مدارهای مبهم‌سازی شده است؛ سربار مساحت، که نشان‌دهنده میزان افزایش مساحت مدار به دلیل استفاده از تکنیک مبهم‌سازی است؛ سربار توان، که میزان افزایش مصرف توان را به دلیل به‌کارگیری این تکنیک‌ها ارزیابی می‌کند؛ و پیچیدگی طراحی و پیاده‌سازی، که به میزان دشواری و پیچیدگی در پیاده‌سازی و طراحی روش‌های ارائه‌شده می‌پردازد.

جدول شماره ۲:مقایسه ی روش های مبتنی بر LUT

متد ها	مقاومت در برابر حملاتSAT	سربار مساحت	سربار توان	پیچیدگی طراحی و پیاده‌سازی
Logic Locking over TFHE	بسیار بالا	متوسط	متوسط	بالا
Dynamic Key Updates for LUT	بالا	بالا	بالا	متوسط
LUT-Lock	بسیار بالا	بالا	بالا	بالا
Hybrid STT-CMOS Designs	بسیار بالا	پایین	پایین	بسیار بالا
Customized LUT-based Obfuscation	بالا	متوسط	متوسط	متوسط
HLROوELBO	بسیار بالا	متوسط	متوسط	متوسط

بخش پنجم :نتایج

انتخاب روش قفل‌گذاری منطقی به‌طور مستقیم به نیازها و محدودیت‌های خاص هر سیستم بستگی دارد. اگر هزینه و پیچیدگی کم اهمیت دارد و امنیت بالا مورد نیاز است، روش‌هایی مانند LUT/Routing-Orientedیا eFPGA-Oriented گزینه‌های مناسبی هستند که سطح بالایی از امنیت را فراهم می‌کنند. اگر دستیابی به توازن بین امنیت و هزینه مد نظر باشد، می‌توان از روش‌هایی مانند Point-Functionalیا Cyclic-Orientedاستفاده کرد که امنیت مطلوبی را با هزینه‌های معقول فراهم می‌کنند.برای سیستم‌هایی که تست‌پذیری و عیب‌یابی اهمیت بالایی دارند، روش Scan Chaining Logical Locking با تدابیر امنیتی اضافی می‌تواند انتخاب خوبی باشد. همچنین، در طراحی‌هایی که به توسعه سریع نیاز دارند و انعطاف‌پذیری در اولویت است، روش Higher-Level Logical Lockingگزینه مناسبی است. علاوه بر این، در بسیاری از موارد، ترکیب چندین روش قفل‌گذاری می‌تواند امنیت و کارایی را به طور چشمگیری افزایش دهد.

روش‌های مبتنی بر LUT یکی از رویکردهای پیشرفته و موثر برای مبهم‌سازی مدارها هستند. اگر مقاومت در برابر حملات SATبا کمترین پیچیدگی طراحی اولویت اصلی باشد، روش‌های ELBOو HLROبه دلیل دستیابی به سطح بالایی از امنیت با سربار کمتر، گزینه‌های مناسبی هستند. این روش‌ها با کاهش تعداد گیت‌های جایگزین شده، امنیت را بهبود می‌بخشند و هزینه‌های طراحی را به طور قابل توجهی کاهش می‌دهند.برای سیستم‌هایی که کاهش سربار توان و مساحت اهمیت بیشتری دارد، Hybrid STT-CMOS Designsبهترین انتخاب است. این روش با حفظ امنیت بالا، سربارهای مرتبط با توان و

مساحت را به حداقل می‌رساند و به‌ویژه در طراحی‌های با منابع محدود بسیار مؤثر است.اگر انعطاف‌پذیری در پیاده‌سازی و سطح بالای امنیت در محیط‌های مختلف مورد نظر باشد، روش‌های LUT-Lock و Dynamic Key Updates for LUT گزینه‌های مناسبی هستند، اگرچه این روش‌ها ممکن است با افزایش سربار مساحت و توان همراه باشند. این روش‌ها به‌ویژه در طراحی‌هایی که نیاز به امنیت بالا دارند اما پیچیدگی طراحی و پیاده‌سازی قابل قبول است، کاربرد دارند.در نهایت، ترکیب چندین روش مبتنی بر LUT با یکدیگر یا با سایر روش‌های قفل‌گذاری، می‌تواند به طور قابل توجهی امنیت سیستم را در برابر حملات مختلف افزایش داده و از هزینه‌ها و سربارهای غیرضروری جلوگیری کند.توصیه نهایی این است که قبل از انتخاب هر روش قفل‌گذاری مبتنی برLUT ، تحلیل دقیقی از نیازهای امنیتی، محدودیت‌های سخت‌افزاری، هزینه‌ها و کاربرد مورد نظر انجام شود تا بتوان به بهترین تصمیم دست یافت

منابع:

Roy, Jarrod A., Farinaz Koushanfar, and Igor L. Markov. "EPIC: Ending piracy of integrated circuits." In *Proceedings of the conference on Design, automation and test in Europe*, pp. 1069-1074. 2008.

Engels, Susanne, Max Hoffmann, and Christof Paar. "A critical view on the real-world security of logic locking." Journal of Cryptographic Engineering 12, no. 3 (): 229-244. 2022,

Pecht, Michael, and Sanjay Tiku. "Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics." *IEEE spectrum* 43, no. 5 37-46. 2006

Azar, Kimia Zamiri, Hadi Mardani Kamali, Houman Homayoun, and Avesta Sasan. "From cryptography to logic locking: A survey on the architecture evolution of secure scan chains." *IEEE Access* 9 (2021): 73133-73151.

M. Yasin, B. Mazumdar, J. Rajendran, O. Sinanoglu, SARLock: SAT attack resistant logic locking, in Hardware Oriented Security and Trust (HOST) Symposium, (), pp. 236–241, 2016.

L. Li, A. Orailoglu, JANUS: Boosting logic obfuscation scope through reconfgurable FSM synthesis, in IEEE International Symposium on Hardware Oriented Security and Trust (HOST), (), pp. 1–11, 2021.

Hashemi, Mona, Siamak Mohammadi, and Trevor E. Carlson. "LOTUS: A Scalable Framework to Lock Multi-Module Designs With One-Time Key and Self-Destructive Approaches." *IEEE Embedded Systems Letters* (2024).

Chakraborty, Rajat Subhra, and Swarup Bhunia. "HARPOON: An obfuscation-based SoC design methodology for hardware protection." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 28, no. 10 (): 1493-1502, 2009.

Azar, Kimia Zamiri, Hadi Mardani Kamali, Houman Homayoun, and Avesta Sasan. "From cryptography to logic locking: A survey on the architecture evolution of secure scan chains." IEEE Access 9 (): 73133-73151, 2021.

Kamali, Hadi Mardani, Kimia Zamiri Azar, Kris Gaj, Houman Homayoun, and Avesta Sasan. "Lut-lock: A novel lut-based logic obfuscation for fpga-bitstream and asic-hardware protection." In *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 405-410. IEEE, 2018.

Yasin, Muhammad, Chongzhi Zhao, and Jeyavijayan JV Rajendran. "SFLL-HLS: Stripped-functionality logic locking meets high-level synthesis." In *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1-4. IEEE, 2019.

Han, Zhaokun, Mohammed Shayan, Aneesh Dixit, Mustafa Shihab, Yiorgos Makris, and Jeyavijayan JV Rajendran. "{FuncTeller}: How Well Does {eFPGA} Hide Functionality?." In 32nd USENIX Security Symposium (USENIX Security 23), pp. 5809-5826. 2023.

Shamsi, Kaveh, Meng Li, Travis Meade, Zheng Zhao, David Z. Pan, and Yier Jin. "AppSAT: Approximately deobfuscating integrated circuits." In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 95-100. IEEE, 2017.

Xie, Yang, and Ankur Srivastava. "Anti-SAT: Mitigating SAT attack on logic locking." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 38, no. 2 (2018): 199-207.

Limaye, Nimisha, Satwik Patnaik, and Ozgur Sinanoglu. "Valkyrie: Vulnerability assessment tool and attack for provably-secure logic locking techniques." IEEE Transactions on Information Forensics and Security 17 744-759. (2022)

Winograd, Theodore, et al. "Hybrid STT-CMOS designs for reverse-engineering prevention." *Proceedings of the 53rd Annual Design Automation Conference*. 2016.

Gandhi, Jugal, Diksha Shekhawat, M. Santosh, and Jai Gopal Pandey. "Logic locking for IP security: A comprehensive analysis on challenges, techniques, and trends." *Computers & Security* 129 (): 103196. 2023,

Slowik, Jakub, et al. "Dynamic key updates for LUT locked design." *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2022.

Suemitsu, Kohei, et al. "Logic Locking over TFHE for Securing User Data and Algorithms." *2024 29th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2024.

Chowdhury, Subhajit Dutta, Gengyu Zhang, Yinghua Hu, and Pierluigi Nuzzo. "Enhancing SAT-attack resiliency and cost-effectiveness of reconfigurable-logic-based circuit obfuscation." In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1-5. IEEE, 2021.

Kolhe, Gaurav, Hadi Mardani Kamali, Miklesh Naicker, Tyler David Sheaves, Hamid Mahmoodi, PD Sai Manoj, Houman Homayoun, Setareh Rafatirad, and Avesta Sasan. "Security and complexity analysis of LUT-based obfuscation: From blueprint to reality." In *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1-8. IEEE, 2019.

Rahman, M. Sazadur, Rui Guo, Hadi M. Kamali, Fahim Rahman, Farimah Farahmandi, Mohamed Abdel-Moneum, and Mark Tehranipoor. "O'clock: lock the clock via clock-gating for soc ip protection." In *Proceedings of the 59th ACM/IEEE Design Automation Conference*, pp. 775-780. 2022

Abstract:

Logical locking has emerged as a key technique in hardware security, aimed at protecting integrated circuits (ICs) from threats such as unauthorized production, reverse engineering, and intellectual property theft. Given the increasing importance of security in the hardware industry, a comprehensive review and detailed analysis of previous works in this area is crucial. This paper reviews and analyzes research conducted on logical locking, organized based on different classifications of these techniques. In particular, this paper focuses on the examination of LUT-based logic locks (LUT), and the results of these types of locks are analyzed. The main goal of this analysis is to identify the strengths, limitations, and challenges in various logical locking approaches. Additionally, a comprehensive analysis of the results of LUT-based locks is presented.