УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 681.3.006

Плонковски Мартин Даниел

Модели передачи и криптографического преобразования информации на основе нейросетевых технологий и расширения поля используемых чисел

Автореферат диссертации
на соискание ученой степени кандидата технических наук
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск, 2008

Работа выполнена в учреждении образования «Белорусский государственный технологический университет»

Научный руководитель – **Урбанович Павел Павлович**, доктор технических наук, профессор, профессор кафедры информационных систем и технологий учреждения образования «Белорусский государственный технологический университет

Официальные оппоненты: **Бобов Михаил Никитич**, доктор технических наук, профессор, начальник отдела унитарного предприятия «Научно-исследовательский институт средств автоматизации»

Хижняк Александр Вячеславович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления войсками учреждения образования «Военная академия Республики Беларусь»

Оппонирующая организация – Учреждение образования «Белорусский национальный технический университет»

Защита состоится 4 июня 2009 г. в 14^{00} часов на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу 220013, г. Минск, ул. П.Бровки, 6, тел. 293-89-89, dissovet@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан «13» апреля 2009 г.

КРАТКОЕ ВВЕДЕНИЕ

В своей основе вся современная криптография базируется на теории чисел. Надежность криптографических систем зависит от трудности решения задач в рассматриваемой области (например, задача факторизации, задача дискретного логарифмирования). Однако рост вычислительной мощности современных компьютеров требует применения все более длинных целых чисел, составляющих параметры криптографических систем.

Одной из новых идей является применение нейронных сетей в криптографии. Она касается проблемы обмена закрытыми (секретными) ключами по незащищенным (общественным) каналам связи.

Протокол обмена ключами, использующий нейронные сети, базируется на синхронном обучении сетей. Обучение двух нейронных сетей с использованием их общих выходных величин ведет к возникновению идентичных векторов весов (входных значений). Сети обмениваются между собой выходными величинами, при этом секретными остаются внутренние состояния векторов весов. Третья сторона (интруз), следящая за обменом информацией между обеими сетями, практически не в состоянии восстановить внутренние значения векторов весов ни одной из сетей. Следовательно, вектор весов может составлять секретный ключ, использующийся для дальнейшей передачи информации по незащищенным каналам. Второе, не менее эффективное, применение нейронных сетей в криптографии – использование их в качестве хеш-функций.

Использование нейронных сетей для решения задач защиты информации впервые предложено И. Кантером и В. Кинцелем и основывается на использовании известной архитектуры TPM (англ. Tree Parity Machine, древовидная машина четности). При этом известные методы предполагают использование целых действительных чисел как поля для описания и анализа процессов в сети. Это является серьезным ограничением для дальнейшего совершенствования методов и обусловливает актуальность исследований, направленных на теоретическое обоснование возможности расширения поля используемых чисел, а также возможности практической реализации новых методов.

В этой работе представлены архитектуры и модели нейронных сетей, основанные на алгебре последовательных расширений поля действительных чисел (комплексные числа, кватернионы, октонионы) и позволяющие описывать, анализировать и более эффективно решать вышеупомянутые криптографические проблемы. Ввиду своей специфики они позволяют обеспечить более высокий уровень безопасности, чем классические модели, основанные на арифметике действительных чисел.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами, темами

Работа выполнялась в соответствии с заданием 12 Государственной программы ориентированных фундаментальных исследований Республики Беларусь «Инфотех»: Разработка и исследование методов криптопреобразования информации на основе помехоустойчивых кодов и шифрования данных с использованием нейросетевых технологий (НИР ГБ 26-114, № ГР 20063589) на кафедре информационных систем и технологий Белорусского государственного технологического университета.

Цель и задачи исследования

Цель: теоретическое обоснование и разработка архитектур и моделей нейронных сетей на основе последовательного расширения поля используемых для их описания чисел в системах передачи криптографической информации, а также нейронных сетей, используемых в качестве хеш-функции.

Для достижения поставленных целей необходимо решить следующие задачи:

1) проанализировать современное состояние проблемы применения нейронных сетей в криптографических пространствах (обмен ключами, хеш-функции), учитывая уровень безопасности и эффективности применяемых решений;

2) разработать архитектуру и математические модели нейронных сетей, обеспечивающие безопасность обмена ключами и основанные на последовательном расширении поля действительных чисел; исследовать качество предложенных архитектур нейронной сети с точки зрения безопасности и эффективности действия;

3) разработать алгоритмы обмена конфиденциальной информацией на основе созданных моделей и оптимизировать их с точки зрения практического использования в информационных системах;

4) разработать математическую модель нейронной сети, позволяющей генерировать криптографическую хеш-функцию; представить реализацию модели нейронной хеш-функции с учетом проблемы ее эффективности.

Положения, выносимые на защиту

1. Новые архитектуры и соответствующие им математические модели нейронных сетей для целей обмена конфиденциальной информацией, отличительной особенностью которых является использование в качестве

алгебраической основы последовательных расширений поля действительных чисел: комплексных чисел, кватернионов и октонионов, что позволяет повысить уровень безопасности системы передачи конфиденциальных данных на основе двух сетей в десятки и сотни раз.

2. Математические модели нейронных сетей, отличающиеся использованием алгебры комплексных чисел и кватернионов и основанные на использовании нескольких функций перехода в архитектурах нейронных сетей: множество Жюлиа (Julia), уравнение Даффинга (Duffing) и уравнение Хэнона (Henon), что позволяет повысить скорость хеширования текстовых сообщить произвольной длины, обусловленную возможностью программной реализация математических операций в арифметике целых чисел (в известных решениях необходимо было использовать числа с плавающей запятой).

3. Компьютерные имитационные модели нейронных сетей для криптографического преобразования и передачи конфиденциальных данных, построенные на основе созданных по пп.1 и 2 архитектур и математических моделей и позволяющие оценить эффективность предложенных архитектур сетей.

Личный вклад соискателя

Все описанные в кандидатской диссертации результаты, получены самостоятельно автором. В публикациях с соавторами вклад соискателя определяется рамками изложенных в диссертации результатов.

Апробация результатов диссертации

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: 69-72-я научно-технические конференции профессорско-преподавательского состава, научных сотрудников и аспирантов БГТУ (Минск, февраль 2005-08гг.); III и IV Международные НТК «New Electrical and Electronic Technologies and Their Industrial Implementation» (Zakopane, Poland, June, 2005, June, 2007); XII Środowiskowa Konferencja Matematyczno-Informatyczna (Rzeszów - Lublin - Chełm – Łuck, 2-5.7.2006); Международная научно-практическая конференция, (апрель 2006г., Брест); Международная научно-практическая конференция, (апрель 2007г., Брест).

Опубликованность результатов диссертации

По результатам выполненных исследований опубликовано 14 печатных работ, в том числе: 6 статей, 8 тезисов докладов и материалов конфе-

ренций. Без соавторов опубликовано 7 работ. Суммарный объем публикаций составляет примерно 2,8 авторских листа.

Структура и объем диссертации

Работа состоит из перечня условных обозначений, общей характеристики работы, введения, четырех глав, заключения, списка использованных источников, включающего 103 наименования, списка работ соискателя из 14 наименований и приложений. Первая глава содержит обзор научно-технической литературы и постановку задачи. Вторая и третья глава посвящены описанию разработанных математических моделей и алгоритмов. Четвертая глава содержит описание программной реализации разработанных моделей и алгоритмов. Общий объем – 127 страниц, в том числе 21 страница приложений, 17 иллюстраций, 8 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении определены область и актуальность исследования диссертационной работы, кратко проанализировано общее состояние проблемы и основные пути ее решения.

В первой главе диссертации представлена информация о современных знаниях и проблемах в области криптографии и искусственных нейронных сетей.

Рассмотрены основные современные направления развития симметричных и асимметричных криптографических систем. Асимметричные системы являются наиболее распространенными и востребованными в настоящее время. Однако их главным недостатком является сложность математических операций, которые значительно увеличивают время, необходимое на выполнение вычислений. Поэтому, по-прежнему все еще достаточно часто используются симметричные криптосистемы. Проблема создания быстрых протоколов согласования ключа до сих пор остается актуальной.

Вторым недостатком асимметричных криптосистем является тот факт, что их безопасность основывается на сложности вычислительных операций в задачах из теории чисел. Однако в работе Шора (Shor) дано описание быстрых алгоритмов, позволяющих осуществлять факторизацию больших натуральных чисел с использованием квантовых компьютеров. Следовательно, если бы удалось создать такой компьютер, то алгоритмы асимметричных криптосистем (например, RSA) стали бы бесполезными. Поэтому большой интерес представляет разработка новых методов, не использующих в своей конструкции теорию чисел.

В течение последних нескольких десятков лет большой интерес для различных исследований представляют искусственные нейронные сети. Они нашли применение во многих сферах, в том числе и в криптографии. И. Кантер и В. Кинцель предложили идею использования нейронных сетей для обмена криптографической информацией. Значение векторов весов обоих персептронов, отличающееся только знаком, может быть использовано в качестве секретного ключа. Протокол этого типа, выполняет ту же роль, что и хорошо известный протокол обмена ключами Диффи–Хеллмана. При этом исследования в этом направлении предполагают использование лишь целых действительных чисел, что ограничивает эффективность применения метода. Процесс синхронизации двух сетей, основанный на использовании двух одиночных персептронов, передает слишком много информации, что является слабым местом этой системы. Поэтому необходимо модифицировать всю систему таким образом, чтобы скрыть как можно больше информации, чтобы оппонент не был в состоянии синхронизировать свои вектора весов с наблюденными сетями. С другой стороны, степень скрытности должна давать возможность синхронизировать оба вектора, и таким образом, не может быть слишком высокой.

Резюмируя вышесказанное, заметим, что нейронные сети могут внести качественно новые идеи в решении современных криптографических проблем. Именно их применение может обеспечить увеличение уровня безопасности и эффективности криптографических решений.

На основе выполненного анализа сформулированы выводы, которые и предопределили цель и направления диссертационного исследования.

Во второй главе рассмотрены модели нейронных сетей, ориентированные на их использование в области криптографии. В основу здесь положены классические архитектуры нейронных сетей, использующие действительные целые числа. Однако использование конструкции Кэли–Диксона (Cayley–Dickson) позволяет создавать расширения поля действительных чисел. Аксиомы поля выполняют действия на основе только двух алгебр – действительных и комплексных чисел. Главным достоинст-

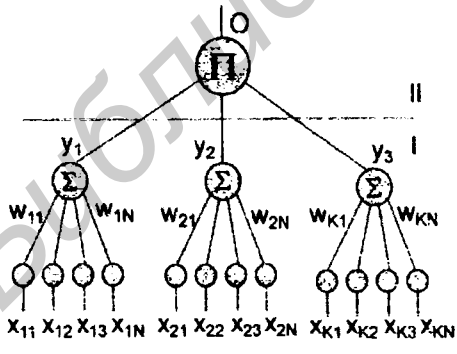

Рисунок 1 – Схема двух уровней модели TPM

вом создаваемых моделей является гарантированно более высокий уровень безопасности.

Отмеченные в первой главе задачи решает многослойная нейронная сеть с внесенными в ее строение некоторыми модификациями, которые позволяют реализовать эти требования. Это сеть с тремя внутренними нейронами, называемая машиной четности (англ. Parity Machine) или, более точно, древовидная машина четности (см. рисунок 1). Нейроны представляют собой персептроны с дискретными векторами весов.

Модель архитектуры TPM основана на алгебре целых действительных чисел, что допускает практическое применение модели в компьютерных системах. Все же главным вопросом всей системы является ее безопасность. Следовательно, развитие архитектур TPM должно идти по направлению увеличения сложности вычислительной алгебры, что гарантировало бы больший уровень безопасности и возможности применения такого подхода.

В рамках настоящего исследования была предложена модификация архитектуры TPM путем расширения используемой алгебры за счет комплексных чисел. Естественно, в соответствии с определением TPM, действительные и мнимые части комплексных чисел, применяемых в данной архитектуре, должны быть целыми числами. Эта архитектура получила условное название TPCM (англ. Tree Parity Complex Machine, древовидная машина четности на основе комплексных чисел).

Сама архитектура сети TPCM, как и идея ее функционирования, схожа с архитектурой TPM. Предложенные здесь изменения касаются методов применения правила обучения и модификации функции знака.

Архитектура TPCM состоит из двух уровней. Элементы первого уровня – это персептроны, имеющие N- элементные векторы весов – ($[w_{k,1}, w_{k,2}, ..., w_{k,N}]$, где $1 \le k \le K$, K – число персептронов), величины которых – это комплексные числа. Как и в случае архитектуры TPM, значения вышеуказанные весов ограничены промежутком $[-L, L]$ x $[-L, L]$ (который является естественным расширением промежутка $[-L, L]$ для архитектуры TPM). Вход персептронов составляет $K{\cdot}N$-элементных векторов $[x_{k,1}, x_{k,2}, ..., x_{k,N}]$, часто отождествляемых с одним $N{\cdot}K$-элементным вектором $[x_1, x_2, ..., x_{kN}]$ четырехвалентных комплексных чисел, выбранных из множества {(1, 1), (-1, 1), (-1, -1), (1, -1)}. Выходы нейронов – это четырехвалентные комплексные числа, принадлежащие множеству {(1, 0), (0, 1), (-1, 0), (0, -1)} и обозначенные через $y_1, y_2, ..., y_K$. Второй уровень составляет один персептрон, выходное значение которого – это произведение выходов всех персептронов, составляющих первый уровень.

Математическая модель сети ТРСМ рассматривается нами в традиционном ее толковании: как зависимость выходных значений от входных с учетом некоторых преобразований, условно обозначаемых в общем случае «черным ящиком». Выход *O* архитектуры ТРСМ вычисляется по следующей формуле:

$$O^{A/B} = \prod_{k=1}^{K} y_k^{A/B} = \prod_{k=1}^{K} \sigma\left(\alpha_k^{A/B}\right) = \prod_{k=1}^{K} \sigma\left(\sum_{j=1}^{N} w_{kj}^{A/B} x_{kj}\right). \quad (1)$$

Индекс *A/B* обозначает, что данная операция касается обеих сетей (*A* и *B*), которые будут использованы в процессе обучения. Функция знака σ представлена следующими соотношениями:

$$\sigma(\alpha_k) = \begin{cases} (1,0), & при \quad \frac{7\pi}{4} < \arg(\alpha_k) \le \frac{\pi}{4}, \\ (0,1), & при \quad \frac{\pi}{4} < \arg(\alpha_k) \le \frac{3\pi}{4}, \\ (-1,0), & при \quad \frac{3\pi}{4} < \arg(\alpha_k) \le \frac{5\pi}{4}, \\ (0,-1), & при \quad \frac{5\pi}{4} < \arg(\alpha_k) \le \frac{7\pi}{4}, \end{cases} \quad (2)$$

Ввиду специфики алгебры комплексных чисел, как расширения действительных чисел, любая производимая с ними математическая операция сохраняет свой смысл и вычислительную корректность. Изменению же будет подвергаться функция знака. В случае целых чисел она может принимать два значения: (-1, 1). В случае комплексных чисел это будут четыре возможных варианта: (1, 0), (0, 1), (-1, 0), (0, -1). Следовательно, учитывая размещение этих величин, нужно произвести соответствующее разделение плоскости комплексных чисел (традиционно обозначаемой R^2) (см. рисунок 2).

В зависимости от положения входных аргументов в одной из четвертей вышеуказанная функция приписывает им одну из четырех выходных величин.

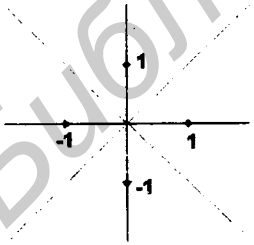

Рисунок 2 – Упрощенная схема представления функции знака

Рассматриваемая модель должна строиться с учетом некоторых ограничивающих параметров. Основа такого ограничения в данном случае связывается с правилом обучения сети. Правило обучения в модели ТРСМ аналогично правилу в архитектуре ТРМ. Изменения же требует действие, накладывающее ограничения на величины элементов вектора весов. Оно будет происходить в два этапа, отдельно для каждой части ком-

плексного числа согласно следующим формулам:

$$\mathrm{Re}(w_{kj}^{A/B}) = \begin{cases} sign(\mathrm{Re}(w_{kj}^{A/B}))L, & при \quad \left|\mathrm{Re}(w_{kj}^{A/B})\right| > L, \\ \mathrm{Re}(w_{kj}^{A/B}), & в\ противном\ случае \end{cases}, \tag{3}$$

$$\mathrm{Im}(w_{kj}^{A/B}) = \begin{cases} sign(\mathrm{Im}(w_{kj}^{A/B}))L, & при \quad \left|\mathrm{Im}(w_{kj}^{A/B})\right| > L, \\ \mathrm{Im}(w_{kj}^{A/B}), & в\ противном\ случае \end{cases}. \tag{4}$$

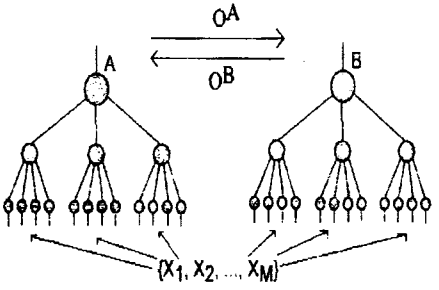

Рисунок 3 – Схема процесса синхронизации двух сетей

Процесс обучения сети на основе архитектуры TPCM происходит таким же образом, как и в известной модели TPM (по правилу Хебба). Процесс обучения сети TPCM, однако, должен строиться с учетом вышеприведенных формул, а также с учетом того, что входные величины (вектор X) принадлежат следующему множеству: {(1, 1), (-1, 1), (-1, -1), (1, -1)}. Величины векторов весов – это комплексные числа, заключенные в квадрате $[-L, L]$x$[-L, L]$.

