2020, Volume 7, Number 1
http://www.jcomsec.org

Journal of Computing and Security

Persian Abstract

تولید S_جعبه‌های پویا با استفاده از نگاشت یک‌بعدی چبیشف

علی شکیبا [آ,*]،

[آ] گروه علوم کامپیوتر، دانشگاه ولی‌عصر(عج) رفسنجان، رفسنجان، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 19 April 2019
اصلاح: 6 January 2020
پذیرش: 4 April 2020
انتشار آنلاین: 30 May 2020

کلمات کلیدی:
جعبه جانشینی، آشوب، چبیشف

چکیده

در این مقاله روشی برای تولید جعبه‌های جانشینی (S_جعبه) پویا با استفاده از چندجمله‌ای‌های آشوبی چبیشف نوع اول ارائه می‌شود. روش ارائه شده در مقایسه با بیست و یک روش اخیر، S_جعبه‌هایی با عملکرد امنیتی قابل قبولی فراهم می‌کند. از الگوریتم ارائه شده برای تولید ۸۰ جعبه‌ی جانشینی از ابعاد ۸۰ × ۸۰ استفاده شده است و عملکرد امنیتی جعبه‌های تولید شده مورد تحلیل قرار گرفته‌اند. به صورت میانگین، عملکرد امنیتی S_جعبه‌های تولیدشده قابل قبول بوده‌اند. معیارهای امنیتی ضروری برای امنیت یک S_جعبه عبارتند از معیار بهمنی اکید (SAC)، احتمال تقریب خطی (LAP)، احتمال تقریب تفاضلی، معیار استقلال بیتی (BIC)، ایمنی از همبستگی، ایمنی جبری، خودهمبستگی و معیار انتشار. همچنین، S_جعبه‌های تولید شده توسط مجموعه‌ای از معیارهای منطق اکثریت نیز برای بررسی مقاومت و کیفیت آن‌ها در رمزگذاری تصاویر مورد بررسی قرار گرفته است. از آنجا که تولید دنباله‌های آشوبی با استفاده از چندجمله‌ای‌های چبیشف نوع اول بسیار ساده‌تر از تولید دنباله‌های آشوبی از نگاشت‌های ابرآشوبی است، الگوریتم ارائه شده نسبت به سایر الگوریتم‌های ارائه شده‌ی اخیر از سرعت و عملکرد بهتری برخوردار است.

* نویسنده مسئول.
آدرس رایانامه:
a.shakiba.iran@gmail.com;ali.shakiba@vru.ac.ir (ع. شکیبا)
 ISSN: 2322-4460