АППАРАТНЫЕ ШИФРАТОРЫ

НА ОТЕЧЕСТВЕННОЙ ЭЛЕМЕНТНОЙ БАЗЕ

И.Лукашов

В криптографической защите информации важнейшую роль играют аппаратные средства, которые имеют ряд существенных преимуществ перед программными. Заметных успехов в их развитии достигли российские разработчики.

Это подтверждают производимые фирмой АНКАД устройства серии "Криптон", основанные на отечественных шифрпроцессорах "Блюминг".

С развитием информационных технологий все большую актуальность приобретает проблема защиты информации – предотвращение ее утечки, несанкционированных и непреднамеренных воздействий на нее. Одна из важнейших областей этой деятельности – *криптография*, которая призвана обеспечить аутентичность и конфиденциальность передаваемых сообщений. Для решения первой задачи используется технология электронной цифровой подписи как компьютерного аналога подписи ответственного лица и печати организации, для решения второй – *шифрование*.

Под шифром в криптографии понимается совокупность обратимых преобразований множества возможных открытых данных во множество возможных зашифрованных данных, расшифровать и понять которые нелегальный пользователь (злоумышленник) не в силах. Эти преобразования осуществляются по определенному алгоритму с применением ключа – конкретного секретного состояния некоторых параметров криптоалгоритма, обеспечивающего выбор одного преобразования из всей совокупности вариантов, возможных для данного алгоритма. Стойкие криптоалгоритмы (к числу которых, например, относится отечественный ГОСТ 28147-89) способны обеспечить конфиденциальность сообщений даже при условии, что злоумышленнику известны открытые и зашифрованные тексты и сами правила преобразования. Иными словами, в открытых криптосистемах необходимо сохранять в тайне только ключи. При этом полностью исключены ситуации, когда, скажем, кража шифратора или публикация текста алгоритма даст злоумышленнику возможность раскрыть зашифрованные данные.

Схема криптографической системы, обеспечивающей шифрование передаваемой информации, представлена на рис.1. Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу. Для того чтобы злоумышленник не смог узнать содержание сообщения M, отправитель зашифровывает его по ключу K с помощью обратимого преобразования E_K и создает шифртекст (или криптограмму) $C = E_K(M)$, который отправляет получателю. Законный получатель, приняв шифртекст C, расшифровывает его с помощью обратного преобразования $D_K(C) = E_K^{-1}$ и получает исходное сообщение в виде открытого текста M: $D_K(C) = E_K^{-1}[E_K(M)] = M$.

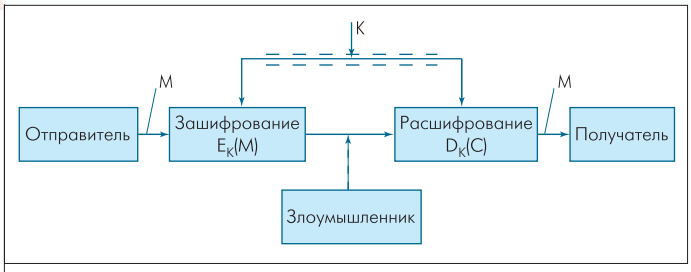

Рис.1. Схема криптографической системы

Данная система шифрования называется симметричной, поскольку зашифрование и расшифрование производятся с помощью одного и того же ключа K. При этом необходимо обеспечение конфиденциальности этого ключа (симметричные системы именуются также одноключевыми или системами с секретным ключом).

ШИФРОВАНИЕ – ПРОГРАММНОЕ ИЛИ АППАРАТНОЕ?

