عنوان مقاله:
پیاده سازی سخت افزاری و نرم افزاری الگوریتم رمز سبک وزن SKINNY بر رویمیکروکنترلر FPGA و ASIC

محل انتشار:
کنفرانس بین المللی پژوهش ها و فناوری های نوین در مهندسی برق (سال: 1401)

تعداد صفحات اصل مقاله: 7

نویسندگان:
حسین حسین پور - *کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی برق و کامپیوتر*

محمدامین امیری - *استادیار، دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی برق و کامپیوتر*

خلاصه مقاله:
الگوریتم های رمزنگاری سبک وزن به دلیل استفاده در کاربردهای با محدویت منابع سخت افزاری بیش از پیش مورد توجه و توسعه قرار گرفته.اند محققان این حوزه در طراحی تلاش میکنند عملکرد این الگوریتمها در یک بستر پیاده سازی علاوه بر تضمینهای امنیتی قوی در رابطه با حملات بهترین کارایی را داشته باشند. یکی از الگوریتمهایی که با این رویکرد طراحی و ارائه شده است الگوریتم رمزنگاری سبک وزن SKINNY میباشد در این تحقیق برای بررسی کارآمدی این الگوریتم در بستر سخت افزاری و نرم افزاری نسخه SKINNY۶۴-۶۴ آن را بر روی بسترنرم افزاری میکروکنترلر ۸ ،بیتی بستر سخت افزری FPGA و ASIC پیاده سازی ، و میزان سطح مصرفی و توان عملیاتی آن محاسبه شده است با استفاده از نتایج بدست آمده در این پیاده سازی میتوان برای استفاده از این الگوریتم در سامانه هایی که با محدودیت منابع مصرفی و توان پردازشی مواجه هستند تصمیم گیری شود.

کلمات کلیدی:
الگوریتم رمز سبک وزن، بستر پیاده سازی ،منابع سخت افزاری، میکروکنترلر، FPGA، ASIC

لینک ثابت مقاله در پایگاه سیویلیکا: