بخشی از ترجمه مقاله

عنوان فارسی مقاله :

رهیافت های سیستم ایمنی برای الگوریتم رمزنگاری

عنوان انگلیسی مقاله :

Immune systems approaches for cryptographic algorithm

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل

با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

6. نتیجه‌گیری‌ها و تحقیقات بعدی

نتایج نشان داده شده در طرح آزمایشیِ سیستم‌های ایمنی را می‌توان با موفقیت برای طراحیِ رمزگذاری‌های بلوکی رقابتی به کار برد. در این راستا، تابع $3D-RotateSlice$ به عنوان مؤلفه‌ی اصلی در 3D-AES را می‌توان به عنوان نمونه‌ای از یک خانواده از طرح‌ها دانست که می‌توان با استفاده از این الگو مورد بررسی قرار داد. شاید مرتبط‌ترین جنبه در این الگو، انتخاب مناسب مفاهیم و الگوریتم‌های AIS می‌باشد. این رمزگذاری بلوکی ایجاد شده به طور موفقیت‌آمیز از آزمون‌های آماری خیلی سخت عبور کرده است. یکی از یافته‌های مهمی که از این مقاله بیرون می‌آید این است که یکی از ارزیابی‌های امنیتِ رمزگذاری بلوکی 3D-AES با رمزگذاری بلوکی AES قابل مقایسه می‌باشد. هر چند این مطلب سطح امنیت معینی را برای رمزگذاری بلوکی 3D-AES تضمین نمی‌کند، اطمینان می‌دهد که هیچگونه نقص بدیهی یا اِشکالی در پیاده‌سازی آن وجود ندارد. تحقیقات بعدی باید تحلیل عمیق‌تر رمزگذاری را شامل شود، مخصوصاً در مقابل حمله‌های اصلی، مانند کشف رمز خطی، تفاضلی (دیفرانسیلی) و مربوط به کلید.

VI. Conclusions And Future Work

The results shown in the experimental design those immune systems can be successfully applied to design competitive block ciphers. In this line, the *3D-RotateSlice* function as the core components in 3D-AES can be thought as an instance of a family of designs that can be explored with this paradigm. Perhaps the most relevant aspect in this scheme is the appropriate selection of the AIS algorithms and concepts. The generated block cipher has successfully passed of very demanding statistical tests. One of the significant findings to emerge from this paper is that the one of the security evaluation of the 3D-AES block cipher is comparable with AES block cipher. Although this does not ensures a certain security level for 3D-AES block cipher, it guarantees that neither trivial weaknesses nor implementation bugs exist. Future work should include deeper analysis of the cipher, particularly against basic attacks, such as linear, differential or related-key cryptanalysis.