عنوان مقاله:
روند پیاده سازی ضرب پیمانه ای مونتگومری

محل انتشار:
همایش ملی علوم و مهندسی کامپیوتر (سال: 1391)

تعداد صفحات اصل مقاله: 10

نویسندگان:
مهناز رفیعی - *دانشگاه آزاد اسلامی واحد اهواز، باشگاه پژوهشگران جوان، اهواز، ایران*

مجتبی علیپور حسکویی - *گروه مهندسی فناوری اطلاعات، دانشگاه پیام نور، دستجرد قم*

سیدمجتبی قریشی امیری - *گروه مهندسی فناوری اطلاعات، دانشگاه پیام نور، دستجرد قم*

محمد جعفرآباد - *دانشجوی دکتری، گروه مهندسی کامپیوتر، دانشگاه مدیترانه شرقی، قبرس شمالی*

خلاصه مقاله:
در این مقاله ویژگی های ضرب کننده های سیستولیک مانند هزینه کم، سرعت بالا، بیت های سریال ورودی و سریال خروجی که مبتنی بر ا لگوریتم مونتگومری می باشد، مورد بحث قرار می گیرند. از آنجائیکه هسته محاسباتی در سیستم های رمزنگاری RSA، عملیات ضرب و به طور خاص ضرب پیمانه ای است، با بررسی روش های اجرای الگوریتم مونتگومری و نحوه پیاده سازی آن با ضرب کننده های سیستولیک، می توان سرعت محاسبات ضرب پیمانه ای را بهبود بخشید. در اینجا ساختار عنصر پردازشی جدیدی برای اجرای موثر الگوریتم مونتگومری به طور مؤثری تأخیر مسیر را کاهش می دهد و در نتیجه میزان سرعت افزایش می یابد. الگوریتم اصلاح شده در این مقاله، ضرب پیمانه ای مونتگومری را به میزان 1.3 برابر سریعتر از قبل اجرا می کند.

کلمات کلیدی:
سیستم رمزنگاری RSA، ضرب پیمانه ای، الگوریتم مونتگومری، معماری سیستولیک، رمزنگاری کلید عمومی