نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۴، زمستان ۱۳۹۸، ص ۵۷-۵۱

تحلیل کانال جانبی الگوریتم رمزنگاری IDEA

عبدالرسول میرقدری[۱*]، حسین باقری[۲]
۱- دانشیار، ۲- دانشجوی ارشد، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۷/۱۱/۲۳، پذیرش: ۹۸/۰۳/۲۸)

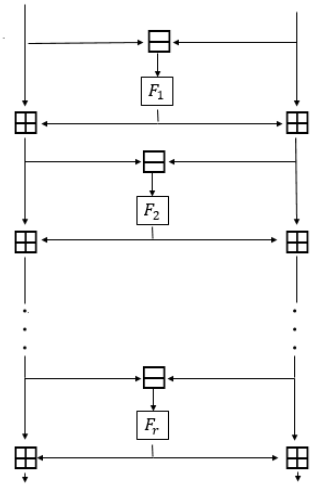
چکیده

الگوریتم رمزنگاری IDEA یک رمزنگار متقارن از نوع قالبی است که دارای طول قالب ۶۴ بیت و کلید رمز ۱۲۸ بیتی می‌باشد. این الگوریتم طی ۸،۵ دور فرآیند رمزنگاری ۶۴ بیت متن آشکار را به ۶۴ بیت متن رمزی نگاشت می‌دهد. این الگوریتم تا کنون در برابر اغلب حمله‌های مطرح تحلیل رمز مقاوم می‌باشد. در این مقاله مقاومت الگوریتم IDEA در برابر تحلیل کانال جانبی همبستگی توان بررسی شده است. با پیاده‌سازی این الگوریتم بر بستر میکروکنترلر PIC، چندین نمونه از توان مصرفی دستگاه در حین پردازش اندازه‌گیری شده است. نتایج تجزیه و تحلیل نمونه‌های اندازه‌گیری‌شده نشان‌دهنده مقاومت خوب الگوریتم در برابر تحلیل کانال جانبی همبستگی توان می‌باشد.

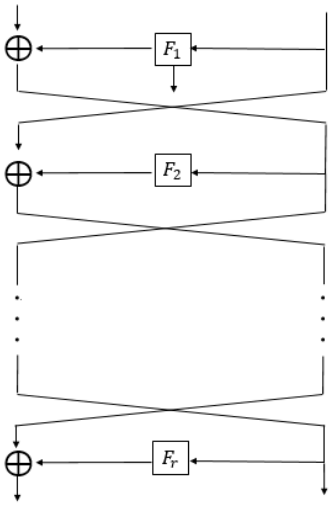
کلیدواژه‌ها: الگوریتم رمزنگاری IDEA، تحلیل کانال جانبی، میکروکنترلر PIC

۱. مقدمه

الگوریتم‌های رمزنگاری متقارن به دو شاخه رمزهای دنباله‌ای و قالبی تقسیم‌بندی می‌شوند که الگوریتم‌های رمزنگاری قالبی شاخه‌ای پرکاربرد در مبحث رمز و حوزه امنیت اطلاعات و ارتباطات هستند. الگوریتم رمزنگاری متقارن IDEA از ساختار لی– مسی پیروی کرده و از نوع قالبی است. این ساختار با اعمال تغییراتی روی ساختار فیستل ابداع شد که هر دو ساختار در شکل‌های (۲-۱) دیده می‌شود [۱].



شکل (۱): ساختار لی- مسی، r دوری [۱]

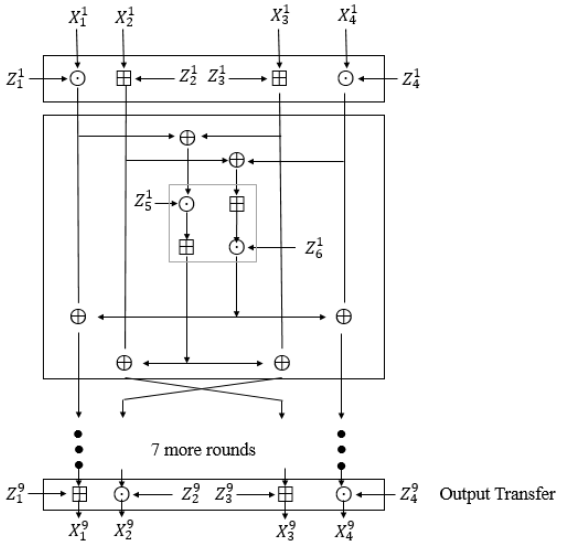


شکل (۲): ساختار فیستل، r دوری [۱]

سؤال مهم این است که آیا این الگوریتم در برابر حمله کانال جانبی توان مقاوم است؟ با مطالعات میدانی و کتابخانه‌ای و بررسی دقیق برخی مقالات و گزارش‌های علمی مرتبط با موضوع و نیز پیاده‌سازی سخت‌افزاری الگوریتم IDEA بر بستر میکرکنترلر PIC و تحلیل استنباطی نتایج حاصل از نمونه‌های توان مصرفی سخت‌افزار در حین پردازش به این سؤال پاسخ داده می‌شود. الگوریتم رمز IDEA دارای زیربنای مستحکمی از دیدگاه نظری بوده و تا به حال هیچ حمله موفقی که منجر به کشف کامل کلید آن شود گزارش نشده است [۲].

* رایانامه نویسنده مسئول: amrghdri@ihu.ac.ir

یکی از دلایل استحکام این الگوریتم را می‌توان استفاده از عملگرهای مناسب به‌خصوص عملگر ضرب در پیمانه 2^{16} دانست. این الگوریتم علاوه بر عملگر XOR ($\oplus$) از عملگر جمع در پیمانه 2^{16} با نماد $\boxplus$ و عملگر ضرب در پیمانه 2^{16} با نماد $\odot$ بهره می‌برد. طول کلید این الگوریتم ۱۲۸ بیت و طول قالب ورودی و خروجی آن ۶۴ بیت می‌باشد. متن رمزی خروجی این الگوریتم پس از ۸ دور فرایند رمزنگاری و نیم دور تبدیل نهایی تولید می‌شود که ساختار شکلی آن در شکل (۳) مشاهده می‌شود [۳].



شکل (۳): الگوریتم رمزنگاری IDEA [۳]

بهترین حمله معرفی‌شده (از نوع جعبه سیاه) روی IDEA تا سال ۲۰۰۶ حمله بهبودیافته دمیرسی- سلکوچر[1] بود، که تنها روی پنج دور از IDEA عمل می‌کرد و توسط آیاز[2] و سلکوک[3] ارائه شد [۴]. با توجه به این‌که این تحلیل 2^{124} بار پیچیدگی داشت، تنها اندکی از حمله جستجوی کور کارآمدتر بود. در همان سال بیهام[4] و همکارانش توسط روش کلید ضعیف Biryukuv-Demirci حمله‌ای روی پنج دور از الگوریتم IDEA اعمال کردند و توانستند پیچیدگی را به 2^{103} کاهش دهند [۵].

در سال ۲۰۰۷ بیهام تحلیل روی ۶ دور از الگوریتم را توسط بهبود و توسعه برخی روش‌های تحلیل، اعمال کرد. که پیچیدگی آن روش به شدت بالا بود و فقط سرعت اجرای آن دو برابر بیشتر از روش جستجوی کور بود. برای انجام این حمله نیاز به 2^{64} زوج Plaintext و Ciphertext بود [۶].

پس از آن در سال ۲۰۰۹ حمله‌ای روی شش دور از IDEA توسط لی[5] و سان[6] بهبود داده شد که به جای 2^{64} از 2^{49} زوج متن آشکار و متن رمزی استفاده می‌شد [۷].

در سال ۲۰۱۱ بیهام حمله دیگری معرفی کرد که قوی‌ترین تحلیل اعمال‌شده بر IDEA بود. با ترکیب کلید ضعیف Biryukov-Demirci و حمله ملاقات در میان، حمله جدیدی بر روی ۶ دور به وجود آمد، که پیچیدگی اطلاعات را به 2^{49} کاهش داد و سرعت بیشتری نسبت به حمله لی و سان داشت. برای افزایش دورهای مورد حمله نیز از روش Splice-and-cut استفاده شد که در نتیجه آن تعداد دورهای مورد حمله از ۶ دور به ۷/۵ دور افزایش یافت [۸]. حملات انجام‌شده روی این الگوریتم در جدول (۱) مشخص شده است.

جدول (۱): مشخصات حملات انجام‌شده روی الگوریتم IDEA

سال حمله	پیچیدگی زمان	پیچیدگی داده	نوع حمله	تعداد دور
۱۹۹۳	2^{40}	2^{10}	Differential	۲
۱۹۹۷	2^{44}	2^{29}	Differential-linear	۳
۱۹۹۹	$2^{66.6}$	$2^{36.6}$	Impossible differential	۴
۲۰۰۶	2^{124}	$2^{24.6}$	Demirci-Selcuk-Ture	۵
۲۰۰۷	$2^{126.8}$	2^{32}	ZitM BD-relation	۵,۵
۲۰۰۷	$2^{126.8}$	2^{64}	ZitM BD-relation	۶
۲۰۰۹	$2^{112.1}$	2^{49}	Key-dependent linear	۷
۲۰۱۱	$2^{123.4}$	۲	MitM BD-relation	۶
۲۰۱۱	$2^{111.9}$	۱۶	MitM BD-relation	۶
۲۰۱۱	2^{122}	2^{10}	SaC MitM BD-relation	۶,۵
۲۰۱۱	$2^{111.9}$	2^{32}	SaC MitM BD-relation	۶,۵
۲۰۱۱	2^{112}	2^{48}	SaC MitM BD-relation	۷
۲۰۱۱	$2^{125.9}$	۱۶	SaC MitM BD-relation	۷,۵
۲۰۱۱	2^{114}	2^{63}	SaC MitM BD-relation	۷,۵
۲۰۱۱	2^{103}	2^{25}	RK ZitM BD-relation	۷,۵
۲۰۱۱	$2^{126.8}$	۱۶	SaC MitM BD-relation	۸,۵
۲۰۱۲	$2^{126.5}$	2^{18}	Biclique BD-relation	۷,۵
۲۰۱۲	$2^{123.9}$	2^{52}	Biclique BD-relation	۷,۵
۲۰۱۲	2^{126}	2^{52}	Biclique BD-relation	۸,۵

