عنوان مقاله:

پیاده سازی سخت افزاری پر سرعت ضرب نقطه ای بر روی خم های باینری ادواردز و هشیان کلی شده

محل انتشار:

فصلنامه مهندسی برق و الکترونیک ایران, دوره 21, شماره 1 (سال: 1402)

تعداد صفحات اصل مقاله: 15

نویسندگان:

بهرام رشیدی – Ayatollah Boroujerdi university

محمد عابدینی – Ayatollah Boroujerdi university

خلاصه مقاله:

در این مقاله پیاده‌سازی ساختارهایی پر سرعت برای محاسبه ضرب نقطه‌ای برای خم‌های بیضوی باینری ادواردز و هشیان کلی‌شده بر اساس الگوریتم نردبان منتگومری ارائه شده است. در ساختار پیشنهادی برای کاهش تعداد سیکل ساعت، ضرب‌کننده‌های میدانی برای انجام محاسبات جمع دو نقطه و دو برابر کردن یک نقطه به صورت موازی استفاده شده‌اند. ضرب‌کننده ی میدانی استفاده شده با پایه نرمال گوسی می‌باشد، که به صورت خط لوله ای و دارای ساختار رقمی–سریال در پایه نرمال گوسی است. این ضرب‌کننده دارای ساختاری منظم با مسیر بحرانی کم و سخت‌افزار مصرفی مناسب می‌باشد. در ساختار ارائه شده عمل ضرب نقطه ای برای خم‌های بیضوی باینری ادواردز در دو حالت کلی و خاص آن به ترتیب از چهار و سه ضرب‌کننده ی میدانی استفاده شده است. همچنین از سه ضرب‌کننده‌ی میدانی برای خم باینری هشیان کلی‌شده استفاده شده است. ضرب‌کننده‌ها در طول محاسبات برای کاهش تعداد سیکل ساعت، زمان‌بندی و به اشتراک گذاشته شده‌اند. نتایج پیاده سازی معماری های پیشنهادی بر روی FPGA Virtex-۵ XC۵VLX۱۱۰ نشان می دهد که زمان اجرای ضرب نقطه برای خم‌های بیضوی باینری ادواردز و هشیان کلی‌شده بر روی میدان های متناهی GF(۲۱۶۳) و GF(۲۲۳۳) به ترتیب ۸.۶۲ μs و ۱۱.۰۳ μs است. نتایج نشان می دهد که ساختارهای پیشنهادی، در مقایسه با ساختارهای قبلی، از نظر پارامترهای مانند تاخیر و بازدهی بهبود یافته اند.

کلمات کلیدی:

Elliptic Curve Cryptosystems, Point multiplication, Finite Fields, Gaussian normal basis, Binary Edwards curves, generalized Hessian curves, FPGA,
سیستم رمزنگاری خم بیضوی, ضرب نقطه ای, ضرب کننده در پایه نرمال گوسی, رقمی–سریال, خم های بیضوی باینری ادواردز, خم های باینری هشیان کلی شده.

لینک ثابت مقاله در پایگاه سیویلیکا: