## عنوان مقاله:
طراحی توابع S-box به کمک روش بهینه سازی PSO

## محل انتشار:
پانزدهمین کنفرانس کامپیوتر سالانه انجمن کامپیوتر ایران (سال: 1388)

تعداد صفحات اصل مقاله: 8

## نویسندگان:
ندا خیری - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر*

بابک صادقیان - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر*

سیدسعید صادقیان - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر*

## خلاصه مقاله:
دراین مقاله روشی جدید برای طراحی S-box های الگوریتم های رمزنگاری با استفاده از روش بهینه سازی PSO مطرح می کنیم به طوریکه S-box های تولید شده در برابر حملات خطی و تفاضلی مقاوم باشند. از انجایی که شایستگی S-box ها براساس معیارهای غیرخطی، خودهمبستگی و بهمنی الزاما سبب تولید S-box مناسب نمی شود. در روش جدید احتمالهای مشخصه تفاضلی و خطی را نیز لحاظ کرده ایم. برای انکه روش بهینه سازی PSO بتواند با کاربردهای رمزنگاری که نحوه ارزیابی در آنها به صورت بیتی است سازگار شود نحوه ی محاسبه سرعت حرکت در روش جدید مطابق با این نیازمندی تغییر کرده است همچنین تکنیک جدیدی برای منظم کردن S-boxها در روش جدید پیشنهاد شده است با استفاده از روش مطرح شده S-box های 4×6 تولید شدند که احتمال مشخصه خطی و تفاضلی، مقادیر غیرخطی و خودهمبستگی و مقدار مربوط به معیار بهمنی ان ها به مراتب بهتراز مقادیر متناظر S-box های الگوریتم رمز DES می باشند و در نتیجه در برابر تحلیلهای خطی و تفاضلی مقاومتر می باشند

## کلمات کلیدی:
روش بهینه سازی PSO، ویژگی غیرخطی، S-box، خودهمبستگی، بهمنی، احتمال مشخصه تفاضلی و خطی