دانشکده مهندسی برق (پردیس ولنجک)
Faculty of Electrical Engineering

بسمه تعالی

زمان نصب در تابلوی اعلانات:

☐ **دفاع از رساله دکتری** ☐ سمینار عمومي **(Colloquium)**

☑ دفاع از پایان‌نامه کارشناسی‌ارشد ☐ **سمینار تخصصي (Seminar)**

☐ **سمینار تخصصي و مشورتي (Informal Seminar)**

عنوان : **طراحی شتاب‌دهنده‌های سخت‌افزاری الگوریتم‌های رمزنگاری مبتنی بر اسپینترونیک**

سخنران : پگاه ایران‌فر

چکیده: با افزایش تمایل به کوچک‌سازی ابعاد ترانزیستورها، افزایش جریان نشتی به یکی از مهم‌ترین چالش‌های فناوری CMOS تبدیل شده است که امنیت اطلاعات را تحت تاثیر قرار می‌دهد. به کارگیری فناوری نوظهور اسپینترونیک مانند سلول پیوند تونل مغناطیسی (MTJ) دلیل خاصیت غیرفرار بودن و سازگاری با فناوری CMOS راه‌حلی کارامد به منظور کنترل توان مصرفی ایستا و افزایش امنیت داده‌ها است و می‌تواند در ساختارهای منطقی در حافظه (LiM)، معماری‌های پردازش در حافظه (PiM) و یا الگوریتم‌های رمزنگاری استفاده شود. گرچه این مدارها در برابر حملات قوی مانند حملات کانال جانبی به ویژه تجزیه و تحلیل توان تفاضلی (DPA) و تجزیه و تحلیل همبستگی توان (CPA) مستعد نشت اطلاعات خواهند بود. این پایان‌نامه ابتدا به ارائه مدارهای پایه بر اساس مدار تقویت‌کننده حسی پیش‌شارژ (PCSA) و مدارهای ترکیبی MTJ/CMOS با رویکرد تضمین امنیت در برابر حملات DPA و CPA می‌پردازد. با استفاده از نرم‌افزارVirtuoso Cadence نتایج پساچینش استخراج شده و با به کارگیری فناوری ۴۰ نانومتر TSMC و نرم‌افزار HSPICE شبیه‌سازی شده است. مطابق با نتایج شبیه‌سازی پساچینش، الگوی توان مصرفی، شبیه‌سازی موردی مونت‌کارلو بر روی سلول حافظه MRAM و بررسی معیارهای امنیتی نتیجه گرفته می‌شود الگوی مصرف توان در مدارهای با ساختار متقارن در مرحله خواندن حتی در حضور تغییرات فرایند ساخت یکنواخت خواهد بود. بنابراین این دسته مدارها در برابر حملات تجزیه و تحلیل توان به ویژه DPA و CPA مقاوم عمل می‌کنند و گزینه‌ای مناسب به منظور استفاده در کاربردهای امنیتی مانند الگوریتم‌های رمزنگاری هستند. در مقابل، مدارهای با ساختار نامتقارن فاقد الگوی توان مصرفی یکنواخت هستند و در برابر این دست حملات آسیب‌پذیر خواهند بود. در ادامه روشی نوین به منظور پیاده‌سازی شتاب‌دهنده سخت‌افزاری الگوریتم رمزنگاری AES128 با استفاده از نتایج بخش اول پایان‌نامه و با هدف حفظ امنیت کامل در برابر حملات تجزیه و تحلیل توان DPA و CPA ارائه شده است. نتایج شبیه‌سازی به دست آمده بر اساس طراحی‌های پساچینش نشان می‌دهد الگوی مصرف توان هر بخش از الگوریتم رمزنگاری AES128 پیاده‌سازی شده با وجود تغییرات فرایند ساخت یکنواخت خواهد بود. نتایج چندین حمله CPA مرتبه اول و دوم با تعداد ۵۰۰۰۰ نمونه توان ردیابی شده که به منظور بررسی دقیق‌تر استحکام شتاب‌دهنده سخت‌افزاری پیاده‌سازی شده صورت گرفته است نیز با شکست مواجه شده است. بنابراین ساختار پیشنهادی در برابر نشت اطلاعات و حملات تجزیه و تحلیل توان به ویژه DPA و CPA مقاوم خواهد بود و اجازه دسترسی مهاجم به کلید رمزنگاری و دیگر اطلاعات مخفی سلب می‌شود. همچنین نتایج نشان می‌دهد الگوریتم رمزنگاری AES128 پیاده‌سازی شده راندمان مصرف توان ایستا را به میزان ۹۸% نسبت به طرح ASIC بهبود می‌دهد و در مقایسه با طراحی‌های ASIC و FPGA حداکثر فرکانس کاری را به میزان ۷۲% و ۹۱% افزایش می‌دهد. لازم به ذکر است معماری پیشنهادی برای اجرای هر نسخه از AES (AES192 و AES256) و دیگر الگوریتم‌های رمزنگاری مبتنی بر جایگزینی قابل استفاده است.

زمان برگزاری: یکشنبه ۱۴۰۳/۰۶/۱۱ ساعت ۱۳:۳۰

مکان برگزاری: کلاس ۲۰۰ دانشکده برق