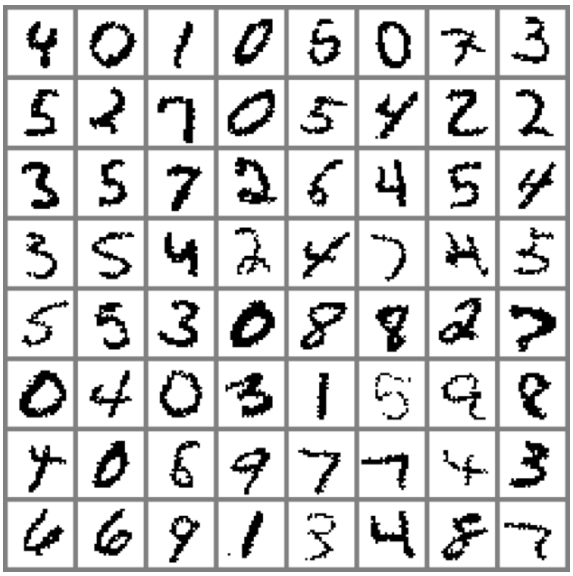
шаблонов различных классов. В случаях, когда структура сети правильно разработана и размер обучающего набора достаточно велик, нейронные сети способны показать высокую точность при классификации данных, не проходящих ранее через эту сеть. В виду широкого распространения и большой популярности нейронных сетей, имеется большой интерес к методам ускорения процесса их обучения. Отдельно стоит вопрос повышения обобщающей способности нейронной сети.

Среди множества обучающих алгоритмов, которые предложены для нейронных сетей со сложным соединением, метод обратного распространения (Back-Propagation), вероятно, является самым распространенным. Необходимо определиться с двумя измерениями производительности, скоростью обучения и обучающей способностью, во время тестирования обучающего алгоритма. Обобщение определяет количество данных, необходимое для обучения системы таким образом, чтобы система корректно реагировала на входные данные, которые не были представлены в обучающем наборе.

Для распознавания изображений использованы следующие нейронные сети: 1) однослойная нейронная сеть; 2) двухслойная полностью соединенная нейронная сеть; 3) сверточная нейронная сеть. Проведен сравнительный анализ результатов работ этих сетей.

Для обучения и тестирования использованы базы данных MNIST[2], в которых представлены рукописные изображения цифр 0-9 (рис. 1), принадлежащих различным авторам.



Риуснок 1 – Рукописные изображения

Список использованных источников:

1. le Cun, Y. A theoretical framework for back-propagation / Y. le Cun. – CMU, Pittsburgh, 1988.
2. База данных рукописных символов (цифр) MNIST. [Электронный ресурс] / – Режим доступа: http://yann.lecun.com/exdb/mnist/

КОНВЕЙЕРНЫЙ ПРОЦЕССОР АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ХЭШИРОВАНИЯ SHA-1 НА БАЗЕ FPGA

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

Листопад Е. В.

Петровский А. А. – д-р. техн. наук, профессор

При построении современных встраиваемых вычислительных систем реального времени одной из главных задач является эффективная аппаратная реализация различных криптографических функций и алгоритмов, в том числе алгоритмов хэширования. Это обязывает к применению различных архитектурных вариантов их построения, одним из которых является конвейерный процессор.

Известные на сегодняшний день различные аппаратные реализации алгоритма SHA-1 имеют преимущественно итеративную архитектуру, использующую только один блок обработки данных, который реализует один шаг алгоритма SHA-1. Такая архитектура обеспечивает минимальное использование ресурсов FPGA, однако, и минимальное быстродействие. Для определенного класса задач требуется максимальное быстродействие процесса хэширования, которое обеспечивается аппаратными реализациями алгоритма SHA-1, имеющими конвейерную архитектуру вычислений.

Алгоритм хэширования SHA-1 выполняется в четыре этапа по 20 операций в каждом. Определяются четыре нелинейные операции $F_t(m,l,k)$ и четыре константы K_t. Блок сообщения преобразуется из 16 32-битовых слов M_t в 80 32-битовых слов W_t по следующему правилу:

$$W_t = M_t \qquad 0 \le t \le 15$$

$$W_t = W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16} <<1 \qquad 16 \le t \le 79$$

Первоначально значения регистров A,B,C,D,E сохраняются во временных переменных. Затем, на каждом шаге $t = 0,\ldots,79$ выполняются требуемые действия (Рисунок 1). На рисунке 2 приведена структурная схема вычислительного блока конвейерного процессора алгоритма SHA-1.

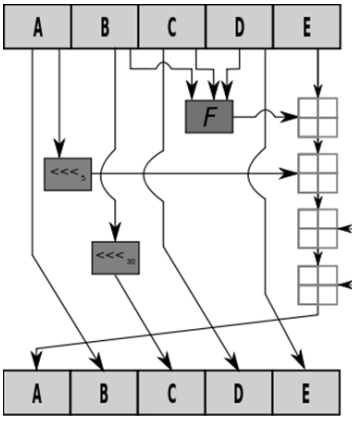


Рис. 1 – Схема выполнения одной итерации алгоритма SHA-1

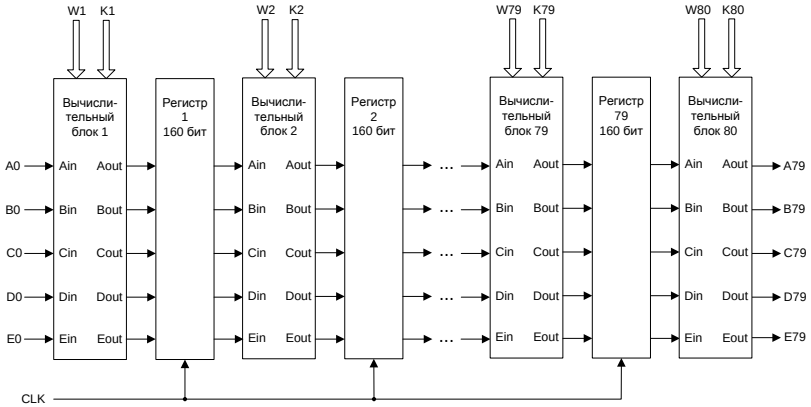


Рис. 2 – 80-ступенчатый конвейерный процессор

В конвейерном процессоре используется 80 вычислительных блоков по одному на каждый шаг алгоритма SHA-1. В результате цикл вычисления хэша разворачивается во времени, образуя конвейерную (поточную) структуру. В такой структуре одновременно вычисляются хэши 80 входных сообщений, причем первый хэш получается через 82 такта, а последующие – в каждом такте.

Реализация процессора осуществлялась для кристалла FPGA xc5vlx110-1ff1153 для случая длины входного сообщения менее размера одного блока данных алгоритма SHA-1 (512 бит). Реализация процессора требует 40% ресурсов кристалла (slices), имеет тактовую частоту 195 МГц и пропускную способность 99,8 Гбит/с, что позволяет использовать ее при построении специализированных вычислительных систем реального времени.

Список использованных источников:

1. Nalini C. Iyer, Sagarika Mandal, Implementation of Secure Hash Algorithm-1 using FPGA // Dept. of Electronics and Communication Engineering, 2013. P. 757-764.
2. Murat Askar, Tugba Siltu Celebi, Design and FPGA Implementation of Hash Processor // ISC Turkey, 2007. P. 85-89.

ЗАРЯДНОЕ УСТРОЙСТВО НА БАЗЕ МИКРОКОНТРОЛЛЕРА

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

Рёмин В.А.

Качинский М.В. – канд. техн. наук, доцент

На сегодняшний день существует множество переносных и носимых ЭВС, питание которых осуществляется от встроенного источника. Зачастую этим источником является аккумуляторная батарея (далее АКБ). Разнообразие форм, размеров и питающих напряжений всех устройств делает невозможным унификацию питающих элементов или АКБ. На сегодняшний день существует огромное количество устройств, производимых в азиатских странах, в которых для удешевления конструкции зачастую используются нестандартные или несертифицированные АКБ. Для зарядки всего разнообразия устройств существует большое количество зарядных, которые так же могут быть унифицированными (например, порт USB 5V 0.5-1A) и уникальными. Также очень часто встречается ситуация, когда попросту невозможно определить номинал аккумулятора (например, из вышедшего из производства устройства, или несерти-