عنوان مقاله:
بهینه سازی الگوریتمAESبا موازی سازی مرحله توسعه کلید

محل انتشار:
اولین همایش تخصصی برق و کامپیوتر (سال: 1393)

تعداد صفحات اصل مقاله: 13

نویسندگان:
زهرا طالع احمد - *دانشگاه صنعتی تحصیلات تکمیلی و فناوری پیشرفته، دانشکده برق و کامپیوتر، کرمان دانشجوی کارشناسی ارشد مهندسی معماری کامپیوتر*

حمیدرضا ناجی - *دانشگاه صنعتی تحصیلات تکمیلی و فناوری پیشرفته، دانشکده برق و کامپیوتر، کرمان استادیار مهندسی کامپیوتر، دانشگاه تحصیلات تکمیلی صنعتی و ف*

خلاصه مقاله:
در دنیای امروز که اطلاعات نقشی اساسی را در زندگی مردم بازی میکنند، محافظت از اطلاعات از موضوعات بسیاربا اهمیت است. با توجه به این مسئله رمزنگاری پیشرفته استاندارد با توجه به توانایی منحصربفردش در حفاظت ازسیستمهای اطلاعاتی مورد توجه بسیاری از سیستمهای امنیتی قرار گرفتهاست. الگوریتم ارائه شده توسط این مقاله با تمرکز بر بهینه سازی مراحل عملیات الگوریتمAESو از بین بردن تاخیر انتظار برای کلید لحظهای، یک الگورتیم فوق سریع ارائه داده است که در مقایسه با الگوریتمهای تولید شده توسط سایر محققان از برتریهای حائز اهمیتی برخوردار است. با استفاده از تکنیک موازی سازی عمل توسعه کلید با سایر مراحل پردازش پیام تلاش شده الگوریتمی ارائه شود که بیشترین میزان استفاده از پردازنده را داشته و تاخیرهای موجود را تا حد امکان کاهش دهد

کلمات کلیدی:
رمزنگاری متقارن، الگورتیم استاندارد رمزنگاری پیشرفته، توسعه کلید، شبکههای سنسوربیسیم

لینک ثابت مقاله در پایگاه سیویلیکا: