



УКРАЇНА

(19) UA (11) 40626 (13) C2

(51) 7 G07F7/10, G06K19/07

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВІНАХІД

(54) СПОСІБ ПЕРЕВІРКИ АВТЕНТИЧНОСТІ НОСІЯ ІНФОРМАЦІЇ І БЛОК ДЛЯ ЙОГО ЗДІЙСНЕННЯ

(21) 96020416

(22) 02.06.1995

(24) 15.08.2001

(31) P 44 19 805.1

(32) 06.06.1994

(33) DE

(86) PCT/EP95/02104, 02.06.1995

(46) 15.08.2001, Бюл. № 7, 2001 р.

(72) Ламла Міхель, DE, Ранкль Вольфганг, DE,
Вайкманн Франц, DE, Еффінг Вольфганг, DE

(73) ГІЗЕКЕ УНД ДЕВРІНТ ГМБХ, DE

(56) 1. DE, A, 4230866, 17.03.1994.

2. US, A, 5034596, 23.07.1991.

3. EP, A, 0409701, 23.01.1991.

4. EP, A, 0337185, 18.10.1989.

5. EP, A, 0256768, 24.02.1988.

6. FR, A, 2471003, 12.06.1981.

(57) 1. Способ проверки подлинности носителя информации, имеющего, по меньшей мере, интегральную схему с устройствами памяти и логическими схемами, содержащий операцию обмена данными с внешним устройством по линии данных, в процессе которой операционные и управляющие сигналы, необходимые для работы, носитель информации получает от внешнего устройства, **отличающийся** тем, что с помощью упомянутой интегральной схемы, дополнительно содержащей отдельную жестко прошитую схему для передачи и/или приема данных во время определенной согласно протоколу последовательности включения, используемую для проверки подлинности, начальную передачу или прием данных, используемых для проверки подлинности, завершают в течение определенного промежутка времени последовательности включения, при котором линия данных не находится в состоянии, определенном протоколом.

2. Способ по п. 1, **отличающийся** тем, что последовательность включения осуществляют согласно стандартизованному протоколу ISO/IEC 7816-3, начальную передачу или прием данных завершают в течение промежутка времени t_2 , определенного протоколом.

3. Способ по п. 2, **отличающийся** тем, что данные передают внешним устройством и принимают их носителем информации в течение промежутка времени t_2 , полученные данные передают обратно во внешнее устройство носителем информации также в течение промежутка времени t_2 и/или во

время определенного протоколом сигнала носителя информации "Ответ на сброс".

4. Способ по п. 3, **отличающийся** тем, что данные, принятые от внешнего устройства, комбинируют носителем информации с идентификационными данными носителя информации, и результат комбинирования передают обратно во внешнее устройство в течение промежутка времени t_2 или во время сигнала "Ответ на сброс".

5. Способ по п. 4, **отличающийся** тем, что результат комбинирования с идентификационными данными носителя информации передают последним во внешнее устройство для проверки подлинности.

6. Способ по п. 4, **отличающийся** тем, что данные, переданные внешним устройством, содержащие сгенерированное последним случайное число, комбинируют носителем информации с помощью операции "ИСКЛЮЧАЮЩЕЕ ИЛИ" с идентификационными данными носителя информации, или путем полиномиального деления по модулю упомянутого случайного числа на идентификационные данные в качестве полиномиального делителя.

7. Способ по п. 3, **отличающийся** тем, что данные, принятые от внешнего устройства, комбинируют с идентификационными данными носителя информации специальной схемой носителя информации, результат комбинирования (A) передают обратно во внешнее устройство в течение промежутка времени t_2 или во время сигнала "Ответ на сброс", и результат комбинирования (A) дополнительно передают в логические схемы интегральной схемы носителя информации.

8. Способ по п. 7, **отличающийся** тем, что результат логического комбинирования (A), переданный в логическую схему, передают логической схемой во внешнее устройство и проверяют во внешнем устройстве его соответствие заданному соотношению с результатом (A), переданным специальной схемой во внешнее устройство.

9. Способ по п. 8, **отличающийся** тем, что результат логического комбинирования (A) логически комбинируют с последующими данными в логической схеме носителя информации для получения результата (x), результат логического комбинирования (x) передают во внешнее устройство, и результат (A), полученный от специальной схемы, логически комбинируют с последующими данными во внешнем устройстве для получения ре-

зультата (x'), и результаты (x) и (x') проверяют во внешнем устройстве для получения заданного соотношения, согласно которому считают доказанным, что результат (A), переданный специальной схемой в логические схемы носителя информации правилен, и логически комбинирован также правильно, если указанное заданное соотношение после проверки оказывается верным.

10. Способ по п. 9, **отличающийся** тем, что данные внешним устройством передают в логическую схему носителя информации и логически комбинируют в нем с результатом (A) для получения результата (x), и ту же самую логическую комбинацию, что и в логической схеме носителя информации, выполняют во внешнем устройстве, что приводит к результату (x'), и результаты (x) и (x') проверяют во внешнем устройстве на совпадение.

11. Способ по любому из пп. 8, 9, **отличающийся** тем, что в логической схеме носителя информации результат (A) логически комбинируют с данными, хранимыми в устройствах памяти носителя информации для получения результата (x), и специальной схемой носителя информации передают данные во внешнее устройство, и результат (A) комбинируют во внешнем устройстве с данными, дополнительно переданными специальной схемой для получения результата (x'), и результат (x), переданный логической схемой, проверяют во внешнем устройстве на соответствие заданному соотношению с результатом (x'), вычисленным в нем, согласно чему считают доказанным, что данные, хранимые в устройствах памяти носителя информации, находятся в заданном соотношении с данными, хранимыми в специальной схеме, если результат проверки положительный.

12. Способ по п. 2, **отличающийся** тем, что идентификационные данные носителя информации передают во внешнее устройство носителем информации в течение промежутка времени t_2 и затем оценивают их внешним устройством для проверки подлинности носителя информации.

13. Способ по п. 12, **отличающийся** тем, что идентификационные данные носителя информации комбинируют носителем информации со случайным числом, сгенерированным носителем информации до передачи во внешнее устройство, а результат этой комбинации передают во внешнее устройство для проверки подлинности носителя информации.

14. Способ по любому из пп. 1-13, **отличающийся** тем, что данные, используемые для проверки подлинности, передают синхронно с временным сигналом, передаваемым внешним устройством в носитель информации.

15. Способ по п. 14, **отличающийся** тем, что передачу данных для проверки подлинности осуществляют синхронно с множеством внешних тактовых частот.

16. Блок проверки подлинности носителя информации, содержащий носитель информации, имеющий, по меньшей мере, интегральную схему с устройствами памяти и логическими схемами и выполненный с возможностью обмена данными с внешним устройством по линии данных и получающий от внешнего устройства операционные и управляющие сигналы, необходимые для работы носителя информации, и внешнее устройство,

имеющее доступ для считывания и/или записи, по меньшей мере, в отдельные области устройств памяти носителя информации, **отличающийся** тем, что интегральная схема дополнительно содержит отдельную жестко прошитую схему для передачи и/или приема данных во время определенной согласно протоколу последовательности включения, используемую для проверки подлинности, причем отдельная жестко прошитая схема выполнена с возможностью начальной передачи или приема данных, используемых для проверки подлинности независимо от логических схем и устройств памяти носителя информации в течение определенного промежутка времени последовательности включения, при котором линия данных не находится в состоянии, определенном протоколом.

17. Блок проверки подлинности носителя информации по п. 16, **отличающийся** тем, что идентификационные данные носителя информации в отдельной жестко прошитой схеме реализованы аппаратно.

18. Блок проверки подлинности носителя информации по п. 17, **отличающийся** тем, что идентификационные данные носителя информации реализованы с помощью плавких перемычек, причем, по меньшей мере, некоторые из них прожжены, а каждая отдельная плавкая перемычка идентификационных данных имеет соответствующую ей комплементарную плавкую перемычку, находящуюся в противоположном ей состоянии.

19. Блок проверки подлинности носителя информации по п. 18, **отличающийся** тем, что его отдельная жестко прошитая схема включает устройство для проверки нахождения комплементарной плавкой перемычки, связанной с каждой плавкой перемычкой, в своем правильном состоянии, а идентификационные данные носителя информации считываемы только в случае, если все плавкие перемычки и соответствующие им комплементарные перемычки находятся в правильном состоянии.

20. Блок проверки подлинности носителя информации по любому из пп. 17-19, **отличающийся** тем, что отдельная жестко прошитая схема носителя информации выполнена с возможностью передачи идентификационных данных носителя информации во внешнее устройство в течение промежутка времени t_2 , определенного протоколом ISO/IEC 7816-3.

21. Блок проверки подлинности носителя информации по п. 17, **отличающийся** тем, что отдельная жестко прошитая схема носителя информации выполнена с возможностью генерирования случайного числа и комбинирования его с идентификационными данными носителя информации.

22. Блок проверки подлинности носителя информации по п. 17, **отличающийся** тем, что отдельная жестко прошитая схема носителя информации выполнена с возможностью комбинирования случайного числа, принятого от внешнего устройства, с идентификационными данными носителя информации.

23. Блок проверки подлинности носителя информации по п. 16, **отличающийся** тем, что его внешнее устройство содержит микропроцессорное

устройство и модуль защиты, управляемый микропроцессорным устройством.

24. Блок проверки подлинности носителя информации по любому из пп. 22, 23, **отличающийся** тем, что модуль защиты соединен напрямую с логическими схемами носителя информации так, что обмен данными между модулем за-

щиты и логическими схемами осуществляется в одном или двух направлениях.

25. Блок проверки подлинности носителя информации по любому из пп. 22-24, **отличающийся** тем, что модуль защиты выполнен в виде платы интегральных схем с возможностью установки его в разъем внешнего устройства.

Данное изобретение относится к способу проверки подлинности носителя информации, а также к конструкции носителя информации, реализующей данный способ.

Способ тестирования подлинности известен, например, из EP-A10 321728. В известном способе носитель информации переключается управляющим сигналом, переданным внешним устройством, из нормального режима в режим проверки, в котором осуществляется тестирование. Для этой цели носитель информации имеет дополнительное переключающее логическое устройство, которое осуществляет указанное переключение в соответствии с внешним сигналом. В режиме проверки затем носитель информации получает извне проверяющие данные, которые обрабатываются дополнительным электронным устройством, например, аналоговым компьютером. Время, которое требуется аналоговому компьютеру для обработки проверяющих данных, составляет характерную черту подлинности для носителя информации. В известном способе тестирования подлинности, производимое в режиме проверки носителя информации, отделено от нормального режима так, что нормальный режим, который, как правило, подчиняется стандартизованным протоколам, не нарушается тестированием подлинности. Однако, это означает, что переключение из нормального режима в режим тестирования с помощью дополнительной переключающей логической схемы необходимо перед каждым тестированием подлинности.

Задачей изобретения является предложение способа тестирования подлинности носителя информации, в котором указанное тестирование подлинности совместимо с существующими стандартизованными протоколами и может быть выполнено с небольшим усложнением схем.

Данная задача решается с помощью признаков, указанных в п. 1 формулы изобретения.

Основная идея изобретения состоит в том, что первая передача или прием данных, используемых для тестирования подлинности, имеют место во время последовательности включения для носителя информации, в течение которой линия данных имеет еще не определенное состояние для обмена данными с внешним устройством. Например, линия данных может быть в неопределенном состоянии в течение определенного промежутка времени во время последовательности включения в соответствии со стандартом ISO/IEC 7816-3. Так как первая передача или прием данных завершается в течение интервала времени, определенным стандартом, то обмен данными, стандартизованный для связи с платами ин-

тегральных микросхем, не нарушается. Тестовая процедура поэтому может быть проведена, согласно данному изобретению, с существующими протоколами, подчиняющимися стандартам.

Носитель информации имеет дополнительное специальное устройство для передачи во внешнее устройство или приема от него данных, требуемых для тестирования подлинности за указанный промежуток времени, в течение которого линия данных должна иметь состояние, не определенное протоколом.

В первом воплощении, например, идентификационные данные носителя информации, реализованные в аппаратуре, могут быть переданы на внешнее устройство в течение указанного промежутка времени. Внешнее устройство, например, плата устройства считывания, также имеет специальное устройство, разрешающее прием данных, переданных платой в течение этого промежутка времени так, чтобы устройство могло выполнить тестирование подлинности. Но даже если устройство не имеет такого специального устройства и поэтому не находится в положении приема данных, переданных платой в течение указанного времени, протокол обмена не нарушается передачей данных. Поэтому при запуске протокола не возникает никаких ошибок, когда плата обменивается с обусловленным устройством в течение указанного времени.

Согласно изобретению, специальное устройство, расположенное в интегральной схеме носителя информации, может также генерировать случайное число в течение указанного интервала времени, которое затем логически комбинируется с идентификационными данными носителя информации специальной переключающей логической схемой носителя информации, результат комбинирования передается от носителя информации на внешнее устройство в течение указанного промежутка времени, но самое позднее - во время сигнала "Ответ на сброс" (ATP). Использование случайного числа делает ответную атаку невозможной, т.е. ответ ранее переданных данных.

В следующем воплощении внешнее устройство, т.е. плата считывающего устройства, может иметь также дополнительное устройство, которое служит для генерации случайного числа. Случайное число затем передается на носитель информации синхронно с временным сигналом в течение указанного промежутка времени из-за высокой скорости передачи. Специальное дополнительное устройство носителя данных находится в положении приема переданного случайного числа в указанном промежутке времени, в течение которого контактный элемент имеет неустановив-

шееся состояние, и передачи, по меньшей мере, части принятого случайного числа обратно во внешнее устройство в течение этого промежутка времени. Дополнительно к этому специальная перекрывающаяся логическая схема носителя информации может также логически комбинировать принятое случайное число с идентификационными данными носителя информации и передавать результат комбинирования обратно во внешнее устройство в течение указанного промежутка времени или самое позднее - во время сигнала ATP для определения факта приема случайного числа. Внешнее устройство может затем использовать результат комбинирования, принятый от носителя информации, для проверки способен ли носитель информации правильно принимать переданное случайное число в течение указанного промежутка времени, корректно комбинировать его с идентификационными данными носителя информации и передавать его на внешнее устройство в течение заданного промежутка времени. Наличие результата комбинирования в ATP сигнале образует идентификационные данные класса для носителя информации, которые могут быть оценены как таковые внешним устройством, в то время как содержимое результата комбинирования образует идентификационные данные, специфичные для носителя информации.

Другие преимущества и достоинства могут быть найдены в описании изобретения со ссылками на чертежи, на которых фиг. 1 изображает устройство носителя информации для тестирования подлинности; фиг. 2 изображает образец стандартизованного сигнала в последовательности включения носителя информации; фиг. 3 по фиг. 5 изображают реализацию изобретенной процедуры тестирования во время передачи носителем информации данных; фиг. 6 и фиг. 7 каждая изображают воплощение изобретенного способа, в которой данные передаются внешним устройством и принимаются носителем информации; фиг. 8 изображает устройство носителя информации, состоящего из внешнего устройства и носителя информации для тестирования подлинности носителя информации; фиг. 9 изображает модуль безопасности, который является частью внешнего устройства и используется для выполнения тестирования подлинности; фиг. 10 изображает устройство носителя информации, состоящего из внешнего устройства и носителя информации для тестирования подлинности носителя информации; фиг. 11 изображает носитель информации, в который встроен модуль безопасности; фиг. 12 изображает поперечное сечение электронного модуля носителя информации, изображенного на фиг. 8а; фиг. 13 изображает базовую электрическую схему носителя информации; фиг. 14 изображает воплощение специального устройства; фиг. 15 изображает дальнейшее воплощение специального устройства носителя информации; фиг. 16 изображает часть специального устройства; фиг. 17 и 18 изображают диаграммы тестирования подлинности носителя информации.

Фиг. 1 изображает устройство носителя информации, предназначенное для тестирования подлинности в виде платы интегральных микросхем 1, которая обменивается через линию данных

2 с внешним устройством 3, например, платой устройства считывания. Плата интегральных микросхем может быть контактирующей или бесконтактной, который обменивается с внешним устройством без контакта.

Фиг. 2 изображает образец сигнала сброса носителя информации так, как он стандартизован, например, в международном стандарте ISO/IEC 7816-3. Можно видеть потенциал земли GND, подачи напряжения питания VCC, сигнал сброса RST, подаваемый извне для сброса носителя информации, временной сигнал CLK и линию данных ввода/вывода (I/O). Когда подано питающее напряжение, и напряжение стабилизировано, и подан временной сигнал в момент времени T_0 , линия данных I/O находится в режиме приема сигнала сброса RST, подаваемого внешним устройством в момент времени T_1 . С момента времени T_0 линия данных I/O может быть в неопределенном состоянии в течение времени t_2 в соответствии с указанным стандартом. Согласно стандарту промежуток времени t_2 должен быть меньше или равен длительности 200 временных циклов, разделенной на временную частоту f_1 . Когда этот промежуток времени превышен, то линия данных ввода/вывода должна быть в определенном состоянии и поэтому не может быть использована для передачи или приема данных до прихода сигнала RST. После приема сигнала сброса RST в момент времени T_1 носитель информации отвечает сигналом "Ответ на сброс" ATP после периода времени t_1 .

Фиг. 3 изображает процесс первой передачи, например, передачи своих идентификационных данных KN носителем информации к внешнему устройству в течение промежутка времени t_2 . Как только принимается временной сигнал CLK, носитель информации автоматически передает идентификационные данные, например, серийный номер, прямо во внешнее устройство, предпочтительно, синхронно с временным сигналом. Синхронная передача предполагает более высокую скорость передачи, чем асинхронная передача. Конечно серийный номер может быть также передан асинхронно с временным сигналом, если это может быть сделано в течение промежутка времени t_2 . В любом случае носитель информации имеет не только обычные логические устройства и устройства памяти, но также и специальное устройство, которое позволяет осуществить эту быструю передачу в течение оговоренного промежутка времени. С помощью стандартной команды внешнее устройство может затем считать серийный номер, хранящийся в памяти в носителе информации и сравнить его с серийным номером, принятым от носителя информации. Если серийный номер, переданный носителем информации посредством специального устройства, совпадает с серийным номером, считанным из памяти носителя информации, то носитель информации определенно способен передать данные, необходимые для тестирования подлинности, очень быстро в течение промежутка времени t_2 . Это свойство является свойством подлинности, которое может быть осуществлено не оговоренным носителем информации, т.е. носителем информации без указанного специального устройства.

Этап способа, изображенный на фиг. 4, является расширением способа, изображенного на фиг. 3.

Идентификационные данные KN комбинируются, например, с помощью схемы "ИСКЛЮЧАЮЩЕЕ ИЛИ" со случайным числом RND, сгенерированным носителем информации, а результат комбинирования со сгенерированным случайным числом RND передается во внешнее устройство. Случайное число генерируется в течение промежутка времени t_2 . Результат комбинирования со случайным числом RND также передается преимущественно в течение промежутка времени t_2 . Однако также возможно, как показано на фиг. 5, передать результат комбинирования и случайное число в сигнале "Ответ на сброс" носителя информации, например, в исторических символах АТР сигнала. Внешнее устройство может затем на более позднем шаге подлинности в соответствии с запуском нормального протокола комбинировать принятое случайное число с идентификационными данными KN, считанными из памяти в носителе информации, повторно с помощью той же самой логической операции и сравнивать результаты комбинирования с результатом комбинирования из носителя информации, переданного во время сигнала АТР. Использование случайного числа делает ответную атаку невозможной, т.е. ответную атаку ранее записанных данных.

Фиг. 6 изображает дальнейшее воплощение изобретенного способа. На первом шаге способа внешнее устройство передает случайное число RND, которое может включать, например, 8 байт, в носитель информации в течение промежутка времени t_2 . Передача преимущественно осуществляется синхронно с временным сигналом, но может быть реализована также и асинхронно. В течение промежутка времени t_2 носитель информации передает, по меньшей мере, последний байт R_8 принятого случайного числа обратно во внешнее устройство. Внешнее устройство затем сравнивает последний байт R_8 случайного числа, сгенерированного им, с байтом R_8 , принятым от носителя информации. Если они совпадают, то носитель информации может принимать передаваемое случайное число правильно и передавать, по меньшей мере, часть обратно. Тот факт, что носитель информации может принимать данные очень быстро, является особенностью подлинности. Носитель информации может, конечно, передавать также и все случайное число, принятое в течение промежутка времени t_2 обратно во внешнее устройство, что лучше, чем передача последнего байта случайного числа. Это может иметь место также, например, во время сигнала АТР.

К тому же случайное число RND, принятое от внешнего устройства в течение промежутка времени t_2 , может быть скомбинировано с помощью логической операции с идентификационными данными KN носителя информации специальной логической переключатальной схемой носителя информации. Что касается логической операции, то она может использовать, например, полиномиальное деление по модулю, используя идентификационные данные в качестве полиномиального делителя для случайного числа. Эта логическая операция хорошо известна специалистам и не

требует поэтому более подробного описания. Идентификационные данные KN, скомбинированные указанным способом со случайным числом носителя информации, могут быть затем переданы во внешнее устройство в течение промежутка времени t_2 или в течение сигнала АТР носителя информации. Оба варианта здесь допустимы. Затем внешнее устройство опять вычисляет случайное число, принятое носителем информации, из результата комбинирования случайного числа и идентификационных данных путем выполнения обратной функции применительно к логической операции и сравнивает его со случайным числом, сгенерированным внешним устройством. Если они совпадают, то это говорит о том, что носитель информации, в частности - специальное устройство носителя информации, способно принимать и комбинировать случайное число очень быстро и передавать результат комбинирования во внешнее устройство в течение промежутка времени t_2 или в течение самого позднего сигнала АТР носителя информации, например, в исторических символах.

Фиг. 7 изображает дальнейшее воплощение, в котором случайное число RND, переданное внешним устройством, и которое может включать, например, несколько байт, принимается носителем информации в течение промежутка времени t_2 посредством чего или целое случайное число или, по меньшей мере, последний байт переданного случайного числа, в зависимости от длины случайного числа, комбинируется с идентификационными данными KN носителя информации схемой "ИСКЛЮЧАЮЩЕЕ ИЛИ", а результат комбинирования передается во внешнее устройство совместно с идентификационными данными носителя информации в течение промежутка времени t_2 или в течение сигнала АТР. Внешнее устройство затем опять выполняет ту же самую логическую операцию, начиная от принятых идентификационных данных KN и сгенерированного случайного числа RND, и сравнивает результат комбинирования, полученный внешним устройством, с результатом комбинирования, принятым от носителя информации.

Чертежи на фиг. с 3 по 7 показывают, что для тестирования подлинности носителя информации внешнее устройство должно выполнить операции вне периода нормального обмена, между внешним устройством и носителем информации. Например, внешнее устройство передает в носитель информации случайное число, которое логически комбинируется с идентификационными данными, как описано выше, а результат логического комбинирования проверяется во внешнем устройстве.

Возможно создание микропроцессорного устройства во внешнем устройстве в правой части чертежа так, чтобы оно выполняло операции, необходимые для тестирования подлинности носителя информации. В уже работающих внешних устройствах микропроцессор не формируется таким образом. Если они, тем не менее, должны использоваться для тестирования подлинности, то особенно выгодно предложить внешнее устройство с дополнительно подключенным к его микропроцессорному устройству модулем безопасности для выполнения тестирования. Многие уже ис-

пользуемые внешние устройства снабжаются, по меньшей мере, одним дополнительным разъемом для, по меньшей мере, одного дополнительного модуля так, что специальной адаптации внешнего устройства не требуется. Эти разъемы труднодоступны снаружи, поэтому нет также проблемы безопасности при обеспечении функций, необходимых для тестирования подлинности в отдельном модуле безопасности.

В особенно выгодном воплощении модуль безопасности может быть сделан, как и носитель информации, в виде платы интегральных микросхем, которая предпочтительно формируется как встраиваемая (т.е. плата с меньшими размерами, чем стандартная плата) из-за пространственного ограничения в большинстве внешних устройств.

Фиг. 8 изображает схематически конструкцию носителя информации для тестирования подлинности носителя информации в виде платы 1, которая обменивается с внешним устройством 3. Показаны только те соединяющие линии между компонентами, которые необходимы для понимания последующих положений. Внешнее устройство 3 имеет, кроме всего прочего, микропроцессорное устройство 4 и модуль безопасности 5. Для обмена данными между носителем информации 1 и внешним устройством 3 микропроцессорное устройство 4 сначала включается, затем распознает, что носитель информации находится во внешнем устройстве 3. Затем модуль безопасности 5 включается микропроцессорным устройством 4 и запрашивается для тестирования подлинности носителя информации 1. Это может быть осуществлено, например, по линиям управления ST1 и ST2, на которые подается определенный сигнал, соответствующий запросу, например, сигнал логический 1, на линию управления ST1 и на линию управления ST2. Случайное число затем генерируется модулем безопасности 11 и сначала запоминается в модуле безопасности 5 после запроса микропроцессорным устройством 4. Запрос может быть сделан опять, например, по линиям управления ST1 и ST2, на которые опять подается определенный сигнал, например, сигнал логического 0 на линию управления ST1 и сигнал логической 1 на линию управления ST2.

После запоминания случайного числа в модуле безопасности 5, носитель информации 1 включается микропроцессорным устройством 4, как объяснено выше применительно к фиг. 2. Когда напряжение питания подается на носитель информации 1, напряжение стабилизировано и временной сигнал подается на носитель информации 1 в момент времени T_0 , а линия данных ввода/вывода подключается к носителю информации 1, который находится в режиме приема сигнала сброса RST, поданного на носитель информации микропроцессорным устройством 4. Начиная с момента времени T_0 , линия данных ввода/вывода, подключенная к носителю информации 1, может находиться в неопределенном состоянии в течение промежутка времени t_2 , как описано выше, применительно к фиг. 2. Промежуток времени t_2 используется для тестирования свойства подлинности носителя информации 1 с помощью модуля безопасности 5.

С этой целью модуль безопасности 5 передает вышеуказанное запомненное случайное

число в носитель информации 1 по линии ввода/вывода после включения носителя информации, а микропроцессорным устройством 4 выдается запрос. Запрос для передачи случайного числа может быть осуществлен опять по линиям управления ST1 и ST2, на которые подается определенный сигнал (например, сигнал логической 1 на линию управления ST1 и сигнал логического 0 на линию управления ST2).

В носителе информации 1 переданное случайное число логически комбинируется с идентификационными данными KN в течение промежутка времени t_2 , а результат комбинирования передается носителем информации 1 вместе с идентификационными данными KN обратно в модуль безопасности 5 внешнего устройства 3.

В модуле безопасности 5 переданные идентификационные данные KN также логически комбинируются со случайным числом точно так же, как и в носителе информации 1, и результат комбинирования сравнивается с результатом, переданным носителем информации. Совпадение результатов доказывает, что носитель информации 1 является подлинным. Соответствующее сообщение передается модулем безопасности 5 в микропроцессорное устройство 4, которое затем начинает обмен между внешним устройством 3 и носителем информации 1.

Хотя тестирование свойства подлинности, описанное применительно к фиг. 8, на первый взгляд аналогично тестированию, описанному применительно к фиг. 6, модуль безопасности 5 в действительности также может использоваться для выполнения любых, отличных от данного, тестов подлинности (см. например, фиг. 3 и фиг. 8). Модуль безопасности 5 затем должен быть адаптирован к конкретному свойству подлинности носителя информации 1.

Фиг. 9 схематически показывает пример конструкции модуля безопасности 5. Как и фиг. 8, фиг. 9 показывает только те линии соединения между отдельными компонентами, которые необходимы для понимания. На изображенной конструкции модуль безопасности 5 имеет стандартное микропроцессорное устройство 6, выполненное в виде отдельной интегральной схемы. Более того, модуль безопасности 5 имеет интегральную схему 7, подсоединенную к стандартному микропроцессорному устройству 6. Интегральная схема 7 имеет возможно более простую структуру для того, чтобы она могла быстро и легко управляться, а тест свойства подлинности носителя информации 1 (не показан) проходил быстро.

Интегральная схема 7 предпочтительно имеет жесткую логику, которая может быть быстро и легко управляться микропроцессорным устройством 4 по линиям управления ST1 и ST2 (сравни также фиг. 6). Могут быть определены, к примеру, следующие сигналы управления:

- логический 0 на линии управления ST1, логический 0 на линии управления ST2 означают: свойство подлинности не может быть протестировано;

- логическая 1 на линии управления ST1, логическая 1 на линии управления ST2 означают: свойство подлинности может быть протестировано;

- логический 0 на линии управления ST1, логическая 1 на линии управления ST2 означают: случайное число, сгенерированное в модуле безопасности 5, должно быть сначала запомнено в регистрах интегральной схемы 7 (сравни также фиг. 8);

- логическая 1 на линии управления ST1, логический 0 на линии управления ST2 означают: содержимое вышеуказанных регистров, т.е. случайное число, должно быть передано в носитель информации (сравни также фиг. 8).

Две линии управления ST1 и ST2, таким образом, позволяют осуществить управление интегральной схемой 7 и, таким образом, внешнее управление модулем безопасности.

Далее будет рассматриваться внутренний обмен между интегральной схемой 7 и стандартным микропроцессорным устройством 4. После запроса на интегральную схему 7 от микропроцессорного устройства 4 для тестирования свойства подлинности носителя информация 1, интегральная схема 7 включает стандартное микропроцессорное устройство 6 в соответствии с последовательностью включения по стандарту ISO (ISO/IEC 7816-3). Последовательность включения известна специалистам и, кроме того, кратко объяснялась выше применительно к фиг. 2, поэтому нет необходимости обсуждать это более подробно.

Стандартное микропроцессорное устройство 6 затем генерирует случайное число, которое передается в интегральную схему 7 и запоминается там в вышеуказанном регистре. Запомненное случайное число передается в носитель информации 1 после запроса микропроцессорным устройством 4 (см. выше) и логически комбинируется там, как объяснено выше применительно к фиг. 8. Носитель информации 1 затем передает информацию, необходимую для тестирования свойства подлинности в модуль безопасности 5, что также объяснялось выше применительно к фиг. 8. Переданная информация запоминается во временных регистрах интегральной схемы 7. Стандартный микропроцессор 6 затем запрашивает запомненную информацию из интегральной схемы 7 и проверяет исходное случайное число (см. выше).

Применительно к фиг. 9 объяснялось, что модуль безопасности 5 имеет две интегральные схемы, которые выполняют оговоренные функции. Очевидно также, что возможно объединить две интегральные схемы в одну или предложить интегральную схему с микропроцессорным устройством, которая управляется, как обычно, некоторыми командами от микропроцессорного устройства 4 и независимо тестирует свойство подлинности. Однако такое управление посредством команд микропроцессора, как правило, требует больше времени, чем вышеуказанное управление интегральной схемой 7 по линиям управления ST1 и ST2.

Техническая реализация, в которой модуль безопасности 5 имеет только одну интегральную схему, показана на фиг. 10. Интегральная схема имеет микропроцессорное устройство, построенное так, чтобы оно могло выполнять функции, необходимые для тестирования свойства подлинности. Обмен между микропроцессорным устройством 4, модулем безопасности 5, внешним

устройством 3 и носителем информации 1 внешне производится аналогично описанному выше, применительно к фиг. 8, так что далее будут обсуждаться только отличия.

Интегральная схема 7 управляется микропроцессорным устройством 4 по линиям ввода/вывода 1 (I/O₁). Команды микропроцессора, необходимые для тестирования свойства подлинности, также передаются по линии ввода/вывода 1. Соответствующие команды были объяснены выше применительно к фиг. 9. В показанном воплощении, не показаны также линии управления ST1 и ST2, как это показано на фиг. 8.

Данные, переданные в носитель информации 1 интегральной схемой 7 модуля безопасности 5, также соответствуют данным, переданным на фиг. 8. Эти данные могут быть переданы из интерфейса ввода/вывода 2 (I/O₂) интегральной схемы 7, который всегда присутствует в коммерческих интегральных схемах для плат интегральных микросхем, в интерфейс ввода/вывода 1 (I/O₁) носителя информации. В этом случае пути передачи команд от микропроцессорного устройства 4 до интегральной схемы 7 и данных из интегральной схемы 7 в носитель информации 1 отличаются друг от друга. Очевидно также, что возможно передавать данные из интерфейса ввода/вывода 1 (I/O₁) интегральной схемы 7 в интерфейс I/O₁ носителя информации 1, что также показано на фиг. 8.

Фиг. 11 изображает в большом увеличении и неточном масштабе встраиваемую карту 8, в которой модуль безопасности 5 построен в виде электронного модуля 9. Миниплата микросхем 8 вставляется в один из вышеуказанных разъемов во внешнем устройстве 3 так, что свойство подлинности носителя информации может быть проверено теперь с помощью карты 8 (см. фиг. 1).

Фиг. 12 изображает также в большом увеличении и неточном масштабе поперечное сечение электронного модуля по линии AA, показанной на фиг. 11. Структура такого электронного модуля известна (например, из EP 0299530 B1), поэтому нет необходимости это подробно объяснять. Электронный модуль одержит стандартное микропроцессорное устройство 6 и интегральную схему 7, которые электрически соединяются с контактными поверхностями 10. Две интегральные схемы накладываются друг на друга, как показано на фиг. 12, но могут быть, конечно, расположены и рядом. Обе микросхемы могут обмениваться данными друг с другом и с микропроцессорным устройством 4 после подачи на них соответствующего напряжения и сигналов через контактные поверхности 10. Последовательность обмена между компонентами была описана выше.

Теперь, когда обмен между внешним устройством 3 и носителем информации 1 и внутренний обмен между во внешнем устройстве 3 объяснены, будет обсуждаться сам носитель информации 1.

Носитель информации 1, схематически изображенный на фиг. 13, отличается от обычных носителей информации, например, наличием микропроцессора, в котором, дополнительно к обычному микроконтроллеру 11 добавлена специальная схема 12 для передачи или приема данных и,

может быть, комбинирования данных с идентификационными данными носителя информации, реализованными в аппаратуре, например, серийным номером. Идентификационные данные носителя информации могут быть записаны, например, во время процесса производства интегральной схемы прожиганием плавких перемычек в качестве свойства аппаратуры для специального устройства интегральной схемы. Аппаратная реализация таких идентификационных данных описана, например, в еще не опубликованной заявке на патент РСТ/ЕР 93/03668. Дополнительно к реализации, описанной в настоящем изобретении, идентификационные данные могут быть записаны также установкой перемычек лазерным резцом на подложке при изготовлении так, что перемычки необратимо устанавливаются в определенное логическое состояние.

Следующей возможностью реализации идентификационных данных в аппаратуре является возможность формирования некоторых областей в кремниевой подложке интегральной схемы в качестве аморфных кремниевых областей и использования этих областей в качестве плавких перемычек. Эти аморфные области являются непроводящими, но могут быть преобразованы в кристаллические проводящие кремниевые области путем пропускания достаточно сильного тока через эти области. Не прожженные плавкие перемычки являются непроводящими, а прожженные - проводящими. Особым преимуществом формирования перемычек для идентификации в качестве аморфных кремниевых областей является то, что визуально аморфный кремний нельзя отличить от кристаллического. Таким образом, идентификационные данные не могут быть считаны с помощью оптических методов.

Микроконтроллер 11 носителя информации может также прямо обращаться к специальному устройству 12 в показанной конфигурации. Например, микроконтроллер 11 может считывать результат комбинирования, вычисленный специальной логической переключающей схемой 12, когда результат, вычисленный специальной логической схемой 12, должен быть передан во внешнее устройство как часть АТР сигнала, например, в исторических символах. Однако, специальная логическая схема 12 может также передать результат комбинирования прямо во внешнее устройство через линии данных ввода/вывода в течение промежутка времени t_2 без участия микроконтроллера 11, т.к. специальная схема 12 соединена линиями GND, VCC, сброса, временных импульсов и линией ввода/вывода данных (I/O). Такая конфигурацию аппаратуры носителя информации допускает, чтобы быстрая передача или прием данных и, возможно, комбинация данных с идентификационными данными носителя информации, были выполнены в течение указанного промежутка времени t_2 . Вместо линии ввода/вывода специальное устройство 12 может быть также подсоединено с помощью одной из двух RFU (зарезервированных для будущего использования) линий, которые здесь не показаны. Инсталляция этой специальной схемы в качестве свойства подлинности для носителя информации предотвращает способ тестирования подлинности от эмуляции или модели-

рования его определенными носителями информации, например, устройствами, имеющими микропроцессор, микропроцессором или внешним логическим устройством.

Фиг. 14 изображает существенные части специального устройства 12 носителя информации, которое, например, способно выполнять полиномиальное деление по модулю случайного числа с идентификационными данными носителя информации в качестве полиномиального делителя. Специальная схема 12 включает, например, 32 схемы "ИСКЛЮЧАЮЩЕЕ ИЛИ", 32 схемы "И", вентиль (схему) "НЕ" и регистр сдвига А. Кроме того, интегральная схема носителя информации содержит перемычки (не показаны), которые установлены, например, посредством лазерного резца, в определенное состояние во время производства подложки. Эти плавкие перемычки могут быть использованы, например, для установки идентификационных данных в качестве свойства аппаратуры, далее регистра В, содержащего комбинацию логических состояний набора перемычек. Случайное число RND, переданное внешним устройством, загружается в сдвиговый регистр А, а логические схемы - вентили - используются для выполнения полиномиального деления по модулю битовых позиций случайного числа, находящегося в регистре А, на число в регистре В, которое определяется идентификационными данными носителя информации, например серийным номером.

Фиг. 15 изображает дальнейшее воплощение дополнительной логической специальной схемы 12 носителя информации. В данном воплощении случайное число RND, переданное внешним устройством, передается на первый регистр сдвига SR1, в то время как идентификационные данные KN носителя информации содержатся в регистре В. Идентификационные данные носителя информации могут состоять, например, из двух частей, вторая часть является отрицанием (инверсией) битовой последовательности первой части. Синхронно с временной последовательностью случайное число RND затем комбинируется с помощью операции "ИСКЛЮЧАЮЩЕЕ ИЛИ" с идентификационными данными, например, серийным номером. Когда комбинирование завершено, что устанавливается посредством соответствующего счетчика, результат комбинирования, также как и идентификационные данные, пересылаются во второй регистр сдвига синхронно с временной последовательностью и передаются обратно во внешнее устройство. Этот процесс имеет место преимущественно в течение промежутка времени t_2 .

Вышеуказанные положения показывают, что идентификационные данные, содержащиеся в специальной схеме 12 носителя информации 1, являются существенными для тестирования подлинности носителя информации. Если они являются специфическими идентификационными данными носителя информации, например, то другая специфическая особенность может быть смоделирована посредством изменения идентификационных данных. По этой причине особенно важно, чтобы идентификационные данные информации 1 нельзя было фальсифицировать.

Если идентификационные данные носителя информации реализованы, например, как аппарат-

ные идентификационные данные с помощью прожигания плавких перемычек (см. также положения к фиг. 13), идентификационные данные могут быть защищены от фальсификации при использовании устройства, показанного на фиг. 16, которое является частью специальной схемы 12 (см. фиг. 13). Фиг. 16 показывает тридцать две плавкие перемычки, которые являются или прожженными, как перемычки первая и вторая, или не прожженными, как перемычка тридцать вторая. Прожженная перемычка вследствие этого ассоциируется с логической первой, а не прожженная - с логической нулевой. Перемычки с первой по тридцать вторую представляют собой идентификационные данные носителя информации. Каждая отдельная плавкая перемычка с первой по тридцать вторую имеет связанную с ней комплементарную (дополнительную) плавкую перемычку, которая находится в комплементарном состоянии со связанной перемычкой (т.е. комплементарная перемычка для прожженной перемычки является не прожженной и наоборот). Первая комплементарная перемычка, ассоциированная с первой перемычкой, является соответственно не прожженной, т.к. показанная плавкая перемычка первая является прожженной. То же самое относится ко второй комплементарной перемычке, ассоциированной со второй плавкой перемычкой. Наоборот, комплементарная перемычка тридцать вторая является прожженной в данном примере согласно фиг. 16, т.к. плавкая перемычка тридцать вторая показана как не прожженная.

Вентили "ИСКЛЮЧАЮЩЕЕ ИЛИ" 13, показанные на фиг. 16, проверяют, какая комплементарная плавкая перемычка, связанная с перемычкой, в действительности находится в комплементарном состоянии. Вентиль 13 выдает логическую один со своего выхода 14 только в случае, если входы 15 и 16 вентилля находятся в комплементарном состоянии; входы 15 и 16, соответствуют логическим состояниям плавкой перемычки и связанной с ней комплементарной перемычки.

Наконец, вентиль "И" 17 проверяет, есть ли логические один на всех выходах вентилей "ИСКЛЮЧАЮЩЕЕ ИЛИ" 13, которые поступают на входы вентилля "И" 13. В этом случае выход вентилля "И" 17 выдает логическую один, в противном случае - логический 0. Только в случае, когда вентиль "И" 17 выдает логическую один, можно быть уверенным, что комплементарные плавкие перемычки, связанные с каждой перемычкой, находятся в своем правильном состоянии. Специальная схема 12 носителя информации построена так, чтобы идентификационные данные могли быть использованы для тестирования подлинности носителя информации только, если они подлинны, т.е. если логическая 1 присутствует на выходе вентилля "И" 17.

Если идентификационные данные носителя информации 1 должны быть фальсифицированы с целью обмана, то состояния плавких перемычек с первой по тридцать вторую, которые определяют идентификационные данные, должны быть установлены, по крайней мере частично, в другое состояние. На устройстве, показанном на фиг. 16, перемычка тридцать два может быть, например, прожжена для фальсификации идентификацион-

ных данных так, чтобы она показывала состояние логической один. В этом случае, однако, состояние комплементарной перемычки тридцать два должно быть нарушено так, чтобы она показывала состояние логического 0, а схема "ИСКЛЮЧАЮЩЕЕ ИЛИ" 13, связанная с перемычкой тридцать два и комплементарной перемычкой тридцать два, опять показывала логическую один на выходе 14. Если состояние комплементарной перемычки тридцать два не может быть изменено, то вентиль "ИСКЛЮЧАЮЩЕЕ ИЛИ" 13 показывает состояние логического 0 на выходе 14, а вентиль "И" 17 также показывает состояние 0 на своем выходе, указывающее на манипуляции с идентификационными данными.

Существует возможность сформировать перемычки таким образом, чтобы прожигание не могло быть сделано без оправданных усилий, так что идентификационные данные специальной схемы 12, а следовательно, и носителя информации будут очень хорошо защищены от фальсификации, сделанной с целью обмана.

Вышеуказанные положения относятся главным образом к тестированию свойства подлинности носителя информации 1 внешним устройством 3. Свойство подлинности формируется как отдельное устройство с жесткой логикой на интегральной схеме носителя информации. Если проверка свойства подлинности внешним устройством 3 дает положительный результат, то это доказывает, что носитель информации 1 является внутрисистемным подлинным носителем информации. Для большинства реализаций носителей информации более важным является удостовериться, были ли некоторые данные, содержащиеся в интегральной схеме носителя информации, фальсифицированы. Такая проверка данных, содержащихся в интегральной схеме носителя информации 1, может быть также проведена особенно выгодным способом с помощью свойства подлинности, заключенного в специальной схеме 12, как объясняется на примере на фиг. 17.

Левая колонка фиг. 17 относится к внешнему устройству 3 и показывает поле 18, содержащее переменные, хранимые во внешнем устройстве 3 для выполнения арифметических операций, описанных ниже. Они представляют собой, в частности, основной ключ K_m . Кроме того, левая часть фиг. 17 содержит все арифметические операции, выполняемые во внешнем устройстве.

Средняя колонка фиг. 17 относится к специальной схеме 12 носителя информации 1 (см. также фиг. 8), а поле 19 содержит переменные, хранимые в специальной схеме 12, для выполнения арифметических операций, объясненных ниже. В частности, существуют данные В и С, информация В является, например, номером группы, а информация С, например, - номером платы или другими идентификационными данными носителя информации. Кроме того, средняя колонка фиг. 17 содержит те арифметические операции, которые выполняются специальной схемой 12.

Правая колонка фиг. 17 относится к микроконтроллеру 11 носителя информации 1 (см. также фиг. 8) и содержит в поле 20 те переменные, хранимые в микроконтроллере 11, которые нужны для выполнения арифметических операций в мик-

роконтроллере 11, как объясняется ниже. Они представляют собой, в частности, частный ключ K_{ISS} , связанный с носителем информации, который является функцией основного ключа K_m и данных В и С. Ключ K_{ISS} может уже храниться в микроконтроллере 11 во время работы носителя информации 1.

