УДК 004.03

ИДЕНТИФИКАЦИЯ СМАРТ-КАРТ НА ОСНОВЕ ОДНОСТОРОННИХ ПРЕОБРАЗОВАНИЙ

***Д. А. Крюков*[1],**
аспирант
Московский государственный институт радиотехники, электроники и автоматики

Рассматривается подход к построению системы идентификации для устройств с ограниченными ресурсами и памятью, таких как смарт-карты, брелоки, устройства RFID и т. п. Стойкость протокола основывается на стойкости используемых криптопримитивов, а также на предполагаемой возможности стойкого объединения логики при проектировании схем устройства терминала.

Ключевые слова *— смарт-карты, RFID, симметричные алгоритмы, системы идентификации.*

Введение

Стандартным и широко распространенным способом реализации процедуры идентификации являются так называемые парольные системы [1, 2], в которых каждому участнику системы соответствует пара (имя, пароль). Для прохождения идентификации пользователь должен назвать себя (сообщить имя) и назвать правильный пароль, соответствующий этому имени. Очевидный недостаток данной системы состоит в том, что для прохождения идентификации терминал должен знать все секретные пароли всех пользователей. Таким образом, требуется построение системы, в которой терминал способен проверить наличие у пользователя, выдающего себя за U, секрета S_U, не зная этого секрета.

В работе [3] Шамир предложил идею использования в качестве открытого ключа P_U пользователя U непосредственно данных об идентичности этого пользователя (или значения, напрямую вычисляемого из этих данных). Помимо удобства, достоинством этого подхода является то, что решается проблема аутентичности открытого ключа. Такой подход получил название «основанного на идентичности» (ID-based) или «личностного». Стоит отметить, что личностная криптография особенно удобна в задаче идентификации, так как в любом протоколе идентификации пользователь вначале должен сообщить терминалу, «за кого он себя выдает»; в личностной криптографии это позволяет одновременно передать открытый ключ.

Автор построил систему личностной идентификации, которая может быть использована на смарт-картах как устройствах с ограниченными ресурсами.

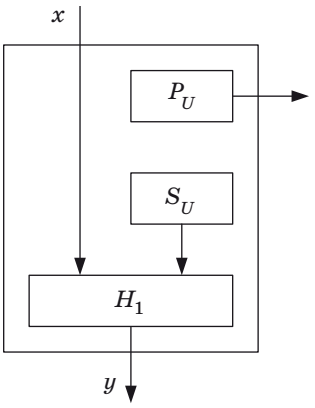
Схема идентификации, основанная на изолировании запроса

Рассмотрим подход к организации идентификации между картой и терминалом, основанный на так называемом изолировании запроса.

Предположим, что мы рассматриваем карту, принадлежащую пользователю U. В дальнейшем не будем различать пользователя и его карту и будем называть карту «картой U». Предположим далее, что мы рассматриваем личностную криптографию, и открытый ключ пользователя получается из данных об идентичности данного пользователя. Будем считать в связи с этим, что $P_U = U$.

Секретный ключ S_U вычисляется авторизованным центром с помощью секретного преобразования E. Фактически это означает, что при вычислении E используется дополнительный секретный аргумент. Будем считать, что авторизованный центр A вычисляет секретный ключ пользователя U как $S_U = E_{S_A}(U)$, где S_A — секретный ключ центра A. Структура карты изображена на рис. 1. Здесь H_1 — (несекретное) одностороннее преобразование. Карта способна со-

[1] Научный руководитель — кандидат технических наук, доцент кафедры корпоративных информационных систем Московского государственного института радиотехники, электроники и автоматики *Е. Г. Андрианова*.

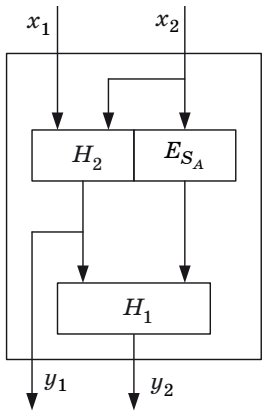


■ ***Рис. 1.*** Структура карты U

общать свой открытый ключ P_U, а также вычислять функцию $y = H_1(x, S_U)$ для некоторого входа x. Отметим, что сама архитектура карты, представленная на рис. 1, не является новой — например, она используется в микрочипах ST1335 и SLE4436 карт оплаты телефонии T2G.

Функциональная структура терминала изображена на рис. 2. Важнейшим условием предлагаемой системы является то, что устройство, реализующее данную функциональность и предоставляемое авторизованным центром всем терминалам, является для них «черным ящиком». Оно принимает на вход два аргумента x_1 и x_2 и вычисляет y_1 и y_2, но не может быть (за приемлемое время) разложено на составляющие H_1, H_2 и E_{S_A} или эквивалентные им. На практике это может быть осуществлено на уровне логики интегральной схемы. Таким образом, на рис. 2 показана именно функциональность блока на стороне терминала, а не действительная архитектура.

Блоки H_1 и H_2 — открытые, но односторонние преобразования, а E_{S_A} — секретное преобразование авторизованного центра (см. рис. 2). Вследствие предполагаемой невозможности обратного инжиниринга преобразование E_{S_A}, а также все



■ ***Рис. 2.*** Структура терминала

промежуточные значения «внутри» изображенного блока остаются недоступными извне. При этом само устройство, как некоторое отображение из двух входов в два выхода, может рассматриваться как общедоступное и служить аналогом открытого ключа авторизованного центра A.

Теперь рассмотрим осуществление протокола идентификации между картой и терминалом.

1. На первом шаге протокола карта называет себя и таким образом передает терминалу свой открытый ключ $U = P_U$.

2. Терминал подает на вход своего устройства $x_1 = R$ и $x_2 = P_U$, где R — случайное число, получая на выходе y_1 и y_2. Значение y_1 передается карте.

3. Карта подает на вход своего устройства полученное значение $x = y_1$ и вычисляет соответствующий y, который передает терминалу.

4. Терминал проверяет $y_2 = y$ и в случае равенства считает идентификацию успешной. В противном случае идентичность карты отвергается.

Рассмотрим описанный протокол более подробно. Фактически, он представляет собой протокол типа «оклик-отзыв» [1, 2], в котором терминал задает вопрос (случайное число), а карта должна правильно на него ответить, используя свой секретный ключ. Терминал при этом должен иметь возможность проверить правильность ответа карты.

В данном случае в качестве критерия правильности служит выработка картой и терминалом общего значения. Однако в качестве оклика используется не само случайное число, а его образ, вычисляемый с помощью односторонней функции H_2. Мотивация этого будет приведена ниже. Легко видеть, что значение, вычисляемое картой, представляет собой

$$y = H_1(y_2, S_U),$$

а значение, вычисляемое терминалом:

$$y_2 = H_1(H_2(R),\ E_{S_A}(U)) = H_1(y_1, S_U) = y.$$

Таким образом, при правильном функционировании и обладании картой знанием S_U, должно выполняться $y_2 = y$, что и проверяет терминал.

Отметим, что основными «строительными блоками» схем карты и терминала на рис. 1 и 2 являются секретная однонаправленная функция E_{S_A} и две открытые однонаправленные функции H_1 и H_2 (при этом нет необходимости специально публиковать H_1 и H_2). Можно заметить, что требования однонаправленности функций H_1 и H_2 удовлетворяются использованием (бесключевых) криптографических хэш-функций, а требование секретной односторонней функции может быть

реализовано с помощью симметричного блочного шифра или ключевой хэш-функции (например, кода аутентификации сообщения MAC) [1, 2].

Анализ протокола

Рассмотрим различные свойства полученного протокола.

Личностная идентификация. По построению данный протокол является основанным на идентичности пользователя, что являлось желаемым свойством, сформулированным выше.

Быстрая и компактная реализация. Протокол использует эффективно реализуемые криптопримитивы: хэш-функции и симметричный блоковый шифр, — что дает значительный выигрыш по ресурсоемкости в сравнении с теоретико-числовыми протоколами идентификации. Для многих практических систем этот выигрыш может достигать тысяч раз.

Требуемый трафик. Терминал пересылает карте значение y_1, являющееся выходом H_2. Карта пересылает терминалу идентичность U и значение y, являющееся выходом H_1. Если предположить, что в качестве однонаправленных функций используются хэш-функции ГОСТ Р 34.11–94 с 256-битными выходами, то терминал передает карте 256 бит, и карта передает 256 бит плюс размер U. Если считать, что размер U не превышает 256–512 бит, получаем общий трафик не более 1024 бит. Это соответствует всего лишь среднему размеру одного числа в теоретико-числовом протоколе идентификации (например, Фиата–Шамира [1, 4]), при этом в протоколе количество подобных передаваемых чисел оценивается примерно как $2t$, где t — количество раундов, обычно выбираемое порядка нескольких десятков.

Универсальность карты. Представленная на рис. 1 карта является универсальной в том смысле, что при смене пользователя или даже алгоритма преобразования E авторизованного центра нет необходимости проектировать новую карту — достаточно перезаписать хранимые в ней значения U и S_U (конечно, аппаратное обеспечение терминала при этом все же придется проектировать заново).

Стойкость. Сначала рассмотрим необходимость использования одностороннего преобразования H_2. В самом деле, в его отсутствие можно было бы описать схожий протокол следующим образом.

1. Карта называет себя и передает терминалу свой открытый ключ $U = P_U$.

2. Терминал отправляет карте случайное число R, одновременно вычисляя при этом $y_2 = H_1(R, E_{S_A}(U))$.

3. Карта подает на вход своего устройства полученное значение $x = R$ и вычисляет соответствующий y, который передает терминалу.

4. Терминал проверяет $y_2 = y$ и в случае равенства считает идентификацию успешной. В противном случае идентичность карты отвергается.

Легко видеть, что описанный протокол также «работает» с точки зрения легальных пользователей в том смысле, что если все участники честны, то действительно выполняется $y = y_2$.

Однако вспомним, что мы считали устройство терминала доступным всем участникам как своеобразный открытый ключ авторизованного центра A. В этом случае ничто не мешает злоумышленнику, не обладающему картой U, но желающему себя выдать за U, воспользоваться точно таким же устройством, что и у терминала, подать на его вход известные ему R и U и вычислить то же самое y_2, что и значение, полученное терминалом. Для предотвращения такой атаки случайный оклик терминала закрывается с помощью односторонней функции.

Стойкость данной системы основывается на стойкости используемых функций хэширования (необходима устойчивость к вычислению второго прообраза [3]) и шифрования.

Заключение

В статье рассмотрена схема идентификации, использующая в качестве базовых блоков эффективно реализуемые и не требовательные к ресурсам симметричные алгоритмы, применяемая в устройствах с ограниченными ресурсами, в которых затруднено использование традиционной теоретико-числовой криптографии с открытым ключом.

Литература

1. **Шнайер Б.** Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — 816 с.
2. **Menezes A. J., van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. — CRC Press, 1996. — 780 p.
3. **Shamir A.** Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology // Advances in Cryptology — CRYPTO 84: Lecture Notes in Computer Science. 1984. Vol. 196. N 7. P. 47–53.
4. **Fiat A., Shamir A.** How to Prove Yourself: Practical Solutions to Identification and Signature Problems // Advances in Cryptology — CRYPTO 86: Lecture Notes in Computer Science. 1987. Vol. 263. P. 186–194.