СМАРТ-КАРТЫ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ И ПРОГРАММ

А.Новоселов, Д.Погибельский

Смарт-карты (СК) стали неотъемлемой частью нашей жизни. Ежегодно их производится свыше 500 млн. штук. Сотовые телефоны, таксофоны, платежные системы, средства контроля доступа уже невозможно представить без СК. Современные смарт-карты – это сложные устройства с встроенным компьютером, для которого разработаны различные операционные системы. Обзору существующих типов СК и принципов их использования для защиты информации и программ посвящена статья специалистов компании "Орга Зеленоград".

ЗАЩИТА ИНФОРМАЦИИ И ПРОГРАММ

Обычно информация при хранении и передаче защищается либо посредством закрытых устройств и каналов связи, либо с помощью шифров. Шифрование в открытых носителях и каналах связи теоретически может обеспечить очень высокий уровень безопасности. Однако на практике этот способ требует либо запоминания пользователями множества длинных паролей, либо построения системы управления криптографическими ключами и их хранения внутри закрытых устройств. В противном случае безопасность оказывается под угрозой.

Простые закрытые устройства, поддерживающие распределение доступа (например, flash-диски), обычно защищены очень слабо. Информация из подобных устройств легко извлекается при физическом взломе с помощью спецсредств.

Профессиональные закрытые устройства, надежно защищающие данные от физического извлечения, например HSM (Hardware Security Module), имеют высокую стоимость и сложны в управлении. Поэтому они практически недоступны для широкого использования.

Весьма перспективна защита информации и программ с помощью карт с интегральной микросхемой, называемых также чиповыми картами, или СК. Такие карты лишены большинства указанных недостатков. Они компактны, достаточно дешевы и обладают высоким уровнем защиты данных от логического и физического извлечения. Данные карты защищены и от экзотических атак, таких как анализ радиоизлучения и лазерный удар, например точечный нагрев чипа лазером с целью изменения битов памяти, хранящихся в точке нагрева. Такие атаки приводят к неправильному функционированию карты – вплоть до отключения всех ограничений на извлечение информации. Сейчас наиболее распространены СК для хранения закрытой информации в мобильных телефонах – SIM-карты.

СК представляет собой миниатюрный компьютер с одним каналом связи. Хотя у СК нет интерфейса с пользователем и внутреннего источника энергии, она может обладать собственным процессором, оперативной и постоянной памятью (ОЗУ и ПЗУ), шиной данных и операционной системой. Объем ресурсов на СК не очень велик. В наиболее распространенных СК объем энергонезависимой памяти (EEPROM или Flash), доступной для приложений и данных, составляет порядка 32 Кбайт, а ОЗУ – до 2 Кбайт. Однако существуют и более совершенные СК, в которых объем энергонезависимой памяти достигает 1 Мбайт, а ОЗУ – до 16 Кбайт.

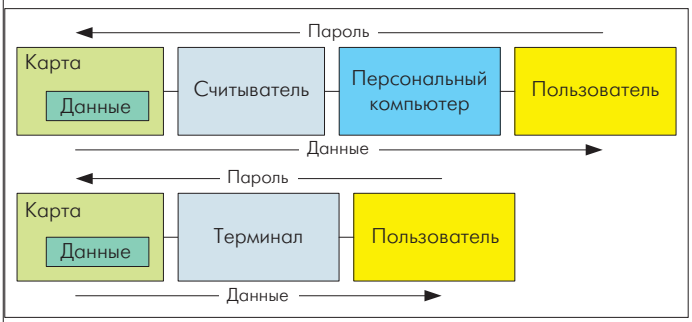

Рис.1. Применение СК для хранения информации. Закрытая информация отображается или обрабатывается с помощью персонального компьютера или специализированного терминала

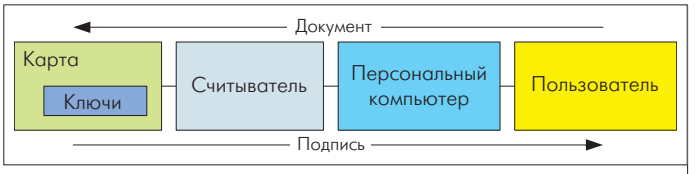

Рис.2. Схема использования СК для формирования цифровой подписи документа

Технологии защиты информации в СК весьма разнообразны. Простейший способ, используемый для защиты данных, – PIN-код (Personal Identification Number), или пароль, который блокирует данные на СК после нескольких неправильных предъявлений (рис.1).

Гораздо больше возможностей предоставляют специально разработанные загружаемые в СК программы со сложной логикой защиты информации. Если внутри таких СК хранятся криптографические ключи, они могут выполнять шифрование, а также вычислять криптографические подписи для блоков информации. Например, СК хранит пару асимметричных ключей, предназначенных для создания цифровой подписи (рис.2). Или же СК хранит ключ (рис.3), на котором выполняется шифрование информации при передаче сообщения по открытым каналам (например, по электронной почте).

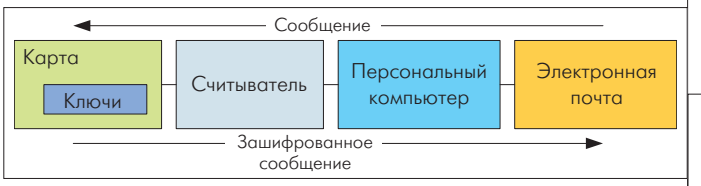

Рис.3. Схема использования СК для шифрования информации

Весьма активно СК используются и для защиты программ. Следует отметить, что надежная защита прикладной программы от несанкционированного копирования невозможна, если эта программа целиком выполняется центральным процессором (ЦП) персонального компьютера. В этом случае всегда можно полностью скопировать программу, а затем удалить систему проверок, из которых и состоит защита.

Для построения надежной защиты от несанкционированного извлечения информации и программного кода некоторая часть программы должна выполняться вне ЦП – внутри закрытого устройства, например в СК (рис.4). Недоступность защищенной части программы должна делать всю программу нефункциональной. Таким образом, для полного копирования программы необходимо скопировать и СК.

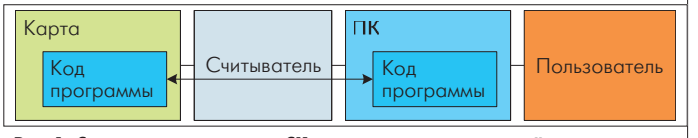

Рис.4. Схема использования СК для защиты прикладной программы от несанкционированного копирования

Однако к компьютеру одновременно можно подключить ограниченное количество смарт-карт – существенно меньше, чем число установленных программ. Поэтому нужно, чтобы одна СК защищала несколько программ. Такие карты должны допускать загрузку в них программного кода уже в процессе эксплуатации, что позволяют, например, СК открытых платформ.

АРХИТЕКТУРА СК

Контактные СК представляют собой микрочип с контактной площадкой, имплантированный в пластиковую основу с привычными "карманными" размерами 54×86 мм (рис. 5).

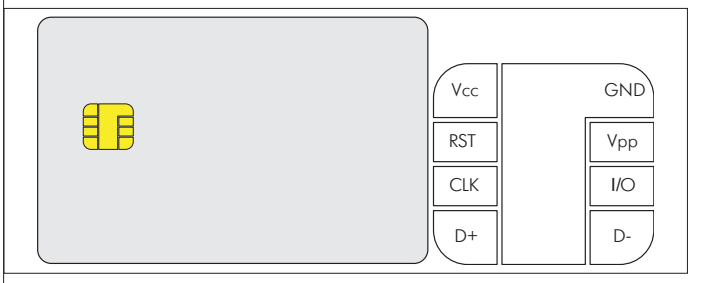

Рис.5. Контактная СК на пластиковой основе и ее контактная площадка в стандарте ISO 7816

Карты памяти – это самый простой тип СК. Они состоят только из энергонезависимой памяти (как правило, EEPROM) и внешнего канала связи (рис.6). Карты памяти обладают наиболее простой защитой. Как правило, это пароль или PIN-код, ограничивающий возможности записи.

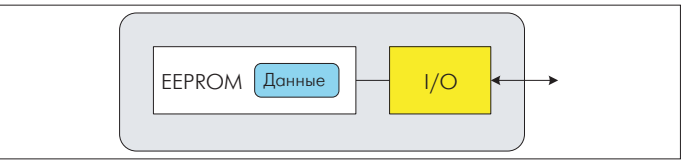

Рис.6. Устройство карты памяти

Например, СК SLE4442, разработанные компанией Infineon и производимые в настоящее время большим количеством компаний, оснащены всегда доступной для чтения памятью объемом 256 байт. Для записи данных необходимо ввести PIN-код из трех байт, имеющий ограничение по количеству попыток предъявления. Смена PIN-кода возможна только после его правильного предъявления.

Физические параметры карт памяти соответствуют стандарту ISO 7816. Однако протокол обмена данными обычно нестандартный (для реализации стандартного протокола

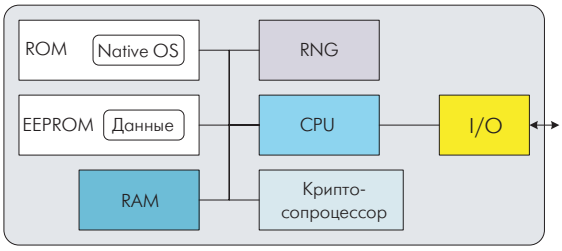

Рис.7. Микропроцессорная СК с собственной операционной системой

ISO 7816 необходим микроконтроллер, отсутствующий в картах памяти), что затрудняет поиск подходящего считывающего устройства.

Микропроцессорные СК с собственной операционной системой. Более сложные СК обладают микропроцессором, оперативной и постоянной памятью. Они используют специализированную операционную систему. Она записана в энергонезависимую память микроконтроллера (ROM, EEPROM), которая реализует всю логику работы СК. Как правило, подобные СК содержат криптографический сопроцессор, ускоряющий криптографические операции (рис.7). Такие СК обычно соответствуют стандарту ISO 7816.

Примером простой микропроцессорной СК является карта ICC4.1. Память ICC4.1 [1] организована в виде файловой структуры, которая задается при выпуске СК (структура каталогов, названия и длины файлов задаются производителем СК). Файлы и каталоги на такой смарт-карте имеют двухбайтные имена. Для доступа к данным внутри файлов используются два PIN-кода, а также два супер PIN-кода для разблокирования самих PIN-кодов. Для каждого файла задаются условия чтения и изменения. Предусмотрены варианты доступа: "всегда возможен", "доступ по одному из PIN-кодов" или "никогда". Сами PIN-коды также могут быть изменены.

Более сложная микропроцессорная смарт-карта – ICSC 2.0 – обладает динамической файловой структурой. Ее файлы и каталоги могут создаваться после выпуска СК. Условиями чтения и записи каждого файла могут быть предъявление PIN-кода либо выполнение аутентификации на ключе по стандарту 3DES. Предусмотрены два PIN-кода, общие для всей СК. Кроме того, допускается до 14 ключей в каждом каталоге. В случае аутентификации команды чтения и записи данных подписываются с помощью MAC-кода (Message Authentication Code), что исключает подделку таких команд без знания ключа аутентификации.

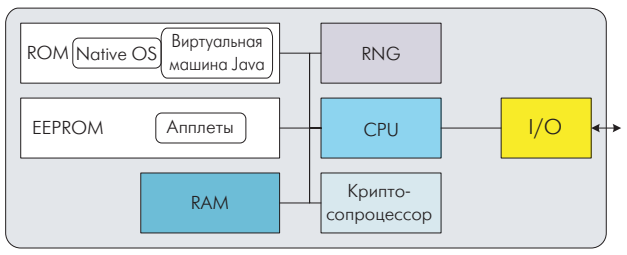

Рис.8. Микропроцессорная СК на открытой платформе JavaCard

Микропроцессорные СК открытых платформ обладают операционной системой, которая разрешает загрузку в энергонезависимую память СК прикладных программ, в том числе и самим пользователем. Программируемость СК открытых платформ допускает, что открывает широкие возможности для организации защиты и обработки информации. Основные открытые платформы для СК – это JavaCard, MULTOS и BasicCard.

Для СК наиболее распространена открытая платформа – JavaCard [2], основанная на технологи Java фирмы Sun (рис.8). Преимущество данной платформы – виртуальная машина Java – промежуточное звено между универсальным кодом приложений и различными чипами СК. При этом прикладные программы (апплеты) независимы от аппаратных возможностей СК. Это делает программно совместимыми Java-карты различных производителей.

Разработка приложений для Java-карт может быть освоена даже начинающим программистом, а вся необходимая для этого информация доступна в Интернете. Таким образом, приложения для Java-карт могут писать и сами пользователи. Благодаря виртуальной машине Java-карты достаточно устойчивы – ошибки приложений не приводят к сбоям в работе СК. Кроме того, код приложений для JavaCard проще подвергать тщательному криптоанализу – это необходимо для оценки уровня безопасности приложения.

В качестве примера СК открытых платформ можно привести семейство СК JCOP (JavaCard Open Platform) компании NXP (бывшее подразделение Philips), широко представленное на российском рынке.

СК JCOP10 [3] поддерживает базовую функциональность JavaCard и необходимый минимум криптографии: симметричное шифрование по стандартам DES и 3DES, хэш-функции по алгоритмам MD5 (Message Digest) и SHA-1 (Secure Hash Algorithm), а также криптографически надежный генератор случайных чисел. Объем EEPROM, в зависимости от конфигурации, составляет 16 или 32 Кбайт, ОЗУ – 1300 байт. Часть апплетов также могут быть "предынсталлированы" – зашиты в масочное ПЗУ карты – с помощью дополнительных 16–64 Кбайт ПЗУ.

СК JCOP20 [4] и JCOP30 [5], помимо базовой функциональности и минимума криптографии, поддерживают асимметричную криптографию по алгоритму RSA (Rivest-Shamir-Adleman). Объем их ОЗУ увеличен до 2300 байт. СК серии JCOP30 также обладают дуальным интерфейсом (контактным и бесконтактным).

Последнее пополнение в этом семействе – СК JCOP31 [6] и JCOP41 – помимо возможностей JCOP30 поддерживают относительно новый алгоритм симметричного шифрования AES (Advanced Encryption Standard) и асимметричную крипто-

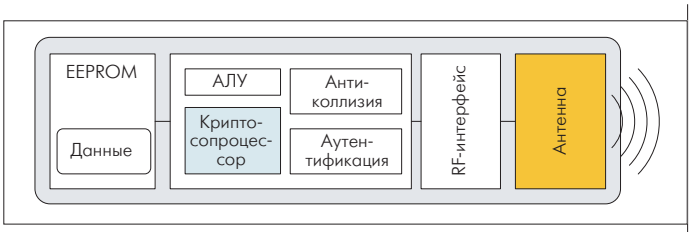

Рис.9. Бесконтактная СК стандарта Mifare

графию на эллиптических кривых ECC (Elliptic Curve Cryptosystem). Объем энергонезависимой памяти этих смарт-карт – 72 Кбайт.

Бесконтактные СК считываются по радиоканалу на расстоянии не более 5–10 см от считывающего устройства. Антенна располагается в толще пластиковой основы СК и служит одновременно каналом связи и источником энергии для микрочипа. Такие СК эффективны, когда необходимо быстро считать информацию, но не нужно существенно изменять данные на СК. Характерный пример подобных применений – задачи идентификации.

Весьма распространенным стандартом бесконтактных СК является Mifare Standard [7], разработанный компанией NXP (рис.9). Данный стандарт основан на ISO 14443 Type A, однако использует собственный протокол верхнего уровня (отличный от ISO 14443-4) и собственные технологии аутентификации и шифрования радиоканала.

СК стандарта Mifare выпускаются с памятью 1 и 4 Кбайт. Каждая СК обладает уникальным 32-разрядным идентификатором. Память разбита на блоки по 16 байт. Каждый четвертый блок памяти служит для хранения ключей и условий доступа, остальные блоки предназначены для пользовательской информации. Доступ к информации возможен только после предъявления одного из двух ключей, относящихся к данному блоку. Как правило, один из ключей дает право на считывание блока, а второй – на запись. Однако условия доступа можно изменить. В частности, блок может быть превращен в 32-битный счетчик, имеющий повышенную надежность (в 16-байтном блоке хранятся три копии 32-битного значения, оставшиеся 4 байта содержат маркер, упрощающий отличие блока со счетчиком от блока с данными). Причем с помощью первого ключа значение счетчика можно будет только считывать и уменьшать, а с помощью второго – изменять произвольным образом. Возможны и другие варианты программирования СК.

Недостаток бесконтактных СК – в невозможности гарантировать длительное нахождение СК в поле считывателя, поскольку она в любой момент может быть извлечена пользователем из считывающего устройства. А поскольку у СК нет защиты от ошибок при потере питания в момент записи, возможности изменения информации в бесконтактных картах ограничены.

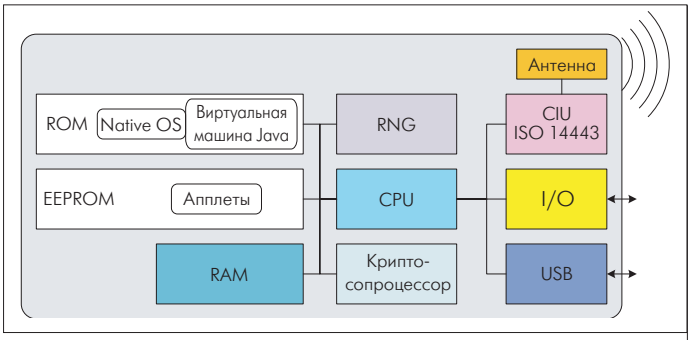

Рис.10. Java-карта с дуальным интерфейсом и USB-разъемом

Дуальные СК имеют как контактный, так и бесконтактный интерфейсы. Они допускают взаимодействие между контактной и бесконтактной частями. К таким СК относятся карты JCOP30, JCOP31 и JCOP41. Их бесконтактный интерфейс соответствует стандарту ISO 14443. Он делает возможной коммуникацию с Java-апплетами этих карт (по протоколу T = CL). Апплеты, в свою очередь, могут читать и записывать блоки данных Mifare, если предъявят соответствующие пароли доступа.