Во время обмена между внешним устройством 3 и носителем информации 1 сначала проверяется свойство подлинности носителя информации 1, как объяснено выше. С этой целью случайное число R_1 , сгенерированное уже во внешнем устройстве 3, сначала передается внешним устройством 3 в специальную схему 12 (см. шаг 1, номера шагов показаны слева на фиг. 17). В специальной схеме случайный номер R_1 логически комбинируется с данными В и С для формирования результата А (см. шаг два). Данные А, В и С передаются на шаге три из специальной схемы 12 во внешнее устройство 3. Затем переданные данные В и С логически комбинируются во внешнем устройстве 3 со случайным числом R_1 , хранимом в нем для формирования результата А' (см. шаг четыре). На шаге пять информация А' сравнивается с информацией А, переданной специальной схемой 12. Если эти два числа совпадают, то можно быть уверенным, что носитель информации 1 является подлинным внутрисистемным носителем информации, т.к. сравнение свойств подлинности внешним устройством дало положительный результат.

На шаге шесть информация А, вычисленная специальным устройством 12, передается в микроконтроллер 11 носителя информации 1 (см. также фиг. 8). В микроконтроллере 11 функция g применяется к информации А, используя ключ K_{ISS} , а результатом является ключ K_S , верный для данного конкретного обмена (см. шаг семь); сгенерированное случайное число R_1 вводит ключ K_S посредством информации А так, что ключ K_S реально изменяется от одного обмена к другому.

Внешнее устройство затем передает случайное число R_2 , сгенерированное в нем, в микроконтроллер 11 носителя информации 1 (см. шаг восемь). В микроконтроллере 11 функция g применяется к случайному числу R_2 , используя ключ K_S так, что получается результат х (см. шаг девять). Результат х передается микроконтроллером 11 во внешнее устройство 5 (см. шаг десять).

Во внешнем устройстве ключ K_{ISS} носителя информации вычисляется исходя из данных В и С, переданных на шаге три с помощью основного ключа K_m , хранящегося в устройстве 3 (см. шаг одиннадцать). Вычисленный ключ K_{ISS} носителя информации теперь может использоваться для вычисления текущего ключа K_S , исходя из информации А, которая также была передана во внешнее устройство на шаге три (см. шаг двенадцать). Наконец, информация х' может быть вычислена из сгенерированного случайного числа R_2 , используя ключ K_S (см. шаг тринадцать), указанная информация наконец сравнивается с информацией х, переданной микроконтроллером 11 (см. шаг четырнадцать).

Если данные х' и х совпадают, то для внешнего устройства 3 считается доказанным, что специальная схема 12 носителя информации 1 может

обмениваться данными с микроконтроллером 3 носителя информации 1, т.к. микроконтроллер 11 носителя информации 1 может вычислить информацию х правильно, только в случае, если правильная информация А была ранее передана в микроконтроллер 11 специальной схемой 12 на шаге шесть. Поэтому невозможно предложить не подлинный и внесистемный носитель информации совместно со специальной схемой, не соединенные с микроконтроллером носителя информации.

Кроме того, для внешнего устройства 3 считается доказанным, что специальная схема 12 и микроконтроллер 11 носителя информации 1 объединены вместе, т.к. только если специальная схема 12 и микроконтроллер 11 объединены вместе, то микроконтроллер 11 содержит те же самые данные В и С, что и специальная схема 12 и соответствующий ключ K_{ISS} носителя информации. Только в этом случае может быть вычислена та же самая информация х в микроконтроллере 11, что и во внешнем устройстве 3.

Так как для внешнего устройства 3 доказано, что специальная схема 12 и микроконтроллер 11 объединены вместе, то становится невозможным предложить носитель информации, который является недостоверным и внесистемным совместно со специальной схемой 12 с целью обмана и таким образом моделировать подлинность и системное присоединение носителя информации 1.

Кроме того, невозможно фальсифицировать данные В и С в микроконтроллере 11 подлинного внутрисистемного носителя информации с целью обмана. С одной стороны, ключ носителя информации K_{ISS} также должен быть адаптирован соответствующим образом, т.к. ключ K_{ISS} может быть вычислен в любое время из данных В и С, запомненных в микроконтроллере 11 во внешнем устройстве 3 и сравнен с запомненным ключом K_{ISS} . Такая адаптация, однако, невозможна, т.к. обманщик не имеет основного ключа K_m . С другой стороны, данные В и С в специальной схеме 12 также должны быть изменены соответствующим образом, т.к. в противном случае отличающаяся информация х будет вычислена во внешнем устройстве 3 и микроконтроллере 11. Но данные В и С специальной схемы могут быть хорошо защищены от фальсификации, как описано, например, применительно к фиг. 16.

Данные В и С могут быть, например, групповым номером и номером конкретной микросхемы, или персональными данными собственной платы, такими как имя или номер счета, и т.д.

Тестовые программы, объясненные выше, очевидно также могут быть выполнены, если используются, например, только данные В или данные, отличные от данных В и С.

Фиг. 10 показывает, как доказать, что специальная схема 12 и микроконтроллер 11 носителя информации 1 объединены вместе, используя асимметричный алгоритм кодирования. Фиг. 18 схематически построена так же, как фиг. 17, т.е. поля 18, 19 и 20 содержат информацию, хранимую в соответствующих компонентах. Кроме того, тестирование свойства подлинности носителя информации 1 выполняется внешним устройством 3 так, как объяснено выше применительно к шагам с

первого по пятый на фиг. 17. Соответственно, здесь это повторно не обсуждается.

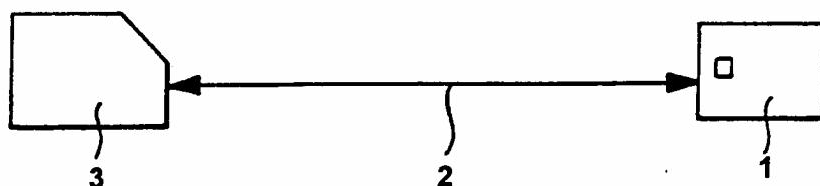
После тестирования свойства подлинности носителя информации 1 специальная схема 12 передает информацию А в микроконтроллер 11 носителя информации 1 (сравни также фиг. 6) и на шаге семь генерируется случайное число R_2 во внешнем устройстве 3. На шаге восемь из случайного числа R_2 и данных А, В и С формируется сертификат ZER2 в микроконтроллере 11, используя секретный ключ SK_{ICCS} носителя информации 1. Сертификат ZER2 передается с сертификатом ZER1, хранимым в микроконтроллере 11, во внешнее устройство 3 (см. шаг девять).

Электронный модуль 9, данные В и С и общий ключ PK_{ICCS} носителя информации вычисляются, исходя из сертификата ZER1, используя общий ключ PK_Z учреждения Z (см. шаг десять). Затем случайное число R_2' и информация А', В' и С' вычисляются из сертификата ZER2, используя общий ключ PK_{ICCS} носителя информации, также уже полученного (см. шаг одиннадцатый). Наконец, на шаге двенадцать случайное число R_2' , уже полученное, сравнивается со случайным числом, сгенерированным во внешнем устройстве, а данные А, В и С, также уже полученные, сравниваются с данными А, В и С, переданными на шаге три (см. также фиг. 17).

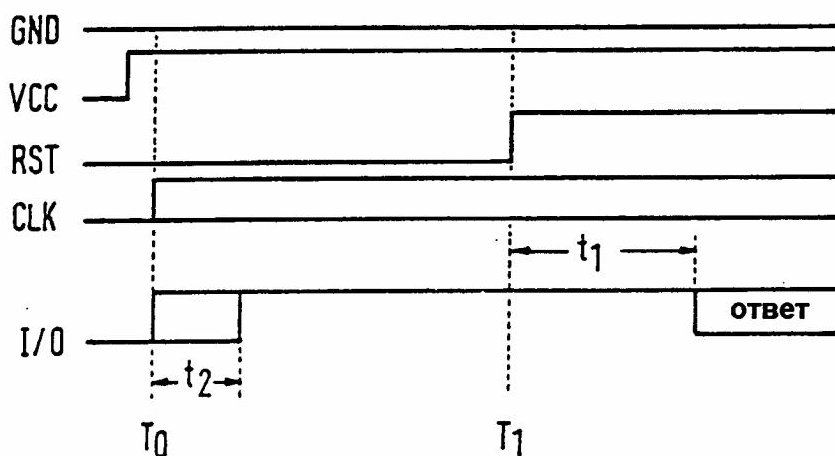
Если сравнение дало положительный результат, то считается доказанным, что специальная схема 12 находится в положении для обмена с микроконтроллером 11 (см. шаг шесть), и также считается доказанным, что специальная схема 12 и микроконтроллер 11 объединены вместе. В противном случае данные, сравненные на шаге двенадцать, не совпадут, т.к. различные данные В и С должны затем быть запомнены в специальной схеме 12 и микроконтроллере 11 носителя информации 1.

Также считается доказанным, что данные В и С, хранимые в микроконтроллере 11, не были фальсифицированы, т.к. эта информация в противном случае не совпадает с данными В и С, хранимыми в сертификате ZER1. Эти данные тестируются на совпадение на шаге двенадцать, поэтому подделка должна быть обнаружена. Кроме того, эти данные не совпадут с данными В и С, хранимыми в специальной схеме 12, которые также тестируются на шаге двенадцать. Если используется способ асимметричного кодирования, то данные В и С очень хорошо защищены от фальсификации.

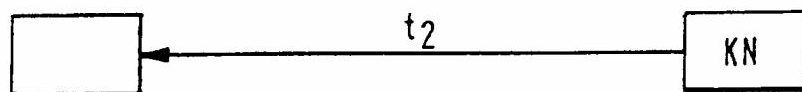
Операции, упомянутые применительно к фиг. 17 и 18 и выполняемые во внешнем устройстве 3, могут быть предпочтительно выполнены модулем безопасности 5, как описано применительно к фиг. с 8 по 11.



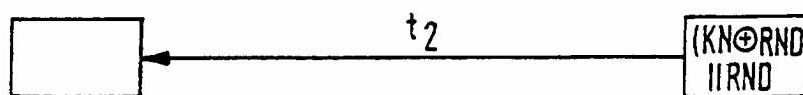
Фиг. 1



Фиг. 2



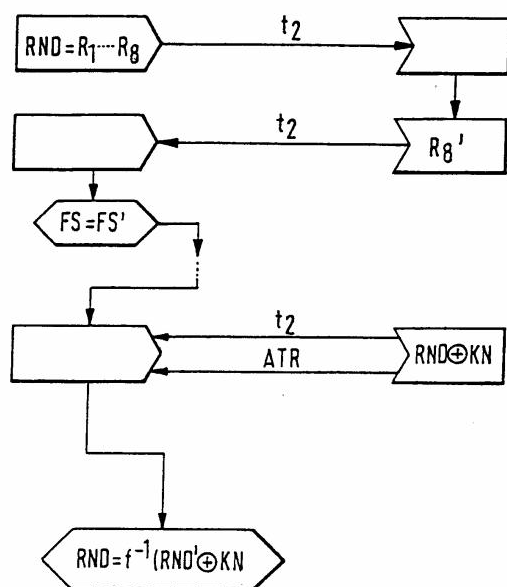
Фиг. 3



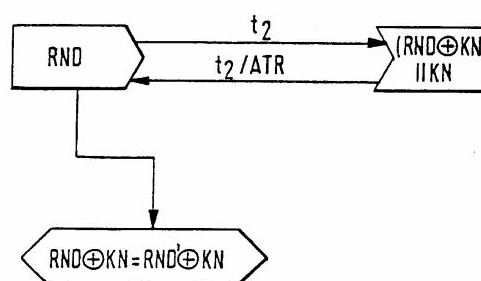
Фиг. 4



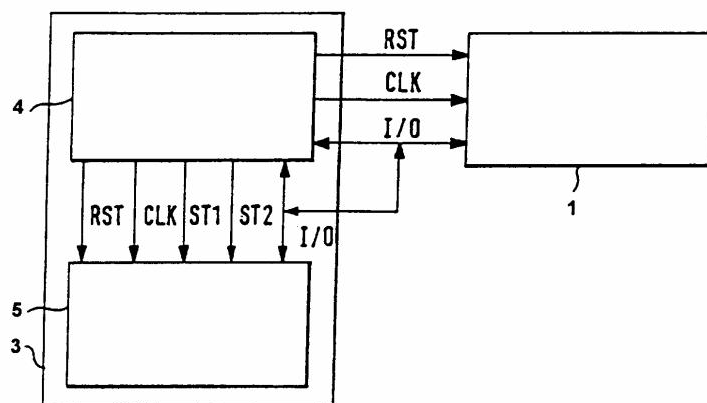
Фиг. 5



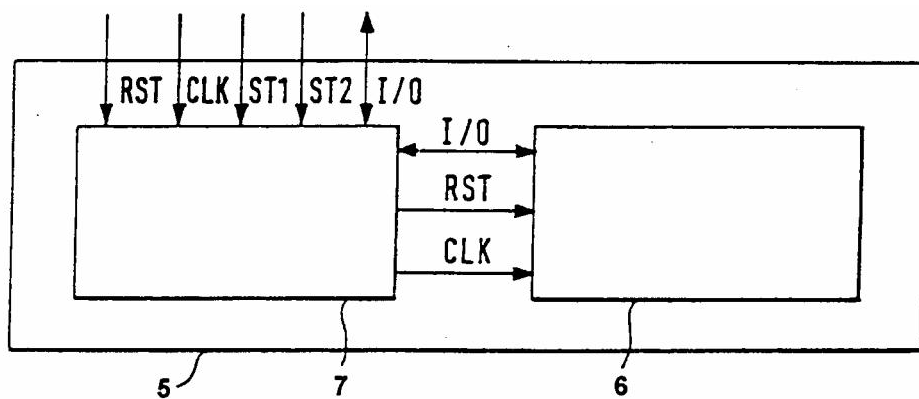
Фиг. 6



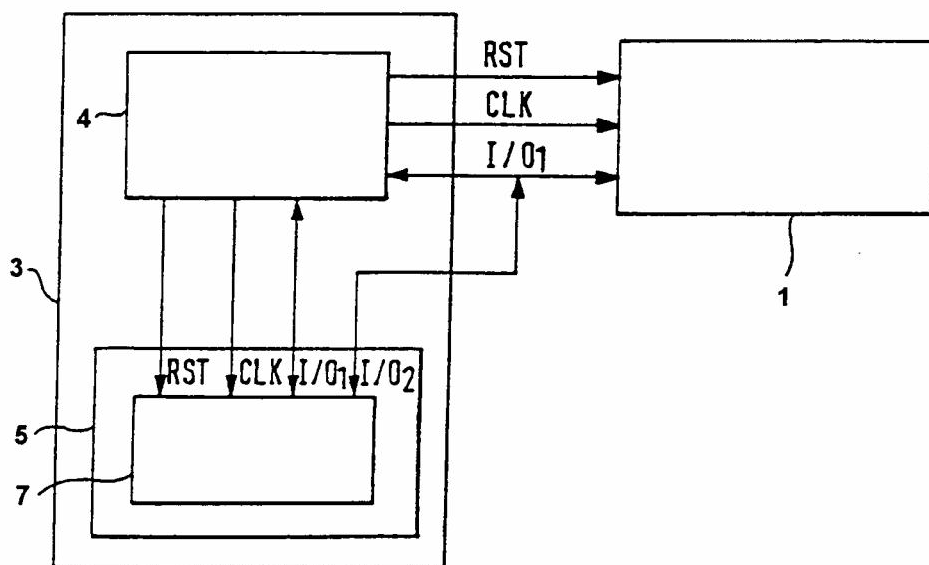
Фиг. 7



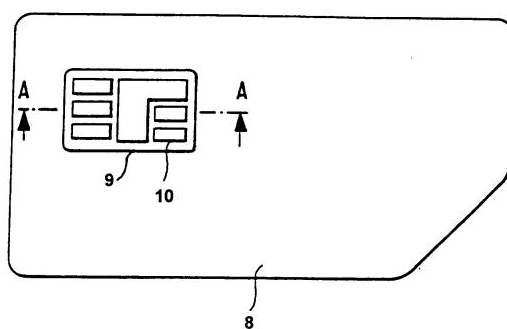
Фиг. 8



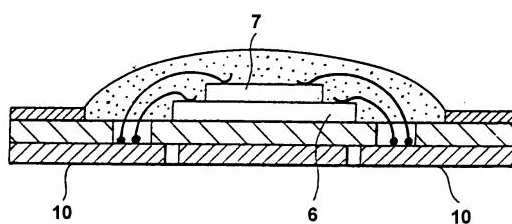
Фиг. 9



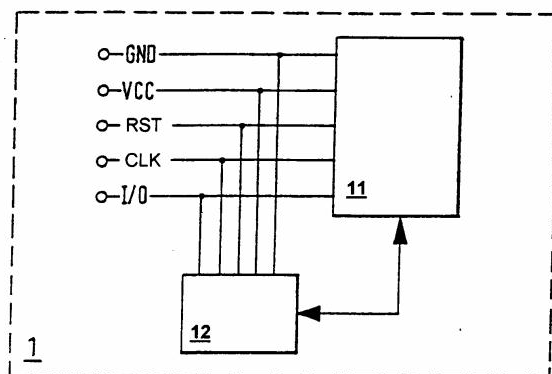
Фиг. 10



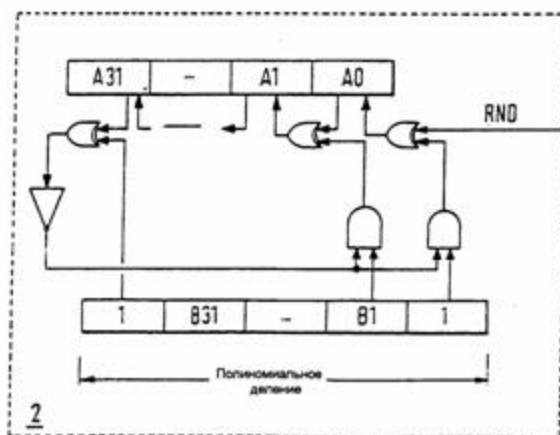
Фиг. 11



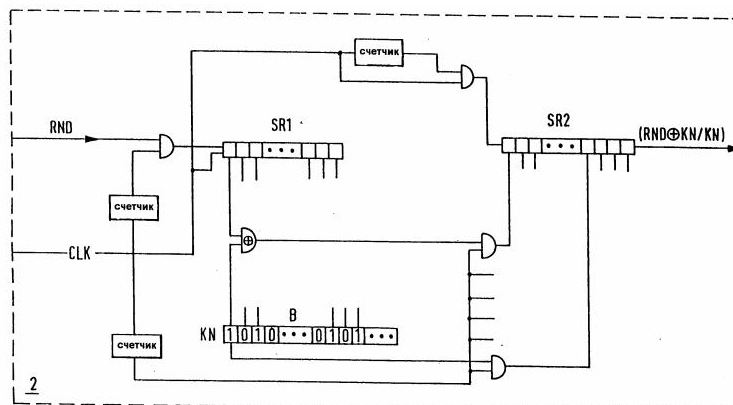
Фиг. 12



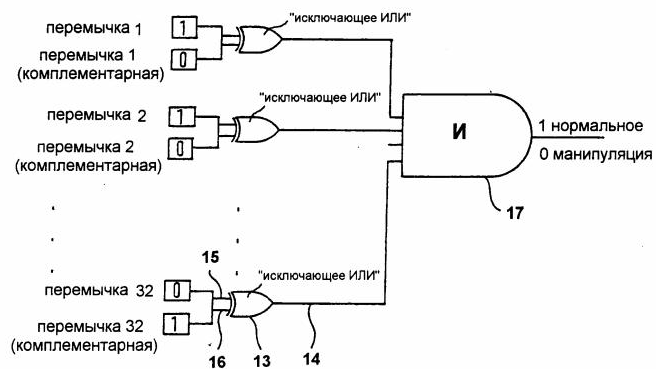
Фиг. 13



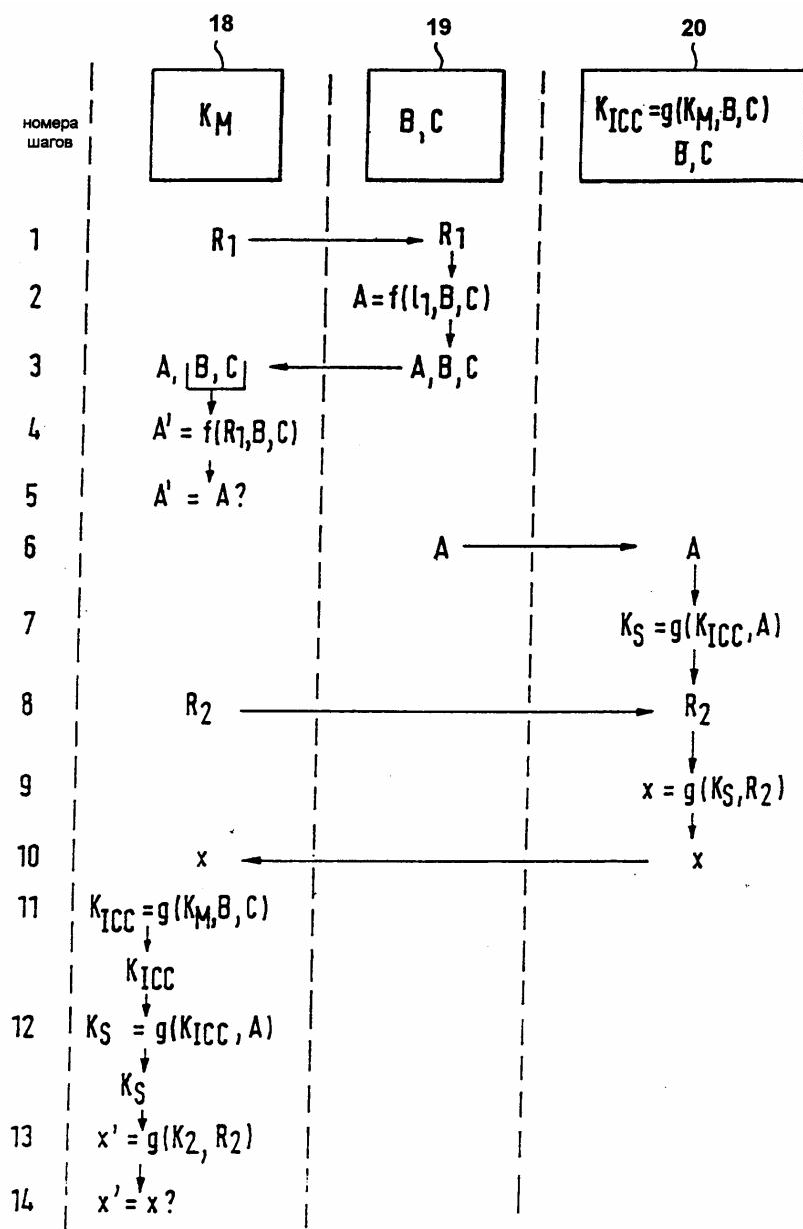
Фиг. 14



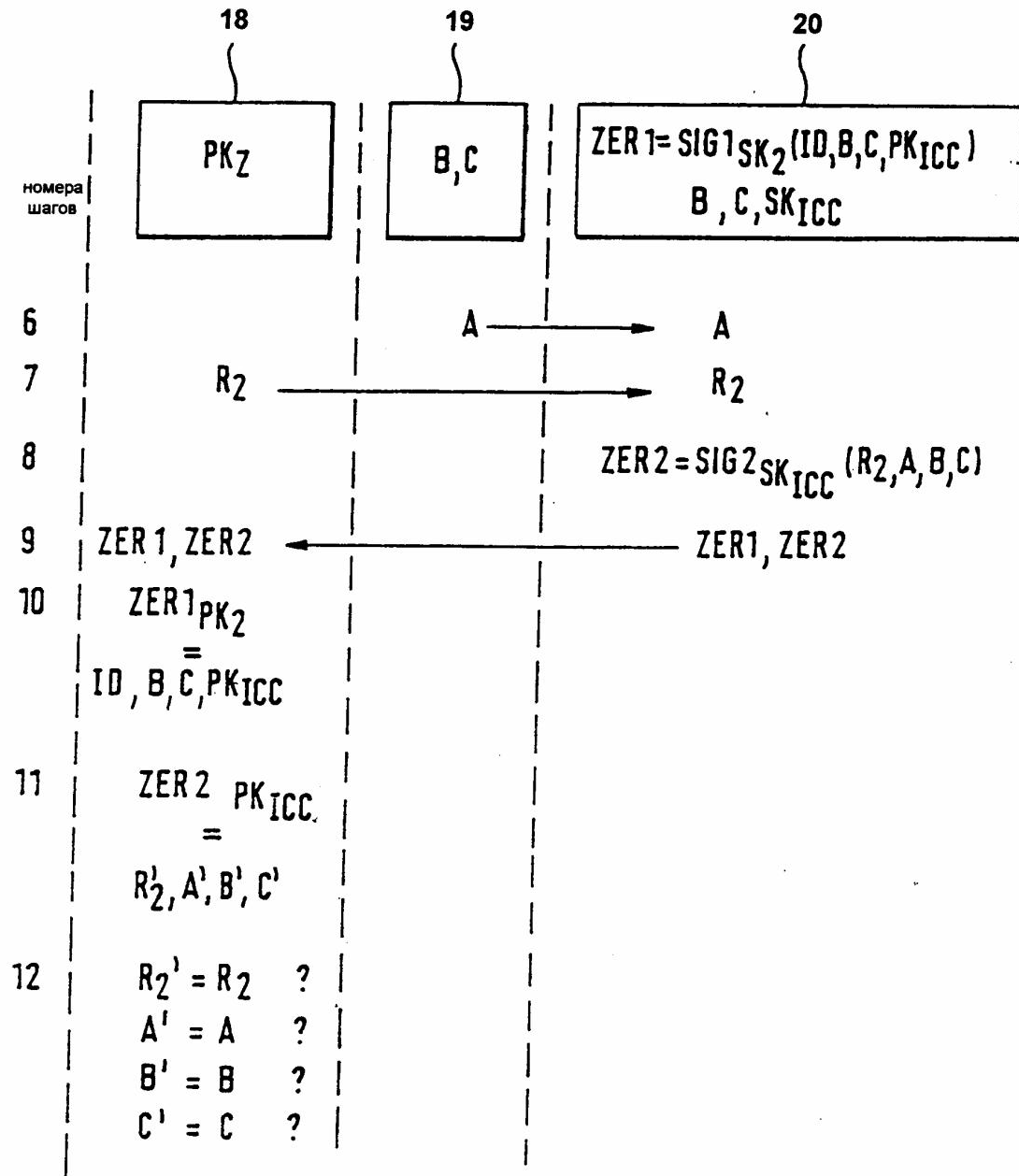
Фиг. 15



Фиг. 16



Фиг. 17



Фиг. 18

Тираж 50 экз.

Відкрите акціонерне товариство «Патент»
Україна, 88000, м. Ужгород, вул. Гагаріна, 101
(03122) 3 – 72 – 89 (03122) 2 – 57 – 03