(19) Евразийское патентное ведомство

(11) 041824 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.12.07

(21) Номер заявки
201700121

(22) Дата подачи заявки
2016.03.04

(51) Int. Cl. ***G06F 21/60*** (2013.01)
H04L 9/00 (2006.01)

(54) УСТРОЙСТВО ШИФРОВАНИЯ ДАННЫХ (ВАРИАНТЫ), СИСТЕМА НА КРИСТАЛЛЕ С ЕГО ИСПОЛЬЗОВАНИЕМ (ВАРИАНТЫ)

(31) **2015107429**
(32) **2015.03.04**
(33) **RU**
(43) **2017.10.31**
(86) **PCT/RU2016/000123**
(87) **WO 2016/140596 2016.09.09**

(71)(73) Заявитель и патентовладелец:
АКЦИОНЕРНОЕ ОБЩЕСТВО "БАЙКАЛ ЭЛЕКТРОНИКС" (RU)

(72) Изобретатель:
Гнатюк Владимир Леонидович, Осипенко Павел Николаевич, Красик Константин, Гурин Константин Львович, Хренов Григорий Юрьевич, Стариковский Алексей Юрьевич, Витковский Арсений Александрович, Лукьянов Владимир Алексеевич, Шимко Сергей Николаевич (RU)

(74) Представитель:
Казьмина С.А. (RU)

(56) US-B1-7783037
RU-C1-2287222

(57) Изобретение относится к области шифрования потоков данных. Технический результат - повышение быстродействия процессов криптопреобразования данных. Устройство шифрования данных согласно ГОСТ 28147-89 характеризуется тем, что включает в себя контроллер прямого доступа к памяти, обеспечивающий загрузку массива данных из памяти для шифрования устройством шифрования данных и сохранение криптопреобразованных данных обратно в память, вычислительный блок с возможностью реализации шифрования данных в соответствии с выбранным алгоритмом, регистры данных для хранения таблиц подстановки, регистры данных для хранения ключей для шифрования, регистры для хранения векторов синхропосылки и имитовставки, а также блок управления.

041824 B1

041824 B1

Область техники

Изобретение относится к устройствам шифрования данных, которые могут использоваться в составе вычислительных систем, например в системах на кристалле (СнК) для шифрования данных, поступающих из сети Интернет, с жестких дисков или из других хранилищ информации.

Уровень техники

Известно изобретение по патенту РФ 2412479 (правообладатель Сименс, МПК G06F 21/00 G06F 1/00, 2006), относящееся к комплексной системе защиты данных, содержащей функциональный модуль шифрования, посредством которого данные или программные коды могут зашифровываться и расшифровываться, при этом схема предполагает как возможность, так и отсутствие возможности хранения в ней ключей, встроенные часы реального времени для контроля изменения частоты, встроенный источник питания для уничтожения ключей. В известном решении для шифрования используют отдельные вычислительные устройства в составе единой интегральной схемы. Известное решение является наиболее близким к заявляемому изобретению устройством того же назначения, однако в нем есть существенные недостатки, обусловленные тем, что

а) на уровне аппаратуры в нем не поддерживается выполнение отдельных алгоритмов шифрования таких как режим простой замены, режимы гаммирования и гаммирования с обратной связью, а также режим выработки имитовставки (указанные режимы предусмотрены, например, ГОСТ 28147-89),

б) для него предусмотрен единственный режим работы: считывание данных из памяти, проведение шифрования и запись результата во внутренний регистр центрального процессора или встроенную кэш-память;

в) в нем не предусмотрен режим работы с потоковым шифрованием данных, находящихся во внешней памяти (например, внешнем ОЗУ), с последующим помещением расшифрованных/зашифрованных данных обратно во внешнее ОЗУ, как это предусмотрено в заявленном устройстве;

г) нет возможности сокращения общего времени, требуемого для шифрования массива данных, которое осуществляется в заявленном решении, которое стало возможным благодаря схеме, прямо специфицирующей сокращение общего времени, требуемого для шифрования массива данных, путем использования встроенного оборудования, позволяющего одновременно передавать данные из памяти для зашифровывания/расшифровывания с последующим возвратом результатов шифрования обратно в память.

Другие известные вычислительные системы без устройства шифрования, представленного в данном изобретении, осуществляют процесс шифрования данных программными средствами, используя только ресурсы центрального микропроцессора.

Сущность изобретения

Заявленное решение представляет собой устройство шифрования данных (2 варианта), реализованное в виде интегральной схемы с функциональными модулями, и СнК с его использованием (2 варианта).

Устройство шифрования работает в следующих режимах криптопреобразований, а именно в режиме простой замены, в режимах гаммирования и гаммирования с обратной связью, в режиме замены с зацеплением, а также в режиме выработки имитовставки. Данные режимы можно использовать для реализации блочного симметричного шифратора, использующего технологию замены открытых данных другими элементами по определенным правилам (например, в соответствии с ГОСТ 28147-89).

В описании изобретения под шифрованием понимаем процесс криптопреобразования (либо зашифровывание, либо расшифровывание) данных, происходящий в устройстве шифрования. Свойство симметричности означает использование для зашифровывания и расшифровывания одного и того же секретного ключа. Разница лишь в последовательности применения различных составных элементов ключа при зашифровывании и расшифровывании. Эта последовательность определяется алгоритмически и не изменяется. Данные алгоритмы реализуют блочный тип шифрования, это означает, что массив шифруемых данных разделяется на блоки одинакового размера. Обработка каждого блока осуществляется аналогично друг другу.

В устройство (7) шифрования данные могут поступать из любого доступного хранилища информации в формате, удовлетворяющем требованиям, предъявляемым к работе алгоритмов, реализованных в заявленном изобретении, например блоками по 64 бит каждый, из (внешней для устройства шифрования) памяти (6) (например, последовательного ОЗУ), подключаемой по стандартному интерфейсу. После окончания работы устройство (7) шифрования отправляет криптопреобразованные данные обратно в память (6) (получателю, например в последовательное ОЗУ), подключаемое по стандартному интерфейсу.

Целью создания устройства шифрования является повышение быстродействия процессов криптопреобразования данных с использованием режима простой замены, режимов гаммирования и гаммирования с обратной связью, режима замены с зацеплением, а также режима выработки имитовставки. Повышение быстродействия процессов криптопреобразования данных (ускорение шифрования) осуществляется за счет использования в составе устройства шифрования отдельных вычислительных устройств, обрабатывающих потоковые данные непосредственно из внешней памяти по отношению к устройству шифрования, а не путем использования специализированного программного обеспечения, использующего ресурсы центрального процессора, особенно, если это устройство шифрования используется в составе

СнК.

В таком случае ускорение шифрования в заявленном устройстве (7) шифрования достигается за счет следующих факторов.

1) В отличие от стандартного подхода устройство шифрования обеспечивает шифрование данных без непосредственного участия центрального процессора, тем самым освобождая его ресурсы для других операций. Центральный процессор при использовании заявленного устройства (7) шифрования в составе СнК играет роль системного арбитра при включении, выключении устройства, управляет прерываниями и отвечает за управление режимами его работы. Автономная от центрального процессора работа устройства (7) шифрования обеспечивается за счет встроенного в СнК контроллера (4), обеспечивающего прямой доступ к памяти.

2) Шифрование каждого блока данных выполняется последовательно, в частности, удовлетворяя требованию, предъявляемому к работе блочных алгоритмов шифрования, реализованных в данном устройстве. В заявленном решении время криптопреобразования одного блока является фиксированным, не зависящим от нагрузки на центральный процессор СнК.

3) Данные для шифрования и результаты шифрования могут передаваться (см. фиг. 1, 2) между блоком (3) внутренней коммутации, контроллером (4) прямого доступа к памяти и вычислительным устройством (8) или устройствами (8), (9) в зависимости от принятой конфигурации устройства (7) шифрования по внутренним шинам (12), (13), (14), (15), (16) пакетами, состоящими из кадров. Размер кадра соответствует размеру блока обрабатываемых данных (например, 64 бита), его размер остается неизменным в процессе работы. Кадры из пакета поступают на вычислительные устройства также потоком, обеспечивая бесперебойность процесса шифрования.

4) Блок (3) внутренней коммутации способен одновременно передавать данные в обоих направлениях: в контроллер (4) прямого доступа к памяти и из него. Данные могут накапливаться во встроенных хранилищах контроллера (4) для устранения задержек, которые могут возникнуть при работе с внешней памятью.

5) Для обеспечения шифрования в устройство (7) шифрования могут быть включены или один вычислительный модуль (8) (фиг. 1, 5) или два независимых вычислительных модуля (8) и (9) (фиг. 2, 6). Вычислительный модуль (8) используется для реализации базового цикла шифрования в соответствии с выбранным режимом работы, если только он один присутствует в устройстве (7) шифрования, при этом он используется последовательно как для вычисления результата шифрования блока данных, так и для вычисления имитовставки (фиг. 1, 5). При использовании двух независимых вычислительных модулей (8) и (9) одновременно вычисляются как результат шифрования блока данных с использованием модуля (8) базового цикла, так и результат выработки имитовставки с использованием модуля (9) выработки имитовставки (ИВ) (фиг. 2, 6). Использование отдельного вычислительного блока (9) для выработки имитовставки позволяет дополнительно повысить быстродействие всего устройства (7) шифрования благодаря тому, что основной вычислительный модуль (8) в этом случае используется только для процесса шифрования.

Алгоритмы шифрования, поддерживаемые в заявленном устройстве, содержат требование рекурсивной блочной обработки массива данных, иными словами, для шифрования следующего блока требуется результат обработки предыдущего. При использовании известных подходов общее время выполнения процесса шифрования увеличивается прямо пропорционально объему шифруемых данных.

Заявленное устройство (7) шифрования позволяет не только сократить время шифрования, но и уменьшить затраты программных ресурсов СнК, в которой оно может быть использовано, в частности, на изоляцию от криптоатак секретных ключей, используемых в процессе шифрования данных и хранящихся обычно в оперативной памяти на общих основаниях. Секретные ключи в рассматриваемом случае хранятся во внутренних регистрах (18) устройства (7) шифрования, не допускающих считывание их содержимого программными средствами.

СнК, работающая с использованием устройства (7), описанного в данной заявке в 2-х вариантах, позволяет существенно сократить время выполнения процесса шифрования по сравнению с известными вычислительными системами, в которых процесс шифрования данных осуществляют программными средствами, используя ресурсы центрального микропроцессора. В таких системах обработка каждого блока данных требует исполнения небольшой подпрограммы, осуществляющей загрузку данных, выполнение необходимых вычислений и запись результата криптопреобразования.

Заявленная СнК (1) (2 варианта), включающая в себя заявленное устройство шифрования (в 2-х вариантах), представляет собой систему на кристалле (СнК) с возможностью использования внутренней памяти (6) по отношению к СнК (входящей в состав СнК) (по первому варианту - фиг. 1, 5) или внешней памяти (6) по отношению к СнК (подключаемой к СнК по стандартному интерфейсу по второму варианту - фиг. 2, 6) (например, в качестве памяти может использоваться последовательное ОЗУ в обоих случаях. В СнК включены

центральный процессор (2) общего назначения, который может исполнять программы;

устройство шифрования (7), благодаря которому данные могут зашифровываться и расшифровываться;

блок (3) внутренней коммутации, который обеспечивает обмен данными между элементами системы;

контроллер (5) доступа к памяти (6).

Перечень чертежей

Фиг. 1 - архитектура СнК с использованием заявленного устройства (7) шифрования (с использованием первого варианта устройства шифрования) на базе одного вычислительного модуля (8), когда память является внешней по отношению к СнК,

фиг. 2 - архитектура СнК с использованием заявленного устройства (7) шифрования (с использованием второго варианта устройства шифрования), включающего дополнительный вычислительный модуль (9) для выработки имитовставки, когда память является внешней по отношению к СнК,

фиг. 3 - алгоритм функционирования устройства (7) шифрования, представленного в данном изобретении,

фиг. 4 - описание режима простой замены с зацеплением при зашифровывании (а) и расшифровывании (б),

фиг. 5 - архитектура СнК с использованием заявленного устройства (7) шифрования (с использованием первого варианта устройства шифрования) на базе одного вычислительного модуля (8), когда память является внутренней памятью, входящей в СнК,

фиг. 6 - архитектура СнК с использованием заявленного устройства (7) шифрования (с использованием второго варианта устройства шифрования), включающего дополнительный вычислительный модуль (9) для выработки имитовставки, когда память является внутренней памятью, входящей в СнК.

Примеры осуществления изобретения

Заявленное устройство шифрования (7) данных по алгоритмам, простой замены, простой замены с зацеплением, гаммирования и гаммирования с обратной связью, а также вычисления имитовставки включает в себя контроллер (4) прямого доступа к памяти (6), обеспечивающий передачу данных для шифрования из внешней по отношению к устройству шифрования памяти (6) (например, последовательного ОЗУ), которое может использоваться в частном случае осуществления изобретения, рассматриваемого ниже в двух вариантах, но не ограничивая его только рассмотренными случаями используемой памяти) в устройство (7) шифрования и зашифрованных или расшифрованных данных из устройства (7) шифрования обратно в память (6) (например, последовательное ОЗУ, которое может быть как внешним по отношению к СнК, так и входить в СнК), вычислительный модуль (8), обеспечивающий шифрование данных в соответствии с выбранным режимом работы, модуль вычисления имитовставки (9) (данный модуль не используется в устройстве (7) шифрования по первому варианту), а также управляющие регистры, хранящие информацию, необходимую для проведения шифрования, а именно регистр (17) (например, 512-бит), в который загружается таблица замен, регистр (18) (например, 256-бит), в который загружается ключ для шифрования, регистр (19) (например, 64-бит), в который загружается инициализирующий вектор синхропосылки, используемый для шифрования в режимах гаммирования и гаммирования с обратной связью, а также регистр (20) (например, 64-бит), в который загружается инициализирующий вектор имитовставки. Указанные выше устройства соединяются между собой, как показано на фиг. 1, 5 (для первого варианта устройства (7) шифрования) и на фиг. 2, 6 (для второго варианта устройства (7) шифрования). В качестве контроллера (4) прямого доступа к памяти, одновременно обрабатывающего запросы на чтение/запись данных из/в память, может быть использовано известное (IP)-решение от фирмы Synopsys или другое оборудование, основное требование к которому - это возможность одновременной работы канала чтения данных из памяти (6) (например, внутреннего или внешнего последовательного ОЗУ) в устройство (7) шифрования и канала записи криптопреобразованных данных из устройства (7) шифрования обратно в память (6) (например, последовательное ОЗУ). Для передачи данных для шифрования в вычислительные модули (8) и (9) может быть использована шина (14) адрес-данные, например, удовлетворяющая стандарту AHB (Advanced High-performance Bus). Для передачи криптопреобразованных данных в контроллер (4) прямого доступа в память (6) может быть использована шина (15) адрес-данные, удовлетворяющая, например, стандарту AHB (Advanced High-performance Bus). Вычислительный модуль (8) имеет возможность реализации алгоритмов, обеспечивающих реализацию режима простой замены, режима гаммирования и режима гаммирования с обратной связью, предусмотренных, например, ГОСТ 28147-89.

Для шифрования в режиме простой замены с зацеплением вычислительный (8) модуль дополняется оборудованием для сложения по модулю 2 (операция $\oplus$ - "исключающее ИЛИ"). Этот режим отличается от режима простой замены, который описан, например, в ГОСТ 28147-89 тем, что каждый следующий блок данных перед началом обработки "зацепляется" с результатом, полученным при обработке предыдущего блока данных, путем сложения по модулю 2, как представлено на фиг. 4.

Для оптимизации процесса шифрования устройство (7) шифрования по второму варианту дополняется вычислительным модулем (9), имеющим возможность параллельной реализации алгоритма выработки имитовставки (предусмотренного, например, ГОСТ 28147-89).

В состав устройства шифрования входит блок (21) управления, который реализован в виде конечного автомата, находящегося в состоянии ожидания поступления команды, переводящей устройство (7)

шифрования в один из рабочих режимов. Под выбором режима работы устройства (7) шифрования, представленного в данном изобретении, понимается установление в активное состояние одного из алгоритмов шифрования путем программирования блока (21) управления в устройстве (7) шифрования.

После выставления одного из рабочих режимов работы начинается процесс шифрования. По окончании шифрования центральный процессор (2) переводит устройство (7) шифрования обратно в режим ожидания.

Блок (21) управления вырабатывает также управляющие и статусные сигналы, необходимые для работы устройства (7) шифрования. По меньшей мере, вырабатываются следующие виды сигналов:

статус работы устройства (7) шифрования (шифрование завершено/шифрование продолжается);

сигналы, управляющие передачей данных в вычислительные устройства (8), (9) из контроллера (4) и криптопреобразованных данных обратно в контроллер (4), удовлетворяющие, например, стандарту AHB (Advanced High-performance Bus);

сигналы, управляющие записью и чтением данных в/из блок(а) (21) управления, удовлетворяющие, например, стандарту APB (Advanced Peripheral Bus).

Для передачи данных для шифрования в вычислительные модули (8) и (9) может быть использована шина (14) адрес-данные, например, удовлетворяющая стандарту AHB. Для передачи криптопреобразованных данных в контроллер прямого доступа в память может быть использована шина (15) адрес-данные, например, удовлетворяющая стандарту AHB.

Вычислительные модули (8), (9) соединяются с регистрами (17), (18), (19), (20) и блоком (21) управления одно или двунаправленным шинам данных, например, шириной 64 бита.

В зависимости от требований к производительности устройство (7) шифрования может не содержать вычислительного устройства, выделенного только для вычисления имитовставки (9), как показано на фиг. 1. Часть алгоритмов шифрования, реализованных в заявляемом изобретении устройства (7), не требует вычисления имитовставки, поэтому такая реализация может оказаться оптимальным вариантом.

В случае, если пользователь желает осуществлять шифрование с вычислением имитовставки, то устройство (7) шифрования (фиг. 1) может быть переведено в режим, сопровождаемый вычислением имитовставки, а ее вычисление будет производиться в вычислительном устройстве (8) после окончания процесса основного процесса шифрования. Блок (21) управления перенаправляет соответствующие операнды в вычислительное устройство (8). Результат вычисления имитовставки, в независимости от конфигурации устройства (7) шифрования, сохраняется в регистре (20) данных.

Алгоритм работы устройства (7) шифрования данных в общем виде представлен на фиг. 3. Устройство (7) шифрования находится в режиме ожидания прихода управляющих команд.

Перед выставлением активного режима работы устройства (7) проверяется условие-1, относительно того, требуется ли обновление таблицы замен в регистре (17), используемой при шифровании в соответствии со стандартом ГОСТ 28147-89. По умолчанию блок (21) управления может хранить стандартное значение таблицы замен. Если "Да", то таблица загружается, если "Нет", то далее проверяется условие-2 относительно того, требуется ли загрузка шифровального ключа в регистр (18). В общем случае один и тот же ключ может использоваться для нескольких блоков данных и его обновление не требуется. Если "Да", то ключ загружается, если "Нет", то далее проверяется условие-3 относительно того, требуется ли загрузка инициализирующего вектора синхропосылки в регистр (19), используемого лишь в части рабочих режимов работы, предусмотренных стандартом ГОСТ 28147-89. Если "Да", то вектор синхропосылки загружается, если "Нет", то далее проверяется условие-4 относительно того, требуется ли загрузка инициализирующего вектора имитовставки в регистр (20), используемого лишь в части рабочих режимов, предусмотренных стандартом ГОСТ 28147-89. Если "Да", то вектор имитовставки загружается, если "Нет", то далее выставляется рабочий режим шифрования.

Далее проверяется условие-5 относительно того, установлен ли режим работы с прямым доступом в память.

Если выставлен режим работы с прямым доступом в память (6), то центральным процессором (2) производится программирование контроллера (4) с указанием, по крайней мере, адреса в памяти, откуда данные для шифрования должны быть загружены, адреса в памяти, по которым криптопреобразованные данные должны быть сохранены, и размер массива данных для шифрования. Затем по мере поступления данных из памяти они поступают блоками в вычислительное устройство (8) или устройства (8), (9), в зависимости от режима работы и конфигурации устройства (7) шифрования. После проведения шифрования данные передаются обратно в память по известному адресу. Затем проверяется условие-6 относительно того, является ли только что обработанный блок последним в массиве данных. Если "Да", то устройство шифрования заканчивает работу и ожидает команды от центрального процессора (2), который переведет устройство (7) шифрования в режим ожидания, если "Нет", то следующий блок данных обрабатывается аналогично описанному выше.

Если выставлен режим без прямого доступа к памяти, то устройство (7) шифрования ожидает загрузки центральным процессором (2) блока данных для шифрования по выставленному режиму работы. По окончании шифрования устройство (7) шифрования ожидает команды от центрального процессора (2) на чтение криптопреобразованных данных. После чтения результата устройство переводится в режим

ожидания.

Заявлено СнК (1) с использованием устройства шифрования (7) данных и с возможностью обращения к памяти, включенной в состав СнК (внутренней) или памяти, имеющей возможность подключения к СнК по стандартному протоколу (внешней), в частном случае в качестве любой памяти может быть использовано последовательное ОЗУ (6), помимо устройства (7) шифрования включает в себя центральный процессор (2), посредством которого могут исполняться программы и обрабатываться внешние прерывания, блок внутренней коммутации (3), обеспечивающий обмен информацией (данными) между функциональными блоками СнК (1) по единому протоколу между устройством (7) шифрования, центральным процессором (2) и памятью (6) через стандартный контроллер (5) памяти (6). В качестве блока внутренней коммутации (3) и в качестве контроллера памяти (5) могут быть использованы известные (IP)-решения от фирмы Synopsys. Обмен данными между центральным процессором и остальными узлами СнК осуществляется через блок внутренней коммутации с использованием шины адрес-данные, например, удовлетворяющей стандарту Advanced extensible Interface (AXI).

Функционирование СнК (1) осуществляется путем программирования центрального процессора (2), в качестве которого может использоваться, например, микропроцессорная система MIPS P-5600 от фирмы Imagination Technologies, и команды от которого передаются через конфигурационный интерфейс (11), имеющей в своем составе, по крайней мере, шину адреса, данных и шину контроля передаваемой информации. Управляющие сигналы поступают в контроллер (4) прямого доступа к памяти и в блок (21) управления устройства (7) шифрования.

Аналогично управлению режимами работы блока (21) управления, входящего в состав устройства шифрования (7), через команды от центрального процессора (2), программируется контроллер (4) прямого доступа к памяти, устанавливая адреса по которым необходимо взять данные для шифрования из памяти (6) (например, внешнего или входящего в состав СнК последовательного ОЗУ) и возвратить (сохранить, направить) обратно в память (6) данные, криптопреобразованные устройством (7) шифрования, а также программируются правила выработки прерываний по окончании передачи данных в/из памяти (6).

При использовании обоих вариантов устройства (7) шифрования в составе СнК результат шифрования накапливается в блоке (21) управления устройства (7) шифрования и в зависимости от выбранного режима работы направляется обратно в память (6) (например, внешнее или входящее в состав СнК последовательное ОЗУ) через контроллер (4) прямого доступа к памяти, либо хранится в блоке (21) управления, дожидаясь запроса на "чтение" из центрального процессора (2), при использовании устройства шифрования в составе вычислительной системы. Результат выработки имитовставки также считывается по запросу из центрального процессора (2) из соответствующего регистра (20). При этом может быть использована конфигурационная шина (11) адрес-данных для управления работой устройства шифрования, например, удовлетворяющая стандарту APB. Для передачи криптопреобразованных данных в блок внутренней коммутации может быть использована шина (12) адрес-данные, например, удовлетворяющая стандарту AXI. Для передачи данных для шифрования в контроллер (4) прямого доступа к памяти может быть использована шина (13) адрес-данные, например, удовлетворяющая стандарту AXI. Для передачи данных для шифрования в вычислительные модули (8) и (9) может быть использована шина (14) адрес-данные, например, удовлетворяющая стандарту AHB. Для передачи криптопреобразованных данных в контроллер (4) прямого доступа в память может быть использована шина (15) адрес-данные, например, удовлетворяющая стандарту AHB. Данные из памяти передаются в контроллер (5) памяти и обратно по стандартному интерфейсу. Для передачи данных в/из контроллера (5) памяти в/из блока (3) внутренней коммутации может быть использована шина (16) адрес-данные, например, удовлетворяющая стандарту AXI.

В зависимости от режима работы устройства (7) шифрования данные для шифрования могут либо поступать в потоковом виде напрямую из памяти (6) (например, последовательного ОЗУ) через контроллер (4) прямого доступа к памяти, либо поступать в виде одиночного блока данных по команде центрального процессора (2). В последнем случае результат криптопреобразования становится доступен центральному процессору для чтения через блок внутренней коммутации. В случае потокового режима работы требуется предварительное программирование контроллера (4), с указанием адреса, по которому данные располагаются в памяти (6) (во внешнем или входящем в состав СнК последовательном ОЗУ), адреса, по которому криптопреобразованные данные должны быть сохранены (направлены) обратно в память (6), а также размер данных для криптопреобразования. В случае одиночного блока данных, загружаемого в устройство (7) шифрования по команде центрального процессора, предварительного программирования контроллера (4) не требуется.

При использовании в составе СнК (1) первого варианта устройства шифрования, изображенного на фиг. 1, получаем первый вариант СнК, а при использовании в составе СнК (1) второго варианта устройства шифрования, изображенного на фиг. 2, получаем второй вариант СнК. Функционирование СнК в обоих вариантах осуществляется аналогично, за исключением процессов шифрования, происходящих в устройстве (7) шифрования. При этом второй вариант СнК предпочтительнее использовать для ускорения процесса шифрования в режимах, сопровождаемых вычислением имитовставки, с использованием вычислительного блока (9) устройства (7) шифрования, позволяющего осуществлять ее вычисление па-

раллельно основному процессу шифрования, происходящему в вычислительном блоке (8).

В качестве памяти (6) при обоих вариантах осуществления устройства шифрования (7) и СнК с использованием этих вариантов может быть использовано внешнее последовательное ОЗУ (например, SRAM, DDR, DDR2, DDR3 и т.п.).

Основная сфера применения устройства - защищенные соединения с использованием TLS (Transport Layer Security - криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет). Изобретение также может широко применяться в СнК, управляющих контроллерах, выполняющих шифрование данных, поступающих из сети Интернет или находящихся на жестких дисках.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Устройство шифрования данных согласно ГОСТ 28147-89, отличающееся тем, что включает в себя контроллер внешнего последовательного ОЗУ, устройство отображения адресов данных в адресное пространство микропроцессорного ядра, а также регистр считанных данных и конечный автомат устройства отображения адресов данных, располагающихся во внешнем последовательном ОЗУ, в адресное пространство микропроцессорного ядра, преобразования запросов на чтение со стороны микропроцессорного ядра в последовательность обращений к контроллеру внешнего последовательного ОЗУ и передачи по шине данных последовательности слов данных, считанных из внешнего последовательного ОЗУ, подключаемого по стандартному интерфейсу, в микропроцессорное ядро, обеспечивая тем самым загрузку массива данных из памяти для шифрования устройством шифрования данных и сохранение криптопреобразованных данных обратно в память, вычислительный блок с возможностью реализации шифрования данных в соответствии с выбранным алгоритмом с использованием регистров данных для хранения таблиц подстановки, для хранения ключей для шифрования, векторов синхропосылки и имитовставки, а также блок управления, выполненный с возможностью установления статуса устройства шифрования, сигналов управления передачей данных в вычислительный блок и переключения режимов работы устройства шифрования.

