مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۲، تابستان ۱۳۹۷، ص ۱۳۴-۱۲۳

یک روش جدید و کارآمد نقاب‌گذاری جمعی و ارزیابی مقاومت آن در برابر تحلیل توان

مسعود معصومی[1*]، علی دهقان منشادی[2]، اقبال مددی[3]، سبحان ساعی مقدم[3]

۱- استادیار، دانشکده فنی دانشگاه آزاد واحد اسلامشهر، ۲ - کارشناس ارشد مخابرات، دانشگاه تربیت مدرس ۳- کارشناس ارشد الکترونیک

(دریافت: ۹۶/۰۷/۱۴، پذیرش: ۹۶/۱۱/۰۹)

چکیده

تحلیل توان برای بازیابی کلید از وابستگی توان مصرفی ابزار رمزنگاری به مقادیر میانی در حین اجرای الگوریتم استفاده می‌کند. از این‌رو، برای جلوگیری و ناکام گذاشتن حمله، این وابستگی باید تا حد ممکن کاهش یافته یا از بین برود. در سال‌های اخیر تحقیقات زیادی برای مقابله با حمله تحلیل توان انجام شده است. از جمله مهم‌ترین این روش‌ها می‌توان به نقاب‌گذاری مقادیر میانی با استفاده از مقادیر تصادفی با هدف پنهان کردن مقادیر وابسته به کلید رمز و متغیرهای میانی حساس الگوریتم رمز اشاره کرد. در این مقاله یک روش جدید و کارآمد برای نقاب‌گذاری (جمعی) الگوریتم رمز پیشرفته استاندارد پیشنهاد شده که در مقایسه با نقاب‌گذاری مرتبه اول، متداول و حتی روش نقاب‌گذاری مجزا از عملکرد و کارایی بالاتری از نظر میزان نشت اطلاعات و نیز میزان سربار پیاده‌سازی برخوردار است. امنیت روش پیشنهادی با آزمایش عملی عملکرد آن بر روی بستر کارت هوشمند بورد استاندارد ارزیابی حملات کانال جانبی و همچنین آزمون **T** نمونه‌های توان به‌دست‌آمده ارزیابی و بررسی شده است. نتایج پیاده‌سازی، نشان می‌دهد که حتی پس از پنج هزار بار نمونه‌گیری میزان نشت اطلاعات توان و مقدار آزمون **T** روش نقاب‌گذاری پیشنهادی همچنان زیر مقدار آستانه باقی می‌ماند و در برابر حمله مرتبه دوم نیز مقاوم است. در حالی‌که، مقدار آزمون **T** روش نقاب‌گذاری مرتبه اول متداول و نقاب‌گذاری مجزا هر دو از سطح آستانه تجاوز می‌کنند.

واژه‌های کلیدی: الگوریتم پیشرفته رمز استاندارد، تحلیل کانال جانبی توان، نقاب‌گذاری، آزمون T

۱- مقدمه[1]

حملات تحلیل توان نوعی از حملات رمزشکنی هستند که مهاجم را قادر به استخراج اطلاعات حساس از ابزار رمز می‌کنند. این حملات از خانواده حملات غیرمهاجم و غیرفعال هستند و به‌جای استفاده از روش‌های ریاضی یا تحلیل‌های آماری دنباله خروجی رمز، از ویژگی‌ها واطلاعات نشتی توان مصرفی ابزار برای دست‌یابی به اطلاعات حساس آن استفاده می‌کنند. الگوی مصرف توان یا انرژی مصرفی یک سخت‌افزار می‌تواند اطلاعات مهمی در مورد دستورالعمل‌های اجرا شده توسط آن، توالی اجرای دستورالعمل‌ها و حتی عمل‌وندها در اختیار مهاجم قرار بدهد. این حملات برای پیاده‌سازی نیاز به تجهیزات و ادوات گران‌قیمت ندارند و با وسایل در دسترس در یک آزمایشگاه مدرن الکترونیک قابل پیاده‌سازی هستند و از این‌رو، یک تهدید کاملاً جدی برای امنیت سامانه‌های رمز معاصر هستند. تحلیل توان ساده، روشی است که مستقیماً از تفسیر اندازه‌گیری‌های مصرف توان در حین اجرای عملیات رمز برای تحلیل آن استفاده می‌کند و در غالب مواقع لازم است تا مهاجم از الگوریتم و نیز تا حدی از نحوه پیاده‌سازی آن آگاهی داشته باشد. اما حملات تفاضلی توان، به‌مراتب قدرتمندتر و موثرتر هستند. تحلیل تفاضلی توان نیازی به دانستن جزئیات پیاده‌سازی ندارد و از این‌رو، مقابله با آن به‌سادگی تحلیل توان ساده نیست. این حمله به‌طور معمول قسمتی از الگوریتم رمز که در آن بخشی از کلید رمز مورد پردازش قرار می‌گیرد را هدف قرار می‌دهد [۵-۱]. در سال‌های اخیر تحقیقات زیادی برای مقابله با حمله تحلیل توان انجام شده است. بر این مبنا این روش‌ها را می‌توان به دو دسته روش‌های مقابله نرم‌افزاری و روش‌های مقابله سخت‌افزاری تقسیم‌بندی کرد. روش‌های نرم‌افزاری روش‌هایی مانند تصادفی کردن کدها، شیفت‌دهنده‌ها و تاخیردهنده‌های تصادفی و افزودن واحدهای مصرف‌کننده توان به‌صورت تصادفی هستند که باعث به‌هم‌ریختن پروفایل مصرف توان و مشکل‌تر

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

شدن کار مهاجم می شوند اما نمی‌توانند جلوی انجام حمله را گرفته یا حمله را به‌طور کامل خنثی سازند. روش‌های مختلفی در سطح سخت‌افزار برای عقیم گذاشتن حملات تحلیل توان بسته به نوع الگوریتم و بستر پیاده‌سازی آن پیشنهاد شده که در سطوح مختلف از سطح گیت و الگوریتم تا سطح معماری پیاده‌سازی و پروتکل قابل به‌کارگیری هستند. از جمله این روش‌ها می‌توان به نقاب‌گذاری[1] مقادیر میانی با استفاده از مقادیر تصادفی با هدف پنهان کردن مقادیر و متغیرهای میانی حساس، پنهان‌سازی[2] با هدف مستقل‌سازی توان مصرفی ابزار رمز از مقادیر میانی حساس و عملیات های وابسته به آنها و کور کردن[3] به‌معنای استفاده از نقاب‌های ریاضی برای محافظت از الگوریتم‌های نامتقارن اشاره کرد. البته پیاده‌سازی این ایده‌ها در بسترهای مختلف مقوله‌ای چالش برانگیز و متفاوت است. به‌عنوان مثال در نقاب‌گذاری الگوریتم رمز پیشرفته استاندارد، محاسبه جداول نقاب‌گذاری‌شده جانشینی بایت‌ها کارایی پیاده‌سازی را بسیار کاهش می‌دهد و حتی در برخی موارد اجرای عملیات نقاب‌گذاری به‌اندازه اجرای خود الگوریتم طول می‌کشد [۶]. علاوه بر آن، غالب روش‌های ارائه‌شده مبتنی بر نقاب‌گذاری مرتبه اول از امنیت لازم برای مقابله با انواع حملات تحلیل توان از مرتبه بالاتر (و حتی مرتبه اول) برخوردار نیستند و روش‌های نقاب‌گذاری مرتبه بالاتر نیز هزینه زیادی را به کاربر تحمیل می‌کنند به‌نحوی‌که در عمده موارد این روش‌ها قابل پیاده‌سازی بر روی بسترهای کم وزن و هشت بیتی مانند کارت‌های هوشمند نیستند [۷]. در این مقاله روش جدید و کارآمدی برای غلبه بر نقطه ضعف امنیتی نقاب‌گذاری جمعی مرتبه اول ارائه شده که نه تنها از امنیت بالاتری در برابر تحلیل توان برخوردار است و قادر به عقیم گذاشتن حملات مرتبه اول و دوم توان است بلکه هزینه پیاده‌سازی به‌مراتب کمتری در مقایسه با سایر کارهای گزارش‌شده را به کاربر تحمیل می‌کند. روش پیشنهادی به‌صورت عملی در مورد الگوریتم پیشرفته رمز استاندارد بر روی بورد استاندارد ارزیابی حملات کانال جانبی موسوم به ساسبو[4] [۸] پیاده‌سازی شده و نتایج در هر دو حوزه زمان و فرکانس [۹] مورد بررسی قرار گرفته است. علاوه بر آن نتایج با استفاده از آزمون آماری T^5 [۱۰] نیز مورد تحلیل و ارزیابی قرار گرفته اند که نتایج به‌دست‌آمده از این آزمون نشان دهنده کارآمدتر بودن روش پیشنهادی از حیث مقاومت در برابر تحلیل توان در مقایسه با نقاب‌گذاری مرتبه اول است. در ادامه مقاله ابتدا در بخش (۲) به‌طور مختصر حملات تحلیل توان را مرور خواهیم کرد سپس در بخش (۳) نقاب‌گذاری جمعی مرتبه اول و نقاط ضعف آن را تشریح خواهیم نمود. سپس در ادامه آزمون آماری T را در بخش (۴) به‌طور مختصر مرور خواهیم کرد. پس از آن به تشریح روش نقاب‌گذاری پیشنهادی در بخش (۵) خواهیم پرداخت. در بخش (۶) نتایج پیاده‌سازی تحلیل‌های مرتبه اول و دوم را بر روی پیاده‌سازی هر دو روش نقاب‌گذاری متعارف و نقاب‌گذاری پیشنهادی و نیز نتایج تحلیل آماری T را ارائه خواهیم داد. سپس انتها به جمع‌بندی نتایج پرداخته و نتایج نهایی را ارائه خواهیم داد.

1- Masking
2- Hiding
3- Blinding
4- Side-Channel Standard Evaluation Board (SASEBO)
5- T-Test

۲- حملات تحلیل توان

حملات تحلیل توان از نوع حملات غیرتهاجمی هستند که نیاز به تغییر فیزیکی یا آسیب رساندن به ابزار رمز ندارد. این حملات از نشت اطلاعات فیزیکی مرتبط با پیاده‌سازی الگوریتم در حین انجام عملیات رمز استفاده می‌کنند. ایده اصلی در پس این روش در یک ویژگی جذاب فن آوری CMOS[6] از دیدگاه رمزشکنی نهفته است: عمده توان مصرف‌شده در این فن آوری هنگامی اتفاق می‌افتد که ترانزیستورها بین حالت روشن و خاموش سوئیچ می‌کنند و از این‌رو، اطلاعات فیزیکی مانند توان مصرفی هم‌بسته با داده‌های در حال پردازش به بیرون نشت می‌کند. این کلاس از حملات بسیار قدرتمند هستند و نیاز به تجهیزات گران‌قیمت ندارد. به‌طور معمول اطلاعاتی که از این نوع به بیرون نشت می‌کند و قابل اندازه‌گیری است توان مصرفی ابزار رمز و نیز تشعشعات ساطع شده از تراشه رمز در زمان اجرای الگوریتم است. یک کارت هوشمند فاقد محافظت‌های ویژه در برابر این حملات با ثبت نشت اطلاعات صدها یا چند هزار عملیات رمز در زمان کوتاهی (چند دقیقه یا چند ساعت با استفاده از یک رایانه شخصی متداول) قابل شکستن است خواه الگوریتم رمز آن الگوریتمی متقارن مانند DES یا AES[7] یا الگوریتمی غیرمتقارن مانند ECC[8] یا RSA[9] باشد.

تحلیل تفاضلی توان که برای اولین بار توسط کوچر و همکارانش منتشر شد روش قدرتمندی است که پیاده‌سازی فیزیکی الگوریتم رمز را مورد هدف قرار می‌دهد و مهاجم را قادر به حدس زدن کلید مخفی در بسیاری از اشکال رمزنگاری می‌سازد. پس از انتشار مقاله اولیه، محققین بسیاری این حمله را بهبود داده و یا روش‌های مختلفی برای محافظت از پیاده‌سازی الگوریتم‌های رمز در برابر این حملات را تشریح کرده اند. این

6- Complementary-Metal-Oxide-Semiconductor
7- Advanced Encryption Standard Algorithm
8- Elliptic Curve Cryptography
9- Rivest-Shamir-Adleman

حمله یک حمله نوع سوم[1] با معلوم بودن متن آشکار و متن رمزشده معادل آن است. مهاجم N متن آشکار ورودی[2] (PTI) را به رمزکننده داده و متناظر با آن N متن رمزشده خروجی معادل[3] (CTO) را دریافت می‌کند و توان مصرفی هر عملیات رمز را ردیابی و ذخیره می‌کند در حالی که کلید مخفی درون ابزار رمز ذخیره شده است. البته این مشاهدات باید به‌خوبی هم‌تراز باشد به‌نحوی که اندیس زمانی تمام عملیات رمز در همه اندازه-گیری‌ها باید یکسان باشد. پس از جمع‌آوری تعداد لازم از مشاهدات مصرف توان، مهاجم به تحلیل آماری آنچه به‌دست آمده می پردازد. در حمله به الگوریتم استاندارد رمز پیشرفته، مهاجم به‌طور معمول کلید دور اول را هدف می‌گیرد و از آنجا که مجموعه تمام مقادیر کلید دور اول فضای نسبتا بزرگی را تشکیل می‌دهد، این مجموعه مقادیر را به هشت قسمت شش بیتی که زیرکلید[4] خوانده می‌شوند تقسیم می‌کند و به هرکدام جداگانه حمله می‌کند [۲].

در حمله به الگوریتم استاندارد رمز پیشرفته، مهاجم برای هر بایت زیرکلید مورد حمله یک فرض در نظر می‌گیرد و بر مبنای آن فرض خروجی تبدیل جانشینی بایت‌های متناظر را محاسبه می‌کند. این مقدار، مقدار میانی[5] نامیده شده و با IV نشان داده می‌شود. شخص کنجکاو، سپس یک بیت خاص از این چهار بیت مثلا کم‌ارزش‌ترین بیت (LSB) آن را در نظر می‌گیرد. اگر این بیت IV برابر صفر باشد، مشاهده مصرف توان متناظر با آن (T_1) در مجموعه A قرار می‌گیرد و در غیر این‌صورت در مجموعه B قرار می‌گیرد. شخص کنجکاو این کار را برای تعدادی (مثلا چند ده یا چند صد) مشاهده مصرف توان زوج متن آشکار و رمزشده معادل آن انجام می‌دهد. سپس از هر دو دسته میانگین می‌گیرد و تفاضل آنها را محاسبه می‌کند. اگر منحنی تفاضل با Δ نشان داده شود، برای هر حدس از کلید K_s، Δ به این‌صورت محاسبه می‌شود [۲].

$$\Delta_{K_s}[j] = \frac{\sum_{i=1}^{N} D(PTI_i, K_s) T_i[j]}{\sum_{i=1}^{N} D(PTI_i, K_s)} - \frac{\sum_{i=1}^{N} (1 - D(PTI_i, K_s)) T_i[j]}{\sum_{i=1}^{N} (1 - D(PTI_i, K_s))} \quad (۱)$$

جائی‌که $\Delta_{K_s}[j]$، j امین نمونه منحنی تفاضل را نشان می‌دهد، N تعداد مشاهدات، PTI_i نشان‌دهنده i امین متن آشکار، $T_i[j]$ نشان‌دهنده j امین نمونه مشاهده و D تابع تصمیم‌گیری[6] است که مشاهدات را در گروه A یا B قرار می‌دهد و تابع انتخاب۷ نیز نامیده می‌شود. اگر فرض در نظر گرفته‌شده برای آن زیرکلید غلط باشد، تمام محاسبات میانی غلط در مقایسه با آن‌چه واقعاً در تراشه اتفاق افتاده غلط خواهد بود و در حقیقت مشاهدات به‌طور تصادفی در دو دسته A و B قرار گرفته‌اند. در این‌صورت میانگین دو دسته A و B بسیار نزدیک به یکدیگر خواهد بود و منحنی تفاضل یک منحنی شبه نویز خواهد بود. در غیر این‌صورت در صورت صحیح بودن حدس اولیه در مورد آن بیت خاص از زیرکلید، محاسبات با آن‌چه واقعاً در تراشه اتفاق افتاده همبستگی خواهد داشت. با توجه به این مساله، در اندیس زمانی خاصی که مقدار میانی مرتبط با کم‌ارزش‌ترین بیت IV مورد پردازش قرار می‌گیرد، اگر این بیت صفر باشد، توان اضافه‌ای برای پردازش آن مصرف نخواهد شد. بالعکس چنانچه این بیت یک باشد مقدار کمی توان بیشتر برای پردازش آن مصرف خواهد شد و لذا در آن لحظه (پالس ساعت) خاص در مجموعه B توان بیشتری در مقایسه با مجموعه A مصرف خواهد شد. از این‌رو چنانچه تفاضل این دو دسته را محاسبه کنیم در آن لحظه خاص، در منحنی تفاضل یک یا چند ضربه دیده می‌شود که نشان دهنده درست بودن فرض اولیه درباره زیرکلید است.این تحلیل هم در حوزه زمان و هم در حوزه فرکانس قابل اجراست جایی‌که تفاضل مورد اشاره از نمونه‌های طیف توان گرفته می‌شود [۲].

از بین انواع حملات تحلیل توان، حملات موسوم به حملات همبستگی با استفاده از ابزار شناخته‌شده آماری ضریب همبستگی پیرسون[8] از سایر انواع این حملات موثرتر و قدرتمندتر هستند. اگر X و Y دو متغیر تصادفی فرض شوند، $cov(X,Y)$ کوواریانس X و Y و σ_X و σ_Y به‌ترتیب انحراف معیارهای X و Y باشند آنگاه ضریب همبستگی پیرسون به‌صورت رابطه (۲) محاسبه می‌شود.

$$\rho(X,Y) = \frac{cov(X,Y)}{\sigma_X \sigma_Y} \quad (۲)$$

این تابع میزان وابستگی دو کمیت به یکدیگر را اندازه‌گیری می‌کند. در مورد حملات کانال جانبی دلیل استفاده از این تابع تقریباً واضح است. اگر N تعداد مشاهدات مصرف توان، K_s فرض کلید، PTI_i نماد i امین متن آشکار ورودی، $H(Ks, PTI_i)$ تعداد بیت‌های سوئیچ‌کننده بر مبنای فرض کلید و متن آشکار ورودی، $T_i(j)$ نشان‌دهنده j امین نمونه مشاهده i ام باشد آنگاه معادله (۲)

1- Chosen Plain-Text Attack
2- Plain-Text Input
3- Cipher-Text Output
4- Sub Key
5- Intermediate Value

6- Decision Function
7- Selection Function
8- Pearson's Correlation Coefficient

به‌صورت معادله (۳) در می‌آید [۲].

$$\rho_{K_s}(j) = \frac{N.\ \sum_{i=1}^{N} H(K_s, PTI_i).T_i(j) - \sum_{i=1}^{N} H(K_s, PTI_i).\ \sum_{i=1}^{N} T_i(j)}{\sqrt{N.\sum_{i=1}^{N} H(K_s, PTI_i)^2 - (\sum_{i=1}^{N} H(K_s, PTI_i))^2} \times \sqrt{N.\sum_{i=1}^{N} T_i(j)^2 - (\sum_{i=1}^{N} T_i(j))^2}} \quad (۳)$$

۳- نقاب‌گذاری جمعی

یکی از روش‌های مقابله با تحلیل توان در سطح الگوریتم روش نقاب‌گذاری است. نقاب‌گذاری بر روی متغیرهای درونی اعمال شده و آنها را تبدیل به اشتراکی از متغیرهای نقاب‌گذاری‌شده و خود نقاب‌ها می‌کند. البته نقاب‌گذاری هم به‌روش سخت‌افزاری و هم به‌صورت نرم‌افزاری قابل پیاده‌سازی است و مطالعات زیادی نیز در این مورد انجام شده است. [۱۰-۶]. این روش بر مبنای پنهان کردن متغیر حساس درونی x توسط نقاب m. این روش بر مبنای پنهان کردن متغیر حساس درونی x توسط نقاب m است که مقادیر تصادفی را به‌خود می‌گیرد. در یک سامانه رمز نقاب گذاری شده، متغیر درونی x بطور مستقیم وجود ندارد ولی می‌توان آن‌را با زوج $(m, x_m = x \circledast m)$ بازسازی کرد. جایی‌که x_m متغیر نقاب‌گذاری‌شده و $\circledast$ یک عملیات است که ممکن است ریاضی (مانند عمل ضرب) یا منطقی (جمعی) باشد. نقاب‌گذاری جمعی از عملگر جمع انحصاری ($\oplus$) استفاده می‌کند.

نقاب‌گذاری ریاضی از یک عملیات پیمانه‌ای مانند ضرب یا جمع پیمانه‌ای در میدان محدود استفاده می‌کند.

$$x_m = x + m \ (mod\ n)$$

$$x_m = x * m \ (mod\ n)$$

جایی‌که $n = 2^{|m|} = 2^{|x|}$ تعداد مقادیر حساس یا نقاب‌ها است. در پیاده‌سازی نقاب‌گذاری، اگر تابع f ویژگی خطی بودن زیر را داشته باشد آنگاه پیاده‌سازی ساده خواهد بود.

$$f(x \circledast m) = f(x) \circledast f(m)$$

که $\circledast$ یک عملگر جمعی است.

مقدار تابع f(x) را می‌توان با به‌کارگیری f(x ⊛ m) و $f(m)^{-1}$ به‌دست آورد و بنابراین محاسبه f(x) را می‌توان در انتهای الگوریتم انجام داد که این باعث جلوگیری از نشت مستقیم اطلاعات می‌شود زیرا x ⊛ m و m مستقل از x هستند. اگر f تابعی غیرخطی باشد ساختار به‌مراتب پیچیده‌تر خواهد شد زیرا f(x) را نمی‌توان به‌راحتی از f(x ⊛ m) و f(m) به‌دست آورد.

در رمزنگاری متقارن، به‌طور معمول قسمت غیرخطی الگوریتم‌ها SBox های آن است.

قبلا و در گزارش‌های متعدد نشان داده شده که نقطه آسیب‌پذیر الگوریتم رمز استاندارد تابع تبدیل غیرخطی جانشینی بایت‌های دور اول آن است جایی‌که کلید رمز با متن آشکار جمع شده و وارد این تبدیل می‌شود. بدیهی است که برای عقیم گذاشتن تحلیل توان در این نقطه باید همبستگی بین مقادیر واقعی پردازش‌شده در این نقطه و مصرف توان را از بین برد. این تبدیل عمدتا در پیاده‌سازی‌های نرم‌افزاری و حتی سخت‌افزاری به‌صورت جدول Look-up پیاده‌سازی می‌شود که خروج داده‌های واقعی از این جدول باعث نشت اطلاعات می‌شود. با نقاب‌گذاری مناسب داده‌های ورودی می‌توان همبستگی بین داده‌های واقعی و مقادیر مصرف توان را از بین برد. ساده‌ترین نوع نقاب‌گذاری، نقاب‌گذاری جمعی یا بولی[1] است که قبلا نیز در مورد آن صحبت شد بدین مفهوم که قبل از اینکه داده‌ها وارد جدول جانشینی بایت‌ها بشوند با مقدار تصادفی n جمع شده و سپس وارد جدول مزبور می‌شوند. شکل (۱) روال نقاب‌گذاری تبدیل جانشینی بایت‌ها را در الگوریتم رمز پیشرفته استاندارد نشان می‌دهد جایی‌که n نقاب ورودی و m نقاب خروجی است. مطابق با الگوریتم مزبور، نقاب ورودی باعث جایگشت عناصر جدول جانشینی بایت‌ها شده و تمام عناصر با نقاب خروجی جمع می‌شوند. پس از خروج هر عنصر از جدول مجدداً آن عنصر با نقاب خروجی جمع شده و نقاب داده‌ها برداشته می‌شود.

$$S(p \oplus k) = y \quad (۴)$$

$$S^*(p \oplus k \oplus n) = y \oplus m \quad (۵)$$

Require n, m
Output: $S^*(x+n) = S(x) + m$
1. for i = 0 to 255 do
2. $S^*(i+n) = S(i) + m$;
3. end
Return $S^*()$

شکل (۱): نقاب‌گذاری کلاسیک تبدیل جانشینی بایت‌ها در الگوریتم رمز پیشرفته استاندارد [۱].

البته برای امنیت بیشتر بهتر است نقاب‌ها بعد از چند بار اجرای الگوریتم تعویض شده و تمام عناصر جدول با عدد تصادفی r جمع شوند.

مطابق با گزارشات منتشرشده در منابع مربوطه، نقاب‌گذاری مرتبه اول نمی‌تواند از پیاده‌سازی الگوریتم در برابر حملات مرتبه دوم یا بالاتر توان محافظت نماید. حمله مرتبه دوم یک یا تعداد

[1] Boolean

بیشتری نمونه را در یک مشاهده ترکیب می‌کند و مهاجم با محاسبه ویژگی‌های آماری توام[1] در چند زمان نمونه‌گیری قادر به شکستن نقاب‌های مقاوم در برابر حملات مرتبه اول خواهد بود. در واقع یک حمله مرتبه n ام حمله‌ای است که مهاجم از n نمونه مختلف از سیگنال توان متناظر با n نقطه میانی الگوریتم برای شکستن نقاب و رمز استفاده می‌کند. برای فهم کارکرد کلی این حمله، AES نقاب‌گذاری‌شده که در قبل به آن پرداختیم را در نظر می‌گیریم جایی‌که داده‌های ورودی قبل از سفیدسازی اولیه با مقدار تصادفی نقاب جمع شده و در مرحله بعد بایت به بایت با کلید رمز جمع می‌شوند. شکل (۲) شبه کد پیاده‌سازی دو قسمت از الگوریتم یا در واقع همان سفیدسازی اولیه را در دو حالت بدون نقاب و نقاب‌گذاری‌شده نشان می‌دهد که پیاده‌سازی نقاب‌گذاری‌نشده در برابر تحلیل مرتبه اول و پیاده‌سازی نقاب‌گذاری‌شده در برابر تحلیل مرتبه دوم توان آسیب‌پذیر است.

پیاده‌سازی نقاب‌گذاری‌شده	پیاده‌سازی نقاب‌گذاری‌نشده
B:{Generate random Mask *m* mPTI = PTI ⊕ m; C: Cinput = PTI ⊕ SecretKey; 10 Consecutive Rounds; Return Coutput}	A:{Start: Cinput = PTI ⊕ SecretKey; 10 Consecutive Rounds; Return Coutput}

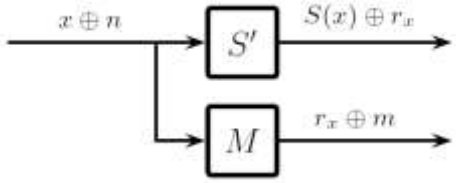
شکل (۲): دو پیاده‌سازی نقاب‌گذاری‌شده و نقاب‌گذاری‌نشده الگوریتم رمز پیشرفته استاندارد در حالی‌که پیاده‌سازی سمت چپ در برابر تحلیل مرتبه اول و پیاده‌سازی سمت راست در برابر تحلیل مرتبه دوم توان آسیب‌پذیر است.

در پیاده‌سازی ارائه‌شده در شکل (۲)، سمت چپ در بخش A آسیب‌پذیر در برابر تحلیل توان مرتبه اول است جایی‌که کلید رمز با داده ورودی رمز جمع می‌شود در حالی‌که پیاده‌سازی سمت راست در بخش های B و C در برابر تحلیل مرتبه دوم توان آسیب‌پذیر است جایی‌که داده ورودی ابتدا با نقاب تصادفی m جمع شده و سپس با کلید رمز جمع می‌شود.

نوع دیگری از این نوع نقاب‌گذاری موسوم به نقاب‌گذاری مجزا[2] پیشنهادشده که ظاهراً کارآیی بهتری از حیث مقاومت در برابر تحلیل توان در مقایسه با نقاب‌گذاری مرتبه اول دارد [۱۱]. این روش از دو جدول برای نقاب‌گذاری داده‌ها استفاده می‌کند که یکی همان جدول جانشینی بایت‌ها و دیگری جدولی موسوم به جدول نقاب است. برای فراهم آوردن امنیت بیشتر می‌توان داده‌های هر دو جدول را با مقدار تصادفی r جمع کرد. شکل (۳) نشان‌دهنده این نوع نقاب‌گذاری است. چنانچه در [۱۱] نشان داده شده، این روش مستقل از تعداد جداول نقاب، در برابر حتی حملات مرتبه اول تفاضلی توان استاندارد نیز آسیب‌پذیر است و از این رو روش مطمئنی برای محافظت از الگوریتم رمز در برابر تحلیل توان نیست. روابط (۶-۷) این نوع نقاب‌گذاری را نشان می‌دهد جایی‌که S' جدول SBox نقاب‌گذاری‌شده و M جدول نقاب‌ها را نشان می‌دهد.

$$S'(x \oplus n) = S(x) \oplus r_x \quad (۶)$$

$$M(x \oplus n) = r_x \oplus m \quad (۷)$$



شکل (۳): شمای روش نقاب‌گذاری مجزا که در آن از دو جدول جداگانه برای نقاب‌گذاری داده‌های جدول جانشینی بایت‌ها استفاده می‌شود.

۴- آزمون آماری T

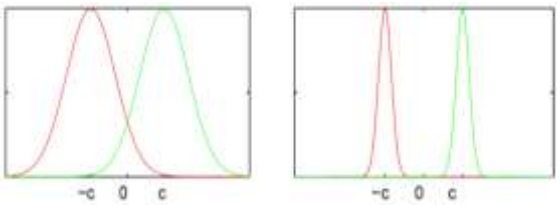
مساله ارزیابی میزان مقاومت پیاده‌سازی الگوریتم‌های رمزنگاری در برابر حملات کانال جانبی و به‌خصوص تحلیل‌های توان و الکترومغناطیس از جمله مسایل باز است که هنوز پاسخ کاملاً روشنی به آن داده نشده است. در میان روش‌های پیشنهادی برای ارزیابی میزان نشت اطلاعات از تحلیل‌های توان و الکترومغناطیس، آزمون آماری T بیش از بقیه مورد توجه قرار گرفته است. این آزمون، یک رابطه متقابل را بین کلید رمز و نمونه‌های به‌دست‌آمده از مشاهدات توان پیاده‌سازی واقعی الگوریتم را برقرار می‌سازد. برای انجام آزمون T، نمونه‌های توان بر مبنای یک تابع انتخاب و مقدار یک بیت در یک ثبات یا مقدار میانی تقسیم‌بندی می‌شوند. سپس نمونه‌های توان بر مبنای مقدار آن بیت خاص به دو دسته تقسیم می‌شوند. سپس با استفاده از تحلیل آماری بررسی می‌کنیم که آیا تفاوتی بین مقادیر میانگین دو دسته وجود دارد یا خیر. شکل (۴) به‌شکل تقریباً واضحی این آزمون و نتیجه آن را تشریح می‌کند جایی‌که دو توزیع نرمال با میانگین یکسان و واریانس‌های متفاوت نشان داده شده‌اند. واریانس یک توزیع یک چهارم واریانس توزیع دیگر است. بدیهی است توزیعی که واریانس بزرگتر دارد میزان هم-

1- Joint Statistics
2- Split Masking

پوشانی بیشتر و نشت اطلاعات کمتری در مقایسه با توزیع دیگر دارد زیرا جدا کردن '0' و '1' ها از یکدیگر به‌مراتب مشکل‌تر از توزیع دیگر است.

آزمون T به‌صورت رابطه (۲) تعریف می‌شود جایی‌که $M_{0,Kh}$ و $M_{1,Kh}$ به‌ترتیب تعداد مشاهدات در حد فاصل (بخش) های '0' و'1' و $\sigma^2_{0,Kh}(t)$ و $\sigma^2_{1,Kh}(t)$ واریانس‌های دو توزیع را متناظراً نشان می‌دهد.

$$T_{K_h}(t) = \frac{\Delta_{K_h}(t)}{\sqrt{\frac{\sigma^2_{0,Kh}(t)}{M_{0,Kh}}+\frac{\sigma^2_{1,Kh}(t)}{M_{1,Kh}}}} = \frac{\mu_{1K_h}(t)-\mu_{0K_h}(t)}{\sqrt{\frac{\sigma^2_{0,Kh}(t)}{M_{0,Kh}}+\frac{\sigma^2_{1,Kh}(t)}{M_{1,Kh}}}} \quad (۲)$$



شکل (۴): دو توزیع نرمال با میانگین یکسان و واریانس‌های متفاوت.

۵- روش نقاب‌گذاری پیشنهادی

یک روش موثرتر و کارآمدتر برای مقابله با تحلیل توان و غلبه بر نقطه ضعف امنیتی روش نقاب‌گذاری متعارف مرتبه اول و نیز روش نقاب‌گذاری مجزا استفاده از روابط (۱۱-۸) به‌جای استفاده از روابط (۷-۶) یا روابط (۵-۴) است جایی‌که داده‌های تبدیل جانشینی بایت‌ها به‌طور مستقیم از جدول نقاب خارج نمی‌شوند و تفکیک داده‌های نقاب‌گذاری‌شده از داده‌های نقاب‌گذاری‌نشده به‌مراتب مشکل از روش‌های متداول موجود است.

$$S^*(p \oplus k \oplus n) = r(p \oplus k) \oplus S(p \oplus k \oplus n) + m \quad (۸)$$

$$m(p \oplus k \oplus n) = S(p \oplus k \oplus n) \oplus S(p \oplus k) \quad (۹)$$

$$M(p \oplus k \oplus n) = r(p \oplus k) \oplus m(p \oplus k \oplus n) \quad (۱۰)$$

$$S(p,k) \oplus m = S^*(p \oplus k \oplus n) \oplus M(p \oplus k \oplus n) \quad (۱۱)$$

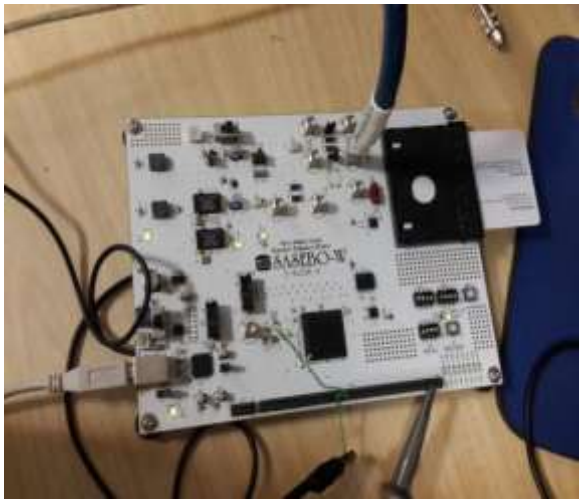
در روابط فوق، M جدول نقاب‌ها است که از پیش محاسبه و ذخیره می‌شود. m و n نیز به‌ترتیب نقاب ورودی و خروجی هستند. S^* نیز جدولی است که مقادیر تبدیل جانشینی بایت‌ها را به‌صورت نقاب‌گذاری‌شده در خود ذخیره می‌کند. مهم‌ترین تفاوت این روش با روش متداول نقاب‌گذاری مرتبه اول (که در عمل یک شیفت ساده و جمع با نقاب خروجی است) آن ست که از جدول جانشینی بایت‌ها مقدار واقعی آن خارج نمی‌شود و مقدار دیگری متناسب با مقدار ماسک از آن خارج می‌شود. r نیز تابع تولیدکننده اعداد تصادفی است که از یک شیفت رجیستر با بازخورد غیرخطی برای تولید اعداد تصادفی استفاده می‌کند. نکته مهم و اصلی در این روش آن ست که در اینجا نیاز به محاسبه جدول نقاب در هر بار عملیات رمز نیست بلکه جدول نقاب به‌ازای یک نقاب ورودی و خروجی مشخص یک بار محاسبه شده و در ابزار رمز ذخیره می‌شود. البته بعد از هر بار عملیات رمز برای به‌هنگام‌سازی جداول مربوطه، تابع r نیز به‌هنگام شده و اعداد تولیدشده توسط آن با تمام عناصر جدول نظیر به نظیر جمع می‌شوند ولی نیاز به به‌هنگام‌سازی جدول نقاب نیست. علاوه بر آن، از جدول نقاب علاوه بر مقدار SBox متناسب با داده ورودی، به‌طور همزمان مقدار دیگری متناسب با ماسک و داده ورودی خارج می‌شودکه عملاً تفکیک کردن این دو از یکدیگر بسیار مشکل‌تر از روش‌های قبلی است که این امر برتری این روش در مقایسه با روش نقاب‌گذاری متعارف و نیز روش نقاب‌گذاری مجزاست. نتایج آزمایشات و نیز نتایج آزمون آماری T که در بخش بعد ارائه خواهد شد درستی این مطلب را نشان می‌دهند. در صورت در اختیار داشتن زمان، می‌توان جدول نقاب را نیز بعد از هرچند بار اجرا به‌هنگام کرد.

۶- نتایج پیاده‌سازی

با توجه به تنوع بسترها و مشکل بودن مقایسه نتایج انجام حملات کانال جانبی بر روی بسترهای مختلف، شرکت ژاپنی موریتا[1] یک بورد آزمایشگاهی موسوم به بورد استاندارد ارزیابی حملات کانال جانبی را طراحی و تولید نموده که می‌توان از آن به عنوان یک بستر استاندارد برای انجام حملات کانال جانبی و ارزیابی نتایج حمله استفاده نمود [۸]. این بورد در چند نسخه مختلف موسوم به بوردهای ساسبو و ساکورا تهیه شده و پایه‌های لازم برای اندازه‌گیری سیگنال توان تراشه‌ها بر روی آن تعبیه شده است. یک نوع کاملا مفید و متداول این بوردها موسوم به ساسبو- دبلیو مجهز به یک کارت‌خوان و یک کارت هوشمند مبتنی بر استاندارد ISO/IEC 7816-3 و میکروکنترولر هشت بیتی ATmega163 AVR است. همچنین این بورد مجهز به واسط سریال و نیز درگاه USB برای برقراری ارتباط با یک کامپیوتر میزبان است. این بورد همچنین حاوی یک تراشه برنامه‌پذیر FPGA از سری Spartan-6 LX150 است که نه تنها عملکرد بورد را کنترل می‌کند بلکه برای آزمایش حملات کانال جانبی بر روی FPGA نیز به‌کار می‌رود. این بورد همچنین دارای سوراخ‌هایی در پشت کارت هوشمند است که اندازه‌گیری و انجام

1- Morita Tech. Co.

حملات الکترومغناطیس را تسهیل می‌کند. کارت هوشمند قرار-گرفته بر روی بورد مبتنی بر یک میکروکنترولر ATMega 163 AVR است که الگوریتم رمز پیشرفته استاندارد ۱۲۸ بیتی[1] را پشتیبانی می‌کند. میکروکنترولر مزبور ساخت شرکت Atmel و دارای معماری ریسک هاروارد[2] است بدین مفهوم که حافظه برنامه و حافظه داده کاملا از یکدیگر مجزا هستند. این پردازنده همچنین دارای ۱۶ کیلو بایت حافظه از نوع فلش ROM، ۵۱۲ بایت حافظه EEPROM به عنوان حافظه غیرفرار داده درونی و یک کیلو بایت حافظه SRAM به عنوان حافظه فرار درونی است. کارت هوشمند همچنین دارای یک حافظه ۲۵۶ کیلو بایت از نوع EEPROM است که به میکروکنترولر متصل شده است. فرکانس پالس ساعت کارت هوشمند ۳/۵۷ مگاهرتز است که بصورت بیرونی و از طریق کارت‌خوان تامین می‌شود. شکل (۵) شمایی از بورد مورد آزمایش در این تحقیق را نشان می‌دهد.



شکل (۵): نمای بورد استاندارد ارزیابی حملات کانال جانبی که در این تحقیق همراه با کارت هوشمند آن مورد استفاده قرار گرفت.

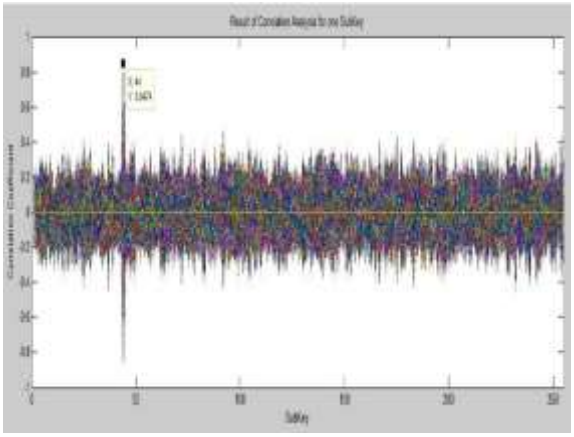
مجموعه آزمایشگاهی برای انجام آزمایشات مورد نظر در این تحقیق شامل یک بورد استاندارد حملات کانال جانبی، یک رایانه قابل حمل شخصی، یک اسیلوسکوپ دیجیتال Infiniium Keysight DSO90604A با نرخ نمونه برداری حداکثر 20 GS/sec است که دو پروب به بورد متصل شده و توان (جریان) مصرفی بورد را اندازه‌گیری می‌کنند. در نهایت هم یک نرم‌افزار برای کنترل فرآیند، همزمان‌سازی بورد و اسیلوسکوپ، ارسال سیگنال چکانه به اسیلوسکوپ و نیز ارتباط بورد و رایانه نوشته شد که انجام عمل نمونه‌گیری به‌صورت خودکار به‌انجام برسد. متون آشکار ورودی از یک شیفت رجیستر با فیدبک خطی به‌طول ۱۶ بیت که در برنامه نرم‌افزار میکروکنترولر نوشته شده بود تولید شدند.

۷- نتایج آزمایشگاهی

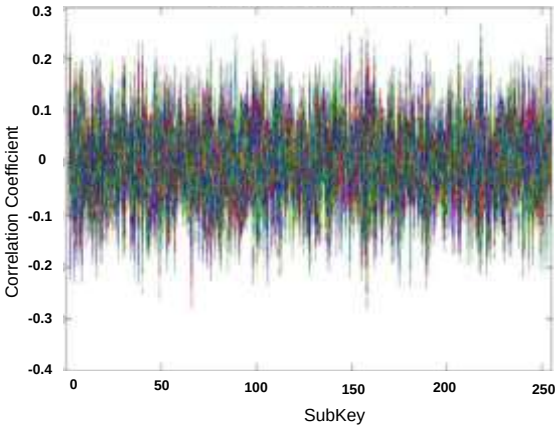
۷-۱- نتایج تحلیل مرتبه اول

برای انجام تحلیل‌های توان و پیدا کردن همبستگی بین داده‌های واقعی و حدس‌های کلید از تابع شناخته‌شده و قدرتمند پیرسون استفاده کردیم. برای کاهش اثر نویز، تمام اندازه‌گیری‌های انجام‌شده ده بار متوسط‌گیری شدند. شکل (۶) نتیجه تحلیل همبستگی توان در پیاده‌سازی محافظت‌نشده را نشان می‌دهد جایی‌که وجود یک پیک واضح نشان‌دهنده کشف کلید صحیح (0x2B) است. شکل (۷) همین آزمایش را در پیاده‌سازی محافظت‌شده یا نقاب‌گذاری‌شده نشان می‌دهد جایی‌که زیرکلید صحیح از سایر زیرکلیدها قابل تشخیص نیست. شکل (۸) منحنی تغییر ضریب همبستگی به‌ازای ۲۰۰ متن آشکار ورودی را نشان می‌دهد. شکل همان‌طور که ملاحظه می‌شود زیرکلید صحیح به‌راحتی از کلیدهای غیرصحیح قابل تشخیص است. شکل (۹) منحنی تغییر ضریب همبستگی به‌ازای ۲۰۰ متن آشکار ورودی را در پیاده‌سازی نقاب‌گذاری‌شده نشان می‌دهد. همان‌طور که از شکل پیداست زیرکلید صحیح از سایر زیرکلیدها قابل تشخیص نیست. مطابق با آنچه در این شکل دیده می‌شود زیرکلید صحیح قابل تمیز دادن از زیرکلیدهای غلط نیست که این امر نشان‌دهنده عملکرد مناسب نقاب در جلوگیری از تحلیل مرتبه اول توان است. شکل (۱۰) نشان‌دهنده تحلیل تفاضلی فرکانس یا همبستگی طیف توان سیگنال توان و پیش‌بینی‌های کلید در پیاده‌سازی نقاب‌گذاری‌نشده است. همان‌طور که در شکل مشخص است وجود یک پیک واضح نشان‌دهنده همبستگی بین کلید صحیح و نمونه های طیف توان مصرفی ابزار است و از این رو این حمله نیز به‌طور موفقیت‌آمیز قادر به کشف کلید در پیاده‌سازی نقاب‌گذاری‌نشده است. مطابق با آنچه در منابع مربوطه گزارش شده تحلیل همبستگی فرکانس در پاره‌ای موارد بهتر از تحلیل توان در حوزه زمان عمل می‌کند زیرا طیف فرکانس نسبت به شیفت زمانی بدون تغییر است و لذا شیفت‌ها و تاخیرهای تصادفی به‌منظور بر هم زدن توان مصرفی در حوزه زمان، تاثیری بر روی طیف توان ندارد [۶]. شکل (۱۱) نتیجه همین حمله بر روی پیاده‌سازی نقاب‌گذاری‌شده را نشان می‌دهد که همان‌طور که از شکل پیداست کلید صحیح قابل تشخیص از زیرکلیدهای اشتباه نیست که این امر به‌معنی موفق بودن نقاب‌گذاری پیشنهادی در برابر حملات مرتبه اول در هر دو حوزه زمان و فرکانس است. آزمایشات مزبور به‌ازای ۱۰۰۰ نمونه ورودی نیز تکرار شده و نتایج مشابهی به‌دست آمد.

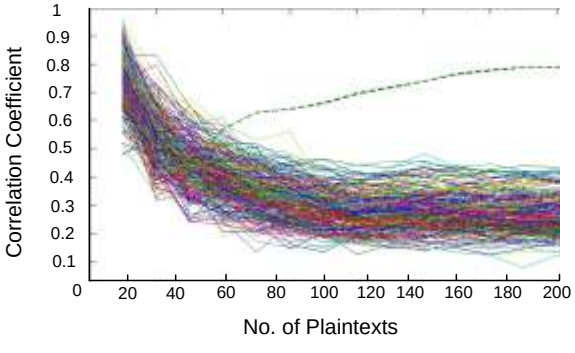
1- AES-128
2- RISC Harvard Architecture



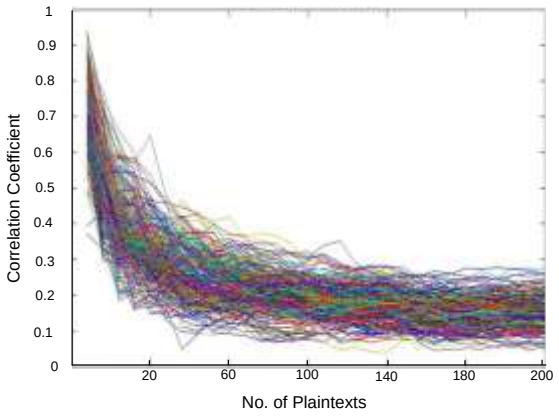
شکل (۶): نتیجه تحلیل همبستگی توان به پیاده‌سازی نقاب‌گذاری‌نشده الگوریتم استاندارد پیشرفته. همان‌طور که از شکل پیداست وجود قله بارز نشان‌دهنده کشف زیرکلید صحیح از زیرکلیدهای اشتباه است.



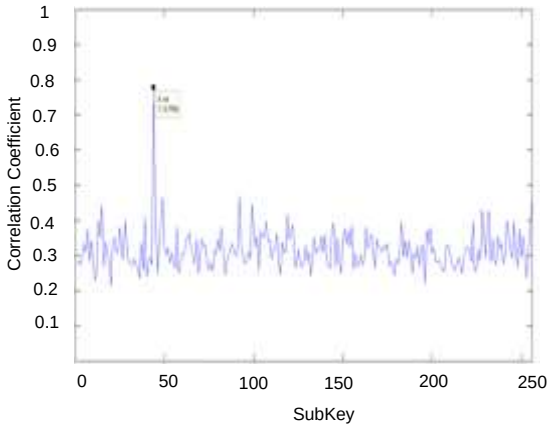
شکل (۷): نتیجه تحلیل همبستگی توان به پیاده‌سازی نقاب‌گذاری‌شده الگوریتم استاندارد پیشرفته. همان‌طور که از شکل پیداست عدم وجود قله بارز نشان‌دهنده غیرقابل تشخیص بودن زیرکلید صحیح از سایر زیرکلیدها است.



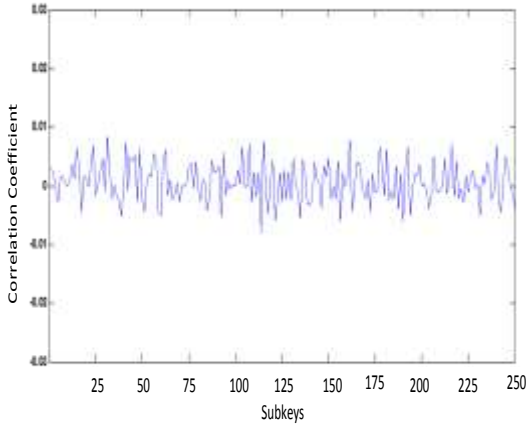
شکل (۸): نتیجه تحلیل همبستگی توان به پیاده‌سازی نقاب‌گذاری‌نشده الگوریتم استاندارد پیشرفته به‌ازای ۲۰۰ متن آشکار ورودی. همان‌طور که از شکل پیداست زیرکلید صحیح به‌راحتی قابل تشخیص از سایر زیرکلیدها است.



شکل (۹). نتیجه تحلیل همبستگی توان به پیاده‌سازی نقاب‌گذاری‌شده الگوریتم استاندارد پیشرفته به‌ازای ۲۰۰ متن آشکار ورودی. همان‌طور که از شکل پیداست زیرکلید صحیح قابل تشخیص از سایر زیرکلیدها نیست.



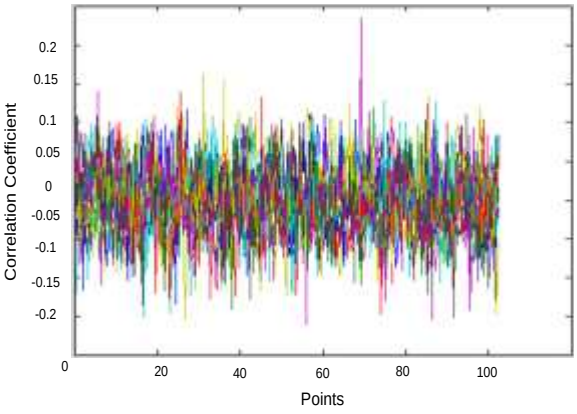
شکل (۱۰): نتیجه تحلیل همبستگی توان در حوزه فرکانس به پیاده‌سازی نقاب‌گذاری‌نشده الگوریتم استاندارد پیشرفته. همان‌طور که از شکل پیداست وجود قله بارز نشان‌دهنده کشف زیرکلید صحیح و همبستگی بین طیف توان نمونه‌های توان و وزن همینگ داده‌های پردازش شده است.



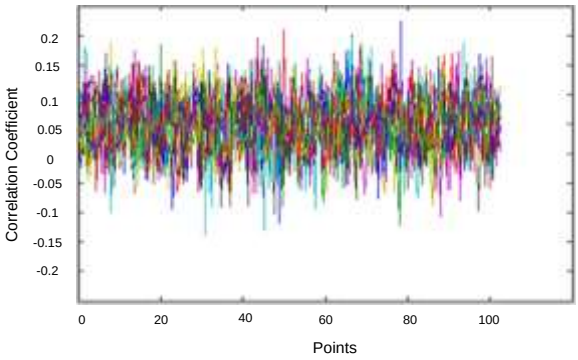
شکل (۱۱): نتیجه تحلیل همبستگی توان در حوزه فرکانس به پیاده‌سازی نقاب‌گذاری‌شده الگوریتم استاندارد پیشرفته. همان‌طور که از شکل پیداست عدم وجود قله بارز نشان‌دهنده عدم کشف زیرکلید صحیح و از بین رفتن همبستگی بین طیف توان نمونه‌های توان و وزن همینگ داده‌های پردازش شده است.

۷-۲- نتایج تحلیل مرتبه دوم

برای پیاده‌سازی حمله مرتبه دوم ما از روش پیشنهادی در [۱۲] استفاده کردیم که در آن فرض بر آن گذاشته شده است که توان لحظه‌ای مصرفی ابزار رمز به‌صورت خطی با وزن همینگ داده‌های پردازش‌شده رابطه خطی دارد. به بیان دیگر چنانچه C توان مصرفی ابزار رمز هنگام پردازش مقدار a باشد آنگاه $C(a) \approx HW(a)$. همچنین فرض بر آن است که با استفاده از $|C(a) - C(b)|$ بتوان $HW(a \oplus a)$ را تخمین زد جایی‌که a و b داده‌های باینری هستند. از این‌رو به‌منظور انجام تحلیل مرتبه دوم توان، یک نقطه از سیگنال توان در نظر گرفته و انتخاب شده و از بقیه سیگنال توان کم شده و قدر مطلق آن محاسبه می‌شود. سپس در مرحله بعد حمله تحلیل توان استاندارد پیاده‌سازی می‌شود به این مفهوم که ضریب همبستگی بین داده‌های توان پیش پردازش‌شده و وزن همینگ جمع انحصاری دو متغیر تحت حمله محاسبه می‌شود. اگر پیک واضحی وجود نداشته باشد آنگاه نقطه دیگری انتخاب می‌شود. برای حمله به نقاب مرتبه اول، نقاط ابتدا و انتهای دور اول هدف قرار گرفتند جایی‌که $p \oplus k \oplus m$ و $S(p \oplus k) \oplus m$ محاسبه می‌شوند. در مرحله بعد همبستگی میان $|C(S(p \oplus k) \oplus m) - C(p \oplus k \oplus m)|$ و $HW(S(P \oplus K) \oplus (P \oplus K))$ محاسبه شده و ترسیم می‌شود. لازم بهذکر است بعد از حمله گزارش‌شده در [۱۲]، این حمله بهبود و ارتقا یافته است [۱۳] و آنچه در این مقاله آمده حمله بهینه نیست و تنها به‌منظور نشان دادن مفهوم اساسی و کارکرد روش پیشنهادی است. شکل (۱۲) نشان‌دهنده شکسته شدن نقاب متعارف در اثر حمله مرتبه دوم و شکل (۱۳) نشان‌دهنده مقاوم بودن نقاب‌گذاری پیشنهادی در برابر حمله مزبور است.



شکل (۱۲): شکسته شدن نقاب مرتبه اول در برابر حمله مرتبه دوم توان. وجود یک قله (پیک) بارز در شکل موید کشف زیرکلید صحیح است.

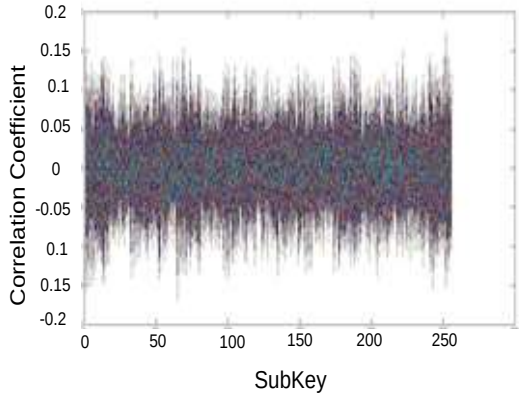


شکل (۱۳): نتیجه پیاده‌سازی حمله مرتبه دوم توان علیه نقاب‌گذاری پیشنهادی. عدم وجود قله (پیک) بارز در شکل موید مقاوم بودن نقاب‌گذاری در برابر این حمله است.

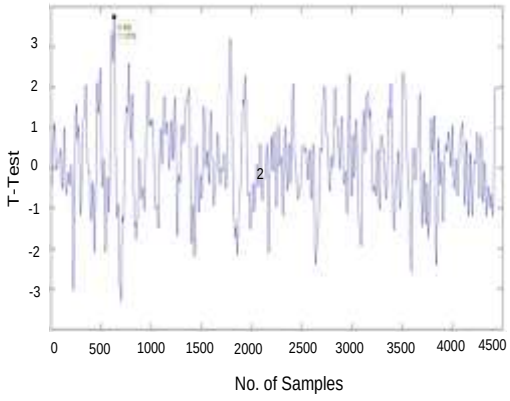
۷-۳- نتایج آزمون T

شکل (۱۴) نتیجه آزمون تحلیل همبستگی را در پیاده‌سازی الگوریتم نقاب‌گذاری‌شده با روش متعارف نقاب‌گذاری جمعی مرتبه اول به‌ازای ۲۰۰۰ متن آشکار ورودی و شکل (۱۵) نتیجه آزمون T در همان پیاده‌سازی به‌ازای همان تعداد متن آشکار ورودی نشان می‌دهد. آنچه از این دو شکل مشخص است آن است که تحلیل همبستگی مرتبه اول قادر به کشف زیرکلید صحیح نیست و مقدار آزمون T برابر با ۳/۷ است که زیر مقدار آستانه $\pm$۴/۵ و قابل قبول است اما چنانچه در شکل (۱۶) نشان داده شده است با فزایش تعداد متون آشکار ورودی به ۳۰۰۰ مقدار این آزمون به ۴/۴۷ افزایش پیدا می‌کند که این به مفهوم نشت اطلاعات از پیاده‌سازی نقاب‌گذاری‌شده است. با افزایش تعداد متون آشکار به ۴۰۰۰ هزار، چنانچه در شکل (۱۷) نشان داده شده است، مقدار آزمون T از مقدار آستانه تجاوز کرده و به ۵/۷۳ می‌رسد که این امر به مفهوم ناامن بودن روش نقاب-گذاری مرتبه اول در برابر حملات از مراتب بالاتر است. مقدار آزمون T با افزایش تعداد متون آشکار به ۵۰۰۰ مقدار آزمون T بازهم افزایش پیدا کرده و به ۵/۷۸- می‌رسد که این مساله در شکل (۱۸) نشان داده شده است. افزایش مقدار آزمون T همراه با افزایش نمونه‌ها نشان‌دهنده این حقیقت است که روش‌هایی که در شکل ظاهری در برابر تحلیل توان مقاوم هستند با افزایش تعداد نمونه‌ها نشتی اطلاعات قابل ردیابی دارند. شکل (۱۹) تحلیل همبستگی توان و شکل (۲۰) نتیجه آزمون T بر روی پیاده‌سازی الگوریتم با روش نقاب‌گذاری پیشنهادی به‌ازای ۵۰۰۰ متن آشکار ورودی را نشان می‌دهد. چنانچه از شکل مشخص است مقدار آزمون T برابر ۴/۰۴ است که به خوبی زیر مقدار آستانه قرار گیرد و نشان‌دهنده آن است که نقاب‌گذاری پیشنهادی به مراتب مقاوم‌تر از نقاب‌گذاری مرتبه اول متداول است. ما همین آزمون را برای نقاب‌گذاری مجزا انجام دادیم که مقدار آزمون T برای آن ۷/۰۲ به‌دست آمد که نشان‌دهنده نشت

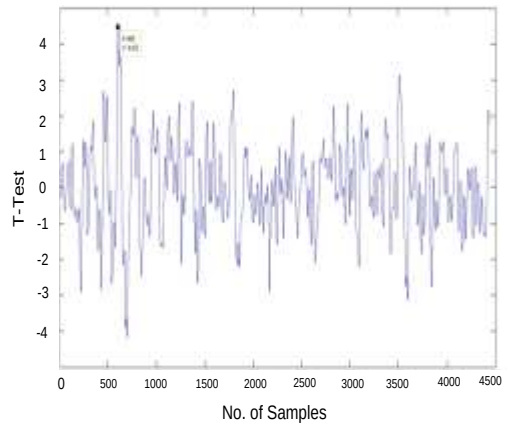
اطلاعات از آن و آسیب‌پذیری آن در برابر تحلیل‌های مرتبه بالاتر است. چنانچه نشان خواهیم داد این نوع نقاب‌گذاری در برابر حمله مرتبه دوم تاب نیاورده و در برابر آن مغلوب می‌شود.



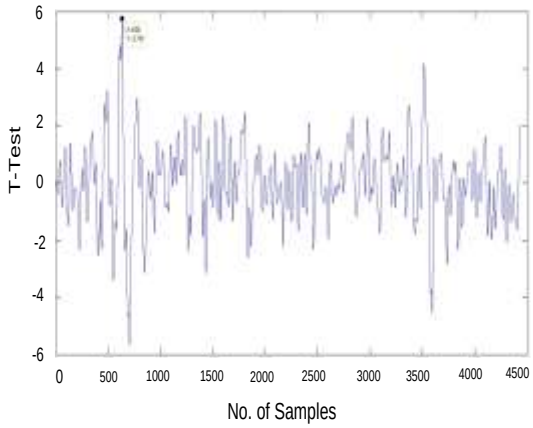
شکل (۱۴): نتیجه تحلیل همبستگی در پیاده‌سازی شده با روش نقاب‌گذاری متعارف مرتبه اول. همان‌طور که از شکل پیداست زیرکلید صحیح قابل تشخیص از سایر زیرکلیدها نیست.



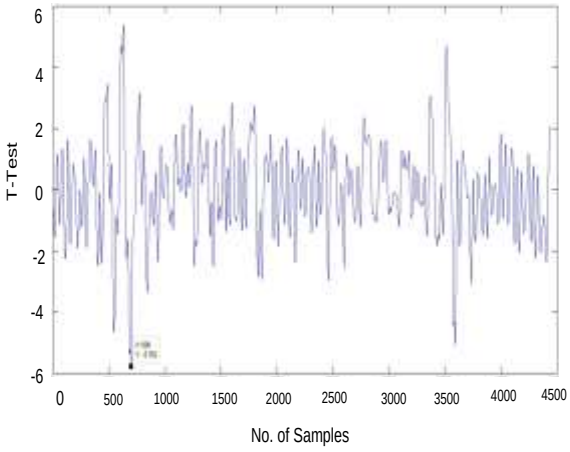
شکل (۱۵): نتیجه آزمون آماری T برای پیاده‌سازی نقاب‌گذاری‌شده بروش متعارف جدول جانشینی بایت‌های الگوریتم پیشرفته رمز استاندارد به‌ازای ۲۰۰۰ متن آشکار ورودی. همان‌طور که از شکل مشخص است حداکثر مقدار این آزمون ۳/۷۲ به‌دست می‌آید.



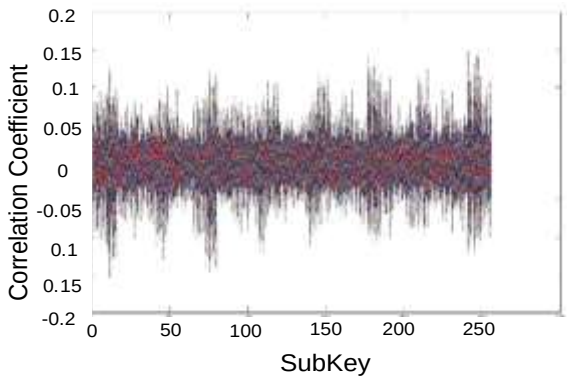
شکل (۱۶): نتیجه آزمون آماری T برای پیاده‌سازی نقاب‌گذاری‌شده به‌روش متعارف جدول جانشینی بایت‌های الگوریتم پیشرفته رمز استاندارد به‌ازای ۳۰۰۰ متن آشکار ورودی. همان‌طور که از شکل مشخص است حداکثر مقدار این آزمون ۴/۴۷ به‌دست می‌آید.



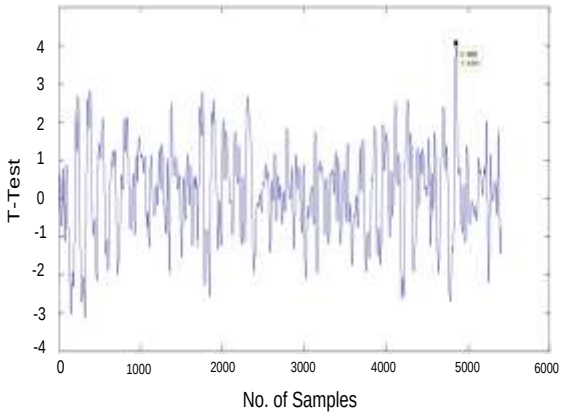
شکل (۱۷): نتیجه آزمون آماری T برای پیاده‌سازی نقاب‌گذاری‌شده به‌روش متعارف جدول جانشینی بایت‌های الگوریتم پیشرفته رمز استاندارد به‌ازای ۴۰۰۰ متن آشکار ورودی. همان‌طور که از شکل مشخص است حداکثر مقدار این آزمون ۵/۷۳ به‌دست می‌آید که از مقدار آستانه تجاوز می‌کند.



شکل (۱۸): نتیجه آزمون آماری T برای پیاده‌سازی نقاب‌گذاری‌شده به‌روش متعارف جدول جانشینی بایت‌های الگوریتم پیشرفته رمز استاندارد به‌ازای ۵۰۰۰ متن آشکار ورودی. همان‌طور که از شکل مشخص است حداکثر مقدار این آزمون ۵/۷۸- به‌دست می‌آید که از مقدار آستانه تجاوز می‌کند.



شکل (۱۹): نتیجه تحلیل همبستگی در پیاده‌سازی‌شده با روش نقاب‌گذاری پیشنهادی. همان‌طور که از شکل پیداست زیرکلید صحیح قابل تشخیص از سایر زیرکلیدها نیست.



شکل (۲۰): نتیجه آزمون آماری T برای پیاده‌سازی نقاب‌گذاری‌شده به‌روش پیشنهادی جدول جانشینی بایت‌های الگوریتم پیشرفته رمز استاندارد به‌ازای ۵۰۰۰ متن آشکار ورودی. همان‌طور که از شکل مشخص است حداکثر مقدار این آزمون ۴/۰۴ به‌دست می‌آید که به‌نحو قابل جمعی، زیر مقدار آستانه است.

۷-۴- نتایج پیاده‌سازی عملی و مقایسه با سایر کارها

همان‌گونه که در مقاله ذکر شد، دو نسخه نقاب‌گذاری‌شده و بدون نقاب الگوریتم استاندارد پیشرفته رمزنگاری بر روی بورد ساسبو به‌صورت نرم‌افزاری پیاده‌سازی شد و نتایج مورد بررسی و آزمایش عملی قرار گرفت. نتایج پیاده‌سازی و مقایسه با سایر کارهای گزارش‌شده در جدول (۱) آمده است.

جدول (۱): مقایسه نتیجه پیاده‌سازی نرم‌افزاری روش پیشنهادی با سایر کارهای گزارش‌شده

مرجع	Platform	ROM / RAM	Cycles (Unprotected)	Cycles (Protected)
[۱۴]	AVR	-	۴۴۲۷	۸۴۲۰
[۱۵]	AVR	-	۱۱۹۰	۴۲۱۲
[۱۶]	AVR	۱۵۳۶	۴۶۲۶	۱۳۶۰۰
[۱۷] مقاوم در برابر تحلیل مرتبه اول	AVR	۲۶۴	۴۶۲۵	۸۷۰۱
[۱۷] مقاوم در برابر تحلیل مرتبه دوم	AVR	۵۹۲	۴۶۲۵	۱۹۳۱۹۹
[۱۸] مقاوم در برابر تحلیل مرتبه اول	32-bit ARM	۲۳۹۳	۷۰۸۶	۱۳۸۷۶
این کار	AVR	۳۸۶	۷۱۴۴	۸۸۴۸

۸- نتیجه‌گیری

سامانه‌های تعبیه‌شده هر روز با خطرات و حملات جدیدی مواجه می‌شوند زیرا اطلاعات خصوصی ذخیره‌شده در آن‌ها روزبه‌روز بزرگتر و مهم‌تر می‌شود. حفظ امنیت این سامانه‌ها موضوعی جدی و پیچیده است. راه حل‌های جدید در تمام مراحل لازم هستند تا از سامانه‌های های موجود و چالش‌های پیش‌روی آن‌ها دفاع و محافظت کنند. حملات تحلیل توان از جمله حملات موثر و قدرتمندی هستند که امنیت سامانه‌های رمزنگاری سخت‌افزاری را تهدید می‌کنند. در سال‌های اخیر تحقیقات زیادی در مورد جلوگیری از حمله تحلیل توان انجام شده است. برخی از روش‌ها که به‌طور حسی و شهودی روش‌های موثری هستند مانند تصادفی کردن اجرای کدها یا افزودن واحدهای مصرف‌کننده توان به‌طور تصادفی مانند تاخیردهنده‌ها یا شیفت‌دهنده‌های تصادفی و یا فروبرنده‌های جریان به‌سختی می‌توانند در مقابل این حمله مقاومت کنند و فقط کار مهاجم را قدری سخت‌تر می‌کنند. دراین مقاله روش کم‌هزینه و موثری برای محافظت از پیاده‌سازی الگوریتم پیشرفته استاندارد ارائه و کارآیی آن بر روی بستر استاندارد ارزیابی حملات کانال جانبی آزمایش شد. نتایج پیاده‌سازی عملی و نیز آزمون آماری T نشان داد که روش پیشهادی نشت اطلاعات کمتری در مقایسه با روش نقاب‌گذاری متعارف و نیز روش نقاب‌گذاری مجزا دارد. باید توجه داشت که باید در ارائه روش مقابله و ادعا در مورد کارایی آن کاملا محتاط بود زیرا بسیاری از روش‌ها که به‌لحاظ ظاهری یا حتی تئوری در مقابل حملات کانال جانبی مقاوم هستند در عمل در مقابل روش‌های پیچیده حمله چندان تاب نمی‌آورند و مغلوب می‌شوند. سوال اساسی اینجاست که آیا می‌توان این تکنیک‌ها را بیشتر بهینه‌سازی کرد و اینکه آیا می‌توان تکنولوژی جدیدی برای مقابله با این حملات ابداع نمود؟ سوال مهم دیگر آن است که آیا می‌توان راه دیگری برای سنجش میزان مقاومت در مقابل حمله بدون پیاده‌سازی حمله بر مبنای ابزارهای آماری یا هر ابزار دیگر برای ارزیابی پیاده سازی پیدا کرد؟ آیا می‌توان معیار دیگری برای اندازه‌گیری میزان مقاومت بر مبنای پارامترهای طراحی مانند فاکتور فعالیت یا پروفایل مصرف توان پیدا کرد؟ با چه معیار یا معیارهایی می‌توان میزان مقاومت دو پیاده سازی مختلف را با یکدیگر مقایسه نمود؟ این سوالات نمونه‌هایی از سوالات مهم و زمینه‌های تحقیقاتی باز در مورد مقابله با تحلیل توان است که پاسخ چندان روشنی به آن‌ها داده نشده است.

۹- مراجع

[1] J. Daemen and V. Rijmen, "AES Proposal Rijndael," National Institute of Standards and Technology, July 2001.

[2] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks (Revealing the Secrets of Smart Cards)," Springer, 2007.

[3] R. Lumbiarres-López, M. López-García, and E. Cantó-Navarro, "Hardware Architecture Implemented on FPGA for Protecting Cryptographic Keys against Side-Channel Attacks," IEEE Transactions on Dependable and Secure Computing, DOI 10.1109/TDSC.2016.2610966, 2016.

[4] M. Masoumi and S. S. Moghadam, "A Simulation-Based Correlation Power Analysis Attack to FPGA Implementation of KASUMI Block Cipher," Int. J. of Internet Technology and Secured Transactions, vol. 17, no. 2, pp. 175-191, 2017.

[5] M. H. Rezayati, A. Amin, M. Masoumi, and H. Momeni, "Successfully Attacking Hardware Implementation of the AES Algorithm using Differential Electromagnetic Analysis," ECDJ Journal, no. 2, pp. 63-70, Summer, 2015. (In Persian)

[6] J. S. Coron, "Higher Order Masking of Look-Up Tables," Eurocrypt 2014, LNCS 8441, pp. 441–458, Springer, 2014.

[7] M. M. Tunstall, C. Whitnall, and E. Oswald, "Masking tables - an Underestimated Security Risk," in FSE 2013, pp. 425–444, 2013.

[8] T. Katashita, Y. Hori, H. Sakane, and A. Satoh, "Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing," Non-Invasive Attack TestingWorkshop(NIAT), 2011. http://csrc.nist.gov/news_events/non-invasive-attack-testingworkshop/ papers/10_Katashita.pdf.

[9] O. Schimmel, P. Duplys, E. Bohl, J. Hayek, and W. Rosenstiel, "Correlation Power Analysis in Frequency Domain", COSADE 2010. cosade.cased.de/files/proceedings/cosade2010_paper_1.pdf

[10] G. Goodwill, B. Jun, J. Jafe, and P. Rohatgi, "A Testing Methodology for Side Channel Resistance Validation", NIST Noninvasive Attack Testing Workshop 2011, http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf.

[11] J. Coron and L. Kizhvatov, "Analysis of the Split Mask Countermeasure for Embedded Systems," https://orbilu.uni.lu/bitstream/10993/10582/1/splimaskanalysis.pdf

[12] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, "Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers," CT-RSA 2006, LNCS 3860, pp. 192–207, Springer, 2006.

[13] E. Prouff, M. Rivain, and R. Bevan, "Statistical Analysis of Second Order Differential Power Analysis," IEEE Transactions on Computers, vol. 58, no. 6, pp. 799–811, 2009.

[14] A. G. Bayrak1, F. Regazzoni, P. Brisk, F. X. Standaert, and P. Ienne, "A First Step Towards Automatic Application of Power Analysis Countermeasures," DAC 2011, pp. 230-235, 2011.

[15] C. Herbst, E. Oswald, and S. Mangard, "An AES Smart Card Implementation Resistant to Power Analysis Attacks," in Applied Cryptography and Network Security, LNCS 3989, Springer-Verlag, pp. 239–252, 2006.

[16] E. Oswald and K. Schramm, "An Efficient Masking Scheme for AES Software Implementations," In WISA 2005, LNCS 3786, pp. 292–305, Springer, 2006.

[17] K. Schramm and C. Paar, "Higher-Order Masking of the AES," CT-RSA 2006, LNCS 3860, pp. 208-225, 2006.

[18] T. Messerges, "Securing the AES Finalists against Power Analysis Attacks," FSE 2000, LNCS 1978, pp. 150–164. Springer-Verlag, 2000.

A New And Efficient Method of Mass Masking and its Resistance Assessment to Power Analysis

M. Masoumi*, A. Dehghan Menshadi, E. Madadi, S. Saee Moghadam

*Islamic Azad University Islamshahr Branch

(Received: 06/10/2017, Accepted: 29/01/2018)

ABSTRACT

Differential Power Analysis (DPA) implies measuring the supply current of a cipher-circuit in an attempt to uncover part of a cipher key. Cryptographic security gets compromised if the current waveforms obtained correlate with those from a hypothetical power model of the circuit. In recent years, the security of the Advanced Encryption Standard (AES) against DPA, has received considerable attention. This paper presents a practical implementation of advanced encryption standard (AES-128) algorithm combined with a simple yet effective masking scheme to protect it against differential and correlation power analysis attacks. The proposed masking scheme has advantages of easy software implementation and lower memory requirement compared to conventional first-order masking technique. In addition, it is robust against both first and second-order differential power analysis. The experimental results and also the results of Welch's T-Test statistical analysis demonstrate that the proposed scheme has less information leakage than other existing conventional first-order masking schemes.

Keywords: Advanced Encryption Standard, Power Analysis Attacks, Masking, T-Test Analysis

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