1 Применение нейроных сетей для апроксимации криптографического примитива ГОСТ 28147

Для оценки точности построенной модели использовалось расстояние Хэмминга.
$w(y, \hat{y}) = \sum_{i=1}^{j} y_i \oplus \hat{y}_i$, где $y_i \in V_j$.

В данной работе рассмотривались 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,
   $K = k_1||k_2||...||k_8, k_i \in V_4$ - ключ,
   $X = x^{(1)}||x^{(2)}||...||x^{(8)}, x^{(i)} \in V_4$ - блок входных данных,
   S - стандартный S-блок из ГОСТ-28147,
   $\hat{X} = \bar{X} \boxplus \bar{K} \equiv \hat{x}^{(1)}||\hat{x}^{(2)}||...||\hat{x}^{(8)}, \hat{x}^{(i)} \in V_4$.

Для решения поставленных задач использовались следующие математические модели:

1. Однослойная нерйоная сеть, 15000 итераций обучения.
2. Многослойная нерйоная сеть с одним скрытым слоем с 4 нейронами на скрытом слое, 15000 итераций обучения.
3. Многослойная нерйоная сеть с одним скрытым слоем с 8 нейронами на скрытом слое, 15000 итераций обучения.
4. Многослойная нерйоная сеть с одним скрытым слоем с 16 нейронами на скрытом слое, 15000 итераций обучения.
5. Многослойная нерйоная сеть с одним скрытым слоем с 32 нейронами на скрытом слое, 15000 итераций обучения.
6. Многослойная нерйоная сеть с двумя скрытым 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	$f(pred, real) = 1.506$
1.	2	$f(pred, real) = 1.209$
1.	3	$f(pred, real) = 0.800$
1.	4	$f(pred, real) = 0.179$
1.	5	$f(pred, real) = 0.000$
1.	6	$f(pred, real) = 2.006$
2.	1	$f(pred, real) = 1.434$
2.	2	$f(pred, real) = 1.4305$
2.	3	$f(pred, real) = 0.698$
2.	4	$f(pred, real) = 0.250$
2.	5	$f(pred, real) = 0.000$
2.	6	$f(pred, real) = 2.009$
3.	1	$f(pred, real) = 1.617$
3.	2	$f(pred, real) = 1.596$
3.	3	$f(pred, real) = 1.340$
3.	4	$f(pred, real) = 1.153$
3.	5	$f(pred, real) = 0.985$
3.	6	$f(pred, real) = 2.006$