ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ

(19) **BY** (11) **5121**

(13) **C1**

(51)[7] **H 04K 01/00,**
H 04L 09/00

НАЦИОНАЛЬНЫЙ ЦЕНТР
ИНТЕЛЛЕКТУАЛЬНОЙ
СОБСТВЕННОСТИ

(54) УСТРОЙСТВО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ С ОБНАРУЖЕНИЕМ И КОРРЕКЦИЕЙ ОШИБОК

(21) Номер заявки: a 19990935
(22) 1999.10.15
(46) 2003.06.30

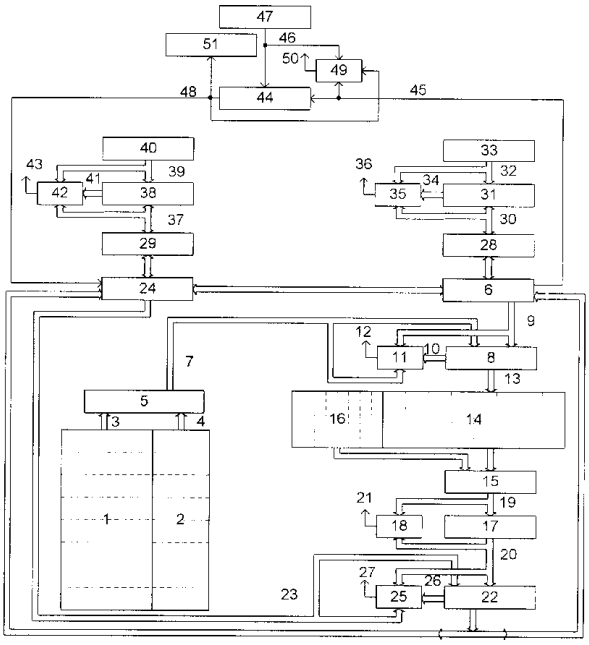
(71) Заявитель: Учреждение образования "Белорусский государственный технологический университет" (BY)

(72) Авторы: Урбанович Павел Павлович; Пацей Наталья Владимировна (BY)

(73) Патентообладатель: Учреждение образования "Белорусский государственный технологический университет" (BY)

(57)

Устройство криптографического преобразования информации с обнаружением и коррекцией ошибок, содержащее ключевое запоминающее устройство (КЗУ), первый 32-разрядный сумматор по модулю 2^{32}, первые входы которого соединены с первыми выходами первого 32-разрядного накопителя, а выходы первого 32-разрядного сумматора по модулю 2^{32} подключены к входам блока подстановки, регистр циклического сдвига, соединенный выходами с первыми входами первого 32-разрядного сумматора по модулю 2, вторые входы которого соединены с выходами второго 32-разрядного накопителя, первые выходы первого 32-разрядного сумматора по модулю 2 соединены с первыми входами первого и второго 32-разрядных накопителей, соединенных первой двунаправленной шиной входа-выхода между собой, а также с третьим и четвертым 32-разрядными накопителями соответственно через вторые двунаправленные шины входа-выхода, третий и четвертый 32-разрядные накопители



Фиг. 1

BY 5121 C1

по третьим двунаправленным шинам входа-выхода соединены со вторым 32-разрядным сумматором по модулю 2^{32} и 32-разрядным сумматором по модулю (2^{32}-1) соответственно, второй 32-разрядный сумматор по модулю 2^{32} вторыми входами соединен с выходами пятого 32-разрядного накопителя, а выходы шестого 32- разрядного накопителя подключены ко вторым входам 32-разрядного сумматора по модулю (2^{32}-1), второй 32-разрядный сумматор по модулю 2, первым входом соединенный с выходом первого 32-разрядного накопителя, вторым входом - с источником данных, а выходом подключенный к потребителю данных и ко второму входу второго 32-разрядного накопителя, при этом КЗУ содержит восемь 32-разрядных накопителей, **отличающееся** тем, что содержит блоки контроля с первого по шестой, первый и второй блоки исправления ошибок, соответствующие 32-разрядным накопителям КЗУ восемь r-разрядных накопителей хранения проверочных разрядов для КЗУ, количество разрядов которых определено мощностью корректирующего кода, накопитель хранения проверочных разрядов для блока подстановки, выходы накопителей хранения проверочных разрядов для КЗУ соединены с первыми входами первого блока исправления ошибок, вторые входы которого связаны с выходами КЗУ, а выходы первого блока исправления ошибок соединены со вторыми входами первого сумматора по модулю 2^{32}, выходы накопителя хранения проверочных разрядов для блока подстановки соединены с первыми входами второго блока исправления ошибок, вторые входы которого подключены к выходам блока подстановки, а выходы соединены со входами регистра циклического сдвига, первые, вторые и третьи входы первого блока контроля соединены с выходами первого блока исправления ошибок, первого 32-разрядного накопителя и вторыми выходами первого сумматора по модулю 2^{32} соответственно, первые и вторые входы второго блока контроля подключены к выходам второго блока исправления ошибок и выходам регистра циклического сдвига соответственно, первые, вторые и третьи входы третьего блока контроля соединены с выходами регистра циклического сдвига, выходами второго 32-разрядного накопителя и вторыми выходами первого сумматора по модулю 2 соответственно, первые, вторые и третьи входы четвертого блока контроля подключены к выходам пятого 32-разрядного накопителя, третьей двунаправленной шине между третьим 32-разрядным накопителем и вторым 32-разрядным сумматором по модулю 2^{32} и выходам второго 32-разрядного сумматора по модулю 2^{32} соответственно, первые, вторые и третьи выходы пятого блока контроля соединены с выходами шестого 32-разрядного накопителя, третьей двунаправленной шиной между четвертым 32-разрядным накопителем и 32-разрядным сумматором по модулю (2^{32}-1), выходами 32-разрядного сумматора по модулю (2^{32}-1) соответственно, первые, вторые и третьи входы шестого блока контроля связаны с выходом источника данных, вторым выходом первого 32-разрядного накопителя и выходом второго 32-разрядного сумматора по модулю 2 соответственно, сигналы на выходах блоков контроля с первого по шестой являются флагами ошибок.

(56)
ГОСТ 28147-89.
US 5432848 A, 1995.
EP 0366589 A2, 1990.
EP 0676876 A1, 1995.
RU 2092890 C1, 1997.

Изобретение относится к криптографическим преобразованиям и корректирующему кодированию и может быть использовано в системах обработки информации вычислительных машин, сетей вычислительных машин и отдельных вычислительных комплексах.

Известны устройства [1] криптографического преобразования (криптосхемы) данных с проверкой корректности функционирования, в которых исходные данные поступают в аналогичные по структуре и алгоритму, но независимые устройства шифрования/дешифрования.

По завершении результаты преобразований этих устройств сравниваются. При совпадении результатов делается предположение, что оба устройства работают корректно, если результаты различны, то можно предположить, что, по меньшей мере, в одном из устройств произошла ошибка, и процесс преобразования повторяется в каждом из устройств.

Недостатком известных устройств является удвоение аппаратурных затрат на шифрование/дешифрование и, кроме того, ошибка будет обнаружена лишь после завершения алгоритма преобразования, что увеличивает время обнаружения и исправления ошибок.

Наиболее близким к предлагаемому изобретению является устройство (криптосхема алгоритма) криптографического преобразования информации [2], содержащее ключевое запоминающее устройство (КЗУ), состоящее из восьми 32-разрядных накопителей, соединенное выходами с первыми входами первого 32-разрядного сумматора по модулю 2^{32}, который вторыми входами соединен с первыми выходами первого 32-разрядного накопителя, а выходами подключенный к входам блока подстановки, который соединен по выходам с входами регистра циклического сдвига, выходами подключенный к первым входам первого 32-разрядного сумматора по модулю 2, вторые входы которого соединены с выходами второго 32-разрядного накопителя, выходы первого сумматора по модулю 2 коммутируются с первыми входами первого и второго 32-разрядных накопителей, соединенных первой двунаправленной шиной входа-выхода между собой, а также с третьим и четвертым 32-разрядными накопителями соответственно через вторые двунаправленные шины входа-выхода, третий и четвертый 32-разрядные накопители по третьим двунаправленным шинам входа-выхода соединены со вторым 32-разрядным сумматором по модулю 2^{32} и 32-разрядным сумматором по модулю $(2^{32}-1)$ соответственно, второй 32-разрядный сумматор по модулю 2^{32} вторыми входами соединен с выходами пятого 32-разрядного накопителя, а выходы шестого 32-разрядного накопителя подключены ко вторым входам 32-разрядного сумматора по модулю $(2^{32}-1)$, второй 32-разрядный сумматор по модулю 2, первым входом соединенный с выходом первого накопителя, вторым входом соединенный с источником данных, а выходом подключенный к потребителю и к входу второго накопителя.

В криптосхеме предусмотрены четыре режима работы: режим простой замены, гаммирование, гаммирование с обратной связью и выработка имитовставки. В зависимости от режима активизируются те или иные блоки устройства.

При криптографических преобразованиях важно быть уверенными, что операции шифрования/дешифрования выполнены точно. Однако из-за большого количества запоминающих устройств, накопителей, а также из-за возникновения какого-либо нарушения нормального функционирования логических или арифметических операций в известном устройстве результат преобразования может быть неверным. При этом, как правило, ошибки остаются необнаруженными либо требуется повторение прямого и обратного преобразования. Указанные недостатки снижают надежность функционирования устройства из-за отказов элементов памяти и блоков преобразования информации.

Задачей изобретения является повышение отказоустойчивости устройства криптографического преобразования информации путем введения схем исправления ошибок для блоков ЗУ и схем проверок операций преобразования основного устройства до завершения алгоритма и с меньшим количеством избыточной аппаратуры, чем в аналогичных устройствах.

Поставленная задача решается тем, что в устройство криптографического преобразования, содержащее ключевое запоминающее устройство, состоящее из восьми 32-разрядных накопителей, 32-разрядный сумматор по модулю 2^{32}, первые входы которого соединены с первыми выходами первого 32-разрядного накопителя, а выходы 32-разрядного сумматора по модулю 2^{32} подключены к входам блока подстановки, регистр циклического сдвига, соединенный по выходам с первыми входами первого 32-разрядного сумматора по модулю 2, вторые входы которого соединены с выходами второго 32-разрядного накопителя, первые выходы первого 32-разрядного сумматора по модулю 2

коммутируются с первыми входами первого и второго 32-разрядных накопителей, соединенных первой двунаправленной шиной входа-выхода между собой, а также с третьим и четвертым 32-разрядными накопителями соответственно через вторые двунаправленные шины входа-выхода, третий и четвертый 32-разрядные накопители по третьим двунаправленным шинам входа-выхода соединены со вторым 32-разрядным сумматором по модулю 2^{32} и 32-разрядным сумматором по модулю $(2^{32}-1)$ соответственно, второй 32-разрядный сумматор по модулю 2 вторыми входами соединен с выходами пятого 32-разрядного накопителя, а выходы шестого 32-разрядного накопителя подключены ко вторым входам 32-разрядного сумматора по модулю $(2^{32}-1)$, второй 32-разрядный сумматор по модулю 2, первым входом соединенный с выходом первого накопителя, вторым входом - с источником данных, а выходом - к потребителю данных и ко второму входу второго накопителя, введены блоки контроля с первого по шестой, первый и второй блоки исправления ошибок, дополнительные накопители хранения проверочных разрядов для ключевого запоминающего устройства (КЗУ) и блока подстановки, выходы дополнительного накопителя КЗУ соединены с первыми входами первого блока исправления ошибок, вторые входы которого связаны с выходами КЗУ, а выходы - со вторыми входами первого сумматора по модулю 2^{32}, выходы дополнительного накопителя хранения проверочных разрядов для блока подстановки соединены с первыми входами второго блока исправления ошибок, вторые входы которого подключены к выходам блока подстановки, а выходы - со входами регистра циклического сдвига, первые, вторые и третьи входы первого блока контроля соединены с выходами первого блока исправления ошибок, первого 32-разрядного накопителя и вторыми выходами первого сумматора по модулю 2^{32} соответственно, первые и вторые входы второго блока контроля подключены к выходам второго блока исправления ошибок и выходам регистра циклического сдвига соответственно, первые, вторые и третьи входы третьего блока контроля соединены с выходами регистра циклического сдвига, выходами второго 32-разрядного накопителя и вторыми выходами первого сумматора по модулю 2 соответственно, первые, вторые и третьи входы четвертого блока контроля подключены соответственно к выходам пятого 32-разрядного накопителя, третьей двунаправленной шине между третьим 32-разрядным накопителем и вторым 32-разрядным сумматором по модулю 2^{32} и выходам второго 32-разрядного сумматора по модулю 2^{32}, первые, вторые и третьи выходы пятого блока контроля соединены соответственно с выходами шестого 32-разрядного накопителя, третьей двунаправленной шиной между четвертым 32-разрядным накопителем и 32-разрядным сумматором по модулю $(2^{32}-1)$, выходами 32-разрядного сумматором по модулю $(2^{32}-1)$, первые вторые и третьи входы шестого блока контроля связаны соответственно с выходом источника данных, вторым выходом 32-разрядного накопителя и выходом второго 32-разрядного сумматора по модулю 2, сигналы на выходах блоков контроля с первого по шестой являются флагами ошибок.

Сущность изобретения заключается в том, что каждое информационное слово данных, хранимых в накопителях (КЗУ и блока подстановки), при записи информации в эти накопители дополняется проверочными (контрольными) разрядами, которые предварительно формируются на основе используемого корректирующего кода [3] и записываются в соответствующие дополнительные накопители. С помощью контрольных разрядов и аппаратуры декодирования возможно обнаружение и исправление возникающих в информационных разрядах ошибок при считывании информации из накопителей. Кроме того, с помощью блоков контроля в схеме осуществляется проверка корректности выполнения основных арифметических и логических операций алгоритма при помощи методов контроля, основанных на свойствах сравнений (контроля по модулю) [4].

Предлагаемое устройство криптографического преобразования (фиг. 1) содержит КЗУ на 256 бит, состоящее из восьми 32-разрядных накопителей 1 и соответствующих им восьми r-разрядных дополнительных накопителей 2 (количество разрядов в дополнительных накопителях определяется мощностью используемого корректирующего кода). В ре-

жиме записи параллельно с занесением информации в накопители 1 вычисляются их проверочные разряды и заносятся в соответствующие накопители 2. Содержимое накопителей 1 и 2 по выходам соответственно 3 и 4 поступает в первый блок исправления ошибок 5, корректирующий возникшие при считывании данных ошибки. По существу заполнение накопителей 1 и 2 представляет собой информационную и проверочную части кодового слова систематического корректирующего кода (32 + r, 32), исправляющего t ошибок, а блок 5 - помехоустойчивый кодер. Заполнение первого 32-разрядного накопителя 6 суммируется по модулю 2^{32} со скорректированными блоком 5 данными (формируются на выходах 7 блока 5), считываемыми из КЗУ, в первом 32-разрядном сумматоре 8. Для контроля операции суммирования слагаемые 7 и 9 так же, как и сама сумма 10, поступают в первый блок контроля 11. Блок 11 функционирует на основе метода контроля по модулю p. Обозначим слагаемые 7 как A, 9 - B, а их сумму 10 - A + B = C. Для контроля целесообразно перейти от двоичного представления исходной информации к новому представлению с основанием $q = 2^s$. Контрольные коды могут быть вычислены путем разбиения двоичных данных на группы по s разрядов с последующим суммированием этих групп по модулю $p = (2^s \pm 1)/m$, где m и s - некоторые целые положительные числа ($s \geq 2$). Этот процесс называется свертыванием [3]:

$$r'_A \equiv \sum_{i=1}^{32/s} a_i \pmod p;$$

$$r'_B \equiv \sum_{i=1}^{32/s} b_i \pmod p;$$

$$r'_C \equiv \sum_{i=1}^{32/s} c_i \pmod p,$$

где a_i, b_i и c_i - двоичные изображения цифр в системе с основанием 2^s, r'_A, r'_B, r'_C - контрольные коды для чисел A, B и C соответственно.

Контрольный код C находим через контрольные коды слагаемых, а именно:

$$r_C \equiv \left[r'_A + r'_B - \alpha\right] \pmod p,$$

$\alpha = 0$ при $A + B < 2^{32}$,

$\alpha = 1$ при $A + B \geq 2^{32}$.

Блок 11 проверяет соответствие сверток r'_C и r_C. При их совпадении операция выполнена корректно. В случае несовпадения сверток выдается сигнал об ошибке 12 (выставляется флаг ошибки), и операция повторяется снова. Достоинством данного метода контроля является достаточно простое получение контрольных кодов без значительных затрат времени.

Результат суммирования 13 преобразуется в блоке подстановки 14.

Полученный вектор корректируется вторым блоком исправления ошибки 15 при помощи проверочных разрядов из дополнительного накопителя 16 и поступает на вход регистра сдвига 17, где циклически сдвигается на одиннадцать шагов в сторону старших разрядов (согласно алгоритму). Контроль циклического сдвига осуществляется вторым блоком контроля 18.

