عنوان مقاله:

بررسی و مقایسه پیاده سازی دو الگوریتم رمزنگاری امضای دیجیتال lattice base بر روی CPU

محل انتشار:

چهارمین کنفرانس بین المللی مطالعات نوین در علوم کامپیوتر و فناوری اطلاعات (سال: 1396)

تعداد صفحات اصل مقاله: 11

نویسندگان:

طوبی ملایی جواران - *دانشجوی کارشناسی ارشد شبکه کامپیوتری دانشگاه آزاد اسلامی واحد کرمان، ایران*

محمد لونی - *کارشناسی ارشد سخت افزار دانشگاه شیراز، ایران*

خلاصه مقاله:

رمزنگاری مبتنی بر لاتیس (Lattice) برای رمزنگاری کوانتومی کاندیدای مناسبی محسوب می شود زیرا امنیت آن برپایه ی بدترین حالت ها در فرض های محاسباتی حتی برای رایانه های کوانتومی از پیچیدگی زمانی مناسبی برخورداراست. هدف این تحقیق پیاده سازی دو الگوریتم Ring-LWE و BLISS به منظور بررسی عملکرد و بهره وری در استفاده از الگوریتم های رمزنگاری امضای دیجیتال مبتنی بر لاتیس است. دراین پیاده سازی امضا برای سطوح امنیتی 128، 160 و 192 بیت صبورت می گیرد در این تحقیق پیاده سازی بر روی پردازنده ی چهار هسته- Intel Core i7-4771 صورم گرفته است. در نهایت پس از اجرا و مقایسه نتایج بدست آمده به طور متوسط الگوریتم Ring-LWE نسبت به الگوریتم BLISS در سطوح امنیتی متوسط و بالا عملکرد بهینه تری را نشان می دهد.

کلمات کلیدی:

رمز نگاری مبتنی بر لاتیس، اماای دیجیتال، BLISS, Ring-LWE

لینک ثابت مقاله در پایگاه سیویلیکا: