به نام خدا

کارگاه آموزشی سمپوزیوم بین‌المللی RTEST 2018

عنوان کارگاه: تحلیل توان الگوریتم AES (حملات، راه‌کارهای مقابله و معیارهای ارزیابی به همراه تجربه عملی)

Power Analysis of AES (Attacks, Countermeasures and Evaluation Metrics Accompanied by a Practical Demonstration)

ارائه دهنده‌گان: سیاوش بیات‌سرمدی (استادیار دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف)

سید محمد حسین فرزام

خلاصه کارگاه آموزشی:

امنیت سامانه‌های رمزنگاری همواره یکی از مباحث مورد توجه فعالان حوزه‌ی امنیت بوده است. منشأ آسیب‌پذیری‌ها، در اکثر موارد، نه در مباحث نظری بلکه در پیاده‌سازی الگوریتم‌ها بوده است. یکی از قدرتمندترین و در عین حال کم‌هزینه‌ترین حملات انجام‌شده به پیاده‌سازی سامانه‌های رمزنگاری، حملات کانال جانبی[1] هستند که با تحلیل اطلاعات جانبی نشت‌شده از پیاده‌سازی الگوریتم‌های رمزنگاری، قادر به افشای کلیدهای محرمانه رمزنگاری می‌باشند. توان مصرفی و تشعشع الکترومغناطیس از مهمترین اطلاعاتی هستند که اندازه‌گیری آن‌ها در حین انجام عملیات رمزنگاری می‌تواند استخراج کلید رمزنگاری را در پی داشته باشد.

تمرکز این کارگاه بر روش‌هایی است که با تحلیل اطلاعات توان مصرفی به سامانه‌های رمزنگاری حمله می‌کنند. در این راستا و برای برجسته نمودن برتری‌های حملات تحلیل توان[2]، ابتدا مقدمه‌ای بر حملات فیزیکی ارائه شده و سپس به حملات کانال جانبی و تحلیل توان پرداخته می شود. از این میان، جزئیات تحلیل توانی ساده، تفاضلی و همبستگی[3] به طور ویژه بررسی می‌شود. در ادامه مرور روش‌های کارآمدتری همچون حملات الگویی[4]، حمله تحلیل توان تفاضلی بر پایه الگو[5] و حمله ترکیبی تصادم و تحلیل توان[6] نیز در دستور کار قرار دارد. انجام عملی حمله تحلیل توان تفاضلی به یک

[1] Side-Channel Attacks (SCA)
[2] Power analysis attacks
[3] Simple/Differential/Correlation Power Analysis (SPA/DPA/CPA)
[4] Template attacks
[5] Template-based DPA
[6] Correlation enhanced power analysis collision attack

پیاده‌سازی از الگوریتم AES بر روی FPGA یکی دیگر از برنامه‌های اصلی کارگاه است. آخرین بخش از کارگاه به بررسی روش‌های مقابله با حملات کانال جانبی اختصاص دارد. در این قسمت ابتدا پیش‌زمینه لازم برای معرفی روش پوشش‌گذاری[۷] ارائه می‌شود. سپس به بررسی جزئیات این روش و تغییراتی که در معماری AES ایجاد می‌کند پرداخته می‌شود. در کنار این راه‌کار مقابله، به بررسی اجمالی روش‌های مقابله دیگری همچون تصادفی‌سازی زمانی[۸] و منطق‌های Dual-Rail Precharge (DRP) نیز پرداخته می‌شود.

عناوین مطالب پوشش داده شده در کارگاه:

۱) آشنایی حملات فیزیکی
۲) آشنایی حملات کانال جانبی
۳) بررسی جزیی تر حملات توانی ساده، تفاضلی و همبستگی
۴) مرروی بر حملات دیگر توانی
۵) انجام عملی یک حمله برروی AES
۶) بررسی جزیی مقابله‌ی پوشش‌گذاری
۷) بررسی اجمالی برخی مقابله‌های دیگر

برنامه زمانی کارگاه:

موضوع	بازه زمانی	شرح موضوع
موضوع ۱	۹ ~ ۱۰:۱۵	**آشنایی با حملات فیزیکی و کانال جانبی:** تحلیل توان ساده، تفاضلی و همبستگی معرفی معیارهای ارزیابی
استراحت	۱۰:۱۵ ~ ۱۰:۴۵	
موضوع ۲	۱۰:۴۵ ~ ۱۲	**انجام عملی تحلیل توان تفاضلی و معرفی حملات پیشرفته:** ۱. تحلیل تفاضلی با مدل شمارش تغییرات ۲. حملات الگویی ۳. تحلیل تفاضلی بر پایه الگو ۴. حمله ترکیبی تصادم و تحلیل توان
ناهار و نماز	۱۲ ~ ۱۳:۳۰	
موضوع ۳	۱۳:۳۰ ~ ۱۴:۴۵	**مقابله:** پوشش‌گذاری، تصادفی‌سازی زمانی و منطق‌های DRP

[7] Masking
[8] Shuffling