Введем следующие обозначения. Пусть значение на шинах 19 до сдвига - D и после циклического сдвига 20 на одиннадцать в сторону старших разрядов - $\overset{\sigma}{D}$. Соответствующим образом обозначим и контрольные коды: r_D и r_D^{σ}. Тогда

$$r_D \equiv \sum_{i=1}^{32/s} d_i \pmod p, \quad r_D^{\sigma} \equiv \sum_{i=1}^{32/s} d_i^{\sigma} \pmod p;$$

$r_D^{'\sigma}$ вычисляется за одиннадцать тактов выполнения присвоений:

$$\begin{cases} r_D^{'\sigma} \equiv \overset{\sigma}{r}_D + d_{k_s} \bmod(2^s - 1), \\ r_D^{\sigma} = r'_D, \end{cases}$$

где первое значение r_D^{σ} - сдвинутый контрольный код r_D, d_{k_s} - старший разряд контрольного кода r_D. Второй блок контроля 18 проверяет правильность выполнения циклического сдвига путем сравнения $r_D^{'\sigma}$ и r_D^{σ}. При несовпадении контрольных кодов выдается сигнал 21 об ошибке. Результат сдвига 20 суммируется по модулю два в сумматоре 22 с заполнением 23 второго накопителя 24. Третий блок контроля 25 сумматора 22 с поступающими на него слагаемыми 20, 23 и результатом суммирования 26, обозначенными как E, F и G ($G = E \oplus F$) соответственно, сравнивает величины r_G (контрольный код G) и $r_\oplus$, вычисляемые следующим образом:

$$r_G \equiv \sum_{i=1}^{32/s} g_i \pmod p, \text{ a}$$

$$r_\oplus \equiv r_{E+F} + \overset{\sigma}{r}_{E \wedge F} \pmod p;$$

здесь r_{E+F} - контрольный код суммы E и F, $\overset{\sigma}{r}_{E \wedge F}$ - инверсия контрольного кода логического произведения E и F со сдвигом кода влево на один разряд. При несовпадении контрольных кодов r_G и $r_\oplus$ выдается сигнал об ошибке 27.

Слово из сумматора 22 записывается в первый 6 или во второй 24 накопитель (определяется алгоритмом функционирования устройства [2]), после чего заполнение накопителей 6 и 24 может перезаписываться между собой или в 32-разрядные третий 28 и четвертый 29 накопители соответственно в зависимости от режима работы. Заполнение 30 третьего накопителя 28 суммируется по модулю 2^{32} в сумматоре 31с константой 32 пятого накопителя 33. Результат записывается в третий накопитель 28 и по выходам 34 подается в четвертый блок контроля 35. Блок 35 функционирует аналогично блоку контроля 11 и в случае некорректного выполнения суммирования выдается сигнал об ошибке 36. Заполнение 37 четвертого накопителя 29 суммируется по модулю (2^{32}-1) в сумматоре 38 с 32-разрядной константой 39 из шестого накопителя 40. Результат записывается в четвертый накопитель 29 и по выходам 41 - в пятый блок контроля суммирования 42. Принцип функционирования блока контроля 42 четвертого сумматора 38 по модулю (2^{32}-1) отличается от функционирования блока 11 вычислением значения:

$$r_C \equiv \left[r'_A + r'_B\right] \pmod p \quad \text{для } A + B \geq 2^{32} \text{ и } A + B > 2^{32}.$$

В случае некорректного выполнения операции суммирования блок контроля 42 выдает сигнал об ошибке 43.

Второй сумматор 44 по модулю два (без ограничения разрядности) в качестве слагаемых получает поразрядно заполнение 45 первого накопителя 6 и 46 блока открытого (в случае шифрования) или закрытого (при дешифровании) текста из источника данных 47. Результат суммирования 48 проверяется на корректность шестым блоком контроля 49, который функционирует так же, как и блок контроля 25, и выдает сигнал об ошибке 50 при несовпадении контрольных кодов. Результат суммирования по выходу 48 поразрядно поступает в потребитель данных 51 либо во второй накопитель 24 (в зависимости от режима). Управляющие шины записи/чтения в схеме не показаны.

Первый блок исправления ошибок 5 может быть построен по схеме, показанной на фиг. 2 (блок 15 строиться аналогично). Структурная схема блока 5 состоит из блока вычисления синдрома 52, на который поступают тридцать два информационных (по входам

3) и r проверочных 4 разрядов, где по закону, определяемому типом кода, формируется r-разрядное слово (синдром) 53. Основу блока вычисления синдрома 52 составляют сумматоры по модулю два [5]. Далее синдром 53 поступает на дешифратор синдрома 54, на одном из выходов 55 которого (или нескольких в зависимости от мощности кода и кратности ошибки) устанавливается сигнал лог. "1", соответствующий разряду (разрядам) информационного слова, где произошла ошибка. В блоке коррекции 56 по данному сигналу происходит исправление ошибки. Исправленное слово поступает на выходы 7 устройства.

Пример.

Пусть контрольные разряды в дополнительных накопителях формируются на основе линейного итеративного кода (по основанию два) (5,4,9,8) [5]. Рассмотрим процесс коррекции одиночной ошибки в 32-разрядном блоке: 11001010101111110001011001111111. Тогда, согласно правилу формирования контрольных разрядов итеративного кода:

1	1	0	0	1	0	1	0	**0**
1	0	1	1	1	1	1	1	**1**
0	0	0	1	0	1	1	0	**1**
0	1	1	1	1	1	1	1	**1**
0	**0**	**0**	**1**	**1**	**1**	**0**	**0**	

формируется 12 проверочных разрядов 011100011100 и записывается в дополнительный накопитель. Пусть при считывании произошла ошибка в 1-ом информационном разряде (подчеркнут сверху):

$\overline{0}$ 10010101011111110001011001111111.

Блок вычисления синдрома, функционирующий на основании проверочной матрицы H, имеющей для выбранного кода, например, следующий вид:

$$H_{(44,32)} = \begin{bmatrix} H_r \\ H_C \; I \end{bmatrix} = \begin{bmatrix}
11111111000000000000000000000000 & 1000000000000 \\
00000000111111110000000000000000 & 0100000000000 \\
00000000000000001111111100000000 & 0010000000000 \\
00000000000000000000000011111111 & 0001000000000 \\
10000000100000001000000010000000 & 0000100000000 \\
01000000010000000100000001000000 & 0000010000000 \\
00100000001000000010000000100000 & 0000001000000 \\
00010000000100000001000000010000 & 0000000100000 \\
00001000000010000000100000001000 & 0000000010000 \\
00000100000001000000010000000100 & 0000000001000 \\
00000010000000100000001000000010 & 0000000000100 \\
00000001000000010000000100000001 & 0000000000010
\end{bmatrix}$$

вычисляет 12 разрядов синдрома:

$S_{r1} = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 1;$

$S_{r2} = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0;$

$S_{r3} = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 0;$

$S_{r4} = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0;$

$S_{c1} = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 1;$

$S_{c2} = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0;$

$S_{c3} = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0;$

$S_{c4} = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0;$

$S_{c5} = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0;$

$S_{c6} = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0;$

$S_{c7} = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 0;$

$S_{c8} = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0.$

Полученный синдром 100010000000 поступает на дешифратор 54, который и определяет его соответствие со столбцами проверочной матрицы H. В данном примере это первый столбец. Следовательно, на выходах 55 выставляется сигнал 10000000000000000000000000000000. Блок коррекции 57 накладывает полученный сигнал на информационные разряды и исправляет ошибку:

10000000000000000000000000000000⊕01001010101111110001011001111111 = 1100101 01011111100010110011111 1.

На фиг. 3 представлен вариант схемы первого блока контроля 11 операции суммирования по модулю 2^{32}. Для вычисления контрольных кодов разряды каждого из слагаемых 7, 9 и суммы 10 разбиваются на группы по s разрядов в каждой и поочередно суммируются по модулю p. Для первого слагаемого 7 формируется 32/s групп 57, 58, 59, которые затем последовательно суммируются в сумматорах 60 по модулю p. Для второго слагаемого 9 и для суммы 10 контрольные коды вычисляются аналогично. Далее, согласно алгоритму [4], вычисленные контрольные коды слагаемых 61 и 62 суммируются в сумматоре 63 по модулю p, а результат суммирования 64 увеличивается на число α - 65 в сумматоре 66. Вычисленный из слагаемых таким образом контрольный код 67 проверяется на соответствие контрольному коду 68 суммы 10 блоком сравнения, построенным на s сумматорах по модулю два 69 и элементе ИЛИ 70 cs входами. Сигнал лог. "1" на выходе 12 свидетельствует об ошибке при суммировании. Аналогичную структуру имеет и блок контроля 35. Блок контроля 42 для сумматора 38 по модулю (2^{32}-1) отличается отсутствием сумматора 66.

Рассмотрим пример контроля сумматора по модулю 2^{32}. Пусть p = 15, m = 1, тогда $s = \log_2(p + 1) = 4$.

Предположим что, A = 11110111011100101010101010111001 и B = 00000001101101011110101010101111, тогда согласно правилу суммирования по МОДУЛЮ 2^{32} : C = A + B = 11111001001010001001010101101000.

Вычислим контрольные коды [4]:

$r'_A \equiv 1111 \oplus 0111 \oplus 0111 \oplus 0010 \oplus 0010 \oplus 1010 \oplus 1011 \oplus 1001 (\mathrm{mod} 15) \equiv 1011;$

$r'_B \equiv 0000 \oplus 0001 \oplus 1011 \oplus 0101 \oplus 1110 \oplus 1010 \oplus 1010 \oplus 1111 (\mathrm{mod} 15) \equiv 0110;$

$r'_C \equiv 1111 \oplus 1001 \oplus 0010 \oplus 1000 \oplus 1001 \oplus 0101 \oplus 0110 \oplus 1000 (\mathrm{mod} 15) \equiv 0010.$

Т.к. $A + B < 2^{32}$, то $\alpha = 0$ и $r_C \equiv r'_A + r'_B \equiv 1011 \oplus 0110 \oplus 0000 (\mathrm{mod} 15) = 0010$, что соответствует равенству: $r_C = r'_C$.

Теперь предположим, что в 29-ом разряде суммы произошла ошибка (1->0) C = 11111001001010001001010101 1 0 0000 (подчеркнуто сверху). Тогда контрольный код: $r'_C \equiv 1111 \oplus 1001 \oplus 0010 \oplus 1000 \oplus 1001 \oplus 0101 \oplus 0110 \oplus 000 \equiv 1001$. Так как $r_C \neq r'_C$ на выходе блока контроля появляется сигнал лог. "1".

Блок контроля 18 циклического сдвига на одиннадцать разрядов (фиг. 4) содержит 32/s сумматоров по модулю p 81, последовательно суммирующих группы исходного 19 и преобразованного 20 содержимого регистра 17 для формирования их контрольных кодов. Контрольный код 82 исходного 19 значения поступает в регистр циклического сдвига 83 на один разряд. После сдвига содержимое 84 регистра 83 поступает на сумматор 85 по модулю p, где суммируется со старшим разрядом контрольного кода до сдвига, результат суммирования 86 записывается в регистр циклического сдвига 83. Цикл повторяется одиннадцать раз, после чего счетчик 87 подает управляющий сигнал 88, который инициирует запись результата суммы 86 в накопитель 89. Блок сравнения контрольных кодов 90 и 91 построен так же, как в блоке контроля 11 на s сумматорах по модулю два 92 и элементе ИЛИ 93, лог. "1" на выходе 21 которого свидетельствует об ошибке.

Блок контроля 25 сумматора по модулю два 22 может быть построен по схеме, как показано на фиг. 5. Блок 25 содержит по s последовательных сумматоров 94 по модулю p для каждого их слагаемых 20, 23 и суммы 26, с помощью которых вычисляются их контрольные коды. Для вычисления контрольного кода суммы 10 посредством контрольных кодов 96 и 97 выполняется следующая последовательность действий. Параллельно с последовательным суммированием 94 вычисляется логическое произведение в блоке 98 (тридцать два двух входовых элемента И) слагаемых 20 и 23, которое затем сдвигается влево на один разряд в регистре 99. По полученному значению 100 вычисляется контрольный код 101 с помощью известной процедуры суммирования, который поступает на инвертор 102. Контрольные коды 96 и 97 соответствующих слагаемых 20 и 23 суммируются сумматором по модулю p 103, и результат суммы 104 суммируется сумматором 105 по модулю p с инверсией контрольного кода логического произведения слагаемых 20, 23 со сдвигом влево на один разряд 106. Полученный результат 107 сравнивается с контрольным кодом суммы 95 в блоке сравнения, состоящий из s сумматоров 108 по модулю два и элемента ИЛИ 109. В случае некорректного выполнения операции сумматором 22 блок контроля 25 выдает сигнал 27 об ошибке. Структура и принцип функционирования шестого блока контроля 49 для сумматора 44 аналогичны приведенным.

Таким образом, предлагаемое устройство выполняет те же функции, что и известное. Однако преимущество данного устройства состоит в увеличении отказоустойчивости аппаратной части, а следовательно - в повышении надежности функционирования и получении более корректных результатов с точки зрения реализации алгоритма. Действительно, избыточные схемы проверок позволяют нейтрализовать влияние отказов элементов памяти при чтении/записи и блоков арифметических и логических операций еще в процессе выполнения преобразований, что может быть возможно в известном устройстве [2] лишь после завершения алгоритма. Зачастую ошибки, возникающие в известном устройстве, остаются необнаруженными, а в случае обнаружения достаточно трудно локализуемы и приводят к снижению производительности в 2 и более раз, что устраняется предложенным устройством.

Источники информации:

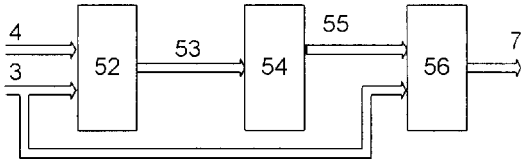
1. Патент США 5432848, МПК H 04K 1/00, H 04L 9/06, 1995.

2. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

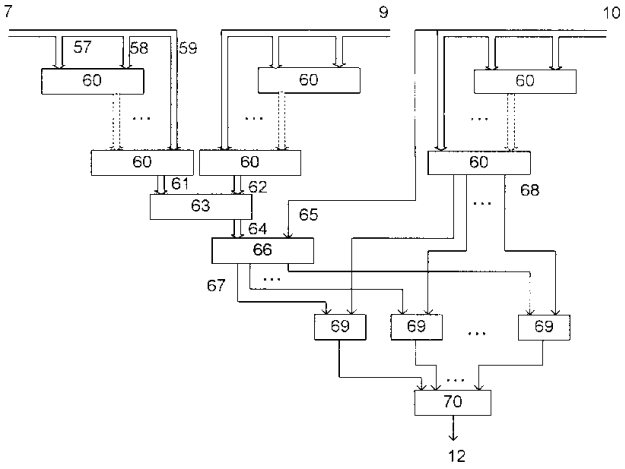
3. Блейхут Р. Теория и практика кодов, контролирующих ошибки. - М.: Мир, 1986. - С. 480.

4. Савельев А.Я. Прикладная теория цифровых автоматов. - М.: Высшая школа, 1987. - С.272.

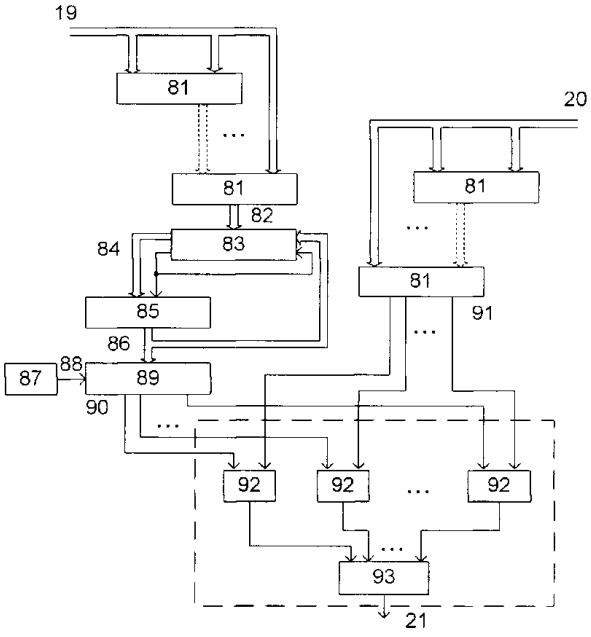
5. Урбанович П.П., Алексеев В.Ф., Верниковский Е.А. Избыточность в полупроводниковых интегральных микросхемах памяти. - Мн.: Навука и тэхніка, 1995. - С.262.



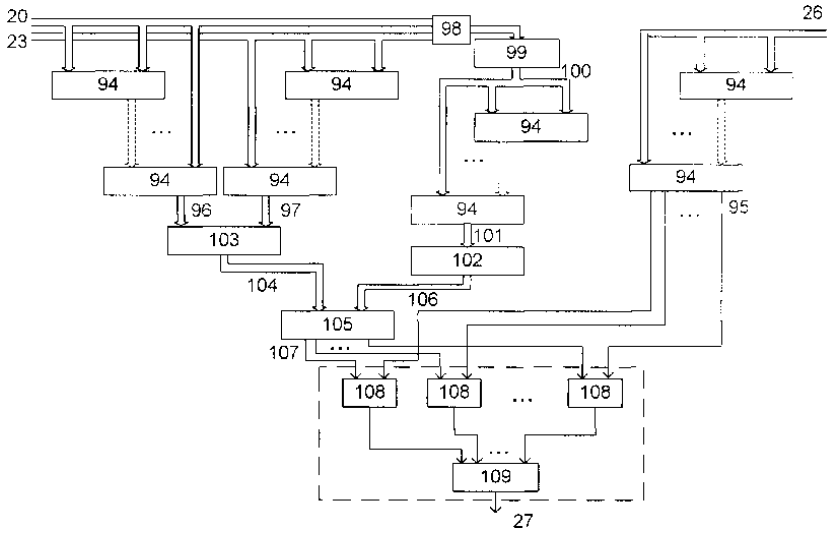
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5

Национальный центр интеллектуальной собственности
220034, г. Минск, ул. Козлова, 20.