Journal of Computing and Security

2020, Volume 7, Number 2
http://www.jcomsec.org

یک تحلیل‌رمز جبری مبتنی بر محاسبه‌ی پایه گروبنر با کارایی بیشتر

حسین عرب‌نژاد خانوکی [آ]، بابک صادقیان [آ،*]

[آ] دانشکده مهندسی کامپیوتر و فن‌آوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 24 June 2020
اصلاح: 15 July 2020
پذیرش: 16 August 2020
انتشار آنلاین: 4 October 2020

کلمات کلیدی:
تحلیل‌رمز جبری، پایه گروبنر، پرونینگ عام، بازنمایی S-box

چکیده

در این مقاله ما یک روش جدید برای انجام تحلیل‌رمز جبری کارآمدتر پیشنهاد می‌دهیم. هدف از تحلیل‌رمز جبری یافتن کلید سرّی با استفاده حل یک دستگاه معادلات است که ساختار داخلی یک الگوریتم رمز را توصیف می‌کند. متن‌های واضح منتخب دارای همبستگی، همانند متن‌های واضحی که در تحلیل رمز تفاضلی مرتبه بالاتر و مشتقات آن مانند حمله‌ی مکعبی و تحلیل‌رمز انتگرال، بکار می‌روند، موجب پدید آمدن روابط خطی زیادی در بین بیت‌های حالت‌های میانی در الگوریتم رمز می‌شوند. در این مقاله ما برای ساده‌سازی دستگاه معادلات ناشی از الگوریتم رمز در تحلیل‌رمز جبری، این چندجمله‌ای‌ها را در نظر می‌گیریم، تا در نهایت بتوان با کارایی بیشتری دستگاه معادلات را حل کرد. برای بدست آوردن این چندجمله‌ای‌های خطی به صورت کارا از تکنیک پرونینگ عام استفاده می‌کنیم. پارامتر مهم دیگری که در تحلیل‌رمز جبری موثر است، توصیف جبری کارا از الگوریتم‌های رمز است. ما از روش توصیف *رو_به_جلو _ رو_به_عقب* برای توصیف جبری S-boxها، به همراه تکنیک پرونینگ عام استفاده می‌کنیم، تا یک تحلیل‌رمز جبری مبتنی بر محاسبه‌ی پایه گروبنر با کارایی بیشتر ارایه دهیم. در این مقاله ما نشان می‌دهیم که روش پیشنهادی نسبت به انجام تحلیل‌رمز جبری مبتنی بر بازنمایی MQ به همراه پرونینگ عام از کارایی بیشتری برخوردار است. برای نشان دادن کارایی ، ما از این رویکرد برای تحلیل‌رمز چند الگوریتم رمز قطعه‌ای سبک‌وزن استفاده کردیم. با استفاده از این رویکرد ما تا کنون موفق به انجام حمله جبری به ۱۲ دور از الگوریتم رمز LBlock، ۶ دور از MIBS، ۷ دور از PRESENT و ۹ دور از SKINNY شدیم.

* نویسنده مسئول.
آدرس‌های رایانامه: arabnezhad@aut.ac.ir (ح. عرب‌نژاد)،
basadegh@aut.ac.ir (ب. صادقیان)

ISSN: 2322-4460