

ارائه حمله تحلیل توان همبستگی روی پیاده‌سازی سخت‌افزاری رمز احراز اصالت شده OCB

محسن جهانبانی^۱، زین‌العابدین نوروزی^۲، منصور باقری^۳

^۱دانش آموخته مقطع دکتری ریاضی - رمز، دانشگاه جامع امام حسین (ع)، mjahanbani@ihu.ac.ir

^۲نویسنده مسئول) دانشیار، دانشگاه جامع امام حسین (ع)، znoroz@ihu.ac.ir

^۳نویسنده مسئول) دانشیار، دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، nbagheri@srttu.edu

چکیده

طراحی رمزهای احراز اصالت شده جدید با هدف ایجاد یکپارچگی بین دو سرویس محرمانگی و جامعیت داده ایجاد شده‌اند. اخیراً مسابقه سزار به منظور طراحی این رمزها برگزار و ۶ طرح به عنوان برنده نهایی انتخاب شده‌اند. یکی از معیارهای ارزیابی این رمزها علاوه بر امنیت تئوری، امنیت در برابر حملات کانال جانبی است که تاکنون کمتر مورد توجه قرار گرفته است. رمز احراز اصالت شده OCB به عنوان یکی از برندگان مسابقه سزار دارای ویژگی‌های امنیتی خاص نظیر استفاده از ساختار رمزهای قالبی تنظیم پذیر در طرح می‌باشد که انجام حملات کانال جانبی را با چالش روبرو می‌نماید. در این مقاله برای اولین بار، یک طرح حمله تحلیل توان همبستگی ۷ مرحله‌ای در زمان پردازش تک‌شمار، ارائه شده است. برای این هدف، رمز OCB به صورت سخت‌افزاری روی برد SAKURA-G پیاده‌سازی شده است. با کمک اثرهای ثبت شده ناشی از توان مصرفی S-box، حمله تحلیل توان CPA با مدل نشت توان مقدار-صفر به صورت موفق اجرا و تمامی بایتهای کلید بازیابی شده است.

کلیدواژه

رمز احراز اصالت شده OCB، تحلیل توان همبستگی، مسابقه سزار، SAKURA-G

مقدمه

حق مالکیت برخی طرح‌ها، تنها رمز AES-GCM [۳] پرکاربردترین رمز برای AE است. با این حال چندین آسیب-پذیری توسط جامعه رمزنگاری نیز برای این رمز شناخته شده است [۴]، [۵].

در ژانویه ۲۰۱۳ مسابقه سزار^۵ [۶] با هدف طراحی رمز-های AE که نسبت به AES-GCM برتر بوده و دارای گستردگی کاربرد باشند، شروع شد. تعداد ۵۷ طرح در مارس ۲۰۱۴، به مسابقه ارسال شدند. در ژوئیه ۲۰۱۶ کمیته برگزاری مسابقه سزار، سه کاربرد را به منظور دسته‌بندی نامزدها مشخص کرد. در مارس ۲۰۱۹ برندگان نهایی برای هر مورد کاربرد اعلام شد. رمز-های ACORN [۷] و ASCON [۸] برای کاربردهای سبک‌وزن، رمزهای AEGIS [۹] و OCB برای کاربردهای با سرعت بالا و رمزهای COLM [۱۰] و Deoxy [۱۱] برای امنیت دفاع در عمق در سناریوهای کاربرد نادرست^۶ انتخاب شده است [۶].

در حوزه رمزهای AE می‌توان در سه زمینه طراحی الگوریتم، تحلیل و ارزیابی امنیتی و تحلیل و ارزیابی حوزه پیاده‌سازی فعالیت نمود. یکی از موارد قابل بررسی در حوزه پیاده‌سازی سخت‌افزاری برندگان مسابقه سزار، ارزیابی مقاومت آن‌ها در برابر حملات کانال جانبی است. درحالی‌که تعداد زیادی ارزیابی

رمزهای احراز اصالت شده، محرمانگی^۱ (AE)، جامعیت و احراز هویت را به صورت هم‌زمان فراهم می‌کنند. ورودی یک رمز AE شامل کلید، تک‌شمار^۲ (N)، داده همراه^۳ (AD) و متن اصلی و خروجی آن اغلب متن رمز می و برچسب^۴ است. رمزگشایی، معکوس فرآیند فوق بوده و کلید، تک‌شمار، داده همراه، متن-رمزی و برچسب را دریافت و خروجی آن یکی از دو مقدار متن-اصلی یا پیام خطا است.

روش سنتی برای رسیدن به چنین ساختاری ترکیب چندین اولیه رمزنگاری است. معمولاً الگوریتم رمزنگاری برای محرمانگی و کدهای احراز اصالت برای جامعیت و احراز اصالت استفاده می-گردد. ترکیب عمومی علاوه بر این که از لحاظ عمل کرد غیربهبوده است، ممکن است با خطای پیاده‌سازی هم همراه شود. بنابراین چندین مُد کاری برای رمزهای قالبی طراحی شده تا یک ساختار رمز احراز اصالت شده کارآمد و امن مانند CCM [۱] و OCB [۲] را فراهم کند. به علاوه به جز مدهای کاری، طرح‌های اختصاصی نیز وجود دارند. با وجود این که طرح‌های AE مختلفی در گذشته طراحی شده بود، اما به دلیل گسترده نبودن پشتیبانی و داشتن

Tag[†]
CAESAR[‡]
Misused[¶]

Authenticated Encryption^¹
Nonce^²
Associated Data^³

آزمون نشت t انجام و نشان دادند این رمزها در برابر این حمله آسیب پذیر بوده ولی به طور مستقیم مسیر حمله تحلیل توان را برای این رمزها ارائه ندادند. سپس رمزها با پیاده سازی آستانه ای محافظت شدند و با آزمون t آسیب پذیری طرحها بررسی نمودند. همچنین آن‌ها کارایی رمزها را برحسب معیارهای نرخ گذردهی و مصرف سطح در دو حالت محافظت نشده و محافظت شده مقایسه نمودند.

نوآوری

رمز احراز اصالت شده^{۱۴} OCB [λ] یکی از برندگان نهایی مسابقه سزار است که از رمز AES به عنوان اولیه استفاده می کند و برای کاربرد سرعت بالا انتخاب شده است. با وجود اینکه تاکنون آسیب پذیری امنیتی برای این رمز گزارش نشده است اما بررسی برای تحلیل آسیب پذیری این رمز در برابر حملات تحلیل توان نیز انجام نشده است. بنابراین در این تحقیق اولین حمله تحلیل توان به این رمز ارائه می شود. رمز OCB دارای ویژگی های امنیتی خاصی است که حملات تحلیل توان را نسبت به دیگر رمزها دشوار می نماید. از جمله این ویژگی های امنیتی ترکیب مقادیر نامعلوم و متغیر Δ با ورودی های AES در تمام بخش های رمز به جز در مرحله پردازش تک شمار است. اما اجرای حمله در مرحله پردازش تک شمار نیز به دلیل ثابت بودن تعدادی از بیت های تک شمار به سادگی قابل اجرا نیست. بنابراین در این کار برای حل این مشکل، یک طرح حمله ۷-مرحله ای ارائه شده است. نتایج حمله نیاز به اقدامات متقابل را نیز تأیید می کند.

