"надежный" ключ — ключ, на расшифровку которого злоумышленникам понадобится 1,5 года и более.

Из таблицы следует, что чем больше разрядность ключа, тем сложнее расшифровать содержащуюся в ключе информацию, и тем выше степень защиты информации в ЭПК. С другой стороны, при увеличении разрядности ключа возрастает сложность ЭПК и, соответственно, ее себестоимость.

Сопоставительный анализ времени на расшифровку ключа ЭПК и затрат на его вскрытие

Атакующая сторона	Затраты, тысяч USD	ТВК СК	Время расшифровки		Длина "надежного" ключа, бит
			Ключ 40 бит	Ключ 56 бит	
Хакер (индивидуальный злоумышленник)			Неделя	бесконечно	45
Малый бизнес	0,4	FPGA	5 часов	38 лет	50
	10	ASIC	12 минут	556 дней	55
Отдел корпорации	300	FPGA	24 секунды	19 дней	60
	300	ASIC	18 секунд	3 часа	60
Крупная компания	10 000	FPGA	7 секунд	13 часов	70
	10 000	ASIC	0,005 секунды	6 минут	70
Федеральное агентство	300 000	ASIC	0,0002 секунды	12 секунд	75

В подразделении НИРУП "ЦНИИТУ", занимающемся разработкой и производством ЭПК, было проведено сравнение по степени защиты информации различных кристаллов, используемых в ЭПК. Установлено, что в телефонном кристалле 4406 защита информации от несанкционированного доступа отсутствует, а в кристалле 4436 имеется ключ длиной 48 бит. Согласно [4] для расшифровки 56-битовых ключей с помощью суперкомпьютера Cray T3D (стоимость такого компьютера в 2000 году составляла 30 млн. долларов) понадобится 453 дня. В то же время длина ключа в телефонной и банковской ЭПК разработки НИРУП "ЦНИИТУ" составляет 256 бит. Это говорит о высокой степени защищенности информации в ЭПК разработки НИРУП "ЦНИИТУ", что в свою очередь свидетельствует о соответствии этих карточек по показателю безопасности информации в них современному научно-техническому уровню и современным тенденциям развития научно-технического прогресса в РБ и за рубежом.

Литература

1. Прибыльский А.В., Таболич Т.Г. Основные направления защиты информации на промышленных предприятиях // В этом сборнике. С.
2. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. Мн. 1999.
3. Харин Ю.С., Агиевич В.С. Компьютерный практикум по математическим методам защиты информации. Мн. 2001.
4. Калинцев Ю.К. Обеспечение безопасности информации в современных сетях связи//Электросвязь. 2000. N 12. С. 6–8.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОИЗВОДСТВЕ И ЭКСПЛУАТАЦИИ ТЕЛЕФОННОЙ ЭПК

В.С. РЕУЦКИЙ, Д.В. ВЕЧЕР, А.В. ПРИБЫЛЬСКИЙ

Основные элементы действующей системы обеспечения информационной безопасности телефонной электронной пластиковой карты (ЭПК) НИРУП "ЦНИИТУ" — это криптозащищенная предоплаченная таксофонная карта и модуль безопасности (МБ). Карта изготавливается на основе кристалла российского производства, разработанного в ОАО "Ангстрем" в 1998 году и известного под маркой "Tay-98". Разработчики кристалла учли и устранили ошибки, допущенные при проектировании наиболее близкого аналога 4436 [1, 2].

ЭПК имеет достаточно большой потенциальный ресурс (до 29 тысяч тарифных единиц) и функцию защиты от прерванной записи. Каждая карта имеет индивидуальный ключ карты длиной 256 бит, зашифрованный по ГОСТ 28147-89 и хранящийся в области памяти, закрытой для чтения. Карта является автономным компонентом системы безналичных расчетов и может использоваться как самостоятельное платежное средство. Однако из-за жесткой логики работы ЭПК гарантировать высокую защищенности информации в ней нельзя.

Поэтому в качестве второго компонента системы предлагается использовать освоенный в производстве в НИРУП "ЦНИИТУ" модуль безопасности. Этот МБ представляет собой 8-разрядный микроконтроллер с RISK архитектурой, внутренней операционной системой и протоколом обмена T=0 по ISO 7816-3. Конструктивно МБ выполнен под разъем "PLUG IN" по GSM 11.11 и предназначен для установки в таксофон. В МБ могут храниться одновременно до 16 ключей, которые недоступны для

чтения, модификации или удаления. Основное назначение МБ в системе - аутентификация (удостоверение подлинности) кристалла на всех этапах производства и эксплуатации ЭПК. Ключи с течением времени могут сменяться, в том числе дистанционно, или одновременно могут действовать несколько ключей.

Важным элементом, обеспечивающим безопасность системы, является бесполезность такого занятия, как получение информации о ключах посредством логического анализатора — информация при очередном сеансе связи повторяться не будет и логику смены данных проследить невозможно.

Система организована так, что защита транспортного пути кристалла может производиться на ключах, которые не используются в системе. Таким образом изготовитель кристаллов не имеет возможности получить информацию о рабочих ключах. Смена транспортных ключей производится на каждой партии, и поэтому вероятная утечка ключевой информации не приведет к взлому системы.

Хищение МБ из таксофона или вместе с таксофоном также не позволяет взломать систему в целом из-за недоступности ключевой информации. Для защиты от имитации ЭПК, кроме традиционных методов в системе предусмотрена модификация индивидуального кода карты после каждого сеанса связи.

Для повышения стойкости системы к взлому в ней используются МБ с различными ключами на этапах изготовления и эксплуатации ЭПК. При изготовлении кристалла изготовителю передается МБ с транспортными ключами А1-А16. Изготовитель использует эти ключи для записи в кристалл зашифрованного транспортного кода и для создания транспортной карты, содержащей опять таки зашифрованный транспортный ключ. При этом для каждой партии кристаллов используются один из ключей А, а по истечении определенного времени может быть произведена полная замена ключей. Прочитать исходные ключи А в открытом виде и получить информацию о рабочих ключах Б изготовитель кристаллов не может.

После изготовления ЭПК транспортная карта и МБ с ключами Аi используются для входа в режим персонализации карты. Войти в этот режим можно только в случае, если зашифрованные транспортные ключи в кристалле и транспортной карте будут успешно расшифрованы и опознаны МБ с ключами А. Непосредственно для персонализации используется МБ с рабочими ключами Бi, которые также должны содержать МБ, установленные в таксофонах. По окончании персонализации транспортный ключ из карты удаляется, но в закрытую для чтения область памяти записывается индивидуальный ключ карты (ИКК) длиной 256 бит, зашифрованный на рабочем ключе Бi. Изготовителю таксофонов передается МБ с рабочими ключами Б1-Б16, также недоступными для чтения, модификации и удаления. При этом ему неизвестны транспортные ключи.

В настоящее время в системе используется лишь малая часть возможностей, предоставляемых МБ. Поэтому в случае внедрения система имеет дальнейшие перспективы развития, например в части шифрации информационного обмена между таксофоном и АТС, защиты от несанкционированного подключения к линиям связи и т.д.

Система в целом может использоваться и для других применений, где требуется использование предварительно оплаченного кредита. В настоящее время все компоненты системы освоены в серийном производстве в НИРУП "ЦНИИТУ" Научно-производственного объединения "Центрсистем" и прошли эксплуатационные испытания на телефонной сети Республики Беларусь. Результаты позволяют говорить о высокой степени защищенности и хорошем качестве ЭПК.

Литература

1. J. Glave. Pirate Cash in on Weak Chips // Wired News. 1998. N 218 (May).
2. Deutsche Telecom hit by Eurochip reload fraud //User Guide 99. P. 57.

СИНТЕЗ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.А. ШАМШУР

В настоящее время генераторы случайных чисел получили широкое распространение благодаря применению в различного рода устройствах для защиты информации от несанкционированного доступа, в средствах встроенного самотестирования и т.д. Рост мобильности устройств выдвигает новые требования ко всем узлам, в том числе и к генератору случайных чисел. Основным требованием в мобильном устройстве является энергопотребление, поэтому на сегодняшний день актуальна проблема построения генератора случайных чисел с наименьшим энергопотреблением.

Известно несколько подходов к решению проблемы энергопотребления: изменение схемы устройства, исключение лишних узлов и т.д.; уменьшение частоты работы, что приводит, однако, к уменьшению производительности; изменение структуры блока.

В данной работе рассматривается внесение структурных изменений в широко распространенную схему генератора псевдослучайных последовательностей на основе сдвигового регистра с линейной обратной связью, известного в англоязычной литераторе как Linear Feedback Shift Register (LFSR). Весь регистр делится на две части, работающие на разных частотах, причем на самой большой частоте — частоте появления наборов на выходе схемы, работает только оконечная часть схемы, вся остальная часть работает на меньших частотах, за счет чего и достигается уменьшение энергопотребления.

Для генерирования выходной псевдослучайной последовательности высокой частоты используется несколько сдвигов одной и той же псевдослучайной последовательности меньшей частоты. После сложения двух последовательностей при помощи сумматора по модулю два, получается так же псевдослучайная последовательность, но уже большей частоты.