УДК 638.322

РЕАЛИЗАЦИЯ ОПЕРАЦИЙ В КОНЕЧНЫХ ПОЛЯХ НА ОДНОМЕРНОМ КАСКАДЕ КОНСТРУКТИВНЫХ МОДУЛЕЙ

В.П. ТАРАСЕНКО, А.К. ТЕСЛЕНКО

Рассмотрена реализация операций в конечных полях на комбинационных схемах линейной сложности — одномерных каскадах конструктивных модулей (ОККМ). На основании предложенных алгоритмов совместной разделительной декомпозиции систем частичных булевых функций сформированы нижние и верхние оценки количества боковых выводов модулей каскада, которые позволяют определить реализуемость операций в конечных полях на ОККМ с заданными конструктивными ограничениями, в том числе и массовых операций. Эффективность этой методики продемонстрирована на примере базисных массовых операций, применяемых в современных несимметричных криптографических преобразованиях.

ВВЕДЕНИЕ

В компьютерной инженерии, например, в помехоустойчивом кодировании, криптографических преобразованиях и т.д., широко применяются специализированные устройства для выполнения операций в конечных полях, что подтверждает актуальность исследования эффективных методов их практической реализации. Развитие компьютерных сетей, повсеместное внедрение электронного документооборота повышают значение такого критерия эффективности, как скорость преобразования информации. В то же время [1] выполнение операций в конечных полях, которые используются, например, в асимметричных криптографических преобразованиях, по скорости существенно уступает симметричным преобразованиям, что приводит к ограничению областей применения ассиметричных преобразований, несмотря на ряд потенциальных преимуществ.

Один из традиционных методов ускорения преобразования информации — реализация их на комбинационных схемах, что находит применение в современной технологии ПЛИС [2]. Однако экспоненциальный рост сложности комбинационных схем с ростом числа независимых переменных n является здесь сдерживающим фактором и в общем случае исключает практическую реализацию на комбинационных схемах массовых операций (т.е. определенных для некоторого ряда значений n). Асимметричные криптографические преобразования и есть примерами массовых операций, которые, кроме того, на практике характеризуются довольно большими значе-

ниями n. Поэтому исследования методов реализации операций в конечных полях на комбинационных схемах с полиномиальной, в частности линейной, зависимостью сложности от числа n разрядов двоичного представления исходных данных вызывают несомненный интерес.

К таким методам относится реализация операций на одномерных каскадах конструктивных модулей (ОККМ), в которых каждый конструктивный модуль (КМ) и каскад в целом являются комбинационными схемами (рис. 1 и рис. 2).

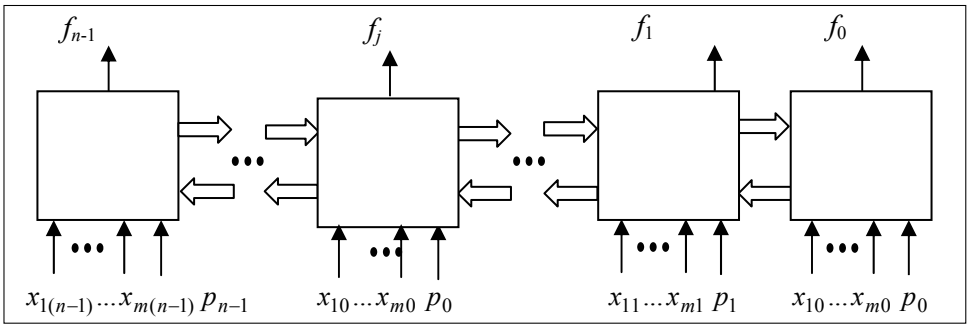

Рис. 1. Структура ОККМ

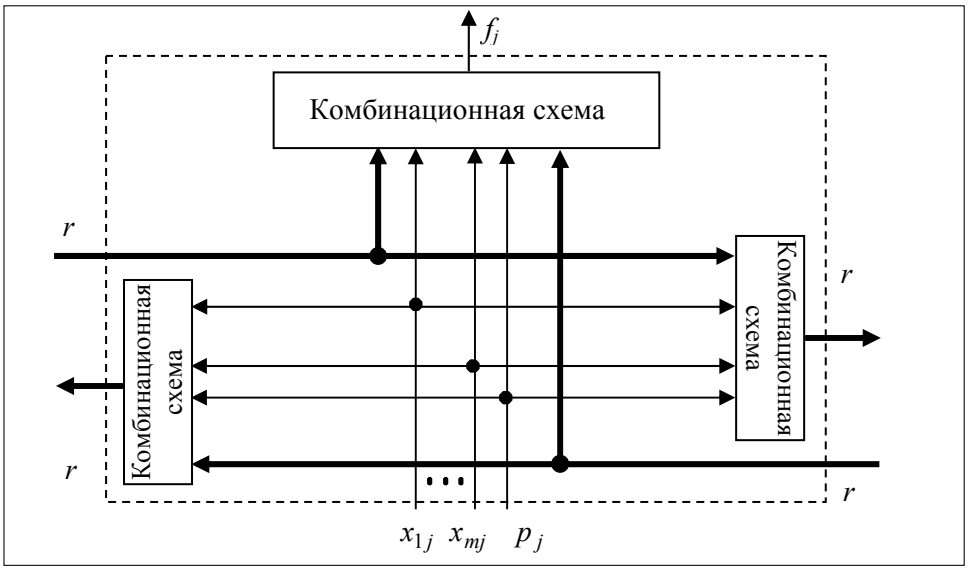

Рис. 2. Структура отдельного КМ

Следует отметить, что ряд типовых операций вычислительной техники (сложение, вычитание, поразрядная логика и т.д.), используемых и в криптографических преобразованиях, реализуется средствами, которые можно считать частными случаями ОККМ.

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ПОСТАНОВКА ЗАДАЧИ

Рассмотрим произвольную операцию $Z = F(X_1, X_2, ..., X_m, P)$ в конечном поле характеристики p и порядка $P = p^w (w \geq 1)$. Будем считать, что эле-

менты конечного поля кодируются целыми числами от 0 до $P-1$, т.е. $Z, X_1, X_2, ..., X_m \in \{0,1,...,P-1\}$. Тогда операция $Z = F(X_1, X_2, ..., X_m, P)$ может быть реализована системой булевых функций

$$f_0(X_1, X_2, ..., X_m, P), f_1(X_1, X_2, ..., X_m, P), ..., f_{n-1}(X_1, X_2, ..., X_m, P),$$

каждая из которых определяет значения разрядов с номером j $(j = 0,1,...,n-1)$ двоичного представления результата операции $Z = F(X_1, X_2, ..., X_m, P)$. Здесь $X_i = \langle x_{i_0}, x_{i_1}, ..., x_{i_{n-1}} \rangle$, $(i = 1,2,\ldots,m)$, $P = \langle p_{i_0}, p_{i_1}, ..., p_{i_{n-1}} \rangle$ — кортежи булевых переменных, определяющих значения разрядов с номером j двоичного представления X_i и P, $n =]\log_2 P[$, $(]u[$ — ближайшее к u большее целое число). В дальнейшем кортежем булевых переменных (или кортежем булевых функций) будем называть последовательность таких переменных (функций), упорядоченную по возрастанию номеров разрядов.

Реализация операций на ОККМ обусловливает следующие конструктивные ограничения. На первичные входы КМ каскада поступают разряды X_i и P с одинаковыми номерами, а на первичном выходе КМ реализуются значения разрядов результата с тем же номером. Для обеспечения возможности увеличения разрядности X_i и P путем присоединения к ОККМ дополнительных модулей потребуем, чтобы при переходе от одного КМ каскада к другому номера разрядов изменялись в порядке возрастания или убывания. Ограничим число боковых входов и выходов каждого КМ по каждому из направлений (как в сторону старших, так и в сторону младших разрядов) некоторым целым значением r. Общее число КМ в ОККМ равно n, а каждый КМ имеет номер, соответствующий номеру разряда.

С учетом принятых ограничений условие реализуемости некоторой массовой операции на ОККМ есть $r < c$, где c — константа, при любых значениях n из ряда возможных значений. В частности $r < c$ при $n \to \infty$. Отсюда возникает задача определения возможных значений количества боковых выводов КМ для реализации на ОККМ операции $Z = F(X_1, X_2, \ldots, X_m, P)$.

ОБЩАЯ МЕТОДИКА РЕШЕНИЯ ЗАДАЧИ

Примем следующие обозначения. Пусть $X_{i_{b,a}} = \langle x_{i_a}, x_{i_{a+1}}, ..., x_{i_b} \rangle$, $(i = 1,2,\ldots,m)$, $P_{b,a} = \langle p_{i_a}, p_{i_{a+1}}, ..., p_{i_b} \rangle$, $U_{b,a} = \langle x_{1_a}, ..., x_{m_a}, p_a, x_{1_{a+1}}, ..., x_{m_{a+1}}, p_{a+1}, x_{1_b}, ..., x_{m_b}, p_b \rangle$ — кортежи булевых переменных, определяемые значениями X_i и P из диапазона номеров разрядов от a до b включительно $(a \le b)$, b, $a < n$. Пусть

$$F_{b,a}(X_1, X_2, ..., X_m, P) =$$

$$= \left\langle f_a(X_1, X_2, ..., X_m, P), f_{a+1}(X_1, X_2, ..., X_m, P), ..., f_b(X_1, X_2, ..., X_m, P) \right\rangle$$

кортеж булевых функций, определяемых значениями разрядов результата с номерами от a до b. При принятых обозначениях

$$X_i \equiv X_{i_{n-1,0}}, P \equiv P_{n-1,0}, \mathrm{X}_{\mathrm{i_{a,a}}} \equiv \langle x_{i_a} \rangle, \langle \mathrm{p_a} \rangle \equiv P_{a,a},$$

$$\mathrm{F_{a,a}}(X_1, X_2, ..., X_m, P) \equiv \langle \mathrm{f_a}(X_1, X_2, ..., X_m, P),$$

$$U_{n-1,0} \equiv \langle X_1, X_2, ..., X_m, P \rangle, F(X_1, X_2, ..., X_m, P) \equiv$$

$$\equiv F_{n-1,0}(X_1, X_2, ..., X_m, P) \equiv F_{n-1,0}(U_{n-1,0}).$$

Произвольный набор значений булевых переменных из кортежа $X_{i_{b,a}}$ обозначим как $g_{i_{b,a}}$ $(i = 1,2,\ldots,n-1)$, а из кортежа $P_{b,a}$ как $s_{b,a}$. Пусть $q_{b,a}$ — вектор $(g_{1_{b,a}}, g_{2_{b,a}}, ..., g_{m_{b,a}}, s_{b,a})$ значений переменных из $U_{b,a}$, а $Q_{b,a}$ — множество всевозможных векторов $q_{b,a}$.

Разделим множество разрядов двоичного представления аргументов X_i, P и результата операции Z на два непустых подмножества: младшее (разряды с номерами от 0 до j) и старшее (от $j+1$ до $n-1$), $(j = 0,1,\ldots,n-2)$.

Основываясь на этом, будем анализировать совместную разделительную декомпозицию [3] функций из кортежа $F_{n-1,j+1}(X_1, X_2, ..., X_m, P)$ при отделении аргументов из кортежа $U_{j,0}$, а также функций из кортежа $F_{j,0}(X_1, X_2, ..., X_m, P)$ при отделении аргументов из кортежа $U_{n-1,j+1}$, т.е.

$$F_{n-1,j+1}(U_{n-1,0}) = F_1(U_{n-1,j+1}, F_2(U_{j,0})),$$

$$F_{j,0}(U_{n-1,0}) = F_3(U_{j,0}, F_4(U_{n-1,j+1})), \quad (j = 1,2,\ldots,n-2),$$

где минимально возможное число функций в кортежах F_2 и F_4 определяется свойствами булевых функций и в конечном итоге свойствами операции $Z = F(X_1, X_2, ..., X_m, P)$.

Определим на множестве векторов $Q_{j,0}$ отношение равенства. Векторы $q_{j,0}, r_{j,0} \in Q_{j,0}$ находятся в отношении равенства, если равны кортежи функций $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$ и $F_{n-1,j+1}(U_{n-1,j+1}, r_{j,0})$. Два кортежа функций равны, если число функций в кортежах одинаково, а булевы функции, находящиеся на одних и тех же позициях в кортежах, равны. Очевидно, что отношение равенства кортежей функций является отношением эквивалентности, которое разбивает множество $Q_{j,0}$ на классы эквивалентности, число которых составляет $d_{j,0}$. Аналогично $d_{n-1,j+1}$ обозначим число классов эквивалентности, на которое разбивается множество $Q_{n-1,j+1}$ по отношению равенства кортежей $F_{j,0}(q_{n-1,j+1}U_{j,0})$. Очевидно, что число функций в кор-

теже F_2 не меньше, чем $]\log_2 d_{j,0}[$, а в кортеже F_4 — не меньше, чем $]\log_2 d_{n-1,j+1}[$.

Согласно [4], для реализации системы булевых функций $F(X_1, X_2, ..., X_m, P)$ на ОККМ **необходимо и достаточно**, чтобы $d_{j,0} \le 2^r$ и $d_{n-1,j+1} \le 2^r$ для всех $j = 0,1,\ldots,n-2$. Отметим, что этот результат может быть использован только тогда, когда булевы функции определены на всех значениях аргументов, например, в случае конечных полей характеристики 2. В этом случае число n модулей ОККМ однозначно определяет значение $P = 2^n$, а функции из кортежа $F(X_1, X_2, ..., X_m)$ определены на всех значениях аргументов из X_i $i = 1,2,\ldots,m$. В случае же конечных полей характеристики $p > 2$ булевы функции из $F(X_1, X_2, ..., X_m, P)$ являются частично определенными даже при фиксированном значении P $(P = \text{const})$. Если же переменные из кортежа P определяются не величиной порядка поля, а одним из возможных неприводимых нормированных многочленов степени n, то функции из $F(X_1, X_2, ..., X_m, P)$ будут частично определенными даже для полей характеристики 2.

Однако методы оптимальной (по заданному критерию) реализации частичных булевых функций по сравнению с методами реализации полностью определенных функций в общем случае более сложны и трудоемки. Поэтому для оценки возможности реализации систем частично определенных булевых функций на ОККМ целесообразно использовать нижние и верхние границы боковых выводов КМ.

Нижней оценкой будем называть такое число боковых выводов КМ по каждому из направлений (в стороны как старших, так и младших разрядов), которое **не превышает** их фактического значения, полученного согласно [4] при **любом** доопределении булевых функций из кортежа $F(X_1, X_2, ..., X_m, P)$. **Верхней** оценкой будем называть число боковых выводов КМ по каждому из направлений, которое **не меньше** их фактического значения, полученного согласно [4] **хотя бы для одного** из возможных доопределений.

Приведенные определения нижней и верхней оценок упрощают анализ реализаций произвольной операции $Z = F(X_1, X_2, ..., X_m, P)$ на ОККМ. Действительно, некоторая операция принципиально не может быть реализована на ОККМ с числом боковых выводов модулей, меньшим, чем нижние оценки. В то же время достоверно существуют реализации операции на ОККМ с числом боковых выводов модулей, равным верхней оценке. В случае массовых операций, если хотя бы одна из нижних оценок — возрастающая функция от n, ее реализация на ОККМ невозможна. Если обе верхние оценки не являются возрастающими функциями от n, то массовая операция реализуема на ОККМ.

Для определения верхних и нижних оценок числа боковых выводов КМ рассмотрим совместную разделительную декомпозицию систем частичных булевых функций. При этом на множестве векторов значений отделяемых

аргументов (например, $Q_{j,0}$) в общем случае нельзя установить отношение равенства кортежей функций из-за неполного определения функций в кортежах. Можно лишь определить отношение совместимости кортежей функций.

Два кортежа функций являются совместимыми, если они содержат одинаковое число функций, и совместимы функции, находящиеся на одинаковых позициях в кортежах. В свою очередь, две функции совместимы, если они равны на всех тех наборах значений аргументов, где они определены. Векторы значений отделяемых аргументов, порождающие совместимые кортежи функций, назовем совместимыми. В дальнейшем, для упрощения изложения, отношение равенства будем рассматривать как частный случай отношения совместимости, что не противоречит определению этих отношений.

АЛГОРИТМЫ ОЦЕНКИ ЧИСЛА ВЫВОДОВ МОДУЛЕЙ ОККМ

В общем случае отношение совместимости на множестве векторов значений отделяемых переменных не является отношением эквивалентности. Это приводит к постановке задачи определения покрытия множества векторов значений отделяемых переменных минимально возможным числом подмножеств совместимых векторов — задачи определения кратчайшего покрытия. Известен алгоритм (далее **Алгоритм 1**) решения такой задачи [5], заключающийся в выполнении всевозможных совмещений (склеиваний) векторов, формировании тупиковых покрытий и выборе среди них кратчайшего.

Необходимо отметить, что **Алгоритм 1** в общем случае формирует тупиковые покрытия, в которых подмножества покрытия могут пересекаться. Применительно к совместной декомпозиции систем частичных булевых функций это означает, что на векторах, входящих в подмножества пересечения, доопределение булевых функций не является однозначным. Однако любое возможное доопределение булевых функций на этом подмножестве векторов не изменит количества подмножеств тупикового покрытия и может быть использовано для оптимизации реализации функций по дополнительным критериям. Кроме того, любое возможное доопределение кортежей булевых функций на векторах, входящих в подмножества пересечения подмножеств покрытия, фактически приводит к разбиению исходного множества векторов на непересекающиеся подмножества. Тем не менее, с учетом приведенных замечаний в дальнейшем будем использовать термин «покрытие», а термин «разбиение» соотносить, как это принято, с отношениями эквивалентности.

Укажем на следующие, важные для дальнейшего изложения, свойства тупиковых покрытий:

- Любые два вектора, входящие в одно и то же подмножество тупикового покрытия, совместимы.
- Два любых подмножества тупикового покрытия содержат, по крайней мере, по одному несовместимому вектору (в противном случае покрытие не будет тупиковым).

- Каждому подмножеству покрытия совместимых векторов соответствует подмножество совместимых кортежей функций. В результате совмещения кортежей функций из такого подмножества происходит доопределение функций в кортежах на всех или на части значений аргументов, где они не были определены. Этот процесс в дальнейшем будем называть доопределением функций в кортежах или доопределением кортежей, а сформированный кортеж — характеристическим кортежем подмножества покрытия.
- Характеристические кортежи подмножеств тупикового покрытия попарно не совместимы.
- Кратчайшему покрытию соответствует наименьшее число попарно не совместимых характеристических кортежей.

Пусть $d_{j,0}$ и $d_{n-1,j+1}$ — числа подмножеств кратчайшего покрытия множества $Q_{j,0}$ и $Q_{n-1,j+1}$, соответственно, полученные при независимом анализе для каждого значения n. Поскольку никакие доопределения функций из двух несовместимых кортежей не преобразуют кортежи в совместимые, то значения $]\log_2 d_{j,0}[$ и $]\log_2 d_{n-1,j+1}[$ позволяют определить **нижние** оценки числа боковых выводов КМ в ОККМ: $L_{\leftarrow}(n) = \max\left(]\log_2 d_{j,0}[\right)$ — в сторону старших разрядов, $L_{\rightarrow}(n) = \max\left(]\log_2 d_{n-1,j+1}[\right)$ — в сторону младших разрядов, $j = 0,1,\ldots,n-2$.

Для формирования верхних оценок введем понятие **непротиворечивости** покрытий множеств векторов. Согласно изложенному выше, подмножеству покрытия соответствует подмножество совместимых кортежей функций. При совмещении таких кортежей происходит доопределение функций в кортежах. Если доопределения любой функции из $F(X_1, X_2, ..., X_m, P)$, вызванные покрытиями двух различных множеств векторов $Q_{a,b}$ и $Q_{c,d}$, являются одинаковыми, то такие покрытия будем называть непротиворечивыми. Отсюда следует, что некоторые покрытия (не обязательно тупиковые) множеств $Q_{n-1,j+1}$ и $Q_{j,0}$, ($j = 0,1,\ldots,n-2$) являются непротиворечивыми, если существует, по крайней мере, одно доопределение функций из кортежа $F(X_1, X_2, ..., X_m, P)$, в результате которого любые два вектора из любого подмножества покрытия останутся совместимыми (напомним, что отношение равенства рассматривается как частный случай отношения совместимости).

Обозначим $e_{j,0}$ и $e_{n-1,j+1}$ числа подмножеств непротиворечивых покрытий множеств $Q_{j,0}$ и $Q_{n-1,j+1}$ ($j = 0,1,\ldots,n-2$). Эти числа позволяют определить **верхние** оценки числа боковых выводов модулей ОККМ: $H_{\leftarrow}(n) = \max\left(]\log_2 e_{j,0}[\right)$ — в сторону старших разрядов и $H_{\rightarrow}(n) = \max\left(]\log_2 e_{n-1,j+1}[\right)$ — в сторону младших разрядов, $j = 0,1,\ldots,n-2$.

Для определения верхних оценок рассмотрим свойства частичных булевых функций из кортежа $F(X_1, X_2, ..., X_m, P)$. Их особенностью является неопределенность всех функций кортежа для одних и тех же векторов значений аргументов. Легко видеть, что таким же свойством обладают любые

кортежи $F_{n-1,\,j+1}(U_{n-1,\,j+1}, q_{j,0})$ и $F_{j,0}(q_{n-1,j+1}U_{j,0})$ где $q_{j,0} \in Q_{j,0}$, $q_{n-1,j+1} \in Q_{n-1,j+1}$ ($j = 0,1,\ldots,n-2$). Это обусловливает следующую классификацию отношений совместимости кортежей частично определенных функций: отношения псевдоравенства, одностороннего и двустороннего доопределений.

Отношение псевдоравенства будем обозначать символом $\cong$, например, $a_{j,0} \cong b_{j,0}$, где $a_{j,0}, b_{j,0} \in Q_{j,0}$ или $F_{n-1,j+1}(U_{n-1,j+1}, a_{j,0}) \cong$ $\cong F_{n-1,j+1}(U_{n-1,j+1}, b_{j,0})$. При данном отношении множество векторов значений не отделяемых аргументов (в рассматриваемом примере $Q_{n-1,j+1}$) разбивается на два подмножества. На первом из них функции из обоих кортежей определены и равны, на втором — не определены. Если первое из подмножеств пустое, то функции в обоих кортежах не определены при всех значениях аргументов. Если второе подмножество пустое, то функции из различных кортежей определены и равны на всех значениях аргументов, т.е. отношение равенства — частный случай отношения псевдоравенства. Легко видеть, что отношение псевдоравенства является отношением эквивалентности. При совмещении векторов значений отделяемых переменных доопределение функций в кортежах может быть произвольным, но одинаковым для функций в различных кортежах (неоднозначное доопределение). Данное отношение будем называть отношением совместимости ранга 1.

Отношение одностороннего доопределения будем обозначать символом $\Rightarrow$, например, $a_{j,0} \Rightarrow b_{j,0}$, где $a_{j,0}, b_{j,0} \in Q_{j,0}$ или $F_{n-1,j+1}(U_{n-1,j+1}, a_{j,0}) \Rightarrow$ $\Rightarrow F_{n-1,j+1}(U_{n-1,j+1}, b_{j,0})$. При данном отношении множество векторов значений не отделяемых аргументов (в рассматриваемом примере $Q_{n-1,j+1}$) разбивается на три подмножества. На первом из них (оно **может** быть пустым) функции из обоих кортежей определены и равны, на втором (оно **не может** быть пустым) функции кортежа слева от знака $\Rightarrow$ не определены, а справа — определены, на третьем из них (оно тоже **может** быть пустым) функции из обоих кортежей не определены. Вектор $a_{j,0}$ и кортеж $F_{n-1,j+1}(U_{n-1,j+1}, a_{j,0})$ будем называть **поглощаемыми**. Отношение одностороннего доопределения обладает свойством транзитивности (из $a_{j,0} \Rightarrow b_{j,0}$ и $b_{j,0} \Rightarrow c_{j,0}$ следует $a_{j,0} \Rightarrow c_{j,0}$), но не обладает свойствами симметричности и рефлексивности (из $a_{j,0} \Rightarrow b_{j,0}$ не следует $b_{j,0} \Rightarrow a_{j,0}$ и не верно $a_{j,0} \Rightarrow a_{j,0}$). Здесь и в дальнейшем будем считать, что в процессе совмещения кортежей функций, для которых существует рассматриваемое отношение, происходит доопределение функций из кортежа $F_{n-1,j+1}(U_{n-1,j+1}, a_{j,0})$ только значениями функций из кортежа $F_{n-1,j+1}(U_{n-1,j+1}, b_{j,0})$ (однозначное доопределение). На векторах из третьего множества (если оно не пустое) функции в обоих кортежах остаются не определенными. Такое доопределение обозначим $F_{n-1,j+1}(U_{n-1,j+1}, a_{j,0}) :=$ $= F_{n-1,j+1}(U_{n-1,j+1}, b_{j,0})$. Очевидно, что в результате совмещения создается

кортеж, совпадающий с имеющимся кортежем $F_{n-1,j+1}(U_{n-1,j+1}, b_{j,0})$, т.е. новый кортеж не создается. Отношение одностороннего доопределения будем называть отношением совместимости ранга 2. Между поглощенным и поглощаемым вектором (кортежем функций) в результате выполнения совмещения устанавливается отношение псевдоравенства.

Отношение двустороннего доопределения (отношение совместимости ранга 3) будем обозначать символом $\Leftrightarrow$, например, $a_{ij} \Leftrightarrow b_{j,0}$ или $F_{n-1,j+1}(U_{n-1,j+1}, a_{j,0}) \Leftrightarrow F_{n-1,j+1}(U_{n-1,j+1}, b_{j,0})$. При данном отношении множество векторов значений аргументов (в рассматриваемом примере $Q_{n-1,j+1}$) разбивается на четыре подмножества. На первом из них (оно **может** быть пустым) функции из обоих кортежей определены и равны, на втором (оно **не может** быть пустым) функции кортежа слева от знака $\Leftrightarrow$ не определены, а справа — определены, на третьем (оно **не может** быть пустым) — функции кортежа слева от знака $\Leftrightarrow$ определены, а справа — не определены, на четвертом (оно тоже **может** быть пустым) — функции из обоих кортежей не определены. Отношение двустороннего доопределения обладает свойством симметричности (например, из $a_{ij} \Leftrightarrow b_{j,0}$ следует $b_{j,0} \Leftrightarrow a_{j,0}$), но не обладает свойством рефлексивности и транзитивности. Здесь и далее будем считать, что процесс совмещения кортежей функций, для которых существует отношение двустороннего доопределения, состоит только во взаимном доопределении функций в кортежах на втором и третьем подмножествах аргументов. На векторах из четвертого множества (если оно не пустое) функции в обоих кортежах остаются не определенными. При этом может создаваться ранее отсутствующий кортеж. Например, в случае совмещения кортежей $F_{n-1,j+1}(U_{n-1,j+1}, a_{j,0})$ и $F_{n-1,j+1}(U_{n-1,j+1}, b_{j,0})$ может создаваться кортеж**,** которого не было в перечне кортежей, порождаемых всеми векторами из множества $Q_{j,0}$. Между кортежем, созданным в результате совмещения, и исходными кортежами устанавливается отношение одностороннего доопределения.

Поскольку в кортежах булевых функций $F(X_1, X_2, ..., X_m, P)$, реализующих операции в конечных полях, при любых значениях аргументов все функции определены или все функции не определены, то между любыми векторами множества $Q_{j,0}$ (или множества $Q_{n-1,j+1}$), $j = 0,1,\ldots,n-2$, может существовать одно из перечисленных отношений совместимости, т.е. приведенная классификация исчерпывает все возможные отношения совместимости векторов и соответствующих им кортежей функций.

Среди рассмотренных отношений совместимости отношение ранга 1 является отношением эквивалентности. Оно разбивает множество $Q_{j,0}$ (и $Q_{n-1,j+1}$), $j = 0,1,\ldots,n-2$, на классы эквивалентности — подмножества совместимых векторов (ранга 1), т.е. такое разбиение является некоторым покрытием (в общем случае не тупиковым) исходного множества непересекающимися подмножествами совместимых векторов. Легко видеть, что

такие покрытия множеств $Q_{j,0}$ и $Q_{n-1,j+1}$, $j = 0,1,\ldots,n-2$, являются непротиворечивыми. Действительно, для этого достаточно доопределить все частичные функции из $F(X_1, X_2, ..., X_m, P)$ на всех тех векторах значений аргументов, где они не определены, одним и тем же значением (например, 0). Следовательно, число классов эквивалентности по отношению совместимости ранга 1 множеств векторов $Q_{j,0}$ и $Q_{n-1,j+1}$, $j = 0,1,\ldots,n-2$, может служить для определения верхних оценок числа боковых выводов модулей ОККМ, реализующего систему частичных булевых функций. Такие верхние оценки назовем оценками по псевдоравенству. В общем случае они могут быть весьма завышенными, поскольку не учитывают отношения совместимости рангов 2 и 3. Тем не менее, оценки по псевдоравенству могут свидетельствовать о принципиальной возможности реализации на ОККМ массовых операций.

Рассмотрим **Алгоритм 2** определения верхних оценок на основе отношений совместимости рангов 1 и 2 (оценок по одностороннему доопределению).

1. Для каждого $j = 0,1,\ldots,n-2$ выполнить пп. 2 и 4.

2. Определить список классов разбиения множеств векторов $Q_{j,0}$ по отношениям совместимости ранга 1.

3. Вычеркнуть из списка классы, векторы которых поглощаются хотя бы одним вектором из $Q_{j,0}$.

4. Определить значение $e_{j,0}$ количества классов, оставшихся не вычеркнутыми.

5. Определить оценку $O_{\leftarrow}(n) = \max(]\log_2 e_{j,0}[)$. Выполнить пп. 1…4 для множеств $Q_{n-1,j+1}$ и определить оценку $O_{\rightarrow}(n) = \max\left(]\log_2 e_{n-1,j+1}[\right)$.

В общем случае из-за отсутствия свойств симметричности и рефлексивности отношений одностороннего доопределения может существовать несколько вариантов поглощения векторов из некоторого класса. Вследствие множественности вариантов поглощения векторов некоторого класса может существовать несколько вариантов результирующего покрытия множеств $Q_{j,0}$ и $Q_{n-1,j+1}$ подмножествами совместимых векторов по отношениям совместимости рангов 1 и 2. Однако число подмножеств таких покрытий неизменно и равно соответственно $e_{j,0}$ и $e_{n-1,j+1}$. Это следует из свойства транзитивности отношений одностороннего доопределения, а также из того, что при совмещении кортежей функций, находящихся в отношении ранга 2, новые кортежи не создаются. Действительно, величина $e_{j,0}$ определяет максимальное число попарно несовместимых векторов множества $Q_{j,0}$ по отношению совместимости рангов 1 и 2, и она не может измениться в результате любого совмещения векторов, находящихся в отношении ранга 1 или 2.

Покажем, что среди всевозможных вариантов результирующего покрытия множеств $Q_{j,0}$ и $Q_{n-1,j+1}$ ($j = 0,1,\ldots,n-2$) в соответствии с **Алгоритмом 2** всегда существуют непротиворечивые покрытия.

Утверждение 1. Для любого покрытия множества $Q_{b,0}$, порождаемого **Алгоритмом 2**, существуют непротиворечивые покрытия, порождаемые этим же алгоритмом, для множества $Q_{c,0}$ $n-2 \geq c > b \geq 0$.

Рассмотрим произвольный вектор $c_{c,0} \in Q_{c,0}$. Представим $c_{c,0} = (c_{c,b+1}, c_{b,0})$. Пусть существует по крайней мере один вектор $d_{c,0} = (d_{c,b+1}, d_{b,0}) \in Q_{c,0}$ такой, что $c_{c,0} \Rightarrow d_{c,0}$ $((c_{c,b+1}, c_{c,0}) \Rightarrow (d_{c,b+1}, d_{b,0}))$ и $c_{b,0} \Rightarrow d_{b,0}$. Тогда или $(c_{c,b+1}, c_{b,0}) \Rightarrow (c_{c,b+1}, d_{b,0})$, или $(c_{c,b+1}, c_{b,0}) \cong (c_{c,b+1}, d_{b,0})$. В первом случае для вектора $c_{c,0} = (c_{c,b+1}, c_{b,0})$ существует альтернативный вариант совместимости ранга 2, а именно вектор $(c_{c,b+1}, d_{b,0})$, не противоречащий совмещению векторов $c_{b,0}$ и $d_{b,0}$.

Во втором случае совмещение векторов $c_{b,0}$ и $d_{b,0}$ не приводит к доопределению функций из кортежа $F_{n-1,c+1}(U_{n-1,c+1}, c_{c,b+1}, c_{b,0})$. Если же вектор $c_{c,0}$ поглощается каким-либо вектором из $Q_{c,0}$, то этим же вектором может быть поглощен и вектор $c_{c,b+1}, d_{b,0}$, что приводит к одинаковому доопределению функций в кортежах $F_{n-1,b+1}(U_{n-1,b+1}, c_{b,0})$ и $F_{n-1,b+1}(U_{n-1,b+1}, d_{b,0})$.

Пусть ни одного вектора $d_{c,0}$ с указанным свойством не существует. Однако это означает, что вектор $c_{b,0}$ не поглощается ни одним вектором из множества $Q_{b,0}$, а также функции из кортежа $F_{n-1,b+1}(U_{n-1,b+1}, c_{b,0})$ не были доопределены ни на одном векторе из $Q_{n-1,b+1}$. В этом случае никакие доопределения функций из кортежа $F_{n-1,b+1}(U_{n-1,b+1}, c_{b,0})$ в результате любых поглощений векторов во множестве $Q_{c,0}$ не изменят свойств вектора $c_{b,0}$ поглощать векторы из множества $Q_{b,0}$, если таковые имелись. Аналогично изложенному доказывается справедливость **Утверждения 2**.

Утверждение 2. Для любого покрытия множества $Q_{n-1,c+1}$, порождаемого **Алгоритмом 2**, существуют непротиворечивые покрытия, порождаемые этим же алгоритмом, для множества $Q_{n-1,b+1}$ ($n-2 \geq c > b \geq 0$).

Утверждение 3. Любые покрытия множеств $Q_{b,0}$ и $Q_{n-1,c+1}$, порождаемые **Алгоритмом 2**, являются непротиворечивыми ($n-2 \geq c > b \geq 0$).

Для доказательства рассмотрим два произвольных вектора $a_{b,0}, b_{b,0} \in Q_{b,0}$ таких, что $a_{b,0} \Rightarrow b_{b,0}$ и два произвольных вектора $c_{n-1,c+1} d_{n-1,c+1} \in Q_{n-1,c+1}$ таких, что $c_{n-1,c+1} \Rightarrow d_{n-1,c+1}$. Покажем, что поглощение вектора $a_{b,0}$ не может привести к несовместимости векторов $c_{n-1,c+1}$ и $d_{n-1,c+1}$. Из принятых условий следует

$$F_{c,0}(c_{n-1,c+1} U_{c,b+1}, U_{b,0}) \Rightarrow F_{c,0}(d_{n-1,c+1}, U_{c,b+1}, U_{b,0}), \qquad (1)$$

$$F_{n-1,b+1}(U_{n-1,c+1}U_{c,b+1}, a_{b,0}) \Rightarrow F_{n-1,b+1}(U_{n-1,c+1}, U_{c,b+1}, b_{b,0}). \qquad (2)$$

Обозначим $T_{n-1,b+1}$ такое непустое по определению подмножество векторов множества $Q_{n-1,b+1}$, где функции в кортеже $F_{n-1,b+1}(U_{n-1,c+1}, U_{c,b+1}, a_{b,0})$ не определены, а в кортеже $F_{n-1,b+1}(U_{n-1,c+1}, U_{c,b+1}, b_{b,0})$ определены. Если не существует ни одного вектора $(t_{n-1,c+1}, t_{c,b+1}) \in T_{n-1,b+1}$ такого, что $t_{n-1,c+1} = c_{n-1,c+1}$, то доопределение функций в кортеже $F_{n-1,b+1}(U_{n-1,c+1}, U_{c,b+1}, a_{b,0})$ не может изменить отношение $c_{n-1,c+1} \Rightarrow$ $\Rightarrow d_{n-1,c+1}$. Пусть существует хотя бы один вектор $(t_{n-1,c+1}, t_{c,b+1}) \in$ $\in T_{n-1,b+1}$ такой, что $t_{n-1,c+1} = c_{n-1,c+1}$. Тогда кортеж значений функций $F_{c,b+1}(c_{n-1,c+1}, t_{c,b+1}, b_{b,0})$ определен и согласно (1) равен кортежу значений функций $F_{c,b+1}(d_{n-1,c+1}, t_{c,b+1}, b_{b,0})$.

В результате поглощения вектора $a_{b,0}$ вектором $b_{b,0}$

$$F_{c,b+1}(c_{n-1,c+1}, t_{c,b+1}, a_{b,0}) := F_{c,b+1}(c_{n-1,c+1}, t_{c,b+1}, b_{b,0})$$

или

$$F_{c,b+1}(c_{n-1,c+1}, t_{c,b+1}, a_{b,0}) = F_{c,b+1}(c_{n-1,c+1}, t_{c,b+1}, b_{b,0}).$$

Если кортеж значений функций $F_{c,b+1}(d_{n-1,c+1}, t_{c,b+1}, a_{b,0})$ определен, то согласно (2) он равен кортежу значений функций $F_{c,b+1}(d_{n-1,c+1}, t_{c,b+1}, b_{b,0})$. Если не определен, то вектор $(d_{n-1,c+1}, t_{c,b+1}) \in T_{n-1,b+1}$, и в результате поглощения вектора $a_{b,0}$ вектором $b_{b,0}$

$$F_{c,b+1}(d_{n-1,c+1}, t_{c,b+1}, a_{b,0}) := F_{c,b+1}(d_{n-1,c+1}, t_{c,b+1}, b_{b,0}).$$

Отсюда следует

$$F_{c,b+1}(d_{n-1,c+1}, t_{c,b+1}, a_{b,0}) = F_{c,b+1}(d_{n-1,c+1}, t_{c,b+1}, b_{b,0}),$$

что не противоречит совместимости векторов $c_{n-1,c+1}$ и $d_{n-1,c+1}$. Аналогично можно показать, что поглощение вектора $c_{n-1,c+1}$ не может привести к несовместимости векторов $a_{b,0}$ и $b_{b,0}$.

Утверждения 1…3 показывают, что среди всевозможных покрытий множеств $Q_{j,0}$ и $Q_{n-1,j+1}$ ($j = 0,1,\ldots,n-2$), порождаемых **Алгоритмом 2**, существуют непротиворечивые покрытия, и поэтому оценки $O_{\leftarrow}(n)$ и $O_{\rightarrow}(n)$ являются верхними оценками, которые далее будем называть верхними оценками по одностороннему доопределению.

Предположим, что существует такое значение $j = t$, когда в результате вычеркивания векторов из поглощаемых классов множества $Q_{t,0}$ между любыми двумя оставшимися векторами не существует отношения двустороннего доопределения. В этом случае любое из покрытий этого множества,

порождаемых **Алгоритмом 2**, является кратчайшим. Действительно, выберем по одному вектору из каждого не вычеркнутого класса. Согласно принятому условию, они будут попарно не совместимы, следовательно, покрытия множества $Q_{t,0}$ тупиковые. С другой стороны, если среди векторов из вычеркнутых классов были векторы с отношениями двустороннего доопределения как между собой, так и с векторами из не вычеркнутых классов, то в результате их совмещения число характеристических кортежей может только увеличиться. Следовательно, покрытия множества $Q_{t,0}$, порождаемые **Алгоритмом 2**, при принятом условии будут и кратчайшими. Если же $e_{t,0}$ не меньше любых $e_{j,0}$ ($j = 0,1,\ldots,n-2$), то согласно определению, оценка $O_{\leftarrow}(n)$ будет и нижней оценкой. Это доказывают следующие утверждения.

Утверждение 4. Если среди множеств $Q_{j,0}$ с максимальными значениями $e_{j,0}$ существует хотя бы одно, где среди векторов из не вычеркнутых классов отсутствуют отношения двустороннего доопределения, то оценка $O_{\leftarrow}(n)$, полученная с помощью **Алгоритма 2**, является нижней. Аналогично для оценки $O_{\rightarrow}(n)$.

Утверждение 5. Если среди множеств $Q_{n-1,j+1}$ с максимальными значениями $e_{n-1,j+1}$ существует хотя бы одно, где среди векторов из не вычеркнутых классов отсутствуют отношения двустороннего доопределения, то оценка $O_{\rightarrow}(n)$, полученная с помощью **Алгоритма 2**, является нижней.

Заметим, что трудоемкость реализации **Алгоритма 2** существенно ниже по сравнению с **Алгоритмом 1**. В то же время **Алгоритм 2** непосредственно не выделяет необходимые покрытия и, соответственно, не формирует доопределения функций из $F(X_1, X_2, ..., X_m, P)$. Для этой цели применяется **Алгоритм 3**.

1. Разбить множество векторов $Q_{0,0}$ по отношению псевдоравенства. Произвольно выполнить поглощение всех поглощаемых векторов и доопределение функций в поглощаемых кортежах.

2. Последовательно для значений $j = 1,2,\ldots,n-2$ выполнить следующие действия.

   2.1. Разбить множество векторов $Q_{j,0}$ по отношению псевдоравенства с учетом предшествующих доопределений функций из $F(X_1, X_2, ..., X_m, P)$.

   2.2. Выполнить поглощение всех векторов из поглощаемого класса векторами одного и только одного поглощающего класса. Выбор поглощающего класса произвольный. Доопределить функции в поглощаемых кортежах.

3. Разбить множество векторов $Q_{n-1,n-1}$ по отношению псевдоравенства с учетом предшествующих доопределений функций из $F(X_1, X_2, ..., X_m, P)$. Произвольным образом выполнить поглощение всех поглощаемых векторов и доопределить функции в поглощаемых кортежах.

4. Последовательно для значений $j = n-3, n-4, \ldots, 1, 0$ выполнить следующие действия:

4.1. Разбить множество векторов $Q_{n-1,j+1}$ по отношению псевдоравенства с учетом предшествующих доопределений функций из $F(X_1, X_2, ..., X_m, P)$.

4.2. Выполнить поглощение всех векторов из поглощаемого класса векторами одного и только одного поглощающего класса. Выбор поглощающего класса произвольный. Доопределить функции в поглощаемых кортежах.

Достоверность **Алгоритма 3** следует из доказательств **Утверждений 1…3**.

ПРИМЕРЫ

Практическое значение полученных результатов проиллюстрируем реализацией на ОККМ одноместных и двуместных операций в конечных полях характеристики $p > 2$ при $w = 1$ (т.е. $P = p$), которые используются в асимметричных криптографических преобразованиях.

Рассмотрим реализацию операции определения значения Z из уравнения $2Z = X \bmod P$, которую назовем операцией деления на 2 (сдвига вправо) в кольце неотрицательных вычетов по модулю P. Аналитически значение Z определяется по следующему алгоритму:

$$\text{If } (X \bmod 2) = 1 \text{ then } Z := (X + P) \operatorname{div} 2 \text{ else } Z := X \operatorname{div} 2.$$

Функции из кортежа $F(X,P)$ не определены на всех тех значениях аргументов, где $X \geq P$, а также где P четно, а X нечетно. Обозначим

$$Z_{j,0} = Z \bmod 2^{j-1},\ X_{j,0} = X \bmod 2^{j-1},\ P_{j,0} = P \bmod 2^{j-1},$$

$$Z_{n-1,j+1} = Z \operatorname{div} 2^{j+1},\ X_{n-1,j+1} = X \operatorname{div} 2^{j+1},\ \mathrm{P}_{n-1,j+1} = P \operatorname{div} 2^{j+1},$$

$$(j = 0,1,\ldots,n-2).$$

Определим список классов эквивалентности по отношению псевдоравенства для множеств $Q_{j,0}$, $(j = 0,1,\ldots,n-2)$.

Класс $\mathbf{L}_1$, где $X_{j,0}$ нечетное, а $P_{j,0}$ четное. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$, где $q_{j,0} \in \mathbf{L}_1$, не определены на всех значениях аргументов.

Класс $\mathbf{L}_2$, где $X_{j,0}$ и $P_{j,0}$ нечетные, $X_{j,0} < P_{j,0}$, а $X_{j,0} + P_{j,0} < 2^{j+1}$. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$ $(q_{j,0} \in \mathbf{L}_2)$ определены как $Z_{n-1,j+1} = (X_{n-1,j+1} + P_{n-1,j+1}) \operatorname{div} 2$ на всех тех значениях аргументов, где $X_{n-1,j+1} \leq P_{n-1,j+1}$.

Класс $\mathbf{L}_3$, где $X_{j,0}$ и $P_{j,0}$ нечетные, $X_{j,0} \geq P_{j,0}$, а $X_{j,0} + P_{j,0} < 2^{j+1}$. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$ ($q_{j,0} \in \mathbf{L}_3$) определены как $Z_{n-1,j+1} = (X_{n-1,j+1} + P_{n-1,j+1}) \operatorname{div} 2$ на всех тех значениях аргументов, где $X_{n-1,j+1} < P_{n-1,j+1}$.

Класс $\mathbf{L}_4$, где $X_{j,0}$ и $P_{j,0}$ нечетные, $X_{j,0} < P_{j,0}$, а $X_{j,0} + P_{j,0} \geq 2^{j+1}$. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$ ($q_{j,0} \in \mathbf{L}_4$) определены как $Z_{n-1,j+1} = (X_{n-1,j+1} + P_{n-1,j+1} + 1) \operatorname{div} 2$ на всех тех значениях аргументов, где $X_{n-1,j+1} \leq P_{n-1,j+1}$.

Класс $\mathbf{L}_5$, где $X_{j,0}$ и $P_{j,0}$ нечетные, $X_{j,0} \geq P_{j,0}$, а $X_{j,0} + P_{j,0} \geq 2^{j+1}$. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$ ($q_{j,0} \in \mathbf{L}_5$) определены как $Z_{n-1,j+1} = (X_{n-1,j+1} + P_{n-1,j+1} + 1) \operatorname{div} 2$ на всех тех значениях аргументов, где $X_{n-1,j+1} < P_{n-1,j+1}$.

Класс $\mathbf{L}_6$, где $X_{j,0}$ четное, $X_{j,0} < P_{j,0}$. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$ ($q_{j,0} \in \mathbf{L}_6$) определены как $Z_{n-1,j+1} = (X_{n-1,j+1}) \operatorname{div} 2$ на всех тех значениях аргументов, где $X_{n-1,j+1} \leq P_{n-1,j+1}$.

Класс $\mathbf{L}_7$, где $X_{j,0}$ четное, $X_{j,0} \geq P_{j,0}$. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1}, q_{j,0})$ ($q_{j,0} \in \mathbf{L}_7$) определены как $Z_{n-1,j+1} = (X_{n-1,j+1}) \operatorname{div} 2$ на всех тех значениях аргументов, где $X_{n-1,j+1} < P_{n-1,j+1}$.

Определим список классов эквивалентности по отношению псевдоравенства для множеств $Q_{n-1,j+1}$, ($j = 0,1,\ldots,n-2$).

Класс $\mathbf{H}_1$, где $X_{n-1,\,j+1} > P_{n-1,\,j+1}$. Функции из кортежей $F_{j,0}(q_{n-1,j+1}, U_{j,0})$, где $q_{n-1,j+1} \in \mathbf{H}_1$, не определены на всех значениях аргументов.

Класс $\mathbf{H}_2$, где $X_{n-1,j+1} = P_{n-1,j+1}$ и $(X_{n-1,j+1} \bmod 2) = 0$. Функции из кортежей $F_{j,0}(q_{n-1,j+1}, U_{j,0})$, ($q_{n-1,j+1} \in \mathbf{H}_2$) определены как

$$Z_{j,0} = X_{j,0} \operatorname{div} 2, \text{ если } X_{j,0} \text{ четное,}$$

$$Z_{j,0} = (X_{j,0} + P_{j,0}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное,}$$

на всех тех значениях аргументов, где $X_{j,0} < P_{j,0}$, $P_{j,0}$ нечетное или $X_{j,0}$ четное.

Класс $\mathbf{H}_3$, где $X_{n-1,j+1} = P_{n-1,j+1}$ и $(X_{n-1,j+1} \bmod 2) = 1$. Функции из кортежей $F_{j,0}(q_{n-1,j+1}, U_{j,0})$, ($q_{n-1,j+1} \in \mathbf{H}_3$) определены как

$$Z_{j,0} = (2^{j+1} + X_{j,0}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ четное,}$$

$$Z_{j,0} = (X_{j,0} + P_{j,0}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное,}$$

на всех тех значениях аргументов, где $X_{j,0} < P_{j,0}$, $P_{j,0}$ нечетное или $X_{j,0}$ четное.

Класс $\mathbf{H}_4$, где $X_{n-1,j+1} < P_{n-1,j+1}$, $((X_{n-1,j+1} + P_{n-1,j+1}) \bmod 2) = 0$ и $(X_{n-1,j+1} \bmod 2) = 0$. Функции из кортежей $F_{j,0}(q_{n-1,j+1}, U_{j,0})$, ($q_{n-1,j+1} \in$ $\in \mathbf{H}_4$) определены как

$$Z_{j,0} = X_{j,0} \operatorname{div} 2, \text{ если } X_{j,0} \text{ четное},$$

$$Z_{j,0} = (X_{j,0} + P_{j,0}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное},$$

на всех тех значениях аргументов, где $P_{j,0}$ нечетное или $X_{j,0}$ четное.

Класс $\mathbf{H}_5$, где $X_{n-1,j+1} < P_{n-1,j+1}$, $((X_{n-1,j+1} + P_{n-1,j+1}) \bmod 2) = 1$ и $(X_{n-1,j+1} \bmod 2) = 0$. Функции из кортежей $F_{j,0}(q_{n-1,j+1}, U_{j,0})$, ($q_{n-1,j+1} \in$ $\in \mathbf{H}_5$) определены как

$$Z_{j,0} = X_{j,0} \operatorname{div} 2, \text{ если } X_{j,0} \text{ четное},$$

$$Z_{j,0} = (X_{j,0} + P_{j,0} - 2^{j+1}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное и } X_{j,0} + P_{j,0} \geq 2^{j+1},$$

$$Z_{j,0} = (X_{j,0} + P_{j,0} + 2^{j+1}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное и } X_{j,0} + P_{j,0} < 2^{j+1},$$

на всех тех значениях аргументов, где $P_{j,0}$ нечетное или $X_{j,0}$ четное .

Класс $\mathbf{H}_6$, где $X_{n-1,j+1} < P_{n-1,j+1}$, $((X_{n-1,j+1} + P_{n-1,j+1}) \bmod 2) = 0$ и $(X_{n-1,j+1} \bmod 2) = 1$. Функции из кортежей $F_{j,0}(q_{n-1,j+1}, U_{j,0})$, ($q_{n-1,j+1} \in$ $\in \mathbf{H}_6$) определены как

$$Z_{j,0} = (2^{j+1} + X_{j,0}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ четное},$$

$$Z_{j,0} = (X_{j,0} + P_{j,0}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное},$$

на всех тех значениях аргументов, где $P_{j,0}$ нечетное или $X_{j,0}$ четное.

Класс $\mathbf{H}_7$, где $X_{n-1,j+1} < P_{n-1,j+1}$, $((X_{n-1,j+1} + P_{n-1,j+1}) \bmod 2) = 1$ и $(X_{n-1,j+1} \bmod 2) = 1$. Функции из кортежей $F_{j,0}(q_{n-1,j+1}, U_{j,0})$, ($q_{n-1,j+1} \in$ $\in \mathbf{H}_7$) определены как

$$Z_{j,0} = (2^{j+1} + X_{j,0}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ четное},$$

$$Z_{j,0} = (X_{j,0} + P_{j,0} - 2^{j+1}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное и } X_{j,0} + P_{j,0} \geq 2^{j},$$

$$Z_{j,0} = (X_{j,0} + P_{j,0} + 2^{j+1}) \operatorname{div} 2, \text{ если } X_{j,0} \text{ нечетное и } X_{j,0} + P_{j,0} < 2^{j},$$

на всех тех значениях аргументов, где $P_{j,0}$ нечетное или $X_{j,0}$ четное.

Из изложенного следует, что $e_{0,0}=4$ (классы $\mathbf{L_2}, \mathbf{L_3}$ и $\mathbf{L}_4$ пустые), $e_{10}=6$ (класс $\mathbf{L}_2$ пустой), а при $j>1$ $e_{j,0}=7$. Аналогично $e_{n-1,j+1}=7$ ($j=0,1,\ldots,n-2$). Тогда верхние оценки по псевдоравенству $H_{\leftarrow}(n)=$ $=\max(]\log_2 e_{j,0}[)=H_{\rightarrow}(n)=\max(]\log_2 e_{j,0}[)=3$ и не зависят от n, что свидетельствует о принципиальной возможности реализации на ОККМ операции деления на 2 в кольце неотрицательных вычетов.

Для получения верхних оценок по одностороннему доопределению используем **Алгоритм 2**. Легко убедиться, что при $j>1$ векторы из класса $\mathbf{L}_1$ поглощаются векторами из любого иного класса, векторы из класса $\mathbf{L}_3$ поглощаются векторами из класса $\mathbf{L}_2$, векторы из класса $\mathbf{L}_5$ — векторами из класса $\mathbf{L}_4$, а векторы из класса $\mathbf{L}_7$ — векторами из класса $\mathbf{L}_6$. В соответствии с **Алгоритмом 2** не вычеркнутыми останутся классы $\mathbf{L}_2$, $\mathbf{L}_4$ и $\mathbf{L}_6$, т.е. $e_{j,0}=3$. При $j=1$ не вычеркнутыми останутся классы $\mathbf{L}_2$, $\mathbf{L}_4$ и $\mathbf{L}_7$, т.е. $e_{j,0}=3$. При $j=0$ не вычеркнутыми останутся классы $\mathbf{L}_5$ и $\mathbf{L}_6$, т.е. $e_{j,0}=2$. Следовательно, $O_{\leftarrow}(n)=2$. Аналогично векторы из класса $\mathbf{H}_1$ поглощаются векторами из любого иного класса, векторы из класса $\mathbf{H}_2$ — векторами из класса $\mathbf{H}_4$, а векторы из класса $\mathbf{H}_3$ — векторами из класса $\mathbf{H}_6$, и не вычеркнутыми останутся классы $\mathbf{H}_4$, $\mathbf{H}_5$, $\mathbf{H}_6$ и $\mathbf{H}_7$, т.е. $e_{n-1,j+1}\le 4$ и $O_{\rightarrow}(n)=2$. Следовательно, рассматриваемая массовая операция реализуема на ОККМ с $r=2$. Легко проверить, что любые два вектора, взятые из различных классов $\mathbf{L}_2$, $\mathbf{L}_4$ и $\mathbf{L}_6$, не совместимы, а также любые два вектора, взятые из различных классов $\mathbf{H}_4$, $\mathbf{H}_5$, $\mathbf{H}_6$ и $\mathbf{H}_7$, не совместимы. Следовательно, в соответствии с **Утверждениями 4 и 5** приведенная оценка количества боковых выводов модулей ОККМ, реализующего операцию деления на 2 в кольце неотрицательных вычетов, является не только верхней, но и нижней оценкой, т.е. не существует доопределений булевых функций из кортежа $F(X,P)$, при которых $r<2$.

В случае конечных полей характеристики p и $w=1$ порядок поля P — простое число, которое для ОККМ с n КМ должно находиться в диапазоне $2^{n-1}<P<2^n$. Такие ограничения на возможные значения P существенно увеличивают число векторов значений переменных, где функции из $F(X,P)$ не определены, что предположительно может привести к уменьшению полученных оценок. В действительности же изменение оценок не происходит, поскольку при любом конкретном простом P из указанного диапазона всегда существуют значения X, при которых будут выполняться все соотношения, используемые как в определениях классов, так и в определениях значений функций в соответствующих кортежах. Отсюда также следует, что минимальное число боковых выводов модулей по обоим направлениям будет равно двум даже в случае, когда $P=\text{const}$.

В работе [6] показано, что операции $Z=(X+Z)\bmod P$ и $Z=$ $=(X-Z)\bmod P$ в кольце неотрицательных вычетов реализуются на ОККМ со значением $r=2$ при условии конкретного доопределения булевых функций из $F(X,YP)$**,** которое основывалось на следующем доопределении операций — при **любых** X, Y и P в диапазоне от 0 до 2^n-1 в случае сложения $Z=(X+Y)$, если $(X+Y)<P$ и $Z=(X+Y-P)$, если $(X+Y)\ge P$, а в случае вычитания $Z=(X-Y)$, если $X\ge Y$ и $Z=(X-Y+P)$, если $X<Y$.

Согласно изложенному, приведенный в работе [6] результат определяет верхнюю оценку числа боковых выводов модулей ОККМ при реализации операций сложения и вычитания в конечных полях характеристики $p>2$ при $w=1$. В конечных полях функции из $F(X,YP)$ определены на наборах аргументов, соответствующих простым значениям P в диапазоне $2^{n-1}<P<2^n$, а также значениям $X, Y<P$. В связи с этим актуальным является доказательство существования (или отсутствия) доопределений функций из $F(X,YP)$, позволяющих уменьшить эту оценку. Для доказательства воспользуемся **Алгоритмом 2**. Легко проверить, что множество векторов $Q_{j,0}$ разбивается на следующие классы эквивалентности по отношению псевдоравенства:

Класс $\mathbf{L}_1$, где значение $P_{j,0}$ не является остатком от деления простых P из заданного диапазона значений на 2^{j+1}. Функции из кортежей $F_{n-1,j+1}(U_{n-1,j+1},q_{j,0})$, где $q_{j,0}\in\mathbf{L}_1$ не определены на всех значениях аргументов.

Класс $\mathbf{L}_2$, где $X_{j,0}+Y_{j,0}<P_{j,0}$.

Класс $\mathbf{L}_3$, где $P_{j,0}\le X_{j,0}+Y_{j,0}<2^{j+1}$, $X_{j,0}<P_{j,0}$, $Y_{j,0}<P_{j,0}$.

Класс $\mathbf{L}_4$, где $P_{j,0}\le X_{j,0}+Y_{j,0}<2^{j+1}$, $X_{j,0}\ge P_{j,0}$, $Y_{j,0}<P_{j,0}$.

Класс $\mathbf{L}_5$, где $P_{j,0}\le X_{j,0}+Y_{j,0}<2^{j+1}$, $X_{j,0}<P_{j,0}$, $Y_{j,0}\ge P_{j,0}$.

Класс $\mathbf{L}_6$, где $P_{j,0}\le X_{j,0}+Y_{j,0}<2^{j+1}$, $X_{j,0}\ge P_{j,0}$, $Y_{j,0}\ge P_{j,0}$.

Класс $\mathbf{L}_7$, где $2^{j+1}\le X_{j,0}+Y_{j,0}<2^{j+1}+P_{j,0}$, $X_{j,0}<P_{j,0}$, $Y_{j,0}<P_{j,0}$.

Класс $\mathbf{L}_8$, где $2^{j+1}\le X_{j,0}+Y_{j,0}<2^{j+1}+P_{j,0}$, $X_{j,0}\ge P_{j,0}$, $Y_{j,0}<P_{j,0}$.

Класс $\mathbf{L}_9$, где $2^{j+1}\le X_{j,0}+Y_{j,0}<2^{j+1}+P_{j,0}$, $X_{j,0}<P_{j,0}$, $Y_{j,0}\ge P_{j,0}$.

Класс $\mathbf{L}_{10}$, где $2^{j+1}\le X_{j,0}+Y_{j,0}<2^{j+1}+P_{j,0}$, $X_{j,0}\ge P_{j,0}$, $Y_{j,0}\ge P_{j,0}$.

Класс $\mathbf{L}_{11}$, где $2^{j+1}+P_{j,0}\le X_{j,0}+Y_{j,0}$.

Множество векторов $Q_{n-1,j+1}$ разбивается на следующие классы эквивалентности по отношению псевдоравенства:

Класс $\mathbf{H}_1$, где значение $P_{n-1,j+1}$ не является частным от деления простых P из заданного диапазона значений на 2^{j+1}. Функции из кортежей

$F_{j,0}(q_{n-1,j+1}, U_{j,0})$, где $q_{n-1,j+1} \in H_1$ не определены на всех значениях аргументов.

Класс $\mathbf{H}_2$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} < P_{n-1,j+1} - 1$.

Класс $\mathbf{H}_3$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} = P_{n-1,j+1} - 1$.

Класс $\mathbf{H}_4$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} = P_{n-1,j+1}$, $X_{n-1,j+1} < P_{n-1,j+1}$, $Y_{(n-1),(j+1)} < P_{n-1,j+1}$.

Класс $\mathbf{H}_5$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} = P_{n-1,j+1}$, $X_{n-1,j+1} = P_{n-1,j+1}$, $Y_{(n-1),(j+1)} = 0$.

Класс $\mathbf{H}_6$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} = P_{n-1,j+1}$, $X_{n-1,j+1} = 0$, $Y_{(n-1),(j+1)} = P_{n-1,j+1}$.

Класс $\mathbf{H}_7$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} > P_{n-1,j+1}$, $X_{n-1,j+1} < P_{n-1,j+1}$, $Y_{(n-1),(j+1)} < P_{n-1,j+1}$.

Класс $\mathbf{H}_8$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} > P_{n-1,j+1}$, $X_{n-1,j+1} = P_{n-1,j+1}$, $Y_{(n-1),(j+1)} < P_{n-1,j+1}$.

Класс $\mathbf{H}_9$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} > P_{n-1,j+1}$, $X_{n-1,j+1} < P_{n-1,j+1}$, $Y_{(n-1),(j+1)} = P_{n-1,j+1}$.

Класс $\mathbf{H}_{10}$, где $X_{n-1,j+1} + Y_{(n-1),(j+1)} > P_{n-1,j+1}$, $X_{n-1,j+1} = P_{n-1,j+1}$, $Y_{(n-1),(j+1)} = P_{n-1,j+1}$.

При $j < 0$ векторы из класса $\mathbf{L}_1$ поглощаются векторами из любого иного класса, векторы из классов $\mathbf{L}_4$, $\mathbf{L}_5$ и $\mathbf{L}_6$ поглощаются векторами из класса $\mathbf{L}_3$, векторы из классов $\mathbf{L}_8$, $\mathbf{L}_9$ и $\mathbf{L}_{10}$ — векторами из класса $\mathbf{L}_7$. Не вычеркнутыми останутся классы $\mathbf{L}_2$, $\mathbf{L}_3$, $\mathbf{L}_7$ и $\mathbf{L}_{11}$ т.е. $e_{j,0} = 4$.

При $j = 0$ классы $\mathbf{L}_3$, $\mathbf{L}_6$, $\mathbf{L}_7$, $\mathbf{L}_8$ и $\mathbf{L}_9$ пустые, векторы из класса $\mathbf{L}_1$ поглощаются, т.е. $e_{0,0}$ также равно 4. Следовательно $O_{\leftarrow}(n) = 2$.

При $j < n-2$ векторы из класса $\mathbf{H}_1$ поглощаются векторами из любого иного класса, векторы из классов $\mathbf{H}_5$ и $\mathbf{H}_6$ — векторами из класса $\mathbf{H}_4$, векторы из классов $\mathbf{H}_8$, $\mathbf{H}_9$ и $\mathbf{H}_{10}$ — векторами из класса $\mathbf{H}_7$. Не вычеркнутыми останутся классы $\mathbf{H}_2$, $\mathbf{H}_3$, $\mathbf{H}_4$ и $\mathbf{H}_7$, т.е. $e_{n-1,j+1} = 4$.

При $j = n-2$ классы $\mathbf{H}_2$, $\mathbf{H}_4$, $\mathbf{H}_7$, $\mathbf{H}_8$ и $\mathbf{H}_9$ пустые, а векторы из класса $\mathbf{H}_1$ поглощаются, т.е. $e_{n-1,n-1}$ также равно 4. Следовательно, $O_{\rightarrow}(n) = 2$.

Легко убедиться, что любые два вектора, взятые из различных классов $\mathbf{L}_2$, $\mathbf{L}_3$, $\mathbf{L}_7$ и $\mathbf{L}_{11}$ при $j > 0$ не совместимы, а также любые два вектора, взятые из различных классов $\mathbf{H}_2$, $\mathbf{H}_3$, $\mathbf{H}_4$ и $\mathbf{H}_7$ не совместимы. Следовательно, согласно **Утверждениям 4 и 5**, приведенные оценки количества боковых выводов модулей являются не только верхними, но и нижними оценками.

Поэтому при реализации на ОККМ операции $Z=(X+Y) \bmod P$ в конечных полях характеристики $p>2$ при $w=1$ не существует доопределений функций из $F(X,YP)$, при которых $r<2$. Это же касается и случая $P=\text{const}$. В то же время вследствие большого числа вариантов поглощения векторов из классов $\mathbf{L}_1$ и $\mathbf{H}_1$ в соответствии с **Алгоритмом 3** существует много вариантов доопределения функций из $F(X,YP)$, обеспечивающих $r=2$, что может служить источником дальнейшей оптимизации по другим критериям.

Аналогичные результаты можно получить и для операции $Z=$ $=(X-Y) \bmod P$.

В работе [6] рассмотрена также реализация операции умножения $Z=(X*Y) \bmod P$ на основе ОККМ, реализующих операции $Z=$ $=(X+Y) \bmod P$ и $Z=(2*X) \bmod P$. Альтернативным методом реализации операции $Z=(X*Y) \bmod P$ является метод, базирующийся на операции $Z=(2*X+Y) \bmod P$.

Воспользовавшись **Алгоритмом 2**, можно установить следующее. Число классов разбиения множества векторов $Q_{j,0}$ по отношению псевдоравенства при любом $j=0,1,...,n-2$ не превышает 22, а число классов, оставшихся не вычеркнутыми, не превышает 12 ($e_{j,0} \le 12$). При всех значениях j, где $e_{j,0}=12$, векторы, входящие в любые два не вычеркнутые классы не совместимы. Отсюда следует, что $H_{\leftarrow}(n)=\max(]\log_2 e_{j,0}[)=L_{\leftarrow}(n)=4$. Аналогично число классов разбиения множества векторов $Q_{n-1,j+1}$ по отношению псевдоравенства при любом $j=0,1,...,n-2$ не превышает 20, а число классов, оставшихся не вычеркнутыми, не превышает 10 ($e_{n-1,j+1} \le 10$). При всех значениях j, где $e_{n-1,j+1}=10$, векторы, входящие в любые два не вычеркнутые класса, не совместимы. Отсюда следует, что $H_{\rightarrow}(n)=$ $=\max(]\log_2 e_{n-1,j+1}[)=L_{\rightarrow}(n)=4$. Это позволяет утверждать, что массовая операция $Z=(2*X+Y) \bmod P$ в конечных полях характеристики $p>2$ при $w=1$ реализуема на ОККМ со значением $r=4$, причем не существует доопределений функций из $F(X,YP)$, позволяющих уменьшить значение r.

ВЫВОДЫ

Предложенные выше методика и алгоритмы совместной разделительной декомпозиции систем частично определенных булевых функций позволяют сформировать нижние и верхние оценки числа боковых выводов модулей ОККМ. Эти оценки определяют возможность реализации операций в конечных полях на ОККМ с заданными конструктивными ограничениями относительно их числа входов – выходов. Для массовых операций рассмотренная методика позволяет аналитическим путем (даже без использования компьютерных средств) определять возможность их реализации как комбинацион-

ных схем линейной сложности, и тем самым обеспечивать свойство наращиваемости структур, выполненных как ОККМ. Теоретические выкладки подтверждены конкретными примерами реализации массовых операций в конечных полях на ОККМ. Полученные результаты могут быть использованы при реализации любых преобразований $Z = F(X_1, X_2, ..., X_m)$, в которых все разряды значений не определены на подмножестве значений аргументов.

Рассмотренный конструктивный алгоритм определения внутренних структур отдельных КМ обусловливает возможность дальнейших исследований по их оптимизации относительно критериев сложности или быстродействия.

ЛИТЕРАТУРА

1. *Березовский А.И., Задирака В.К., Шевчук Л.Б.* О тестировании быстродействия алгоритмов и программ вычисления основных операций несимметричной криптографии // Кибернетика и системный анализ. — 1999. — № 5. — С. 59–66.
2. *Палагин А.В., Опанасенко В.Н., Сахарин В.Г.* Особенности проектирования цифровых устройств на современных кристаллах ПЛИС фирмы Xilinx // Проблемы управления и информатики. — 2001. — № 1 — С. 105–119.
3. *Тесленко А.К.* Совместная декомпозиция логических функций // Вестник Киевского политехн. ин-та. Серия автоматики и электроприборостроения. — 1975. — Вып.12. — С. 59–61.
4. *Корнейчук В.И., Тарасенко В.П., Тесленко А.К.* Исследование сложности реализации функций на одномерном каскаде модулей // Автоматика и вычислительная техника. — 1977. — № 5. — С. 5–11.
5. *Журавлев Ю.И.* Алгоритмы построения минимальных дизъюнктивных нормальных форм для функций алгебры логики // В кн.: Дискретная математика и математические вопросы кибернетики. Т.1. — М.: Наука, 1974. — С. 67–97.
6. *Тарасенко В.П., Тесленко А.К.* Реализация основных арифметических операций над остатками на одномерных каскадах конструктивных модулей // УСиМ. — 2003. — № 3 (185) — С. 29–42.

Поступила 15. 06. 2005