2. Устройство шифрования данных согласно ГОСТ 28147-89, отличающееся тем, что включает в себя контроллер внешнего последовательного ОЗУ, устройство отображения адресов данных в адресное пространство микропроцессорного ядра, а также регистр считанных данных и конечный автомат устройства отображения адресов данных, располагающихся во внешнем последовательном ОЗУ, в адресное пространство микропроцессорного ядра, преобразования запросов на чтение со стороны микропроцессорного ядра в последовательность обращений к контроллеру внешнего последовательного ОЗУ и передачи по шине данных последовательности слов данных, считанных из внешнего последовательного ОЗУ, подключаемого по стандартному интерфейсу, в микропроцессорное ядро, обеспечивая тем самым загрузку массива данных из памяти для шифрования устройством шифрования данных и сохранение криптопреобразованных данных обратно в память, вычислительный блок, выполненный с возможностью шифрования данных в соответствии с выбранным алгоритмом, дополнительный вычислительный блок, выполненный с возможностью вычисления имитовставки параллельно основному процессу шифрования, регистры данных для хранения таблиц подстановки, для хранения ключей для шифрования, векторов синхропосылки и имитовставки, а также блок управления, выполненный с возможностью установления статуса устройства шифрования, сигналов управления передачей данных в вычислительный блок и дополнительный вычислительный блок и переключения режимов работы устройства шифрования.

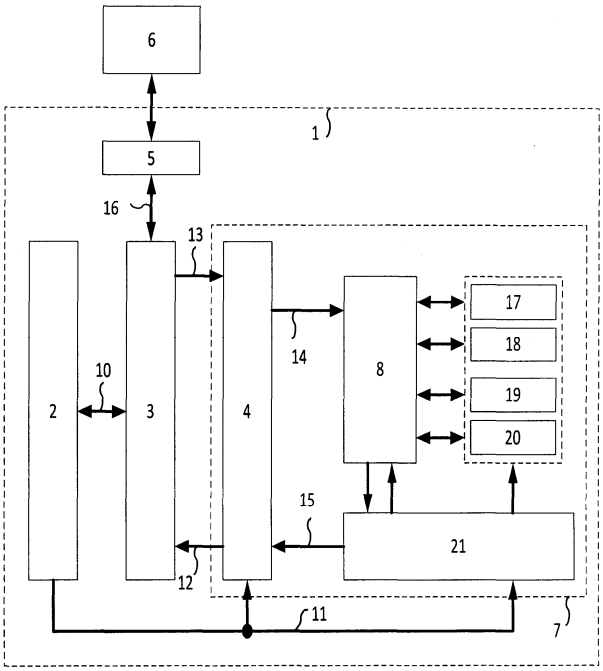
3. Система на кристалле (СнК) для шифрования данных согласно ГОСТ 28147-89, отличающаяся тем, что она включает в себя устройство шифрования данных согласно ГОСТ 28147-89 по п.1, центральный процессор, управляющий работой всей системы в целом, внутреннюю память, блок внутренней коммутации, обеспечивающий возможность обмена данными по единому протоколу через шины адрес-данные между устройством шифрования, центральным процессором и внутренней памятью, при этом данные для шифрования поступают в устройство шифрования из внутренней памяти через контроллер памяти, выполненный с возможностью преобразования последовательных данных в формат, применяемый блоком внутренней коммутации, а результат криптопреобразования направляют во внутреннюю память из устройства шифрования через блок внутренней коммутации и контроллер памяти.

4. Система на кристалле (СнК) для шифрования данных согласно ГОСТ 28147-89, отличающаяся тем, что она включает в себя устройство шифрования данных согласно ГОСТ 28147-89 по п.1, центральный микропроцессор, управляющий работой всей системы в целом, блок внутренней коммутации, обеспечивающий возможность обмена данными по единому протоколу через шины адрес-данные между устройством шифрования, центральным процессором и внешней памятью, при этом данные для шифрования поступают в устройство шифрования из внешней памяти через контроллер памяти, входящий в состав СнК и который выполнен с возможностью преобразования последовательных данных в формат, применяемый блоком внутренней коммутации, а результат криптопреобразования направляют из устройства шифрования во внешнюю память через блок внутренней коммутации и контроллер памяти.

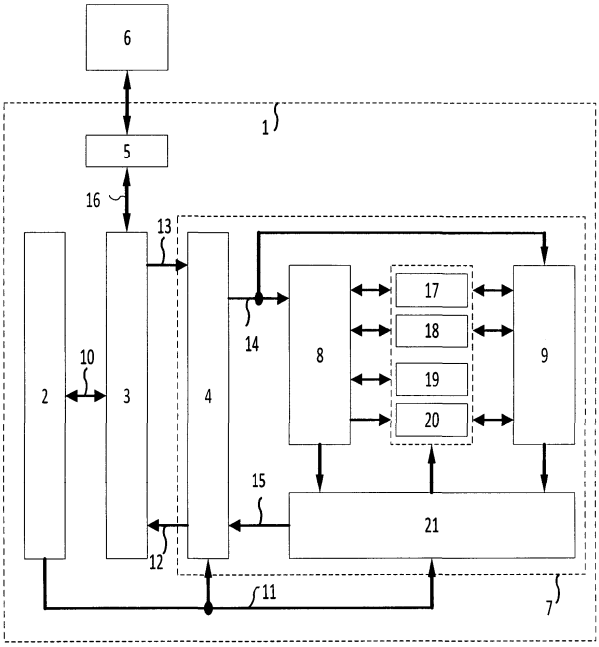
5. Система на кристалле (СнК) для шифрования данных согласно ГОСТ 28147-89, характеризую-

щаяся тем, что она включает в себя устройство шифрования данных согласно ГОСТ 28147-89 по п.2, центральный микропроцессор, управляющий работой всей системы в целом, внутреннюю память, блок внутренней коммутации, обеспечивающий возможность обмена данными по единому протоколу через шины адрес-данные между устройством шифрования, центральным процессором и внутренней памятью, при этом данные для шифрования поступают в устройство шифрования из внутренней памяти через контроллер памяти, выполненный с возможностью преобразования последовательных данных в формат, применяемый блоком внутренней коммутации, а результат криптопреобразования направляют во внутреннюю память из устройства шифрования через блок внутренней коммутации и контроллер памяти, при этом в качестве памяти используют последовательное ОЗУ.

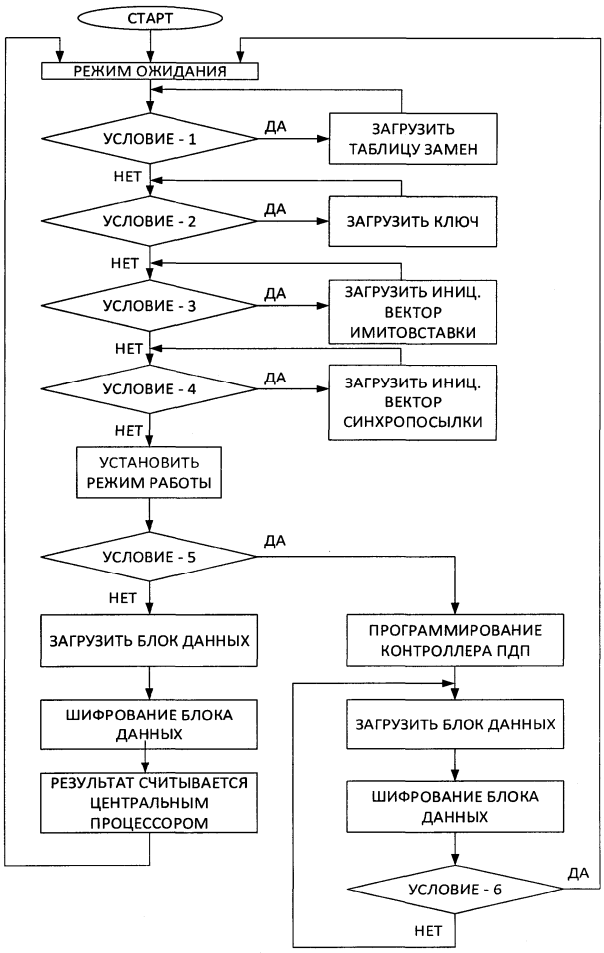
6. Система на кристалле (СнК) для шифрования данных согласно ГОСТ 28147-89, характеризующаяся тем, что она включает в себя устройство шифрования данных согласно ГОСТ 28147-89 по п.2, центральный микропроцессор, управляющий работой всей системы в целом, блок внутренней коммутации, обеспечивающий возможность обмена данными по единому протоколу через шины адрес-данные между устройством шифрования, центральным процессором и внешней памятью, при этом данные для шифрования поступают в устройство шифрования из внешней памяти через контроллер памяти, входящий в состав СнК и который выполнен с возможностью преобразования последовательных данных в формат, применяемый блоком внутренней коммутации, а результат криптопреобразования направляют из устройства шифрования во внешнюю память через блок внутренней коммутации и контроллер памяти.



