

Изобретение относится к вычислительной технике и может быть использовано в кодирующих и декодирующих устройствах систематических кодов.

Известно устройство умножения в конечных полях, содержащее четыре регистра, блок определения старшего ненулевого разряда, m переключателей, $(2m-1)$ элементов И, $(m-1)$ элементов И с первыми инверсными входами и $(2m-1)$ сумматоров по модулю два [1].

Недостатком такого устройства являются низкое быстродействие, определяемое m тактами, а также невозможность выполнения операции умножения над элементами различных полей $GF(2^m)$, образованных различными образующими полиномами, где m - степень расширения поля, $2 \leq m \leq n$, n - граничное значение m .

Наиболее близким к предлагаемому является устройство для умножения элементов конечных полей $GF(2^n)$, содержащее первый и второй регистры, n групп по n элементов И в каждой, n многовходовых сумматоров по модулю два и $(n-1)$ блоков матричного преобразования, причем, входы первого и второго регистров являются входами коэффициентов первого и второго сомножителей соответственно, выходы первого регистра соединены с объединенными первыми входами n элементов И в одноименных с номерами выходов первого регистра группах элементов И соответственно, а выходы второго регистра подсоединены к одноименным входам первого блока матричного преобразования и ко вторым входам одноименных элементов И первой группы элементов И соответственно, при этом, выходы предыдущих блоков матричного преобразования подсоединены к одноименным входам следующих блоков матричного преобразования и ко вторым входам одноименных элементов И следующих групп соответственно, причем, выходы одноименных элементов И каждой группы соединены со входами, одноименными с элементами И многовходовых сумматоров по модулю два, выходы которых являются выходами устройства [2].

Недостатком устройства является невозможность выполнения операции умножения над элементами различных полей $GF(2^m)$, образованных различными образующими полиномами, где m - степень расширения поля, $2 \leq m \leq n$, n - граничное значение m .

В основу изобретения поставлена задача создать такое устройство умножения элементов конечных полей, которое выполняет операции формирования над элементами различных полей $GF(2^m)$, образованных различными образующими полиномами, где m - степень расширения поля, $2 \leq m \leq n$, n - граничное значение m , т. е. обладает широкими функциональными возможностями.

Поставленная задача решается тем, что в устройство для умножения элементов конечных полей $GF(2^m)$, содержащее блок формирования частичных произведений, состоящий из n групп по n элементов И в каждой, $(n-1)$ блоков матричного преобразования и блок суммирования, выходы которого соединены с выходом результата устройства, вход i -го разряда первого ($i = 1, \dots, n$) сомножителя которого соединен с объединенными первыми входами элементов И i -ой группы блока формирования частичных произведений, входы текущей суммы j -го блока матричного преобразования ($j = 2, \dots, n-1$) соединены с выходами текущей суммы $(j-1)$ -го блока матричного преобразования, согласно изобретению введен дешифратор, а каждый блок матричного преобразования содержит первую и вторую группы из соответственно n и $(n-1)$ сумматоров по модулю два, первую и вторую группы соответственно из $(n-2)$ и n элементов И и элемент ИЛИ, причем входы дешифратора соединены с соответствующими входами коэффициентов образующего полинома устройства и входами коэффициентов образующего полинома каждого из $(n-1)$ блоков матричного преобразования, а выходы - с входами коэффициентов расширения k -го блока матричного преобразования ($k = 1, \dots, n-2$), выходы текущей суммы $(n-1)$ -го блока матричного преобразования соединены с первыми входами блока суммирования, вторые входы которого соединены с выходами соответствующих элементов И n -ой группы блока формирования частичных произведений, выходы элементов И с первой по $(n-1)$ группу которого соединены соответственно с входами частичных произведений с первого по $(n-1)$ блок матричного преобразования, вход i -го разряда второго сомножителя устройства соединен с объединенными вторыми входами i -ых элементов И в каждой группе блока формирования частичных произведений, при этом в каждом блоке матричного преобразования первые входы сумматоров по модулю два первой группы соединены с входами текущей суммы блока, входы частичных произведений которого соединены с вторыми входами сумматоров по модулю два первой группы, выходы которых, начиная со второго, соединены соответственно с первыми входами сумматоров по модулю два второй группы, вторые входы которых соединены соответственно с выходами с первого по $(n-1)$ -ый элемент И второй группы, выходы сумматоров по модулю два и выход $(n-2)$ -го элемента И второй группы соединены с соответствующими выходами текущей суммы блока, выходы сумматоров по модулю два с первого по $(n-2)$ -ой первой группы соединены соответственно с первыми входами элементов И первой группы, вторые входы которых соединены с соответствующими входами коэффициентов расширения блока, а выходы - с входами элемента ИЛИ, выход которого соединен с объединенными первыми входами элементов И второй группы, вторые входы которых соединены с соответствующими входами коэффициентов образующего полинома блока.

Умножение элементов конечных полей производится как умножение многочленов и сводится к вычислению суммы частичных произведений с приведением ее по модулю образующего полинома, что обеспечивает умножение элементов произвольных конечных полей $GF(2^m)$ ($2 \leq m \leq n$), образованных различными образующими полиномами, т.е. расширяются функциональные возможности устройства.

Структурная схема устройства умножения элементов конечных полей $GF(2^m)$ приведена на фиг. 1, структурная схема блока матричного преобразования - на фиг. 2, структурная схема дешифратора - на фиг. 3.

Устройство умножения элементов конечных полей $GF(2^m)$ (фиг. 1) содержит входы коэффициентов образующего полинома, входы 2 первого сомножителя, входы 3 второго сомножителя, блок 4 формирования частичных произведений, $(n-1)$ блоков 5 матричного преобразования, блок 6 суммирования, дешифратор 7 и выходы 8 результата.

Блок 5 матричного преобразования (фиг. 2) содержит входы 9 текущей суммы, входы 10 частичных произведений, входы 11 текущего коэффициента расширения, входы 12 коэффициентов образующего полинома, первую группу из n сумматоров 13 по модулю два, первую группу из $(n-2)$ элементов И 14, $(n-2)$ -входовый элемент ИЛИ 15, вторую группу из n элементов И 16, вторую группу из $(n-1)$ сумматоров 17 по модулю два и выходы 18 текущей суммы.

Дешифратор 7 (фиг. 3) содержит входы 19 коэффициентов образующего полинома, группу из $(n-3)$ инверторов 20, группу из $(n-3)$ элементов И 21 и выходы 22 текущего коэффициента расширения.

Блок 4 формирования частичных произведений, состоящий из n групп по n элементов И в каждой, предназначен для получения последовательности частичных произведений вида $a(x) \cdot v_k$, a_i - множество коэффициентов первого сомножителя, v_k - k -тый коэффициент второго сомножителя. Таким образом на выходах элементов И первой группы формируются частичные произведения $a_{(n-1)} \cdot v_{(n-1)}$, $a_{(n-2)} \cdot v_{(n-1)}$, $a_{(n-3)} \cdot v_{(n-1)}$, ..., $a_1 \cdot v_{(n-1)}$, $a_0 \cdot v_{(n-1)}$, на выходах второй группы элементов И - $a_{(n-1)} \cdot v_{(n-2)}$, $a_{(n-2)} \cdot v_{(n-2)}$, $a_{(n-3)} \cdot v_{(n-2)}$, ..., $a_1 \cdot v_{(n-2)}$, $a_0 \cdot v_{(n-2)}$, и т.д. на выходах n -ой группы элементов И - $a_{(n-1)} \cdot v_0$, $a_{(n-2)} \cdot v_0$, $a_{(n-3)} \cdot v_0$, ..., $a_1 \cdot v_0$, $a_0 \cdot v_0$.

Дешифратор 7 предназначен для определения коэффициента расширения поля. Так как степень расширения поля определяется старшим коэффициентом обращаемого полинома $g^m(x)$, то появление сигнала "1" в старшем коэффициенте образующего полинома трактуется на выходах дешифратора как текущий коэффициент расширения. При этом все остальные выходы блокируются ("0").

Блоки 5 матричного преобразования предназначены для вычисления текущей суммы частичных произведений и приведения ее по модулю образующего полинома $g^m(x)$. Вычисление текущей суммы $\overline{a(x)} \cdot v_i \oplus \overline{P_{(i-1)}}(x)$, где $\overline{a(x)}$ - коэффициенты первого сомножителя: v_i - i -тый коэффициент второго сомножителя, соответствующий номеру i -го текущего блока 5 матричного преобразования; $\overline{P_{(i-1)}}(x)$ - коэффициенты текущей суммы $(i-1)$ -го предыдущего блока 5 матричного преобразования; \oplus - сумма по модулю два, производится первой группой сумматоров 13 по модулю два. Приведение по модулю два образующего полинома $g^m(x)$ происходит следующим образом. Если сумма по модулю два $a_k v_i \oplus P_{(i-1)k} = 1/a_k$ и $P_{(i-1)}$ - соответственно k -тые коэффициенты первого сомножителя и текущей суммы предыдущего блока 5 матричного преобразования) совпадает со значением коэффициента расширения поля ("1"), то из суммы $\overline{a(x)} \cdot v_i \oplus \overline{P_{(i-1)}}(x)$ вычитается значение коэффициентов $g^m(x)$ образующего полинома, что и является результирующей текущей суммой данного блока. Если совпадения $a_k v_i \oplus P_{(i-1)k}$ со значением коэффициента расширения нет ("0"), то вычитание не производится, и сумма $\overline{a(x)} \cdot v_i \oplus \overline{P_{(i-1)}}(x)$ передается на выход блока. Первая группа элементов И 14 предназначена для сравнения коэффициента расширения со знаком $a_k v_i \oplus P_{(i-1)k}$, а вторая 16 - для управления вычитанием, $(n-3)$ - входовой элемент ИЛИ 15 предназначен для мультиплексирования коэффициентов расширения.

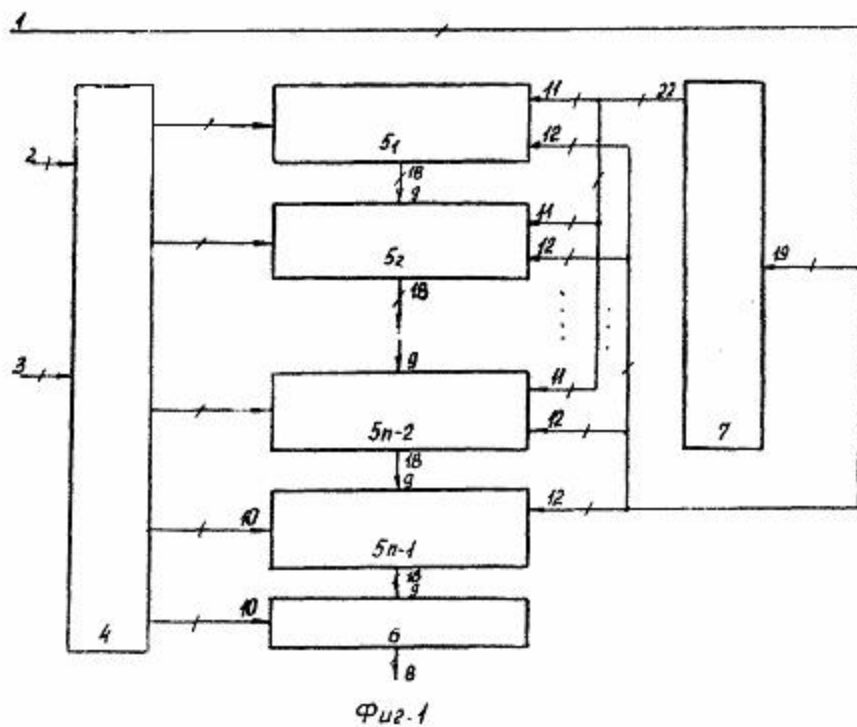
Блок 6 суммирования, состоящий из $(n-1)$ сумматоров по модулю два, предназначен для формирования коэффициентов результирующего произведения, которые определяются как сумма $\overline{a(x)} \cdot v_0 \oplus \overline{P_{(i-1)}}(x)$.

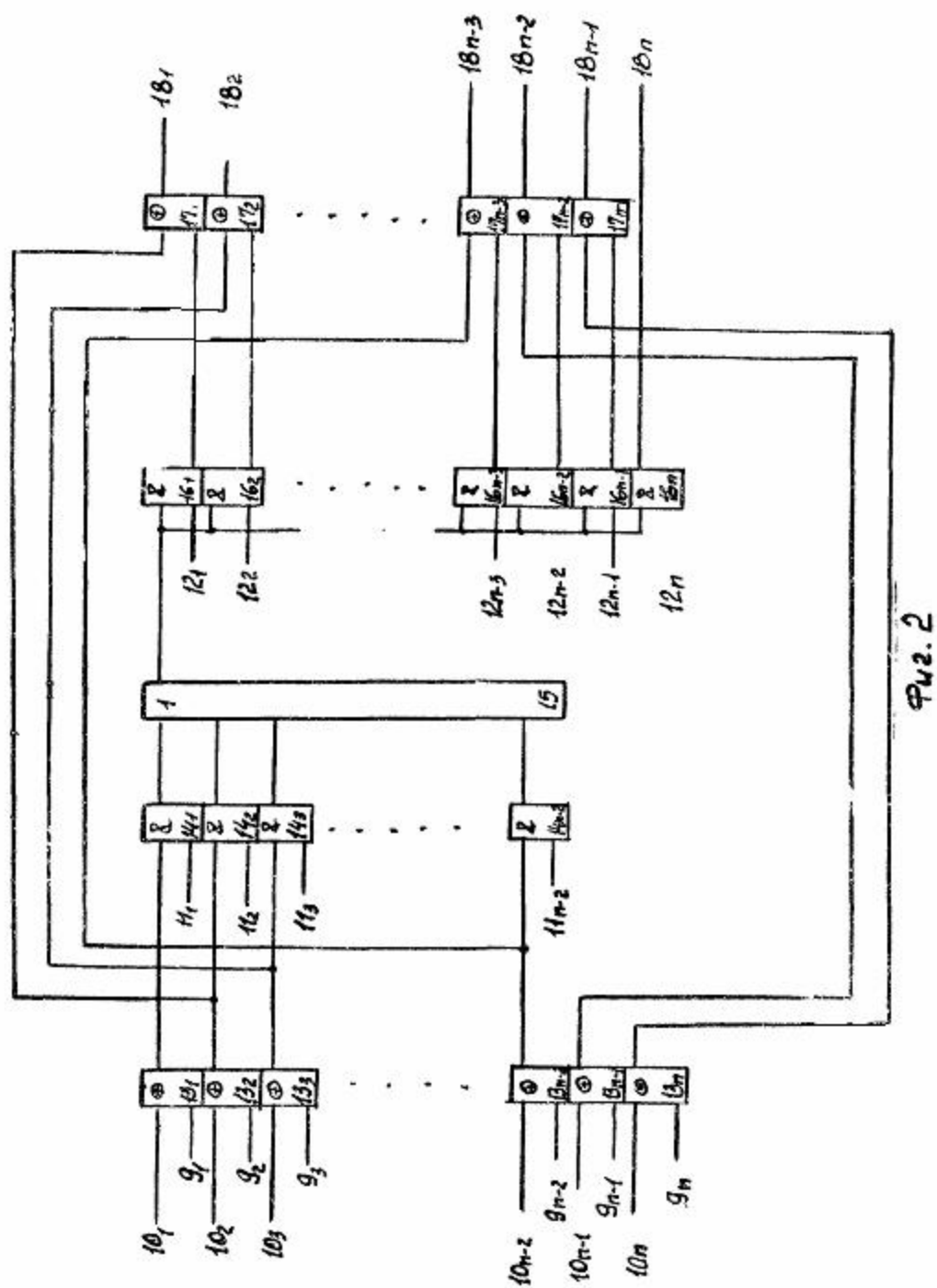
Умножение элементов конечных полей $GF(2^m)$ производится как умножение многочленов и сводится к вычислению суммы частичных произведений с приведением ее по модулю образующего полинома.

