عنوان مقاله:
پیاده سازی سخت افزاری و نرم افزاری الگوریتم های رمز سبک وزن SIMON و SPECK بر روی میکروکنترلر، FPGA و ASIC

محل انتشار:
اولین کنفرانس ملی توسعه پایدار در مهندسی برق و کامپیوتر (سال: 1399)

تعداد صفحات اصل مقاله: 12

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

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

سیدمجتبی دهنوی - *دکتری، دانشگاه خوارزمی، دانشکده علوم ریاضی و کامپیوتر*

خلاصه مقاله:
در سال ۲۰۱۳ آژانس امنیت ملی آمریکا دو خانواده از رمزهای قالبی سبک وزن را منتشر کرد که این دو خانواده simon و speck نامگذاری شدند. با توجه به اینکه، اکثر رمزهای قالبی سبک وزن برای اجرا روی یکی از زمینه های سخت افزاری یا نرم افزاری طراحی شده اند، ولی این دو رمز،علاوه بر امنیت بالا و مقاومت در برابر روش های حمل شناخته شده، عملکرد بهینه ای را در زمینه سخت افزار و زمینه نرم افزار از خود نشان داده اند که برای تمام کاربردهای سبک قابل استفاده می باشد. دراین تحقیق، الگوریتم های رمز simon۳۲ و speck۳۲ بر روی بستر نرم افزاری میکروکنترلر ۸ بیتی، بسترسخت افزری FPGA و ASIC پیادهسازی ، ومیزان سطح مصرفی و توان عملیاتی آنها محاسبه شده است. با استفاده از نتایج بدست آمده در این پیاده سازی، می توان برای استفاده از این الگوریتم ها در سامانه هایی که با محدودیت منابع مصرفی و توان پردازشی مواجه هستند تصمیم گیری شود.

کلمات کلیدی:
الگوریتم رمز سبک وزن، میکروکنترلر، FPGA، ASIC، پیاده سازی

لینک ثابت مقاله در پایگاه سیویلیکا: