Плюсы [2] данного метода в устойчивости к зашумлению данных и в быстром и неуправляемом обучении. Минусы метода в том, что результат работы нейронных сетей зависит от начальных установок сети.

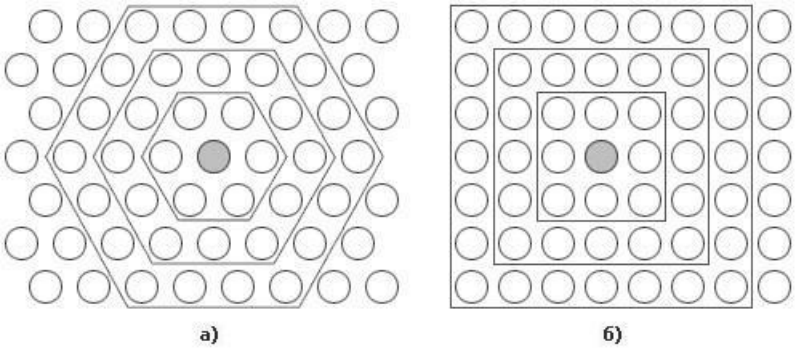

Рисунок 2 – Расстояние между нейронами на карте для шестиугольной (а) и четырехугольной (б) сеток

Рассмотренная нейронная сеть лучше всего подходит для данной задачи. Важнейшим отличием этой сети от других аналогов является то, что все нейроны упорядочены в одно- либо двумерную сетку, при этом в ходе обучения изменяется не только нейрон – победитель, но и в меньшой степени его соседи. За счёт этого самоорганизующуюся карту Кохонена можно считать методом проецирования многомерного пространства в пространство с более низкой размерностью. Это является важным аспектом в реализации данной задачи, так как самой большой проблемой задачи является потеря качества при выделении мелких деталей переднего плана.

Список использованных источников:

1. Уоссермен, Ф. Нейрокомпьютерная техника / Ф. Уоссерман // М.: Мир, 1992. – 58с.
2. Ежов. А, Шумский. С. Нейрокомпьютинг и его применение в экономике и бизнесе / А. Ежов, С. Шумский // М.: Мифи, 1998 – 87с.

ВЫСОКОСКОРОСТНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ ХЭШ-ФУНКЦИЙ НА БАЗЕ FPGA

Гридюшко А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Качинский М.В. – к.т.н.,доцент

В связи с быстрым развитием технологий в области беспроводной связи и систем персональной связи обеспечение информационной безопасности становится все более важной задачей. Криптографические хэш-функции используются для защиты целостности и подлинности информации в широком спектре приложений.

Хэш-функции используются в качестве «строительных блоков» в различных криптографических приложениях. Наиболее важными областями применения являются защита аутентификации информации и являются инструментом для схем цифровой подписи. Хэш-функция - это функция, которая отображает вход произвольной длины в фиксированное количество выходных битов, значение хэш-функции. Хэш-функции можно разделить на следующие две основные категории:

1) односторонние хэш-функции – функции, которые должны быть устойчивыми к прообразу и второму прообразу, то есть должно быть трудно найти сообщение с данным хэшем (прообразом) или хэширующим до того же значения, что и данное сообщение (второй прообраз);
2) устойчивые к коллизиям, т.е. односторонние хэш-функции, для которых трудно найти два разных сообщения, которые хэшируют одно и то же значение.

Большинство хэш-функций предназначены для работы в качестве итерационных процессов, которые хэшируют входные сообщения произвольной длины. Эти функции обрабатывают блоки входных данных фиксированного размера и выдают хэш-значение заданной длины (рис. 1).

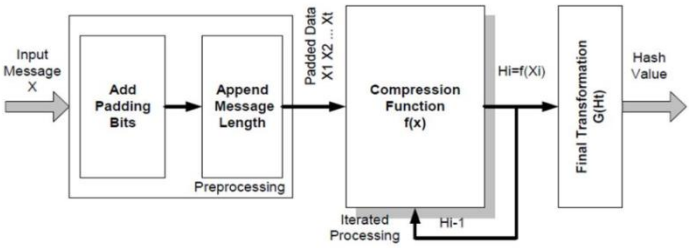

Рисунок 1 –Общая модель хэш-функции.

Процедура разделена на предварительную обработку, сжатие и окончательное преобразование. Предварительная обработка в основном добавляет необходимое количество битов к входному сообщению, чтобы сформировать заполненный блок данных заданной длины. Дополненные данные делятся на t блоков одинаковой длины. Каждый блок X_i служит входом для функции сжатия h, которая каждый раз вычисляет новое преобразованное сообщение данных H_i, как функцию предыдущего H_{i-1} и входного X_i. После определенного количества циклов обработки данные окончательно модифицируются в результате окончательного преобразования. Таким образом генерируется хэш-значение (дайджест сообщения), соответствующее входному сообщению x. Предложенная архитектура гарантирует высокий уровень безопасности во всех приложениях, требующих аутентификации сообщения, посредством создания кода аутентификации сообщения. Уровень безопасности и преимущества хэш-функции SHA-2, на которой основана предложенная архитектура, обеспечивают высокий уровень безопасности. При реализации этой схемы аутентификации Хэш-функция SHA-2 представляет собой криптографические алгоритмы, которые принимают в качестве входных данных сообщение произвольной длины, и которые возвращают дайджест (или хэш-значение) фиксированной длины (от 160 до 512 бит в большинстве приложений). Хэш-функции используются во множестве протоколов, будь то для цифровых подписей на высокопроизводительных серверах или для аутентификации встроенных систем

Список использованных источников:

1. Качинский, М. В. Конвейерный процессор хэш-функции SHA-256 / М. В. Качинский, А. В. Станкевич // Информационные технологии и системы 2018 (ИТС 2018) = Information Technologies and Systems 2018 (ITS 2018) : материалы международной научной конференции, Минск, 25 октября 2018 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2018. – С. 158 - 159.

2. Качинский, М. В. Высокопроизводительная реализация криптографической хэш-функции SHA-256 на базе FPGA / М. В. Качинский, А. В. Станкевич // Технические средства защиты информации : тезисы докладов XVI Белорусско-российской научно – технической конференции, Минск, 5 июня 2018 г. – Минск: БГУИР, 2017. – С. 47.

3. Xiao-yang Zeng, Shi-tingLu, "A core-based multi-function security processor with GALS Wrapper",Solid-State and Integrated-Circuit Technology 2008. ICSICT 2008. 9th International Conference on, pp. 1839-1842, 2008.

ЛОГИЧЕСКАЯ ОПТИМИЗАЦИЯ НЕПОЛНОСТЬЮ ОПРЕДЕЛЁННЫХ ФУНКЦИЙ

Грицовец А.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бибило П.Н. – д.т.н., профессор

С каждым днём задачи проектирования цифровой аппаратуры становятся более объёмными, а требования к электронным вычислительным средствам по габаритам и затраченным ресурсам становятся всё жёсткими. Многие функциональные блоки управляющих и вычислительных устройств описываются булевыми функциями, поэтому оптимизация различных форм представлений систем булевых функций по-прежнему остается актуальной задачей.

На сегодняшний день многие задачи требуют большей производительности при меньших затратах при производстве электронных вычислительных средств. Производители стараются найти наилучшее решение при проектировании устройств. Для выполнения этой задачи часто прибегают к логической оптимизации булевых функций, которые являются математическими моделями функционирования многовыходных комбинационных схем.

Один из подходов к оптимизации булевых функций – аппарат диаграмм двоичного выбора [1-5]. Диаграммы двоичного выбора – компактная форма представления булевых функций в виде ациклического графа, которая соответствует многоуровневому представлению на базе разложения Шеннона. В начале логической оптимизации булевых функций на основе диаграмм двоичного выбора