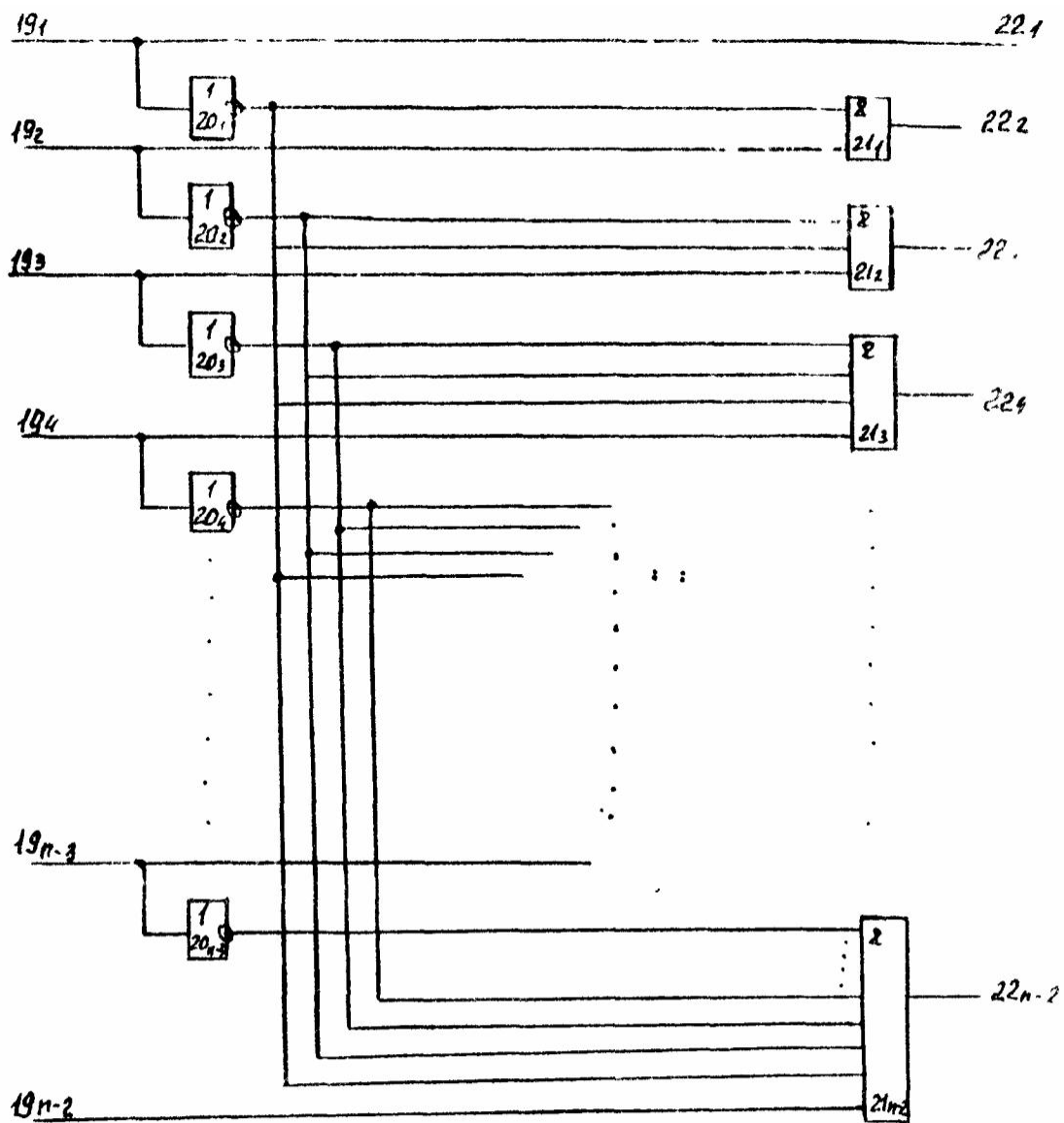
Устройство (фиг. 1) работает следующим образом. Перед началом умножения (или одновременно с ним) на входы 1 образующего полинома устройства подаются значения коэффициентов образующего полинома $g^m(x)$, что приводит к формированию на соответствующем выходе дешифратора 7 коэффициента расширения m . При подаче на входы 2 и 3 устройства соответственно первого $\overline{a(x)}$ и второго $\overline{v(x)}$ сомножителем на выходах блока 4 формирования частичных произведений формируются частичные произведения $\overline{a(x)} \cdot v_i$, которые подаются на входы 10 частичных произведений соответствующих i -тых блоков 5 матричного преобразования, входы 9 текущей суммы каждого из них соединены с одноименными выходами 18 предыдущего $(i-1)$ -го блока 5 матричного преобразования. На выходах 18 каждого i -го блока 5 матричного преобразования формирует i -ая текущая сумма как приведенная по модулю образующего полинома сумма i -го частичного произведения и $(i-1)$ -й текущей суммы, $\langle \overline{a(x)} \cdot v_i \oplus \overline{P_{(i-1)}}(x) \rangle \bmod g^m(x)$. Таким образом на выходах 18 $(n-1)$ -го блока 5 матричного преобразования формируется текущая сумма $\overline{P_{(n-1)}}(x)$ как сумма $\langle \overline{a(x)} \cdot v_i \oplus \overline{P_{(n-2)}}(x) \rangle \bmod g^m(x)$. Окончательно результат умножения элементов конечных полей формируется на выходах 8 блока 6 суммирования.

Эффективность предлагаемого устройства определяется широтой его функциональных возможностей (диапазон степени расширения поля), регулярностью структуры и возможностью реализации в виде законченных БИС и СБИС.

Предлагаемое устройство реализовано в виде макета устройства декодирования кода Рида-Соломона с применением микросхем К531ЛН1, К531ЛП5, К531ЛИ1.







Фиг. 3