

عنوان مقاله:

جستجوی مشخصه های تفاضلی دارای احتمال قابل قبول برای تحلیل تفاضلی در الگوریتم رمز قالبی سایمون به کمک حل کننده های SAT/SMT

محل انتشار:

دهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات (سال: 1399)

تعداد صفحات اصل مقاله: 10

نویسندگان:

منصور مولایی نژاد - دانشگاه صنعتی جندی شاپور دزفول

احمد حلالی - دانشگاه صنعتی جندی شاپور دزفول

محسن شکبیا - دانشگاه صنعتی جندی شاپور دزفول

خلاصه مقاله:

در این مقاله به جستجوی مشخصه های تفاضلی الگوریتم رمز قالبی سایمون با بهره گیری از حل کننده های SAT/SMT پرداخته شده است. به این ترتیب که مسئله ی یافتن مشخصه های تفاضلی برای این رمز، ابتدا به یک مسئله ی ارضاپذیری تبدیل و سپس با استفاده از ابزارها و کتابخانه های مهیا شده، حل می شود. برای اینکار ابتدا به بی ان مسائل SAT/SMT و حل کننده های آنها پرداخته ایم. سپس تحلیل تفاضلی و ارتباط آن با این نوع حل کننده ها تبیین شده است. این مقاله مروری از کار استفان کوبل در زمینه استفاده از حل کننده های SAT/SMT برای جستجوی مشخصه های تفاضلی رمز سایمون است [6]. در بخش 2 الگوریتم رمزنگاری سایمون را مورد بررسی قرار داده ایم؛ سپس یک قضیه پایه برای محاسبه احتمال تفاضل در الگوریتم های شبه- سایمون بیان گردیده است. در مرحله بعد، برای محاسبه احتمال تفاضل رمز سایمون در دوره ای متوالی ارائه شده است. در نهایت با استفاده از حل کننده های SAT/SMT و بازنویسی معادلات برای آن ها بهترین مشخصه های تفاضلی به دست خواهد آمد.

کلمات کلیدی:

الگوریتم رمز سایمون، مشخصه تفاضلی، حل کننده های SAT/SMT

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1041740>

