پیاده‌سازی حمله الکترومغناطیس بر روی سیستم رمزنگاری AES با ساخت پروبی بهینه و با حساسیت بالا

فرهاد تقیان[۱]، رضا حق مرام[۲]، یعقوب قانع[۳]

۱- دانشجوی کارشناس ارشد الکترونیک دانشگاه جامع امام حسین (ع)، *farhadtaghian@ihu.ac.ir*

۲- استادیار دانشگاه جامع امام حسین (ع)، *rhaghmrm@ihu.ac.ir*

۳- مربی دانشگاه جامع امام حسین (ع)، *yqane@ihu.ac.ir*

چکیده

تحلیل الکترومغناطیس یک تکنیک حمله‌ی کانال جانبی است که می‌تواند اطلاعات محرمانه‌ی قطعات رمزنگاری را با استفاده تشعشعات تابشی الکترومغناطیس ایجاد شده بر روی سطح این قطعات استخراج نماید. حمله الکترومغناطیس زمانی جذاب می‌شود که نشت قطعات داخل تراشه فیلتر شده باشد یا بسیار ضعیف باشد یا نویز به سیگنال توان اضافه شود. در دیگر موارد، معمولاً تحلیل الکترومغناطیس تلاش کمتری برای شکستن یک محصول محافظت نشده نیاز دارد. در این مقاله پروب الکترومغناطیسی بهینه برای اندازه‌گیری مؤثر و با کمترین نویز ممکن تشعشعات ساطع شده از سطح تراشه‌ی رمزنگار در بستر سخت افزار موجود، معرفی شده است. به منظور بررسی عملکرد پروب معرفی شده‌ی بهینه، حمله‌ی الکترومغناطیسی بر علیه الگوریتم رمزنگاری AES بر روی مدار رمزکننده و پیاده‌ساز این الگوریتم محقق شد. نتایج این حمله صحت عملکرد، افزایش حساسیت و بهینه‌شدن پروب را نشان می‌دهدکه در نتیجه موجب افزایش دقت و کاهش سرعت در این حمله‌ها می‌شود.

واژگان کلیدی: پروب الکترومغناطیس، بهینه‌سازی پروب الکترومغناطیسی، حمله الکترومغناطیس، حملات کانال جانبی، رمزگشای

۱- مقدمه

همواره هدف تمام حمله‌ها به ابزارهای رمزنگاری آشکارسازی کلید خصوصی ابزارهای رمزنگاری است. بااین‌حال، تکنیک‌های گوناگونی برای دست‌یابی به این هدف استفاده می‌شوند. حمله‌ها به ابزارهای رمزنگاری برحسب هزینه، زمان، تجهیزات و تخصص مورد نیاز، با یکدیگر متفاوت‌اند[۱] . از متداول‌ترین حملات امروزی می‌توان به حملات غیرتهاجمی اشاره نمود که توجه زیادی را در سال‌های اخیر به خود معطوف کرده است. این حملات به حملات کانال جانبی متداول گشته‌اند. سه نوع از مهم‌ترین انواع کانال جانبی عبارت‌اند از حملات زمانی، حملات تحلیل توان و حملات الکترومغناطیسی. ایده اصلی این حملات مبتنی بر تعیین کلید ابزار رمزنگاری با اندازه‌گیری زمان اجرایی آن، توان مصرفی و میدان‌های مغناطیسی آن است.

تجزیه و تحلیل الکترومغناطیس یک تکنیک است که می‌تواند مورد استفاده برای تست نشت اطلاعات محرمانه از طریق تابش قطعات رمزنگاری باشد. اولین مقالات منتشر در این زمینه توسط کویز کواتر[۱] و سامید[۲] [۲] و تیم جیم پلاس[۳] [۳] است. کواتر و سامید نشان دادند که اندازه‌گیری تشعشعات الکترومغناطیسی از کارت هوشمند ممکن است. کواتر همچنین روش‌های حمله الکترومغناطیس ساده[۴] (SEMA) و حمله الکترومغناطیس تفاضلی[۱] (DEMA)، را معرفی کرده است. مدارات دیجیتال هنگام

1 Quisquater
2 Samyde
3 Gemplus Team
4 Simple ElectroMagnetic Analysis