БЕЛАРУСКІ ДЗЯРЖАЎНЫ ЎНІВЕРСІТЭТ

Оценивание надежности криптографических преобразований на основе нейронных сетей

Максим Юрьевич Деркач

Научный руководитель: Юрий Семенович Харин

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Минск, 2020

Содержание

Введение

Обзор литературы

- Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. – 2003. – Минск.
- Mohammed M. Alani.Neuro-Cryptanalysis of DES and Triple-DES. – 2012.
- Kinzel F., Kanter I. Neural Cryptography. – 2002.
- Pattanayak S., Ludwig S.A. Encryption based on Neural Cryptography. – 2017.
- M. Kim, P. Smaragdis, Bitwise Neural Networks. – 2010.

Цель исследования - оценивание надежности криптографических преобразований сети Фейстеля, используя искусственные нейронные сети.

Задачи:

1. Провести аналитический анализ работ по теме нейронные сети в криптографии.
2. Основываясь на задачах исследования, определить архитектуру и параметры нейронной сети.
3. Определить математические модели криптографических примитивов преобразования Фейстеля.
4. Определить математические модель криптографического преобразования Фейстеля.
5. Разработать генератор модельных данных.
6. Построить нейронные сети, аппроксимирующие данную математическую модель. Провести компьютерные эксперименты.
7. Оценить результаты полученные в ходе компьютерных экспериментов.

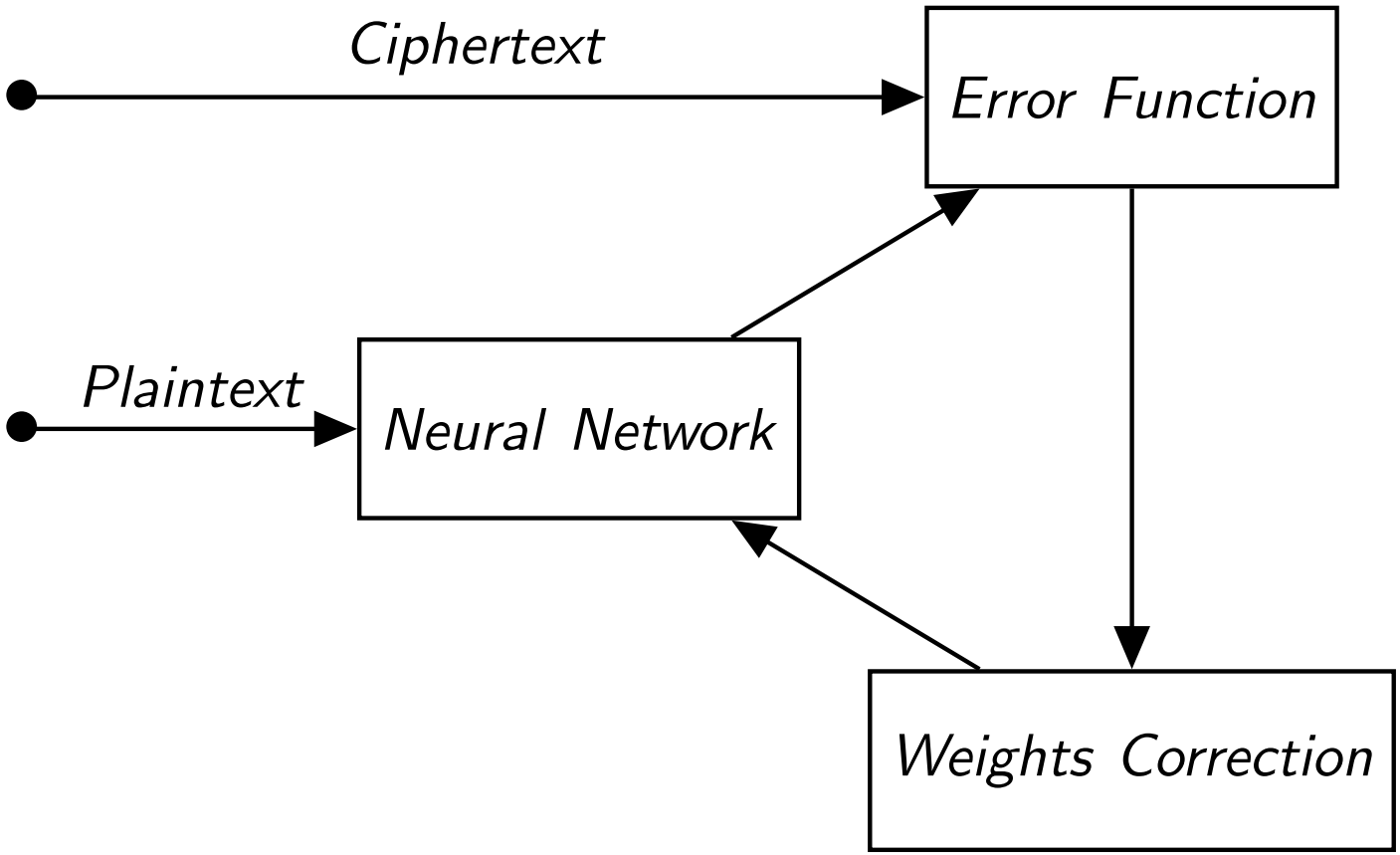


Рис.: Модель криптоанализа на основе нейронной сети

Опишем однотактовое преобразование шифрования ГОСТ 28147-89:

$Y = g(X, K) = g(X_1||X_2, K) \equiv (S[X_1 \boxplus K] \ll 11) \oplus X_2||X_1$, где
$X \in V_{64}$ - вектор входных данных,
$Y \in V_{64}$ - выходные данные,
$K \in V_{32}$ - ключ,
S - стандартный S-блок из ГОСТ-28147.

1. $Y_{g_0} = g_0(x) = g_0(x_1||x_2) \equiv x_1 \oplus x_2$, где
   $x \in V_8$ - вектор входных данных,
   $x_1, x_2 \in V_4$ - левая и правая часть входного вектора,
   $Y_{g_0} \in V_4$ - выходные данные модели g_0;

2. $Y_{g_1} = g_1(x) = g_1(x_1||x_2, k) \equiv S[x_1] \oplus x_2$, где
   $x \in V_8$ - вектор входных данных,
   $x_1, x_2 \in V4$ - левая и правая часть входного вектора,
   $Y_{g_1} \in V_4$ - выходные данные модели g_1,
   S - первый узел из стандартного S-блока из ГОСТ-28147
   $(S = \{13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7\})$;

3. $Y_{g_2} = g_2(x) = g_2(x_1||x_2, k) \equiv S[x_1 \boxplus k] \oplus x_2$, где
$x \in V_8$ - вектор входных данных,
$x_1, x_2 \in V4$ - левая и правая часть входного вектора,
$k \in V_4$ - некоторый неизвестный постоянный в эксперименте ключ,
$Y_{g_2} \in V_4$ - выходные данные модели g_2,
S - первый узел из стандартного S-блока из ГОСТ-28147;
4. $Y_{g_3} = g_3(X) = g_3(x_1||x_2, k) \equiv (S[x_1 \boxplus k] \ll 11) \oplus x_2$, где
$x \in V_{64}$ - вектор входных данных,
$k \in V_{32}$ - некоторый неизвестный постоянный в эксперименте ключ,
$Y_{g_3} \in V_{32}$ - выходные данные модели g_3,
S - стандартный S-блок из ГОСТ-28147;

5. $Y_{g_4} = g_4(x) \equiv x \boxplus K$, где
   $x \in V_4$ - вектор входных данных,
   $k \in V_4$ - некоторый неизвестный постоянный в эксперименте ключ,
   $Y_{g_4} \in V_4$ - выходные данные модели g_4;

6. $Y_{g_8} = g_8(x) \equiv x \boxplus K$, где
   $x \in V_8$ - вектор входных данных,
   $k \in V_8$ - некоторый неизвестный постоянный в эксперименте ключ,
   $Y_{g_8} \in V_8$ - выходные данные модели g_8;

7. $Y_{g_{16}} = g_{16}(x) \equiv x \boxplus K$, где
   $x \in V_{16}$ - вектор входных данных,
   $k \in V_{16}$ - некоторый неизвестный постоянный в эксперименте ключ,
   $Y_{g_{16}} \in V_{16}$ - выходные данные модели g_{16};

8. $Y_{g_{32}} = g_{32}(x) \equiv x \boxplus K$, где
   $x \in V_{32}$ - вектор входных данных,
   $k \in V_{32}$ - некоторый неизвестный постоянный в эксперименте ключ,
   $Y_{g_{32}} \in V_{g_{32}}$ - выходные данные модели g_{32}.

Аппроксимация криптографических примитивов преобразования Фейстеля

Численные результаты

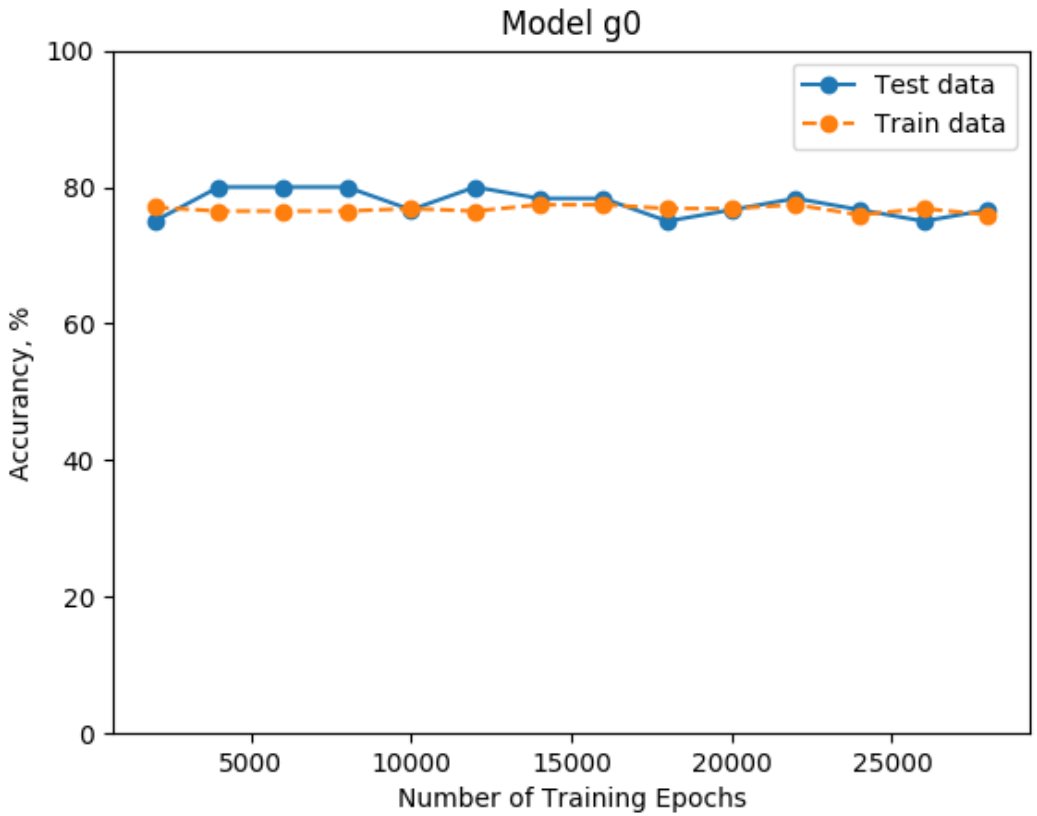
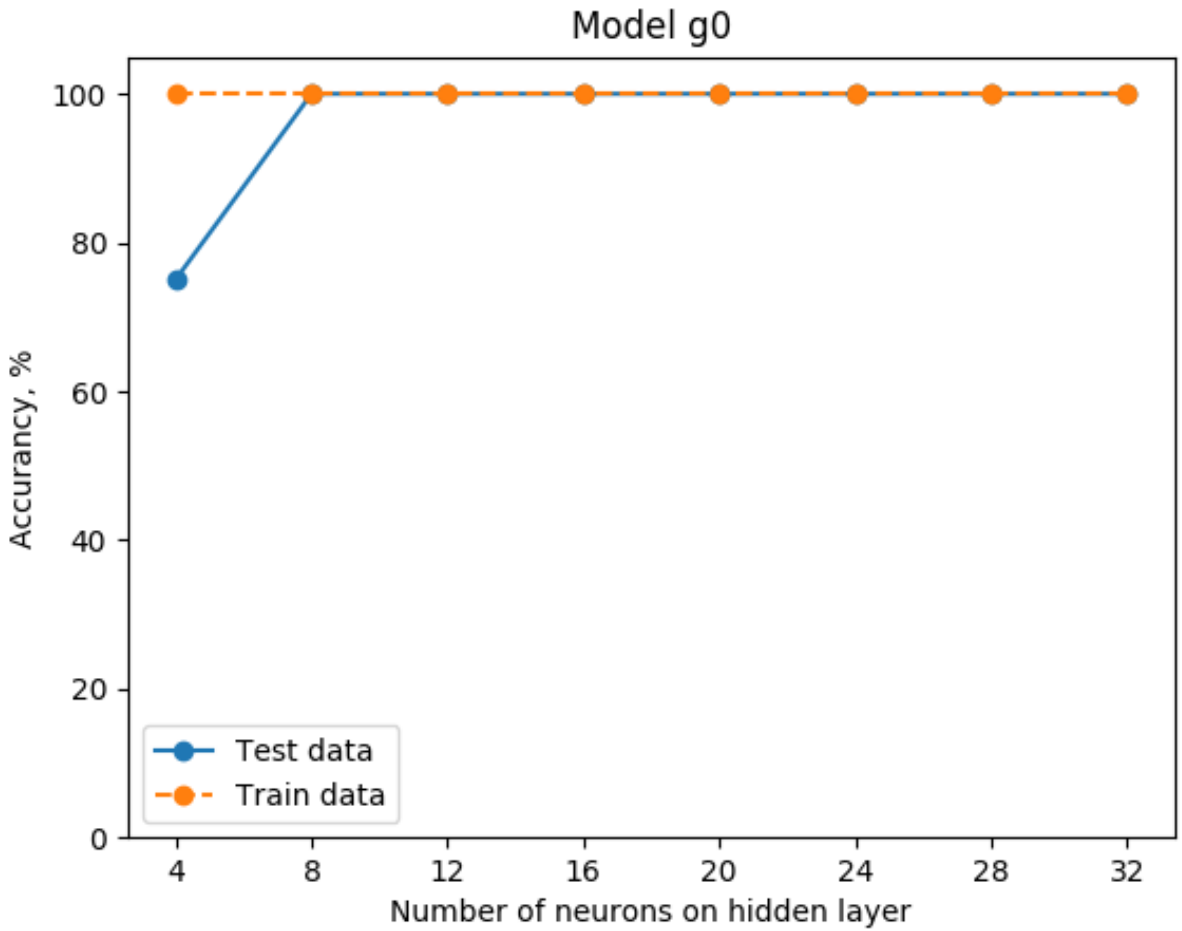


Рис.: График точности построенной однослойной нейронной сети модели g_0 от количества итераций обучения

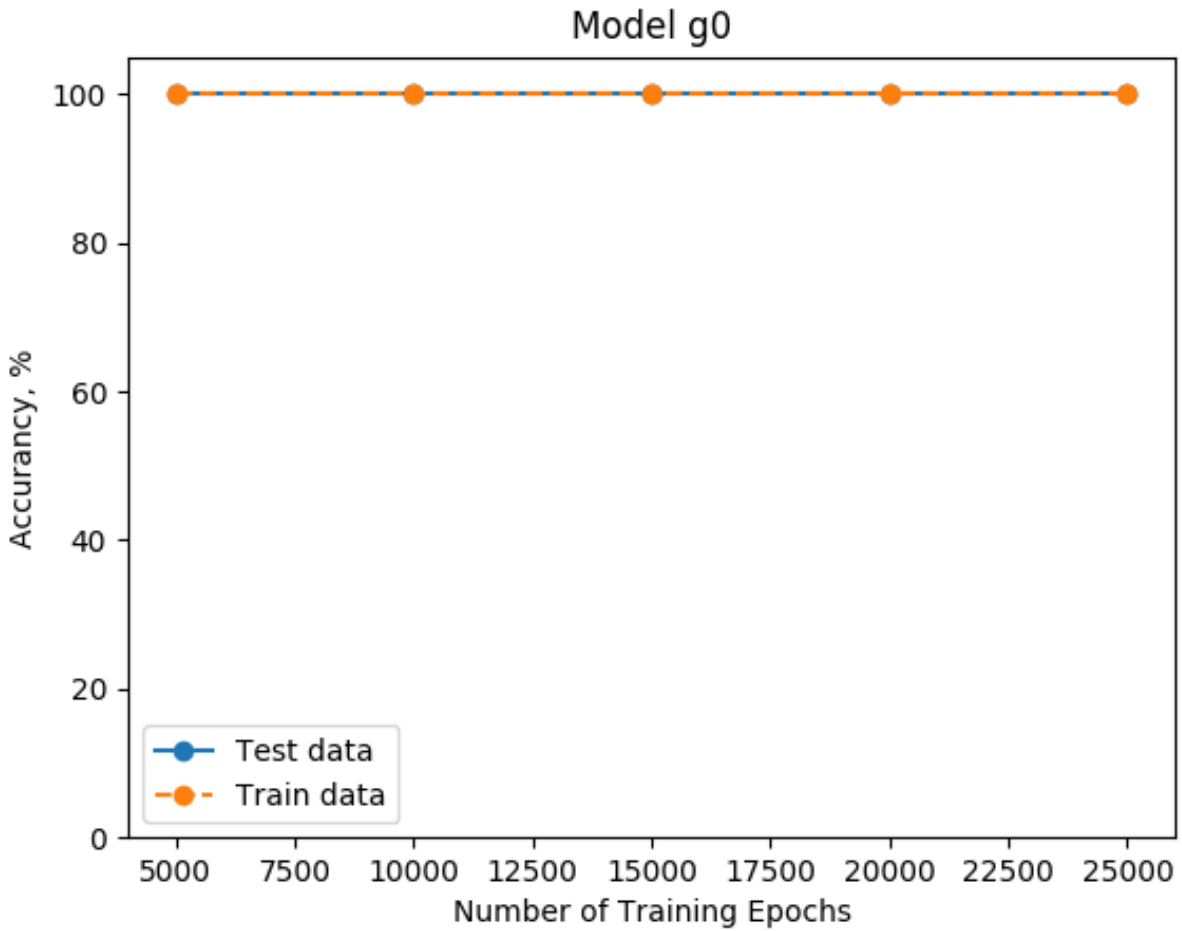
Аппроксимация криптографических примитивов преобразования Фейстеля

Численные результаты



Аппроксимация криптографических примитивов преобразования Фейстеля

Численные результаты



Аппроксимация криптографических примитивов преобразования Фейстеля

Численные результаты

Модель	НС	N	NP	T_o	T_e	$\hat{f}$	I	Σ	Ψ
g_0	MNN	8	96	128	24	4	0.1072	5000	1.3754
g_0	NN	0	96	128	24	3.2	0.5867	5000	1.6164
g_1	MNN	8	96	128	24	4	0.1365	10000	2.7018
g_1	NN	0	96	128	24	2.300	0.6505	25000	6.1263
g_2	MNN	8	96	128	24	4	0.1585	20000	5.4420
g_2	NN	0	96	128	24	2.6539	0.6341	20000	7.1460
g_4	MNN	4	32	10	5	4	0.0720	10000	2.0639
g_4	NN	0	32	10	5	3.500	0.5526	10000	3.1317
g_8	MNN	8	128	128	24	8	0.0519	5000	2.4865
g_8	NN	0	128	128	24	7.5385	0.5039	10000	3.8590
g_{16}	MNN	16	512	512	129	16	0.0520	15000	6.3108
g_{16}	NN	0	512	512	129	14.3650	0.5386	20000	9.5851
g_{32}	MNN	32	4096	2048	409	32	0.0120	10000	18.8175
g_{32}	NN	0	4096	2048	409	27.2161	0.5614	15000	20.2561

Таблица: Сравнение построенных нейронных сетей

$V = 0, 1$;
N- размерность;
$X = (x_i) \in V^{2N}, X = (X_1 \| X_2) \in V^{2N}, X_i \in V^N, i = 1, 2$;
$Y = (y_i) \in V^{2N}, Y = (Y_1 \| Y_2) \in V^{2N}, Y_i \in V^N, i = 1, 2$;
$K = (K1 \| ... \| K_8) = (k_1, ..., k_{8N})$ - ключ тактового преобразования;
$< K_i > \in \{0, 1, ..., 2^N - 1\}$ - числовое представление двоичного вектора K_i;
$\lll L$ - циклический сдвиг влево на L бит;
$f(\cdot) : V^N \times V^N \to V^N$ - функция криптографического преобразования Фейстеля;
$g(\cdot) : V^N \to V^N$ - расписание ключей.

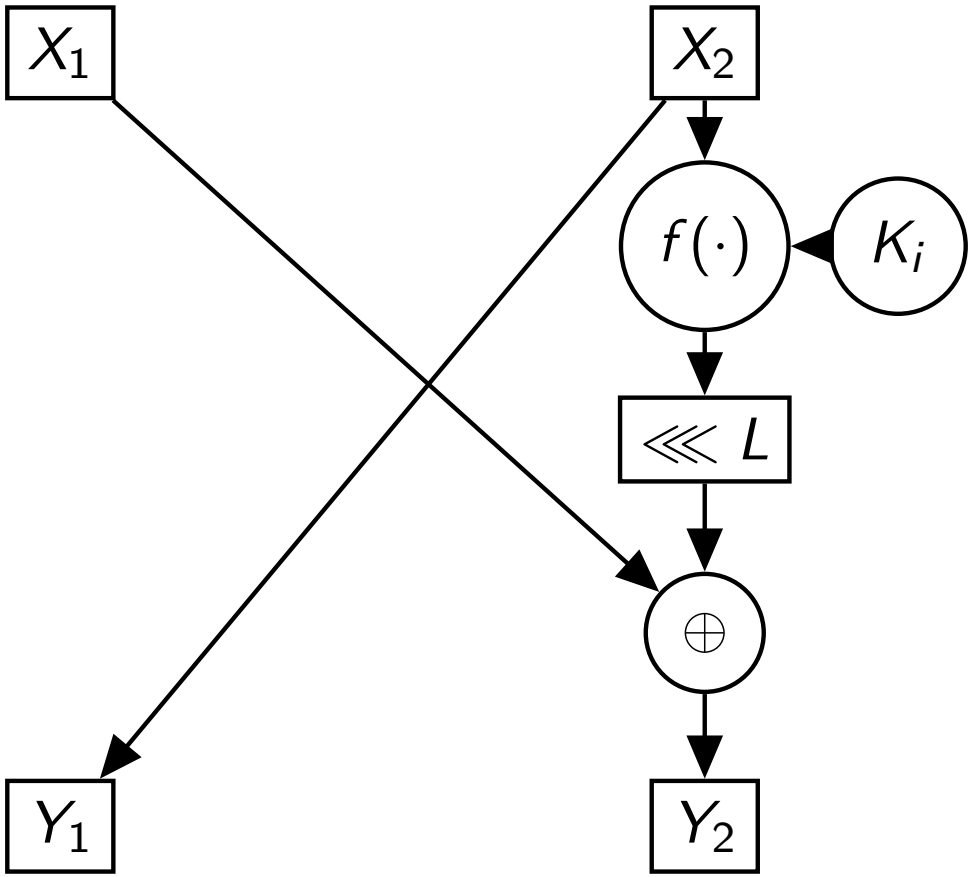


Рис.: Модельное 1-тактовое преобразование с i-ым подключом

$f(X_2; K) = S[X_2 \boxplus K]$, где S - два первых стандартных S-блока из ГОСТ-28147.
$g(K) = K_1, ..., K_8; K_1, ...K_8; ...; K_1, ...K_8$.
Параметр N постоянный и равен $= 8$.
Параметры L, I - изменяемые параметры в следующих диапозонах:

- $L \in \{0, 1, ..., 7\}$;
- $I \in \{1, ..., 8\}$;

Оценка надежности криптографического преобразования Фейстеля с помощью его аппроксимации нейронной сетью

Численные результаты

Заключение

Основные результаты:

1. Для математических моделей криптографических преборазований Фейстеля был разработан генератор и построенны нейронные сети;
2. Была проведена оценка полученных результатов.
3. Проведены компьютерные эксперименты, иллюстрирующие теоретические результаты.

Спасибо за внимание!

БЕЛАРУСКІ ДЗЯРЖАЎНЫ УНІВЕРСІТЭТ

Оценивание надежности криптографических преобразований на основе нейронных сетей

Максим Юрьевич Деркач

Научный руководитель: Юрий Семенович Харин

Минск, 2020