Research Article, 2021, Volume 8, Number 1
http://www.jcomsec.org

Journal of Computing and Security

طراحی کمک پردازنده خم بیضوی موازی بیتی مقاوم در برابر حملات تحلیل توان تفاضلی در فضای GF(2m)

هاشم رضایی [آ]، علیرضا شفیعی نژاد [آ،*]

[آ] گروه مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 26 June 2020
اصلاح: 22 March 2021
پذیرش: 18 April 2021
انتشار آنلاین: 23 May 2021

کلمات کلیدی:
حملات توان تفاضلی، الگوریتم موازی بیتی، پردازنده ECC، الگوریتم مونتگمری تصادفی.

چکیده

رمزنگاری خم بیضوی به دلایل امنیت بالا و مصرف پایین منابع یکی از گسترده‌ترین سیستم‌های رمز عمومی در چند سال اخیر بوده است. از اینرو این سیستم رمز برای کاربردهای اینترنت اشیاء، که نیاز به مصرف پایین منابع دارد، بسیار مناسب است. اما از جنبه امنیت، حملات کانال جنبی غیرتهاجمی مهمترین تهدید در به کارگیری این سیستمهای رمز است. در این مقاله، کمک پردازنده‌ای برای رمز خم بیضوی در فضای باینری طراحی شده است که نسب به حملات تحلیل تفاضلی توان مقاوم است. واحدهای اصلی این کمک پردازنده، ماژول‌های ضرب و تقسیم پیمانه‌ای مونتگمری هستند که با افزودن یک عدد تصادفی در ابتدای هر عملیات انجام تحلیل تفاضلی روی آنها غیرممکن می‌شود. از جنبه کارآیی نیز، ایده‌ی اصلی این مقاله باز کردن حلقه‌های ماژولهای ضرب و جمع با هدف افزایش سرعت آنها است به عبارت دیگر، طراحی موازی بیتی جایگزین طراحی سریال بیتی شده است. نتایج نشان می‌دهد که علیرغم پیچیدگی نسخه‌های چندبیتی که باعث بالا رفتن محدودی در مساحت تراشه مصرفی نشان می‌دهد، سرعت محاسبات نهایی ضرب نقطه‌ای افزایش قابل ملاحظه‌ای دارد. علاوه بر این، طراحی پیشنهادی کاملاً انعطاف‌پذیر است به گونه‌ای که ماژول اصلی بر اساس بده‌ـبستان سرعت‌ـمساحت می‌تواند با نسخه‌های مختلف چندبیتی واحدهای ضرب و جمع پیمانه‌ای پیکربندی شود. نتایج پیاده‌سازی FPGA نشان می‌دهد که پیکربندی تقسیم‌کننده‌ی دوبیتی‌ـضرب کننده‌ی سه بیتی بر اساس معیار Slice × Time بهبودی نزدیک به ۴۰% را نسبت به روشهای قبلی نشان می‌دهد. همچنین با تکرار ماژول‌های ضرب و جمع، بهبود بر اساس این معیار به ۵۰% می‌رسد. از جنبه سرعت نیز (بدون در نظر گرفتن اسلایس مصرفی) افزایشی در محدوده ۸۷.۱ تا ۲۹.۳ برابر ایجاد می‌شود. همچنین، پیاده‌سازی ASIC با به کارگیری ضرب‌کننده‌ی دوبتی نشان از بهبودی ۱۹% بر اساس معیار Area × Time نسبت به روشهای قبلی دارد. با قابلیت تکرار ماژولهای ضرب و جمع می‌توان این میزان را به ۳۶% رسانید.

* نویسنده مسئول.
آدرس‌های رایانامه: h.rezaei@modares.ac.ir (ه. رضایی)،
shafieinejad@modares.ac.ir (ع. شفیعی نژاد)

ISSN: 2322-4460