ساختار مقاله

ساختار بقیه مقاله به این شرح است که در قسمت ۲ مروری بر ادبیات موضوع شامل حمله تحلیل توان و رمز احراز اصالت شده OCB به صورت مختصر انجام شده است. در قسمت ۳، طرح حمله تحلیل توان علیه رمز OCB ارائه شده است. نتایج پیاده سازی طرح حمله به سخت افزار در قسمت ۴ ارائه شده است. در قسمت ۵، نتیجه گیری نهایی و پیشنهاد کارهای آتی بیان شده است.

ادبیات موضوع

در این بخش مفاهیم تحلیل توان و مشخصات رمز OCB ارائه می شود.

سخت افزاری برای برندگان این مسابقه وجود دارد اما تاکنون حملات فیزیکی به خصوص حملات تحلیل توان کم تر مورد توجه قرار گرفته است.

حملات تئوری مانند حملات آماری، خطی و تفاضلی به الگوریتم رمز شناخته شده ای مانند AES ممکن است به سختی یک حمله جستجوی جامع کلید باشد، اما این الگوریتم در دنیای واقعی ممکن است روی وسائلی پیاده سازی شود که بتوان مثلاً از طریق حملات کانال جانبی مانند تحلیل توان، تمامی مقادیر حساس آن را بازیابی نمود. بنابراین رمزهای AE هم از این قاعده مستثنی نبوده و باید در این زمینه ارزیابی شوند.

کارهای مرتبط

آدومنیکی^۷ و همکاران [۱۲] مقاومت دو برنده نهایی سبک وزن ACORN و ASCON را در برابر حملات تحلیل توان بررسی کردند. این ارزیابی روی پیاده سازی نرم افزاری و میکروکنترلر ARM با پردازنده مدل Cortex-m3 انجام شده است. نتایج پیاده سازی آن‌ها نشان داد، حملات تحلیل توان علیه رمز ASCON در مراحل مقداردهی اولیه و پایانی به صورت بدیهی قابل انجام است. همچنین به دلیل این که رمز ACORN دارای ساختار رمزهای جریان است و در این رمزها جریان کلید مستقل از متن اصلی محاسبه می شود، حملات کانال جانبی علیه مرحله رمزنگاری قابل انجام نیست ولی در مرحله مقداردهی اولیه یا مکانیزم هم زمان سازی مجدد قابل انجام است. نتایج آن‌ها نیاز به محافظت این دو رمز را در پیاده سازی نشان داد. بنابراین یک رمز پوشانه گذاری^۸ اختصاصی برای این دو رمز ارائه دادند.

ساموئل^۹ و دیمن^{۱۰} [۱۳] حمله تحلیل توان را علیه رمز Keyak [۱۴] (نامزد دور سوم) و ASCON (از برندگان مسابقه سزار) انجام دادند. هر دو رمز دارای ساختار اسفنجی^{۱۱} بوده و از یک نوع S-box استفاده می کنند. بنابراین در هر دو رمز حمله به S-box انجام شده است. همچنین گراس^{۱۲} و همکاران [۱۵] برای رمز ASCON، چند نوع پیاده سازی سخت افزاری ارائه داده و نشان دادند که محافظت این رمز در برابر حملات تحلیل توان به روش پیاده سازی آستانه ای به آسانی قابل انجام است.

اخیراً دیل^{۱۳} و همکاران [۱۶] بر روی تعدادی از نامزدهای دور سوم و برندگان مسابقه سزار شامل ACORN، JAMBU [۱۷]، SILC [۱۸]، CLOC [۱۸]، Ketje [۱۹] Jr به منظور ارزیابی مقاومت در برابر حملات تحلیل توان،

^{۱۱} Sponge

^{۱۲} Gross

^{۱۳} Diehl

^{۱۴} Offset Codebook

^۷ Adomnicai

^۸ Masking

^۹ Samwel

^{۱۰} Daemen

حمله تحلیل توان

اثرهای مورد نیاز برای حمله موفق و جلوگیری از تکرار اندازه-گیری موثر است. مرور جامعی بر کاربردهای ML در حملات کانال جانبی در [۲۴] ارائه شده است.

به طور معمول در تحلیل توان طرح‌های رمزنگاری، بخش غیرخطی طرح (S-box) به عنوان نقطه حمله انتخاب می‌گردد. در پیاده‌سازی‌های سخت‌افزاری می‌توان با استفاده از محاسبات میدان مرکب، S-box را به صورت مدار ترکیبی پیاده‌سازی نمود. در چنین پیاده‌سازی اگر ورودی S-box صفر باشد، مصرف توان آن بخش نسبت به دیگر مقادیر کمتر است. این پدیده به این صورت توصیف می‌گردد، در حالتی که ورودی صفر باشد ضرب-های استفاده شده در S-box، در مقدار صفر ضرب می‌شوند و بنابراین مصرف توان کمتری دارند. از این ویژگی می‌توان در حملات CPA استفاده نمود که در این صورت مدل نشت توان، مقدار صفر (ZV^{23}) نامیده می‌شود. رابطه ۱ این مدل را توصیف می‌کند. h_{ij} مدل حدسی توان و v_{ij} مقادیر میانی هستند. در عمل نشان داده شده است که استفاده از مدل ZV در حالتی که اندازه‌گیری مصرف توان در زمان محاسبه S-box باشد، ضرایب همبستگی بالاتری نسبت به دیگر مدل‌های توان ایجاد می‌کنند [۲۵].

$$h_{ij} = ZV(v_{ij}) = \begin{cases} 0 & \text{for } v_{ij} = 0 \\ 1 & \text{for } v_{ij} \neq 0 \end{cases} \quad (1)$$

رمز احراز اصالت شده OCB

رمز احراز اصالت شده OCB یک مد رمزنگاری قالبی است. نسخه اولیه OCB (OCB1) [۲۶] در سال ۲۰۰۱ ارائه شده بود. نسخه کنونی آن (OCB3) در FSE 2011 ارائه شد که به عنوان استاندارد اینترنتی در RFC 7253 [۲] پیشنهاد شده است. به علاوه OCB3 به عنوان یکی از برندگان نهایی مسابقه سزار برای کاربردهای سرعت بالا انتخاب شده است. این رمز در نسخه‌های متفاوت از طول کلید ۱۲۸، ۱۹۲ و ۲۵۶ بیت پشتیبانی می‌کند، متن اصلی در قالب‌های ۱۲۸ بیتی پردازش و متن رمزی ۱۲۸ بیتی و برچسب به طول‌های ۶۴، ۹۶ و ۱۲۸ بیت را تولید می‌کند. شکل ۱ ساختار کلی OCB3 را نشان می‌دهد. در بخش بالای شکل نحوه محاسبه مقادیر آفست ($\Delta[i]$) نمایش داده شده است. تک‌شمار N دارای اندازه ۹۶ بیتی است که از سمت چپ با تعدادی صفر و یک تک بیت ۱ دنباله‌زنی^{۲۴} می‌شود تا تک‌شمار ۱۲۸ بیتی را بسازد. برای هر عملیات رمزنگاری

حملات کانال جانبی شامل هر نوع حملاتی است که بر اساس اطلاعات به دست آمده از پیاده‌سازی‌های فیزیکی سیستم رمزنگاری است. یکی از معروف‌ترین و مؤثرترین حملات عملی به سخت‌افزارهای رمزنگار حمله تحلیل توان است که با استفاده از نشت توان مصرفی، کلید مخفی را آشکار می‌کند. حملات تحلیل توان دارای انواع گوناگونی هستند: حمله تحلیل توان ساده^{۱۵} (SPA) و تفاضلی^{۱۶} (DPA) [۲۰]، همبستگی^{۱۷} (CPA) [۲۱]، حمله بر اساس الگو^{۱۸} [۲۲] و تحلیل اطلاعات متقابل^{۱۹} [۲۳]. هر یک از این حملات از جنبه خاصی دارای برتری بوده و در شرایط خاص، مناسب است. به طور مثال در حملات SPA، مصرف توان تجهیز رمزنگار در محور زمان مورد تحلیل قرار می‌گیرد و حمله‌کننده سعی در یافتن یک الگو در اثر یا تطبیق آن با یک اثر است. اما در حملات DPA شکل اثرها در طول زمان اهمیت ندارد بلکه مهم، تحلیل چگونگی ارتباط مصرف توان در یک لحظه ثابت از زمان با داده‌های پردازش شده است. حمله CPA که یک فرم تعمیم یافته از DPA است و به دلیل توانایی بیشتر آن در آشکارسازی مقدار مخفی الگوریتم رمز، بیشتر مورد توجه قرار گرفته است.

در حمله CPA مقادیر اندازه‌گیری شده با مقادیر تخمینی به دست آمده از مدل تئوری توان مقایسه و مقدار همبستگی این دو محاسبه می‌گردد. مدل تئوری توان (مدل نشت) بر مبنای تأثیر مقادیر میانی بر مصرف توان انتخاب می‌گردد که معمولاً در پیاده‌سازی‌های نرم‌افزاری مانند میکروکنترلر از وزن همینگ^{۲۰} (HW) و برای پیاده‌سازی‌های سخت‌افزاری از فاصله همینگ^{۲۱} (HD) استفاده می‌شود. با انتخاب درست مدل نشت، مقادیر توان با نتایج آن به ازای مقادیر میانی به شدت وابسته می‌گردند. استفاده از مدل HD در پیاده‌سازی‌های سخت‌افزاری زمانی که ثبات‌ها به‌روز می‌شود، مناسب است.

استفاده از تکنیک‌های یادگیری ماشین^{۲۲} (ML) در سال‌های اخیر موجب بهبود حملات تحلیل توان شده است. می‌توان از ML به صورت مستقیم به منظور حدس مقادیر مخفی الگوریتم یا کلید استفاده نمود یا برای تقریب تابع نشت توان در حملات تحلیل توان استفاده نمود. در حالت کلی کاربرد تکنیک‌های ML در کاهش اثرات نویز اثرهای اندازه‌گیری شده، کاهش تعداد

^{۲۱} Hamming Distance
^{۲۲} Machin Learning
^{۲۳} Zero-value Power Model
^{۲۴} Padding

^{۱۵} Simple Power Analysis
^{۱۶} Differential Power Analysis
^{۱۷} Correlation Power Analysis
^{۱۸} Template Attack
^{۱۹} Mutual Information Analysis
^{۲۰} Hamming Weight

محاسبه می‌گردد. AD در قسمت پایین شکل ۱ پردازش و برای محاسبه برچسب نهایی استفاده می‌شود.

حمله تحلیل توان CPA به رمز OCB

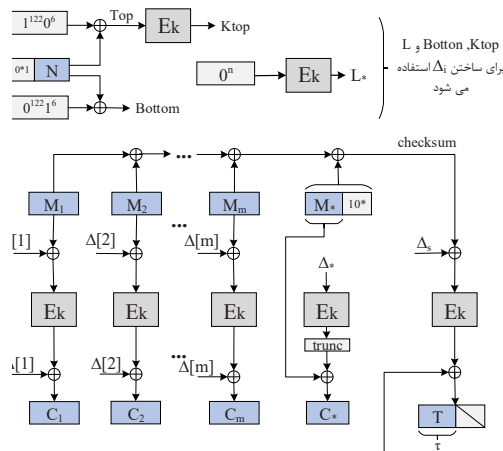
اجرای حمله تحلیل توان نیازمند مشخص شدن نقاط قابل حمله طرح است. به‌طور کلی نقاطی از طرح قابل حمله است که اولاً ورودی آن مقدار متغیر و معلوم باشد و ثانیاً کلید نامعلوم رمز با آن قسمت ترکیب شود. بخش‌های قابل بررسی برای حمله CPA در رمز OCB، E_K بخش‌های محاسبه $\Delta[i]$ پردازش متن اصلی، پردازش AD و تولید برچسب مطابق شکل ۱ است.

رمز OCB دارای دو ویژگی امنیتی است: (۱) استفاده از تابع چکیده‌ساز XOR-فراگیر 2^{25} به کارگیری ساختار رمزهای قالبی تنظیم‌پذیر (TBC^{۲۶}). این دو ویژگی حملات تحلیل توان را نسبت به رمزهای قالبی سخت می‌نماید. برای حل این مسئله، زمان پردازش تک‌شمار به عنوان نقطه حمله انتخاب شده است؛ زیرا در کل طرح تنها در این نقطه ترکیب کلید و تک‌شمار در پردازش E_K می‌شود و در سایر بخش‌ها به دلیل ویژگی دوم امنیتی طرح، مقادیر نامعلوم و متغیر Δ با ورودی‌های E_K ترکیب می‌شود. بنابراین ورودی E_K به‌صورت مستقیم قابل کنترل نیست. لذا حمله‌کننده با حمله به آن نمی‌تواند کلید مخفی K را محاسبه کند.

در زمان پردازش تک‌شمار، برای استخراج کلید در حمله تحلیل توان نیازمند متغیر بودن ورودی آن دارد. مطابق الگوریتم ۱ تک‌شمار دارای طول ۹۶ بیتی بوده که ابتدا ۹۰ بیتی شده و سپس با ۳۷ بیت صفر و یک بیت ۱ دنباله‌زنی شده و به عنوان ورودی E_K پردازش می‌شود. بنابراین ۳۸ بیت از ورودی آن ثابت بوده و امکان استخراج بیت‌های متناظر کلید با یک بار اجرای حمله تحلیل توان وجود ندارد. به‌دلیل اینکه در رمز OCB تابع E_K همان الگوریتم AES است می‌توان از ایده حمله ارائه شده در [۲۸] برای استخراج کلید با وجود ثابت بودن بخشی از ورودی E_K استفاده نمود.

بنابراین در اینجا یک حمله ۷ مرحله‌ای طراحی شده است. ابتدا حمله CPA روی خروجی S-box دور اول AES برای استخراج بایت‌های ۴ تا ۱۴ کلید اصلی انجام می‌شود. با توجه به مشخص شدن این ۱۱ بایت از کلید، محاسبه بخشی از ورودی دور دوم امکان‌پذیر می‌شود. سپس با اجرای عملیات جابجایی سطری (SR) و مخلوط‌سازی ستونی (MC) در دور اول، خروجی دور اول محاسبه می‌شود. این خروجی به‌صورت ترکیبی از مقادیر معلوم و نامعلوم است. با انتقال مقادیر نامعلوم ورودی S-box مرحله دوم به جزئی از کلید، با اجرای حمله CPA دوم بر روی

مقادیر تازه برای تک‌شمار استفاده می‌گردد. اگر تک‌شمار دو یا چند مرتبه استفاده گردد محرمانگی رمز به مخاطره می‌افتد.



شکل ۱. مراحل رمزنگاری رمز OCB [۲۷] (N: تک‌شمار، Auth: احراز اصالت AD، T: طول برچسب، trunc: حذف بیت‌های کم‌ارزش برای تطابق با سایر ورودی‌ها)

$\Delta[i]$ نیز با استفاده از الگوریتم ۱ محاسبه می‌شود.

| الگوریتم ۱- محاسبه $\Delta[i]$ |
|---|
| 1. $Nonce \leftarrow 0^{127-N} \ 1 \ N$ |
| 2. $Top \leftarrow Nonce \wedge 1^{122} 0^6$ |
| 3. $K_{top} = E_K(Top)$ |
| 4. $Bottom \leftarrow Nonce \wedge 0^{122} 1^6$ |
| 5. $Stretch \leftarrow K_{top} \ (K_{top} \oplus (K_{top} \ll 8))$ |
| 6. $\Delta[0] \leftarrow (Stretch \ll Bottom)[1 \dots 128]$ |
| 7. $L_* \leftarrow E_K(0^{128})$ |
| 8. $L_\$ \leftarrow 2 \cdot L_*$, $L[0] \leftarrow 2 \cdot L_\$$ |
| 9. $L[i] = 2 \cdot L[i-1]$ |
| 10. $\Delta[i] = \Delta[i-1] \oplus L[ntz(i)]$ |
| 11. $\Delta_* = \Delta[m] \oplus L_*$, $\Delta_\$ = \Delta[m] \oplus L_\$$ |

در اینجا عملگرهای \wedge ، $\|$ و \ll به ترتیب، AND منطقی، الحاق و چرخش به چپ است. همچنین $ntz(0)$ تعداد صفرهای ورودی را برمی‌گرداند و E_K تابع رمزنگاری است که در اینجا AES مورد نظر است. مطابق الگوریتم ۱ اگر N به صورت شمارنده انتخاب و برای هر پیام جدید به آن یک واحد اضافه گردد برای هر ۶۴ پیام مقادیر Top و در نتیجه K_{top} محاسبه شوند. سپس لازم است یک مقدار جدید برای N انتخاب گردد.

در این رمز متن رمز به صورت $C[i] = M[i] \oplus E_K(M[i] \oplus \Delta[i]) \oplus \Delta[i]$ برای هر قالب ۱۲۸ بیتی پیام $M[i]$

مرحله سوم: محاسبه ورودی دور دوم AES. به دلیل ثابت بودن مقادیر تک‌شمار دنباله‌زنی شده در ۵ بایت ۰ تا ۳ و ۱۵، امکان استخراج این بایت‌ها با اجرای حمله در دور اول وجود نداشت. راهکار پیشنهادی محاسبه ورودی دور دوم AES و اجرای مجدد حمله CPA در دور دوم است.

اگر خروجی دور اول (ورودی دور دوم) با Z_1 و خروجی S-box با $W_{1,j}$ ($0 \leq j \leq 15$) نمایش داده شود، مطابق ماتریس شکل (۳-الف) خروجی S-box برای بایت‌های ۰ تا ۳ و ۱۵ ثابت و نامعلوم است. پس از اعمال SR (شکل ۳-ب) و MC (شکل ۳-ج) خروجی دور سوم ساخته می‌شود. در اینجا مقادیر نامعلوم ماتریس MC با $X_{1,j}$ نمایش داده شده است.

$$\begin{bmatrix} ? & W_{1,4} & W_{1,8} & W_{1,12} \\ W_{1,5} & W_{1,9} & W_{1,13} & ? \\ W_{1,10} & W_{1,14} & ? & W_{1,6} \\ ? & ? & W_{1,7} & W_{1,11} \end{bmatrix} \begin{bmatrix} ? & W_{1,4} & W_{1,8} & W_{1,12} \\ ? & W_{1,5} & W_{1,9} & W_{1,13} \\ ? & W_{1,6} & W_{1,10} & W_{1,14} \\ ? & W_{1,7} & W_{1,11} & ? \end{bmatrix}$$

(ب) خروجی SR (الف) خروجی S-box

$$\begin{bmatrix} 3W_{1,5} + W_{1,10} + X_{1,1} & 2W_{1,4} + 3W_{1,9} + W_{1,14} + X_{1,2} & \dots \\ 2W_{1,5} + 3W_{1,10} + X_{1,5} & \dots & \dots \\ W_{1,5} + 2W_{1,10} + X_{1,9} & \dots & \dots \end{bmatrix}$$

(ج) خروجی MC (ماتریس Z_1 برابر ورودی دور دوم)
شکل ۳. محاسبات دور اول AES

مرحله چهارم: اجرای حمله CPA دوم. جمع با کلید دور دوم با استفاده از رابطه ۲ محاسبه می‌شود.

$$\begin{aligned} AddRoundKey(W_{1,j} \oplus X_{1,j}, K_2) & \quad (۲) \\ &= (W_{1,j} \oplus X_{1,j}) \oplus K_2 \\ &= W_{1,j} \oplus (X_{1,j} \oplus K_2) = W_{1,j} \oplus \tilde{K}_2 \end{aligned}$$

یعنی مقادیر نامعلوم $X_{1,j}$ از ماتریس Z_1 حذف و به بخشی از کلید دور دوم منتقل می‌گردد. کلید جدید با عنوان کلید دور دوم تغییر یافته (\tilde{K}_2) نامگذاری می‌شود. سپس بر روی خروجی S-box (نقطه دوم حمله در شکل ۲) حمله CPA به ازای کلیه بایت‌ها اجرا می‌گردد که منجر به بازیابی تمام بایت‌های کلید دور دوم تغییر یافته \tilde{K}_2 می‌شود.

مرحله پنجم: محاسبه ورودی دور سوم AES. خروجی دور دوم (ورودی دور سوم) به صورت شکل ۴ محاسبه می‌گردد.

$$\begin{bmatrix} W_{2,0} & W_{2,4} & W_{2,8} & W_{2,12} \\ W_{2,5} & W_{2,9} & W_{2,13} & W_{2,1} \\ W_{2,10} & W_{2,14} & W_{2,2} & W_{2,6} \\ W_{2,1} & W_{2,3} & W_{2,7} & W_{2,11} \end{bmatrix} \begin{bmatrix} W_{2,0} & W_{2,4} & W_{2,8} & W_{2,12} \\ W_{2,1} & W_{2,5} & W_{2,9} & W_{2,13} \\ W_{2,2} & W_{2,6} & W_{2,10} & W_{2,14} \\ W_{2,3} & W_{2,7} & W_{2,11} & W_{2,1} \end{bmatrix}$$

(ب) خروجی SR (الف) خروجی S-box

$$\begin{bmatrix} 2W_{2,0} + 3W_{2,5} + W_{2,10} + W_{2,1} & 2W_{1,4} + 3W_{1,9} + W_{1,14} + W_{2,3} & \dots \\ W_{2,0} + 2W_{2,5} + 3W_{1,10} + W_{2,1} & \dots & \dots \\ \dots & \dots & \dots \end{bmatrix}$$

(ج) خروجی MC (Z_2 برابر ورودی دور سوم)
شکل ۴. محاسبات دور دوم AES

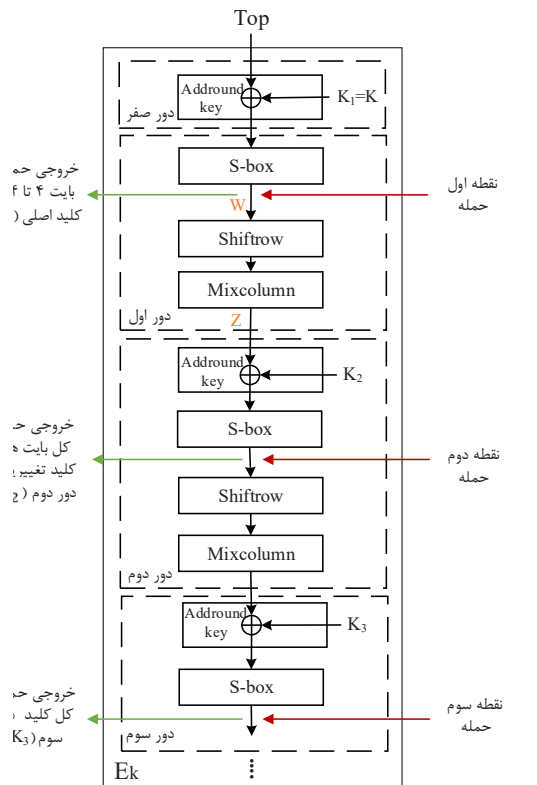
S-box این مرحله، تمامی بایت‌های کلید تغییر یافته دور دوم بازیابی می‌گردد. با استفاده از این کلید، ورودی دور سوم محاسبه می‌گردد. سپس با اجرای سومین حمله CPA بر روی S-box این مرحله، کلید واقعی این دور به طور کامل استخراج شده و با استفاده از معکوس تابع فرامای کلید، کلید اصلی از کلید دور سوم بازیابی می‌شود. در ادامه جزئیات طرح حمله تحلیل توان به OCB، بیان می‌گردد.

طرح حمله OCB

حمله CPA علیه E_K پردازش تک‌شمار برای رمز OCB طی مراحل زیر قابل اجرا است (شکل ۲):

مرحله اول: جمع‌آوری اثر توان. اثرهای توان برای ۳ دور اول AES برای قالب‌های ورودی تک‌شمار متفاوت به تعداد کافی ثبت می‌شود.

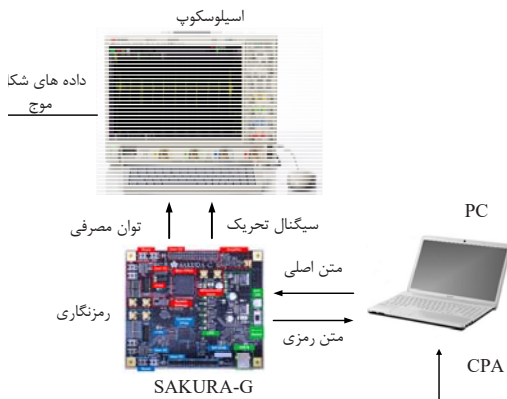
مرحله دوم: استخراج ۱۱ بایت کلید اصلی. حمله CPA اول با مدل توان ZV بر روی خروجی S-box دور اول (نقطه اول حمله در شکل ۲) اجرا تا بایت‌های ۴ تا ۱۴ کلید اصلی ($K = K_1$) استخراج گردد. برای محاسبه ۱۱ بایت از استراتژی تقسیم‌کن و پیروز شو استفاده می‌شود. یعنی هر بایت به صورت جداگانه استخراج می‌گردد.



شکل ۲. طرح حمله OCB

شده است. این برد دارای طراحی با نویز فوق العاده پایین و هم-چنین دارای تقویت کننده سیگنال روی برد است که تحلیل توان را آسان تر نموده است.

اندازه گیری توان به صورت اندازه گیری افت ولتاژ روی مقاومت 1Ω در V_{dd} مربوط به FPGA اصلی پس از تقویت شدن انجام می شود. این اندازه گیری توسط اسیلوسکوپ دیجیتال مدل Infinium Keysight DS090604A با نرخ نمونه برداری 20 Gs/s و پهنای باند 6 GHz انجام شده است. برای پیاده سازی AES معماری شکل ۵ در سطح RTL به زبان VHDL کدنویسی و با استفاده از نرم افزار Xilinx ISE V14.7 سنتز شده است. صحت عمل کرد مدار با ابزار Mentor Graphic Modelsim 10.1c بررسی و فایل خروجی تولید شده روی FPGA برنامه ریزی شده است. راه اندازی و تنظیمات برد SAKURA مطابق راهنمای [۳۰] انجام گرفته است. شکل ۶ تصویری از برد تجهیزات مورد استفاده را نشان می دهد.



شکل ۶. تجهیزات مورد استفاده در حمله

به منظور هم زمان سازی اسیلوسکوپ با FPGA برای اندازه گیری و ضبط سیگنال، سیگنال تحریک^{۲۸} توسط FPGA تولید و به اسیلوسکوپ ارسال می شود. هم چنین جهت ارتباط بین PC برد SAKURA و اسیلوسکوپ برنامه واسطی به زبان C# نوشته شده است. وظیفه این برنامه تولید متن اصلی و کلید و سپس ارسال آن به FPGA و دریافت خروجی از طریق پورت USB است. هم چنین از طریق این برنامه با ارسال دستور، اسیلوسکوپ کنترل شده و ذخیره سازی اثرها روی حافظه جانبی انجام می گیرد. سپس اثرها به رایانه منتقل و پردازش روی آن انجام شده است. برای کاهش اثر نویز برای هر ورودی مشخص ۱۰۰۰ بار داده ها ذخیره شده و با کمک نرم افزار MATLAB R2017 میانگین گیری و تحلیل شده است.

شکل ۷ اثر توان مصرفی اندازه گیری شده را برای بخشی از دوره های اول تا سوم AES نمایش می دهد. قبل از شروع دور اول

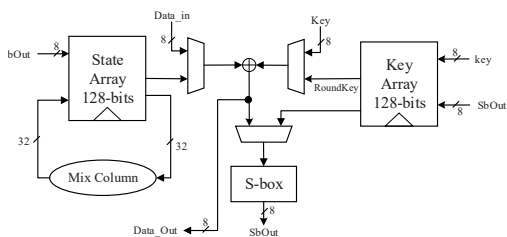
^{۲۸} Trigger

مرحله هشتم: اجرای حمله CPA سوم. اجرای حمله CPA روی خروجی S-box (نقطه سوم حمله در شکل ۲) با استفاده از ورودی های معلوم و متغیر Z_2 به ازای کلیه بایت ها، منجر به بازیابی تمامی بایت های کلید واقعی دور سوم K_3 می شود.

مرحله هفتم: بازیابی کلید اصلی K . با اجرای معکوس تابع فرآیندی کلید AES بر روی کلید دور سوم K_3 ، کلید اصلی الگوریتم یعنی K به آسانی قابل بازیابی است.

نتایج عملی حمله تحلیل توان به رمز OCB

به منظور اجرای حمله CPA در رمز OCB، رمز AES به صورت سخت افزاری پیاده سازی شده است. برای این کار از معماری ارائه شده برای AES در [۲۹] برای پیاده سازی سخت افزاری آن استفاده شده که یک معماری سریال بوده و در شکل ۵ نمایش داده شده است. این معماری دارای مسیر داده ۸-بیتی است و از یک S-box برای دو بخش جانشینی بیتی و فرآیندی کلید به صورت سریال استفاده شده است و هر S-box در یک کلاک محاسبه می شود. مزیت معماری سریال نسبت به معماری موازی کاهش نویز کلیدزنی^{۲۷} است. هم چنین در معماری موازی توان مصرفی اندازه گیری شده ناشی از برهم نهی توان مصرفی تعدادی S-box است که کار تحلیل را بسیار سخت می کند. به علاوه در معماری غیر سریال که چندین S-box پیاده سازی می شود اثر های ایجاد شده از S-box های متفاوت با ورودی یکسان، دقیقاً یکسان نیست. بنابراین بهترین حالت استفاده از ساختار سریال است.

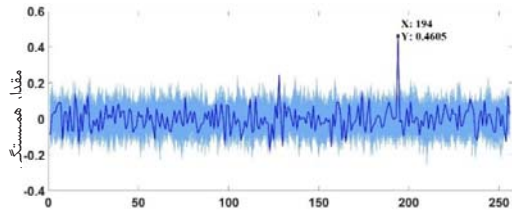


شکل ۵. معماری AES مورد استفاده در رمز OCB [۲۹]

تجهیزات آزمایشگاهی حمله شامل FPGA، اسیلوسکوپ دیجیتال و رایانه است. برد SAKURA-G [۳۰] یکی از معروف ترین بردهای مورد استفاده در حملات کانال جانبی است. این برد شامل دو FPGA سری SPARTAN-6 از شرکت Xilinx است که یکی برای کنترل و دیگری برای رمز اصلی در نظر گرفته

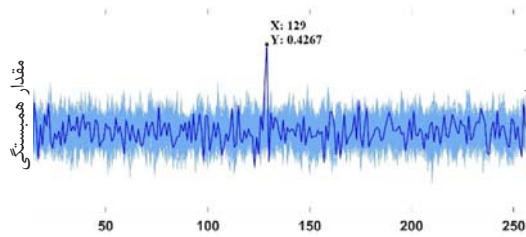
^{۲۷} Switching

حمله به دور سوم تکرار می‌شود. برای مثال مطابق شکل ۱۰ بایت اول کلید دور دوم مقدار ۱۲۸ یا ۸۰ هگزادسیمال به دست آمده است. با توجه به اینکه محور نمودار از یک شروع می‌شود، مقدار ۱۲۹ روی نمودار برابر مقدار کلید ۱۲۸ است. با ادامه حمله به ازای ۱۶ بایت، تمامی بایت‌های کلید دور سوم برابر می‌شود.



زیرکلید

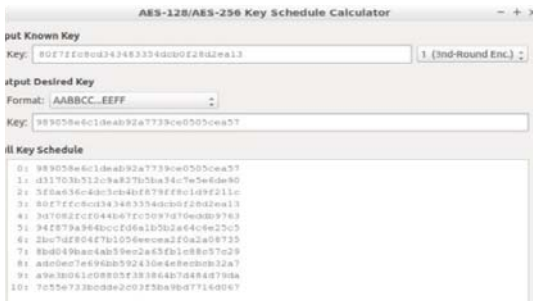
شکل ۹. بایت چهارم کلید اصلی حاصل از حمله CPA به رمز OCB با مدل ZV با ۳۰۰۰ اثر



زیرکلید

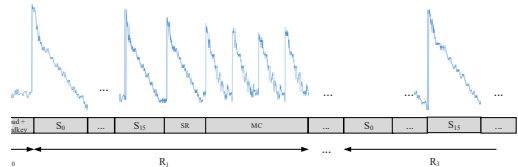
شکل ۱۰. بایت اول کلید دور سوم از حمله CPA به رمز OCB با مدل ZV با ۳۰۰۰ اثر

در نهایت مطابق با مرحله هفتم از طرح حمله با استفاده از یک برنامه محاسبه فرامای کلید [۳۱] مطابق شکل ۱۱ تمام بایت‌های کلید اصلی محاسبه می‌شود. به این صورت که کلید دور سوم به دست آمده از حمله به عنوان ورودی برنامه داده شده و با تنظیم شماره دور، کلید اصلی به عنوان خروجی برنامه برابر مقدار $K=989058E6C1DEAB92A7739CE0505CEA57$ به دست می‌آید.



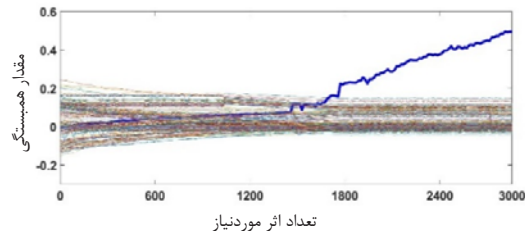
شکل ۱۱. بازیابی کلید اصلی با اجرای معکوس تابع فرامای کلید بر روی کلید دور سوم حاصل از حمله CPA به رمز OCB

کلید اصلی با پیام XOR می‌شود. در دور اول به ترتیب S-box، SR و MC انجام می‌پذیرد. چون در طرح از یک S-box استفاده شده است هم‌زمان با مخلوط‌سازی ستونی عملیات فرامای کلید برای تولید کلید دور دوم اجرا می‌گردد. این عملیات به اجرای ۴ مرتبه S-box نیاز دارد. در دور دوم و سوم همین روند تکرار می‌شود.



شکل ۷. توان مصرفی اندازه‌گیری شده AES در سه دور

برای جمع‌آوری داده مطابق مرحله اول حمله (بخش طرح حمله OCB) از ۳۰۰۰ اثر ثبت شده است. نتایج تحلیل همبستگی بر حسب تعداد اثر موردنیاز در شکل ۸ نشان می‌دهد که حدود ۱۸۷۰ اثر برای اجرای موفق حمله کافی است.



شکل ۸. نتایج حمله CPA بر حسب تعداد اثرها

متناظر با مرحله دوم طرح حمله (بخش طرح حمله OCB)، حمله CPA با استفاده از مدل ZV روی خروجی S-box استفاده از ۳۰۰۰ اثر انجام شده است. به طور مثال نتایج برای بایت چهارم کلید در شکل ۹ نمایش داده شده است. قله همبستگی در این شکل، مربوط به حدس درست کلید و خط پررنگ مربوط به زمان خاص است که قله در آن قرار دارد. در اینجا بایت چهارم کلید یعنی ۱۹۳ بر مبنای ده‌دهی یا C1 بر مبنای هگزادسیمال استخراج می‌شود. با توجه به اینکه محور نمودار از یک شروع می‌شود، مقدار ۱۹۴ روی نمودار برابر مقدار کلید ۱۹۳ است. با تکرار حمله، بایت‌های ۴ تا ۱۵ کلید به صورت $K=????C1DEAB92A7739CE0505CEA?$ بازیابی می‌گردد.

بعد از استخراج ۱۱ بایت کلید اصلی، مطابق مرحله چهارم از طرح حمله (بخش طرح حمله OCB)، حمله به دور دوم برای همه بایت‌ها تکرار و کلید تغییر یافته دور دوم برابر مقدار $K_2=2875005834EAC69B7075850A2C04D13F$ بازیابی می‌شود.

بعد از استخراج تمام بایت‌های کلید تغییر یافته دور دوم، مطابق مرحله ششم از طرح حمله (بخش طرح حمله OCB)،

نتیجه‌گیری و کارهای آینده

- mode of operation (GCM),” Submiss. to NIST Modes Oper. Process, vol. 20, 2004.
- [4] N. Ferguson, “Authentication weaknesses in GCM,” Comments submitted to NIST Modes of Operation Process, 2005. [Online]. Available: <https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/comments/cwc-gcm/ferguson2.pdf>.
- [5] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, and P. Jovanovic, “Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS,” IACR Cryptology ePrint Archive, Report 2016/475, 2016. [Online]. Available: <https://eprint.iacr.org/2016/475>.
- [6] “CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness.” [Online]. Available: <http://competitions.cr.yt.to/caesar.html>.
- [7] H. Wu, “ACORN: a lightweight authenticated cipher (v3),” Candidate for the CAESAR Competition, 2016. [Online]. Available: <http://competitions.cr.yt.to/round3/acornv3.pdf>.
- [8] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, “Ascon v1.2,” Submission to the CAESAR Competition, 2016. [Online]. Available: <http://competitions.cr.yt.to/round3/asconv1.2.pdf>.
- [9] A. Baksi, V. Pudi, S. Mandal, and A. Chattopadhyay, “Lightweight ASIC Implementation of AEGIS-128,” in 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2018, pp. 251–256.
- [10] E. T. and K. Y. A. Elena, A. Bogdanov, N. Datta, A. Luykx, B. Mennink, M. Nandi, “COLM v1.,” CAESAR competition proposal, 2016. [Online]. Available: <https://competitions.cr.yt.to/round3/colmv1.pdf>.
- [11] A. Mehrdad, F. Moazami, and H. Soleimany, “Impossible differential cryptanalysis on Deoxys-BC-256,” ISC Int. J. Inf. Secur., vol. 10, no. 2, pp. 93–105, 2018.
- [12] A. Adomnicai, J. J. Fournier, and L. Masson, “Masking the Lightweight Authenticated Ciphers ACORN and Ascon in Software,” Cryptogr. Inf. Secur. Balk. Springer Int. Publ. Cham, 2018.
- [13] N. Samwel and J. Daemen, “DPA on hardware implementations of Ascon and Keyak,” in Proceedings of the Computing Frontiers Conference, 2017, pp. 415–424.
- [14] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, and R. Van Keer, “Keyak v2,” CAESAR Submiss., 2015. [Online]. Available: <http://competitions.cr.yt.to/round3/keyakv22.pdf>
- [15] H. Gross, E. Wenger, C. Dobraunig, and C. Ehrenhöfer, “Ascon hardware

در این تحقیق برای اولین بار حمله CPA روی پیاده‌سازی سخت‌افزاری رمز احراز اصالت شده OCB به منظور بررسی مقاومت طرح در برابر این حمله انجام شد. به دلیل اینکه ویژگی امنیتی خاص مانند به کارگیری ساختار رمزهای قالبی تنظیم‌پذیر در این طرح، حمله مستقیم به بخش‌های اصلی طرح از جمله به بخش پردازش متن اصلی امکان‌پذیر نیست. زمان پردازش تک‌شمار تنها نقطه طرح می‌باشد که در آن ورودی AES، با مقادیر نامعلوم، XOR نمی‌شود. بنابراین یک طرح حمله ۷-مرحله‌ای برای حمله به این نقطه طراحی شد. نتایج پیاده‌سازی با کمک تجهیزات آزمایشگاهی، برد SAKURA و استخراج ۳۰۰۰ اثر، منجر به استخراج کلید اصلی شد.

تاکنون کارهای کمی در زمینه ارزیابی آسیب‌پذیری بردگان نهایی مسابقه سزار در برابر حملات کانال جانبی و ارائه طرح محافظت برای آن‌ها انجام شده‌است، بنابراین ارائه طرح حمله، ارائه طرح‌های محافظت جدید یا پیاده‌سازی رمزهای نقاب‌گذاری مانند [۳۲] روی رمزها و مقایسه نتایج هزینه‌های سخت‌افزاری محافظت برای این بردگان می‌تواند یک زمینه تحقیق باشد. البته اخیراً، در مراجع [۳۳ و ۳۴]، جهانیان و همکاران تلاش‌های موثری در این راستا انجام داده‌اند، اما هنوز کارهای تحقیقاتی زیادی در این زمینه می‌تواند انجام شود. همچنین، لازم است مسابقه NIST-IWC که با موضوع استاندارد سازی رمزهای احراز اصالت شده و توابع چکیده ساز در جریان است [۳۵] را نیز مد نظر قرار داد، که می‌تواند نتایج این تحقیق در ارزیابی طرح‌های مشابه حاضر در آن مد نظر قرار گیرد. همچنین استفاده از تکنیک‌های یادگیری ماشین در حملات پیشنهادی تحلیل توان برای کاهش تعداد اثرهای توان قابل بررسی است.

تقدیر و تشکر

نصورت باقری، در قالب قرارداد ۲۰۶۳۲، از حمایت مالی دانشگاه تربیت دبیر شهید رجایی برخوردار بوده است.

مراجع

- [1] D. Whiting, R. Housley, and N. Ferguson, “Counter with cbc-mac (ccm), RFC3610,” 2003.
- [2] T. Krovetz and P. Rogaway, “The OCB authenticated-encryption algorithm, RFC 7253,” 2014. [Online]. Available: <https://tools.ietf.org/html/rfc7253>.
- [3] D. McGrew and J. Viega, “The Galois/counter

- Media, 2008.
- [26] P. Rogaway, M. Bellare, J. Black, and T. Krovetz, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption," in Proceedings of the 8th ACM conference on Computer and Communications Security, 2001, pp. 196-205.
- [27] W. Stallings, "The offset codebook (OCB) block cipher mode of operation for authenticated encryption," *Cryptologia*, vol. 42, no. 2, pp. 135-145, 2018.
- [28] J. Jaffe, "A first-order DPA attack against AES in counter mode with unknown initial counter," in International Workshop on Cryptographic Hardware and Embedded Systems, 2007, pp. 1-13.
- [29] H. Gross, S. Mangard, and T. Korak, "Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order.," IACR Cryptology ePrint Archive, Report 2016/486, 2016. [Online]. Available: <https://eprint.iacr.org/2016/486>.
- [30] "Side-channel Attack User Reference Architecture." [Online]. Available: <http://satoh.cs.uec.ac.jp/SAKURA/hardware.html>.
- [31] [Online]. Available: "<https://github.com/newaetech/chipwhisperer>".
- [32] م. معصومی، ع. دهقان منشادی، ا. مددی و س. ساعی-مقدم، "یک روش جدید و کارآمد نقاب‌گذاری جمعی و ارزیابی مقاومت آن در برابر تحلیل توان"، *پدافند الکترونیکی و سایبری*، جلد ۶، شماره ۲، صفحه ۱۲۳-۱۳۴، ۱۳۹۶.
- [33] M. Jahanbani, N. Bagheri, Z.n Norouzi "Lightweight implementation of SILC, CLOC, AES-JAMBU and COLM authenticated ciphers." *Microprocess. Microsystems* 72, 2020.
- [34] M. Jahanbani, N. Bagheri, Z.n Norouzi: "DPA Protected Implementation of OCB and COLM Authenticated Ciphers". *IEEE Access* 7: 139815-139826, 2019.
- [35] NIST. Nist lightweight cryptography standardization process. In NIST-LWC, pages 2-3. Springer, accessed 01 November 2019.
- implementations and side-channel evaluation," *Microprocess. Microsyst.*, vol. 52, pp. 470-479, 2017.
- [16] W. Diehl and K. Gaj, "RTL implementations and FPGA benchmarking of selected CAESAR Round Two authenticated ciphers," *Microprocess. Microsyst.*, vol. 52, pp. 202-218, 2017.
- [17] A. E. Mode, "The JAMBU Lightweight Authentication Encryption Mode (v2. 1)," CAESAR competition proposal, 2016. [Online]. Available: <http://competitions.cr.yt.to/round3/jambuv21.pdf>.
- [18] T. Iwata, K. Minematsu, J. Guo, and E. Kobayashi, "CLOC and SILC," CAESAR competition proposal, 2016. [Online]. Available: <http://competitions.cr.yt.to/round3/clocsilcv3.pdf>.
- [19] R. V. K. Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, "Ketje v2," CAESAR Submiss., 2015. [Online]. Available: <http://competitions.cr.yt.to/round3/ketjev2.pdf>.
- [20] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Annual International Cryptology Conference, 1999, pp. 388-397.
- [21] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in International workshop on cryptographic hardware and embedded systems, 2004, pp. 16-29.
- [22] D. Agrawal, J. R. Rao, and P. Rohatgi, "Multi-channel attacks," in International Workshop on Cryptographic Hardware and Embedded Systems, 2003, pp. 2-16.
- [23] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in International Workshop on Cryptographic Hardware and Embedded Systems, 2008, pp. 426-442.
- [24] B. Hettwer, S. Gehrler, and T. Güneysu, "Applications of machine learning techniques in side-channel attacks: a survey," *J. Cryptogr. Eng.*, pp. 1-28, 2019.
- [25] S. Mangard, E. Oswald, and T. Popp, "Power analysis attacks: Revealing the secrets of smart cards," vol. 31. Springer Science & Business

