عنوان مقاله:
پیاده سازی نرم افزاری کارآمد سیستم رمزنگاری خم بیضوی در میدان های اولیه و باینری

محل انتشار:
سومین کنفرانس ملی و اولین کنفرانس بین المللی پژوهش هایی کاربردی در مهندسی برق، مکانیک و مکاترونیک (سال: 1394)

تعداد صفحات اصل مقاله: 10

نویسنده:
فیض اله کاویانی - *کارشناس ارشد مخابرات (گرایش رمز)*

خلاصه مقاله:
سیستم رمزنگاری خم بیضوی (ECC) یک سیستم رمزنگاری کلید عمومی می باشد که اندازه کلید عمومی آن کوچکتر از دیگر سیستم های کلید عمومی شناخته شده نظیر RSA در سطح امنیتی معادل است. کوتاه بودن طول کلید در رمز نگاری خم بیضوی باعث تسریع در محاسبات شده و حافظه مورد نیاز را کاهش می دهد و همچنین استفاده بهینه و کارآمد از پهنای باند را فراهم می سازد. پیاده سازی رمزنگاری خم بیضوی شامل بسیاری از عملیات های ریاضی می باشد که یکی از آنها عملیات ضرب نقطه ای خم بیضوی می باشد که نفوذ زیادی در پروتکل های رمزنگاری خم بیضوی دارد. در این مقاله ما روشهای ضرب نقطه ای خم بیضوی که توسط محققان پیشنهاد شده را مورد مطالعه قرار داده و پیاده سازی نرم افزاری این روش ها را درزبان برنامه نویسی C در یک رایانه CORE i 5 با استفاده از پیشنهاد NIST بر روی میدان های اولیه و باینری اجرا نموده ایم و پس از آن پیاده سازی الگوریتم های ضرب نقطه ای خم بیضوی را در الگوریتم امضای دیجیتال خم بیضوی (ECDSA) انجام داده و روش های مختلف را قیاس و در نهایت نتایج بدست آمده را با مطالعات اخیر مقایسه نموده ایم.

کلمات کلیدی:
رمزنگاری خم بیضوی، ضرب نقطه ای خم بیضوی، امضای دیجیتال خم بیضوی