بهبود حمله مکعبی کانال جانبی بر روی الگوریتم‌های بلوکی

شهرام جمالی[۱]، دانشیار، عرفان آقایی کیاسرایی[۲]، دانشجوی ارشد معماری کامپیوتر

۱- دانشکده فنی مهندسی – دانشگاه محقق اردبیلی - اردبیل - ایران - jamali@iust.ac.ir
۲- دانشکده فنی مهندسی – دانشگاه محقق اردبیلی - اردبیل - ایران – erfanaghaei69@gmail.com

چکیده: حمله مکعبی کانال جانبی ازجمله حملات ترکیبی است که در زیرشاخه حملات جبری کانال جانبی قرار می‌گیرد. در سال‌های اخیر، این حمله بر روی انواع الگوریتم‌های بلوکی سبک‌وزن پیاده‌سازی شده و به‌عنوان یک حمله بسیار قدرتمند بر روی الگوریتم‌های بلوکی سبک‌وزن شناخته می‌شود. ازنقطه‌نظر تئوریک این مقاله، با ارائه تکنیک‌هایی مانند جستجوی فضای محلی، شناسایی ورودی‌های تکراری و مدل تکرار حمله مکعبی به بهبود جنبه تئوریک حمله مکعبی کانال جانبی بر روی الگوریتم‌های بلوکی پرداخته است. در جنبه عملی، با پیاده‌سازی الگوریتم استاندار بلوکی هدف (AES) بر روی میکروکنترلر ARM و پیشنهاد بهره‌گیری از تابع چگالی احتمال چندمتغیره در فاز خطی حمله مکعبی کانال جانبی میزان عملیاتی بودن این حمله را بررسی کرده و نشان می‌دهد، حمله مکعبی کانال جانبی بهبودیافته نه‌تنها بر روی الگوریتم‌های سبک‌وزن بلکه بر روی انواع الگوریتم‌های بلوکی مانند AES می‌تواند به‌صورت کارا پیاده‌سازی شود. نتایج این مقاله بیان‌گر آن است که حمله مکعبی کانال جانبی تنها به $2^{6/13}$ متن اصلی منتخب برای بازیابی ۸۰ بیت از کلید الگوریتم PRESENT-80 و $2^{7/3}$ متن اصلی منتخب برای بازیابی ۱۲۸ بیت کلید AES-128 نیاز دارد. با توجه به بررسی‌های انجام‌شده، این حمله بهترین حمله مکعبی کانال جانبی شناخته‌شده ازنظر تعداد متن اصلی منتخب بر روی الگوریتم PRESENT-80 و AES-128 است.

واژه‌های کلیدی: حمله مکعبی کانال جانبی، الگوریتم‌های بلوکی سبک‌وزن، حمله مکعبی، AES-128، الگوریتم PRESENT-80، وزن همینگ

Improved Side Channel Cube Attack on Block Ciphers

S. Jamali, Associate Professor[1], E. Aghaee Kiasaraee, Master Student of Computer Architecture[2],

1- Faculty of Technical and Engineering, University of Mohaghegh Ardabili, Ardabil, Iran, Email: jamali@iust.ac.ir
2- Faculty of Technical and Engineering, University of Mohaghegh Ardabili, Ardabil, Iran, Email:erfanaghaei69@gmail.com

Abstract: Side Channel Cube Attack (SCCA) is a kind of Algebraic Side Channel Attacks (ASCA). In recent years, this kind of attack is implemented on different light weight block ciphers, and it is known as the most powerful attack on these kinds of algorithms. In this paper, we proposed some advanced techniques such as locality space search, elimination of iterated chosen plaintexts, dynamic iteration, and choosing intelligent intermediate states to improve SCCA on block ciphers. Accordingly, the improved SCCA can mount efficiently on not only light weight but also high weight block ciphers. Our results show, the proposed model of SCCA can recover 80 bit key of PRESENT-80 only with $2^{6.13}$ chosen plaintexts and recover 128 key bit of AES-128 only with $2^{7.3}$ chosen plaintexts. To the best of our knowledge, there are the most efficient SCCA on PERESENT-80 and AES-128.

Keywords: Side channel cube attack, block ciphers, cube attack, AES-128, PRESENT-80, hamming weight

تاریخ ارسال مقاله: ۱۳۹۳/۰۲/۱۳
تاریخ اصلاح مقاله: ۱۳۹۳/۹/۱ و ۱۳۹۳/۱۰/۲۵ و ۱۳۹۳/۱۱/۵
تاریخ پذیرش مقاله: ۱۳۹۳/۱۱/۷
نام نویسنده مسئول: شهرام جمالی
نشانی نویسنده مسئول: ایران - اردبیل - دانشگاه محقق اردبیلی - دانشکده فنی مهندسی

۱- مقدمه

حمله مکعبی کانال جانبی در سال ۲۰۰۹ توسط آدی شمیر (*Adi Shemir*) معرفی شده است [۱]. این حمله از ترکیب دو حمله مکعبی [۲] و کانال جانبی تشکیل شده و به‌عنوان یک حمله جبری کانال جانبی شناخته می‌شود. حمله مکعبی که به‌عنوان بخش جبری حمله مکعبی کانال جانبی است، با بهره‌گیری از متد خطی، معادلات خطی از کلید را از الگوریتم هدف استخراج می‌کند و قادر به بازیابی کلید در هر سیستم رمزنگاری است که هر بیت رمز آن به‌صورت تابع درجه پایینی از کلید و متن اصلی توصیف شود.

مشکل اصلی حمله مکعبی آنجا نمایان می‌شود که در الگوریتم‌های بلوکی، درجه چندجمله‌ای از کلید و متن اصلی برای هر بیت رمز به حدی بالا می‌رود که حمله مکعبی را در برابر این دسته از الگوریتم‌ها غیرکارا می‌سازد. برای حل این مشکل، حمله مکعبی کانال جانبی توسط شمیر در سال ۲۰۰۹ معرفی شد [۱].

حمله مکعبی کانال جانبی با بهره‌گیری از اطلاعات به‌دست‌آمده از کانال جانبی (از طریق تحلیل توان [۳]، امواج الکترومغناطیس [۴] یا زمان [۵]) به توصیف معادلات بر روی بیت‌های میانی الگوریتم رمز هدف، جایی که هنوز درجه چندجمله‌ای از کلید به‌طور قابل‌توجهی رشد نکرده است، می‌پردازد. نتیجه این حمله ترکیبی، معرفی یکی از قدرتمندترین حملات رمزنگاری بر روی تعدادی از الگوریتم‌های سبک‌وزن بلوکی از قبیل SERPENT، PRESENT و LBlock است.

۱-۱- نوآوری

با توجه به اینکه حمله مکعبی کانال جانبی از دو جنبه تئوریک در حمله مکعبی و عملی در بخش کانال جانبی تشکیل شده است. لذا، این مقاله با ارائه تکنیک‌های زیر به بهبود حمله مکعبی کانال جانبی پرداخته است:

۱- در بخش تئوریک با پیشنهاد مدل تکرار پویا و حذف ورودی‌های تکراری به میزان قابل‌توجهی میزان پیچیدگی داده‌ای حمله مکعبی کانال جانبی را کاهش داده است.

۲- در بخش عملی با بهره‌گیری از مدل‌سازی نویز گوسی اثر توانی و بهره‌گیری از تابع چگالی احتمال نرمال چندمتغیره تعداد اثرهای توانی را به میزان قابل‌توجهی کاهش داده است.

لازم به ذکر است مدل ارائه‌شده در این مقاله به‌منظور صحت‌سنجی بر روی دو الگوریتم بلوکی PRESENT-80 [۶] و AES-129/256 [۷] پیاده‌سازی شده است.

۲- مروری بر مطالعات انجام‌شده

در ابتدا دینر (Dinur) و آدی شمیر مدل حمله مکعبی کانال جانبی را بر روی دو الگوریتم رمز بلوکی SERPENT و AES پیاده‌سازی و بررسی می‌کنند [۱]. در الگوریتم SERPENT، آن‌ها با به دست آوردن ۱۲۸ معادله خطی به کمک حمله مکعبی و نشت یک بیت در دور سوم الگوریتم SERPENT، ۱۲۸ بیت این الگوریتم را با پیچیدگی 2^{18} عملگر که کمتر از مدل حمله خطی با پیچیدگی 2^{32} است، بازیابی می‌کنند. سپس این حمله را بر روی الگوریتم بلوکی AES کرده و توانستند با پیچیدگی 2^{35} عملگر ۱۲۸ بیت کلید آن را بازیابی کنند.

بعد از اولین حمله مکعبی کانال جانبی معرفی‌شده بر روی الگوریتم‌های رمز بلوکی SERPENT و AES، الگوریتم‌های بلوکی دیگر از قبیل PRESENT [۸-۱۳]، NOEKEON [۱۴]، KATAN [۱۵]، Hummingbird-2 [۱۶]، LBlock [۱۷-۱۸] موردحمله قرار گرفته‌اند. اغلب حملات مکعبی کانال جانبی انجام‌شده بر روی الگوریتم‌های رمز بلوکی از مدل تک‌بیتی نشتی (Single Bit Leakage Model) بهره می‌برند. تنها مدل عبدول لطیف (Abdul latip) [۹] و مدل ژائو (Zaho) [۱۰] بر اساس وزن همینگ نشتی (Hamming weight Leakage Model) است. قابل‌ذکر است، تنها ژائو [۱۰] در شرایط آزمایشگاهی مدل خود را بررسی می‌کند و بقیه مقالات در این زمینه به بیان تئوریک این حمله بسنده می‌کنند و به چگونگی به دست آوردن اطلاعات در شرایط واقعی از کانال جانبی نمی‌پردازند.

۳- مدل پیشنهادی برای بهبود حمله مکعبی کانال جانبی

این مقاله، فازهای پیش‌پردازش و فاز آنلاین حمله مکعبی کانال جانبی را به ترتیب زیر اصلاح می‌کند.

در فاز پیش‌پردازش، با اضافه کردن مرحله شناسایی وضعیت هدف میانی مناسب فضای جستجو تصادفی به فضای جستجوی محلی اصلاح می‌شود. سپس به توصیف نحوه آزمون خطی و استخراج معادلات درجه‌یک در فاز پیش‌پردازش می‌پردازد. در ادامه با شناسایی ورودی‌های تکراری و بهره‌گیری از مدل تکرار به بهبود فاز پیش‌پردازش حمله مکعبی کانال جانبی پرداخته است.

فاز آنلاین در مدل پیشنهادی به سه زیرفاز راه‌اندازی، تولید و تطبیق الگو تقسیم می‌شود. در این فاز، به تولید الگو بر اساس ماتریکس کوواریانس و بردار میانگین پرداخته و در فاز تطبیق الگو تابع چگالی احتمال توزیع نرمال چند متغیره را پیشنهاد می‌دهیم که به‌موجب آن دقت در اندازه‌گیری مقدار وضعیت میانی تا حد بسیار قابل‌توجهی افزایش یافته است.

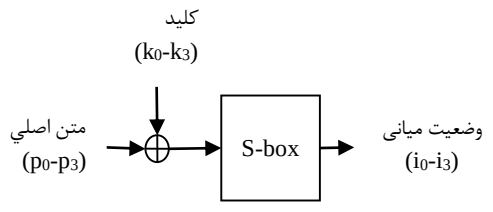
۳-۱- فاز پیش‌پردازش

این فاز را به مراحل زیر تقسیم کرده‌ایم و به توصیف هر مرحله و نکات حائز اهمیت آن می‌پردازیم.

۳-۱-۱- شناسایی وضعیت هدف

شناسایی وضعیت هدف نقش بسیار مهمی در موفقیت و میزان پیچیدگی حمله مکعبی کانال جانبی بازی می‌کند. یک وضعیت هدف ایده‌آل وضعیت هدفی است که تغییر کوچک در ورودی، باعث تغییر بزرگی در خروجی باشد. از طرفی درجه تابع به‌دست‌آمده از سیستم

آن‌قدر بزرگ نباشد که فضای جستجو را غیرعملی سازد. لذا خروجی S-box در دور اول جایی که درجه چندجمله‌ای هنوز رشد نمایی نکرده است می‌تواند هدف مناسبی برای این حمله قرار گیرد. برای مثال شکل ۱ نشان‌دهنده بایت هدف در الگوریتم PRESENT-80 است.



شکل ۱: بایت هدف: خروجی S-box در دور نخست الگوریتم PRESENT-80

۳-۱-۲- جستجوی فضای محلی

در مدل اولیه حمله مکعبی، جستجوی فضای ورودی به‌صورت تصادفی است. جستجوی تصادفی بسیار زمان‌بر است. با مدل کردن یک S-box در الگوریتم بلوکی T و بسط آن به S-boxهای دیگر سیستم، نشان می‌دهیم که تابع هر S-box تنها به چند بیت ورودی وابسته است. لذا، فضای جستجو تصادفی را به فضای محلی مرتبط به هر S-box اصلاح می‌کنیم.

۳-۱-۳- آزمون خطی

در ابتدا ماکزیمم درجه تابع چندجمله‌ای وزن همینگ خروجی S-box در الگوریتم هدف را به دست می‌آوریم. برای مثال، درجه چندجمله‌ای وزن همینگ خروجی S-box در دور نخست الگوریتم PRESENT-80 برابر سه است. در گام آزمون خطی، هدف پیدا کردن عبارت‌های t_I به‌طوری است که سوپرپالی مربوطه آن‌ها خطی از کلید باشد. ازاین‌رو، به‌طور تصادفی I هایی با d-1 (d=3) متغیر عمومی انتخاب کرده و از آزمون BLR [۲۳] به‌منظور آزمون خطی روی I انتخاب‌شده بهره می‌بریم. آزمون خطی BLR، دو بردار کلید تصادفی و مستقل $k', k'' \in \{0,1\}^n$ رو انتخاب کرده و معادله ۱ را بررسی می‌کند. آزمون خطی BLR تضمین می‌کند که اگر $F_{S(I)}$ خطی باشد، آزمون همواره موفقیت‌آمیز خواهد بود. اما اگر $F_{S(I)}$ خطی نیست، با احتمال زیادی آزمون با شکست روبرو خواهد شد و معادله (۱) برقرار نخواهد بود.

$$F(0)+F(k')+F(k'')=F(k'+k'') \qquad (۱)$$

برای مثال، ما به‌طور تصادفی $\mathbf{I}=\{۱,۰\}$ را انتخاب می‌کنیم. تعداد پرسش و پاسخ که برای آزمون خطی ضروری هستند در جدول ۱ لیست شده است. در جدول ۱ تابع وزن همینگ خروجی S-box به‌صورت $F(p_0,p_1,p_2,p_3,k_0,k_1,k_2,k_3)=\sum_{i=0}^{3} i_i$ تعریف شده است که نشان می‌دهد خروجی هر S-box تابعی از چهار متغیر عمومی و چهار متغیر کلید است. در جدول ۱ در گام‌های یک تا چهارم مقدار $F_{S(I)}$ به ازای $k=0,k',k'',k'+k''$ محاسبه می‌کنیم. اگر معادله (۱) برقرار باشد، آزمون را چندین بار بررسی می‌کنیم تا زمانی که مطمئن شویم I انتخاب‌شده دارای $F_{S(I)}$ خطی است در غیر این صورت $F_{S(I)}$ مربوطه خطی نیست.

جدول ۱: تعداد پرسش و پاسخ‌های موردنیاز برای آزمون خطی ($\mathbf{I}=\{۱,۰\}$)

گام	پرسش و پاسخ موردنیاز
۱	$F(0)=F(0,0,0,0,0,0,0,0)+F(1,0,0,0,0,0,0,0)$ $+F(0,1,0,0,0,0,0,0)+F(1,1,0,0,0,0,0,0)$
۲	$F(k')=F(0,0,0,0,k')+F(1,0,0,0,k')$ $+F(0,1,0,0,k')+F(1,1,0,0,k')$
۳	$F(k'')=F(0,0,0,0,k'')+F(1,0,0,0,k'')$ $+F(0,1,0,0,k'')+F(1,1,0,0,k'')$
۴	$F(k'+k'')=F(0,0,0,0,k'+k'')+F(1,0,0,0,k'+k'')$ $+F(0,1,0,0,k'+k'')+F(1,1,0,0,k'+k'')$
۵	$F(0)+F(k')+F(k'')=F(k'+k'')$

۳-۱-۴- محاسبه سوپرپالی

یک سوپرپالی خطی می‌تواند به‌صورت معادله (۲) توصیف شود. با توجه به تئوری بیان‌شده در مرجع [۱]، عبارت ثابت c معادله (۲) می‌تواند به‌وسیله بردار $k=0$ و جمع تمامی حالت‌های ممکن I محاسبه شود. اگر حاصل جمع یک باشد، سوپرپالی خطی دارای عبارت‌های مستقل یک است. ضرایب خطی (a_i) متغیرهای کلید می‌توانند با مقدار یک قرار دادن k_i و صفر قرار دادن مابقی بیت‌های کلید و جمع تمامی حالت‌های ممکن برای I محاسبه شود.

$$F_{S(I)}=c+\sum_{i=0}^{3} a_i.k_i \mod 2 \qquad (۲)$$

$$c, a_i \in \{0,1\}$$

برای مثال، فرض کنید در گام پیشین آزمون خطی $\mathbf{I}=\{۱,۰\}$ با موفقیت انجام شده است. به‌منظور استخراج معادلات خطی از کلید، پرسش و پاسخ جدول ۲ موردنیاز است. همان‌طور که در جدول ۲ مشاهده می‌شود، در گام دوم به‌منظور یافتن ضریب خطی a_0، k_0 را برابر یک کرده و مابقی بیت‌های کلید صفر قرار داده شده است و نتیجه به‌دست‌آمده با c جمع می‌شود. اگر جواب یک بود بدین معنا است که متغیر k_0 در سوپرپالی خطی از کلید وجود دارد. به‌عنوان نمونه، هنگامی‌که $\mathbf{I}=\{۱,۰\}$ در نظر گرفته می‌شود، سوپرپالی خطی از کلید $F_{S(I)}=1+k_3$ از سیستم استخراج می‌شود.

جدول ۲: پرسش و پاسخ موردنیاز به ازای $\mathbf{I}=\{۱،۰\}$

گام	پرسش و پاسخ موردنیاز
۱	$c = F(0,0,0,0,0,0,0,0) + F(1,0,0,0,0,0,0,0)$ $+F(0,1,0,0,0,0,0,0) + F(1,1,0,0,0,0,0,0)$
۲	$a_0 = F(0,0,0,0,1,0,0,0) + F(1,0,0,0,1,0,0,0)$ $+F(0,1,0,0,1,0,0,0) + F(1,1,0,0,1,0,0,0) + c$
۳	$a_1 = F(0,0,0,0,0,1,0,0) + F(1,0,0,0,,1,0,0)$ $+F(0,1,0,0,0,1,0,0) + F(1,1,0,0,0,1,0,0) + c$
۴	$a_2 = F(0,0,0,0,0,0,1,0) + F(1,0,0,0,,0,1,0)$ $+F(0,1,0,0,0,0,1,0) + F(1,1,0,0,0,0,1,0) + c$
۵	$a_3 = F(0,0,0,0,0,0,0,1) + F(1,0,0,0,,0,0,1)$ $+F(0,1,0,0,0,0,0,1) + F(1,1,0,0,0,0,0,1) + c$

۳-۱-۵- شناسایی ورودی‌های تکراری

یک ویژگی بسیار مهمی که در حمله مکعبی کانال جانبی وجود دارد، تکراری بودن خیلی از پرسش و پاسخ‌ها به ازای Iهای مختلف است. این امر باعث کاهش تعداد متن اصلی منتخب می‌شود. برای مثال، با توجه به جدول ۳ وقتی شاخص ورودی $\mathrm{I}=\{۳،۰\}$ و $\mathrm{I}=\{۱،۰\}$ باشد، خیلی از پرسش و پاسخ‌ها تکراری خواهد بود.

جدول ۳: شناسایی ورودی‌های تکراری به ازای $\mathbf{I}=\{۱،۰\}$ و $\mathbf{I}=\{۳،۰\}$

$\mathrm{I}=\{۳،۰\}$	$\mathrm{I}=\{۱،۰\}$
$F(0,0,0,0,k)$	$F(0,0,0,0,k)$
$F(1,0,0,0,k)$	$F(1,0,0,0,k)$
$F(0,0,0,1,k)$	$F(0,1,0,0,k)$
$F(1,0,0,1,k)$	$F(1,1,0,0,k)$

دو پرسش و پاسخ اولیه به ازای $\mathrm{I}=\{۳،۰\}$ و $\mathrm{I}=\{۱،۰\}$ در سیستم تکراری است. اجتناب از این تکرارها در ورودی به میزان قابل‌توجهی تعداد پرسش و پاسخ‌ها از سیستم را کاهش می‌دهد.

۳-۱-۶- مدل تکرار پویا

ایده بسیار ساده اما بسیار کارایی پشت مدل تکرار پویا حمله مکعبی کانال جانبی است. مدل تکرار حمله مکعبی کانال جانبی بدین شکل عمل می‌کند که ما پس از اعمال آزمون خطی و بازیابی یک سری از بیت‌های کلید، بیت‌های بازیابی شده کلید را در متغیرهای کلید مرتبط جایگزین کرده و دوباره حمله مکعبی کانال جانبی را اعمال می‌کنیم. مدل تکرار از استراتژی تقسیم و غلبه بهره می‌برد، تأثیر طول کلید را بر روی حمله مکعبی کانال جانبی به حداقل می‌رساند و سرباری که آزمون معادلات غیرخطی در مدل‌های توسعه‌یافته حمله مکعبی ارائه‌شده در (ژائو، ۲۰۱۳)، (عبدول لطیف، ۲۰۱۱) و (ژنگ لی، ۲۰۱۱) را از بین می‌برد.

برای مثال، وقتی $\mathrm{I}=\{۳،۰\}$ است $F_{S(I)} = k_0$ است. بعد از جایگزین کردن مقدار بیت k_0 و اعمال مجدد حمله مکعبی کانال جانبی به خروجی S-box دور نخست دو حالت رخ می‌دهد. حالت اول، اگر $k_0 = 0$ باشد نتیجه اعمال حمله به ازای $\mathrm{I}=\{۳\}$ استخراج معادله $F_{S(I)} = k_2$ خواهد بود. حالت دوم، اگر $k_0 = 1$ باشد نتیجه اعمال حمله به ازای $\mathrm{I}=\{۳\}$ استخراج معادله $F_{S(I)} = 1 + k_1$ خواهد بود و مقدار k_2 به دست خواهد آمد.

۳-۲- فاز برخط

نتیجه تکمیل فاز پیش‌پردازش، سیستم معادلات خطی از کلید خواهد بود. در فاز برخط، مقدار معادلات خطی از کلید به ازای کلید مخفی محاسبه می‌شود. نمونه‌ای از پرسش و پاسخ موردنیاز برای $\mathrm{I}=\{۱،۰\}$ که سوپرپالی $F_{S(I)} = 1 + k_3$ استخراج می‌شود در جدول ۴ نشان داده شده است. چالش اصلی موجود در این فاز این است که چگونه می‌توان با حضور نویز با دقت بالا مقدار وزن همینگ وضعیت میانی را محاسبه کرد. در ادامه به توصیف نحوه راه‌اندازی سخت‌افزار رمز، نحوه نمونه‌برداری اثر توانی و استراتژی محاسبه مقدار وزن همینگ وضعیت میانی خواهیم پرداخت.

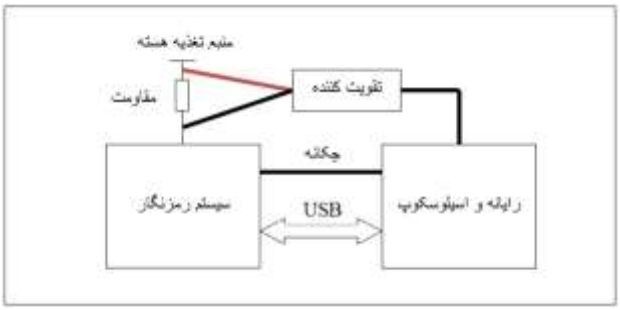
جدول ٤: پرسش و پاسخ موردنیاز در فاز برخط (کلید مخفی)

گام	پرسش و پاسخ موردنیاز
۱	$1 + k_3 = F(0,0,0,0,k) + F(1,0,0,0,k) +$ $F(0,1,0,0,k) + F(1,1,0,0,k)$

۳-۲-۱- راه‌اندازی سخت‌افزار رمز

برای پیاده‌سازی فاز برخط حمله مکعبی کانال جانبی، ابتدا الگوریتم AES را روی میکروکنترلر AT91SAM7S256 پیاده‌سازی کردیم، بدین ترتیب سخت‌افزار رمز خود را آماده ساختیم. میکروکنترلر AT91SAM7S256 محصول شرکت ARM است و سهم بسزایی در بازار میکروکنترلرها و کارت‌های هوشمند دارد. رمزکننده ساخته‌شده از طریق درگاه USB به رایانه متصل شده است. از طریق رایانه قالب‌های ۱۲۸ بیتی داده را برای سخت‌افزار رمز کننده ارسال می‌کنیم. سخت‌افزار رمزکننده با دریافت یک قالب داده آن را رمز می‌کند و نتیجه را به رایانه باز می‌گرداند. ما به ذخیره‌سازی اثرهای توانی در حین رمزنگاری سخت‌افزار می‌پردازیم. برای نمونه‌برداری از یک اسیلوسکوپ دیجیتال حافظه دار استفاده می‌کنیم.

در شکل ۲ مدار راه‌اندازی حمله را مشاهده می‌کنید. در این حمله ما اختلاف ولتاژ دو سر مقاومت را به‌عنوان تغییرات ولتاژ که متناسب با تغییرات توانی است اندازه‌گیری می‌کنیم. اختلاف ولتاژ به‌دست‌آمده، در مسیر ارسال به اسیلوسکوپ، به‌منظور تسهیل در تحلیل به کمک یک تقویت‌کننده تقویت می‌شود.



شکل ۲: مدار راه‌اندازی سخت‌افزار رمزنگار

روش کلی و هم‌زمان‌سازی اسیلوسکوپ و سخت‌افزار رمزکننده برای حمله به شرح زیر است:

برای شروع یک نمونه‌برداری از سیگنال توان، ابتدا اسیلوسکوپ آماده می‌شود و اسیلوسکوپ منتظر سیگنال چکانه (Trigger) برای شروع نمونه‌برداری می‌ماند. این چکانه به‌صورت خارجی از طریق رمزنگار تولید خواهد شد. علت این امر آن است که به‌محض شروع یک عملیات خاص، اسیلوسکوپ شروع به نمونه‌برداری کند و داده‌ای از دست نرود. حال رایانه داده موردنظر برای رمزنگاری را به رمزنگار می‌فرستد. سپس به رمزنگار فرمان شروع می‌دهد. کد شروع فرمان در قطعه کد جدول ۵ نمایش داده شده است.

جدول ۵: کد راه‌اندازی تحلیل توانی

```
PIO _ SET _ TRIG
for(i = 0;i < 16;i++)
state[i] = P ⊕ K[i];
for(i = 0;i < 16;i++)
state[i] = S _ box[state[i]];
PIO _CLEAR_ TRIG
```

رمزنگار با دریافت این دستور، عملیات خود را آغاز می‌کند و در ابتدای عملیات سیگنال چکانه را نیز تولید می‌کند. با این کار اسیلوسکوپ شروع به نمونه‌برداری کرده و کد نمونه از اثر توان، شامل ۱۲۵۰ نقطه برداشت می‌شود. وقتی رمزنگار عملیات خود را تمام کرد، اتمام کار خود را به اسیلوسکوپ اعلام می‌کند. اسیلوسکوپ نمونه توان برداشت‌شده را روی حافظه‌اش ذخیره می‌کند و سپس اسیلوسکوپ برای نمونه بعدی آماده می‌شود.

نمونه‌های توان لازم در این رساله به ترتیب بالا و درحالی‌که فرکانس کاری سخت‌افزار ۴۸ مگاهرتز بوده است تهیه شده است.

در حملات تحلیل توان برای داشتن یک نتیجه خوب باید اثر نویز را حذف کرد. برای حذف نویز، عملیات رمزنگاری برای یک داده مشخص را چندین بار تکرار کرده و اثرهای توان را ذخیره می‌کنیم. سپس با انتقال داده‌ها به رایانه، از این اثرها میانگین‌گیری می‌کنیم. اثر توان ذکرشده در فایل txt ذخیره شده سپس در نرم‌افزار MATLAB با استفاده از دستور 'textread' داده‌ها را به محیط نرم‌افزار فراخوانی می‌کنیم و پردازش خود را روی آن‌ها انجام می‌دهیم. شمایی از برد استفاده‌شده به‌عنوان سخت‌افزار رمزکننده در شکل ۳ نمایش داده شده است. همان‌طور در نمایشگر شکل ۳ دیده می‌شود مدار به ازای ورودی متن اصلی ۱۵۷ و کلید صفر مقدار وزن همینگ خروجی S-box اول در دور نخست را برابر ۵ می‌دهد.

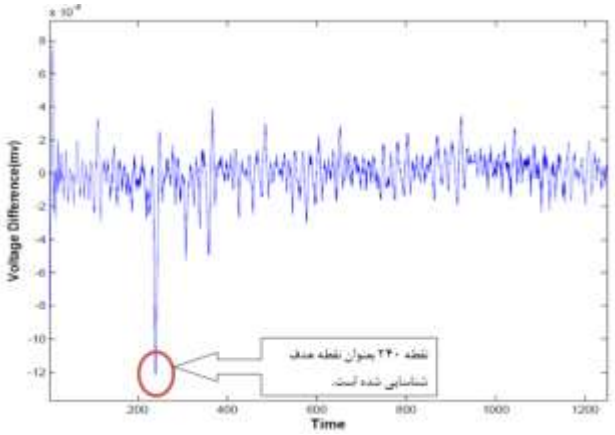
شکل ۳: سخت‌افزار رمزکننده

۳-۲-۲- شناسایی نقاط هدف در اثر توانی

پس از محاسبه اثر توانی توسط اسیلوسکوپ و ذخیره آن در حافظه، چالش پیش‌رو تشخیص نقاطی از اثر توانی است که نشان دهند توان مصرفی خروجی S-box در دور نخست است. بعد از ذخیره ۵۰۰۰ اثر توانی به‌منظور یافتن نقاط اثر توانی مرتبط با خروجی S-box در دور نخست، مقدار وزن همینگ برای خروجی S-box اول در دور نخست، اثرهای توانی بر اساس بزرگ‌تر و کوچک‌تر بودن از وزن همینگ ۴ به دو دسته تقسیم می‌شوند. میانگین هر دسته محاسبه شده و اختلاف این دو دسته از هم به دست می‌آید. همان‌طور که در شکل ۴ نشان داده شده است، بیشترین اختلاف بیان‌گر نقطه هدف است که در اینجا نقطه ۲۴۰ نقطه هدف یعنی خروجی S-box اول در دور نخست است.

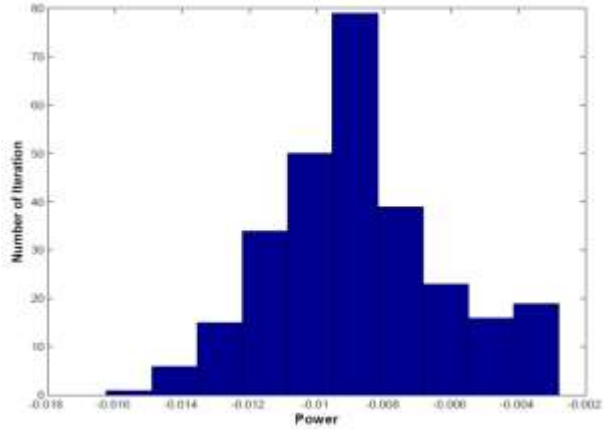
۳-۲-۳- تولید الگو

تولید الگو به معنای شناخت خصوصیات رفتاری اثر توانی وضعیت هدف است. بدین معنا که وقتی بر اساس وزن همینگ وضعیت میانی تولید الگو انجام می‌دهیم، خصوصیات هر وزن همینگ قابل‌تفکیک از خصوصیات وزن‌های همینگ دیگر باشد. با توجه به اینکه نقطه هدف، نقطه ۲۴۰ در گام پیشین به دست آمد، به توصیف خصوصیات اثر توانی در این نقطه خواهیم پرداخت. عملیات رمزنگاری برای یک داده مشخص را چندین بار تکرار کرده و اثرهای توان برای نقطه ۲۴۰ ذخیره می‌کنیم. سپس به‌منظور پی بردن به نحوه توزیع اثر توانی در نقطه ۲۴۰، هیستوگرام این نقطه را رسم می‌کنیم. با توجه به هیستوگرام نقطه ۲۴۰ نمایش داده‌شده در شکل ۵، متوجه می‌شویم که اثر توان در این نقطه دارای توزیع نرمال است.



شکل ٤: نقطه ۲۴۰ به‌عنوان نقطه هدف در اثر توانی

توزیع نرمال که توزیع گوسی نیز نامیده می‌شود در بسیاری از برنامه‌های کاربردی در عمل رخ می‌دهد. بنابراین توزیع نرمال ازنظر آماری بسیار مورد اهمیت است. تابع چگالی توزیع نرمال وابسته به دو پارامتر میانگین و انحراف معیار است. تابع چگالی احتمال توزیع نرمال یک نقطه به‌صورت معادله (۳) تعریف می‌شود.



شکل ٥: هیستوگرام اثر توانی نقطه ۲۴۰

تا به اینجا، مشخص شد که نقطه ۲۴۰ دارای توزیع نرمال اثر توانی است. با توجه به اینکه نه‌تنها نقطه ۲۴۰ بلکه رفتار نقاط همسایه این نقطه نسبت به این نقطه برای ما به‌منظور تولید الگو اهمیت دارد ما از توزیع نرمال چندمتغیره بهره گرفته‌ایم.

$$f(x)=\frac{1}{\sqrt{2.\pi.\sigma}}.\exp(-\frac{1}{2}.(\frac{x-\mu}{\sigma})^2) \qquad (۳)$$

توزیع نرمال چندمتغیره زمانی استفاده می‌شود که هم‌بستگی چند نقطه نسبت به هم مهم باشد. توزیع نرمال چندمتغیره می‌تواند به کمک ماتریس کوواریانس C و بردار میانگین m توصیف شود. احتمال تابع چگالی توزیع نرمال چندمتغیره از معادله ۴ به دست می‌آید.

$$f(x)=\frac{1}{\sqrt{2.\pi.\det(C)}}.\exp(-\frac{1}{2}.(x-m)'.C^{-1}.(x-m)) \qquad (۴)$$

برای تولید الگو برای هر وزن همینگ خروجی S-box در دور نخست، پنج نقطه ۲۳۸،۲۳۹،۲۴۰،۲۴۱ و ۲۴۲ را به‌عنوان نقاط هدف در نظر می‌گیریم و الگو برای هر وزن همینگ را به‌صورت یک ماتریس کوواریانس و بردار میانگین در نظر می‌گیریم. برای مثال الگو وزن همینگ صفر به‌صورت زیر نمایش داده می‌شود:

$$C_0=\begin{pmatrix} C_{238,238} & C_{238,239} & C_{238,240} & C_{238,241} & C_{238,242} \\ C_{239,238} & C_{239,239} & C_{239,240} & C_{239,241} & C_{239,242} \\ C_{240,238} & C_{240,239} & C_{240,240} & C_{240,241} & C_{240,242} \\ C_{241,238} & C_{241,239} & C_{241,240} & C_{241,241} & C_{241,242} \\ C_{242,238} & C_{242,239} & C_{242,240} & C_{242,241} & C_{242,242} \end{pmatrix}$$

$$m_0=(m_{238} \quad m_{239} \quad m_{240} \quad m_{241} \quad m_{242})'$$

۳-۲-۴- تطبیق الگو

در اصل، به‌منظور تطبیق الگو با اثر توانی گرفته‌شده از معادله ۴ استفاده می‌شود. اما ما در اینجا به‌منظور پرهیز از به توان رسیدن، از دو طرف معادله ۴ لگاریتم می‌گیریم. درنتیجه معادله ۴ به‌صورت معادله ۵ اصلاح می‌شود.

$$\ln p(t;(m,C))=-\frac{1}{2}(\ln((2.\pi)^{NIP}.\det(C))+(x-m)'.C^{-1}.(x-m)) \qquad (۵)$$

لذا به ازای هر اثر توانی گرفته‌شده در هنگام مخفی بودن کلید، به‌منظور محاسبه وضعیت میانی، معادله ۵ با هر وزن همینگ محاسبه می‌شود. آن احتمالی که مقدار بیشتری داشته باشد، می‌توان تشخیص داد که مقدار وضعیت میانی برابر الگو متناظر آن است.

۴- پیاده‌سازی مدل پیشنهادی

گام پیش‌پردازش حمله مکعبی کانال جانبی در محیط Visual C++ روی یک پردازنده Core-i3 با فرکانس باس ۳/۱ گیگاهرتز پیاده‌سازی شده است. به‌منظور بررسی کارایی مدل پیشنهادی حمله مکعبی کانال جانبی، این حمله را بر روی دو الگوریتم PERESENT-80 [۶] و AES-128/256 [۷] پیاده‌سازی کرده‌ایم. در زیر نتایج پیاده‌سازی بیان شده است.

۴-۱- پیاده‌سازی مدل پیشنهادی بر روی PRESENT-80

پس از اعمال حمله مکعبی کانال جانبی پیشنهادی، توانستیم ۴۸ معادله خطی از کلید را در دور نخست از الگوریتم PRSENT-80 استخراج کنیم. نتیجه استخراج ٤٨ معادله بازیابی ۳۲ بیت از کلید است. پس از اعمال مدل تکرار حمله مکعبی کانال جانبی توانستیم ١٦ معادله خطی دیگر از سیستم استخراج کنیم که به کمک آن‌ها توانستیم ٦٤ بیت در همان دور نخست بازیابی کنیم.

نتایج به‌دست‌آمده از مدل پیشنهادی حمله مکعبی کانال جانبی حاکی از آن است که پیچیدگی داده‌ای این مدل پیشنهادی به دلیل بهره‌گیری از بازیابی کلید در دور نخست الگوریتم PRESESNT-80، حذف ورودی‌های تکراری و بهره‌گیری از مدل تکرار کمتر از مدل‌های پیشین ارائه‌شده است. خلاصه‌ای از پیچیدگی داده‌ای حمله مکعبی

کانال جانبی بر روی PRESENT-80 در جدول ۶ نمایش داده شده است.

۴-۲- پیاده‌سازی مدل پیشنهادی بر روی AES-128/256

در طول گام پیش‌پردازش حمله مکعبی کانال جانبی بهبودیافته قادر به استخراج ۷ معادله خطی در ۰/۴۶۸ ثانیه و یک معادله غیرخطی در ۱/۱۹۷ ثانیه بر روی یک S-Box الگوریتم AES است. این اختلاف‌زمانی سرباری را که استخراج یک معادله درجه‌دو به همراه خواهد داشت را نشان می‌دهد. ما با بهره‌گیری از مدل تکرار از سربار استخراج معادلات درجه ۲ جلوگیری می‌کنیم. بدین ترتیب، توانسته‌ایم تا ۱۸ برابر در اعمال حمله مکعبی کانال جانبی سریع‌تر عمل کنیم.

جدول ٦: پیچیدگی داده‌ای حمله مکعبی کانال جانبی بر روی PRESENT-80

تعداد بیت بازیابی شده	تعداد متن اصلی منتخب	منبع
۴۸	2^{15}	یانگ [۸]
۶۴	2^{13}	عبدول لطیف [۱۰]
۴۸	2^{12}	ژائو [۱۱]
۷۲	$2^{15/154}$	ژائو [۱۲]
۸۰	$2^{10/2}$	ژانگ [۱۴]
۸۰	$2^{6/13}$	مدل پیشنهادی در این مقاله با بهره‌گیری از تکرار

جدول ۷ تابع خروجی S-Box اول در دور نخست را نشان می‌دهد. معادلات به‌دست‌آمده درجه یک، با توجه به ثابت بودن تابع S-Box ها، ثابت بوده و قابل بسط به دیگر S-Boxهای الگوریتم AES است. جدول ۸ معادله خطی استخراج‌شده پس از مدل تکرار را نشان می‌دهد که این معادله مقدارش وابسته به مقدار بیت کلید k_4 است. زمانی که $k_4 = 0$ معادله $F_{S(I)} = k_7$ استخراج می‌شود و وقتی $k_4 = 1$ باشد معادله خطی از کلید $F_{S(I)} = 1 + k_6$ است. این تعداد معادله استخراج‌شده برای هر S-box برای بازیابی ۱۲۸ بیت کلید در دور نخست کافی است. لازم به ذکر است، قبل از اعمال مدل تکرار، تنها قادر به بازیابی ۴۸ بیت کلید در هر دور بودیم. درحالی‌که با بهره‌گیری از این مدل قادر به بازیابی ۱۲۸ بیت کلید در هر دور هستیم.

نتایج به‌دست‌آمده در فاز برخط پس از راه‌اندازی سخت‌افزار رمز و نمونه‌برداری اثر توانی به‌منظور بازیابی مقدار وضعیت میانی به هنگام مخفی بودن کلید به ترتیب زیر است.

جدول ۷: معادلات خطی استخراج‌شده (AES)

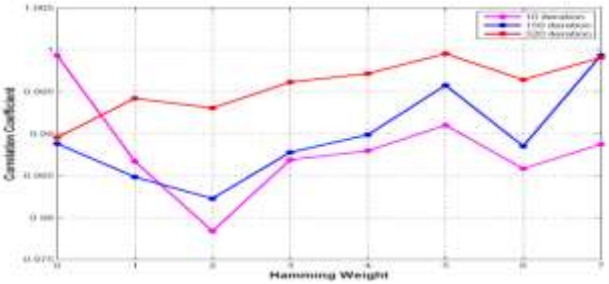
شاخص ورودی دور نخست	معادلات استخراج‌شده
I={۰،۱،۲،۳،۴،۵}	$1 + k_6 + k_7$
I={۶،۰،۱،۲،۳،۴}	k_5
I={۷،۵،۰،۱،۲،۳}	$1 + k_4$
I={۰،۱،۲،۴،۵،۶}	k_3
I={۰،۱،۳،۴،۵،۶}	$1 + k_2 + k_7$
I={۰،۲،۳،۴،۵،۶}	$k_1 + k_7$
I={۱،۲،۳،۴،۵،۶}	$1 + k_0 + k_7$

جدول۸: معادلات خطی استخراج‌شده (AES)

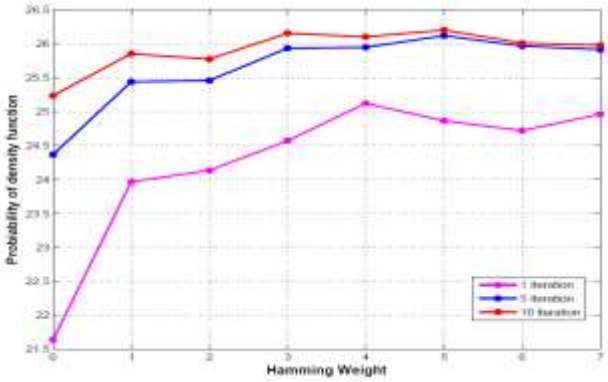
شاخص ورودی دور نخست	k_4	معادلات استخراج‌شده
I={۰،۱،۲،۳،۵}	۰	k_7
	۱	$1 + k_6$

حمله مکعبی کانال جانبی بهبودیافته به الگوریتم رمزنگاری AES پیاده‌سازی شده بر روی میکرکنترلر ARM با فرکانس ۴۸ مگاهرتز اعمال شده است. یک اسیلوسکوپ دیجیتال اختلاف ولتاژ بین دو سر مقاومت متصل شده به پایه منبع تغذیه میکروکنترلر را با نرخ ۱۵۰ نمونه بر ثانیه اندازه‌گیری می‌کند. میکروکنترلر ARM با بهره‌گیری از USB اطلاعات را از PC دریافت می‌کند. با توجه به توضیحات ارائه‌شده در فصل ۳ با ۱۲۵۰ نقطه نمونه‌برداری شده، تنها خروجی چهار S-box را قادر به موقعیت‌یابی در اثر توانی ذخیره شده هستیم. همان‌طور که در شکل ۶ نشان داده شد، نقطه هدف برای بایت نخست خروجی S-box نقطه ۲۴۰ است. پنج نمونه در اطراف این نمونه اثر توانی برای ایجاد کامل‌تر الگو در نظر می‌گیریم. به‌منظور بررسی دقت اندازه‌گیری مقدار وضعیت میانی با بهره‌گیری از تولید الگو بر اساس ماتریس کوواریانس و میانگین، تولید الگو پیشنهادی خود را با تولید الگو بر اساس میانگین مقایسه می‌کنیم.

برای مثال، هنگامی‌که وزن همینگ برابر ۵ است از الگو میانگین استفاده کرده‌ایم. همان‌طور که در شکل ۶ نشان داده شده است. با ۱۰ تکرار بر اساس الگو میانگین و تطبیق الگو همبستگی مقدار وزن همینگ به غلط مقدار ۴ به دست می‌آید. اما هنگامی‌که تعداد تکرار به ۳۲۰ تکرار می‌رسانیم، مقدار وزن همینگ به‌درستی به دست می‌آید. سپس، تولید الگو پیشنهادی یعنی ماتریس کوواریانس و بردار میانگین بهره می‌گیریم و در فاز تطبیق الگو از تابع چگالی احتمال چندمتغیره استفاده می‌کنیم. همان‌طور که در نمودار شکل ۷ مشاهده می‌کنید با ۱۰ تکرار ورودی و میانگین‌گیری از آن‌ها به‌منظور حذف نویز در هنگام مخفی بودن کلید، مقدار دقیق وزن همینگ را به دست آورده‌ایم. این نشان می‌دهد که تولید الگو و استفاده از استراتژی مناسب در تطبیق الگو نقش بسیار مهمی در سرعت اعمال حمله مکعبی کانال جانبی بازی می‌کند.



شکل ٦: محاسبه همبستگی به ازای وزن همینگ پنج و تعداد تکرار موردنیاز



شکل ۷: محاسبه تابع چگالی احتمال توزیع نرمال چند متغیره به ازای وزن همینگ ۵ و تعداد تکرار موردنیاز

در فاز آنلاین، نیاز به استخراج ۱۵۶ وزن همینگ مختلف برای هر S-box است. بنابراین پیچیدگی داده‌ای حمله مکعبی کانال جانبی برابر $2^{7/3}$ برای استخراج ۱۲۸ بیت کلید و $2^{7/75}$ (۱۵۶+۶۰) برای استخراج ۲۵۶ بیت کلید AES-128/256 است.

پیچیدگی زمانی حمله مکعبی کانال جانبی $2^{15/74}$ (۱۵۶ × ۳۵۰) برای بازیابی ۱۲۸ بیت کلید و $2^{16/2}$ برای بازیابی ۲۵۶ بیت کلید AES-128 و AES-256 به هنگام استفاده از الگو بر اساس میانگین است. این عدد را با بهره‌گیری از الگو بر اساس ماتریس کوواریانس و بردار میانگین به $2^{10/61}$ برای ۱۲۸ بیت کلید و $2^{11/07}$ بهبود داده‌ایم.

با توجه به ۵ نقطه N_{IP} برای ایجاد الگو، پیچیدگی حافظه‌ای به میزان قابل‌توجهی در حمله مکعبی کانال جانبی کاهش یافته است. به‌نحوی‌که پیچیدگی حافظه‌ای حمله مکعبی کانال جانبی $2^{7/65}$ (۱۵۶+۵ × ۹) برای AES-128 و $2^{8/03}$ برای AES-256 است. همان‌طور که در جدول ۹ می‌بینید، مدل پیشنهادی در این مقاله با بهره‌گیری از مدل تکرار و حذف ورودی‌های تکراری نسبت به حمله مکعبی کانال جانبی پیشنهادشده توسط دینر و شمیر [۱] بر روی الگوریتم AES دارای پیچیدگی داده‌ای، زمانی و حافظه‌ای بسیار کمتری است.

۵- بحث

در این بخش با توجه به نتایج به‌دست‌آمده از مدل پیشنهادی حمله مکعبی کانال جانبی از جنبه‌های مختلف بررسی شده است. در ابتدا، حمله مکعبی کانال جانبی در سناریوهای مختلف با حمله کانال جانبی مقایسه شده، سپس ازنظر تعداد پرسش و پاسخ و میزان موفقیت آن در برابر اقدامات متقابل برای جلوگیری از نشت توان، به بحث گذاشته می‌شود.

۵-۱- مقایسه حمله مکعبی کانال جانبی و حمله کانال جانبی

حمله کانال جانبی و حمله مکعبی کانال جانبی را نمی‌توان به‌طور دقیق ازنظر تعداد تحلیل‌های توانی موردنیاز مورد بررسی قرار داد. چراکه تعداد تحلیل‌های توان مصرفی و موفقیت حمله، به سیگنال به نویز و دقت در محاسبه مدل توانی دستگاه بستگی دارد. ازاین‌رو، بررسی و مقایسه بین حمله مکعبی کانال جانبی و حمله کانال جانبی را برحسب سناریوهای مختلف، توانایی در بازیابی یا عدم توانایی در بازیابی کلید بیان می‌کنیم.

جدول ۹: مقایسه بین مدل پیشنهادی و مدل دینر و شمیر بر روی AES

حمله	طول کلید	پیچیدگی داده‌ای	پیچیدگی زمانی	پیچیدگی حافظه‌ای
دینر و شمیر	۱۲۸	2^{28}	2^{35}	2^{28}
ارائه‌شده در این مقاله	۱۲۸	$2^{7/3}$	$2^{10/61}$	$2^{7/6}$
ارائه‌شده در این مقاله	۲۵۶	$2^{7/75}$	$2^{11/07}$	$2^{8/03}$

جدول ۱۰، سه سناریو مختلف را نشان می‌دهد. در سناریو یک، قادر به تغییر ورودی کلید هستیم. از طرف دیگر، نسبت به الگوریتم رمز استفاده‌شده در دستگاه مورد هدف آگاهی داریم. این فرض یک فرض بسیار قوی برای یک حمله رمزنگاری است. در سناریو یک، هم حمله مکعبی کانال جانبی و هم حمله کانال جانبی هر دو قادر به بازیابی کلید می‌باشند.

جدول ۱۰: موفقیت حمله مکعبی کانال جانبی و کانال جانبی در سناریوهای مختلف

سناریو	حمله کانال جانبی	حمله مکعبی کانال جانبی
سناریو۱: تغییر کلید و دسترسی به الگوریتم هدف	بله	بله
سناریو۲: عدم توانایی تغییر کلید. دسترسی به الگوریتم هدف.	بله	خیر
سناریو۳: تغییر کلید. عدم دسترسی به الگوریتم هدف	خیر	بله

در سناریو ۲، قادر به تغییر کلید نخواهیم بود، به‌اصطلاح کلید در سیستم قفل شده است و تنها به الگوریتم هدف دسترسی داریم. در این بخش با توجه به نتایج به‌دست‌آمده از مدل پیشنهادی حمله مکعبی کانال جانبی از جنبه‌های مختلف بررسی شده است. در ابتدا، حمله

مکعبی کانال جانبی در سناریوهای مختلف با حمله کانال جانبی مقایسه شده، سپس ازنظر تعداد پرسش و پاسخ و میزان موفقیت آن در برابر اقدامات متقابل برای جلوگیری از نشت توان، به بحث گذاشته می‌شود.

۵-۲- مقایسه حمله مکعبی کانال جانبی و حمله کانال جانبی

حمله کانال جانبی و حمله مکعبی کانال جانبی را نمی‌توان به‌طور دقیق ازنظر تعداد تحلیل‌های توانی موردنیاز مورد بررسی قرار داد. چراکه تعداد تحلیل‌های توان مصرفی و موفقیت حمله، به سیگنال به نویز و دقت در محاسبه مدل توانی دستگاه بستگی دارد. ازاین‌رو، بررسی و مقایسه بین حمله مکعبی کانال جانبی و حمله کانال جانبی را برحسب سناریوهای مختلف، توانایی در بازیابی یا عدم توانایی در بازیابی کلید بیان می‌کنیم.

جدول ۹: مقایسه بین مدل پیشنهادی و مدل دینر و شمیر بر روی AES

حمله	طول کلید	پیچیدگی داده‌ای	پیچیدگی زمانی	پیچیدگی حافظه‌ای
دینر و شمیر	۱۲۸	$۲^{۲۸}$	$۲^{۳۵}$	$۲^{۲۸}$
ارائه‌شده در این مقاله	۱۲۸	$۲^{۲۷/۳}$	$۲^{۱۰/۶۱}$	$۲^{۲۷/۶}$
ارائه‌شده در این مقاله	۲۵۶	$۲^{۲۷/۷۵}$	$۲^{۱۱/۰۷}$	$۲^{۲۸/۰۳}$

جدول ۱۰، سه سناریو مختلف را نشان می‌دهد. در سناریو یک، قادر به تغییر ورودی کلید هستیم. از طرف دیگر، نسبت به الگوریتم رمز استفاده‌شده در دستگاه مورد هدف آگاهی داریم. این فرض یک فرض بسیار قوی برای یک حمله رمزنگاری است. در سناریو یک، هم حمله مکعبی کانال جانبی و هم حمله کانال جانبی هر دو قادر به بازیابی کلید می‌باشند.

جدول ۱۰: موفقیت حمله مکعبی کانال جانبی و کانال جانبی در سناریوهای مختلف

سناریو	حمله کانال جانبی	حمله مکعبی کانال جانبی

این سناریو، تنها حمله کانال جانبی قابلیت بازیابی کلید را خواهد داشت و حمله مکعبی کانال جانبی در این سناریو غیرکارا خواهد بود.

در سناریو ۳، قادر به تغییر کلید هستیم ولی در مورد الگوریتم هدف هیچ‌گونه اطلاعاتی در دسترس نیست. درواقع این سناریو یک سناریو جعبه سیاه است. در سناریو ۳ تنها حمله مکعبی کانال جانبی قادر خواهد بود کلید را بازیابی کند و حمله کانال جانبی در این سناریو غیرکارا است

۵-۳- حمله مکعبی کانال جانبی در برابر اقدامات متقابل

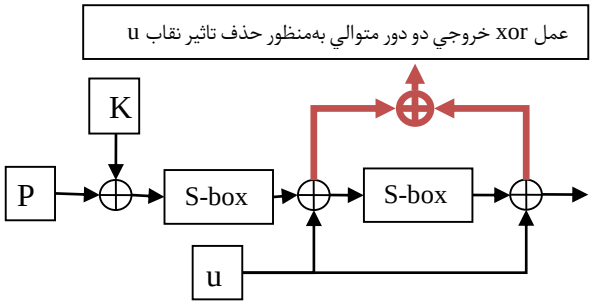
تکنیک‌های مختلفی از قبیل نقاب‌گذاری برای جلوگیری از نشت اطلاعات کانال جانبی وجود دارد. بررسی‌ها نشان می‌دهد که حمله مکعبی کانال جانبی تنها در سناریوی می‌تواند موفق باشد که الگوریتم رمز هدف از یک نقاب ثابت برای هر دور سیستم استفاده کند.

فرض کنید یک نقاب ثابت با نام u در سیستم استفاده شده است. نقاب u با تزریق مقادیر تصادفی به خروجی هر S-Box از نشت اطلاعات کانال جانبی معنادار از سیستم جلوگیری می‌کند. حمله مکعبی کانال جانبی می‌تواند بر روی این سناریو حمله موفقی داشته باشد. حمله مکعبی کانال جانبی به‌جای حمله به خروجی S-Box در یک دور، به جمع بولی خروجی S-Box دو دور متوالی مختلف حمله می‌کند.

جمع بولی بر روی خروجی دو S-Box نقاب‌گذاری شده در دو دور متفاوت باعث از بین رفتن تأثیر نقاب ثابت بر روی الگوریتم هدف می‌شود. شکل ۸ بیان‌گر این مهم است. اگر ما در هر دور از یک نقاب تصادفی متفاوت بهره ببریم، حمله مکعبی کانال جانبی قادر به بازیابی کلید در این ساختار نخواهد بود. این امر می‌تواند نکته بسیار مهمی در طراحی الگوریتم‌های رمز بلوکی باشد.

۶- نتیجه‌گیری

در این مقاله، ابتدا ساختار حمله مکعبی کانال جانبی با ارائه تکنیک‌های پیشرفته‌ای از قبیل جستجوی فضای محلی، شناسایی ورودی‌های تکراری و مدل تکرار پویا بهبود یافته است و نشان می‌دهد که حمله مکعبی کانال جانبی نه‌تنها بر روی الگوریتم‌های سبک‌وزن بلوکی از قبیل PRESESNT-80 بلکه بر روی الگوریتم‌های استاندارد بلوکی دیگر نیز مثل AES-128/256 می‌تواند به‌صورت کارا پیاده‌سازی شود. سپس نقاط ضعف و قدرت حمله مکعبی کانال جانبی بیان شده و این حمله با حمله کانال جانبی در سه سناریو مختلف مورد بررسی قرار گرفته است.



شکل ۸: استخراج تابع وضعیت میانی بر اساس xor دو دور مختلف به‌منظور از بین بردن تأثیر نقاب u

نتایج به‌دست‌آمده از مدل پیشنهادی حاکی از آن است که با اضافه کردن آزمون درجه دو به الگوریتم حمله مکعبی کانال جانبی می‌توانیم تعداد ۴۸ بیت کلید بازیابی شده در هر چرخه را به ۱۲۸ بیت در الگوریتم AES افزایش دهیم. شناسایی ورودی‌های تکراری باعث

کاهش ۴۱۶ وزن همینگ به ۱۵۶ وزن همینگ به‌منظور استخراج کلید می‌شود. مدل تکرار پویا باعث کاهش تأثیر طول کلید بر پیچیدگی داده‌ای و انتخاب دقیق تعداد نقاط هدف در مدل توانی باعث کاهش حافظه و افزایش دقت در به دست آوردن مقدار وزن همینگ در حمله مکعبی کانال جانبی می‌شود.

نتایج به‌دست‌آمده بیانگر آن است که برای بازیابی ۱۲۸ بیت از کلید الگوریتم AES-128، حمله مکعبی کانال جانبی پیشنهادی، نیازمند $۲^{۷/۳}$ متن اصلی منتخب و برای بازیابی ۲۵۶ بیت از کلید الگوریتم AES-256 نیازمند $۲^{۷/۷۵}$ متن اصلی منتخب است. این حمله بهترین حمله مکعبی کانال جانبی شناخته‌شده ازنظر تعداد متن اصلی منتخب بر روی الگوریتم AES-128/256 است. لذا، حمله مکعبی کانال جانبی می‌تواند به‌عنوان یک تهدید جدی برای الگوریتم‌های رمزنگاری بلوکی در نظر گرفته شود. علاوه این حمله می‌تواند به‌عنوان یک حمله ارزیابی فیزیکی در طراحی سخت‌افزارهای رمزنگاری استفاده شود.

با توجه به نتایج به‌دست‌آمده در فاز برخط حمله مکعبی کانال جانبی، درست است که توانستیم ۳۲۰ تکرار در ورودی به‌منظور حذف نویز را با بهره‌گیری مدل‌سازی نویز گوسی به ۵ الی ۱۰ تکرار برسانیم. ولی ۱۰ تکرار در شرایط عملی که فقط ممکن است شما یک فرصت اندازه‌گیری توانی داشته باشید، عدد بزرگی به نظر می‌رسد. با حضور نویز، به دست آوردن مقدار وضعیت میانی بزرگ‌ترین چالش در حمله مکعبی کانال جانبی است و تحقیقات بیشتر در این زمینه حس می‌شود. به نظر می‌رسد الگوریتم‌های هوشمندی همچون شبکه عصبی به‌منظور تولید و تطبیق الگو می‌تواند ما را در این مهم یاری رساند و به‌عنوان بستر مناسب تحقیقاتی در آینده دیده شود.

مراجع

[1] I. Dinur and A. Shamir, "Side channel cube attacks on block ciphers," Cryptology ePrint Archive, http://eprint.iacr.org/2009/127.pdf

[2] I. Dinur and A. Shamir, "Cube attacks on tweakable black-box polynomials," In: Advances in Cryptology – EUROCRYT, vol. 5479, pp. 278–299, 2009.

[3] P. C. Kocher, J. Jaffe and B. Jun, "Differential power analysis," In: Advances in CryptologyCRYPTO 1999, LNCS, vol. 1666, pp. 388–397, 1999.

[4] J. J. Quisquater and D. Samyde, "A new tool for non-intrusive analysis of smart cards based on electro-magnetic emissions: the SEMA and DEMA methods," In: Eurocrypt Rump Session.

[5] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," In: Advances in Cryptology CRYPTO 1996, LNCS, vol. 1109, pp. 104–113, 1996.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe, "PRESENT: an ultra-lightweight block cipher", In: Paillier, CHES 2007. LNCS, vol. 4727, pp. 450–466, 2007.

[7] J. Daemon and V. Rijnemn, "AES proposal: Rijndael. technical evaluation," CD-1: Documentation, 1198.

[8] L. Yang, M. Wang and S. Qiao, "Side channel cube attack on PRESENT," In Proceeding of the 8th International Conference on Cryptology and Network Security, vol. 5888, pp. 379- 391, 2009.

[9] S. F. Abdul-Latip, M. R. Reyhanitabar, W. Susilo and J. Seberry, "Extended cubes enhancing the cube attack by extracting low-degree non-linear equations," In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security – ASIACCS 2011, ACM Society, pp. 296–305, 2011.

[10] X. Zhao, S. Guo, F. Zhang, T. Wang, Z. Shi, H. Liu, K. Ji and J. Huang, "Efficient hamming weight-based side-channel cube attacks on PRESENT," Journal of Systems and Software, vol. 86, no. 3, pp. 728–743, March 2013.

[11] X. Zhao, T. Wang and S. Guo, "Improved side channel cube attacks on PRESENT," Cryptology ePrint Archive, http://eprint.iacr.org/2011/165.pdf

[12] X. Zhao, S. Guo, F. Zhang ,T. Wang, Z. Shi, H. Liu, K. Ji and J. Huang, "Black-box side-channel cube attacks on Present-like ciphers," IMCCC '13 Proceedings of the 2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 1352-1358, 2013.

[13] Z. Li, B. Zhang, J. Fan and I. Verbauwhede, "A new model for error-tolerant side-channel cube attacks," Cryptographic Hardware and Embedded Systems - CHES 2013, Lecture Notes in Computer Science Volume 8086, pp. 453-470, 2013.

[14] S. F. Abdul-Latip, M. R. Reyhanitabar, W. Susilo and J. Seberry, "On the security of NOEKEON against side channel cube attacks," In: Proceedings of the 5th InformationSecurity Practice and Experience Conference. Future Conference – ISPEC2010, LNCS, vol. 6047, pp. 45–55, 2010.

[15] G. V. Bard, N. T. Courtois, J. Nakahara, P. Sepehrdad and B. Zhang, "Algebraic, AIDA/cube and side channel analysis of KATAN family of block ciphers," In: Progress in Cryptology-indocryt, LNCS, vol. 6498, pp. 176–196, 2010.

[16] X. Fan and G. Gong, "On the security of Hummingbird-2 against side channel cube attacks," In: Proceedings of WEWoRC 2011, pp. 100–104, 2011.

[17] Z. Li, B. Zhang, Y. Yao and D. Lin, "Cube cryptanalysis of LBlock with noisy leakage," Information Security and Cryptology – ICISC 2012, Lecture Notes in Computer Science, vol. 7839, pp. 141-155, 2013.

[18] S. Islam, M. Afzal and A. Rashdi, "On the security of LBlock against the cube attack and side channel cube attack," Security Engineering and Intelligence Informatics, Lecture Notes in Computer Science, vol. 8128, pp. 105-121, 2013.

[19] S. F. Abdul-Latip, M. R. Reyhanitabar, W. Susilo and J. Seberry, "Extended cubes enhancing the cube attack by extracting low-degree non-linear equations," In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 296–305, 2011.

[20] Z. Li, B. Zhang, J. Fan and I. Verbauwhede, "A new model for error-yolerant side-channel cube attacks," Cryptographic Hardware and Embedded Systems, pp. 453-470, 2013.

[21] S. Mangard, E. Oswald and T. Popp, *Power analysis attacks*, Springer, Berlin Heidelberg, 2007.

[22] J. Daemen, V. Rijmen, "AES Proposal: Rijndael," National Institute of Standards and Technology. pp. 1. 2013.

[23] M. Blum, M. Luby and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems," Journal of Computer and System Sciences, vol. 47, pp. 549–595, 1993.