به‌طور کلی حملات فیزیکی [۱۱-۱۰] بر اساس شرایط و محدودیت‌های مهاجم در اعمال حمله، به سه دسته تقسیم می‌شوند که عبارتند از:

- حملات تهاجمی: در این حالت مهاجم بدون هیچ محدودیتی به دستگاه رمزنگار دسترسی دارد. برای مثال می‌تواند تراشه را باز کرده به‌صورت اتصالات الکتریکی القای خطا کند. در این دسته از حملات به‌طوری کلی مهاجم هیچ محدودیتی از نظر دسترسی به دستگاه رمزنگار، در این نوع حمله ندارد.

[1] Demirci-Selcukture
[2] Eyüp Serdar Ayaz
[3] Ali Aydın Selçuk
[4] Eli Biham
[5] Xuejia Lai
[6] Xiaorui Sun

● حملات نیمه‌تهاجمی[1]: در این حالت مهاجم تراشه را باز کرده، یعنی پوشش روی دستگاه رمزنگار را برداشته تا به سطح زیرین آن (سیلیکون) برسد. در این دسته از حملات مهاجم قادر به اتصال الکتریکی به تراشه نبوده و در سطح لایه‌های تراشه تخریب ایجاد نمی‌کند.

● حملات غیرتهاجمی[2]: در این حالت مهاجم به هیچ وجه در دستگاه رمزنگار تخریب ایجاد نمی‌کند و حتی پوشش تراشه را نیز برنمی‌دارد.

همچنین هریک از این دسته‌ها بر اساس رفتار مهاجم به دو دسته فعال[3] و غیرفعال[4] تقسیم می‌شوند. در حالت غیرفعال مهاجم هیچ مشکل و خطایی برای تراشه به ایجاد نکرده و فقط به اندازه‌گیری سیگنال می‌پردازد. اما در حالت فعال مهاجم با ایجاد مشکل برای دستگاه باعث اختلال در فرایند رمزنگاری می‌شود.

اولین حمله کانال جانبی اعمال‌شده روی IDEA در سال ۲۰۰۰ توسط اشنایر[5]، کلسی[6] و واگنر[7] معرفی شد. سازوکار اساسی این حمله، جستجو برای یافتن یک یا دو مقدار آشکار ۱۶ بیتی برای تحلیل رمز است، که نشانگر مقدار ورودی صفر در عملگر ضرب پیمانه‌ای می‌باشد. با محاسبه مدت زمانی که برای رمز شدن یک قالب الگوریتم IDEA مورد نیاز است را می‌توان به روش‌های زیر مورد تحلیل قرار داد [۹].

الف- اجرای تمام عملگرهای الگوریتم به غیر از عملگر ضرب پیمانه‌ای، مقدار زمان تقریبی ثابتی را صرف می‌کنند.

ب- همه عملگرهای ضرب پیمانه‌ای به غیر از آنهایی که برای یک مرتبه مورد حمله قرار گرفته‌اند، دارای توزیع نرمال تقریبی هستند.

ج- عملگر ضرب پیمانه‌ای مورد حمله، در حالتی که مقدار داخلی صفر دارد نسبت به حالتی که مقدار داخلی آن صفر نیست ممکن است زمان کمتری صرف کند.

اگر بتوان تفاوت مدت زمان آماده شدن خروجی عملگر ضرب پیمانه‌ای مورد حمله، در حالتی که مقدار داخلی آن صفر است نسبت به حالتی که مقدار داخلی این عملگر صفر نیست را تشخیص داد، می‌توان پی برد که عملگر ضرب پیمانه‌ای که مورد حمله قرار گرفته دارای مقدار داخلی صفر یا غیرصفر است. در این حمله گروه تحلیلگر به دنبال شکست کامل الگوریتم نبودند، بلکه به دنبال یافتن تعداد بیت‌های برابر صفر در متن آشکار بودند. در نهایت اعلام شد که این حمله کانال جانبی دارای همبستگی بسیار پایینی با بیت‌های اختیار شده در حالت داخلی داشته و در نتیجه نمی‌توان مقدار ورودی عملگر ضرب پیمانه‌ای را به دست آورد. دیگر تحلیل کانال جانبی اعمال‌شده روی IDEA توسط داس و باندوپادیا در سال ۲۰۱۶ با اندازه‌گیری مدت زمان اجرای الگوریتم و بررسی آن به‌منظور بازیابی کلید صورت گرفت [۱۰]. در نهایت به علت زمان‌های متفاوت فرایند رمزنگاری، به‌طوری که مدت زمان اندازه‌گیری شده مستقل از طول کلید و ورودی سیستم رمزنگار بوده و زمان اجرای الگوریتم به خصوصیات پردازشگر و چگونگی پیاده‌سازی روی سخت‌افزار وابسته است لذا گروه تحلیلگر اعلام کرد که تحلیل کانال جانبی روی IDEA موفقیت‌آمیز نبوده و اطلاعات زمانی دریافت شده در این تحلیل هیچ همبستگی بین ورودی و خروجی را نشان نمی‌دهد.

۲. پیاده‌سازی الگوریتم IDEA روی میکروکنترلر PIC

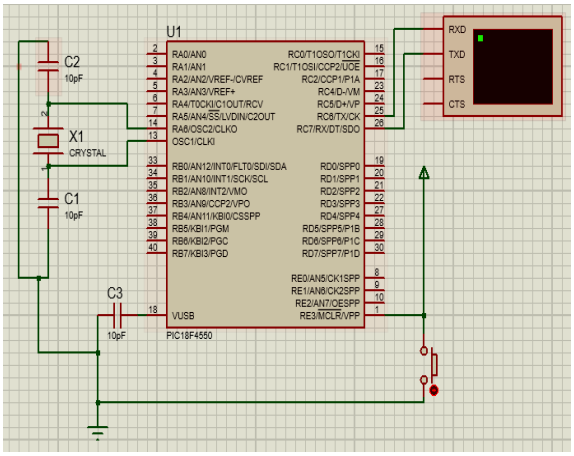
برای پیاده‌سازی الگوریتم IDEA روی میکروکنترلر PIC از زبان برنامه‌نویسی C استفاده شد. سورس کد این پیاده‌سازی را می‌توان به روش‌های گوناگون نوشت. در این مقاله عملگرهای الگوریتم به‌صورت ساده نوشته شدند تا در قبال کاهش سرعت اجرای الگوریتم، احتمال تشخیص عملگرهای الگوریتم حین انجام فرآیند رمزنگاری در زمان انجام حمله کانال جانبی افزایش یابد (شکل (۴)).

```
Bin key, plain, mul, cipher,
void _encryption()
{
cipher = plain+key;
} {
if (key == 0)
key2 = 65536;
else
key2 = key;
if (plain == 0)
plain2 = 65536;
else
plain2 = plain;
ans = plain2*key2;
mul = ans;
key3 = mul;
plain3 = mul>>16;
if (key3 >= plain3)
cipher = key3-plain3;
else
cipher= (key3-plain3)+m;  }
```

شکل (۴): پیاده‌سازی جمع و ضرب در پیمانه 2^{16} در کامپایلر MikroC PRO for PIC

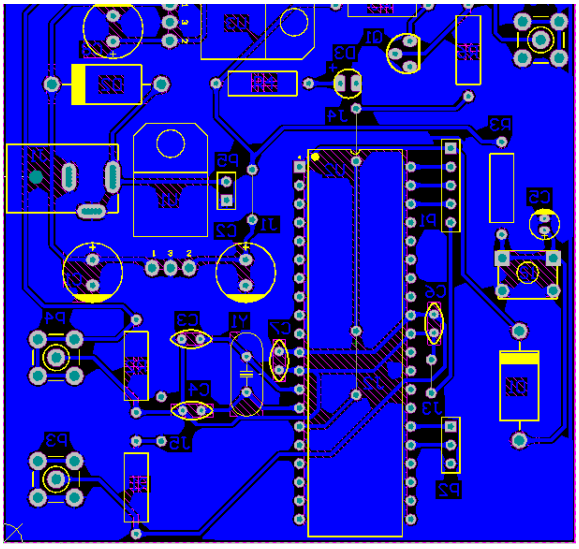
[1] Semi-Invasive Attacks
[2] Non-Invasive Attacks
[3] Active
[4] Passive
[5] Bruce Schneier
[6] John Kelsey
[7] David Wagner

پس از نوشتن سورس کد الگوریتم IDEA برای بررسی صحت عملکرد آن از شبیه‌ساز پروتئوس (Proteus) استفاده شد. برای این منظور ابتدا مدار مورد نیاز برای پیاده‌سازی در این نرم‌افزار طراحی و صحت عملکرد سورس‌کد نوشته‌شده الگوریتم بر بستر این مدار تائید شد (شکل (۵)).



