پیاده سازی و شبیه سازی الگوریتم در هم ساز 3-SHA بر روی FPGA

یعقوب میرچی *,دکتر سیاوش امین نژاد,

1395-10-19

چکیده: توابع هاش نهفتۀ 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. در سال 2012، موسسه ملي فناوري (NIST) پس از رقابت طولاني مدتِ 5 ساله الگوريتم Keccak را بعنوان تابع هاشي كه بايد بصورت 3-SHA استاندارد شود، انتخاب كرد. در طي و پس از اين رقابت، اجراهاي مختلفي از براي كمي بسيار نتايج ،هرچند .اند شده ارزيابي و پيشنهاد افزاري سخت هاي فرم پلت براي Keccak اجراهاي غيراستاندارد منتشر شدند. از آنجایی که الگوریتم 3-SHA تا به امروز عملیاتی نشده و فقط در حد چند workshop ارائه شده است در این پژوهش ابتدا به بررسی این الگوریتم و چگونگی کار این الگوریتم پرداخته میشود، سپس با استفاده از نرم افزار Matlab به بررسی این الگوریتم پرداخته میشود. بعد از بررسی نرم افزاری توسط برنامه Quartus به صورت سخت افزاری توسط زبان و شده سازی پیاده EP2C20F484C7N برد روی بر انتها در و گرفته قرار بررسی مورد برنامه Verilog نتایج با مقدار واقعی که توسط Keccak ارائه شده مقایسه شده است.

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