USING ML FOR GENERATING CRYPTOGRAPHIC FUNCTIONS

A PREPRINT

David S. Hippocampus*
Department of Computer Science
Cranberry-Lemon University
Pittsburgh, PA 15213
hippo@cs.cranberry-lemon.edu

Elias D. Striatum
Department of Electrical Engineering
Mount-Sheikh University
Santa Narimana, Levand
stariate@ee.mount-sheikh.edu

November 18, 2018

ABSTRACT

In this paper we unite machine learning and cryptography: using ML methods trying to solve one of the most important problem in cryptography: to find boolean function with acceptable cryptological properties. Neural network for making pseudorandom function is developed. This function used as round function in Feistel Network, which we finally test on NIST test battery.

***K*eywords** First keyword · Second keyword · More

1 Introduction

Cryptography is widely used in information security. Everyone is using it in messagers, shops, in internet of things and many others aspects of life. Many users encrypt its personal data without even knowing what cryptography is.

There are a lot of basic templates for cryptographic encryption functions called schemes - Feisteil network, SP-network, XSL-scheme etc. Every scheme has adjustable set of parameters such as plaintext and key size, internal round functions, number of rounds. Best practice in constructing new encryption algorithm is to choose a good scheme, then select perfect parameters of chosen scheme. For example, algorithm AES is a XSL-scheme with choosen internal operations, including s-boxes.

Chosing excellent round functions in another part of cryptographic art. When new algorithm is published, researchers of whole world trying to find weakness in it. Besides, absence of attacks doesn't mean that algorithm is strong. Many people, besides, prefer concept of «nothing up my sleeve numbers» **?**, which require generating s-boxes only by random choise. Otherwise one can say that you try to hide specific propeties of your algorithm.

On the other hand, ML methods can be applying as approach to find a good

That's why in this paper we use neuronal network for generating good round function for Feisteil Network - one of the most popular scheme. Then we test properties of our algorithm on the NIST test battery.

*Use footnote for providing further information about author (webpage, alternative address)—*not* for acknowledging funding agencies.