ИНФОРМАТИКА

Квантово-устойчивое шифрование на основе нейросети

Чайко Владимир Иванович, студент

Кузбасский гуманитарно-педагогический институт Кемеровского государственного университета (г. Новокузнецк)

В данной статье автор предлагает новый метод шифрования данных с применением нейронов, теоретически устойчивый к взлому квантовым суперкомпьютером.

Ключевые слова: *квантово-устойчивый шифр, нейронная сеть, шифрование.*

Благодаря квантовым суперкомпьютерам все шифрование (в том числе и военное) оказалось под угрозой. Причина в том, что квантовые суперкомпьютеры могут за короткий промежуток времени взламывать шифр RSA и протоколы распределения ключей. [1] На данный момент времени еще не было собрано ни одного стабильного квантового суперкомпьютера, однако эксперимент ученых из Китая показал, что это лишь вопрос времени. [2] Решением может стать предлагаемый автором шифр, основанный на математических нейронах.

Математическим нейроном называется математическая модель биологического нейрона (клетки головного мозга), предложенная Мак-Каллоком и Питтсом в 1943 году. [3] Схема данной модели представлена на рисунке 1.

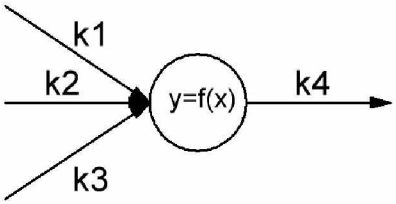

Рис. 1. **Схема математического нейрона**

Механизм работы математического нейрона следующий: сигнал от источника или предыдущих нейронов поступает в нейрон. Нейрон суммирует все сигналы, а полученную сумму преобразует при помощи активационной функции. В качестве функции активации, чаще всего, используется сигмоида. Результат активационной функции передается на выход или входы следующих нейронов. Каждое соединение обладает своим передаточным коэффициентом, изменение которого и является обучением. Последовательности математических нейронов образуют нейронную сеть. [4] Пример нейронной сети из 4-х нейронов представлен на рисунке 2.

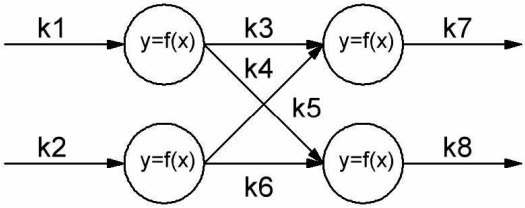

Рис. 2. **Пример нейронной сети**

Шифрованием называют обратимое преобразование данных в целях сокрытия информации, которую они несут. [5] Поэтому мы можем использовать прохождение информации через нейронную сеть как метод шифрования.

Механизм шифрования при помощи нейронной сети таков: Алиса (A) хочет передать сообщение Бобу (B). Для этого она пропускает свое сообщение через шифровальную нейронную сеть (SA). Полученное значение она отправляет Бобу (B). Боб, получив его, тоже пропускает через свою нейронную шифровальную сеть (SB), а результат отправляет обратно Алисе. Алиса, получив сообщение, пропускает его через дешифровочную нейронную сеть (dSA), а полученный результат отправляет Бобу. Боб получает сообщение, которое пропускает через свою дешифровальную нейронную сеть (dSB) и получает открытое сообщение. Наглядно данный метод представлен на рисунке 3.

Ключами шифрования в данном методе являются непосредственно сами коэффициенты связей нейронных сетей и то, какие активационные функции были выбраны для нейронов.

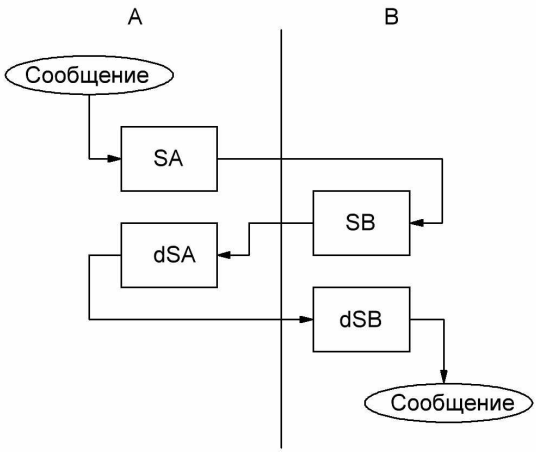

Рис. 3. **Наглядное представление метода**

Разница между шифровальной и дешифровальной нейронной сетью заключается в следующем:

1. В качестве функций активации нейронов используются взаимообратные математические функции.
2. При передаче данных между нейронами, при шифровании, осуществляется умножение на коэффициенты, а при дешифровании деление.

Наглядно это представлено на рисунке 4.

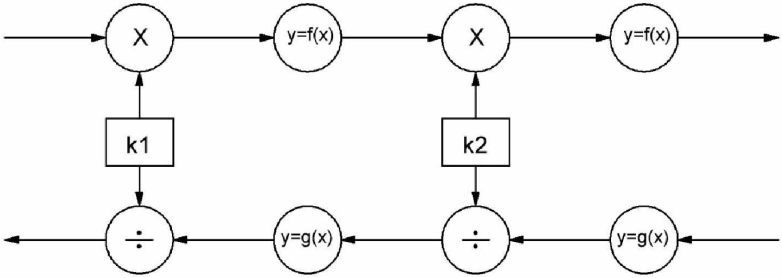

Рис. 4. **Шифровальная и дешифровальная нейронные сети**

Наличие в алгоритме шифрования математических нейронов накладывает определенные ограничения на формат шифруемых данных и ключей шифро-

вания (коэффициентов). Они должны быть представлены в виде чисел, находящихся в области значения активационных функций. [6] Учитывая, что активационные функции бывают различными, диапазон допустимых значений так же разнится и зависит от каждого конкретного случая.

Для проверки работоспособности предлагаемого метода шифрования была осуществлена передача числа «0,675» с применением данного шифра. В качестве функций активации были выбраны гиперболический арксинус (для шифрования) и гиперболический арккосинус (для дешифровки). Все программное обеспечение было реализовано на языке программирования PHP 8.4 [7] и проверено при помощи онлайн интерпретатора OnlineGDB. [8] Программный код представлен в листинге 1. Результат работы представлен на листинге 2.

Листинг 1. Код программы.

```
<?php
	function neiro($x) {
		$y=asinh($x);
		return $y;
	}
	function anti_neiro($y) {
		$x=acosh($y);
		return $y;
	}
	$key1=0.10; //Первый ключ Алисы
	$key2=0.20; //Второй ключ Алисы
	$key11=0.30; //Первый ключ Боба
	$key22=0.40; //Второй ключ Боба
	$pered=0.675; //Передаваемое сообщение
	echo $pered.” // Сообщение \n”;
	$etap1=neiro(neiro($pered*$key1)*$key11); //
	Шифрование Алисы
	echo $etap1.” // Сообщение зашифрованное Алисой \n”;
	$etap2=neiro(neiro($etap1*$key2)*$key22); //
	Шифрование Боба
	echo $etap2.” // Сообщение зашифрованное Бобом \n”;
	$etap3=anti_neiro(anti_neiro($etap2)/$key11)/$key1;
	//Дешифровка Алисы
	echo $etap3.” // Алиса сняла свое шифрование \n”;
	$etap4=anti_neiro(anti_neiro($etap3)/$key22)/$key2;
```

```
        //Дешифровка Боба
        echo $etap4." // Боб снял свое шифрование \n";
        echo "\n";
?>
```

Листинг 2. Результат работы программы

```
0.675 // Сообщение
0.020233273536787 // Сообщение зашифрованное Алисой
0.0016186567584387 // Сообщение зашифрованное Бобом
0.053955225281292 // Алиса сняла свое шифрование
0.675 // Боб снял свое шифрование
```

Значения функций активации нейронов, при реализации данного шифра на ЭВМ, могут быть неточными по причине накопления погрешности при их вычислениях компьютером. [9] От программиста может потребоваться прибегать к различным методам уточнения вычислений [10] или корректировки результата дешифровки. Наиболее простым решением данной проблемы является метод корректировки результата дешифровки при помощи остатка от деления. [11]

Для взлома данного шифра необходимо не только подобрать ключи, но и функции активации. Вычислить их не представляется возможным связи с тем, что они никак не передаются и держаться в секрете. Иными словами, взломщику необходимо решить следующее уравнение:

$$text = f_1\left(\frac{f_2\left(\frac{x}{k_2}\right)}{k_1}\right)$$

где: f_1 и f_2 — неизвестные функции активации, k_1 и k_2 — неизвестные ключи, x — зашифрованное послание.

Решить такое уравнение возможно только методом перебора всех возможных вариантов, что приводит к большому количеству равновероятных вариантов расшифровок. Взломщик оказывается в той же ситуации, что и во время взлома шифра Вернама. Это говорит о том, что данный шифр невозможно взломать при любых вычислительных мощностях, в том числе и на квантовом суперкомпьютере. [12]

Для увеличения надежности шифрования можно увеличивать количество нейронов и/или внедрить шифр Вернама в структуру данного алгоритма.

Литература:

1. Взломают ли шифрование RSA на квантовом компьютере в 2023 году? // Kaspersky Daily. URL: ttps://www.kaspersky.ru/blog/quantumcomputers-and-rsa-2023/34503/ (дата обращения: 03.01.2025).
2. Factoring integers with sublinear resources on a superconducting quantum processor // Arxiv. URL: https://arxiv.org/abs/2212.12372 (дата обращения: 03.01.2025).
3. Mcculloch W. S., Pitts W. A logical Calculus of Ideas Immanent in Nervous Activity. // Mathematical Biophysics. — 1943. — № 5. — С. 115–133.
4. Исмаилов Ш. А., Поздняков Н. В. Математическая модель нейронаи возможности его технической реализации // Системные технологии. — 2014. — № 12.
5. Singh S. L. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Vintage, 2000.
6. Rashid, Tariq. Make Your Own Neural Network / Tariq Rashid. CreateSpace, 2016. — 222с. — Текст: непосредственный.
7. PHP 8.4 // PHP. URL: https://www.php.net/releases/8.4/ru. php (дата обращения: 04.01.2025).
8. OnlineGDB. URL: https://www.onlinegdb.com/online_php_interpretern (дата обращения: 04.01.2025).
9. Разрешающая способность и точность вычислений. Не только машинных. // Разумный мир. URL: https://dzen.ru/a/YvHfJjc83Vgxmek_?ysclid=m5k1mcm4mi120531683 (дата обращения: 06.01.2025.).
10. Компенсация погрешностей при операциях с числами с плавающей запятой // Хабр. URL: https://habr.com/ru/articles/266023/ (дата обращения: 06.01.2025.).
11. Mod function // Microsoft Learn Challenge URL: https://learn.microsoft.com/en-us/power-platform/power-fx/reference/functionmod (дата обращения: 06.01.2025.).
12. Невзламываемый шифр Вернама // КОД. Код журнал Яндекс Практикума. URL: https://thecode. media/vernam/ (дата обращения: 03.01.2025).