Союз Советских Социалистических Республик

Государственный комитет СССР по делам изобретений и открытий

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

К ПАТЕНТУ

(11) 963479

(61) Дополнительный к патенту -

(22) Заявлено 04.10.80 (05.02.80) (21) 2987385/18-24 (PCT/FR 80/ /00018м)

(23) Приоритет - (32) 06.02.79

(31) 79 02995 (33) Франция

(51) М. Кл.[3] G 08 C 19/28

Опубликовано 30.09.82 Бюллетень № 36

Дата опубликования описания 30.09.82

(53) УДК 621.398 (088.8)

(72) Автор изобретения: Иностранец Луи Клод Гийу (Франция)

(71) Заявители: Иностранные фирмы "Этаблиссеман Пюблик де диффюзьон ДИ "Теледиффюзьон де Франс" и "Д'Эта Франсэ Репрезанте Пар Ле Секретэр Д'Эта о пост Э Телекоммюникасьон (Сантр Насьональ Д'этюд де Телекоммюникасьон")" (Франция)

(54) СИСТЕМА ПЕРЕДАЧИ И ПРИЕМА ИНФОРМАЦИИ

1

Система относится к информационным системам и может быть применена, например, в телевизионных информационных системах.

Известна система передачи и приема информации, содержащая источники информации, центральный процессор, пульт управления, линии связи и устройства отображения информации [1].

Недостатком указанной системы является отсутствие контроля доступа к передаваемой информации [1].

Наиболее близкой по технической сущности к предлагаемой является система передачи и приема информации, содержащая источники информации, соединенные через формирователи сигналов с первым входом узла блокировки, выход которого подключен к первому входу передатчика, второй вход передатчика соединен с выходом формирователя сообщений, выполненного на микропроцессоре, на приемной стороне - приемник и индикатор, а также блок управления и ручного ввода информации, соединенный с микропроцессором [2].

2

Недостатком известной системы является отсутствие контроля доступа к передаваемой информации, что ограничивает функциональные возможности устройства.

Цель изобретения - расширение функциональных возможностей системы.

Поставленная цель достигается тем, что в систему передачи и приема информации, содержащую на передающей стороне источник информации, соединенный через формирователь сообщений с первым входом узла блокировки, выход которого подключен к первому входу передатчика, второй вход передатчика соединен с выходом формирователя сообщений, выполненного на микропроцессоре, на приемной стороне - приемник и индикатор, введены на передающей стороне блок управления записью абонементных

кодов и генератор ключевых сигналов, выходы которого соединены соответственно с первым входом формирователя сообщений и с вторым входом узла блокировки, выход блока управления записью абонементных кодов подключен к второму входу формирователя сообщений, на приемной стороне введены блок ввода служебной информации, абонементная запоминающая карта, блок восстановления ключевых сигналов и узел разблокировки, первый выход приемника подключен к первому входу узла разблокировки, выход которого соединен с входом индикатора, выход блока ввода служебной информации через абонементную запоминающую карту подключен к входу блока восстановления ключевых сигналов, второй выход приемника подключен к второму входу блока восстановления ключевых сигналов, выход которого соединен с вторым входом узла разблокировки, второй выход блока управления записью абонементных кодов подключен к второму входу блока ввода служебной информации.

На чертеже показана схема системы передачи и приема информации.

Система содержит блок 1 управления записью абонементных кодов, передающий центр 2, формирователь 3 сообщений, генератор 4 ключевых сигналов, источник 5 информации, формирователь 6 сигналов, узел 7 блокировки, передатчик 8, блок 9 ввода служебной информации, приемник 10, абонементную запоминающую карту 11, блок 12 восстановления ключевых сигналов, узел 13 разблокировки и индикатор 14.

Система передачи и приема информации работает следующим образом.

Сигналы источника 5 информации через формирователь 6 сигналов поступают на первый вход узла 7 блокировки, работой которого управляет генератор 4 ключевого сигнала. Блок 1 управления записью абонементных кодов управляет работой формирователя 3 сообщений, выполненного на микропроцессоре, сигналы с выхода которого и сигналы узла блокировки поступают на вход передатчика. С выходов приемника 10 сигналы через блок 12 восстановления и через узел 13 разблокировки поступают на вход индикатора.

Схема формирователя 3 сообщений организована вокруг программированного микропроцессора для введения в действие алгоритма, базирующегося на двух полях Галуа, имеющих в качестве характеристик простые числа Марсенна $2^{61}-1$ и $2^{127}-1$. Этот алгоритм использует абонементные ключи 12 и 128 двоичных элементов и один служебный ключ из 56 двоичных элементов следующим образом.

а) образуется кодовая группа π беспорядочной избыточности, содержащая 61 двоичный элемент, передаваемый в случайном порядке при каждом введении в действие алгоритма;

б) подсчитывается π^{-1}, обратное π по модулю $2^{61}-1$, посредством арифметической программы, использующей вариант алгоритма Эвклида;

в) осуществляется первое перемножение с другой арифметической программой $\nu = K \cdot \pi^{-1}$ по модулю $2^{61}-1$;

г) подсчитывается γ, обратное С по модулю $2^{127}-1$, посредством программы, аналогичной в пункте б;

д) наконец, подсчитывается сообщение посредством программы, аналогичной в пункте в $(\nu + 2^{64}\pi)$ по модулю $2^{127}-1$.

Таким образом, сформированы сообщения, и разворачиваемый алгоритм в формирователе 3 для восстановления служебного ключа из сообщения M_i и из одного абонементного ключа 12 является следующим:

а) сообщением M_i (127 используемых двоичных элементов) захватывается байт за байтом и происходит умножение C_i на первое поле С $2^{127}-1$. Так образуется группа μ: $\mu = M \cdot C$ по модулю $2^{127}-1$.

Согласно условию М в передаче двоичные элементы μ с 1 по 61 представляют группу ν, тогда как двоичные элементы с 65 по 126 представляют группу π. Разумеется, двоичные элементы 62-64, 126 и 127 должны быть нулевыми. Если они ими не являются, перед продолжением подсчета группу приводят к нулю.

б) π и ν умножаются на второе поле С $(2^{61}-1)$, что устраняет беспорядочную избыточность, и получают $K = \nu\pi$ по модулю $2^{61}-1$,

в) 56 используемых двоичных элементов К таким образом приводятся к виду восьми непарных байтов.

Для каждой платной службы примерно каждые пять минут произвольно передается каждым интересующим передающим центром новый служебный ключ К. Таким образом, в течение одного периода работы службы (один или несколько часов) могут следовать один за другим несколько служебных ключей.

С момента передачи передающим центром нового служебного ключа К он рассчитывает для каждого существующего для этой службы абонементного ключа C_i сообщением M_i с помощью алгоритма $M_i=F_{C_i}(K)$, причем ключи C_i играют роль параметров.

Таким образом, для службы, снабженной вышеуказанной абонементной схемой, в любой момент действуют 22 различных сообщений. Длительность существования сообщения равна длительности служебного ключа К, и для одной данной службы в любой момент существует столько сообщений, сколько имеется существующих абонементных ключей.

Совокупность действующих сообщений М образуют информацию контроля доступа, участвующую в передаваемой службе, что и обеспечивает расширение функциональных возможностей устройства.

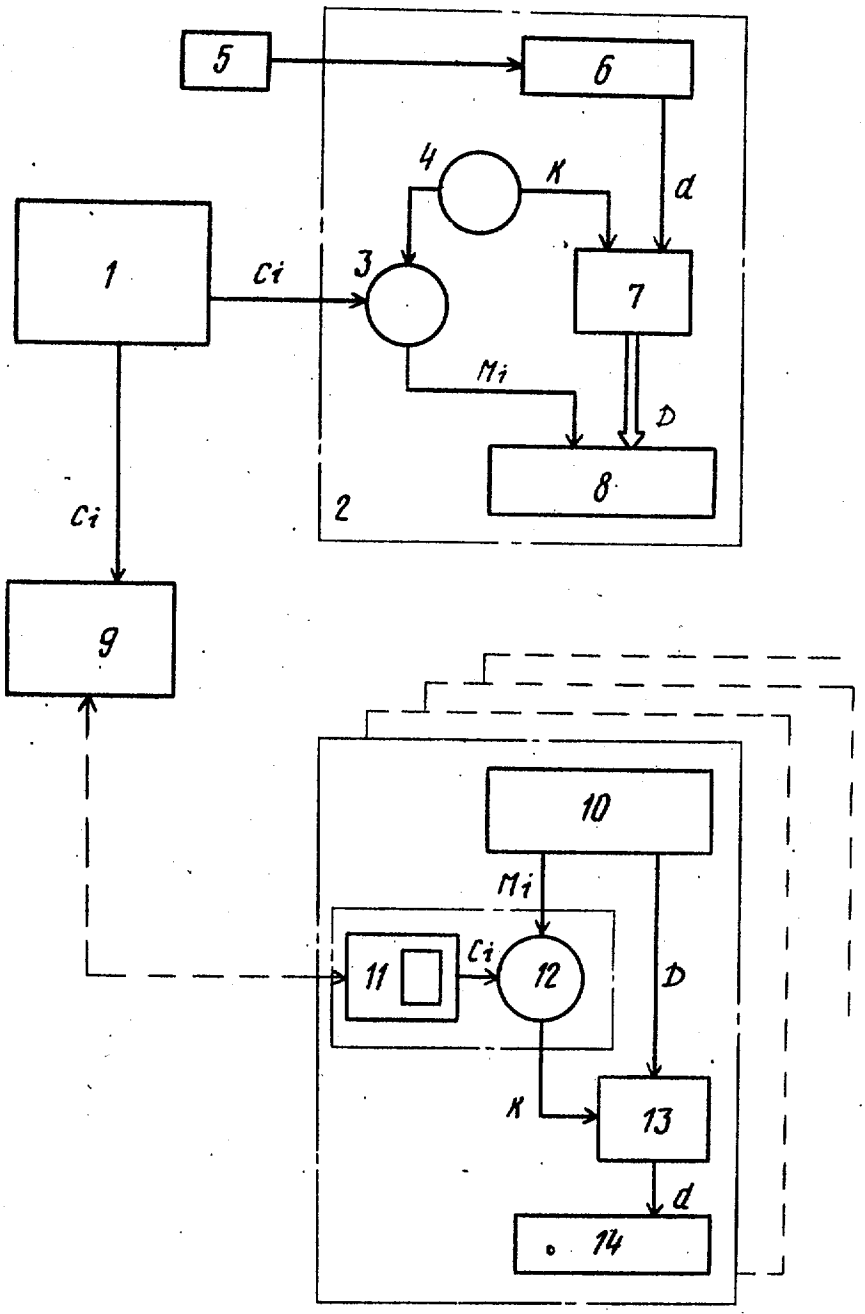
Формула изобретения

Система передачи и приема информации, содержащая на передающей стороне источник информации, соединенный через формирователь сообщений с первым входом узла блокировки, выход которого подключен к первому входу передатчика, второй вход передатчика соединен с выходом формирователя сообщений, на приемной стороне - приемник и индикатор, о т л и ч а ю щ а я с я тем, что, с целью расширения функциональных возможностей системы, в нее введены на передающей стороне блок управления записью абонементных кодов и генератор ключевых сигналов, выходы которого соединены соответственно с первым входом формирователя сообщений и с вторым входом узла блокировки, выход блока управления записью абонементных кодов подключен к второму входу формирователя сообщений, на приемной стороне введены блок ввода служебной информации, абонементная запоминающая карта, блок восстановления ключевых сигналов и узел разблокировки, первый выход приемника подключен к первому входу узла разблокировки, выход которого соединен с входом индикатора, выход блока ввода служебной информации через абонементную запоминающую карту подключен к входу блока восстановления ключевых сигналов, второй выход приемника подключен к второму входу блока восстановления ключевых сигналов, выход которого соединен с вторым входом узла разблокировки, второй выход блока управления записью абонементных кодов подключен к второму входу блока ввода служебной информации.

Источники информации, принятые во внимание при экспертизе

1. Лоскутов В.И. Управляющие математические машины, М., 1967, с. 472. рис. 215.

2. Там же, с. 474, рис. 216 (прототип).



Составитель
Редактор С.Крупенина Техред М.Гергель Корректор М.Демчик

Заказ 7555/80 Тираж 642 Подписное
ВНИИПИ Государственного комитета СССР
по делам изобретений и открытий
113035, Москва, Ж-35, Раушская наб., д. 4/5

Филиал ППП "Патент", г. Ужгород, ул. Проектная, 4