هفتمین کنفرانس بین المللی انجمن رمز ایران
۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی
!
انجمن رمزایران
دانشگاه صنعتی خواجه نصیرالدین طوسی

پیاده‌سازی عملی تحلیل تفاضلی توان روی سیستم رمزنگاری AES!

مهدی معصومی[۱]، مسعود معصومی[۲]، محمود احمدیان[۳]

دانشگاه صنعتی خواجه نصیرالدین طوسی، دانشکده‌ی دانشکده‌ی مهندسی برق و کامپیوتر، آزمایشگاه شناسه و رمز[۱]
masoomi_ms@ee.kntu.ac.ir

تهران، دانشگاه صنعتی خواجه نصیرالدین طوسی [۲و۳]
m_masoumi@eetd.kntu.ac.ir, m_ahmadian@kntu.ac.ir

چکیده

با استفاده از تحلیل تفاضلی توان (DPA) می‌توان با اندازه‌گیری جریان تغذیه‌ی یک دستگاه رمزنگاری، بخشی از کلید رمز یا تمام آن را کشف کرد. اگر شکل موج حاصله از جریان با آنچه که از مدل فرضی مصرف توان یک مدار به دست می‌آید شباهت داشته باشد، امنیت سیستم رمزنگاری به خطر می‌افتد. در سال‌های اخیر، امنیت الگوریتم استاندارد رمزنگاری پیشرفته (AES) در مقابل DPA اهمیت قابل توجهی پیدا کرده است. با اینکه FPGAها به طور فزاینده‌ای در کاربردهای رمزنگاری رواج پیدا کرده‌اند پژوهش‌های محدودی یافت می‌شود که آسیب‌پذیری AES را در برابر چنین حملاتی ارزیابی می‌کند. هدف از این مقاله توصیف پیاده‌سازی عملی و موفقیت‌آمیز حمله و ارائه‌ی مستنداتی است که نشان می‌دهد DPA تهدیدی جدی برای سیستم رمزنگاری AES غیرامن پیاده‌سازی‌شده روی FPGAهای مبتنی بر SRAM است.

واژه‌های! کلیدی

حملات کانال جانبی، تحلیل تفاضلی توان (DPA)، الگوریتم استاندارد رمزنگاری پیشرفته (AES)، حمله‌ی هم‌بستگی.

۱- مقدمه !

مدل متداول سنتی ارزیابی سیستم‌های رمزنگاری، امنیت را از منظر توابع ریاضی به‌کار رفته در آن مورد ارزیابی قرار می‌دهد. این روش آثار فیزیکی جانبی استفاده از این توابع را در دنیای واقعی در نظر نمی‌گیرد. در اواسط دهه‌ی ۹۰ انواع جدیدی از حملات موسوم به حملات کانال جانبی[۱] معرفی شدند. این حملات از نشت اطلاعات همانند اطلاعات مصرف توان، تشعشات الکترومغناطیسی یا زمان محاسبات استفاده می‌کنند تا کلید مخفی را به دست آورند. حملات کانال جانبی به علت سادگی و مؤثر بودن اهمیت زیادی در رمزنگاری پیدا کرده‌اند و تحقیقات در مورد آنها در حال رشد است.

یک حمله‌ی تحلیل ساده‌ی توان (SPA) به این صورت توصیف می‌شود که در آن حمله‌کننده می‌تواند به طور مستقیم از مصرف توان دستورالعمل‌ها و عملوندهای یک سیستم رمزنگاری در حال اجرای عملیات رمز برای شکستن آن استفاده کند. اما با توسعه‌ی سیستم رمزنگاری به وسیله‌ی کدهای تصادفی ساختگی[۲] و یا جلوگیری از دسترسی به حافظه با استفاده از پردازش داده‌ها در ثبات‌ها می‌توان از سیستم رمزنگاری در مقابل حمله‌ی SPA[۳] محافظت نمود. در عوض، محافظت از یک دستگاه رمزنگاری در

[1] Side-Channel Attacks

[2] Dummy codes

[3] Simple Power Analysis

حال اجرای عملیات رمز برای شکستن آن استفاده کند. اما با توسعه‌ی سیستم رمزنگاری به وسیله‌ی کدهای تصادفی ساختگی[1] و یا جلوگیری از دسترسی به حافظه با استفاده از پردازش داده‌ها در ثبات‌ها می‌توان از سیستم رمزنگاری در مقابل حمله‌ی SPA[2] محافظت نمود. در عوض، محافظت از یک دستگاه رمزنگاری در مقابل حمله‌ی تحلیل تفاضلی توان[3] (DPA) بمراتب سخت‌تر است، زیرا این روش از خواص آماری و روش اصلاح خطا برای استخراج اطلاعات مخفی از سیگنال توان مصرفی استفاده می‌کند. کلید مخفی را با در اختیار داشتن صدها و یا هزاران ورودی نمونه و آثار توان مصرفی[4] متناظرشان می‌توان حدس زد. نویزهای تصادفی را می‌توان در اندازه‌گیری‌های توان از طریق فرآیند متوسط‌گیری با استفاده از تعداد زیادی از نمونه‌ها فیلتر کرده و اثر آنها را کاهش داد. حفاظت از پیاده‌سازی‌ها در برابر این حمله‌ی مؤثر و پیچیده از اهمیت ویژه‌ای برخوردار است زیرا DPA حمله‌ای است که به سادگی نمی‌توان با آن مقابله کرد. شخص توسعه‌دهنده همیشه باید اقدام متقابل تحلیل توان را به ویژه برای یک دستگاه با توان مصرفی پایین، مثل کارت‌های هوشمند، در نظر داشته باشد در غیر این صورت دستگاه رمزنگاری اطلاعات کانال جانبی مربوط به کلید مخفی داخلی را، در حین اجرای الگوریتم رمزنگاری فاش می‌کند. لازم به ذکر است که در واقع، تهدید اصلی برای طرح رمزنگاری، شکستن و یا به دست آوردن خود الگوریتم نیست، بلکه کشف نقاط ضعف مربوط به پیاده‌سازی است [۲-۴]. بیشتر مقالات گزارش‌شده حملات را بر روی کارت‌های هوشمند انجام داده‌اند و مقالات کمی به موضوع آسیب‌پذیری پیاده‌سازی FPGA در مقابل حملات تحلیل توان و روش پیاده‌سازی عملی آنها پرداخته‌اند. پیاده‌سازی الگوریتم‌های رمز بر روی FPGA به دلایل متعددی مانند چابکی الگوریتم[5]، سهولت بارگذاری الگوریتم[6]، بازدهی[7] بالا و هزینه‌ی کم بسیار متداول است. با این حال، هنوز پرسش‌های بسیاری در مورد آسیب‌پذیری FPGAها به عنوان یک ماژول برای پیاده‌سازی توابع امنیتی وجود دارد. متأسفانه مقالات بسیار کمی در دسترس است که یک حمله‌ی فیزیکی علیه FPGAهای مبتنی بر SRAM انجام داده باشند [۵-۹]. در این مقاله ما ویژگی این نوع FPGA را در چهارچوب حمله‌ی تحلیل تفاضلی توان نشان می‌دهیم. الگوریتم استاندارد رمزنگاری پیشرفته (AES) به عنوان الگوریتم رمز و Spartan-II Xilinx- به عنوان بستر پیاده‌سازی استفاده شده‌اند.

این پژوهش زمینه‌ی تحقیقات آینده را جهت بررسی تهدید DPA بر FPGAهای مبتنی بر SRAM به منظور حفاظت بهتر از سیستم‌های رمزنگاری در برابر حملات سخت‌افزاری فراهم می‌کند. ادامه‌ی این مقاله به شرح زیر است: در بخش ۲ الگوریتم AES را به طور خلاصه توضیح می‌دهیم. اصول حمله‌ی DPA در بخش ۳ بررسی خواهد شد. بخش ۴ شامل تنظیمات اندازه‌گیری و پیاده‌سازی حمله می‌شود. نتایج و بحث‌ها در بخش ۴-۲ ارائه شده‌است. در نهایت، نتایج کار خود را در قسمت نتیجه‌گیری خلاصه کرده‌ایم.!

۲-الگوریتم AES

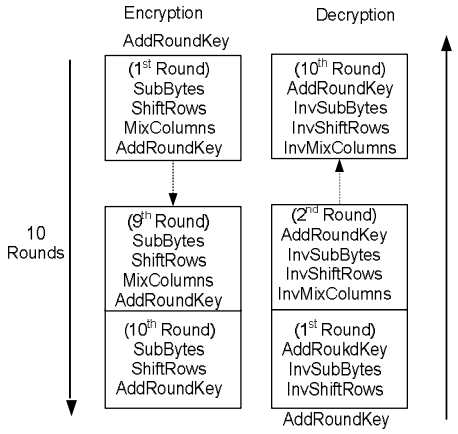
سیستم رمزنگاری AES توسط Daemen و Rijmen توسعه یافته و منتشر شده‌است [۱۰]. این الگوریتم به عنوان یک الگوریتم رمزنگاری بایت‌گرای بلوکی با کلید متقارن، متشکل از ۴ تابع اولیه است که عبارتند از: SubBytes، ShiftRows، MixColumns و AddRoundKey، که این توابع در هر دور اجرا می‌شوند. قبل از هر دور عملیات AddRoundKey که ترکیبی از ورودی با کلید رمزنگاری است اجرا می‌شود. در حالت عملیات ۱۲۸ بیتی، در آغاز رمزنگاری، پیام اصلی به بلوک‌هایی به طول ۱۲۸ بیت تقسیم شده و در آرایه‌ای ۱۶ بایتی موسوم به State ذخیره می‌شود. AddRoundKey یک عملیات ساده‌ی XOR است که در آن عناصر آرایه‌ی State با کلید هر دور (RoundKey) بیت به بیت XOR می‌شوند. SubBytes یک تابع غیرخطی است که عملیات تعویض بایت‌ها را در بردار حالت (State) انجام می‌دهد. در SubBytes، هر بایت آرایه‌ی State توسط بایت متناظر آن در جدول دیگری که S-Box نام دارد جایگزین می‌شود. S-Box شامل مقادیر معکوس ضربی همه‌ی حالت‌های ممکن یک بایت (۲۵۶ حالت) در میدان $GF\left(2^8\right)$، با یک تبدیل affine است. هر بایت در واقع عنصری از میدان گالوای $GF\left(2^8\right)$ است که با چندجمله‌ای ساده‌نشدنی زیر ساخته می‌شود.

$$m(x)=x^8+x^4+x^3+x+1$$

در تبدیل ShiftRows، هر سطر از State به طور جداگانه در نظر گرفته می‌شود و بایت‌های موجود در این سطرها بر اساس اندازه‌ی کلید الگوریتم به صورت گردشی به سمت چپ شیفت پیدا می‌کنند. برای کلید ۱۲۸ بیتی سطر اول تغییر نمی‌کند. درحالی که، سطرهای دوم، سوم و چهارم هر کدام به ترتیب یک، دو و سه بایت شیفت پیدا می‌کنند. تبدیل MixColumns یک جایگشت آجرچین[8] است که به هر ستون از State اعمال می‌شود. در MixColumns، ستون‌های State را به عنوان چند جمله‌ای‌هایی با ۴ جمله در میدان $GF\left(2^8\right)$ در نظر گرفته، آنگاه در چند

[1] Dummy codes
[2] Simple Power Analysis
[3] Differential Power Analysis
[4] Power consumption traces
[5] Algorithm agility
[6] Algorithm upload
[7] Throughput
[8] Bricklayer Permutation

جمله‌ای ثابت $c(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$ ضرب می‌کنیم. ضرب‌ها در پیمانه‌ی (x^4+1) اعمال می‌گردد. الگوریتم رمزگشایی ساختار مشابهی با رمزگذاری دارد با این تفاوت که از معکوس ریاضی مراحل رمزگذاری استفاده می‌کند. یعنی InvSubBytes، InvShiftRows و InvMixColumns. کلیدهای دور همان کلیدها در عملیات رمزگذاری هستند اما در جهت معکوس استفاده می‌شوند. در شکل ۱ پیاده‌سازی استاندارد AES مشاهده می‌شود.



شکل ۱. پیاده‌سازی استاندارد الگوریتم AES

۳-حملات تحلیل توان

تقریباً امروزه تمام مدارهای مجتمع دیجیتال با تکنولوژی CMOS ساخته‌می‌شوند. اگر خروجی یک گیت CMOS تغییر وضعیت دهد، می‌توان این تغییر را در پایه‌ی V_{dd} (یا V_{ss}) اندازه‌گیری کرد. مدارهای CMOS وقتی تغییر وضعیت می‌دهند، توان قابل ملاحظه‌ای مصرف می‌کنند. توان مصرف شده توسط مدار را می‌توان با سری کردن یک مقاومت کوچک R_m بین V_{dd} (یا V_{ss}) و منبع اصلی(یا زمین) مشاهده کرد. از آنجایی که تغییر در حالات و فعالیت سوئیچ زنی وابسته به داده‌ی اصلی است بدیهی است که کلید مورد استفاده در الگوریتم رمزنگاری را می‌توان با استفاده از خصوصیات آماری توان مصرفی وسیله‌ی رمزنگاری و با اعمال تعداد زیادی داده‌ی ورودی به دست آورد. این حملات همان حملات تحلیل توان هستند که از نوع حملات غیر فعال[1] به شمار می‌روند. انتشار توان مصرفی به دو شکل قابل بیان است. زمانی‌که وزن همینگ متناسب با تعداد بیت‌های با ارزش ۱ باشد تعداد تغییر وضعیت‌ها اطلاعاتی راجع به تعداد تغییرات در بیت‌هایی می‌دهد که به طور همزمان پردازش می‌شوند. حملات تحلیل تفاضلی توان (DPA) که توسط Kocher و همکارانش ارائه شد [۲]، از نمونه‌های توان اندازه‌گیری‌شده‌ی متعددی استفاده می‌کند و برای بازیابی اطلاعات مخفی روش‌های آماری در آن اعمال می‌شود.

در DPA، مهاجم با استفاده از یک مدل فرضی به دستگاه رمزنگاری حمله می‌کند و کیفیت این مدل وابسته به دانش مهاجم است. معمولاً در عمل خروجی SubBytes مورد حمله قرار می‌گیرد. حمله به خروجی MixColumns از آنجایی‌که تابعی تعریف شده برای ۳۲ بیت است، بسیار پر هزینه است. هر گونه حمله به این تابع نیاز به فرضیه‌های راجع به کلید برای 2^{32} ترکیب متفاوت دارد که غیر ممکن نیست، ولی هزینه‌ی پردازشی قابل توجهی را به حمله‌کننده تحمیل می‌کند.

لازم به ذکر است که خروجی S-Box در دور اول هدف اصلی حمله است زیرا تنها عملیاتی است که در آن متن اصلی و کلید رمز به‌طور مستقیم با یکدیگر ترکیب می‌شوند. این مدل برای پیش‌بینی مقادیر متعددی از اطلاعات کانال جانبی خروجی یک وسیله‌ی رمزنگاری استفاده می‌شود. این پیش‌بینی‌ها با مقادیر واقعی اندازه‌گیری‌شده برای کانال جانبی رمزکننده مقایسه می‌شوند. این مقایسه‌ها با استفاده از روش‌های آماری بر روی داده‌ها اعمال می‌شوند. از میان روش‌های آماری موجود، معروف‌ترین آنها عبارتند از: آزمون فاصله‌ی میانگین[2] و تحلیل همبستگی[3]. در این کار ما از هر دو روش برای بازیابی کلید مخفی استفاده کرده‌ایم. در روش تحلیل همبستگی، مدل مورد نظر میزان نشت کانال جانبی را برای لحظه‌ای خاص از زمان که عملیات در حال اجرا است پیش بینی می‌کند. این پیش‌بینی‌ها با خروجی واقعی کانال جانبی از لحاظ شباهت و همبستگی مقایسه می‌شوند. مقدار این همبستگی را می‌توان با استفاده از ضریب همبستگی پیرسون (Pearson) اندازه‌گیری کرد [۵].

فرض کنیم t_i مقدار i ام توان مصرفی و T مجموعه‌ای از این مقادیر توان مصرفی اندازه‌گیری‌شده باشد و هم‌چنین فرض‌کنیم p_i پیش‌بینی صورت گرفته از مدل برای مقدار i ام و P مجموعه‌ای از این پیش‌بینی‌ها باشد. حال تابع همبستگی را می‌توان به شکل زیر تعریف نمود:

$$C(T,P)=\frac{E(T\cdot P)-E(T)E(P)}{\sqrt{Var(T)\cdot Var(P)}} \qquad (۱)$$

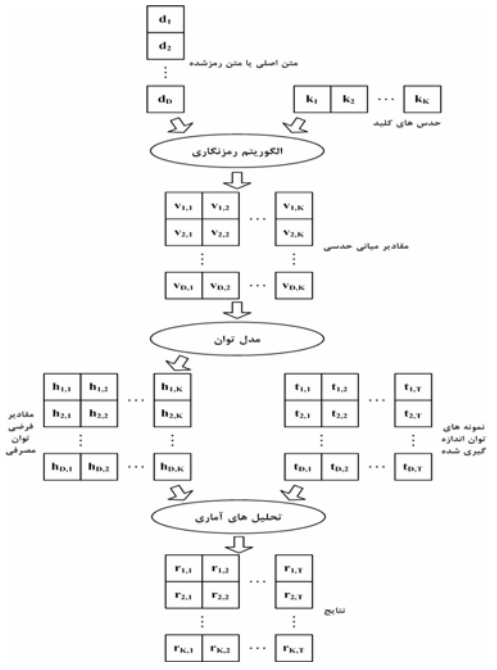
در این رابطه $E(T)$ نشان‌دهنده‌ی میانگین آماری اثری از مجموعه‌ی مقادیر توان T و $Var(T)$ نشان‌دهنده‌ی واریانس مجموعه‌ای از آثار T است. اگر مقدار این همبستگی زیاد باشد، می‌توان گفت که پیش‌بینی مدل، و متعاقباً حدس کلید رمزنگاری درست است [۵].

سناریوی حمله‌ی DPA مبتنی بر آزمون فاصله‌ی میانگین، به شرح زیر است [۵]:

[1] Passive attacks

[2] Distance-of-mean
[3] Correlation Analysis

در ابتدا N متن آشکار به صورت تصادفی تولید می‌شود. مقادیر توان مصرفی برای هر متن آشکار اندازه‌گیری می‌شود. حمله‌کننده N مقدار اندازه‌گیری شده را که هر کدام دارای n نمونه هستند به دست می‌آورد. سپس به یک مدل فرضی از AES (طوری که شامل یک تابع AddRoundKey و جدول جستجوی S-Box در دور اول است) متن آشکار و یک بایت از کلید رمزنگاری را اعمال می‌کند. به خروجی این فرضیه، یک تابع انتخاب‌گر[1] S اعمال می‌شود. این تابع انتخاب‌گر مقادیر اندازه‌گیری‌شده را به دو مجموعه تقسیم می‌کند. یک مجموعه شامل مقادیری است که تابع انتخابگر خروجی ۱ و مجموعه‌ی دیگر مقادیری است که تابع انتخابگر خروجی ۰ را برمی‌گرداند. برای هر مجموعه مقدار متوسط محاسبه می‌شود. سپس تفاوت بین دو میانگین محاسبه می‌شود. برای هر یک از منحنی‌های تفاضلی بالاترین پیک و مقدار متوسط هر منحنی محاسبه می‌گردد. سپس این دو مقدار بر هم تقسیم می‌شوند (مقدار متوسط/ بیشترین پیک). مراحل فوق برای هر یک از فرضیه‌ها تکرار می‌شود. این منجر به 2^8 منحنی تفاضلی می‌شود. منحنی‌های تفاضلی به دست آمده را مورد بررسی قرار می‌دهیم. فقط برای زیرکلید صحیح تابع انتخاب درست کار کرده و پیک‌هایی در نمودار به خوبی دیده می‌شود. این روش ۱۶ بار (برای کلید ۱۲۸ بیتی) برای دریافت همه‌ی زیرکلیدها تکرار می‌شود. روند کلی تحلیل تفاضلی توان در شکل ۲ به صورت دیاگرام روندی قابل مشاهده است.



شکل ۲. مراحل کلی پیاده‌سازی تحلیل تفاضلی توان

[1] Selection Function

۴-پیاده‌سازی عملی حمله

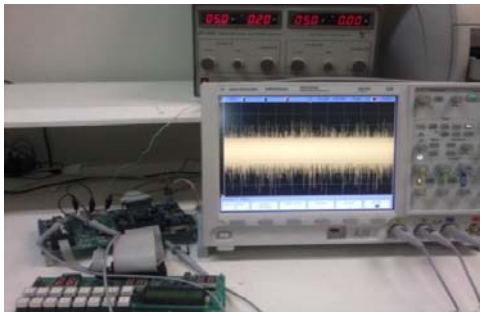
در این قسمت ابتدا تنظیمات اندازه‌گیری برای حمله‌ی DPA را مورد بحث قرار می‌دهیم و پس از آن نتایج عملی به‌دست آمده را ارائه خواهیم کرد.

۴-۱-تنظیمات آزمایشی برای پیاده‌سازی حمله‌ی DPA روی Xilinx Spartan-II مبتنی بر SRAM

ابتدا الگوریتم AES را با معماری Loop-Unrolled بر روی FPGA پیاده‌سازی کردیم به‌گونه‌ای که در هر زمان تنها یک بلوک از داده مورد پردازش قرار می‌گیرد.

لوازم مورد نیاز شامل بورد FPGA Xilinx Spartan-II، اسیلوسکوپ دیجیتال Agilent MSO-7034A با نرخ نمونه‌برداری 2 Gs/sec و پهنای باند BW=350 MHz و پروب جریان Agilent 10073C برای اندازه‌گیری جریان تغذیه است. این بورد از ۲ منبع تغذیه جداگانه، منبع ۳/۳ V برای تغذیه‌ی I/O و یک منبع ۲/۵ V برای تغذیه‌ی مدارهای منطقی و هسته‌ی اصلی تراشه استفاده می‌کند. به منظور اندازه‌گیری توان مصرفی هسته‌ی رمزنگاری یک مقاومت کوچک (۱۰ اهم) بین بورد FPGA و منبع تغذیه‌ی ۲/۵ V قرار داده شده است.

برای کاهش نویز سوئیچینگ تمام اندازه‌گیری‌ها ۱۰ بار تکرار شده و از آنها متوسط‌گیری کردیم. فرکانس کار بورد FPGA برای کاهش نویز سوئیچینگ، جمع‌آوری اطلاعات بیشتر و بهبود دقت و صحت حمله، با استفاده از تقسیم‌کننده‌ی کلاک داخلی در حالی‌که فرکانس واقعی ۱۰ مگاهرتز بود به 1 KHz کاهش یافته‌است. از آنجایی که با استفاده از اسیلوسکوپ موجود قادر به ذخیره‌ی اطلاعات مربوط به مصرف توان تمام داده‌های رمزشده نبودیم لذا در شروع عملیات رمز هر داده سیستم قربانی یک سیگنال تریگر برای اسیلوسکوپ ارسال کرده و در انتها داده‌های آن را ذخیره می‌نمودیم. این سیگنال برای نمونه‌برداری و ذخیره‌ی چندین نمونه از جریان در دور مورد نظر عملیات رمزنگاری و در پالس‌های ساعت متعددی استفاده شده است. متن آشکار توسط یک LFSR ۱۲۸ بیتی در FPGA تولید شد. تجهیزات مورد نیاز برای پیاده‌سازی حمله‌ی توان در شکل ۳ مشاهده می‌شود.



شکل ۳. تجهیزات آزمایشگاهی به کار رفته در پیاده‌سازی حمله‌ی تحلیل توان

۴-۲-نتایج تجربی!

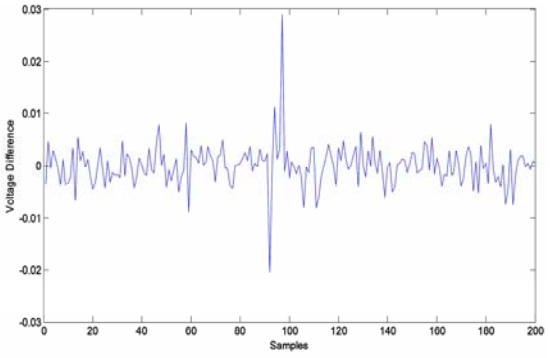
بر اساس مرجع [۲] تحلیل تفاضلی توان AES به یک تابع انتخاب‌گر S نیاز دارد که ما برای محاسبه‌ی مقدار بیت b که قسمتی از بردار میانی SB_1 است از آن استفاده می‌کنیم. می‌توان b را به شکل زیر تعریف نمود:!

$$b = \text{one output bit of } SB_1\ (P_i \oplus SK_1) \qquad (۲)$$

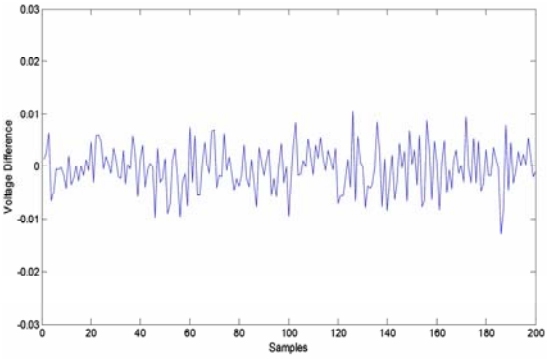
در معادله‌ی (۲) SB_1 تبدیل SubBytes، P_i بیانگر i امین متن-آشکار و SK_1 اولین زیرکلید است.

برای بهبود SNR و دقت حمله ما از یک تابع اتخاب‌گر ۴ بیتی استفاده کرده‌ایم به این مفهوم که وقتی وزن همینگ خروجی تبدیل SubBytes بزرگتر از چهار است مقدار تابع انتخاب‌گر یک می‌شود و در غیر این صورت صفر خواهد بود. در مرجع [۱۱] نشان داده شده که به علت کاهش پیک‌های نامرئی و پیک‌های ثانویه وقتی که ۴ بیت با هم در نظر گرفته شوند بازدهی حمله افزایش می‌یابد.

نتایج تجربی برای مقادیر تفاضلی توان و حدس زیرکلید صحیح و یک زیرکلید غلط به ترتیب در شکل‌های ۴ و ۵ نشان داده شده‌اند. همان‌طور که مشاهده می‌شود نمودار مذکور فرضیه‌ی قابل اندازه‌گیری بودن نشتی اطلاعات وزن‌های همینگ را تایید می‌کند. برای مشخص کردن کلید صحیح که معادل 0x4F است تقریباً ۱۰۰۰ بار اندازه‌گیری توان مصرفی برای متون آشکار تصادفی مورد نیاز خواهد بود.

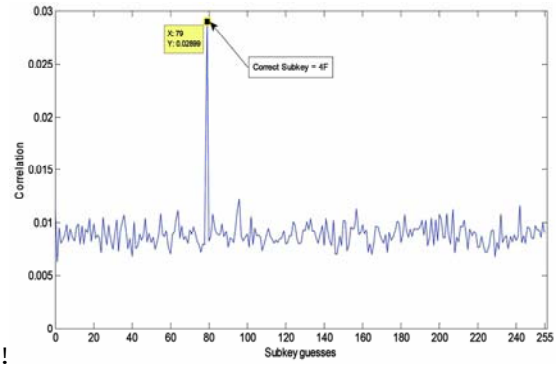


شکل ۴. نمودار تفاضل توان مصرفی برای حدس صحیح از زیرکلید



شکل ۵. نمودار تفاضل توان مصرفی برای یک حدس غلط از زیرکلید

برای پیاده‌سازی تحلیل همبستگی، FPGA را طوری برنامه‌ریزی کردیم که تعداد N متن‌آشکار را با کلید یکسان رمز کند. هنگامی که تراشه در حال انجام عملیات است توان مصرفی اولین پالس ساعت هر فرآیند رمزنگاری را اندازه گرفتیم یعنی پالسی که در آن عمل S-box انجام می‌شود. سپس اثرات توان مصرفی هر عمل رمزگذاری ۱۰ بار میانگین‌گیری شد تا نویز از اندازه‌گیری‌هایمان حذف شود و بیشترین مقدار هر پالس رمزگذاری را ذخیره کردیم تا یک ماتریس ستونی از مقادیر توان مصرفی برای همه‌ی متن بدست آوریم. به این ماتریس به دست‌آمده ماتریس توان کل می‌گوییم. برای هر کدام از N متن رمزشده حمله‌کننده ابتدا هدف یعنی خروجی اولین S-box را برای تابع انتخاب‌گر S انتخاب می‌کند. سپس مقدار S (یعنی تعداد تغییر بیت‌های خروجی S-box) را برای ۲۵۶ حدس کلید با استفاده از یک ابزار شبیه‌سازی پیش‌بینی می‌کند. نتیجه‌ی فاز پیش‌بینی یک ماتریس پیش‌بینی انتخاب‌شده‌ی $N \times 256$ است که محتوی اعدادی صحیح بین ۰ تا ۷ است. سپس ضریب همبستگی بین ماتریس توان مصرفی کل و همه‌ی ستون‌های ماتریس پیش‌بینی انتخاب‌شده (مربوط به همه‌ی ۲۵۶ حدس کلید) را محاسبه می‌کنیم. اگر حمله موفقیت‌آمیز باشد، انتظار می‌رود فقط یک مقدار که مربوط به مقدار حدس صحیح است منجر به مقدار بالای ضریب همبستگی شود. نتایج همه‌ی این همبستگی‌ها برای اولین بایت کلید در شکل ۶ نشان داده شده است. مقدار صحیح یعنی 0x4F مثل یک پیک واضح مشاهده می‌شود. آزمایش ما نشان داد که بازیابی کامل یک کلید ۱۲۸ بیتی با این روش و با رایانه‌ای با پردازنده‌ی Intel 2.5 GHz Core2 Quad تقریباً ۲ ساعت طول می‌کشد.



!

شکل ۶. بازیابی زیرکلید صحیح با استفاده از یک حمله‌ی همبستگی که با مقادیر واقعی اندازه‌گیری شده‌است.

۵- نتیجه‌گیری

پیاده‌سازی عملی DPA روی AES هنوز موضوع مهمی برای تحقیق و پژوهش است و پتانسیل بالقوه‌ای برای بهبود کیفیت آن وجود دارد. این کار نشان داد که تحلیل تفاضلی توان تهدیدی جدی برای امنیت سیستم‌های رمزنگاری پیاده‌شده روی

FPGAهای مبتنی بر SRAM است به گونه‌ای که توانستیم ۱۲۸ بیت کلید مخفی را در مدت زمان ۲ ساعت بازیابی کنیم. اگر چه ویژگی‌های خاص FPGA به‌طور قابل ملاحظه‌ای پیاده‌سازی عملی حملات توان را در مقایسه با کارت‌های هوشمند مشکل می‌کند اما ما آزمایش‌های تجربی مناسبی برای رسیدن به نتایج دلخواه انجام دادیم. بسیاری از راه‌کارها به ما اجازه می‌دهد که اندازه‌گیری‌های خود را بهبود دهیم که این موضوع پژوهش‌های بعدی است. هم‌چنین ابهاماتی در مورد امنیت فیزیکی FPGAها وجود دارد که از دیگر موضوعات تحقیق ما در آینده است. حمله را می‌توان با ترکیب حملات توان و دیگر تکنیک‌های کانال جانبی نیز پیاده‌سازی کرد که آنها نیز به نوبه‌ی خود می‌توانند موضوعات جذاب دیگری برای تحقیق و پژوهش باشند.

مراجع!

[۱] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks (Revealing the Secrets of Smart Cards)*, Springer, Graz University of Technology-Austria, 2007.

[۲] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis”, Advances in Cryptology-Crypto 1999, LNCS 1666, Springer-Verlag, 1999, pp. 388-397.

[۳] F.X. Standaert, L.van Oldeneel, D.Samyde, and J.J. Quisquater, “Power Analysis of FPGAs, How Practical is the Attack?”, in the proceedings of FPL 2003, Lecture Notes in Computer Science, vol. 2278, Springer-Verlag, 2003, pp. 701-711.

[۴] L.T. Mc Daniel, *An Investigation of Differential Power Analysis Attacks on FPGA-based Encryption Systems*, Master Thesis, Virginia Polytechnic Institute, May 29, 2003.

[۵] S.B. Ors, E. Oswald, “Power Analysis Attacks against FPGA-First Experimental Results”, Advances in Cryptology-CHES2003, LNCS 2779, Springer-Verlag, 2003, pp. 35-50.

[۶] F.X. Standaert, E. Peeters, F. Mace, J. J. Quisquater, “Updates in Security of FPGA against Differential Power Attacks”, in the Proceedings of ARC2006, LNCS 3958, Springer-Verlag, 2006, pp. 335-346.

[۷] T. Wollinger, J. Guajardo, and C. Paar, “Security on FPGAs: State-of-the-Art Implementations and Attacks”, *ACM Transactions on Embedded Computing Systems*, Vol. 3, No. 3, August 2004, pp. 534-574.

[۸] J. Goodwin and P.R. Wilson, “Advanced Encryption Standard (AES) Implementation with Increased DPA Resistance and Low Overhead”, International Symposium on Circuits and Systems (ISCAS2008), IEEE, Washington, USA, May 2008, pp. 3286-3289.

[۹] H. Yu, Z. Xue-cheng, L. Zheng-lin, C. Yi-cheng, “The Research of DPA Attacks Against AES Implementation”, *The Journal of China Universities of Posts and Telecommunications*, Elsevier, Dec. 2008, 15(4), pp. 101-106.

[۱۰] J. Daemen and V. Rijmen, “AES Proposal: Rijndael”, National Institute of Standards and Technology (NIST), July 2001, pp. 165-188.

[۱۱] T-Ha Lee, C. Canovas, and J. Cledier, “An overview of side-channel analysis attacks”, Proceedings of the 2008 ACM symposium on Information, computer and communications security, ACM, Tokyo, Japan, March 18-20, 2008, pp. 33-43.