دانشگاه صنعتی خواجه نصیرالدین طوسی

تاسیس ۱۳۰۷

دانشکده مهندسی برق و کامپیوتر

پایان‌نامه‌ی کارشناسی ارشد در رشته مخابرات-سیستم

موضوع پایان‌نامه:

تحقق عملی حمله‌ی تحلیل تفاضلی توان (DPA) روی پیاده‌سازی FPGA الگوریتم رمزنگاری AES

استاد راهنما:

دکتر محمود احمدیان

استاد مشاور:

دکتر مسعود معصومی

نگارش:

مهدی معصومی

شهریور ماه ۱۳۸۹


بسم الله الرحمن الرحيم

تأییدیه هیأت داوران

هیأت داوران پس از مطالعه پایان‌نامه و شرکت درجلسه دفاع از پایان‌نامه تهیه شده تحت عنوان: "تحقق عملی حمله‌ی تحلیل تفاضلی توان (DPA) روی پیاده‌سازی FPGA الگوریتم رمزنگاری AES" توسط آقای مهدی معصومی، صحت و کفایت تحقیق انجام شده را برای اخذ درجه کارشناسی ارشد در رشته: مهندسی برق گرایش مخابرات-سیستم در تاریخ / / ۱۳ مورد تأیید قرار می‌دهند.

۱- استاد راهنما	جناب آقای دکتر محمود احمدیان	امضاء
۲- استاد مشاور	جناب آقای دکتر مسعود معصومی	امضاء
۳- ممتحن داخلی	جناب آقای دکتر حسین شمسی	امضاء
۴- ممتحن خارجی	جناب آقای دکتر علی پاینده	امضاء
۵- نماینده تحصیلات تکمیلی	جناب آقای دکتر خالوزاده	امضاء

اظهار نامه دانشجو

عنوان پایان‌نامه:

تحقق عملی حمله‌ی تحلیل تفاضلی توان (DPA) روی پیاده‌سازی FPGA الگوریتم رمزنگاری AES

استاد راهنما: دکتر محمود احمدیان

استاد مشاور: دکتر مسعود معصومی

نام دانشجو: مهدی معصومی

شماره دانشجویی: ۸۶۰۰۸۸۴

اینجانب مهدی معصومی دانشجوی دوره کارشناسی ارشد مهندسی برق گرایش مخابرات-سیستم دانشکده مهندسی برق و کامپیوتر دانشگاه صنعتی خواجه نصیرالدین طوسی گواهی می‌نمایم که تحقیقات ارائه شده در این پایان‌نامه توسط شخص اینجانب انجام شده و صحت و اصالت مطالب نگارش شده مورد تأیید می‌باشد، و در موارد استفاده از کار دیگر محققان به مرجع مورد استفاده اشاره شده‌است. به‌علاوه گواهی می‌نمایم که مطالب مندرج در پایان‌نامه تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب یا فرد دیگری در هیچ جا ارائه نشده‌است و در تدوین متن پایان‌نامه چارچوب (فرمت) مصوب دانشگاه را به‌طور کامل رعایت کرده‌ام.

امضاء دانشجو:

تاریخ:

فرم حق طبع و نشر و مالکیت نتایج

۱- حق چاپ و تکثیر این پایان نامه متعلق به نویسنده آن می‌باشد. هرگونه کپی برداری بصورت کل پایان‌نامه یا بخشی از آن تنها با موافقت نویسنده یا کتابخانه دانشکده مهندسی برق دانشگاه صنعتی خواجه نصیرالدین طوسی مجاز می‌باشد.

ضمناً متن این صفحه نیز باید در نسخه تکثیر شده وجود داشته باشد.

۲- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی خواجه نصیرالدین طوسی می‌باشد و بدون اجازه کتبی دانشگاه به شخص ثالث قابل واگذاری نیست.

هم‌چنین استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد.

چکیده:

الگوریتم رمزنگاری Rijndael که در سال ۲۰۰۰ میلادی از سوی موسسه ملی استاندارد و فن‌آوری ایالات متحده (NIST) به‌عنوان الگوریتم استاندارد رمزنگاری داده مورد پذیرش قرار گرفت الگوریتم استاندارد پیشرفته رمزنگاری (Advanced Encryption Standard Algorithm) یا الگوریتم AES نام دارد و از سوی ISO و IEEE نیز به‌عنوان الگوریتم استاندارد رمزنگاری داده شناخته شده‌است. از سال ۲۰۰۰ تاکنون نحوه‌ی پیاده‌سازی سخت‌افزاری هرچه بهتر و مؤثرتر این الگوریتم و مقاومت آن در برابر حملات سخت‌افزاری و بخصوص حملات کانال جانبی از جمله مباحث مورد توجه صاحب‌نظران رمزنگاری بوده‌است. با توجه به اهمیت AES در صنعت و ارتباطات و کاربردهای متنوعی از قبیل کارت‌های هوشمند، وب سرورها، تلفن‌های سلولی، شبکه‌های ATM و ... به عنوان رمزکننده‌ی داده‌ها تلاش برای شکستن این الگوریتم از سوی افراد غیرمجاز و دسترسی به اطلاعات امنیتی صورت می‌پذیرد. دشمن می‌تواند با استفاده از روش‌های مختلفی امنیت سیستم‌های رمزنگاری را تهدید کند. یکی از این تهدیدات که موسوم به حملات کانال جانبی است از اطلاعاتی مثل توان مصرفی, زمان اجرای الگوریتم, تشعشعات الکترومغناطیسی و ... تراشه حین اجرای الگوریتم رمزنگاری استفاده کرده و کلید رمزنگاری را به‌دست می‌آورد. یک نوع حمله‌ی کانال جانبی موسوم به حمله‌ی تحلیل تفاضلی توان (DPA) از قوی‌ترین حملات سخت‌افزاری بوده و می‌تواند در زمان کوتاهی کلید رمز یک الگوریتم پیچیده‌ی رمزنگاری را فاش کند. با استفاده از تحلیل تفاضلی توان (DPA) می‌توان با اندازه‌گیری جریان تغذیه‌ی یک دستگاه، 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 به‌دست می‌آید شباهت داشته باشد، امنیت سیستم رمزنگاری به خطر می‌افتد. وقتی کلید رمزنگاری یک الگوریتم فاش شود به راحتی می‌توان آن سیستم را هک کرد و به اطلاعات آن دسترسی پیدا کرد. در این پایان‌نامه ابتدا یک پیاده‌سازی سخت‌افزاری از الگوریتم Rijndael روی FPGA انجام داده‌ایم. سپس از اطلاعاتی که این تراشه در هنگام اجرای الگوریتم AES می‌دهد استفاده کرده و حمله‌ی تحلیل تفاضلی توان را روی الگوریتم اعمال کردیم و موفق به بازیابی کلید رمزنگاری در مدت ۲ ساعت شدیم. بنابراین اگر الگوریتم و یا تراشه‌ی رمزنگاری غیرامن باشد می‌توان به راحتی و با استفاده از حملات سخت‌افزاری سیستم مذکور را به اصطلاح شکست و موفق به بازیابی کلید رمز آن شد. این پژوهش می‌تواند زمینه‌های جدیدی را در حوزه‌ی رمزنگاری و امنیت اطلاعات ایجاد کند. پیاده‌سازی دیگر حملات سخت‌افزاری یا حمله‌ی DPA از چشم‌اندازهای آینده‌ی این پژوهش است.

واژه‌های کلیدی

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

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فهرست اختصارات استفاده‌شده در متن پایان‌نامه

AES ..... Advanced Encryption Standard Algorithm
ASIC..... Application Specific Integrated Circuit
CBC..... Cipher Block Chaining Mode
CFB ..... Cipher Feedback Mode
CLB..... Configurable Logic Block
CMOS ..... Complementary Metal Oxide Semiconductor
DES ..... Data Encryption Standard Algorithm
DFA..... Differential Fault Analysis Attack
DPA..... Differential Power Analysis Attack
DSA ..... Digital Signature Algorithm
DSP..... Digital Signal Processor
ECB..... Electronic Code Book Mode
EEPROM..... Electrically Erasable Programmable Reed-Only Memory
FIPS ..... Federal Information Processing Standard
FPGA ..... Field Programmable Gate Array
GF..... Galois Field
HDL ..... Hardware Description Language
IPsec..... Internet Protocol Security
LUT..... Look-Up Table
MAC..... Message Authentication Codes
NIST..... U. S. National Institue of Standard and Technology
OFB..... Output Feedback Mode
RSA ..... Rivest-Shamir-Adleman Cryptosystem
S-Box..... Subsituation Box
SCA ..... Side-Channel Attack
SPA..... Simple Power Anslysis Attack
SRAM ..... Static Random Access Memory
VLSI..... Very Large Scale Integrated Circuit
XOR ..... Exclusive OR

فصل اول:

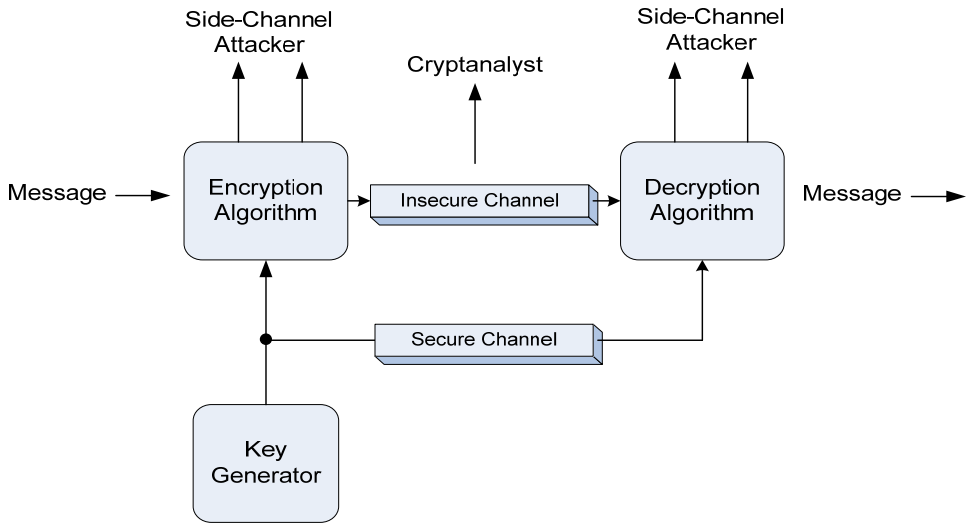
مقدمه

هم‌زمان با پیشرفت و فراگیری روزافزون مخابرات دیجیتال و افزایش حجم مبادله‌ی اطلاعات از طریق شبکه‌های متنوع مخابـره‌ی داده نیاز به استانـداردها و الگوریتم‌های مخابراتی با کارآیی بالا از جملـه ضـروریات دنیـای امروز محسوب می‌شود. یکی از وظایف مهم صاحب‌نظران امروز دنیای ارتباطات طراحی الگوریتم‌هایی با قابلیت و انعطاف‌پذیری بالاست که بتواند پاسخگوی تقاضا برای شبکه‌های مخابراتی پرسرعت، پرظرفیت، کم‌حجم، کم‌هزینه و در عین حال امن باشد. بدون شک امنیت داده‌های مبادله‌شده و رمزکردن آنها از مهم‌ترین مسائل در این حوزه به‌شمار می‌آید. تأمین امنیت در مبادلات مالی و بانکی و نیز ارتباطات نظامی نمونه‌هایی از اهمیت موضوع است. رمزشکن‌ها همیشه و همه جا در کمین اطلاعات مالی یا نظامی هستند که فاش‌شدن آنها ممکن است عواقب جبران‌ناپذیر و وخیمی به دنبال داشته باشد. معمولاً شخص کنجکاو یا رمزشکن گاه سعی می‌کند اطلاعات مبادله‌شده را به دست بیاورد و محرمانگی[1] آن را از بین ببرد. گاهی سعی در تغییر محتوای اطلاعات و خدشه‌دار کردن اصالت[2] آن دارد و بعضاً سعی می‌کند تا خود را به‌جای شخص دیگری معرفی کند و به مطالب مورد علاقه‌اش پی ببرد[3]. رمزنگاری[4] دانش به‌حداقل رساندن مخاطراتی است که ممکن است از این حیث متوجه ما بشود.

یکی از روش‌های رمزکردن اطلاعات، رمزنگاری بلوکی کلیدمتقارن[5] است. از جمله مزایای این روش سرعت، بازدهی و فراهم آوردن امنیت بالاست و واژه‌ی کلیدمتقارن به‌معنای یکسان بودن کلید رمزنگاری بین فرستنده و گیرنده است. پیشرفت سریع میکروالکترونیک به این روند سرعت بیشتری بخشیده و مهندسان را قادر ساخته تا این الگوریتم‌ها را بر روی تراشه‌هایی سریع، اما فشرده و کم-مصرف پیاده‌سازی کنند. استفاده از تراشه‌های رمزنگاری از جنبه‌های سرعت و قابل‌اعتماد بودن بر رمزکردن نرم‌افزاری اطلاعات مزیت دارد زیرا رمزشکن نمی‌تواند به آسانی اطلاعات موجود در آن را بخواند یا عوض کند. البته برخلاف بسیاری از مدارات VLSI موجود، طراحی و پیاده‌سازی چنین

[1] Confidentiality
[2] Integrity
[3] Entity Authentication
[4] Cryptology
[5] Symmetric Key Block Ciphering

تراشه‌هایی از جمله مقولاتی است که هرگز نمی‌تواند توسط یک غیرخودی انجام بگیرد. احتمال آنکه یک غریبه دریچه‌هایی[1] را هنگام طراحی یا پیاده‌سازی در تراشه تعبیه کند که بتواند در موقع لزوم به اطلاعات آن دسترسی پیدا کند مانع از اعتماد به طراحی یا پیاده‌سازی توسط وی خواهد شد. علاوه بر آن طراحی چنین تراشه‌هایی باید به‌دست افرادی توانا و کاملاً آگاه به مقوله‌ی رمزنگاری انجام بگیرد زیرا چنانچه در موقع طراحی برخی مسائل و جوانب مهم در نظر گرفته نشود دشمن با استفاده از اطلاعات جانبی به‌دست آمده از تراشه‌ی در حال رمزنگاری قادر به پی‌بردن به کلید و شکستن رمز خواهد بود. چنانچه در شکل ۱-۱ نشان داده شده‌است ابتدا فرستنده و گیرنده از طریق یک کانال امن بر قسمت کوچکی از اطلاعات که معمولاً کلید رمزنگاری است توافق می‌کنند و سپس از طریق کانالی که ممکن است در معرض استراق سمع دشمن یا هر شخص دیگر قرار بگیرد اطلاعات را به‌صورت رمزشده با یکدیگر مبادله می‌کنند. رمزشکنی در این ساختار به دو دسته‌ی عمده تقسیم می‌شود: ۱) استراق سمع از کانال غیرامن و استفاده از تکنیک‌های خاص شکستن رمز که عمدتاً روش‌های نرم-افزاری، ریاضی و آماری هستند و ۲) استفاده از اطلاعاتی نظیر توان مصرفی یا زمان اجرای الگوریتم در یک تراشه‌ی رمزنگاری که به رمزشکنی سخت‌افزاری یا حملات پیاده‌سازی موسوم هستند.



شکل ۱-۱. مدل حمله به سیستم‌های رمزنگاری کلیدمتقارن.

[1] Trapdoors

در رمزشکنی نرم‌افزاری یا کلاسیک تنها الگوریتم مورد تجزیه و تحلیل قرار می‌گیرد که رمزشکنی خطی و تفاضلی از جمله معروف‌ترین مثال‌های آن هستند.

دسته‌ی دوم حملات که برای اولین بار توسط P. Kocher در سال ۱۹۹۶ مطرح شدند به‌گونه ای کاملاً متفاوت از دسته‌ی اول سیستم را مورد تهاجم قرار می‌دهند. هنگامی که سخت‌افزار در حال پردازش و رمزکردن اطلاعات است می‌توان از اطلاعاتی نظیر توان‌مصرفی سخت‌افزار، تشعشات الکترومغناطیسی آن یا زمان اجرای الگوریتم استفاده کرده و با کمک تحلیل‌های آماری و سایر تکنیک‌های رمزشکنی کلید رمزنگاری را به‌دست آورد. بسیاری از الگوریتم‌های معروف و شناخته-شده نظیر RSA، DES، AES، El Gamal، Diffie-Hellman و... که در مقابل حملات کلاسیک کاملاً مقاوم هستند به‌راحتی با این گونه حملات موسوم به حملات کانال جانبی شکسته می‌شوند. در واقع توان مصرفی یا تشعشع الکترومغناطیسی یک ابزار رمزنگاری، یک کانال اطلاعاتی جانبی[1] برای دشمن در کنار کانال واقعی عبور داده ایجاد می‌کند که بعضاً ممکن است اطلاعات فوق‌العاده مفیدی را در اختیار وی قرار دهد. بعضی از این حملات در زمان بسیار کوتاه و با هزینه‌ی اندک قادر به شکستن رمز هستند. مثلاً طبق گزارش منابع مربوطه حمله‌ی تحلیل ساده‌ی توان[2] (SPA) در چند ثانیه رمز یک کارت هوشمند را می‌شکند و حمله‌ی تحلیل تفاضلی توان[3] (DPA) ظرف چند ساعت قادر به شکستن رمز یک سیستم پیچیده است. چون این نوع حملات تحقق فیزیکی الگوریتم را هدف قرار می‌دهند و از بی‌دقتی یا ضعف هنگام پیاده‌سازی یک الگوریتم استفاده می‌کنند به آنها حملات پیاده‌سازی[4] یا حملات سخت‌افزاری نیز گفته می‌شود. طراحان و پیاده‌سازان ابزارهای[5] رمزنگاری چنانچه تنها به برآوردن معیارهایی چون سرعت، توان مصرفی یا کاهش ابعاد فیزیکی ابزار رمز بپردازند و از مسأله‌ی محافظت از تراشه در مقابل حملات پیاده‌سازی غافل بمانند دچار خطایی بزرگ و در برخی موارد جبران‌ناپذیر شده‌اند.

[1] Side Channel
[2] Simple Power Analysis Attack
[3] Differential Power Analysis Attack
[4] Implementation Attack
[5] modules

در این پایان‌نامه به پیاده‌سازی نوع خاصی از حملات سخت‌افزاری موسوم به حمله‌ی تحلیل تفاضلی توان (DPA) روی یکی از مهم‌ترین الگوریتم‌های رمزنگاری قالبی کلیدمتقارن معاصر یعنی الگوریتم Rijndael می‌پردازیم. علاوه بر این جهت سهولت در پیاده‌سازی حمله‌ی DPA ابتدا الگوریتم Rijndael را روی بستر FPGA با استفاده از زبان برنامه‌نویسی سخت‌افزار Verilog پیاده‌سازی کرده-ایم. الگوریتم Rijndael یا AES الگوریتمی است که در سال ۲۰۰۰ به دنیا معرفی شد و از سوی NIST، ISO و IEEE به‌عنوان الگوریتم استاندارد رمزنگاری داده مورد پذیرش قرار گرفت. از سال ۲۰۰۰ تاکنون بحث طراحی سخت‌افزاری این الگوریتم و جنبه‌های مختلف آن از جمله مباحث جالب توجه و مهم از سوی صاحب‌نظران رمزنگاری و نیز طراحان VLSI بوده‌است و بحث در این مورد هنوز هم ادامه دارد. افزایش سرعت، کاهش توان مصرفی و حجم تراشه‌های AES و محافظت از آن در مقابل حملات سخت‌افزاری موضوع ده‌ها مقاله، پایان‌نامه‌ی دکتری و گزارش بوده‌است و راه‌کارهای خوبی نیز در این موارد ارائه شده اما هنوز هیچ کدام از طرح‌های ارائه شده نتوانسته تمام ملاک‌های کارآیی که به آنها اشاره شد را به‌طور توأم برآورده سازد و هم‌چنان آن را در معرض حملات سخت-افزاری قرار می‌دهد. در این پایان‌نامه ضمن بررسی اجمالی ساختار ریاضی الگوریتم Rijndael و فلسفه‌ی طراحی آن، گلوگاه‌ها و معماری‌های مناسب برای پیاده‌سازی سخت‌افزاری آن را روی FPGA ارائه داده‌ایم. ضمن تشریح انواع حملات سخت‌افزاری و نحوه‌ی عملکرد آنها به شرح مختصر برخی از این حملات نسبت به پیاده‌سازی Rijndael پرداخته‌ایم. سپس برای آشنایی کامل با حمله‌ی تحلیل تفاضلی توان و توانایی بالای آن در شکستن الگوریتم‌های رمزنگاری یک پیاده‌سازی کاملاً عملی این حمله را روی Rijndael تشریح نموده‌ایم که در آن از دو روش برای پیاده‌سازی حمله و شکستن الگوریتم استفاده شده‌است. روش‌های مذکور مدل‌های آماری هستند که برای انجام تحلیل روی نمونه‌های توان مصرفی یک تراشه‌ی رمزنگاری مورد استفاده قرار می‌گیرند و از خاصیت شباهت نمونه‌ها و اختلاف بین میانگین‌های آنها بهره می‌برند. ایده‌ی حمله‌ی تحلیل توان خیلی ساده است اما پیاده‌سازی آن مشکلات مربوط به خود را دارد. مثلاً در تنظیمات آزمایشگاهی رعایت برخی نکات

خیلی مهم است و در صورتی که رعایت نشوند یک حمله‌ی ناموفق را به همراه خواهد داشت. هم-چنین انتخاب دقیق نمونه‌هایی که بایستی مورد پردازش قرار بگیرند اهمیت زیادی دارد. لازمه‌ی یک پیاده‌سازی موفقیت‌آمیز حمله روی الگوریتم رمزنگاری این است که تمام جزئیات الگوریتم و حمله مورد مطالعه قرار بگیرد و تمامی راه‌کارها و مشکلات پیاده‌سازی بررسی شود از این رو فصل‌بندی و ترتیب مطالب این پایان‌نامه را به‌صورت زیر آرایش داده‌ایم تا خواننده‌ی علاقه‌مند با مطالعه‌ی آن روند کلی این پروژه را بداند و با اطلاعات ترتیبی ارائه شده بتواند کاری مشابه با این پژوهش انجام دهد.

- در فصل دوم الگوریتم AES مورد بررسی قرار می‌گیرد. ضمن معرفی و برشمردن نقاط قوت الگوریتم Rijndael در این فصل و تشریح مبانی ریاضی و ساختار رمزنگاری و رمزگشایی به بررسی اجمالی دلایل انتخاب Rijndael به‌عنوان AES و نیز معرفی سایر نامزدهای AES و مشخصات آنها پرداخته‌ایم. به‌علاوه رمزنگاری بلوکی و حالت‌های مختلف عملکرد آن را نیز تشریح نموده‌ایم.
- فصل سوم معماری VLSI الگوریتم Rijndael را ارائه می‌کند. با توجه به اینکه یکی از اهداف ما در این پایان‌نامه پیاده‌سازی الگوریتم Rijndael روی FPGA است به تشریح مختصر ساختار FPGA، ملاک‌های کارآیی و معماری‌های مناسب برای پیاده‌سازی الگوریتم Rijndael روی آن پرداخته‌ایم و نکاتی که باید هنگام انتخاب یک FPGA برای پیاده‌سازی این الگوریتم مد نظر داشت ذکر کرده‌ایم. سپس گلوگاه‌های پیاده‌سازی Rijndael را شرح داده و نتایج کارهای قبلی در مورد پیاده‌سازی این الگوریتم را ارائه داده‌ایم.
- آن دسته از حملات رمزشکنی موسوم به حملات پیاده‌سازی یا حملات فیزیکی که از نقاط ضعف پیاده‌سازی یک الگوریتم رمزنگاری برای شکستن رمز استفاده می‌کنند در فصل چهارم مورد بررسی قرار گرفته‌اند. در این فصل حملات مختلف به پیاده‌سازی الگوریتم‌هایی نظیر RSA، DES و به‌خصوص Rijndael را بررسی می‌کنیم و روش‌های مقابله با آنها را ارائه می-کنیم.