разбиения на ступени следующий: каждая ступень должна содержать один вычислительный блок SHA-1, поскольку он имеет наибольшую временную задержку. На первой ступени конвейера два блока SHA-1 работают параллельно. На остальных ступенях, кроме последней, блок SHA-1 работает параллельно с блоком задержки. На последней ступени работает один блок SHA-1.

Кроме того, на первой ступени начальными значениями переменных состояния A, B, C, D, E являются константы (на остальных ступенях это результат обработки предыдущей ступени), что учитывается при разработке упрощенной структуры вычислительного блока SHA-1 специально для этой ступени.

Рассматриваемая архитектура обеспечивает самую высокую скорость вычисления MAC-значения, однако, требует максимального использования ресурсов FPGA по сравнению с другими вариантами.

АНАЛИЗ МЕТОДОВ ПАРАМЕТРИЗАЦИИ ЛИНИЙ НА ИЗОБРАЖЕНИЯХ

Д.И. Кирилюк, А.В. Костусев, Ю.И. Кулаженко

В настоящее время в связи с развитием мобильных систем наблюдения специального назначения стоит актуальная задача – обработка изображений в реальном масштабе времени. Для ее решения широко используются методы, которые учитывают распределение градиента яркости в окрестностях реперных точек. Однако, в условиях проекционных искажений эффективность градиентного подхода снижается. Устранение данного недостатка возможно за счет геометрического подхода. Геометрические методы применялись в задачах для обработки изображений, имеющих искусственную природу (например, печатные платы, детали конструкций, САПР). Поэтому актуальной задачей в настоящее время является модернизация существующих геометрических методов и создание новых методов для обработки изображений, имеющих естественный характер (например, спутниковые, ландшафтные). Целью настоящей работы является теоретический анализ методов геометрической параметризации линий на изображениях.

Основными требованиями к дескрипторам линий являются: устойчивость к проективным преобразованиям; устойчивость к шуму; высокая скорость формирования; произвольность формы кривой. Теоретический анализ показал, что для решения поставленной задачи, с учетом вышеуказанных требований, наиболее эффективны методы на основе Фурье-дескрипторов, сигнатур или цепных кодов.

Методы на основе Фурье-дескрипторов используют дискретное преобразование Фурье конечной последовательности комплексных чисел (координаты точек рассматриваются как комплексные числа), позволяют по коэффициентам преобразований восстановить линию.

Сигнатуры – одномерные функции, взаимно-однозначно определяющие кривую линию, строятся относительно некоторой фиксированной точки (центра). Особенностью цепных кодов является кодирование направлений и длин прямых отрезков линии.

Вычислительная сложность вышеназванных методов примерно одинаковая. Методы на основе Фурье-дескрипторов устойчивы к повороту, параллельному переносу. Устойчивость методов на основе сигнатур и цепных кодов зависит от выбора фиксированной (начальной) точки.

БЕЗОПАСНОСТЬ USB УСТРОЙСТВ

М.И. Кошевник

Цель исследования – оценить безопасность USB устройств от различного вида угроз.

В ходе работы установлено, что клавиатура отправляет данные о всех исходящих событиях, а в качестве входящих принимает только сведения о состоянии светодиодов – NumLock, CapsLock, ScrollLock. Данное ограничение заложено на уровне операционной системы, что не позволяет организовать аппаратный шпион – аналог программного кейлоггера.

В процессе исследования выявлено, что USB устройства, относящиеся к классу Human Input Device, подвержены разного рода уязвимостям. Так, данные с web-камеры, работающей по принципу постоянного приёма запросов о захвате кадров, могут быть получены в промежуточный момент между запросами.

Драйвер микроконтроллера USB-Flash, находящийся во встроенном ROM, может быть модифицирован в корыстных целях. Операционная система по умолчанию устанавливает драйвера

любых новых устройств вне зависимости от прав пользователя, ведущего в данный момент сеанс работы.

Проведя исследование, определив возможные угрозы и уязвимости было принято решение о создании устройства, обеспечивающего защиту от программных кейлоггеров, работающих в операционной системе. На базе микроконтроллера Arduino организованы приём событий от физической клавиатуры, модификация этих данных и последующая передача операционной системе. Подготовленное программное обеспечение, работающее в операционной системе, в свою очередь, проводит обратную модификацию и передаёт введённые пользователем данные в защищаемое приложение. Таким образом, данные, которые поступят в кейлоггер, будут находиться в модифицированном виде.

БЕЗОПАСНОСТЬ BLUETOOTH УСТРОЙСТВ

В.А. Кузьменко

Цель исследования — оценить безопасность передачи данных по Bluetooth.

В процессе исследования было выявлено следующее:

– передача данных по Bluetooth защищается PIN кодом на устройствах, поддерживающих Bluetooth версии 2.0 и выше.

– данные шифруются 128-битным AES алгоритмом на устройствах, поддерживающих Bluetooth версию 4.0 и выше.

– устройства инициируют пересопряжение, если на частоту, в которой они работают, начинает влиять неизвестный пользователь. Однако если нет свободных частот в диапазоне Bluetooth, то имеется возможность «подслушать» ключ сопряжения и методом подбора взломать PIN код.

Таким образом, сформирована рекомендация пользователям: в случае использования технологии Bluetooth для передачи данных, требующих шифрование, необходимо самостоятельно осуществлять шифрование таких данных.

Также в ходе исследования было разработано приложение, обеспечивающее безопасность рабочего места персонального компьютера на основе контроля наличия рядом ключевого Bluetooth устройства. Данное приложение позволяет также удаленно подавать команды управления с мобильного телефона на компьютер в зашифрованном виде. При разработке приложения использовалось программно-аппаратное средство для построения систем автоматики и робототехники — Arduino.

АППАРАТНЫЕ РЕАЛИЗАЦИИ ОПЕРАЦИЙ УМНОЖЕНИЯ В ПОЛЯХ ГАЛУА ПРИ ПОСТРОЕНИИ ЭЛЕМЕНТОВ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Е.В. Листопад

При построении современных систем на кристалле (в том числе для криптографической защиты информации) часто возникают задачи реализации арифметических операций в полях Галуа. От эффективности их реализации (в первую очередь, операций умножения) существенно зависят характеристики создаваемых систем. Поля Галуа характеризуются двумя параметрами: число двоичных разрядов, необходимых для представления символа, и генерирующий полином, определяющий порядок следования элементов поля [1].

Рассмотрим аппаратные реализации умножения элементов поля с числом двоичных разрядов равным 16. Умножение в поле подразумевает выполнение двух стадий: логическое умножение и приведение по модулю генерирующего полинома. Выполнение данных стадий возможно в следующих вариантах:

1. Выполнение приведения по модулю после умножения одного из множителей на каждый бит, каждую пару бит или каждые 4 бита второго множителя. Вся операция умножения будет выполнена за 16, 8 или 4 такта процессора соответственно.

2. Выполнение приведения по модулю (на 2-м такте) после перемножения элементов поля (на 1-м такте). Вся операция умножения будет выполнена за 2 такта.

3. Выполнение приведения по модулю на том же такте, что и перемножение элементов поля. Вся операция умножения будет выполнена асинхронно за 1 такт.

Лучшие соотношения показателей быстродействия и аппаратных затрат кристалла имеет вариант реализации умножения за 2 такта процессорного времени.