МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Факультет
вычислительной математики
и кибернетики

ТРУДЫ

VIII МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ

«ДИСКРЕТНЫЕ МОДЕЛИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ»

Москва

6–9 апреля 2009 г.

МОСКВА

2009

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Факультет вычислительной математики и кибернетики

ТРУДЫ

VIII МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ

«ДИСКРЕТНЫЕ МОДЕЛИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ»

Москва

6–9 апреля 2009 г.

МАКС ПРЕСС

МОСКВА – 2009

УДК 510.5+519.71
ББК 22.12:22.18
Д48

Печатается по решению Редакционно-издательского совета факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова

Отв. ред. *В.Б. Алексеев, В.А. Захаров*

Д48 **Дискретные модели в теории управляющих систем:** VIII Международная конференция. Москва, 6–9 апреля 2009 г.: Труды/ Отв. ред. В.Б. Алексеев, В.А. Захаров. – М.: Издательский отдел факультета ВМиК МГУ им. М.В. Ломоносова (лицензия ИД N 05899 от 24.09.2001 г.); МАКС Пресс, 2009. – 380 с.
ISBN 978-5-89407-366-8
ISBN 978-5-317-02847-3

В сборнике представлены труды VIII Международной конференции «Дискретные модели в теории управляющих систем», проведенной факультетом ВМК Московского государственного университета имени М.В. Ломоносова. Тематика конференции включает вопросы теории функциональных систем, теории синтеза и анализа управляющих систем, теории графов, теории сложности вычислений, теории кодирования, теории автоматов, криптографии, математической логики, теории программирования, гибридного математического моделирования.

Конференция организована кафедрой математической кибернетики факультета ВМК МГУ имени М.В. Ломоносова при финансовой поддержке Российского Фонда Фундаментальных исследований (грант 09-01-06017).

УДК 510.5+519.71
ББК 22.12:22.18

ISBN 978-5-89407-366-8
ISBN 978-5-317-02847-3

Модулярные числовые формы систем логических функций

О. А. Финько*

г. Краснодар

1. Массовый характер использования криптографических систем защиты информации (КСЗИ) в последние десятилетия привел к пересмотру требований к показателям качества КСЗИ. Достигнуты значительные успехи в достижении необходимой криптографической стойкости шифров. Однако, эволюционные изменения условий и характера применения КСЗИ привели к повышению требований к *скорости*, *гибкости* и *достоверности* реализации шифров. Пока не существует единых методов, обеспечивающих выполнение предъявляемых к КСЗИ требований *совместно* (эффективно).

В настоящее время основная «тяжесть» поиска компромиссного решения ложится на разработчиков шифров. Их задача состоит в получении таких свойств шифров, которые обеспечили бы необходимое сочетание требуемых характеристик при различных условиях их технической реализации (программном и аппаратном). Разработчик при этом жестко ограничен узким перечнем эффективно реализуемых на современных ЭВМ операций (как правило сдвиги, перестановки, конкатенации, подстановки малой размерности, операции по модулю 2^i и $2^i \pm 1$ и др.).

Ценой такого компромисса является *усреднение* различных показателей качества, то есть некоторое ухудшение каждого из них в различной пропорции. Многие шифры, имеющие преимущества по основному показателю — криптостойкости, невостребованы из-за неприемлемого уровня других технических (сервисных) показателей.

Один из основополагающих путей оптимизации криптоалгоритмов — совершенствование методов реализации криптографических функций (рис. 1). Этот путь более универсален, так как *расширяет классы* эффективно реализуемых шифров.

На наш взгляд причины несовершенства существующих методов реализации логических вычислений следует искать в *несогласованности* методов реализации криптографических операций (будем рассматривать только логические операции и другие операции, которые с известной долей условности можно привести к таковым), с принципами построения и тенденциями развития существующей вычислительной техники. Парадоксальность сложившейся ситуации заключается в том, что в основе построения всей вычислительной техники лежат те же законы алгебры логики,

*ofinko@yandex.ru; http://www.mathnet.ru/rus/person/40004

которые с помощью этой техники не удается эффективно реализовать. Исторически сложилось, что «сильные» возможности современной вычислительной техники лежат в области арифметических вычислений (операции выполняются одновременно над *группой* бит). Напротив — произвольные логические вычисления выполняются *побитно*. Таким образом в настоящее время потенциальные возможности современных вычислительных средств (в том числе специализированных) остаются *нераскрытыми*.

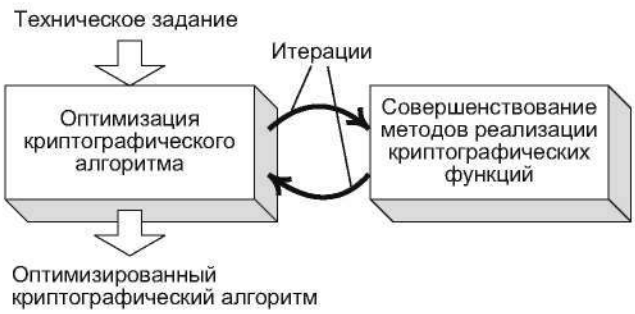

Рис. 1: Оптимизация криптографических алгоритмов на основе совершенствования методов реализации криптографических функций

В данной работе мы будем использовать *арифметические* операции (сильную сторону) для реализации *параллельных логических вычислений*. Это позволит задействовать известные эффективные методы *контроля* ошибок вычислений (функционального диагностирования) и обеспечения *отказоустойчивости* средств вычислений, основанные на избыточных арифметических кодах.

Ключевые результаты в этом направлении получены в [5]. Кратко рассмотрим эти положения и, затем, изложим существо метода [6, 7], позволяющего получить качественно более высокий уровень параллелизма и достоверности реализации произвольных логических криптографических функций.

2. Рассмотрим отображение классической алгебры логики на арифметику кольца целых чисел [5].

Синтез полиномиальных форм булевых функций. Пусть $y_i = f_i(X)$ — i-я булева функция (БФ) n переменных $X = x_1, x_2, \ldots, x_n$; y_i — значение, принимаемое БФ $f_i(X)$. Тогда имеет место единственное представление $f_i(X)$ арифметическим полиномом (АП) [5]:

$$y_i = P_i(X) = \sum_{j=0}^{2^n-1} p_{i,j}\, x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}, \tag{1}$$

где $p_{i,j} \in \mathbb{Z}$ $(i = 0, 1, \ldots, 2^n-1)$; $(i_1 i_2 \ldots i_n)_2 = \sum\limits_{u=1}^{n} i_u 2^{n-u}$ $(i_u \in 0, 1)$; $x_u^{i_u} = \begin{cases} x_u, & i_u = 1, \\ 1, & i_u = 0; \end{cases}$ $(i_1 i_2 \ldots i_n)_q$ — числовое представление с основанием q, i_j $(j = 1, \ldots, n)$ — коэффициенты. Дана система БФ:

$$y_1 = f_1(X), \quad y_2 = f_2(X), \quad \ldots, \quad y_d = f_k(X). \tag{2}$$

Пусть $Y = (y_1 y_2 \dots y_k)_2$ — числовое представление значений y_1, y_2, …, y_k. Тогда имеет место единственное представление системы (2) посредством АП [5]:

$$Y = D(X) = \sum_{i=1}^{k} P_i(X) 2^{i-1} = \sum_{i=0}^{2^n-1} d_i \, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \tag{3}$$

где $d_i \in \mathbb{Z}$ ($i = 0, 1, \dots, 2^n - 1$).

Дискретное преобразование Фурье в базисе A_{2^n}.

Пусть $\mathbf{Y}_i = \begin{bmatrix} y_i^{(1)} & y_i^{(1)} & \dots & y_i^{(2^n-1)} \end{bmatrix}^{\mathrm{T}}$ — вектор значений БФ $f_i(X)$ (столбец значений $f_i(X)$ обычной таблицы истинности, T — символ транспонирования). Тогда прямое и обратное логическое дискретное преобразование Фурье (ЛДПФ) в базисе A_{2^n} вектора $\mathbf{Y}_i$ определяется парой отношений [5]:

$$\mathbf{P}_i = \mathbf{A}_{2^n} \mathbf{Y}_i, \tag{4}$$

$$\mathbf{Y}_i = \mathbf{A}_{2^n}^{-1} \mathbf{P}_i, \tag{5}$$

где $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ — соответственно матрицы прямого и инверсного арифметического преобразования размерности $2^n \times 2^n$ (базис преобразования);
$\mathbf{P}_i = \begin{bmatrix} p_{i,0} & p_{i,1} & \dots & p_{i,2^n-1} \end{bmatrix}$ — векторное представление коэффициентов АП (1).

Для системы БФ (1) прямое и обратное ЛДПФ соответственно примет вид[5]:

$$\mathbf{D} = \mathbf{A}_{2^n} \mathbf{Y}, \tag{6}$$

$$\mathbf{Y} = \mathbf{A}_{2^n}^{-1} \mathbf{D}, \tag{7}$$

где $\mathbf{D} = \begin{bmatrix} d_0 & d_1 & \dots & d_{2^n-1} \end{bmatrix}$ — векторное представление коэффициентов АП (3);
$\mathbf{Y} = [\mathbf{Y}_k | \mathbf{Y}_{k-1} | \dots | \mathbf{Y}_1]^{\mathrm{T}} = \left[Y^{(0)} Y^{(1)} \dots Y^{(2^n-1)} \right]^{\mathrm{T}}$, где $Y^{(i)} = (y_{k,i}^{(1)} y_{k-1,i}^{(1)} \dots y_{1,i}^{(2^n-1)})_2$ — числовое значение, принимаемое k-выходной булевой функцией
$f_1(X)$, $f_2(X)$, …, $f_k(X)$ на i-м наборе булевых аргументов таблицы истинности.

В (4) и (6) матрица $\mathbf{A}_{2^n}$ — результат кронекеровского (тензорного) произведения $\mathbf{A}_{2^n} = \bigotimes_{j=1}^{n} \mathbf{A}_1$ базовой матрицы $\mathbf{A}_1 = \left[\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix} \right]$. Соответственно $\mathbf{A}_{2^n}^{-1} = \bigotimes_{j=1}^{n} \mathbf{A}_1^{-1}$, где $\mathbf{A}_1^{-1} = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix} \right]$ — базовая матрица обратного преобразования.

Из структуры матриц $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ следует, что наибольшее абсолютное значение $2^{n-1}(2^d - 1)$ в арифметических представлениях (1) и (3) может принимать 2^n-й коэффициент. Поэтому для двоичного представления d_i ($i = 0, 1, \dots, 2^n$) в (3) потребуется резервирование (с учетом необходимости представления знака числа)

$$\left\lfloor \log(2^{n-1}(2^d - 1)) + 2 \right\rfloor = n + d \tag{8}$$

двоичных разрядов ЭВМ ($\lfloor x \rfloor$ — наибольшее целое, не превосходящее x) [7].

3. Из (8) следует, что существенным недостатком форм (1) и (3) является большая величина целочисленных коэффициентов. Методы модулярной арифметики [1] активно, например, используемые в задачах цифровой обработки сигналов, дают

пример эффективного решения этой проблемы. Используем, также, эти методы для совершенствования матричных форм — ЛДПФ (4)–(7).

Синтез полиномиальных форм булевых функций в кольце $\mathbb{Z}_{2^k}$.

Предложение 1. *Система k БФ (2) может быть единственным образом представлена модулярной полиномиальной формой: [6, 7]:*

$$Y = M(X) = \sum_{i=0}^{2^n-1} \psi_i \, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \quad (\mathbb{Z}_{2^k}), \tag{9}$$

где $\psi_i = \langle d_i \rangle_{2^k}$ $(i = 0, 1, \dots, 2^n - 1)$; здесь запись $(\mathbb{Z}_{2^k})$ указывает (здесь и далее) на то, что вычисление (9) выполняется в кольце $\mathbb{Z}_{2^k}$; $\langle x \rangle_m$ — получение наименьшего неотрицательного вычета от x по модулю m.

Замечание 1. *В общем случае $m \geq 2^d$.*

Свойство 1. *Так как коэффициенты ψ_i $(i = 0, 1, \dots, 2^n - 1)$ полинома $M(X)$ (9) лежат в $0 \leq \psi_i < m$, то для их представления потребуется резервирование $\lceil \log_2 m \rceil$ ($\lceil x \rceil$ — наименьшее целое число, равное или превышающее x) двоичных разрядов ЭВМ или, при $m = 2^d$, d двоичных разрядов, что в $\frac{n}{d} + 1$ раз меньше по сравнению с количеством разрядов (8), необходимых для представления коэффициентов (3).*

Свойство 2. *Если для одной и той же системы БФ заданы два АП $D(X)$ (3) и $M(X)$ (9), а K_1 и K_2 — количество ненулевых членов этих полиномов, то $K_2 \leq K_1$ (за счет сокращения коэффициентов АП (3), кратных m.*

Введение в логические теоретико-числовые преобразования. Логические теоретико-числовые преобразования (ЛТЧП) определим парой отношений [7]:

$$\mathbf{M} = \mathbf{A}_{2^n} \mathbf{Y} \quad (\mathbb{Z}_{2^k}), \tag{10}$$

$$\mathbf{Y} = \mathbf{A}_{2^n}^{-1} \mathbf{M} \quad (\mathbb{Z}_{2^k}), \tag{11}$$

где $\mathbf{M} = \begin{bmatrix} \psi_0 & \psi_1 & \dots & \psi_{2^n-1} \end{bmatrix}$ — векторное представление коэффициентов АП (3); матрицы $\mathbf{Y}$, $\mathbf{A}_{2^n}$ и $\mathbf{A}_{2^n}^{-1}$ определены ранее. Запись $(\mathbb{Z}_{2^k})$ означает, что арифметические операции, используемые при произведении матриц, выполняются в кольце $\mathbb{Z}_{2^k}$.

К ЛТЧП (10), (11) применимы замечание 1 и свойство 1.

4. Совершенствование средств криптоанализа требует постоянного усложнения шифров. Для эффективного решения задач большой размерности необходимы параллельные методы вычислений.

Синтез многомерных полиномиальных форм в кольце $\mathbb{Z}_{m_1, m_2, \dots, m_v}$.

Предложение 2. *Пусть $m > 2^n$, причем $m = \prod_{i=1}^{v}$ и $\gcd(m_i, m_j) = 1$ $(i, j = 1, 2, \dots, v;\ i \neq j)$, система k БФ (2) может быть единственным образом пред-*

ставлена системой модулярных форм АП [7]:

$$\begin{cases} \phi_1 = \mu_1(X) = \sum\limits_{i=0}^{2^n-1} \psi_{i,1}\, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \quad (\mathbb{Z}_{m_1}), \\ \phi_2 = \mu_2(X) = \sum\limits_{i=0}^{2^n-1} \psi_{i,2}\, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \quad (\mathbb{Z}_{m_2}), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \phi_v = \mu_2(X) = \sum\limits_{i=0}^{2^n-1} \psi_{i,v}\, x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \quad (\mathbb{Z}_{m_v}), \end{cases} \tag{12}$$

где $\psi_{i,j} = \langle d_i \rangle_{2^k}$ $(i = 0, 1, \dots, 2^n{-}1;\ j = 1, 2, \dots, v)$*; причем* $Y = \mathrm{CRT}(\phi_1, \phi_2, \dots, \phi_v)$*, где данная запись (от — Chinese remainder theorem) означает нахождение решения системы уравнений (12) с помощью Китайской теоремы об остатках.*

Многомерные логические теоретико-числовые преобразования. Многомерные ЛТЧП определим парой систем отношений [7]:

$$\begin{cases} \boldsymbol{\Psi}_1 = \mathbf{A}_{2^n} \boldsymbol{\Phi}_1 \quad (\mathbb{Z}_{m_1}), \\ \boldsymbol{\Psi}_2 = \mathbf{A}_{2^n} \boldsymbol{\Phi}_2 \quad (\mathbb{Z}_{m_2}), \\ \dots\dots\dots\dots\dots \\ \boldsymbol{\Psi}_v = \mathbf{A}_{2^n} \boldsymbol{\Phi}_v \quad (\mathbb{Z}_{m_v}); \end{cases} \quad \begin{cases} \boldsymbol{\Phi}_1 = \mathbf{A}_{2^n} \boldsymbol{\Psi}_1 \quad (\mathbb{Z}_{m_1}), \\ \boldsymbol{\Phi}_2 = \mathbf{A}_{2^n} \boldsymbol{\Psi}_2 \quad (\mathbb{Z}_{m_2}), \\ \dots\dots\dots\dots\dots \\ \boldsymbol{\Phi}_v = \mathbf{A}_{2^n} \boldsymbol{\Psi}_v \quad (\mathbb{Z}_{m_v}) \end{cases} \tag{13}$$

где

$$\boldsymbol{\Phi}_i = \begin{bmatrix} \phi_{0,i} & \phi_{1,i} & \dots & \phi_{2^n-1,i} \end{bmatrix}^{\mathrm{T}}; \quad \phi_{j,i} = \left\langle Y^{(j)} \right\rangle_{m_i}; \quad i = 1, \dots, v;$$
$$\boldsymbol{\Psi}_i = \begin{bmatrix} \psi_{0,i} & \psi_{1,i} & \dots & \psi_{2^n-1,i} \end{bmatrix}; \quad i = 1, \dots, v.$$

5. Отображение алгебры логики на модулярную арифметику открывает пути к обобщению имеющихся возможностей по контролю модулярных вычислений и построению отказоустойчивых модулярных структур на область логических вычислений.

Контроль ошибок. Расширим системы АП (12) и матричных преобразований (13), введя избыточные модули $m_{v+1}, \dots, m_{v+r}$, такие, что $m_1 < \dots < m_v < \dots < m_{v+r}$ и $\gcd(m_i, m_j) = 1$ $(i, j = 1, 2, \dots, v + r;\ i \neq j)$. Тогда получаемые в результате вычисления указанных форм наименьшие неотрицательные вычеты
$\{Y\} = (\phi_1, \dots, \phi_v, \dots, \phi_{v+r})$ составят расширенный модулярный код (R-код), обладающий свойствами обнаружения и исправления ошибок [1]. Так как используемая система модулей упорядочена по величине, для восстановления числа Y по вычетам $(\phi_1, \dots, \phi_v, \dots, \phi_{v+r})$ достаточно знать любые v вычетов.

Отказоустойчивые структуры. В отличие от канала связи вычислительную систему (ВС) возможно реконфигурировать таким образом, чтобы временно вывести

из ее состава часть оборудования, в котором обнаружен отказ. Уникальной особенностью ВС, функционирующих в R-кодах, является отсутствие разделения вычислительных каналов на информационные и контрольные (рис. 2). По мере деградации такой ВС из ее состава может быть выведено до $r-1$ вычислительных каналов, соответствующих любым модулям. Более того, возможно продолжение функционирования ВС даже после выхода из строя r и более вычислительных каналов. В этом случае возможен обмен между уровнем производительности ВС и точностью вычислений. Таким образом речь идет о повышенной живучести ВС. В пределе ВС продолжит вычисления даже при наличии одного исправного вычислительного канала, который будет последовательно отрабатывать задания по заданной системе модулей и алгоритм реализации Китайской теоремы об остатках.

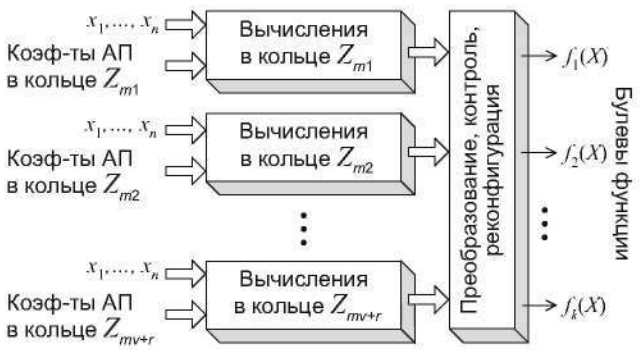

Рис. 2: Структура отказоустойчивого модулярного параллельного вычислителя логических функций

6. Арифметико-логические формы расширяют инструментарий разработчиков (рис. 1) в решении трудной задачи создания эффективных криптоалгоритмов. Модулярные арифметико-логические формы, позволяют адаптировать высокоразвитый математический аппарат и высокопроизводительные, отказоустойчивые технические средства цифровой обработки сигналов, основанные на методах модулярной арифметики [1], для реализации параллельных гибких достоверных вычислений логических криптографических функций. Простота проектирования и существенные преимущества (по объему — на порядки) модулярных табличных операционных устройств делает перспективным создание эффективных криптопроцессоров на основе ПЛИС.

Совмещение достоинств программной (гибкой) и аппаратной (интенсивной, достоверной) реализации криптоалгоритмов позволяет, например, создавать:

- многоканальные *однопроцессорные* криптоускорители, обеспечивающие параллельную реализацию разных криптоалгоритмов;
- типовые криптопроцессоры, в которых конкретный криптоалгоритм закладывается (путем загрузки массива коэффициентов АП) непосредственно при введении их в эксплуатацию или легко модернизируется (модифицируется) в процессе эксплуатации;
- мобильные защищенные средства связи, функционирующие в *независимых* сетях связи, использующих *разные* криптоалгоритмы (данные о криптоалгоритме передается по каналу связи в закрытом или открытом виде).

Важной задачей криптологии является решение задач *криптоанализа* с высокой *точностью*. Известно, что результат решения систем линейных уравнений числен-

ными точными методами может отличаться от истинного на порядки [2]. Создание модулярных арифметико-логических форм делает возможным построение высокопроизводительных и отказоустойчивых средств криптоанализа на основе локальных вычислительных сетей, ЭВМ которых функционируют по заданным значениям модулей. Пример такой вычислительной сети приведен в [3]. Изучению модулярных ВС, функционирующих в больших и сверхбольших числовых диапазонах, посвящены работы [4].

Обобщение числовых представлений на область k-значных функций дано в [8].

Список литературы

[1] *Амербаев В. М.* Теоретические основы машинной арифметики. — Алма-Ата: Наука, 1976. — 324 с.

[2] *Грегори Р., Кришнамурти Е.* Безошибочные вычисления. Методы и приложения. — М.: Мир, 1988. — 207 с.

[3] *Дзегеленок И. И., Оцоков Ш. А.* О распараллеливании безошибочных вычислений на ПМК-сети «Курс-2000»// Вычислительные сети. — 2003. — № 1.

[4] *Инютин С. А.* Параллельные вычисления в сверхбольших компьютерных диапазонах// Тр. Междунар. конф. «Параллельные вычисления и задачи управления» (PACO-2001) (CD). — М.: ИПУ РАН, 2001. — С. 76–87.

[5] *Малюгин В. Д.* Параллельные логические вычисления посредством арифметических полиномов. — М.: Наука. Физматлит, 1997.

[6] *Финько О. А.* Вариант классификации арифметических форм представления логических функций//Тр. XIV Междунар. школы-семинара «Синтез и сложность управляющих систем»./ Под ред. О. Б. Лупанова. — Н. Новгород: Изд-во Нижегород. пед. ун-та, 2003. — С. 83–84.

[7] *Финько О. А.* Реализация систем булевых функций большой размерности методами модулярной арифметики// Автоматика и телемеханика. — 2004. — № 6. — С. 37–60.

[8] *Финько О. А.* Модулярные формы k-значных функций алгебры логики// Автоматика и телемеханика. — 2005. — № 7.