عنوان مقاله:
پیاده سازی کم حجم تابع چکیده ساز KECCAK بر روی FPGA با استفاده از بهینه سازی FSM

محل انتشار:
اولین همایش ملی فناوریهای نوین در صنایع برق و رباتیک (سال: 1392)

تعداد صفحات اصل مقاله: 9

نویسندگان:
نصور باقری - *دانشگاه تربیت دبیر شهید رجایی، دانشکده برق*

حسین بوذرجمهری - *دانشگاه تربیت دبیر شهید رجایی، دانشکده برق*

خلاصه مقاله:
برای فشردهسازی و خلاصه نمودن یک پیام میتوان از توابع چکیده ساز استفاده کرد. این توابع در کاربردهای رمزنگاری مانند امضای دیجیتال، بررسی سندیت و اعتبار پیامهای رمز شده، امنیت پروتکلهای اینترنتی و غیره به طور گسترده استفاده میشوند. تابع چکیده ساز KECCAK برنده توابع SHA-3 است که ساختار این تابع اسفنجی است. در این مقاله حجم فضای مصرفی تابع KECCAK را با بهینه سازی FSM در قسمت کاهش میدهیم. ما از ساختار همپردازنده برای پیادهسازی استفاده میکنیم که از بلوک RAM های خارجی، که در بسیاری از FPG ها وجود دارد استفاده میکند. همچنین این روشرا به صورت کد VHDL و بر روی FPGA های مختلفپیاده میکنیم و با پیادهسازی اولیه تابع KECCAK از نظر فضای اشغالی مقایسه میکنیم.

کلمات کلیدی:
پیاده سازی کم حجم، هم پردازنده KECCAK، FPGA، VHDL، FSM ،