عنوان مقاله:
ویژگی های رمزنگاری نگاشت مجذور به هنگ توانی از دو

محل انتشار:
یازدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1393)

تعداد صفحات اصل مقاله: 7

نویسندگان:
محمدرضا میرزایی شمس آباد - *دانشکده ریاضی و علوم کامپیوتر، دانشگاه شهید باهنر، کرمان*

اکبر محمودی ریشکانی - *دانشکده علوم پایه، دانشگاه تربیت دبیر شهید رجایی، تهران*

سیدمجتبی دهنوی - *دانشکده علوم ریاضی و کامپیوتر، دانشگاه خوارزمی، تهران*

حمیدرضا میمنی - *دانشکده علوم پایه، دانشگاه تربیت دبیر شهید رجایی، تهران*

خلاصه مقاله:
نگاشت مجذور، یکی از نگاشت هایی است که در رمزنگاری مورد استفاده قرار می گیرد. به عنوان مثال در سیستم رمزنگاری رابین،رمز قالبی RC6 و رمز دنباله ای Rabbit از نگاشت مجذور به گونه های مختلفی استفاده شده است. در این مقاله، به حالت خاصی از نگاشت مجذور یعنی نگاشت مجذور به هنگ توانی از دو پرداخته ایم. در ابتدا، توزیع احتمال خروجی این نگاشت را به عنوان یک تابعدودویی برداری محاسبه کردهایم. سپس، توزیع احتمال توابع مولفه ای این نگاشت را به دست آورده ایم. در ادامه، توزیع احتمالدوگانه ی توابع مولفه ای نگاشت مزبور را محاسبه نموده ایم. در پایان، نگاشتی مشابه آنچه در رمز دنباله ای Rabbit مورد استفاده قرار گرفته است، ارایه نموده و توزیع احتمال توابع مولفه ای آن را به دست آورده ایم.

کلمات کلیدی:
نگاشت مجذور به هنگ توانی از دو، توابع دودویی برداری، توابع مولفه ای، توابع مولفه ای توام، رمزهای دنباله ای، رمزهای قالبی

لینک ثابت مقاله در پایگاه سیویلیکا: