4. Online Human-Bot Interactions: Detection, Estimation, and Characterization // arxiv.org [Электронный ресурс]. URL: https://arxiv.org/abs/1703.03107 (дата обращения: 04.11.2017).

5. *Tam J.*, *Simsa J.*, *Hyde S.*, *Von Ahn L.* Breaking audio captchas // NIPS. 2008.

УДК 004.8

И. А. Пятницкий
Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ШИФРОВАНИИ

Аннотация. Криптография стала важнейшим компонентом контроля за аутентификацией, интеграцией, конфиденциальностью и надежностью хранения личных данных, передаваемых через публичные сети. С течением времени, в связи с улучшением производительности и скорости работы компьютеров, старые шифры заменяются на новые, более адаптированные. В статье предложено использовать новые нейросетевые подходы к шифрованию данных.

Ключевые слова: нейронные сети; шифрование; информационная безопасность; инженерно-техническая защита информации.

По мере развития новых методов шифрования [1] математика в них становилась все более и более значимой. Благодаря математике криптография достигла такого уровня развития, что количество математических операций в каждом шифре астрономически высоко. Это означает, что современные криптоалгоритмы стали гораздо более устойчивы к криптоанализу, чем некогда используемые, устаревшие методики, для взлома которых было достаточно ручки и бумаги. Классический криптоанализ не способен эффективно взламывать современные шифры.

По этой причине гораздо большее значение приобретают методы, основанные на перехвате данных, закладке жучков, атаках по сторонним каналам, квантовых компьютерах и бандитском криптоанализе.

Атака по сторонним (или побочным) каналам (от англ. *side-channel attack*) — класс атак, направленный на уязвимости в практической реализации криптосистемы. Такие атаки используют уязвимости в физической реализации алгоритмов. Поскольку любой, даже самый сложный алгоритм в конечном итоге реализуется программой, обрабатывается процессором с определенной конфигурацией, таким образом будет обладать определенной спецификой.

© Пятницкий И. А., 2017

«Классический» криптоанализ рассматривает алгоритмы шифрования только с математической точки зрения, оперируя только алгебраическими свойствами, возможно, параметризованными ключом.

В то время как криптоанализ побочных каналов рассматривает такие параметры, как время выполнения операций, потребляемую мощность, электромагнитное излучение, звуки и другие. Такие атаки обладают меньшей универсальностью, поскольку зависят от конкретного устройства, на котором производится шифрование, однако они существенно эффективнее. Большинство успешных атак используют слабости в реализации примитивов криптоалгоритма.

Известные типы атак:

1) Атака зондированием. Простая инвазивная атака, устройство вскрывается, на контакты процессора устанавливаются щупы, или же при помощи микроскопа исследуются ячейки памяти.

2) Атаки по ошибкам вычислений. Основная идея — воздействие на устройство с целью возникновения ошибок, сравнивая искажения на различных этапах работы системы, возможно определить секретный ключ.

3) Атаки по энергопотреблению — пассивная атака, основанная на точном измерении энергопотребления устройства и получении на основе этих данных информации о выполняемых операциях и их параметрах. Такая атака легко осуществима, достаточно вставить в цепь питания резистор и измерять проходящий через него ток.

4) Атаки по электромагнитному излучению. Электронные устройства испускают электромагнитные излучения во время работы. Определенный спектральный рисунок соответствует определенным операциям, это позволяет получить информацию о работе алгоритма.

Согласно исследованиям, алгоритмы DES и AES крайне сильно подвержены таким типам атак, в некоторых случаях достаточно 1,5 с, или даже 15 измерений.

Нейросети, как следует из названия, являются сетями нейронов, где каждый нейрон — это вычислительная единица, которая получает информацию, производит над ней простые вычисления и передает ее дальше.

Отличительной особенностью нейронных сетей является то, что ими можно представить абсолютно любую функцию, в том числе криптографическую, аппроксимируя такой сетью уже существующий алгоритм, например DES или AES, можно значительно повысить его устойчивость к атакам по сторонним каналам.

Общий вид нейронной сети представлен на рис. 1.

Такая структура обеспечивает большую защищенность к атакам по сторонним каналам, поскольку:

1) Каждый нейрон содержит в себе лишь малую часть информации, необходимой для точной работы алгоритма, криптоаналитику потребуется проанализировать все возможные ячейки памяти.

2) Вычисления производятся для каждого нейрона в независимости от входных данных, в результате время работы сети будет зависеть только от ее архитектуры.

3) Еще одним важным свойством сетей является то, что по весам сети невозможно определить, каким был секретный ключ, а в некоторых случаях даже сам алгоритм шифрования

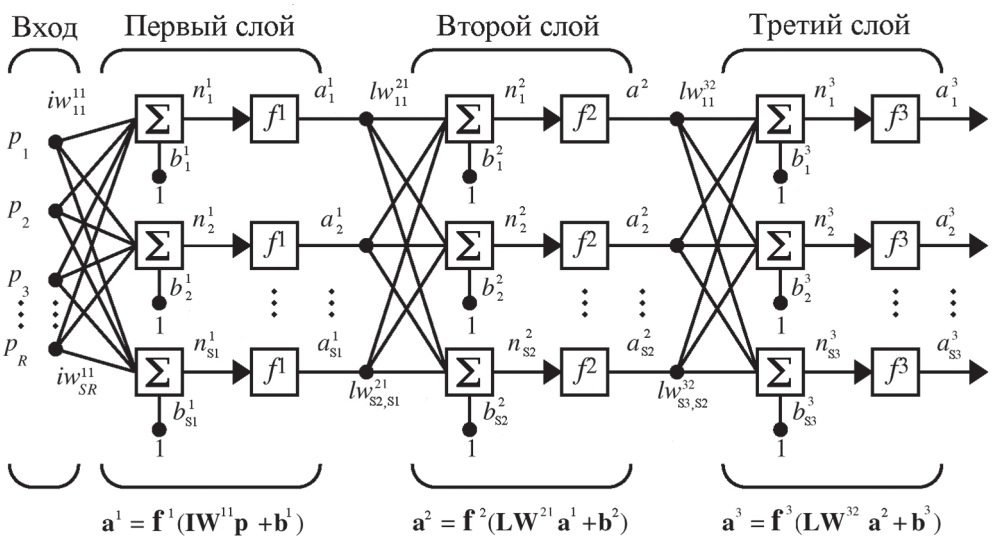

Рис. 1. Общий вид нейронной сети

Все эти особенности позволяют нейронным сетям надежно избегать атак по побочным каналам.

Список литературы

1. Элементы больших порядков в линейных группах и модификация системы эль-гамаля. URL: http://www.info-secur.ru/is_15/Zulyarkina.htm