Более того, СК JCOP41 поддерживают USB-интерфейс: данные смарт-карты могут напрямую подключаться к ПК, без промежуточного считывающего устройства (рис.10). Для этого необходим лишь переходник-адаптер, который соединяет контакты контактной площадки ISO 7816 и контакты USB-разъема. Адаптер может быть выполнен в таком же корпусе, как и обычный настольный считыватель СК (удобный для частого подключения и извлечения СК) или в виде USB-донгла, внешне похожего на USB-флешдиск. В такой USB-донгл, как SIM-карта в мобильный телефон, будет вставляться СК.

ПРИЛОЖЕНИЯ ДЛЯ СК ОТКРЫТЫХ ПЛАТФОРМ

В операционных системах СК открытых платформ нет команд записи данных пользователя в файлы. Но они способны загружать и запускать специальные приложения, которые будут использовать ресурсы смарт-карты для хранения и обработки информации. Другими словами, для того чтобы СК открытых платформ служили конкретному пользователю, необходимо разработать или приобрести у других компаний соответствующее приложение.

Примером приложения, предназначенного для хранения закрытой информации на Java-карте, может быть приложение с интерфейсом, который соответствует стандарту MODS (MasterCard Open Data Storage) [8]. Такое приложение удобно для создания личной записной книжки – хранилища персональной информации (например, медицинской и т.п.). С целью разграничения доступа к информации S-данные могут быть структурированы в разделы, к которым существуют различные ключи. Для отдельной записи можно задать условия доступа на чтение, изменение и удаление. Интерфейс MODS поддерживает технологию взаимной аутентификации и закрытого канала. В режиме закрытого канала все передаваемые данные шифруются. Тогда даже перехват всех данных между считывающим устройством и картой не позволит злоумышленнику декодировать передаваемую информацию или узнать ключ доступа. Апплет jMODS для JavaCard (начиная с серии JCOP10), разработанный в ЗАО "ОРГА ЗЕЛЕНОГРАД", полностью реализует функциональность MODS.

Для хранения и использования криптографических ключей на СК предназначено приложение SmartHSM для JavaCard. С помощью данного приложения Java-карта может хранить в себе ключи, выполнять на них шифрование и дешифрирование внешних данных, формировать и проверять цифровую подпись. Команды работы с ключами на СК при подключении к персональному компьютеру соответствуют международному стандарту PKCS#11 (Public Key Cryptography Standards). Разработано и успешно эксплуатируется множество других приложений для СК открытых платформ.

Таким образом, смарт-карты предоставляют широкий спектр возможностей для защиты от несанкционированного копирования данных и программ. Простые СК могут хранить небольшие объемы информации и реализовать простую логику защиты. Более сложные СК позволяют хранить данные, программный код, а также использовать программируемую логику защиты.

ЛИТЕРАТУРА

1. ICC 4-1/8 KB, Standard Chip Card Application. ORGA Kartensysteme GmbH, February, 2000.
2. Application Programming Interface, JavaCard Platform, Version 2.2.1. Sun Microsystems, Inc., October, 2003.
3. JCOP10 Technical Brief. IBM BlueZ, Revision 2.1. (ftp://ftp.software.ibm.com/software/pervasive/info/JCOP10Brief.pdf).
4. JCOP20 Technical Brief. IBM BlueZ, Revision 2.3. (ftp://ftp.software.ibm.com/software/pervasive/info/JCOP20Brief.pdf).
5. JCOP30 Technical Brief. IBM BlueZ, Revision 2.3 (ftp://ftp.software.ibm.com/software/pervasive/info/JCOP30Brief.pdf)
6. JCOP31bio Technical Brief. IBM BlueZ, Revision 1.2 (ftp://ftp.software.ibm.com/software/pervasive/info/JCOP31bioBrief.pdf)
7. Mifare, Standard 4 kByte Card IC, MF1 IC S70, Functional Specification Philips Semiconductors, Revision 3.1, October, 2002.
8. MasterCard Open Data Storage. Technical Specifications, Version 2.0. MasterCard International, December, 2002.