ანოტაცია

ნაშრომი წარმოადგენს კრიპტოგრაფიაში არსებული პრობლემის გადაწყვეტის ერთ-ერთ მცდელობას. კერძოდ, ნაკადური შიფრებისთვის კრიპტოგრაფიულად საიმედო გამის დაგენერირება, დაკავშირებულია გარკვეულ პრობლემებთან, რომელიც განხილულია მოცემულ ნაშრომში. ჩვენი ნაშრომი შეეხება ნეირონული ქსელის საშუალებით ისეთი გენერატორის შექმნის მცდელობას რომელიც დაფუძნებულია ცალმხრივ ფუნქციაზე. ცალმხრივ ფუნქციაზე დაფუძნებულ გენერატორებს წარმოადგენენ RSA და BBC გენერატორები, რომლებიც წარმოქმნიან საკმაოდ საიმედო გამას, მაგრამ მათი ნაკლი არის ის, რომ ეს გენერატორები არის ძალიან ნელი. სწორედ ამ პრობლემის გადასაჭრელად გადავწყვიტეთ ნეირონული ქსელის საშუალებით ავაგოთ გენერატორი რომელიც დაფუძნებული იქნება RSA გენერატორზე, რომელიც დააგენერირებს საიმედო გამას და ამავე დროს იქნება RSA გენერატორზე სწრაფი.

Annotation

In the work, “ Construct the pseudo-random number generator using neural networks”, represents one attempt to solve the problems in cryptography. Our work is by means of neural network an attempt to create a generator based on a one-way function. A one-way function based on RSA and BBC generators, these generators that produce extremely reliable gamma, but the drawback is that these generators is very slow. To solve this problem, we decided to build a neural network based on the RSA generator to the generator, which will generate reliable gamma and this generator is a fast than RSA generator.