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.

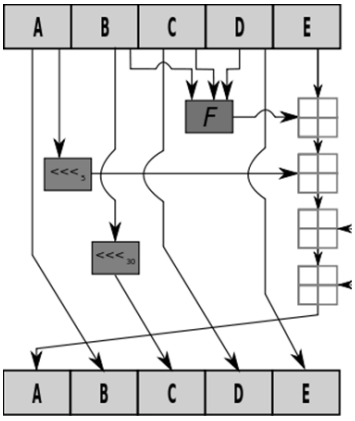

Рис. 1 – Схема выполнения одной итерации алгоритма SHA-1

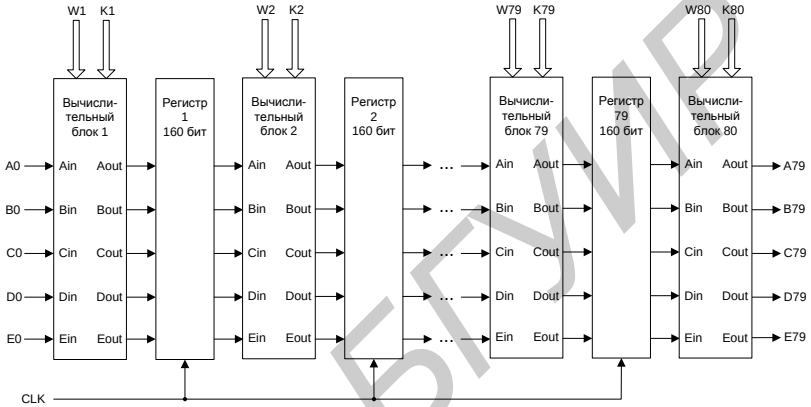

Рис. 2 – 80-ступенчатый конвейерный процессор

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-

фицированного). Для упрощения пользования и уменьшения номенклатуры зарядных устройств было принято решение о разработке устройства, которое сможет зарядить абсолютно любую АКБ в автоматическом режиме.

Разработка подобного устройства подразумевает использование различных подходов и способов для достижения той автоматизации, о которой говорилось выше. Для определения зарядного тока для любой АКБ необходимо оценить номинальную или хотя бы остаточную ёмкость батареи, поскольку требования к зарядке практически всех АКБ подразумевают благоприятный режим зарядки, ток при котором составит 0,1С, где С – номинальная емкость АКБ. В данном случае можно использовать три различных алгоритма:

- определение емкости, путем разрядки АКБ (даже разряженной) используя операционный усилитель и измерение падения напряжения на эталонном резисторе (рисунок 1), что позволит по закону Ома определить максимальный отдаваемый ток и, используя микроконтроллер (далее - МК), определить по простейшим математическим формулам емкость АКБ – данный способ является наиболее очевидным и понятным;
- определение емкости методом сравнения емкости измеряемой АКБ с известной емкостью эталонного конденсатора. В этом способе путем измерения напряжения на измеряемой АКБ и разряде его на конденсаторную нагрузку измеряется время заряда конденсатора известной емкости и рассчитывается ёмкость измеряемого АКБ по формуле:

$$Q = \frac{CU}{2tK},$$

где Q − электрическая ёмкость измеряемой АКБ, C − ёмкость эталонного конденсатора, t − время заряда конденсатора от измеряемого АКБ, K − коэф., учитывающий конструктивные и технологические особенности

- определение внутреннего сопротивления АКБ. По сути, величина снижения напряжение на АКБ при протекании тока определяется внутренним сопротивлением. Ёмкость АКБ связана с ее внутренним сопротивлением и, получив опытным путем значение внутреннего сопротивления можно оценить и ёмкость АКБ. Если внутреннее сопротивление АКБ увеличилось в 2 раза – значит емкость упала в 2 раза.

Когда становится известной ёмкость АКБ, встает вопрос регулировки тока в схеме. В данном случае используется первый закон Кирхгофа (рисунок 2), который позволяет разбить ток в проводнике на его составляющие, потом каждой получившейся ветвью можно управлять тиристорными и транзисторными ключами с помощью МК. И на выходе все эти ветвь снова будут сходиться по первому закону Кирхгофа. Таким образом, можно управлять током, протекающим в цепи, поскольку каждая ветвь будет пропускать строго ограниченный ток.

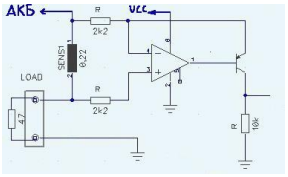

Рисунок 1 – Пример реализации разрядки

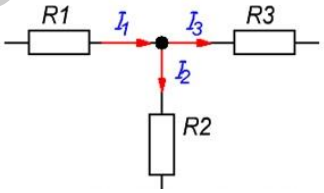

Рисунок 2 –Пример 1-го закона Кирхгофа

После регулировки зарядного тока в схеме остается задача подбора необходимого напряжения. Здесь реализован метод последовательного приближения. Схема имеет несколько выходных каскадов, которые представляют собой стабилизаторы напряжения. Каждый каскад подключен к питающей схеме, выход которой есть сумма токов, посредством управляемого реле. Метод последовательного приближения позволяет МК отслеживать «местонахождение» напряжения на АКБ на экспоненциальном графике, который будет индивидуальным для каждого каскада. При зарядке будет происходить рост напряжения. При приближении напряжения к пороговому, будет происходить переход на другой диапазон напряжений с помощью управляемого реле, т.е. на другой выходной каскад, который имеет более высокое напряжение. И далее МК будет снова отслеживать рост напряжения на АКБ, и при необходимости данная процедура повторится. Окончание зарядки МК будет отслеживать по существенному снижению роста напряжения (снова по экспоненциальному закону), по окончании зарядки подразумевается снижение зарядного тока до 0,05С для поддержания АКБ заряженной.

Таким образом, использование данного устройства позволяет автоматизировать процесс зарядки АКБ, позволяет заменить большую номенклатуру зарядных устройств на одно и позволяет заряжать АКБ с неизвестными ТТХ. Такой вид зарядного устройства позволяет использовать его людям, не имеющим технического образования. Безопасность зарядки будет контролировать датчик температуры, закрепленный на АКБ (к примеру присоской), который при нагреве АКБ первоначально снизит зарядный ток, а при дальнейшем росте температуры прекратит зарядку, после снижения температуры зарядка начнется сначала.

Список использованных источников:

1. Ходасевич, А. Г. Зарядные устройства : информационный обзор / А. Г. Ходасевич, Т.И. Ходасевич – Москва: НТ