Две архитектуры, обученные на основании вышеуказанной схемы, впоследствии достигают состояния синхронизации. Это означает, что их векторы весов имеют идентичные величины ($w^A = w^B$). Схема процесса синхронизации представлена на рисунке 3.

Главным элементом, подтверждающим безопасность процесса синхронизации архитектуры TPCM, является тот факт, что выходная величина не определяется через выходные величины отдельных персептронов. Например, в классической модели архитектуры TPM с параметром $K = 3$ для каждой выходной величины существуют четыре внутренних возможных выходных величины персептронов (для $O = 1$ - (1, 1, 1), (-1, -1, 1), (1, -1, -1), (-1, 1, -1)).

В архитектуре же TPCM количество возможных внутренних величин персептронов, соответствующих одой выходной величине, увеличивается квадратично. Например, для $K = 3$ существует 16 возможных вариантов. Для $O = 1$ – (1, 1, 1), (-1, -1, 1), (1, -1, -1), (-1, 1, -1), (i, i, -1), (i, -1, i), (-1, i, i), (-i, i, 1), (-i, 1, i), (i, 1, -i), (i, -i, 1), (i, i, -i), (1, -i, i), (-i, -i, -1), (-i, -1, -i), (-1, -i, -i) (для упрощения мы использовали каноническую запись комплексных

чисел). Следовательно, можно утверждать, что системы обмена ключами, основанные на архитектуре TPCM, будут характеризоваться более высоким уровнем безопасности, чем их эквиваленты, использующие архитектуру TPM.

Выясним теперь, почему оппонент *C*, который наблюдает за обменом информацией между двумя сетями *A* и *B*, не в состоянии синхронизировать свои вектора весов с наблюдаемыми сетями. В общем случае вероятность того, что сети *A* и *B* активизируют свои векторы весов в одном направлении, определяется соотношением:

$$\frac{p^2}{p^2+(1-p)^2}. \tag{5}$$

В то же время вероятность такого совпадения между сетями *A* и *C* составляет *p*. Из определения вероятности следует, что $0 \le p \le 1$. Из соображений того, что рассмотрение крайних случаев можно опустить, получаем условие $0 < p < 1$. Легко доказать, что отсюда вытекает следующее неравенство:

$$\frac{p^2}{p^2+(1-p)^2} > p. \tag{6}$$

Для простоты и понимания рассмотрим архитектуру TPCM с двумя ($K = 2$) персептронами и определим:

$$p_k = P[y_k^A = y_k^B]. \tag{7}$$

Далее примем также, что $p_1 = p_2 = p$ ($k = 1, 2$). Итак, получим четыре возможных варианта:

$$(y_1^A = y_1^B,\ y_2^A = y_2^B), \tag{8}$$
$$(y_1^A \neq y_1^B,\ y_2^A = y_2^B), \tag{9}$$
$$(y_1^A = y_1^B,\ y_2^A \neq y_2^B), \tag{10}$$
$$(y_1^A \neq y_1^B,\ y_2^A \neq y_2^B). \tag{11}$$

Им соответствуют следующие вероятности: p^2, $p(1-p)$, $(1-p)p$ и $(1-p)^2$. Вариант (8) возникает в ситуации, когда $O^A = O^B$. Варианты (9) и (10) возникают в ситуациях, где $O^A \neq O^B$. Следовательно, веса обеих архитектур не активизируются. Вариант же (11) в 1/3 случаев возможен, если $O^A = O^B$, в остальных 2/3 случаев – $O^A \neq O^B$. Следовательно, вероятность того, что сети *A* и *B* активизируют свои векторы весов в одном направлении, равна

$$\frac{p^2}{p^2+\frac{1}{3}(1-p)^2}, \tag{12}$$

если вероятность наступления согласованного движения между сетями A и C равна p. Легко доказать, что:

$$\frac{p^2}{p^2+\frac{1}{3}(1-p)^2} > \frac{p^2}{p^2+(1-p)^2}. \qquad (13)$$

Отсюда вытекает, что сети A и B на основе архитектуры TPCM быстрее достигнут состояния синхронизации относительно оппонента C, чем сети A, B и C, основанные на архитектуре TPM (при этом справедливо (6)). Предполагаемые результаты подтверждены результатами имитационного моделирования (глава IV).

Дополнительным плюсом архитектур TPCM является большая свобода в выборе конструктивных параметров, определяющих процесс синхронизации: речь идет об ограничении, накладываемом на величины вектора весов. Поскольку в случае TPM данное ограничение представляет собой простой промежуток ($[-L, L]$), то в случае TPCM им может быть любая фигура (из пространства R^2). На основании результатов, приведенных в таблице 1, мы видим, что архитектура TPCM позволяет существенно (примерно в 2.5-3.0 раза) увеличить уровень безопасности системы (данный уровень измерен отношением, представленным в четвертом столбце таблицы; один шаг обозначает одну операцию вычисления и обмена выходными величинами между сетями).

Таблица 1 – Сравнение времени синхронизации архитектур TPM и TPCM с двумя ограничительными множествами

Тип архитектуры	Время синхронизации сетей A и B, измеряемое в количестве шагов	Время синхронизации сетей A и C, измеряемое в количестве шагов	Отношение времен (количества шагов) синхронизации сетей A и B ко времени сетей A и C
TPM	278,1	1209,3	0,230
TPCM ограничение весов в „форме" квадрата	2695,8	30428,2	0,089
TPCM ограничение весов в „форме" окружности	17668,1	408931	0,043

Биты, содержащиеся во входных значениях и преобразованные нейронными сетями, поддаются перемежению и рассеиванию. Это свойство может применяться для кодирования сообщений. Сети также имеют свойство односторонности. Оба этих свойства допускают вычисление хеш-функций, основанное на нейронной сети.

В этой главе разработана также *модель нейронной сети, предназначенной для вычисления хеш-функции* (CNNHF - Complex Neural Network

Hash Function, нейронная сеть для вычисления хеш-функции на основе комплексных чисел). Такая сеть основана на использовании алгебры комплексных чисел. Благодаря применению соответствующих функций хаоса (множество Жюлия (Julia), уравнение Даффинга (Duffing) и уравнение Хенона (Henon)), можно оптимизировать произведенные операции, что затрудняет атаку на хеш-функцию, спроектированную таким образом.

Предложенная модель CNNHF отличается также от известных использованием функций хаоса в качестве функции перехода. Благодаря специфике функций перехода, возможна программная реализация математических операций в арифметике целых чисел (в известных решениях необходимо было использовать числа с плавающей запятой), что обеспечивает более высокое быстродействие выполнения операций.

Таким образом, во-первых, представленные решения позволяют создавать более гибкие криптографические системы, что допускает выбор оптимальных решений. Во-вторых, предложенные решения существенным образом (см. таблицу 2) увеличивают безопасность криптографических систем на основе нейросетевых технологий.

В третьей главе представлены математические модели и архитектуры нейронных сетей на основе кватернионов и октониов.

С математической точки зрения кватернионы – это элементы некоммутативного расширения поля комплексных чисел. Архитектуру сети на основе кватернионов условно будем обозначать TPQM (от англ. Tree Parity Quaternion Machine, древовидная машина четности на основе кватернионов).

Разработана и исследована модель сети TPQM, позволяющая осуществлять согласование криптографического ключа (аналогично протоколу Диффи–Хеллмана). Она использует в своей конструкции кольцо кватернионов, что наделяет ее следующими свойствами:

– выход архитектуры имеет 8 разных величин;

– функция знака делит плоскость на 8 непересекающихся подмножеств (формула 14);

– множество, ограничивающее увеличение величины вектора весов, может принять любую форму.

Упомянутая в последнем анализе функция знака описывается соотношениями (14).

Как видим, отдельные точки выполняют роль аттракторов, «притягивая» точки, лежащие ближе всего к одному из возможных выходных состояний системы. Схематически это может быть представлено рисунком 4.

$$\sigma(q)=\begin{cases}(1,0,0,0),\ a_1=\max(\{a_1,a_2,a_3,a_4\})\wedge a_1\geq 0)\\(-1,0,0,0),a_1=\max(\{a_1,a_2,a_3,a_4\})\wedge a_1<0)\\(0,1,0,0),\ a_2=\max(\{a_1,a_2,a_3,a_4\})\wedge a_2\geq 0)\\(0,-1,0,0),a_2=\max(\{a_1,a_2,a_3,a_4\})\wedge a_2<0)\\(0,0,1,0),\ a_3=\max(\{a_1,a_2,a_3,a_4\})\wedge a_3\geq 0)\\(0,0,-1,0),a_3=\max(\{a_1,a_2,a_3,a_4\})\wedge a_3<0)\\(0,0,0,1),\ a_4=\max(\{a_1,a_2,a_3,a_4\})\wedge a_4\geq 0)\\(0,0,0,-1),a_4=\max(\{a_1,a_2,a_3,a_4\})\wedge a_4<0)\end{cases}, \quad (14)$$

где $q = (a_1, a_2, a_3, a_4)$ и $q \in Q$ (кольцо кватернионов).

Естественно, изображение полной диаграммы в пространстве R^4 не возможно. Вместе с тем эта одна пара (из четырех встречающихся в нашем множестве) вызывает деление пространства на точки, «притягиваемые» к каждому из двух элементов.

Рисунок 4 – Схематическое действие пары аттракторов в функции знака

Благодаря этому, оппоненту C труднее синхронизировать свой внутренний вектор весов с наблюдаемыми сетями. Следовательно, предлагаемое решение является более безопасным, чем в случае использования известной модели (TPM), а также предложенной и описанной во второй главе (TPCM).

Представлена архитектура TPQM, содержащая в своей конструкции кольцо кватернионов. Правильное определение действий и изоморфизм с любым расширением тела действительных чисел, подтверждается теоремой Фробениуса. Вдобавок, кватернионы являются заключительным расширением тела действительных чисел, выполняющим условие ассоциативной операции умножения.

Однако, если мы допустим ослабленное условие ассоциативности умножения, то можем использовать октонионы (числа Кэли) наравне с остальными кольцами (на основе теоремы Фробениуса). Это означает, что все действия сохраняют свой смысл и математическую корректность. Числа Кэли в алгебраическом смысле – это множество (сохраняющее ассоциативность умножения) расширения кватернионов. Таким образом, на основании сказанного, октонионы – это третье (после комплексных чисел и кватернионов) множество, которое возникло благодаря применению конструкции Кэли–Диксона (Cayley–Dickson) к действительным числам.

На основе теоремы Фробениуса разработана и исследована *модель сети TPOM* (англ. Tree Parity Octonion Machine, древовидная машина четности на основе октонионов), позволяющая осуществлять согласование криптографического ключа между двумя нейронными сетями. Она использует в своей конструкции числа Кэли (октонионы), что наделяет ее следующими свойствами:

– выход архитектуры имеет 16 разных величин;

– функция знака делит плоскость на 16 непересекающихся подмножеств;

– множество, ограничивающее увеличение величины вектора весов, может принять любую форму.

В этой главе разработана также *модель QNNHF* (англ. Quaternion Neural Network Hash Function, нейронная сеть на основе кватернионов для вычисления хеш-функции), исполняющая роль хеш-функции. Она основана на использовании кватернионов. Благодаря применению соответствующих функций хаоса, можно оптимизировать произведенные операции, что затруднит атаку на хеш-функцию.

В четвертой главе представлены компьютерные имитационные модели нейронных сетей, описанных во второй и третьей главах. Кроме того, представлены разработанные тесты, имитирующие процесс обмена ключами, позволяющие оценить уровень безопасности предложенных в главах 2 и 3 решений.

Таблица 2 – Сравнение времени синхронизации архитектур TPM, TPCM, TPQM, TPOM

Архитектура	Время синхронизации сетей *A* и *B* (*CA* и *CB*), измеряемое количеством шагов	Время синхронизации сетей *A* и *C* (*CA* и *CO*), измеряемое количеством шагов	Отношение времени синхронизации сетей *A* и *B* (*CA* и *CB*) и сетей *A* и *C* (*CA* и *CO*)
TPM	254,6	758,8	0,33553
TPCM	10438,8	97086,4	0,107521
TPQM	3705,2	310486,8	0,011934
TPOM	48279,4	219848696,6	0,00022

Проанализированы уровни безопасности и эффективности моделей, представляющих множество действительных чисел. Анализ проведенных опытов подтвердил более высокий уровень безопасности этих решений по отношению к известным решениям. Как показано, уровень (коэффициент) безопасности архитектуры TPCM в среднем в 3 раза превышает тот же параметр для известной архитектуры на основе целых действительных чисел; вместе с тем, тот же сравнительный параметр, характеризующий сети

сети TPQM и TPOM соответственно равен: примерно 28 и примерно 1500 (таблица 2).

Время обучения нейронных сетей зависит также от начального состояния векторов весов, которые выбираются случайным образом. Поэтому время синхронизации, представленное в таблицах 1- 2, отличается.

Также показано, что геометрическая атака (чрезвычайно эффективная в случае архитектуры TPM) не эффективна для сети, использующей в своей конструкции комплексные числа (таблица 3; (*) 1000000 – максимальное произведенное количество шагов, при котором оппонент C не смог синхронизироваться с наблюдаемыми сетями A и B).

Таблица 3 – Сравнение эффективности геометрической атаки в контексте безопасности архитектур TPM и TPCM

Архитектура	Время синхронизации сети A и B, измеряемое в количестве шагов	Время реализации геометрической атаки на сети A и B, измеряемое в количестве шагов
TPM	222,9	387,6
TPCM	2324,4	1000000(*)

Проанализирован вид безколлизионной (устойчивой) хеш-функции с использованием трех представленных во 2-й главе функций перехода. Опыты показали, что выбор соответствующей функции существенно влияет на безопасность предлагаемых в работе решений.

Обсуждены проблемы окончания процесса синхронизации. Проведенные испытания показали, что решения, основанные на использовании множеств действительных чисел, гарантируют более высокое качество процесса синхронизации двух сетей абонентов.

В конце главы предложено решение, улучшающее эффективность классических, объектных алгоритмов через максимальное ограничение количества вызываемых функций.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Разработаны базовая архитектура и математическая модель взаимодействующих между собой нейронных сетей на основе алгебры комплексных чисел (TPCM), позволяющие выполнять согласование криптографического ключа (аналогично протоколу Диффи–Хеллмана) двумя взаимодействующими между собой сторонами.

Новизна предложенных решений характеризуется следующими свойствами:

– выходной сигнал архитектуры может принимать 4 разных значения (в сравнении с 2-мя – для известной архитектуры TPM);

– функция знака делит плоскость анализируемых значений на 4 непересекающиеся подмножества (в сравнении с 2-мя);

– множество, ограничивающее увеличение величины вектора весов, может принять любую форму.

Коэффициент, характеризующий уровень безопасности архитектуры TPCM, в среднем в 3 раза превышает тот же параметр для известной архитектуры на основе целых действительных чисел [1–A–3–A, 6–A–8–A, 11–A].

2. Разработана модель нейронной сети, предназначенная для вычисления хеш-функции (CNNHF). Такая сеть основана на использовании алгебры комплексных чисел. Предложенная модель отличается от известных использованием функций хаоса в качестве функций перехода. Благодаря их специфике, возможна программная реализация математических операций в арифметике целых чисел (в известных решениях необходимо было использовать числа с плавающей запятой), что обеспечивает большее быстродействие выполнения операций.

Доказано, что выбор соответствующей функции хаоса (на основе уравнений Жюлиа, Даффинга и Хенона), исполняющей роль функции перехода, существенно влияет на безопасность всей системы криптографического преобразования информации, а также на ее эффективность [4–A, 5–A, 9–A, 10–A, 13–A].

3. Разработаны и исследованы модели сетей на основе кватернионов (TPQM) и октонионов (TPOM), являющихся дальнейшим расширением поля используемых чисел и позволяющих осуществлять согласование криптографического ключа между двумя сетями (аналогично протоколу Диффи–Хеллмана).

Новизна предложенных решений (в сравнении с известной архитектурой и моделью TPM) характеризуется следующими свойствами (соответственно для архитектур TPQM и TPOM):

– выходной сигнал архитектуры принимает одно из 8 либо 16 разных значений;

– функция знака делит плоскость всех значений на 8 либо на 16 непересекающихся подмножеств;

– множество, ограничивающее увеличение величины вектора весов, может принять любую форму.

На основе экспериментального имитационного моделирования показано, что безопасность предложенных архитектур сетей повышается при-

мерно соответственно в 28 и 1500 раз в сравнении с известными решениями.

Показано, что модели на основе более сложных множеств используемых чисел позволяют получить более высокое качество окончания процесса синхронизации [3–А, 11–А, 12–А]

4. Разработана компьютерная имитационная модель в среде объектно-ориентированного программирования, позволяющая оценить в динамике свойства и параметры предложенных моделей и соответствующих архитектур нейронных сетей, предназначенных для передачи и криптографического преобразования информации [5–А, 11–А, 12–А, 14–А].

Таким образом, все предложенные решения используют архитектуру искусственных нейронных сетей. Эти решения основываются на довольно хорошо изученных теоретических положениях. Также эти решения не имеют неясных утверждений, как в случае классических моделей. Например, протокол Диффи–Хеллмана опирается на проблему дискретного логарифма, которая может быть когда-либо решена. Предложенные же в этой работе решения построены на основе нейронных сетей и алгоритмов, которые останутся безопасными даже в случае создания квантового компьютера (позволяющего эффективно производить факторизацию чисел).

Существенным достоинством таких решений, является возможность динамичного испытания нейронных сетей. Это позволит применять все более эффективные и гибкие решения, делая нейро-криптографические модели более безопасными.

Рекомендация по практическому использованию результатов

Разработанные модели и алгоритмы могут быть использованы в компьютерных криптографических системах передачи информации, в системах обмена ключами, а также в системах, требующих проведения операций хеширования. Результаты, полученные в ходе диссертационного исследования, внедрены на предприятии г. Лукова (Польша) при разработке сетевого программного обеспечения, а также при выполнении НИР ГБ 26-114 и в учебном процессе на кафедре информационных систем и технологий УО «Белорусский государственный технологический университет», на кафедре операционных и сетевых систем Люблинского католического университета (Польша).

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в научных журналах

1–А. Plonkowski, M. Trainig neural network for pattern recognition / M. Plonkowski // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – БГТУ, 2004. – С. 149–156.

2–А. Плонковски, М. Использование нейронных сетей в системах криптографического преобразования информации / М. Плонковски, П.Урбанович// Известия Белорусской инженерной академии. – 2004. – № 1 (17)/4. – Р. 13–15.

3–А. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологии / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – БГТУ, 2005. – С. 161–164.

4–А. Плонковски, М. Использование нейронных сетей в операциях над хеш-функциями / М. Плонковски // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – БГТУ, 2007. – С. 169–171.

5–А. Płonkowski, M. Analiza funkcji chaosu w funkcjach skrótu opartych na sieciach neuronowych/ M. Płonkowski // Przegląd Elektrotechniczny, ISSN 0033-2097. – R. 84. – 2008. – N 3. – P. 102–104.

6–А. Карчмарски, Д. Методы и алгоритмы моделирования систем криптопреобразования информации на основе нейросетевых технологий / Д. Карчмарски, М. Плонковски, Е. В. Лисица // Труды БГТУ. Сер. VI, Физ.-Мат. науки и информ. – 2008. – Вып. XVI. – С. 137–140.

Материалы конференций и тезисы докладов

7–А. Плонковски, М. Синхронизация криптографических ключей на основе нейросетевых технологий / М. Плонковски, Д. П. Урбанович // Материалы Междунар. науч.-практ. конф., апрель 2006г. / Брест. гос. ун-т им. А. С. Пушкина. – Брест: Изд-во БрГУ. – С. 29.

8–А. Урбанович, Д. П. Безопасность транзакций в компьютерных системах / Д. П. Урбанович, М. Плонковски // Материалы Междунар. науч.-практ. конф., апрель 2006г. / Брест. гос. ун-т им. А. С. Пушкина. – Брест: Изд-во БрГУ. – С. 37.

9–А. Плонковски, М. Хеширование функции в системах e–commerce на основе нейросетевых технологии / М. Плонковски, Д. П. Урбанович //

Материалы Междунар. науч.-практ. конф., апрель 2006г. / Брест. гос. ун-т им. А. С. Пушкина. – Брест: Изд-во БрГУ. – С. 68.

10–А. Урбанович, Д. П. Защита электронных транзакции в системах e–commerce / Д. П. Урбанович, М. Плонковски // Материалы Междунар. науч.-практ. конф., апрель 2006г. / Брест. гос. ун-т им. А. С. Пушкина. – Брест: Изд-во БрГУ. – С. 75.

11–A. Plonkowski, M. Algebraic aspects of mutual learning of neural networks / M. Plonkowski // New Electrical and Electronic Technologies and Their Industrial Implementation, Zakopane, Poland, 21–24 June. – 2005. – P. 125–127.

12–A. Płonkowski, M. Wykorzystanie ataku geometrycznego do kryptoanalizy procesu synchronizacji architektur TPCM / M. Płonkowski // Materiały XII Środowiskowej Konferencji Matematyczno-Informatycznej Rzeszów, Lublin - Chełm - Łuck, 2–5 VII 2006. – P. 34-36.

13–A. Płonkowski, M. Funkcja skrótu oparta na architekturze zespolonej sieci neuronowej / M. Płonkowski // Materiały XIII Międzynarodowej Konferencji Matematyczno-Informatycznej, Chełmie, 1-4 lipca, 2007. – P. 47-51

14–A. Plonkowski, M. Analysis of chaotic map in hash functions based on neural networks / M. Plonkowski // New Electrical and Electronic Technologies and Their Industrial Implementation – NEET' 2007: proc. of the 5-th Intern. conf., Zakopane, Poland, 12-15 June 2007; ed. T. Kołtunowicz. – Lublin, 2007. – P. 43.

РЭЗЮМЭ

Планкоўскі Марцін Даніел

МАДЭЛІ ПЕРАДАЧЫ І КРЫПТАГРАФІЧНАГА ПЕРАЎТВАРЭННЯ ІНФАРМАЦЫІ НА ПАДСТАВЕ НЕЙРАСЕТКАВЫХ ТЭХНАЛОГІЙ І ПАШЫРЭННЯ ПОЛЯ ВЫКАРЫСТОЎВАЕМЫХ ЛІЧБАЎ

Ключавыя словы: крыптаграфія, нейронныя сеткі, бяспека, сінхранізацыя персяптронаў, абмен ключамі, хэш-функцыя.

Мэтай працы з'яўляецца тэарэтычнае абгрунтаванне і распрацоўка мадэляў нейронных сетак на падставе пашырэння поля выкарыстоўваемых для іх апісання лічбаў у сістемах перадачы канфідэнцаяльнай інфармацыі, а таксама нейронных сетак, выкарыстоўваемых у якасці хэш-функцыі. Аб'ектамі даследаванняў з'яўляюцца структуры нейронных сетак, выкарыстоўваемых у галіне крыптаграфіі. Прадметам – мадэлі і алгарытмы абмена ключамі і генерацыі крыптаграфічнай хэш-функцыі на падставе нейрасеткавых тэхналогій. Метады даследавання грунтуюцца на становішчах тэорыі верагоднасці, тэорыі кадавання інфармацыі, тэорыі нейронных сетак, матэматычнага і кампутарнага мадэлявання.

Атрыманыя вынікі і іх навізна

Распрацавана новая мадэль нейронных сетак, якая заснавана на паслядоўным пашырэнні поля выкарыстоўваемых лічб (з выкарыстаннем канструкцыі Кэлі–Дзіксана (Cayley–Dickson construction)), дазваляючая ўзгодніць крыптаграфічны ключ (як і ў выпадку пратаколу Дзіффі–Хэллмана). Яна адрозніваецца ад існуючых мадэляў значна больш высокім ўзроўнем бяспекі, а таксама большай гібкасцю (дынамічнасцю) пры выбары параметраў самой архітэктуры. Распрацавана мадэль нейроннай сеткі, якая дазваляе хэшыраваць (сціскаць) тэксты любой даўжыні. У структуры нейроннай сеткі выкарыстаны комплексныя лічбы, кватэрніёны. Ад існуючых мадэляў яе адрозніваецца магчымасць адвольнага выбару функцыі пераходу. Дзякуючы гэтаму, магчыма выбраць варыянт з больш высокім узроўнем бяспекі. Створана рэалізацыя нейронных сетак, якая дазваляе больш эфектыўна абменьвацца крыптаграфічнымі ключамі.

Вынікі, атрыманыя падчас даследавання, выкарыстоўваюцца на прадпрыемстве «Twoj Swiat» г. Лукава (Польшча) пры распрацоўцы сеткавага праграмнага забеспячэння, а таксама пры выкананні НДР ГБ 26-114 і ў навучальным працэсе на кафедры інфармацыйных сістэм і тэхналогій УА «Беларускі дзяржаўны тэхналагічны універсітэт», на кафедры аперацыйных і сеткавых сістэмаў Люблінскага каталіцкага універсітэта (Польшча).

РЕЗЮМЕ

Плонковски Мартин Даниел

МОДЕЛИ ПЕРЕДАЧИ И КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ И РАСШИРЕНИЯ ПОЛЯ ИСПОЛЬЗУЕМЫХ ЧИСЕЛ

Ключевые слова: нейронные сети, синхронизация персептронов, обмен ключами, хеш-функции.

Целью работы является теоретическое обоснование и разработка моделей нейронных сетей на основе расширения поля используемых для их описания чисел в системах передачи конфиденциальной информации, а также нейронных сетей, используемых в качестве хеш-функции. Объектами исследований являются структуры нейронных сетей, используемых в области криптографии. Предметом – модели и алгоритмы обмена ключами и генерации криптографической хеш-функции на основе нейросетевых технологий. Методы исследования базируются на положениях теории вероятностей, теории кодирования информации, теории нейронных сетей, математического и компьютерного моделирования.

Полученные результаты и их новизна

Разработана новая модель нейронных сетей, основанная на последовательном расширении поля действительных чисел (с использованием конструкции Кэли–Диксона (Cayley–Dickson construction)), позволяющая согласовать криптографический ключ (как в случае с протоколом Диффи–Хеллмана). Она отличается от существующих моделей более высоким уровнем безопасности, а также большей гибкостью (динамичностью) при выборе параметров самой архитектуры. Разработана модель нейронной сети, позволяющая хешировать (сжимать) тексты любой длины. В структуре нейронной сети использованы комплексные числа и кватернионы. От существующих моделей ее отличает возможность свободного выбора функции перехода. Благодаря этому, возможен выбор варианта с более высоким уровнем быстродействия. Разработана реализация нейронных сетей, позволяющая эффективно обмениваться криптографическими ключами.

Результаты, полученные в ходе диссертационного исследования, внедрены на предприятии «Twoj Swiat» г. Лукова (Польша) при разработке сетевого программного обеспечения, а также при выполнении НИР ГБ 26-114 и в учебном процессе на кафедре информационных систем и технологий УО «Белорусский государственный технологический университет», на кафедре операционных и сетевых систем Люблинского католического университета (Польша).

RESUME

Plonkowski Marcin Daniel

TRANSFER MODELS AND CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION BASED ON NEURAL NETWORK TECHNOLOGIES AND FIELD EXTENSION OF NUMBERS USED

Key words: neural networks, synchronization, key exchange, hash function.

The purpose of the work is to present the theoretical substantiation and development of neural networks models based on the field extension of numbers used for their description in confidential information transfer systems and to present neural networks used as hash function. The structures of neural networks used in the field of cryptography are the object of the research. The subject focuses on models and algorithms of keys' setup and of cryptographic hash function generation on the basis of neural networks technologies. Methods and researches are based on positions of probability theory, information coding theory, theory of neural networks, mathematical and computer modeling.

Results and their originality

A new model of neural networks was developed: model is based on consecutive field extensions of real numbers (with the use of Cayley–Dickson's construction), which allows a setup of cryptographic key (as in the case of Diffie-Hellman's protocol). It differs from the existing models in that it has a much higher level of safety and greater flexibility (dynamism) when it comes to the choice of architecture parameters. A model of neural network which makes it possible to hash (to compress) texts of any length was developed. Complex numbers and quaternions were used in the neural network structure. It differs from the existing models in that it offers greater flexibility of transition function. It is, therefore, possible to select a variant with a higher level of safety. Implementation of neural networks allowing an efficient exchange of cryptographic keys and cryptographic compression of texts of any length was developed.

The results obtained during the research were implemented in the «Twoj Swiat» company (town of Lukov, Poland) in the development of network software, also in the process of carrying out NIR GB 26-114 and educational projects in the Department of Information Systems and Technologies of the Belarus State Technological University and in the Department of Operations and Network Systems of the Catholic University of Lublin.

Научное издание

ПЛЮНКОВСКИ Мартин Даниел

МОДЕЛИ ПЕРЕДАЧИ И КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ И РАСШИРЕНИЯ ПОЛЯ ИСПОЛЬЗУЕМЫХ ЧИСЕЛ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Подписано в печать	21.04.2009.	Формат 60x84 $^1/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Печать ризографическая.		Усл. печ. л. 1,63.
Уч.-изд. л. 1,4.	Тираж 60 экз.		Заказ 265.

Издатель и полиграфическое исполнение: Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0131666 от 30.04.2004. 220013, Минск, П. Бровки, 6.