РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 607 613**(13) **C2**

(51) МПК
H04L 9/06 (2006.01)
G09C 1/04 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2015121014, 03.06.2015**

(24) Дата начала отсчета срока действия патента:
03.06.2015

Дата регистрации:
29.12.2016

Приоритет(ы):
(22) Дата подачи заявки: **03.06.2015**

(43) Дата публикации заявки: **20.12.2016** Бюл. № **35**

(45) Опубликовано: **10.01.2017** Бюл. № **1**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Иванов Александр Геннадьевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2331937 C2, 20.08.2008. RU 2502201 C2, 20.12.2013. RU 120303 U1, 10.09.2012. US 2005058285 A1, 17.03.2005. US 5778074 A, 07.07.1998. US 6031911 A, 29.02.2000.**

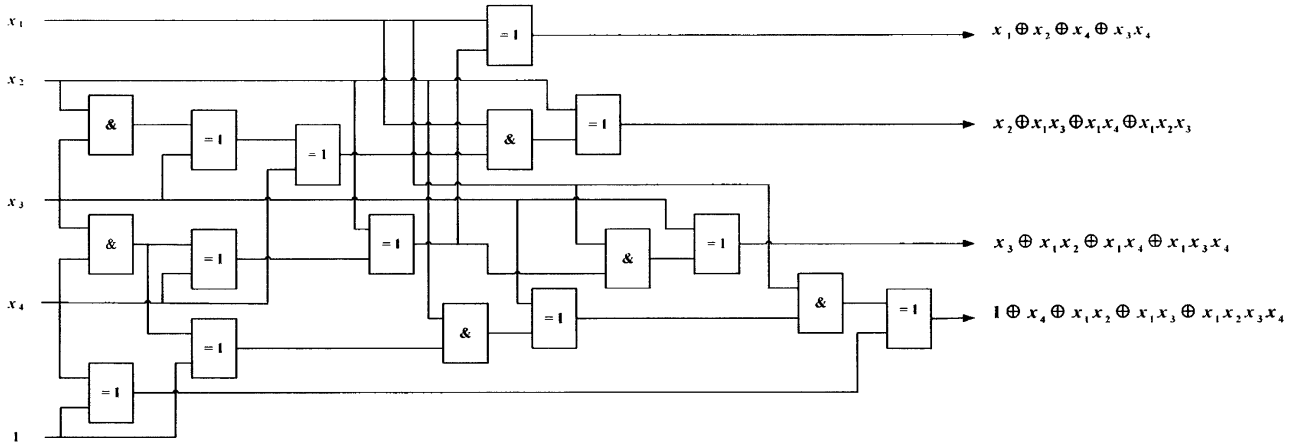
(54) Способ формирования S-блока

(57) Реферат:

Изобретение относится к области обработки информации и криптографии и, в частности, к способам формирования S-блоков замены с минимальным количеством логических элементов. Техническим результатом является уменьшение схемотехнических затрат при реализации S-блока с помощью логических элементов & и ⊕ (XOR), обеспечение возможности учета различных схемотехнических затрат на реализацию элементов & и ⊕ в процессе минимизации результирующей логической схемы S-блока. Заявляемый способ состоит из аналитического этапа, на котором выполняется последовательная декомпозиция исходных многочленов, задающих S-блок, на суммы и произведения более простых многочленов, для реализации которых требуется меньше суммарных схемотехнических затрат, этапа синтеза, на котором создаются схемы реализации этих далее не упрощаемых многочленов и на основе этих схем в порядке обратном декомпозиции строится итоговая логическая схема реализации S-блока, и третьего этапа, в ходе которого итоговая логическая схема реализуется в электронной схеме. 6 ил.

RU 2607613 C2

RU 2607613 C2



Фиг. 6

RU 2607613 C2

RU 2607613 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 607 613**(13) **C2**

(51) Int. Cl.
H04L 9/06 (2006.01)
G09C 1/04 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2015121014, 03.06.2015**

(24) Effective date for property rights:
03.06.2015

Registration date:
29.12.2016

Priority:
(22) Date of filing: **03.06.2015**

(43) Application published: **20.12.2016** Bull. № **35**

(45) Date of publication: **10.01.2017** Bull. № **1**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Ivanov Aleksandr Gennadevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2607613 C2

(54) METHOD OF FORMING S-BLOCK

(57) Abstract:

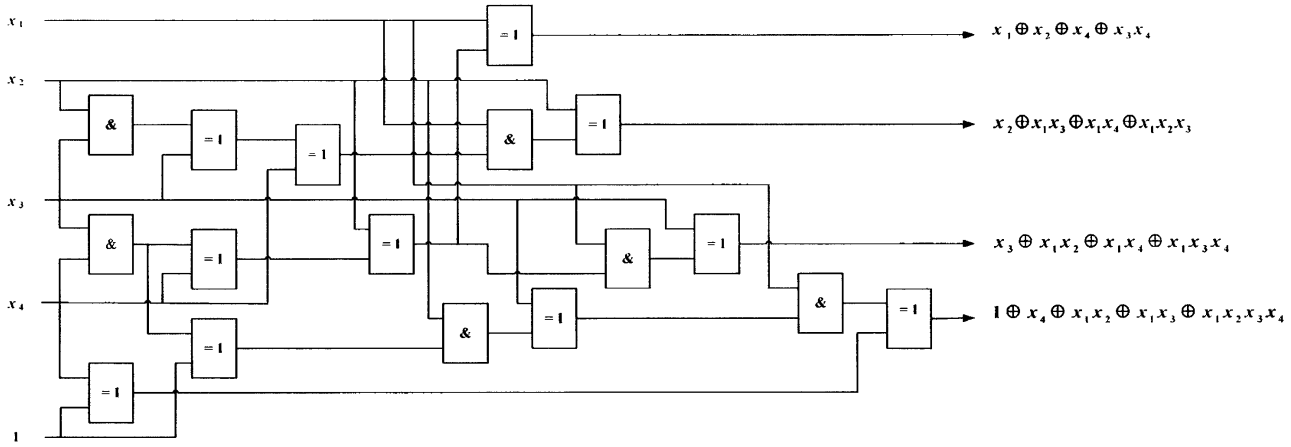
FIELD: information technology.

SUBSTANCE: invention relates to information processing and cryptography and, in particular, to methods of forming S-blocks for replacement with minimum number of logic elements. Proposed method consists of an analytical step, which comprises successive decomposition of initial polynomials, setting S-block, into a sum and product of simpler polynomials, implementation of which requires less total circuit design costs, a synthesis phase, on which are created circuits for implementing said polynomials which cannot be simplified further and on basis of said circuits in reverse order of decomposition final logic circuit for implementation S-block is built, and a third step, during which final logic circuit is implemented in electronic circuit.

EFFECT: reduced circuit design costs when implementing S-block using logic elements & and ⊕ (XOR), providing possibility of taking into account various circuit design costs on implementation of elements & and ⊕ in process of minimising resultant logic circuit of S-block.

1 cl, 6 dwg

RU 2607613 C2



Фиг. 6

RU 2607613 C2

RU 2607613 C2

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к области обработки информации и криптографии и, в частности, к способам формирования S-блоков замены с минимальным количеством логических элементов, для последующего использования в аппаратуре систем обработки данных и криптографической защиты информации.

Уровень техники

Операции замены n-битовых двоичных векторов на k-битовые двоичные вектора, реализуемые в блоках замены (S-блоках), широко используются для криптографического преобразования данных, для сжатия информации и/или защиты от помех при хранении и при передаче информации по каналам связи.

Способы формирования S-блоков с минимальным количеством логических элементов известны и зависят от состава логических элементов схемотехнической реализации.

Так, для набора логических элементов, реализующих логические операции И (&), ИЛИ (V), НЕ (¬), известны метод Квайна-МакКласки, алгоритм Блейка – Порецкого и др. [1]. Однако, известные методы предназначены для оптимизации одной булевой функции, а не набора из k булевых функций, задающих S-блок. Кроме того, эти методы неприменимы к набору логических элементов, реализующих логические операции & и XOR (⊕, исключающее ИЛИ).

Известен способ минимизации булевой функции для набора логических элементов {&, ⊕}, предложенный как составная часть процесса запоминания цифровой информации [2]. Однако, этот способ также предназначен для минимизации только одной булевой функции и не учитывает возможности совместной оптимизации нескольких булевых функций, представляющих S-блок. При этом, в данном способе оптимизируется суммарное число элементов & и ⊕ и не принимается во внимание, что схемотехнические затраты на реализацию операций & и ⊕ могут существенно отличаться друг от друга.

Наиболее близким по своей технической сущности к заявляемому является известный способ эффективной реализации S-блока, используемого в стандарте криптографической защиты информации AES [3], в котором, наряду с оптимизацией времени вычисления S-блока, решается и задача минимизации числа логических элементов {&, ⊕} при реализации данного S-блока.

Известный способ [3] выбирается в качестве прототипа.

Основным недостатком прототипа является то, что он предназначен исключительно для S-блоков частного вида, а именно, для S-блоков, задаваемых несколькими (небольшим числом) операций в конечном поле $GF(2^m)$, к которым и относиться S-блок стандарта криптографической защиты AES. Прототип непосредственно опирается на реализацию операции умножения в конечном поле $GF(2^m)$, поэтому он неприменим к произвольному S-блоку, не основанному на какой-либо алгебраической системе.

Другим недостатком (ограничением) прототипа является то, что он осуществляет минимизацию числа логических элементов {&, ⊕} для реализации S-блока в несколько тактов/шагов (для итеративной схемы реализации). При этом число итераций при вычислениях S-блока возрастает с увеличением размера m конечного поля $GF(2^m)$.

Раскрытие изобретения

Техническим результатом предлагаемого способа является

1) уменьшение схемотехнических затрат при реализации S-блока с помощью логических элементов & и ⊕,

2) возможность учета различных схемотехнических затрат на реализацию элементов & и ⊕ в процессе минимизации результирующей логической схемы S-блока.

В заявленном способе также отсутствуют ограничения на значения n и k размерности S-блока.

S-блок осуществляет замену входного двоичного вектора $(x_1, x_2, ..., x_n)$ длины n на выходной двоичный вектор $(y_1, y_2, ..., y_k)$ длины k, где $x_i, y_j \in \{0,1\}$ для $1 \le i \le n$ и $1 \le j \le k$.

S-блок однозначно задается аналитически координатными булевыми функциями $f_1, f_2, ..., f_k$ от n переменных $x_1, x_2, ..., x_n$, что можно записать в виде

$$S(x_1, x_2, ..., x_n) \equiv \begin{cases} y_1(x_1, x_2, ..., x_n) \\ y_2(x_1, x_2, ..., x_n) \\ \quad ... \\ y_k(x_1, x_2, ..., x_n) \end{cases}$$

В предлагаемом способе рассматривается представление координатных булевых функций S-блока через приведенные многочлены Жегалкина: каждая функция f_j для $1 \le j \le k$ аналитически задана в виде

$$f_j(x_1, x_2, ..., x_n) \equiv p_j[X] = \bigoplus_{i=1}^{t_j} m_{j,i}$$

где $X \equiv \{x_1, x_2, ..., x_n\}$ – множество переменных многочленов p_j, $1 \le j \le k$;

$m_{j,i} \equiv \underset{z \in X_{j,i}}{\&} z$ - моном многочлена $p_j[X]$, который является произведением всех переменных z из подмножества $X_{j,i} = X(m_{j,i}) \subset X$ множества X, причем $X(m_{j,i}) \neq X(m_{j,s})$ при $i \neq s$ для приведенного многочлена $p_j[X]$.

$t_j = \left\| T(p_j[X]) \right\|$ - мощность (число элементов) множества $T(p_j[X])$ - мономов $m_{j,i}$, составляющих многочлен $p_j[X]$.

Существуют и другие, отличные от приведенного многочлена Жегалкина, формы представления булевых функций, например: таблица истинности, дизъюнктивная нормальная форма (ДНФ), конъюнктивная нормальная форма (КНФ). Процессы перехода от одного вида представления к другому хорошо известны. Например, в известном способе [4] приведена последовательность перехода от таблицы истинности к представлению булевой функции через приведенный многочлен Жегалкина. В заявляемом способе не имеет значения, каким образом формируется исходное аналитическое представление S-блока через приведенные многочлены Жегалкина:

$$S(x_1, x_2, ..., x_n) \equiv \begin{cases} y_1 = p_1[x_1, x_2, ..., x_n] \\ y_2 = p_2[x_1, x_2, ..., x_n] \\ \quad ... \\ y_k = p_k[x_1, x_2, ..., x_n] \end{cases}$$

Для построения оптимальной логической схемы реализации S-блока через операции & и $\oplus$ в заявляемом способе используются предварительные аналитические вычисления, использующие операции над множествами. Для получаемого в результате схемотехнического решения не имеет значения, какие используются представления

множеств (характеристический вектор, список элементов, в том числе упорядоченный список, и т.д.) и с помощью каких преобразований осуществляются операции над множествами.

Прямой способ реализации S-блока (1), заданного множеством приведенных многочленов Жегалкина $P = \{p_1[X], p_2[X], ..., p_k[X]\}$, состоит из двух этапов:

1. Составляют множество L мономов, входящих в состав многочленов из множества P, по формуле

$$L = \bigcup_{p[X] \in P} T(p[X]),$$

где $T(p[X])$ – множество мономов, составляющих многочлен $p[X]$.

Каждый моном $m \in L$ реализуют через конъюнкцию & всех элементов множества $X(m)$ - подмножества множества X входных переменных S-блока, где $X(m)$ – множество переменных монома m.

2. Каждый многочлен $p[X]$ из множества P реализуют, как сумму $\oplus$ выходов из схем реализаций мономов $T(p[X])$, полученных на предыдущем этапе.

В этом способе схема реализации монома $m \neq 1$ (свободному члену) требует $\|X(m)\| - 1$ элементов &, где $\|X(m)\|$ – мощность множества $X(m)$ – множества переменных монома m.

Аналогично, схема реализации многочлена $p[X] \in P$ требует $\|p[X])\|_{\oplus} = \|T(p[X])\| - 1$ элементов $\oplus$, где $\|T(p[X])\|$ – мощность множества $T(p[X])$ - множества мономов, составляющих многочлен $p[X]$.

Тем самым, аддитивная сложность $\|P\|_{\oplus}$ и мультипликативная сложность $\|P\|_{\&}$ реализации множества многочленов P составляют:

$$\|P\|_{\oplus} = \sum_{p[X] \in P} \|p[X]\|_{\oplus} = \sum_{p[X] \in P} (\|T(p[X])\| - 1) =$$

$$= \sum_{p[X] \in P} (\|T(p[X])\| - \|P\|,$$

$$\|P\|_{\&} = \sum_{m \in T'_P} (\|X(m)\| - 1) = \sum_{m \in T'_P} \|X(m)\| - \|T'_P\| \quad (1)$$

где $T'_P = \bigcup_{p[X] \in P} T(p[X]) \setminus 1$ – множество мономов, входящих в состав многочленов множества P, за исключением свободного члена 1.

Если схемотехнические затраты на реализацию операции & составляют $C1$ единиц, а затраты на реализацию операции $\oplus$ - $C2$ единиц, суммарные затраты $\|S\|_c$ на реализацию S-блока составят

(2)

Заявляемый способ состоит из аналитического этапа, на котором выполняется последовательная декомпозиция исходных многочленов, задающих S-блок, на суммы и произведения более простых многочленов, для реализации которых требуется меньше суммарных схемотехнических затрат, этапа синтеза, на котором создаются схемы реализации этих, далее не упрощаемых, многочленов и на основе этих схем в порядке

обратном декомпозиции строится итоговая логическая схема реализации S-блока, и третьего этапа, в ходе которого итоговая логическая схема реализуется в электронной схеме.

На каждом шаге декомпозицию множества многочленов осуществляют одним из двух следующих преобразований.

Преобразование 1 определяется парой многочленов $u[X] \neq v[X]$ из рассматриваемого множества многочленов E, и состоит из следующих вычислений:

• выделяют множество M общих мономов многочленов $u[X]$ и $v[X]$

$$M = T(u[X]) \cap T(v[X])$$

• вычисляют мощность $\|M\|$;

• если $\|M\| \leq 1$ (это равносильно тому, что многочлены $u[X]$ и $v[X]$ или не имеют общих мономов или имеют ровно один такой моном), то данное преобразование прекращают, так как оно не дает снижения схемотехнических затрат;

• если $\|M\| \geq 2$, то из мономов множества M составляют многочлен $h[X]$, а из мономов множеств $T(u[X]) \backslash M$ и $T(v[X]) \backslash M$ – многочлены $g[X]$ и $q[X]$ соответственно;

• вычисляют, в качестве декомпозиции многочленов $u[X]$ и $v[X]$, соотношения

$$u[X] = h[X] \oplus g[X],$$

$$v[X] = h[X] \oplus q[X],$$

в которых слагаемые, равные 0, обозначают, что операцию $\oplus$ реализовывать не требуется;

• формируют результирующее множество многочленов

$$R = (E \backslash \{u[X], v[X]\}) \cup \{h[X], g[X], q[X]\}$$

• вычисляют эффективность преобразования (величину уменьшения схемотехнических затрат) в виде

$$d = (\|M\| - 1)C2$$

Преобразование 2 определяется параметром z – переменной из множества $X = \{x_1, x_2, ..., x_n\}$ и состоит из следующих вычислений для каждого многочлена $p[X]$ из рассматриваемого множества многочленов E:

• для рассматриваемого многочлена $p[X]$ формируют множество M мономов, содержащих переменную z

$$M = \{m \in T(p[X]) \mid z \in X(m)\}$$

• вычисляют мощность $\|M\|$ множества M;

• если $\|M\| \leq 1$ (это равносильно тому, что многочлен $p[X]$ или не зависит от переменной z, или имеет ровно один моном, содержащий переменную z), то $p[X]$ не подвергают декомпозиции, в неизменном виде включают в результирующее (формируемое) множество многочленов R, а сложность его декомпозиции $D_z(p[X])$ полагают равной нулю;

• если $\|M\| \geq 2$, то осуществляют декомпозицию многочлена $p[X]$, выполняя

следующие действия:

○ из мономов множества M исключают переменную z и формируют многочлен $g[X]$

$$g[X]=\bigoplus_{m\in M,\ x\in X(m),\ x\neq z}\ \&\ x,$$

причем моном m, состоящий из единственной переменной z, переходит в свободный член 1 многочлена $g[X]$;

○ из мономов множества $T(p[X])\setminus M$ (мономов многочлена $p[X]$, не содержащих переменную z) формируют многочлен $h[X]$

$$h[X]=\bigoplus_{m\in T(p[X])\setminus M} m$$

○ вычисляют многочлен

$$q[X]=g[X]\oplus h[X]$$

○ приводят подобные члены в $q[X]$ (исключают повторяющиеся мономы)

$$T(q[X])=(T(g[X])\cup T(h[X]))\setminus(T(g[X])\cap T(h[X]))$$

○ если число мономов многочлена $q[X]$ меньше числа мономов многочлена $h[X]$ на 2 и более, что равносильно условию на мощности множеств

$$\|M\|+1<2\|T(p[X])\cap T(g[X]\|,$$

то в качестве декомпозиции многочлена $p[X]$ используют выражение

$$p[X]=(z\oplus 1)\,\&\,g[X]\oplus q[X],$$

▪ включают в результирующее множество многочленов R многочлены $g[X]$, $q[X]$ и $z\oplus 1$;

▪ принимают значение сложности декомпозиции $D_Z(p[X])$ многочлена $p[X]$ равной $C1$, если $q[X]\neq 0$, то увеличивают значение $D_Z(p[X])$ на $C2$

$$D_Z(p[X])=C1+C2;$$

○ если же

$$\|M\|+1\geq 2\|T(p[X])\cap T(g[X]\|,$$

то в качестве декомпозиции многочлена $p[X]$ используют выражение

$$p[X]=z\,\&\,g[X]\oplus h[X],$$

▪ включают в результирующее (формируемое) множество многочленов R многочлены $g[X]$ и $h[X]$;

▪ принимают значение сложности декомпозиции $D_Z(p[X])$ многочлена $p[X]$ равной $C1$, если $h[X]\neq 0$, то увеличивают значение $D_Z(p[X])$ на $C2$

$$D_Z(p[X])=C1+C2$$

Эффективность преобразования 2 (величину уменьшения схемотехнических затрат) для рассматриваемого множества многочленов E и переменной z рассчитывают по

формуле:

$$d = \|E\|_C - \|R\|_C - \sum_{p[X] \in E} D_Z(p[X]),$$

где значения $\|E\|_C$ и $\|R\|_C$ вычисляются по формулам (1) и (2).

Для минимизации схемотехнических затрат на реализацию мономов из множества T проводят разложение мономов T в произведение мономов с меньшим числом переменных, используя следующее преобразование.

Преобразование 3 состоит из следующих вычислений и операций:

• осуществляют во множестве мономов T поиск для обнаружения пары мономов (u, v), причем $u \neq v$, с наибольшим числом общих переменных, путем последовательного перебора, то есть находят пару мономов с максимальным значением

$$s = \|X(u) \cap X(v)\|$$

где $X(m)$ – множество переменных в мономе m

• если $s = 0$ (это равносильно тому, что у мономов рассматриваемого множества T нет общих переменных), то завершают преобразование

• если $s \geq 1$, то выполняют следующие действия:

• составляют мономы a, b, w из переменных $X(u) \setminus X(v)$, $X(v) \setminus X(u)$ и $X(u) \cap X(v)$, соответственно; в качестве разложения мономов u и v используют выражения

$$u = w \,\&\, a,$$

$$v = w \,\&\, b,$$

в которых сомножители, равные 1, обозначают, что операцию & реализовывать не требуется;

• формируют результирующее множество мономов R, удаляя из множества T мономы u и v и добавляя мономы a, b, w, т.е. вычисляют

$$R = (T \setminus \{u, v\}) \cup \{a, b, w\}$$

Предлагаемый способ минимизации схемотехнических затрат на реализацию S-блока, заданного многочленами Жегалкина $p_1[X]), p_2[X]), ..., p_k[X]$, состоит из 7 этапов.

1. Исходное множество многочленов

$$P[1] = \{p_1[X]), p_2[X]), ..., p_k[X]\}$$

последовательно преобразовывают с использованием преобразований 1 и 2:

$$P[1] \to P[2] \to ... \to P[r]$$

где каждый переход имеет эффективность больше нуля (т.е. приводит к снижению оценки суммарных схемотехнических затрат и осуществляется к результирующему множеству многочленов, формируемому в ходе этих преобразований). Результирующее множество $P[r]$ характеризуется тем, что никакое из преобразований 1 и 2 не приводит к дальнейшему снижению оценки затрат ни при каких параметрах.

2. Затем, по результирующему множеству $P[r]$ формируют множество мономов $L[1]$, входящих в многочлены множества $P[r]$ и добавляют к нему множество входных переменных $\{x_1, x_2, ..., x_n\}$

$$L[1] = \{x_1, x_2, ..., x_n\} \cup \bigcup_{p[X] \in P[r]} T(p[X]),$$

где $T(p[X])$ – множество мономов, составляющих многочлен $p[X]$.

3. Затем осуществляют разложение мономов множества $L[1]$, многократно используя преобразование 3 до тех пор, пока преобразование станет неприменимым, и получают последовательность множеств

$$L[1] \to L[2] \to ... \to L[t]$$

Поскольку переменные $x_1, x_2, ..., x_n$ не удаляют в процессе преобразования множества мономов, то невозможность применения преобразования 3 к множеству $L[t]$ равносильно тому, что $L[t]$ состоит только из элементов $x_1, x_2, ..., x_n$, которые и являются входами S-блока.

4. Построение логической схемы S-блока начинают проходом по цепочке $L[1] \to L[2] \to ... \to L[t]$ в обратном порядке, соединяя операцией & выходы схем мономов, участвующих в разложении, схемы которых, в свою очередь, были составлены на предыдущих шагах.

5. После построения логических схем мономов из множества $L[1]$ формируют логические схемы многочленов из множества $P[r]$, соединяя операцией $\oplus$ выходы схем мономов $L[1]$, составляющих этот многочлен.

6. Далее осуществляют проход по цепочке $P[1] \to P[2] \to ... \to P[r]$ в обратном порядке, и составляют логические схемы очередных многочленов, соединяя операциями & и $\oplus$ выходы схем предшествующих многочленов в соответствии с формулами декомпозиции.

7. Выходы логических схем многочленов множества $P[1]$ используют в качестве выходов логической схемы S-блока.

В описанном способе минимизации схемотехнических затрат не специфицированы параметры, которые используются для переходов $P[i] \to P[i+1]$ и $L[j] \to L[j+1]$. Однако, от выбора этих параметров зависит получаемый эффект снижения схемотехнических затрат. Эффективный метод выбора наилучшего набора параметров, обеспечивающих наименьшее из возможных значений суммарных схемотехнических затрат, неизвестен, а полный перебор всех наборов требует экспоненциальных вычислительных затрат от величины 2^n, что делает перебор неприемлемым для практически интересных значений n.

В заявляемом способе предлагается выбирать параметры перехода так, чтобы на каждом переходе $P[i] \to P[i+1]$ и $L[j] \to L[j+1]$ уменьшение оценки схемотехнических затрат было максимально возможным, а среди параметров, обеспечивающих такое снижение оценки, использовать параметры, запись (представление) которых предшествует записям остальным в лексикографическом порядке.

Необходимо отметить, что построение (формирование) логической схемы, реализующей соответствующую булеву функцию, является известным процессом (этот процесс описан, например, в [1, 4]).

Реализация электронной схемы на основе полученной логической схемы также является известным процессом и может быть выполнена как на дискретных элементах,

так и с использованием интегральных микросхем, в том числе программируемых логических интегральных микросхем (ПЛИС), по выбору разработчика.

Краткое описание чертежей

На фиг. 1 показана начальная логическая схема для примера реализации способа.

На фиг. 2 показана промежуточная логическая схема для примера реализации способа.

На фиг. 3 показана промежуточная логическая схема для примера реализации способа.

На фиг. 4 показана промежуточная логическая схема для примера реализации способа.

На фиг. 5 показана промежуточная логическая схема для примера реализации способа.

На фиг. 6 показана финальная логическая схема для примера реализации способа.

Осуществление изобретения

Рассмотрим пример реализации предложенного способа для S-блока, имеющий $n=$ 4 входов и $k=4$ выходов и заданного следующими многочленами Жегалкина от четырех переменных x_1, x_2, x_3, x_4

$$S(x_1,x_2,x_3,x_4) \equiv \begin{cases} y_1 = x_1 \oplus x_2 \oplus x_4 \oplus x_3x_4 \\ y_2 = x_3 \oplus x_1x_2 \oplus x_1x_4 \oplus x_1x_3x_4 \\ y_3 = x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_2x_3 \\ y_4 = 1 \oplus x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_2x_3x_4 \end{cases}$$

Прямой способ реализации этого S-блока требует 11 операций & для формирования мономов x_1x_2, x_1x_3, x_3x_4, $x_1x_2x_3$, $x_1x_3x_4$, $x_1x_2x_3x_4$ и 13 операций $\oplus$ для составления из них многочленов.

Рассмотрим применение предлагаемого способа в условиях, когда схемотехнические затраты на реализацию операций & и $\oplus$ совпадают, т.е. $C1 = C2 = 1$.

Число общих мономов у любой пары многочленов не превышает 1, поэтому способ из прототипа не дает выигрыша по количеству операций, т.е. не приводит к снижению схемотехнических затрат.

В предлагаемом способе этому S-блоку соответствуют исходные значения:

$r=0$

$X_1 = \{x_1, x_2, x_3, x_4\}$

$$P_1 = \left\{ \begin{array}{l} x_1 \oplus x_2 \oplus x_4 \oplus x_3x_4 \\ x_3 \oplus x_1x_2 \oplus x_1x_4 \oplus x_1x_3x_4 \\ x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_2x_3 \\ 1 \oplus x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_2x_3x_4 \end{array} \right\}$$

У любых двух многочленов из множества P_1 совпадает не более одного монома, что при $r=1$ на этапе А1 (согласно обозначению в формуле изобретения), соответствует тому, что $fm \le 1$. Поэтому на этапе А1 после присвоения значения $d=1$ выполняют переход на этап А2, где вычисляют значение dm, характеризующую сложность прямой реализации множества многочленов P_r

$dm = 13*C2 + 11*C1 = 13 + 11 = 24$

и величину имеющегося снижения сложности

$d=0$

С этапа А3 до этапа А4 по очереди перебирают переменные x_i из множества X_r. Для выбранного значения x_i каждый многочлен $u[X]$ из P_r представляют в одном из 2-х вариантов:

$$u[X]=x_i u1[X\setminus x_i]\oplus u2[X\setminus x_i]$$

или

$$u[X]=(x_i\oplus 1)u1[X\setminus x_i]\oplus u3[X\setminus x_i],$$

в записи которого меньше операций $\oplus$. Для полученного разложения многочленов P_r по переменной x_i подсчитывают значение df, характеризующую снижение сложности прямой реализации множества многочленов P_r за счет перехода к прямой реализации выделенных компонент разложения с последующим составлением исходных многочленов по выбранным формулам.

Для рассматриваемого множества многочленов P_1 перебор переменных x_i дает следующие результаты разложения многочленов и соответствующие им оценки сложности использования такого разложения:

Для $i=1$:

$$P_1^1=\left\{\begin{array}{l} x_1\oplus x_2\oplus x_4\oplus x_3x_4\\ x_1(x_2\oplus x_4\oplus x_3x_4)\oplus x_3\\ x_1(x_3\oplus x_4\oplus x_2x_3)\oplus x_2\\ x_1(x_2\oplus x_3\oplus x_2x_3x_4)\oplus x_4\oplus 1\end{array}\right\}$$

сложность

$$dm=13*C2+7*C1=13+7=20$$

$$df=dm-20=24-20=4$$

Для $i=2$:

$$P_1^2=\left\{\begin{array}{l} x_1\oplus x_2\oplus x_4\oplus x_3x_4\\ x_3\oplus x_1x_2\oplus x_1x_4\oplus x_1x_3x_4\\ x_2(x_1x_3\oplus 1)\oplus x_1x_3\oplus x_1x_4\\ x_2(x_1\oplus x_1x_3x_4)\oplus x_1x_3\oplus x_4\oplus 1\end{array}\right\}$$

сложность

$$dm=13*C2+8*C1=13+8=21$$

$$df=dm-21=24-21=3$$

Для $i=3$:

$$P_1^3=\left\{\begin{array}{l} x_1\oplus x_2\oplus x_4\oplus x_3x_4\\ x_3(x_1x_4\oplus 1)\oplus x_1x_2\oplus x_1x_4\\ x_3(x_1\oplus x_1x_2)\oplus x_2\oplus x_1x_4\\ x_3(x_1\oplus x_1x_2x_4)\oplus x_4\oplus x_1x_2\oplus 1\end{array}\right\}$$

сложность

$$dm = 13*C2 + 8*C1 = 13 + 8 = 21$$

$$df = dm - 21 = 24 - 21 = 3$$

Для $i = 4$:

$$P_1^4 = \left\{ \begin{array}{l} x_4(x_3 \oplus 1) \oplus x_1 \oplus x_2 \\ x_4(x_1 \oplus x_1x_3) \oplus x_3 \oplus x_1x_2 \\ x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_2x_3 \\ x_4(x_1x_2x_3 \oplus 1) \oplus x_1x_2 \oplus x_1x_3 \oplus 1 \end{array} \right\}$$

сложность

$$dm = 13*C2 + 8*C1 = 13 + 8 = 21$$

$$df = dm - 21 = 24 - 21 = 3$$

Наибольшее снижение сложности (значение df) имеет место при $i = 1$. Поэтому на этапе А4 при переходе на этап А1 при $r = 2$:

$$X_2 = \{x_2, x_3, x_4\}$$

$$P_2 = \left\{ \begin{array}{l} x_2, x_3, x_4 \oplus 1, \\ x_1 \oplus x_2 \oplus x_4 \oplus x_3x_4, \\ x_2 \oplus x_3 \oplus x_2x_3x_4, \\ x_2 \oplus x_4 \oplus x_3x_4, \\ x_3 \oplus x_4 \oplus x_2x_3 \end{array} \right\}$$

Для множества многочленов P_2 максимальная общая часть двух многочленов состоит из 3-х мономов x_2, x_4, x_3x_4. Поэтому при переходе на этап А2 вычисляемые параметры имеют значения:

$$d = 3$$

$$w_2 = x_2 \oplus x_4 \oplus x_3x_4$$

$$P_3 = \left\{ \begin{array}{l} x_1, x_2, x_3, x_4 \oplus 1, \\ x_2 \oplus x_3 \oplus x_2x_3x_4, \\ x_2 \oplus x_4 \oplus x_3x_4, \\ x_3 \oplus x_4 \oplus x_2x_3 \end{array} \right\}$$

На этапе А2 вычисляют сложность прямой реализации множества многочленов P_2

$$dm = 10*C2 + 4*C1 = 10 + 4 = 14$$

и снижение сложности за счет выделения общего слагаемого $w_2 = x_2 \oplus x_4 \oplus x_3x_4$

$$d = 2*C2 = 2$$

На этапах с А3 по А4 разложение многочленов множества P_2 по переменным x_2, x_3, x_4 из множества X_2 дает следующие оценки сложности использования данного разложения по сравнению с сложностью прямой реализации множества P_2

Для $i=2$:

$$P_2^2=\left\{\begin{array}{l} x_2, x_3, x_4 \oplus 1, \\ x_1 \oplus x_2 \oplus x_4 \oplus x_3 x_4, \\ x_2(x_3 x_4 \oplus 1) \oplus x_3, \\ x_2 \oplus x_4 \oplus x_3 x_4, \\ x_3 \oplus x_4 \oplus x_2 x_3 \end{array}\right\}$$

сложность

$$dm = 10*C2 + 3*C1 = 10 + 3 = 13$$

$$df = dm - 13 = 14 - 13 = 1$$

Для $i=3$:

$$P_2^3=\left\{\begin{array}{l} x_2, x_3, x_4 \oplus 1, \\ x_1 \oplus x_2 \oplus x_4 \oplus x_3 x_4, \\ x_3(x_2 x_4 \oplus 1) \oplus x_2, \\ x_2 \oplus x_4 \oplus x_3 x_4, \\ x_3(x_2 \oplus 1) \oplus x_4 \end{array}\right\}$$

сложность

$$dm = 10*C2 + 4*C1 = 10 + 4 = 14$$

$$df = dm - 14 = 14 - 14 = 0$$

Для $i=4$:

$$P_2^4=\left\{\begin{array}{l} x_2, x_3, x_4 \oplus 1, \\ x_4(x_3 \oplus 1) \oplus x_1 \oplus x_2, \\ x_2 \oplus x_3 \oplus x_2 x_3 x_4, \\ x_4(x_3 \oplus 1) \oplus x_2, \\ x_3 \oplus x_4 \oplus x_2 x_3 \end{array}\right\}$$

сложность

$$dm = 10*C2 + 5*C1 = 10 + 5 = 15$$

$$df = dm - 15 = 14 - 15 = -1$$

Наибольшее снижение сложности (значение $df = 1$) имеет место при $i=2$, что меньше снижения сложности (значение $d=2$) при выделение многочлена w_2.

Поэтому на этапе А4 при переходе на этап А1 при $r=3$ вычисляемые параметры имеют следующие значения:

$$X_3 = \{x_2, x_3, x_4\}$$

$$w_2 = x_2 \oplus x_4 \oplus x_3 x_4$$

$$P_3 = \left\{ \begin{array}{l} x_1, x_2, x_3, x_4 \oplus 1, \\ x_2 \oplus x_3 \oplus x_2 x_3 x_4, \\ x_2 \oplus x_4 \oplus x_3 x_4, \\ x_3 \oplus x_4 \oplus x_2 x_3 \end{array} \right\}$$

Число общих мономов у любой пары многочленов из множества P_3 не превышает 1, поэтому при переходе на этап А3 при $r = 3$ вычисляемые параметры имеют следующие значения

$d = 0$

и сложность прямой реализации P_3

$dm = 7*C2 + 4*C1 = 7 + 4 = 11$

На этапах с А3 по А4 разложение многочленов множества P_3 по переменным x_2, x_3, x_4 из множества X_3 дает следующие оценки сложности использования данного разложения по сравнению со сложностью прямой реализации множества P_3.

Для $i = 2$:

$$P_3^2 = \left\{ \begin{array}{l} x_1, x_2, x_3, x_4 \oplus 1, \\ x_2 (x_3 x_4 \oplus 1) \oplus x_3, \\ x_2 \oplus x_4 \oplus x_3 x_4, \\ x_3 \oplus x_4 \oplus x_2 x_3 \end{array} \right\}$$

сложность

$dm = 7*C2 + 3*C1 = 7 + 3 = 10$

$df = 1$

Для $i = 3$:

$$P_3^3 = \left\{ \begin{array}{l} x_1, x_2, x_3, x_4 \oplus 1, \\ x_3 (x_2 x_4 \oplus 1) \oplus x_2, \\ x_2 \oplus x_4 \oplus x_3 x_4, \\ x_3 (x_2 \oplus 1) \oplus x_4 \end{array} \right\}$$

сложность

$dm = 7*C2 + 4*C1 = 7 + 4 = 11$

$df = 0$

Для $i = 4$:

$$P_3^4 = \left\{ \begin{array}{l} x_1, x_2, x_3, x_4 \oplus 1, \\ x_2 \oplus x_3 \oplus x_2 x_3 x_4, \\ x_4 (x_3 \oplus 1) \oplus x_2, \\ x_3 \oplus x_4 \oplus x_2 x_3 \end{array} \right\}$$

сложность

$dm = 7*C2 + 4*C1 = 7 + 4 = 11$

$df = 0$

Наибольшее снижение сложности имеет место при $i = 2$. Поэтому на этапе А4 при переходе на этап А1 при $r = 4$ вычисляемые параметры имеют следующие значения:

$X_4 = \{x_3, x_4\}$

$$P_4 = \begin{Bmatrix} x_1, x_2, x_3, x_4 \oplus 1, \\ x_3 x_4 \oplus 1, \\ x_2 \oplus x_4 \oplus x_3 x_4, \\ x_3 \oplus x_4 \oplus x_2 x_3 \end{Bmatrix}$$

Число общих мономов у любой пары многочленов из множества P_4 не превышает 1, поэтому переходят на этап А3 - к анализу разложений многочленов множества P_3 по переменным x_3, x_4 из множества X_4.

Никакой из двух вариантов разложения не приводит к снижению оценки сложности, поэтому формируют множество мономов

$L_1 = \{1, x_1, x_2, x_3, x_4, x_2 x_3, x_3 x_4\}$

и переходят к этапу А5 при $t = 1$.

На этапе А5 при $t = 1$ максимальное число общих переменных, равное 1, имеют мономы $x_2 x_3$ и $x_3 x_4$ из множества L_1. Для этих мономов вычисления дают результат: $m_1 = x_3$ и множество мономов $L_2 = \{1, x_1, x_2, x_3, x_4\}$.

В множестве мономов L_2 уже нет мономов с общими переменными, поэтому переходят на этап А6 - к синтезу схемы из элементов $\oplus$ и &.

Схема для множества L_2 проста: входы x_1, x_2, x_3, x_4 соединены с одноименными выходами x_1, x_2, x_3, x_4 и добавлен выход постоянного сигнала 1 (фиг. 1).

Переход к схеме для множества L_1 выполняют путем добавления к схеме L_2 части, осуществляющей вычисления отсутствующих в L_1 мономов $x_2 x_3$ и $x_3 x_4$ (фиг. 2).

При переходе к схеме для множества многочленов P_4 к схеме для L_1 добавляют части, которые соответствуют многочленам P_4 с двумя и более мономами, и которые осуществляют сложение выходов мономов этого многочлена в схеме L_1 для формирования входа, соответствующего данному многочлену (фиг. 3).

При переходе от схемы для множества многочленов P_4 к схеме для множества многочленов P_3 добавляют часть, реализующую многочлен $x_2 \oplus x_3 \oplus x_2 x_3 x_4$: добавляют операцию & над выходом, соответствующем многочлену $x_3 x_4 \oplus 1$, и входом переменной x_2 и соединяют операцией $\oplus$ результат данной операции & с входом

переменной x_3 (фиг. 4).

При переходе от схемы для множества многочленов P_3 к схеме для множества многочленов P_2 добавляют часть, реализующую многочлен $x_1 \oplus x_2 \oplus x_3 \oplus x_2x_3x_4$: соединяют через операцию ⊕ выход, соответствующий многочлену $x_2 \oplus x_3 \oplus x_2x_3x_4$, и вход переменной x_1 (фиг. 5).

Переход от схемы для множества многочленов P_2 к схеме для множества многочленов P_1 полностью аналогичен переходу от схемы P_4 к схеме P_3: добавляются части, являющиеся произведением (в смысле операции &) одного из выходов и одной из входящих переменных с последующим суммированием (в смысле операции ⊕) с другим выходом (фиг. 6).

В полученной финальной схеме реализации S-блока (фиг. 8) использовано 11 операций ⊕ и 6 операций &, что меньше исходных значений 13 операций ⊕ и 11 операций &.

Таким образом, предлагаемый способ уменьшает схемотехнические затраты – количество элементов, реализующих операции & и ⊕ при формировании заданного S-блока.

В случае исходного S-блока большой размерности процедуру построения логической схемы, согласно предложенному способу, целесообразно автоматизировать путем составления программы для ЭВМ, что вполне может выполнить специалист по программированию (программист) на основе знания действий способа.

Последующая схемотехническая реализация полученного S-блока может быть осуществлена известными методами, предпочтительной формой для использования в современной компьютерной технике является реализация на ПЛИС, но это необязательно. Конкретный выбор варианта схемотехнической реализации зависит от разработчика.

Источники информации, принятые во внимание при формировании заявки

1. Самофалов К.Г. и др. Прикладная теория цифровых автоматов (учебник), Киев, Вища Школа, 1987.

2. Патент РФ № 2331937, приоритет от 24.08.2006 г.

3. Патент США № 7421076, приоритет от 17.09.2003 г.

4. Спирин П.А. Спирина М.С. Дискретная математика (учебник), Издательский центр “Академия”, 2004

(57) Формула изобретения

Способ формирования *S*-блока, заключающийся в том, что

задают исходный *S*-блок, имеющий n входов и k выходов, в виде k многочленов Жегалкина от n переменных

$$p[X] = p[x_1, x_2, \ldots, x_n] = \bigoplus_{i=1} m_i,$$

где m_i - моном многочлена $p[X]$, причем

$$m_i = x_{i1}x_{i2}\ldots x_{ij},\ 0 < i1 < i2 < \ldots < ij \le n;$$

задают вес (схемотехнические затраты) C1 для реализации операции & и C2 для реализации операции ⊕ (XOR);

формируют множество многочленов

$P_1 = \{ p_1[X], p_2[X], ..., p_k[X] \}$;

формируют множество переменных

$X_1 = \{ x_1, x_2, ..., x_n \}$;

вычисляют количество выполненных преобразований множества многочленов P

$r = 1$;

(A1) вычисляют максимальное снижение сложности прямой реализации множества многочленов P_r

$d = 1$;

находят пару несовпадающих многочленов $u[X]$, $v[X]$ из множества P_r с максимальным числом общих мономов fm;

если $fm \le d$, то переходят к этапу (A2);

формируют многочлен $g[X]$ в виде суммы мономов многочлена $u[X]$, отличающихся от мономов многочлена $v[X]$;

формируют многочлен $q[X]$ в виде суммы мономов многочлена $v[X]$, отличающихся от мономов многочлена $u[X]$;

формируют многочлен $h[X]$ в виде суммы общих мономов многочленов $u[X]$, $v[X]$;

вычисляют

$d = fm$;

формируют элемент множества W

$w_r = h[X]$;

вычисляют

$X_{r+1} = X_r$;

формируют множество многочленов P_{r+1} из множества P_r, удаляя из него многочлены $u[X]$ и $v[X]$ и добавляя многочлены $h[X]$, $g[X]$ и $q[X]$;

(A2) вычисляют

$d = (d-1)C2$;

вычисляют сложность прямой реализации множества многочленов P_r

$$dm = \Big(\sum_{p[X] \in P_r} \| T(p[X]) \| - \| P_r \| \Big) C2 + \Big(\sum_{m \in T_r} \| X(m) \| - \| T_r \| \Big) C1,$$

где

$T(p[X])$ - множество мономов многочлена $p[X]$,

$T_r = \bigcup_{p[X] \in P_r} T(p[X])$ - множество мономов, входящих в многочлены из множества P_r,

$X(m)$ - множество переменных монома m;

если в составе многочленов P_r имеется многочлен со свободным членом, то вычисляют

$dm = dm + C1$,

$i = 0$;

(А3) вычисляют

$i = i + 1$,

вычисляют снижение сложности прямой реализации множества многочленов P_r

$df = 0$;

формируют пустое множество многочленов E;

если $i > n$, то переходят к этапу А4;

если переменная x_i не входит в множество X_r то переходят к этапу А3;

каждый многочлен $u[X]$ из множества P_r представляют в виде

$u[X] = x_i \& u1_i[X] \oplus u2_i[X]$,

где $u1_i[X]$ является суммой мономов многочлена $u[X]$, не содержащих переменную x_i;

$u2_i[X]$ является суммой мономов многочлена $u[X]$, не вошедших в многочлен $u1_i[X]$, в которых исключили переменную x_i;

формируют многочлен $u3_i[X]$ как сумму многочленов $u1_i[X]$ и $u2_i[X]$, в которой приведены подобные члены

$u3_i[X] = u1_i[X] \oplus u2_i[X]$;

если многочлен $u1_i[X]$ содержит не более одного монома, то к множеству E добавляют многочлен $u[X]$;

если многочлен $u1_i[X]$ содержит более одного монома, то к множеству E добавляют многочлен $u1_i[X]$ и вычисляют

$df = df + C1$;

если многочлен $u1_i[X]$ содержит более одного монома и число мономов в многочлене $u3_i[X]$ меньше число мономов в многочлене $u2_i[X]$, то к множеству E добавляют многочлен $u3_i[X]$ и многочлен $x_i \oplus 1$;

если многочлен $u1_i[X]$ содержит более одного монома и число мономов в многочлене $u3_i[X]$ не меньше число мономов в многочлене $u2_i[X]$, то к множеству E добавляют многочлен $u2_i[X]$;

если многочлен $u1_i[X]$ содержит более одного монома, многочлен $u2_i[X] \neq 0$ и $u3_i[X] \neq 0$, то вычисляют

$df = df + C2$;

вычисляют

$$df = df - dm + (\sum_{p[X] \in E} \| T(p[X]) \| - \| E \|) C2 + (\sum_{m \in T_E} \| X(m) \| - \| T_E \|) C1,$$

где

$T_E = \bigcup_{p[X] \in E} T(p[X])$ - множество мономов, входящих в многочлены из множества E,

$X(m)$ - множество переменных монома m;

если в составе многочленов E имеется многочлен со свободным членом, то вычисляют

$df = df + C1$;

если $df \le d$, то переходят к этапу А3;

выполняют следующие действия:

вычисляют

$d = df$;

выбирают в качестве множества P_{r+1} множество E

$P_{r+1} = E$;

получают множество переменных X_{r+1} из множества X_r, удаляя из X_r переменную x_i

$X_{r+1} = X_r \setminus x_i$;

переходят к этапу А3;

(А4) если $d > 0$ и множество X_{r+1} содержит более одного элемента, то вычисляют

$r = r + 1$

и переходят на этап А1;

вычисляют

$rm = r$;

формируют множество мономов L_1 из мономов многочленов P_r;

добавляют во множество мономов L_1 мономы $x_1, x_2, ..., x_n$;

вычисляют количество выполненных преобразований множества мономов L

$t = 1$;

(А5) находят пару несовпадающих мономов a, b из множества L_t с максимальным числом sm общих переменных;

если $sm = 0$, то вычисляют

$tm = t$

и переходят к этапу А6

формируют моном m_t из общих переменных мономов a и b;

формируют моном ma из переменных монома a, отличающихся от переменных

монома b;

формируют моном mb из переменных монома b, отличающихся от переменных монома a;

формируют множество мономов L_{t+1} из множества L_t, удаляя мономы a и b и добавляя мономы m_t, ma и mb;

вычисляют

$t = t + 1$;

переходят на этап A5;

(A6) вычисляют

$t = tm$;

составляют схемы для мономов L_t, являющихся переменными $x_1, x_2, ..., x_n$

(A7) если $t = 1$, то переходят к этапу A8;

вычисляют

$t = t - 1$;

для каждого монома a из множества L_t, не содержащегося во множестве L_{t+1}, выполняют следующие действия:

вычисляют моном $a1$, состоящий из переменных монома a, не входящих в моном m_t;

составляют схемы для монома a, соединяя с помощью операции конъюнкции выходы схем мономов $a1$ и m_t;

переходят на этап A7;

(A8)

вычисляют

$r = rm$;

составляют схемы для многочленов P_r, соединяя с помощью операции XOR выходы схем мономов, входящих в многочлен;

(A9) если $r = 1$, то переходят к этапу A10;

вычисляют

$r = r - 1$;

если множество X_r и множество X_{r+1} совпадают, то для каждого многочлена $u[X]$ из множества P_r, не входящего в множество P_{r+1}, выполняют следующие действия:

формируют многочлен $v[X]$ из мономов многочлена $u[X]$, не входящих в многочлен w_r;

составляют схему для многочлена $u[X]$, соединяя с помощью операции XOR выходы схем многочленов $v[X]$ и w_r;

переходят к этапу A9;

находят переменную x_i, содержащуюся во множестве X_r и не содержащуюся во множество X_{r+1};

каждый многочлен $u[X]$ из множества P_r, не входящий во множество P_{r+1}, представляют в виде

$$u[X]=x_i \& u1_i[X] \oplus u2_i[X],$$

где $u1_i[X]$ является суммой мономов многочлена $u[X]$, не содержащих переменную x_i,

$u2_i[X]$ является суммой мономов многочлена $u[X]$, не вошедших в многочлен $u1_i[X]$, в которых исключили переменную x_i,

формируют многочлен $u3_i[X]$ как сумму многочленов $u1_i[X]$ и $u2_i[X]$, в которой приведены подобные члены

$$u3_i[X]=u1_i[X] \oplus u2_i[X];$$

если $u2_i[X]=0$, то составляют схему для многочлена $u[X]$, соединяя с помощью операции конъюнкции выход схемы многочлена $u1_i[X]$ и входа x_i;

если $u1_i[X]=u2_i[X]$, то составляют схему для многочлена $u[X]$, соединяя с помощью операции конъюнкции выход схемы многочлена $u1_i[X]$ и выход схемы многочлена $x_i \oplus 1$;

если $u1_i[X] \neq u2_i[X]$ и многочлен $u2_i[X]$ содержится в множестве P_{r+1}, то составляют схему для многочлена $u[X]$, соединяя с помощью операции XOR выход схемы многочлена $u2_i[X]$ и выход операции конъюнкции над выходом схемы многочлена $u1_i[X]$ и входа x_i;

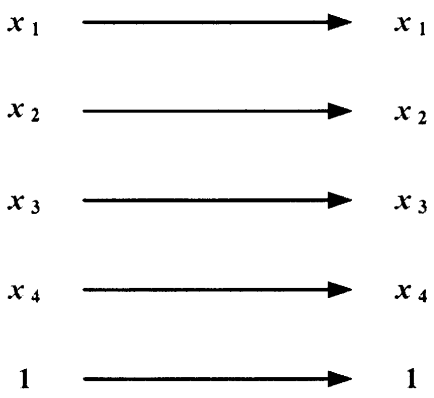
если $u1_i[X] \neq u2_i[X]$ и многочлен $u2_i[X]$ не содержится в множестве P_{r+1}, то составляют схему для многочлена $u[X]$, соединяя с помощью операции XOR выход схемы многочлена $u3_i[X]$ и выход операции конъюнкции над выходом схемы многочлена $u1_i[X]$ и над выходом схемы многочлена $x_i \oplus 1$;

переходят к этапу A9;

(A10) формируют на основе результирующей логической схемы электронную схему для реализации *S*-блока.

1

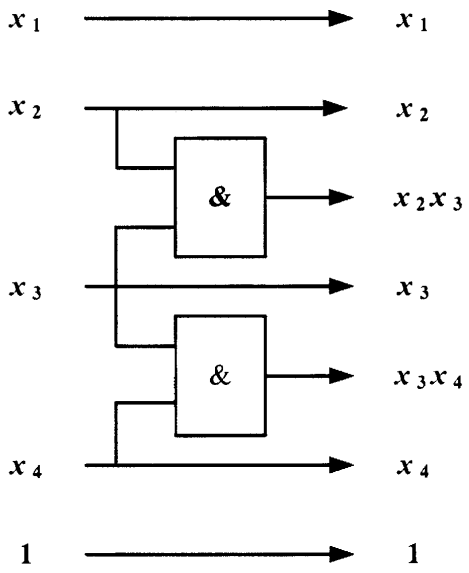
Способ формирования S-блока



Фиг. 1

2

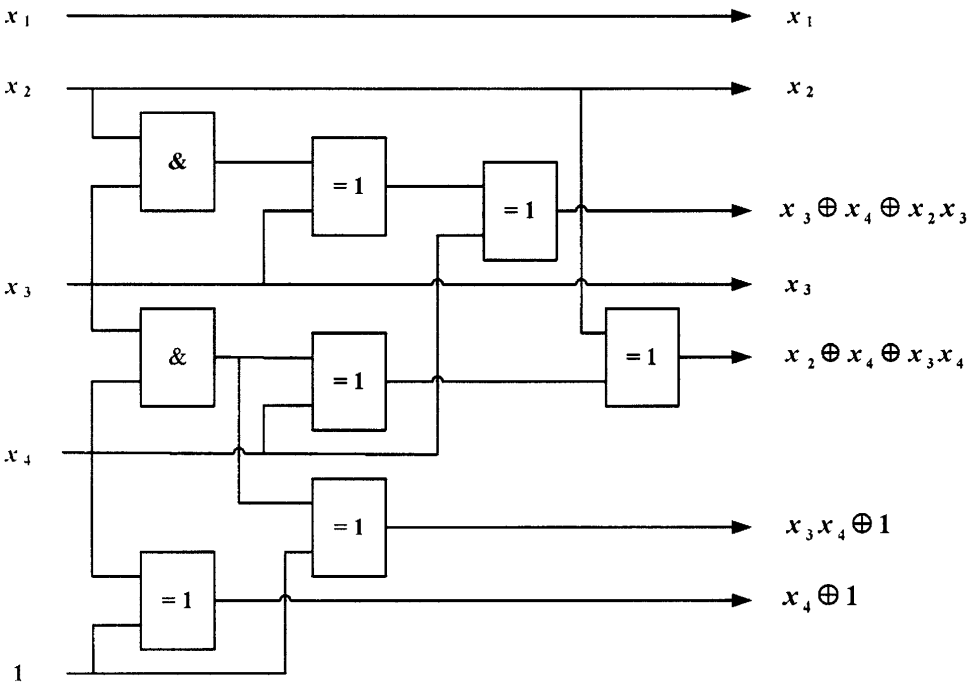
Способ формирования S-блока



Фиг. 2

3

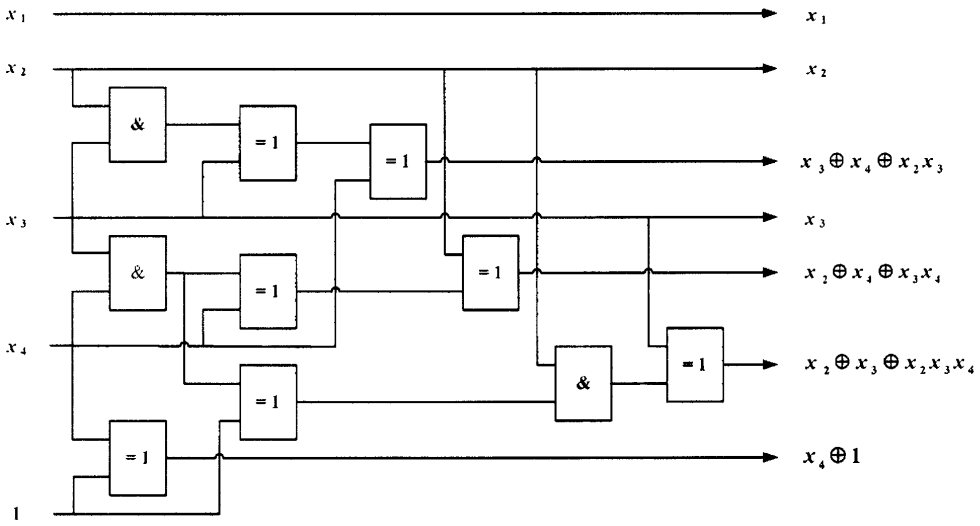
Способ формирования S-блока



Фиг. 3

4

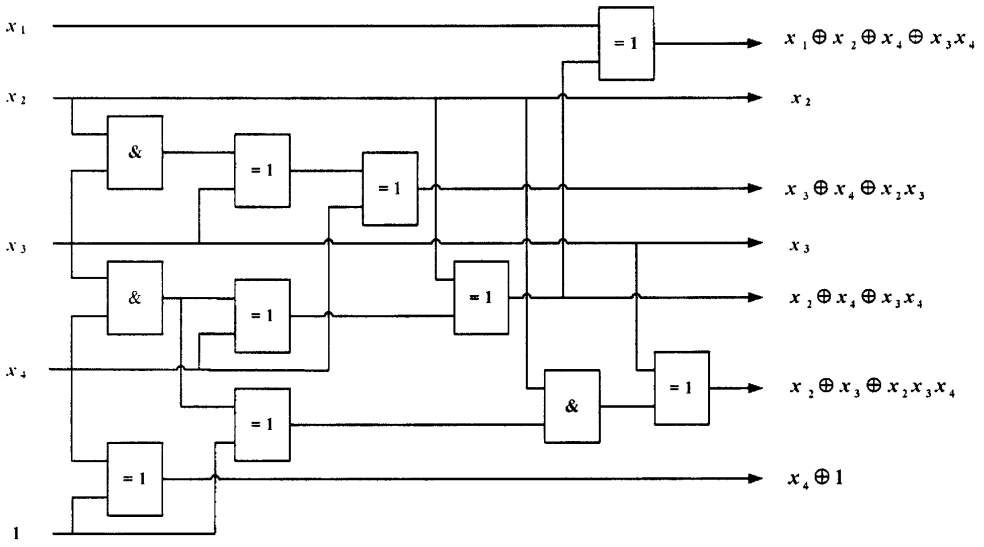
Способ формирования S-блока



Фиг. 4

5

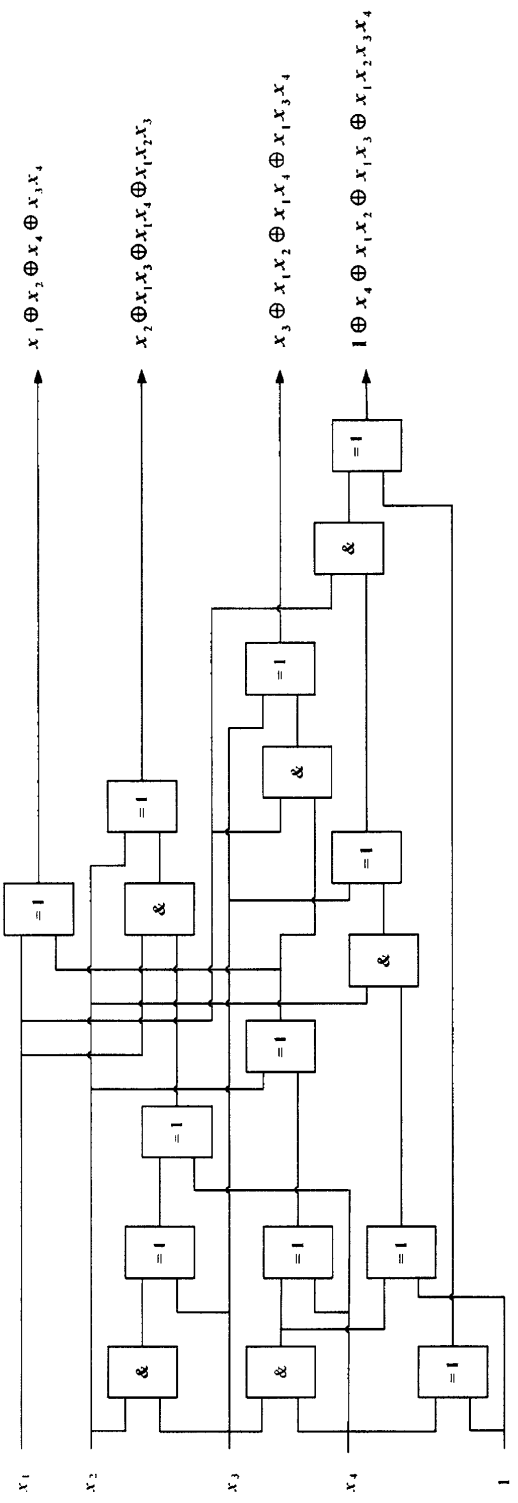
Способ формирования S-блока



Фиг. 5

6

Способ формирования S-блока



Фиг. 6