

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

طوبی ملایی جواران^۱، محمد لونی^۲

۱- دانشجوی کارشناسی ارشد شبکه کامپیوتری دانشگاه آزاد اسلامی واحد کرمان، ایران

۲- کارشناسی ارشد سخت افزار دانشگاه شیراز، ایران

چکیده

رمزنگاری مبتنی بر لاتیس (Lattice) برای رمزنگاری کوانتومی کاندیدای مناسبی محسوب می شود زیرا امنیت آن بر پایه ی بدترین حالت ها در فرض های محاسباتی حتی برای رایانه های کوانتومی از پیچیدگی زمانی مناسبی برخوردار است. 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. در این پیاده سازی امضا برای سطوح امنیتی ۱۲۸، ۱۶۰ و ۱۹۲ بیت صورت می گیرد. در این تحقیق پیاده سازی بر روی پردازنده ی چهار هسته Intel Core i7-4771 صورت 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: رمزنگاری مبتنی بر لاتیس، امضای دیجیتال، Ring-LWE، BLISS.