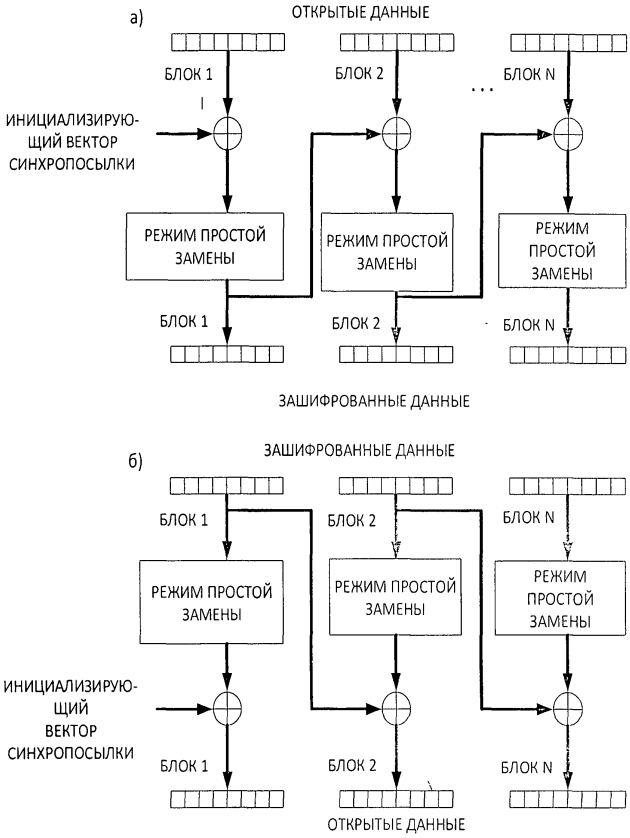
Фиг. 1


6
1
5
16
13
2
10
3
4
14
8
17
18
19
20
9
15
21
12
11
7

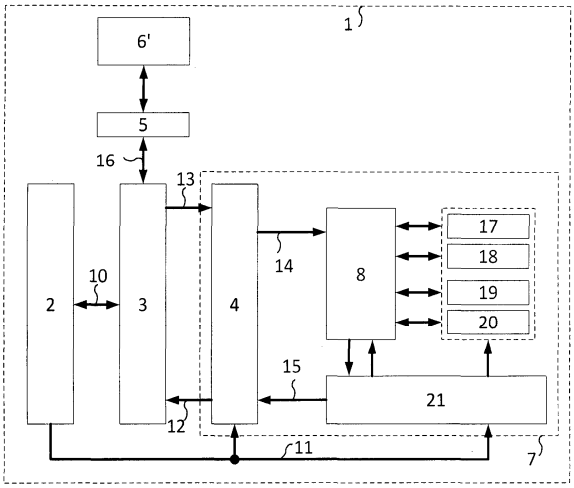
Фиг. 2


СТАРТ
РЕЖИМ ОЖИДАНИЯ
УСЛОВИЕ - 1
ДА
ЗАГРУЗИТЬ ТАБЛИЦУ ЗАМЕН
НЕТ
УСЛОВИЕ - 2
ДА
ЗАГРУЗИТЬ КЛЮЧ
НЕТ
УСЛОВИЕ - 3
ДА
ЗАГРУЗИТЬ ИНИЦ. ВЕКТОР ИМИТОВСТАВКИ
НЕТ
УСЛОВИЕ - 4
ДА
ЗАГРУЗИТЬ ИНИЦ. ВЕКТОР СИНХРОПОСЫЛКИ
НЕТ
УСТАНОВИТЬ РЕЖИМ РАБОТЫ
УСЛОВИЕ - 5
ДА
НЕТ
ЗАГРУЗИТЬ БЛОК ДАННЫХ
ШИФРОВАНИЕ БЛОКА ДАННЫХ
РЕЗУЛЬТАТ СЧИТЫВАЕТСЯ ЦЕНТРАЛЬНЫМ ПРОЦЕССОРОМ
ПРОГРАММИРОВАНИЕ КОНТРОЛЛЕРА ПДП
ЗАГРУЗИТЬ БЛОК ДАННЫХ
ШИФРОВАНИЕ БЛОКА ДАННЫХ
УСЛОВИЕ - 6
ДА
НЕТ

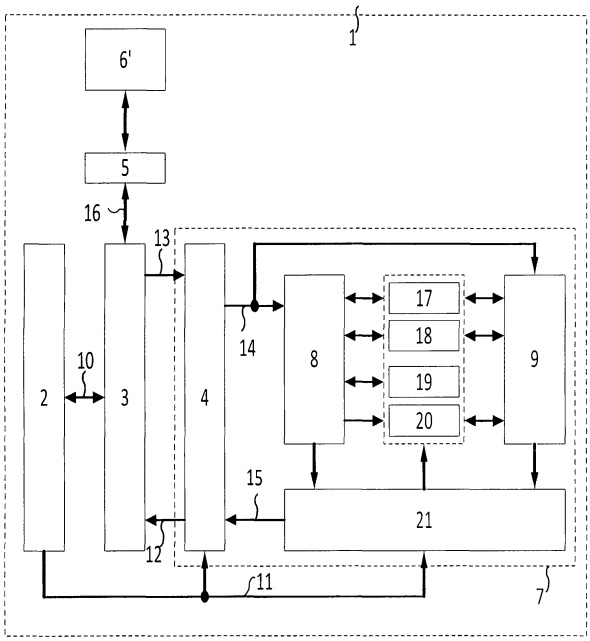
Фиг. 3


а)
ОТКРЫТЫЕ ДАННЫЕ
БЛОК 1
БЛОК 2
БЛОК N
ИНИЦИАЛИЗИРУЮ-
ЩИЙ ВЕКТОР
СИНХРОПОСЫЛКИ
РЕЖИМ ПРОСТОЙ ЗАМЕНЫ
РЕЖИМ ПРОСТОЙ ЗАМЕНЫ
РЕЖИМ ПРОСТОЙ ЗАМЕНЫ
БЛОК 1
БЛОК 2
БЛОК N
ЗАШИФРОВАННЫЕ ДАННЫЕ
б)
ЗАШИФРОВАННЫЕ ДАННЫЕ
БЛОК 1
БЛОК 2
БЛОК N
РЕЖИМ ПРОСТОЙ ЗАМЕНЫ
РЕЖИМ ПРОСТОЙ ЗАМЕНЫ
РЕЖИМ ПРОСТОЙ ЗАМЕНЫ
ИНИЦИАЛИЗИРУЮ-
ЩИЙ
ВЕКТОР
СИНХРОПОСЫЛКИ
БЛОК 1
БЛОК 2
БЛОК N
ОТКРЫТЫЕ ДАННЫЕ

Фиг. 4


1
6'
5
16
13
2
10
3
4
14
8
17
18
19
20
15
21
12
11
7

Фиг. 5



Фиг. 6

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2