شکل (۵): پیاده‌سازی الگوریتم IDEA توسط شبیه‌ساز Proteus

برای اطمینان از صحت عملکرد الگوریتم IDEA در شرایط عملی، مدار طراحی‌شده توسط شبیه‌ساز پروتئوس روی بورد به همراه نوسان‌ساز خارجی با فرکانس ۸ MHz پیاده‌سازی شد. برای تزریق برنامه الگوریتم درون میکروکنترلر، از سخت‌افزار PICkit3 و نرم‌افزار PICkit3 v3.10 استفاده شده که به این ترتیب فایل HEX تولیدشده توسط کامپایلر MikroC Pro for PIC بر روی میکروکنترلر برنامه‌ریزی شد. پس از تائید صحت عملکرد الگوریتم نوشته‌شده درون بورد، توسط نرم‌افزار Altium بورد مدار چاپی تک لایه موردنیاز طراحی و تولید شد (شکل (۶)).



شکل (۶): بورد مدار چاپی طراحی‌شده توسط نرم‌افزار Altium

صحت عملکرد بورد مدار چاپی تولیدشده توسط اتصال پورت سریال دستگاه رمزنگار به رایانه و با استفاده از برنامه Docklight که در آن از طریق رایانه متن آشکار برای دستگاه رمزنگار ارسال شده و دستگاه رمزنگار متن رمزی معادل را نمایش می‌دهد، تائید شد.

۳. تحلیل کانال جانبی الگوریتم رمزنگاری IDEA بر بستر میکروکنترلر PIC

در مدل تحلیل کانال جانبی توان ابتدا باید نقطه هدف برای اعمال تحلیل مشخص شود. این نقطه باید دارای سه شرط اساسی زیر باشد:

۱- کلید اصلی در آن نقطه تزریق شده و یا دخیل باشد.

۲- نقطه مورد حمله دارای نشت توان مؤثر باشد.

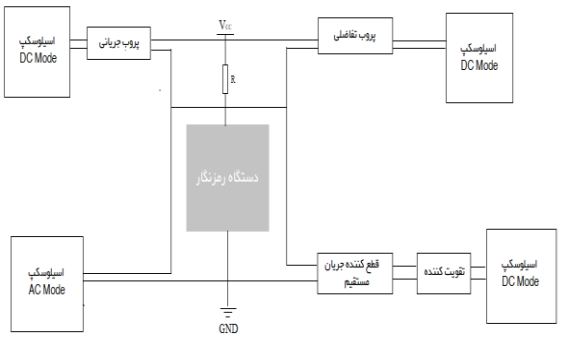
۳- نقطه مورد حمله دارای خروجی غیرخطی باشد.

توجه به این نکته حائز اهمیت است که نقطه مورد حمله، دارای نشت توان مؤثر باشد. زیرا در تحلیل توان باید توان نشتی از عملگر اندازه‌گیری شود و در صورتی که نقطه مورد تحلیل دارای نشت توان مؤثر نباشد، تمیز دادن توان نشت شده از نویز در آن نقطه بسیار مشکل خواهد بود. بنابراین، در عمل امکان موفقیت تحلیل کانال جانبی همبستگی توان در آن نقطه بسیار پائین خواهد بود. عملگر ضرب پیمانه‌ای، در مقایسه با سایر عملگرهای الگوریتم IDEA میزان مصرف توان بیشتری داشته و همچنین دارای خروجی غیرخطی است. بنابراین، در این مقاله عملگر ضرب پیمانه‌ای، به‌عنوان نقطه مناسب جهت اعمال تحلیل کانال جانبی توان تعیین شد.

در این مقاله مسئله بررسی میزان مقاومت عملگر ضرب در پیمانه 2^{16} در برابر تحلیل کانال جانبی همبستگی توان [۱۱] و [۱۲] به مسئله ساده‌تر، یعنی بررسی میزان امنیت عملگر ضرب در پیمانه 2^{8} در برابر تحلیل کانال جانبی همبستگی توان کاهش یافت. بر اساس $2^{8} * 2^{8} = 2^{16}$ و خروجی غیرخطی عملگر ضرب پیمانه‌ای با همبستگی ضعیف می‌توان نتیجه گرفت اگر عملگر ضرب در پیمانه 2^{8} در برابر تحلیل کانال جانبی همبستگی توان مقاوم باشد آنگاه عملگر ضرب در پیمانه 2^{16} نیز در برابر این تحلیل مقاوم بوده و در نتیجه الگوریتم IDEA نیز در برابر تحلیل کانال جانبی همبستگی توان مقاوم خواهد بود. برای بررسی میزان مقاومت عملگر ضرب در پیمانه 2^{8} در برابر تحلیل کانال جانبی همبستگی توان پس از پیاده‌سازی عملگر ضرب در پیمانه 2^{8} با کلید ثابت K=۲ به محاسبه مقدار همبستگی توان مصرفی تراشه با میزان توان مصرفی تخمینی ناشی از خروجی عملگر

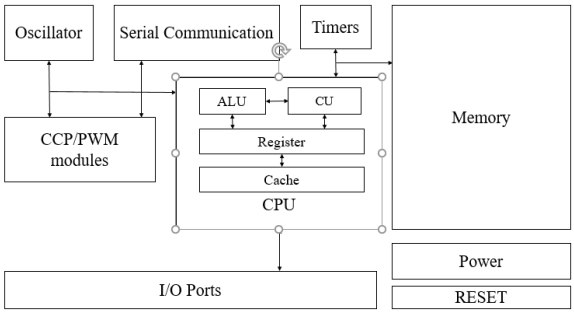
ضرب در پیمانه 2^8 به ازای ورودی‌های ثابت و تمام حالات ممکن کلید پرداخته شد.

برای اندازه‌گیری میزان توان مصرفی دستگاه رمزنگار روش‌های متعددی وجود دارد (شکل (۸)) برای مثال، استفاده از پروب تفاضلی[1] برای اندازه‌گیری اختلاف پتانسیل بین دو نقطه که استفاده از این پروب باعث ایجاد نویز نیز می‌شود و یا استفاده از پروب جریانی[2] که جریان را به ولتاژ تبدیل می‌کند یا استفاده از قطع‌کننده جریان مستقیم[3] که فیلتری است که فرکانس صفر و جریان مستقیم را حذف کرده و باعث مشاهده جریان متناوب می‌شود. همچنین می‌توان از پروب الکترومغناطیسی[4] نیز استفاده کرد که استفاده از این روش به فناوری و کیفیت پروب وابسته است. البته می‌توان از میکروپروب‌ها نیز استفاده کرد که در این روش پیدا کردن بخشی از تراشه که عمل رمز را انجام می‌دهد همچنین فاصله پروب با تراشه حائز اهمیت است.



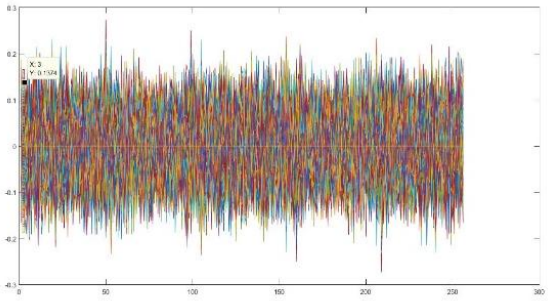
شکل (۷): روش‌های اندازه‌گیری توان مصرفی دستگاه رمزنگار

در این مقاله برای اندازه‌گیری توان مصرفی از اسیلوسکوپ شرکت Tektronix مدل TDS 2024C استفاده شد. این اسیلوسکوپ دارای ۴ کانال و پهنای باند ۲۰۰ MHz بوده و همچنین توانایی نمونه‌برداری ۲ GS/s را دارد. برای اندازه‌گیری دقیق‌تر توان مصرفی دستگاه رمزنگار و کاهش نویزهای محیطی، میکروکنترلر و قطعات به‌کار گرفته‌شده در دستگاه رمزنگار با ورق آلومینیومی پوشانده شد. سپس به اندازه‌گیری توان مصرفی دستگاه رمزنگار با نرخ نمونه‌برداری ۱ GS/s و اعمال تحلیل کانال جانبی همبستگی توان بر روی نمونه‌های اندازه‌گیری شده پرداخته شد. با توجه به ساختار ضرب پیمانه‌ای و نحوه پیاده‌سازی آن روی تراشه، در محاسبه این عملگر داده بین واحد ALU و Register تبادل می‌شود. به‌دلیل آن‌که هر دو واحد ذکرشده درون CPU قرار داشته و خط انتقال داده بسیار کوتاهی دارند انتظار می‌رفت میزان توان مصرفی و نشت توان این عملگر در مقایسه با عملگرهایی که در حین اجرای آن‌ها داده بین واحدهایی با خط انتقال داده بلندتر مثل Memory و CPU تبادل می‌شوند پایین باشد (شکل (۸)).

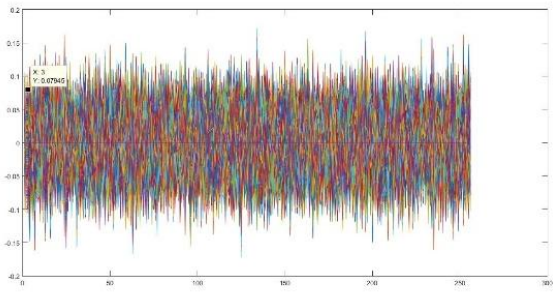


شکل (۸): معماری داخلی میکروکنترلر PIC

شکل‌های (۱۳-۹) نمودار اعمال تحلیل کانال جانبی همبستگی توان روی عملگر ضرب در پیمانه 2^8 را بر بستر میکروکنترلر PIC به‌ازای تعداد نمونه اندازه‌گیری شده نمایش می‌دهند. محور عمودی نمودار نمایانگر میزان همبستگی بین مقدار توان مصرفی تراشه و وزن همینگ خروجی ضرب در پیمانه 2^8 به‌ازای هر یک از حالات ممکن کلید بوده و محور افقی نشانگر تمام حالات ممکن برای کلید است.

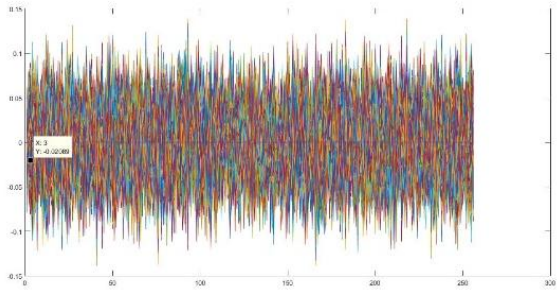


شکل (۹): تحلیل همبستگی توان روی ۳۰۰ نمونه اندازه‌گیری شده از عملگر ضرب در پیمانه 2^8

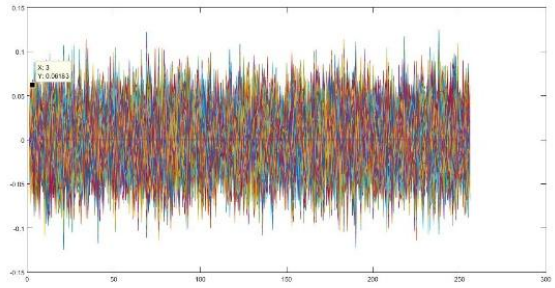


شکل (۱۰): تحلیل همبستگی توان روی ۶۰۰ نمونه اندازه‌گیری شده از عملگر ضرب در پیمانه 2^8

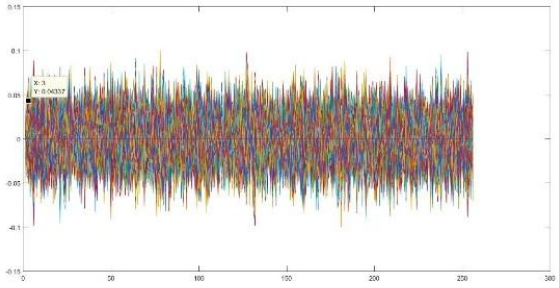
[1] Differential Probe
[2] Current Probe
[3] DC Blocker
[4] Electromagnetic Probe



شکل (۱۱): تحلیل همبستگی توان روی ۹۰۰ نمونه اندازه‌گیری شده از عملگر ضرب در پیمانه 2^8

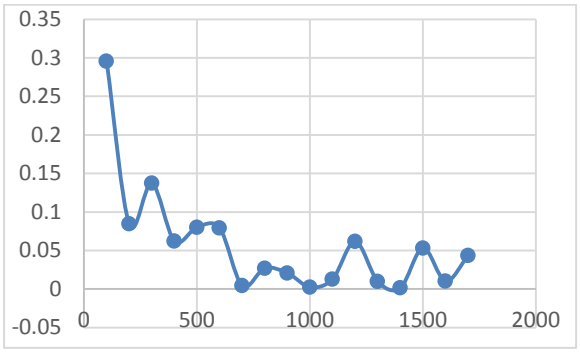


شکل (۱۲): تحلیل همبستگی توان روی ۱۲۰۰ نمونه اندازه‌گیری شده از عملگر ضرب در پیمانه 2^8



شکل (۱۳): تحلیل همبستگی توان روی ۱۷۰۰ نمونه اندازه‌گیری شده از عملگر ضرب در پیمانه 2^8

با دقت در شکل‌های (۱۳-۹) مشاهده می‌شود که در هیچ یک از شکل‌ها نقطه x=۳ دارای مقدار حداکثری نسبت به سایر نقاط نمودار نیست. همچنین هیچ وابستگی بین افزایش نمونه‌های اندازه‌گیری شده‌ی توان مصرفی دستگاه رمزنگار، با کلید صحیح وجود ندارد (شکل (۱۳)). بنابراین، می‌توان نتیجه گرفت که تحلیل کانال جانبی همبستگی توان روی عملگر ضرب در پیمانه 2^8 تحت شرایط بیان شده و به دلیل نشت توان پایین عملگر، وجود نویز سفید، عدم همبستگی قوی بین ورودی و خروجی، ضعیف بودن ابزار اندازه‌گیری توان مصرفی و نویزپذیری بالای بورد مدار چاپی تولیدشده با تعداد نمونه‌های اندازه‌گیری شده برای بازیابی کلید رمز موفقیت‌آمیز نیست.



شکل (۱۴): مقدار همبستگی خروجی ضرب پیمانه‌ای در K=۲ با میزان توان مصرفی دستگاه رمزنگار به‌ازای تعداد نمونه‌های توان

۴. نتیجه‌گیری

در این مقاله برای تحلیل کانال جانبی همبستگی توان الگوریتم IDEA بر بستر میکروکنترلر PIC، خروجی عملگر ضرب در پیمانه 2^{16} به‌عنوان نقطه‌ای مناسب برای تحلیل مشخص شد. همچنین مسئله‌ی تحلیل کانال جانبی همبستگی توان عملگر ضرب در پیمانه 2^{16} به مسئله تحلیل کانال جانبی همبستگی توان روی عملگر ضرب در پیمانه 2^8 کاهش یافت. بنابراین، تحلیل کانال جانبی همبستگی توان تنها زمانی روی عملگر ضرب در پیمانه 2^{16} و الگوریتم IDEA می‌تواند منجر به بازیابی کلید شود، که توسط این مدل حمله بتوان کلید را در عملگر ضرب در پیمانه 2^8 بازیابی کرد. بر این اساس به تحلیل کانال جانبی همبستگی توان روی عملگر ضرب در پیمانه 2^8 پرداخته و مشاهده شد که تحت شرایط موجود تحلیل کانال جانبی همبستگی توان روی عملگر ضرب در پیمانه 2^8 منجر به بازیابی کلید نشد. بر این اساس نتیجه می‌گیریم که تحت شرایط این مقاله، الگوریتم رمزنگاری IDEA در برابر حمله کانال جانبی همبستگی توان مقاوم می‌باشد.

۵. مراجع

[1] S. Vaudenay, "On the Lai-Massey Scheme," ASIACRYPT, vol. 1716, 1999.

[2] H. K. Verma, A. Kumar, and K. Sharma, "Study and Performance Analysis of IDEA with Variable Rounds," International Journal of Advanced Research in Compute Science and Software Engineering, vol. 02, no. 05, 2012.

[3] A. Malekian, "Security of Datas," Nas, 2015.

[4] A. Selcuk and E. Ayaz, "Improved DST Cryptanalysis of IDEA," Lecture Notes in Computer Science (LNCS), vol. 4356, 2006.

[5] O. Dunkelman, N. Keller, and E. Biham, "New cryptanalytic results on IDEA," Lecture Notes in Computer Science (LNCS), vol. 4284, pp. 412–427, 2006.

[6] O. Dunkelman, N. Keller, and E. Biham, "A new attack on 6-round IDEA," in FSE, 2007.

[7] X. Lia and X. Sun, "The key-dependent attack on block ciphers," in ASIACRYPT, 2009.

[8] O. Dunkelman, N. Keller, A. Shamir, and E. Biham, "New Attacks on IDEA with at Least 6 Rounds," Cryptology, pp. 209-239, 2013.

[9] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," Journal of Computer Security, vol. 8, no. 2-3, pp. 141-158, 2000.

[10] S. Bandyopadhyay and K. Das, "Analysis of Side Channel Attacks on Various Cryptographic Algorithms," Journal for Research, vol. 2, no. 5, pp. 36-41, 2016.

[11] Francois Koeune, and Francois-Xavier Standaert, "A Tutorial on Physical Security and Side-Channel Attacks," LNCS, vol. 3655, 2005.

[12] A. Moradi, "Masking as a Side-Channel Countermeasure in Hardware," in Information Security Cryptology, 2016.

Journal of Electronical & Cyber Defence
Vol. 7, No. 4, 2020, Serial No. 28

Side Channel Analysis of International Data Encryption Algorithm (IDEA)

A. Mirghadri*, H. Bagheri

*Imam Hossein Comprehensive University

(Received: 10/06/2018, Accepted: 05/03/2019)

ABSTRACT

The International Data Encryption Algorithm (IDEA)is a symmetric block Cipher with 64 block size and a 128-bit secret key. This algorithm maps a 64-bits plaintext into 64-bits ciphertext in 8.5 encryption rounds. This algorithm has so far been resistant against most known attacks. In this paper, the resistance of IDEA algorithm against correlation power side channel attack is evaluated. By implementing this algorithm on PIC micro controller platform, several samples of power consumption were measured during processing. The results of analyzing the measured samples indicate the resistance of the algorithm to the correlation power side channel analysis.

Keywords: International data Encryption algorithm (IDEA), Side channel attacks, Hardware chips, PIC microcontroller

* Corresponding Author Email: amrghdri@ihu.ac.ir