

عنوان مقاله:

طراحی و ساخت ماتریس های سبک وزن MDS شبه خودمعکوس بر اساس ساختارهای بازگشتی و ماتریس های خلوت دودویی

محل انتشار:

فصلنامه علوم و فناوری های پدافند نوین، دوره 10، شماره 4 (سال: 1398)

تعداد صفحات اصل مقاله: 11

نویسندگان:

علی زاغیان - دانشگاه صنعتی مالک اشتر اصفهان

محسن موسوی - دانشگاه صنعتی مالک اشتر اصفهان

خلاصه مقاله:

ماتریس های یکی از مهم ترین اجزای طراحی در رمزهای قالبی است. یکی از ویژگی های اصلی یک ماتریس برای ساختارهای ، سرعت قابل قبول پیاده سازی ماتریس و معکوس آن، از نظر سخت افزاری است. در این مقاله، نوعی جدید از ماتریس های بلوکی دودویی بنام ماتریس های شبه خودمعکوس استفاده شده است که هزینه پیاده سازی این ماتریس ها و معکوس آن ها برابر است. در ابتدا، با به کارگیری توابع خطی دودویی در ماتریس های خلوت دودویی، یک ماتریس 4×4 شبه خودمعکوس پیشنهاد شده است که هزینه پیاده سازی این ماتریس پیشنهادی برای ورودی 8 بیتی، برابر با 68 یک بیتی است. ماتریس 4×4 پیشنهادی و معکوس آن، پیاده سازی مناسبی از نظر سخت افزاری دارند زیرا ساختار این ماتریس ها، بر اساس ساختارهای است. در ادامه، با استفاده از ساختارهای ، یک ماتریس 8×8 شبه خودمعکوس پیشنهاد شده که برای ورودی 8 بیتی، با 320 یک بیتی پیاده سازی شده است. مهم ترین نتیجه این مقاله، پیشنهاد ماتریس 8×8 شبه خودمعکوس با هزینه 320 است زیرا بهترین نتیجه برای ساخت ماتریس 8×8 با استفاده از الگوریتم های ذاتی و برای ورودی 8 بیتی 392 است. همچنین، با استفاده از ماتریس های مناسب دودویی خلوت، ماتریس 4×4 پیشنهاد شده با هزینه برای ورودی بیتی پیاده سازی شده است.

کلمات کلیدی:

ماتریس MDS، رمزنگاری سبک، لایه های انتشار بازگشتی، شمارش XOR، رمز قالبی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1012940>

