چکیده:

توابع هاشِ نهفتهٔ امن اجزای اصلی بسیاری از برنامه ها از جمله سیستم های احراز هویت یا طرح های امضای دیجیتال هستند. بسیاری از این برنامه ها در بازارهای حساس به هزینه استفاده می شوند و بنابراین پیاده سازی چنین اجزائی با بودجه کم بسیار مهم می باشند.

را بعنوان تابع هاشي كه بايد Keccak پس از رقابت طولاني مدتِ ٥ ساله الگوريتم (NIST) در سال ٢٠١٢، موسسه ملي فناوري براي پلت فرم هاي سخت Keccak استاندارد شود، انتخاب كرد. در طي و پس از اين رقابت، اجراهاي مختلفي از SHA-3 بصورت افزاري پيشنهاد و ارزيابي شده اند. هرچند، نتايج بسيار كمي براي اجراهاي غيراستاندارد منتشر شدند.

ارائه شده است در این پژوهش ابتدا به workshop تا به امروز عملیاتی نشده و فقط در حد چند SHA-3 از آنجایی که الگوریتم به بررسی این الگوریتم Matlab بررسی این الگوریتم و چگونگی کار این الگوریتم پرداخته میشود، سپس با استفاده از نرم افزار برنامه مورد Verilog به صورت سخت افزاری توسط زبان Quartus پرداخته میشود. بعد از بررسی نرم افزاری توسط برنامه ارائه شده Keccak پیاده سازی شده و نتایج با مقدار واقعی که توسط EP2C20F484C7N بررسی قرار گرفته و در انتها بر روی برد مقایسه شده است.

کلمات کلیدی: Keecak الگوریتم ، SHA-3 پیاده سازی، بررسی سخت افزاری، بررسی نرم افزاری ،