عنوان مقاله:
طراحی بهینه رمزنگار تکرارکننده های رادیویی میدان نبرد

محل انتشار:
فصلنامه علوم و فنون نظامی, دوره 10, شماره 29 (سال: 1393)

تعداد صفحات اصل مقاله: 20

نویسندگان:
حسن رفیعی یکتا - - *مربی دانشکده مهندسی برق، دانشگاه علوم و فنون فارابی*

جلیل مظلوم - - *استادیار دانشکده مهندسی برق، دانشگاه علوم و فنون هوایی شهید ستاری*

احمد زوار تربتی - - *دانشجوی دکتری مهندسی برق – مخابرات (سیستم) دانشگاه صنعتی مالک اشتر*

خلاصه مقاله:
با گسترش ارتباطات رادیویی، امینت اطلاعات در معرض تهدید قرار گرفت. رمزکننده ها برای کاهش خطرات ناشی از استفاده نادرست از ارتباطات رادیویی بکار گرفته شدند. البته رمزکننده هایی که سابقا در این حوزه مورد استفاده قرار می گرفتند بسیار ضعیف بودند و به راحتی شکسته می شدند. یکی از الگوریتم های رمز که اخیرا در سامانه های ارتباط رادیویی مورد استفاده قرار می گیرد، الگوریتم رمزAES است. البته استفاده از این الگوریتم در ارتباطات رادیویی به تازگی متداول شده است و سابقه طولانی ندارد. در این مقاله روش پیاده سازی معماری تکراری الگوریتم AES مورد بررسی قرار می گیرد و یک روش جدید برای اجرای کدر و دیکدر الگوریتم AES بر روی سخت افزار واحد FPGA پیشنهاد می گردد. برای بررسی نتایج پیاده سازی هر دو روش، از سه نوع سخت افزار مختلف FPGA در دو حالت بهینه شده برای سرعت و حجم استفاده شده است. نتیجه پیاده سازی الگوریتم رمز AESبه روش پیشنهادی، افزایش گذر دهی، صرفه جویی در سخت افزار و انرژی مورد نیاز است.

کلمات کلیدی:
استاندارد رمزنگاری AES, سخت افزار FPGA, گیرنده و فرستنده رادیویی RTX- زبان توصیف سخت افزار VHDL