## عنوان مقاله:
ارائه یک ضرب میدانی ضربانی سریع مناسب خم ادواردز ۲۵۵۱۹ پیچ خورده

## محل انتشار:
هجدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1400)

تعداد صفحات اصل مقاله: 6

## نویسندگان:
محمدرسول آوندی - *کارشناسی مهندسی کامپیوتر، دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران*

راضیه سالاری فرد - *استادیار، دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران*

## خلاصه مقاله:
رمزنگاری خم بیضوی در مقایسه با سایر رمزنگاری های نامتقارن، با طول کلید کوتاه تر امنیت یکسانی ایجاد می کند. بنابراین بسیارمورد توجه و در بسیاری از سرویس ها مورد استفاده قرار گرفته است. یکی از خم های امن که به تازگی مورد توجه قرار گرفته، خمادواردز ۲۵۵۱۹ پیچ خورده است که توسط NIST استاندارد شده است. پر هزینه ترین عملیات در رمز نگاری خم بیضوی ضربنقطه ای است، که خود این عملیات از ضرب پیمانه ای استفاده می کند. بنابراین اگر بتوان ضرب پیمانه ای سریعی ارائه داد، سرعتضرب نقطه ای به شکل چشم گیری افزایش پیدا خواهد کرد. در این مقاله به کمک الگوریتم ضرب کاراتسوبا و با هدف بهبود ضربنقطه ای روی خم ادواردز ۲۵۵۱۹ پیچ خورده، یک معماری ضربانی طراحی و پیاده سازی شده است. ضرب کننده پیشنهادی دارای ۴سطح رجیستر در معماری ضربانی است. این معماری ضمن بهره بردن از مزیت معماری های ضربانی (تاخیر مسیر بارانی کم) تعدادسیکل زمانی کمی دارد. مزیت دیگر این ضرب کننده بهره وری بالای آن به همگام به کارگیری در ضرب نقطه ای روی خم ادوارز۲۵۵۱۹ پیچ خورده است. این ضرب کننده در مقایسه با کارهای پیشین ۲۸ درصد بهبود در سرعت داشته است. همچنین ضربنقطه ای حاصل از به کارگیری آن نیز ۵۵ درصد بهبود سرعت نسبت به کارهای پیشین دارد.

## کلمات کلیدی:
رمزنگاری خم بیضوی، خم ادوارد ۲۵۵۱۹ پیچ خورده، ضرب نقطه ای، ضرب پیمانه ای، الگوریتم ضرب کاراتسوبا، معماری ضربانی

## لینک ثابت مقاله در پایگاه سیویلیکا: