

# 1 Применение нейронных сетей для аппроксимации криптографического примитива ГОСТ 28147

Для оценки точности построенной модели использовалось расстояние Хэмминга.

$$w(y, \hat{y}) = \sum_{i=1}^j y_i \oplus \hat{y}_i, \text{ где } y_i \in V_j.$$

В данной работе рассматривались следующие задачи:

1.  $y = g_0(x, x_1) \equiv x \oplus x_1$ , где  
 $x \in V_4$  - вектор входных данных,  
 $x_1 \in V_4$  - добавочный вектор данных;
2.  $y = g_1(x, x_1, k) \equiv S[x \boxplus k] \oplus x_1$ , где  
 $x \in V_4$  - вектор входных данных,  
 $x_1 \in V_4$  - добавочный вектор данных,  
 $k \in V_4$  - ключ (4-битная часть ключа),  
 $S$  - стандартный S-блок из ГОСТ-28147;
3.  $y = g_2(\hat{x}, x_1, K) \equiv S[\hat{x}] \oplus x_1$ , где  
 $x \in V_4$  - вектор входных данных,  
 $x_1 \in V_4$  - добавочный вектор данных,  
 $K = k_1 || k_2 || \dots || k_8, k_i \in V_4$  - ключ,  
 $X = x^{(1)} || x^{(2)} || \dots || x^{(8)}, x^{(i)} \in V_4$  - блок входных данных,  
 $S$  - стандартный S-блок из ГОСТ-28147,  
 $\hat{X} = \bar{X} \boxplus \bar{K} \equiv \hat{x}^{(1)} || \hat{x}^{(2)} || \dots || \hat{x}^{(8)}, \hat{x}^{(i)} \in V_4$ .

Для решения поставленных задач использовались следующие математические модели:

1. Однослойная нейронная сеть, 15000 итераций обучения.
2. Многослойная нейронная сеть с одним скрытым слоем с 4 нейронами на скрытом слое, 15000 итераций обучения.
3. Многослойная нейронная сеть с одним скрытым слоем с 8 нейронами на скрытом слое, 15000 итераций обучения.
4. Многослойная нейронная сеть с одним скрытым слоем с 16 нейронами на скрытом слое, 15000 итераций обучения.
5. Многослойная нейронная сеть с одним скрытым слоем с 32 нейронами на скрытом слое, 15000 итераций обучения.
6. Многослойная нейронная сеть с двумя скрытыми слоями с 32 нейронами на скрытых слоях, 15000 итераций обучения.

Компьютерные эксперименты проводились на следующих данных:

1. Обучающая выборка  $T_o = 18 * 10^3$  пар  $(x, x_1)$ ;
2. Экзаменационная выборка  $T_e = 2 * 10^3$  пар  $(x, x_1)$ .

Для оценки точности использовалась следующая функция:  $\hat{f} = \frac{1}{T_e} \sum_{j=1}^{T_e} w(y^{(j)}, \hat{y}^{(j)})$ .

### Результаты:

Задача	Модель	Результаты
1.	1	$f(pred, real) = 1.3699500560760498$
1.	2	$f(pred, real) = 1.4635499715805054$
1.	3	$f(pred, real) = 0.8504499793052673$
1.	4	$f(pred, real) = 0.07020000368356705$
1.	5	$f(pred, real) = 0.001$
1.	6	$f(pred, real) = 2.012$
2.	1	$f(pred, real) = 1.6059999465942383$
2.	2	$f(pred, real) = 1.4520000219345093$
2.	3	$f(pred, real) = 1.253999948501587$
2.	4	$f(pred, real) = 1.1009999513626099$
2.	5	$f(pred, real) = 0.9789999723434448$
2.	6	$f(pred, real) = 2.001212$
3.	1	$f(pred, real) = 1.6059999465942383$
3.	2	$f(pred, real) = 1.4520000219345093$
3.	3	$f(pred, real) = 1.253999948501587$
3.	4	$f(pred, real) = 1.1009999513626099$
3.	5	$f(pred, real) = 0.9789999723434448$
3.	6	$f(pred, real) = 2.001212$