عنوان مقاله:
یک رمز قالبی جدید با استفاده از AES چهار دوری و لایه های انتشار بازگشتی

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 4, شماره 2 (سال: 1395)

تعداد صفحات اصل مقاله: 10

نویسندگان:
عبدالرسول میرقدری - *دانشگاه شیراز/دانشگاه جامع امام حسین(ع)*

محمود یوسفی پور - *جامع امام حسین(ع)*

خلاصه مقاله:
امنیت رمز قالبی AES باعث شده است تا بسیاری از طراحان، هنوز هم از مولفه های AES در طراحی های جدید خود استفاده کنند. لایه ها ی انتشار یکی از مولفه های مهم رمزهای قالبی هستند که روی امنیت و کارآیی رمز تاثیر دارند. سجادیه و همکارانش در ۲۰۱۲ FSE یک دسته خاص از لایه های انتشار، تحت عنوان لایه های انتشار بازگشتی را معرفی کردند که در آنها برخی کلمات خروجی به صورت بازگشتی به عنوان ورودی نیز استفاده می شوند. در این مقاله یک روش جدید برای به دست آوردن یک الگوریتم رمز قالبی ۲۵۶ بیتی مبتنی بر ترکیب چهار دور رمز قالبی AES و یک لایه انتشار بازگشتی معرفی شده است. الگوریتم رمز پیشنهادی در مقایسه با رایندال در برابر تحلیل های خطی و تفاضلی مقاوم تر است. هزینه این افزایش مقاومت، کاهش یک درصدی سرعت آن در مقایسه با رایندال است. علاوه بر این، روش پیشنهادی برای طراحی رمزهای قالبی با طول قالب ۳۸۴ و ۵۱۲ بیتی نیز تعمیم داده شده است.

کلمات کلیدی:
رمز قالبی, لایه انتشار بازگشتی, تحلیل تفاضلی و خطی, جعبه جانشانی