Отечественный алгоритм криптографического преобразования ГОСТ 28147-89 предназначен для программной или аппаратной реализации. Программные шифраторы, как правило, дешевле аппаратных и в ряде случаев способны обеспечить большую скорость обработки информации, однако этим, пожалуй, список их преимуществ исчерпывается. Перечень достоинств аппаратных шифраторов значительно шире:

- аппаратная реализация криптоалгоритма гарантирует его целостность;
- шифрование и хранение ключей осуществляются в самой плате шифратора, а не в оперативной памяти компьютера;
- аппаратный датчик случайных чисел создает действительно случайные числа для формирования надежных ключей шифрования и электронной цифровой подписи;

Представляем автора статьи

ЛУКАШОВ Игорь Владиславович. Кандидат педагогических наук. Начальник отдела маркетинга фирмы АНКАД. Сфера научных интересов — защита информации, документационное и информационное обеспечение управления.
Контактный тел.: (095)531-0000, 531-2050
Факс: (095)531-20-60
e-mail: marketing@ancud.ru; www.ancud.ru

- загрузка ключей в шифратор со смарт-карт и идентификаторов Touch Memory (i-Button) производится напрямую, минуя ОЗУ и системную шину компьютера, что исключает возможность перехвата ключей;
- на базе аппаратных шифраторов можно создавать системы защиты информации от несанкционированного доступа и разграничения доступа к компьютеру;
- применение специализированного шифрпроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера; возможна также установка на одном компьютере нескольких аппаратных шифраторов, что еще более повышает скорость обработки информации (это преимущество присуще шифраторам для шины PCI);
- использование парафазных шин в архитектуре шифрпроцессора исключает угрозу снятия ключевой информации по возникающим в ходе криптографических преобразований колебаниям электромагнитного излучения в цепях "земля – питание" микросхемы.

СПЕЦИАЛИЗИРОВАННЫЕ ШИФРПРОЦЕССОРЫ СЕРИИ "БЛЮМИНГ"

С публикацией трудов К.Шеннона (вторая половина 40-х гг. XX в.) началась эпоха открытой криптографии. В нашей стране важнейший революционный шаг был сделан в конце 80-х–начале 90-х гг., когда с развитием отечественной электроники появилась возможность разрабатывать и серийно производить 32-разрядные универсальные микропроцессоры. Это позволило перейти от специализированной ЭВМ, выполняющей криптографические функции, к превосходящему ее по техническим параметрам одноплатному устройству криптографической защиты данных (УКЗД). Вычислительное ядро УКЗД составляет шифрпроцессор с архитектурой микроЭВМ и размерами ОЗУ, который достаточен для аппаратной реализации алгоритма шифрования и имеет жестко заданный набор команд, управляющих как выполнением алгоритма, так и внутренней ключевой системой. Наличие в шифрпроцессоре внутренней ключевой системы низкого уровня значительно повышает защиту аппаратуры от электромагнитного излучения, а также предоставляет дополнительные возможности в отношении создания ключевых систем верхнего уровня.

Максимально оптимизированная архитектура УКЗД обеспечивает значительную скорость шифрования при невысокой тактовой частоте шифропроцессора:

$$V = F \cdot K/N,$$

где V – скорость шифрования, Мбайт/с; F – частота следования тактовых сигналов, МГц; N – число тактов, необходимых для обработки единичного блока информации; K – размер единичного блока преобразования, байт.

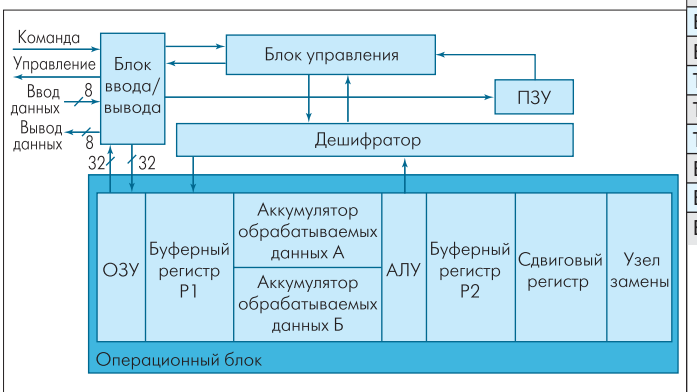

Рис.2. Типовая структурная схема шифрпроцессора

Таблица 1. Характеристики шифрпроцессоров серии "Блюминг"

Характеристика	"Блюминг-1"	"Блюминг-1К"
Реализуемый алгоритм	ГОСТ 28147-89	ГОСТ 28147-89
Число выполняемых режимов	21	50
Число хранимых ключей	3	3
Вид технологии	n-МОП	КМОП (1М)
Уровень технологии, мкм:		
длина p/n-канала транзистора	–/4	2,0/1,5
мин.шаг по Al	8,0	5,0
мин.шаг по Si	8,0	4,0
мин.шаг по n^+/p^+	8,0	4,5
Размер кристалла, мм	4x4	5,8x5,8
Число транзисторов	19000	25728
Число кристаллов на пластине	350	185
Число внешних выводов	42	28
Число тактов на обработку восьми байтов данных	175	116
Тактовая частота, МГц	7,0	15,0
Быстродействие, Мбайт/с	0,32	1,03
Шина данных	Инверсная	Прямая
Уровень входного сигнала	ТТЛ/КМОП	ТТЛ/КМОП

В соответствии со стандартом ГОСТ 28147-89 в 1990 г. был разработан первый отечественный шифрпроцессор "Блюминг-1" (рис.2). Основной узел, выполняющий обработку данных, – операционный блок, который состоит из ОЗУ, где хранится ключевая информация, буферных регистров Р1 и Р2 и аккумуляторов обрабатываемых данных АКА и АКБ, арифметического логического устройства (АЛУ), сдвигового регистра и узла замены. Блок ввода/вывода позволяет организовать совмещенную загрузку, выдачу обрабатываемых данных через байтовые входную и выходную внешние шины. Блок управления обеспечивает формирование внешних сигналов обмена и управление операционным блоком через дешифратор в соответствии со считанными из ПЗУ микрокомандами. Данная архитектура характерна для всех шифрпроцессоров серии "Блюминг". В табл.1 и 2 приведены результаты сравнительного анализа шифрпроцессоров моделей "Блюминг-1" и "Блюминг-1К".

Серийный выпуск специализированных шифрпроцессоров в 90-х годах означал серьезный успех отечественной микроэлектроники и стал основой развития аппаратных шифраторов серии "Криптон".

Таблица 2. Электрические параметры шифрпроцессоров серии "Блюминг"

Параметр	"Блюминг-1"		"Блюминг-1К"	
	Макс.	Мин.	Макс.	Мин.
Напряжение питания, В	4,25	5,25	4,5	5,5
Выходное напряжение низкого уровня, В	–	0,5	–	0,5
Выходное напряжение высокого уровня, В	4,0	–	4,0	–
Входное напряжение низкого уровня, В	0	0,8	0	0,8
Входное напряжение высокого уровня, В	2,4	$E_{пит}$	2,4	$E_{пит}$
Ток потребления в статическом режиме, мА	–	200,0	–	0,2
Ток утечки на входе, мкА	–	1,0	–	1,0
Ток утечки на выходе, мкА	–	5,0	–	5,0
Выходной ток низкого уровня, мА	2,0	–	8,0	–
Выходной ток высокого уровня, мА	-0,5	–	-6,0	–
Емкость нагрузки, пФ	–	100	–	100

АППАРАТНЫЕ ШИФРАТОРЫ СЕРИИ "КРИПТОН"

К 2001 г. выпущено более 18 тыс. устройств криптографической защиты данных серии "Криптон", и можно утверждать, что технология "Криптон" стала де-факто синонимом аппаратной реализации алгоритма ГОСТ 28147-89. Устройства "Криптон" применяются в соста-

ве средств и систем криптографической защиты данных для обеспечения информационной безопасности (в том числе защиты секретной информации) в государственных и коммерческих структурах. Эти устройства гарантируют защиту информации, обрабатываемой на персональном компьютере и/или передаваемой по открытым каналам связи.

Устройства "Криптон" разработаны по техническим заданиям, согласованным с Федеральным агентством правительственной связи и информации при президенте РФ (ФАПСИ), отвечают самым высоким требованиям по безопасности и имеют действующие сертификаты ФАПСИ.

Устройства серии "Криптон" имеют следующие технические характеристики:

Алгоритм шифрования	ГОСТ 28147-89
Разрядность ключа шифрования	256 бит
Число комбинаций ключей	10^{77}
Число уровней ключевой системы	3 (главный ключ — пользовательский/ сетевой ключ — файловый ключ)
Датчик случайных чисел	аппаратный
Отклонение распределения значения случайных чисел от равновероятного	не более 0,0005
Поддерживаемые операционные системы	MS-DOS, Windows'95(98)/ ME/NT 4.0/2000

Первым серийно выпускаемым аппаратным шифратором стало устройство "Криптон-3". Его архитектура и технические параметры отвечали состоянию компьютерного парка страны первой половины 90-х годов, а уровень надежности был таким, что до сих пор устройства "Криптон-3" продолжают функционировать у потребителей, не имеющих средств на обновление техники.

Доработка данного шифратора позволила перейти к выпуску устройства "Криптон-4". Сохранив все преимущества своего предшественника, "Криптон-4" обладает улучшенными потребительскими свойствами: выросла скорость шифрования (до 350 Кбайт/с на компьютерах с процессорами 386/486), появилась возможность хранить криптографические ключи на более надежных по сравнению с дискетами носителях – смарт-картах с открытой памятью.

Серийное производство устройства "Криптон-4" продолжается. Спрос на него остается стабильным как в государственном, так и в коммерческом секторе.

Вместе с тем, развитие компьютерной техники требовало дальнейшего совершенствования устройств "Криптон", и ответом на эту потребность стал переход к новым технологиям. Так, устройство "Криптон-4К/16" построено на шифрпроцессоре "Блюминг-1К" и имеет 16-разрядную шину ISA, что позволило еще больше повысить скорость шифрования, приблизив этот показатель к 1 Мбайт/с. Кроме того, это устройство может быть дополнено комплексом "Замок" и в этом исполнении обеспечить следующие функции:

- контроль доступа к компьютеру;
- разграничение прав пользователей на доступ к компьютеру;
- контроль целостности операционной системы и системных областей;
- ведение журнала регистрации событий, связанных с эксплуатацией УКЗД.

При включении компьютера комплекс "Замок" предлагает пользователю предъявить ключи шифрования и персональный идентификатор. Затем с помощью ключей шифрования инициализируется УКЗД, проверяется наличие и целостность файла с идентификатором пользователя, осуществляется поиск его имени в списке пользователей, производится аутентификация пользователя (ввод пароля и т.п.) и автоматически стартует программа проверки целостности операционной системы компьютера. Она получает от УКЗД информацию о пользователе, разблокирует клавиатуру, проверяет целостность системных областей и файлов операционной системы.

По выполнении этих операций комплекс "Замок" передает управление операционной системе и в дальнейшем в деятельность пользователя не вмешивается. Таким образом, пользователи УКЗД "Криптон", начиная с устройства "Криптон-4К/16", вместе с аппаратным шифратором получают и средство разграничения доступа, что не только повышает функциональность системы защиты, но и позволяет снизить ее стоимость.

УКЗД "Криптон-4К/16" как шифратор сертифицировано ФАПСИ, а как средство защиты компьютерных ресурсов от несанкционированного доступа имеет сертификат Государственной технической комиссии при президенте РФ. Это устройство пользуется особой популярностью у государственных органов и организаций, а также у потребителей, заинтересованных в комплексном решении проблем информационной безопасности, – банковских структур, финансовых компаний и т.п.

Самый "молодой" представитель серии "Криптон" – устройство "Криптон-4/PCI" (рис.3), серийное производство которого началось в 2000 г. Использование шины PCI открывает перспективы применения этого шифратора в компьютерах последних лет выпуска, в которых шина ISA отсутствует либо отведена другим устройствам. УКЗД "Криптон-4/PCI" поддерживает самый широкий спектр ключевых носителей, включая микропроцессорные карты (в том числе Российскую интеллектуальную карту – РИК). В комплект поставки УКЗД входит комплекс разграничения "Замок", т.е. фактически потребитель "в одном флаконе" получает и аппаратный шифратор, и средство защиты от несанкционированного доступа. В настоящее время ФАПСИ завершает сертификационные исследования устройства "Криптон-4/PCI", в том числе для применения в целях защиты информации, составляющей государственную тайну. Потребительские качества и демократичная цена обеспечили повышенный спрос на этот шифратор, и есть все основания полагать, что в ближайшем будущем "Криптон-4/PCI" выйдет в лидеры продаж.

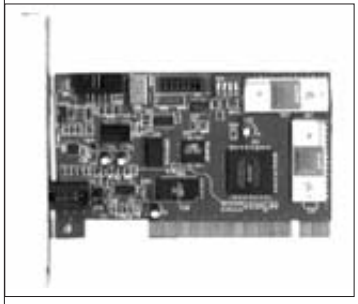

Рис.3. Устройство "Криптон-4/PCI"

Результаты сравнительного анализа устройств серии "Криптон" приведены в табл.3.

Таблица 3. Сравнительная характеристика устройств "Криптон"

Устройство	Шифр-процессор	Шина	Скорость шифрования, Кбайт/с	Носители ключей
"Криптон-3"	"Блюминг-1"	ISA-8	До 50	Дискеты
"Криптон-4"	"Блюминг-1"	ISA-8	До 350	Дискеты, смарт-карты (СК) с открытой памятью*
"Криптон-4К/16"	"Блюминг-1К"	ISA-16	До 950	Дискеты, СК с открытой памятью*, Touch Memory (TM)*
"Криптон-4/PCI"	"Блюминг-1К"	PCI (Target)	До 1100	Дискеты, TM*, СК с открытой и защищенной памятью*,микропроцессорные СК*, в т.ч. РИК

* Работа со смарт-картами или идентификаторами Touch Memory возможна при подключении к шифратору устройства чтения/записи смарт-карт или коннектора TM.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АППАРАТНЫХ ШИФРАТОРОВ

Разумеется, даже самым совершенным технологиям аппаратной реализации алгоритмов шифрования необходимо "подкрепление" программным обеспечением, реализующим интерфейс между пользователем и УКЗД. Развитая структура программного обеспечения устройств серии "Криптон" (табл.4) позволяет удовлетворить самые различные запросы пользователей и найти аппаратным шифраторам применение во многих сферах.

Таблица 4. Программное обеспечение устройств серии "Криптон"

Программный продукт	Назначение
Прикладные программы для конечных пользователей	
"Криптон"®Шифрование	Архивное и абонентское шифрование файлов и каталогов
"Криптон"®Подпись	Электронная цифровая подпись (ЭЦП) с открытым ключом 512, 1024 бит
Crypton ArcMail	Единый сервис архивирования, ЭЦП и шифрования, симметричная и асимметричная схемы управления ключами с открытым ключом 512, 1024 бит
Crypton Sigma	Прозрачное (автоматическое, незаметное пользователю) шифрование логических дисков, в т.ч. на серверах
"Криптон"-IP	Формирование криптографически защищенных виртуальных частных сетей (VPN)
Crypton Word	Защита документов MS Word 97/2000
Crypton Excel	Защита документов MS Excel 97/2000
Средства разработки для системных интеграторов	
Библиотека Crypton DK	Низкоуровневые функции прямого доступа к шифратору
Библиотека Crypton Tools	Архивное и абонентское шифрование
Библиотека Crypton ArcMail	Единый сервис архивирования, ЭЦП и шифрования, симметричная и асимметричная схемы управления ключами с открытым ключом 512, 1024 бит

Наряду с аппаратными шифраторами серии "Криптон" выпускается их программный аналог – Crypton Emulator для Windows'95(98)/ME/NT 4.0/2000, который может работать с перечисленным выше программным обеспечением и полностью совместим по форматам ключей и зашифрованных (подписанных) файлов с устройствами криптографической защиты данных.

ИТОГИ И ПЕРСПЕКТИВЫ

Краткий обзор десятилетней истории развития аппаратных шифраторов на отечественной элементной базе позволяет сделать ряд выводов. Прежде всего можно констатировать, что в отличие от многих других отраслей российская криптография не только не пришла в упадок, но продолжает успешно развиваться. Залогом этих успехов во многом стала сформированная в СССР мощная научная и производственная база, но нельзя не заметить и новых тенденций, свойственных именно последнему десятилетию. Так, проектирование и производство шифрпроцессоров серии "Блюминг" и устройств серии "Криптон" осуществляет фирма АНКАД – коммерческое предприятие, которое в основном за счет собственных средств ведет разработки в интересах обеспечения национальной информационной безопасности. Эффективный менеджмент позволил фирме преодолеть извечную болезнь отечественных инновационных предприятий, зачастую неспособных довести перспективные идеи до выпуска промышленных образцов. Простой перечень выведенных на рынок устройств криптографической защиты данных свидетельствует о том, что даже в современных российских условиях возможна реализация полного цикла "наука – производство". Кооперационное производство фирмы АНКАД обеспечивает стабильные заказы для предприятий во многих регионах России (ОАО "Ангстрем" и т.д.).

Накопленный опыт фирмы АНКАД позволяет предположить, что в ближайшие годы развитию аппаратных шифраторов отечественной разработки и производства будут присущи следующие тенденции:

- повышение быстродействия;
- расширение спектра поддерживаемых операционных систем (ОС), прежде всего за счет доверенных ОС, чьи возможности полностью документированы;
- расширение спектра поддерживаемых ключевых носителей (в частности, перспективным представляется использование брелоков для шины USB – полнофункциональных аналогов смарт-карт, не требующих, в отличие от СК, специальных устройств чтения/записи);
- интеграция функций шифраторов и других устройств (например, создание сетевого шифратора);
- расширение функций прикладного программного обеспечения и средств разработки (встраивание сильной криптографии в популярные почтовые программы, системы управления базами данных, средства электронного документооборота и т.д.). ❍

Новые технологии проверки в аэропортах США

Федеральное авиационное управление США (FAA) развертывает следующие усовершенствованные устройства обнаружения взрывчатых веществ.

Рентгеновские методы. По одному из них багаж подвергается рентгеновскому облучению от быстродействующего прибора VIS-M фирмы Perkin Elmer для оценки атомного состава, плотности и других характеристик объектов в багаже. Компьютер обрабатывает изображения и индицирует любую обнаруживаемую угрозу. Благодаря рассеянию рентгеновских лучей тонкими материалами VIS-M распознает тонкие слои взрывчатых веществ. Для стандартных рентгеновских методов эти рассеянные лучи невидимы.

Аналогичный прибор Zscan-7 той же фирмы использует метод арифметического восстановления, позволяющий вычислить вероятность того, что в багаже имеется взрывчатое вещество.

Прибор HI-Scan фирмы Heiman Systems, используя два рентгеновских источника с различной мощностью, способен различить органические материалы и взрывчатые вещества. Атомное изображение обрабатывается на мощном компьютере.

Квадрупольный резонанс. Прибор Qscan-500 фирмы Quantum Magnetics обнаруживает взрывчатые вещества, используя анализ квадрупольного резонанса. Внутренняя катушка прибора генерирует радиоимпульсы, которые воспринимают структуру взрывчатого вещества. При наличии взрывчатого вещества прибор генерирует уникальный неизменяемый сигнал, который направляется в компьютер для анализа.

Перед размещением этого оборудования операторы должны пройти обучение по его использованию. Новое оборудование влечет за собой новые процедуры проверки, которые интегрируются с другими – такими как проверка пассажиров с помощью компьютеров, ручное обследование и т.д.

С 1994 года FAA занято также разработкой радиочастотного прибора идентификации (RFID), который подходит для автоматизации программы соответствия багажа пассажиру. Первые RFID-системы были установлены в 1999 году в основных аэропортах США. Здесь пассажиры проверяют свой багаж с помощью сертифицированного оборудования проверки. Весь багаж, отобранный для проверки на взрывчатые вещества, маркируется с помощью радиочастотного тега и проходит через радиочастотное сканирующее устройство. Контроллер запрограммирован для интерпретации сообщений от RFID-сканера для поиска специфических данных в теге. Багаж с радиочастотным тегом затем отводится с конвейера автоматическим толкателем на боковой конвейер, ведущий к системе проверки взрывчатых веществ.

RFID-теги и сканирующие устройства работают в полосе 2,400–2,483 ГГц. Преимущество системы – миниатюрные RFID-считыватели и использование одной программы для нескольких сканеров.

www.securitymanagement.com/library/001111.html