عنوان مقاله:
مقایسه سرعت نرم افزاری الگوریتم رمزنگاری احرازاصال تشده NORX با AES_GCM

محل انتشار:
کنفرانس ملی فناوری های نوین در مهندسی برق و کامپیوتر (سال: 1396)

تعداد صفحات اصل مقاله: 15

نویسندگان:
سهراب محمودی آلاشتی - *دانشجوی فوق لیسانس برق، دانشگاه آزاد اسلامشهر*

معصود معصومی - *استادیار دانشکده برق، دانشگاه آزاد اسلامشهر*

خلاصه مقاله:
برای برقراری امنیت اطلاعات و ارتباطات، تامین محرمانگی و احراز اصالت پیام دو هدف اصلی میباشد. در گذشته برای محرمانگی و احراز اصالت پیام از دو الگوریتم مجزا استفاده میکردند، که باعث بالا رفتن بار محاسباتی و هزینه می گردد. لذا در سال 2013 موسسه NIST اقدام به برگزاری یک مسابقه به نام سزار، جهت یافتن یک الگوریتم احراز اصالت شده استاندارد برای تامین محرمانگی و احراز اصالت همزمان مبتنی بر امنیت، دسترسپذیری و قدرتمندی نمود. این مسابقه هماکنون در دور سوم آن قرار دارد. در فراخوان مسابقه ذکر شده است که الگوریتم های شرکت کننده باید از الگوریتم AES-GCM که تا قبل از این مسابقه مرجع مورد استفاده برای رمزنگاری و احرازاصالت بود بهتر باشند. در این مقاله به بررسی الگوریتم های رمزنگاری احرازاصالت شده مسابقه سزار پرداخته شده و کارآیی نرم افزاری این الگوریتم ها مورد ارزیابی قرار میگیرد. در نهایت الگوریتم احرازاصالت شده NORX که یکی از الگوریتم های راه یافته به دور سوم مسابقه سزار با AES_GCM در شرایط یکسان پیاده سازی و سرعت آنها با هم مقایسه میشوند. با توجه به نتایج بهدست آمده سرعت الگوریتم NORX تقریبا دو برابر الگوریتم AES_GCM است

کلمات کلیدی:
سزار ، احرازاصالت، دسترس پذیری NORX، AESD_GCM

لینک ثابت مقاله در پایگاه سیویلیکا: