СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.391

С.Г. РАССОМАХИН, д-р техн. наук

БИБЛИОТЕКА МАЛЫХ АНАЛИТИЧЕСКИХ МОДЕЛЕЙ ТИПОВЫХ ПРЕОБРАЗОВАНИЙ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ И КОММУНИКАЦИОННЫХ ПРОТОКОЛОВ

Введение

Имитационное числовое моделирование - один из основных математических инструментов для исследования перспективных способов построения криптографических алгоритмов, реализации операций криптографического анализа, элементов криптографических и телекоммуникационных протоколов.

Продуктивность исследований напрямую зависит от вычислительной эффективности моделей, которая, в основном, связана с количеством элементарных арифметических операций, необходимых для реализации алгоритма, а также с требуемым объемом памяти [1]. Немаловажным является правильный выбор прикладных программ и языка для построения моделей. При этом результат выбора является решением компромиссной проблемы между технологичностью пакета моделирования – гибкостью, приспособленностью для оперативных модификаций и быстротой вычислений. Скорость вычислений является доминирующим требованием при решении типовых задач криптологии, связанных с реализацией переборных алгоритмов в моделях, обладающих экспоненциальной или высокой полиномиальной вычислительной сложностью. Наибольшим быстродействием обладают модели, реализованные с помощью машинно-ориентированных языков и систем программирования и позволяющие осуществлять операции прямого управления памятью на уровне отдельных битов, байтов и машинных слов. Однако существенный дискомфорт создает отсутствие интеллектуальной среды разработчика, длительность рутинной процедуры редактирования, оптимизации, компоновки и отладки программ [2]. Ассемблерные программные модели наиболее подходят для конечной реализации готовых алгоритмов, построение и отладка которых предварительно осуществлены с использованием прикладных пакетов и языков высокого уровня.

Проведенный анализ и опыт построения моделей криптографических примитивов показал, что наибольшей приспособленностью и эффективностью для оперативного создания и исследования прикладных моделей обладают приложения, реализующие концепцию WYSIWYG (What You See Is What You Get – что вы видите, то и получите). Естественность математического языка, комфортный сервис редактирования и отладки, лаконичность громоздких моделей при замене двоичных массивов и векторно-матричных операций (данных) набором элементов рассматриваемой ниже библиотеки, основанной на элементарных арифметических действиях, – вот далеко не полный перечень аргументов в пользу инструментальной среды, предоставляемой приложением Mathcad [3] и некоммерческими аналогами Scilab, SMath Studio [4]. Построение моделей с использованием разработанных аналитических описаний обеспечивает повышение быстроты вычислений при минимизации необходимой памяти. Оперативность разработки и гибкость аналитических моделей особенно полезна при исследованиях уменьшенных (мини) моделей криптографических преобразований [5]. Описываемый методологический подход позволяет повысить вычислительную эффективность моделирования и, кроме того, компенсировать недостаток программы Mathcad – отсутствие библиотек функций работы с представлением данных в двоичном виде или в цифровых формах систем счисления с произвольным основанием. Устранение данного недостатка особенно актуально при моделировании операций в конечных полях $GF\left(p^q\right)$ типичных для криптографических и телекоммуникационных приложений.

Цель работы - описание методологии аналитического моделирования и отдельных примеров мини-моделей типовых логических и структурных векторных преобразований, основанных на замене матричных операций и операций над массивами данных, представленных в произвольной системе счисления, простыми арифметическими действиями над целыми вещественными числами.

1. Разработка типовых элементов библиотеки аналитических функциональных преобразований

1.1. Общие требования к методологии целочисленного аналитического моделирования.

Основой для создания каждого из элементов библиотеки аналитических преобразований является словесная формулировка рассматриваемого процесса или задачи. Конечной целью каждой мини-модели является получение одного компактного математического выражения, реализующего групповые или поэлементные операции над элементами массивов данных. При этом сами массивы (векторы) должны быть заменены целочисленным эквивалентом. Общие требования к реализуемым аналитическим мини-моделям составляет следующий перечень ограничений на допустимое содержимое:

– стандартные алгебраические операции (сложение, вычитание, умножение, деление, возведение в степень), логарифм и экспонента;

– операции округления (отбрасывания дробной части);

– вычисления по произвольному модулю;

– параметризованные суммы $\sum_{i=a}^{b}(\cdots)$ и произведения $\prod_{j=a}^{b}(\cdots)$;

– формулы сумм элементов стандартных числовых рядов;

– тригонометрические и обратные к ним функции.

В качестве аргументов мини-моделей допустимо применение простых переменных, принимающих вещественные, целые или комплексные значения. Не рекомендуется использовать элементы языка алгоритмов и UML-диаграмм, то есть нельзя строить модель в виде вычислительного алгоритма (использование элементарных и комбинированных функций алгебры логики, циклов, проверки условий и ветвлений запрещено). Указанные требования сформулированы для обеспечения компактности и быстродействия аналитических моделей и их пригодности для конечной реализации в виде подключаемых ассемблерных модулей с минимальным количеством вычислений.

1.2. Примеры реализации элементов библиотеки аналитических мини-моделей.

В рассматриваемых ниже примерах реализации аналитических целочисленных мини-моделей использованы следующие обозначения:

– $X, X1, \ldots, XN$ – (прописные литеры с цифрами) –входные целочисленные аргументы;

– $a, b, \ldots, z$ – (строчные литеры) – параметры функций преобразования;

– $Y[X1, \ldots a, \ldots]$ $Y[X1, \ldots a, \ldots]$ – целочисленный результат преобразования;

– $\lfloor \cdots \rfloor$, $\lceil \ldots \rceil$ – вычисление результата округлением до целого значения «вниз» и «вверх»;

– $(X) \bmod (Q)$ – вычисление X по модулю Q, где X, Q – целые вещественные аргументы;

Циклическая перестановка (сдвиг) вправо. Результат Y является целочисленным представлением состояния цифровой последовательности в системе счисления с основанием Q, заданной числовым эквивалентом X, после циклического сдвига вправо на m позиций:

$$Y[X,Q,m,n]=\left\lfloor X\cdot Q^{-m}\right\rfloor\left(1-Q^{n}\right)+X\cdot Q^{n-m}. \quad (1)$$

В данном выражении сдвиг вправо цифр числа реализован арифметическим делением на Q^m, а циклическое дополнение – сдвигом влево и суммированием. Параметр n обозначает разрядность Q-го представления X, которая задается входным параметром преобразования, либо вычисляется $n=\left\lceil \log_Q X\right\rceil$. Модель (1) при $Q=2$ эквивалентна m-кратному применению однотактной ассемблерной команды ROR для целого беззнакового операнда X.

Проведем оценку достоинств аналитических мини-моделей на первом рассмотренном примере. Вычислительная эффективность Mathcad-реализации аналитической мини-модели (1) может быть оценена сопоставлением с традиционным способом организации модификации значений координат Q-ичного n-элементного вектора при циклическом сдвиге через переменную переноса. В этом случае при единичном сдвиге требуется $(n+1)$ операций пересылки (присвоения) значений целочисленных координат и управление атрибутами цикла (счетчиком и процедурой ветвления по условию) после каждого присвоения. Вычислительную сложность данного процесса приближенно можно охарактеризовать количеством операций $\approx 3m(n+1)$. Модель (1) требует три операции взведения целого числа в целую степень, два умножения целых чисел на целую степень основания системы счисления, эквивалентных арифметическому сдвигу, а также две операции сложения. Примерное число эквивалентных операций с учетом коэффициента сложности мини-модели (1) составляет $\approx(5+n)$. При $n>>1$ оценка выигрыша по сокращению числа элементарных операций составляет $\approx 3m$ раз. Безусловно, данная оценка является достаточно грубой, так как на вычислительную эффективность влияет большое количество дополнительных факторов, однако порядок оценки выигрыша вполне корректен. Модель (1) по сравнению с традиционным алгоритмом, кроме того, обеспечивает выигрыш по уменьшению объема задействованной памяти, величина которого пропорциональна разрядности n. Все последующие примеры реализации аналитических мини-моделей приведены без подробного рассмотрения величины приращения вычислительной эффективности, которая, с небольшими вариациями, имеет тот же порядок.

Циклическая перестановка (сдвиг) влево. Результат Y является целочисленным представлением состояния цифровой последовательности в системе счисления с основанием Q, заданной числовым эквивалентом X, после циклического сдвига влево на m позиций:

$$Y[X,Q,m,n]=\left(X\cdot Q^{m}\right)\bmod\left(Q^{n}\right)+\left\lfloor X\cdot Q^{m-n}\right\rfloor. \quad (2)$$

Структура мини-модели (2) имеет более понятный смысл по сравнению с (1): первое слагаемое реализует операцию сдвига входного аргумента X с потерей цифр разрядов переполнения, а второе – восстанавливает значения разрядов циклической перестановки путем правого сдвига и отбрасывания дробной части. Аргумент Q и параметры n, m выполняют ту же роль, что и в модели (1). Формула модели эквивалентна ассемблерным командам арифметического сдвига SAL и SAR с последующим целочисленным сложением без переноса ADD.

Преобразование целого числа в вектор позиционных цифр произвольной системы счисления Q. Данная мини-модель определяет координаты вектора $Y=\{Y_0,Y_1,\ldots,Y_{n-1}\}$. Каждая координата Y_i обозначает значащую цифру i-го разряда положительного целого числа X, представленного в позиционной системе счисления с основанием Q. Для ранжированных значений $i=0,1,\ldots,(n-1)$ мини-модель реализуется аналитическим выражением

$$Y_i[X,Q]=\left\lfloor X\cdot Q^{-i}\right\rfloor\bmod(Q). \quad (3)$$

Формула (3) фактически реализует кратчайший способ смены позиционной системы счисления.

Вычисление веса Хэмминга целого числа X в Q-м эквиваленте. Мини-модель основана на последовательном сдвиге X влево и накоплении суммы значений позиционных цифр, извлекаемых из младшего разряда:

$$Y[X,Q,n]=\sum_{i=0}^{n-1}\left\{\left\lfloor X\cdot Q^{-i}\right\rfloor \bmod(Q)\right\}, \tag{4}$$

где $n=\lceil \log_Q X\rceil$. Данная мини-модель – кратчайший вариант реализации одной из типовых операций формирования хеш-образов при целочисленном представлении исходного текста X в системе счисления с любым основанием.

Получение десятичного эквивалента обратного кода числа X в позиционной Q-й системе счисления. Функция Y реализуется посредством вычитания каждой позиционной цифры числа X из величины $(Q-1)$ с последующим накоплением десятичной весовой суммы. При этом извлечение цифр из младшей позиции целого числа производится с помощью последовательного правого сдвига (делением) и ограничения по модулю 10:

$$Y[X,Q,n]=\sum_{i=0}^{n-1}Q^i\left[Q-1-\left\lfloor X\cdot 10^{-i}\right\rfloor \bmod(10)\right]. \tag{5}$$

Здесь, по-прежнему, число слагаемых определяется величиной параметра $n=\lceil \log_Q X\rceil$.

Примитивный арифметический аналог вычислений X по модулю Q:

$$Y[X,Q]=X-Q\left\lfloor X\cdot Q^{-1}\right\rfloor. \tag{6}$$

Мини-модель (6) может быть использована во всех рассматриваемых в данной работе моделях как альтернатива встроенной функции $(X)\bmod(Q)$.

Вычисление побитовых логических функций XOR, AND, OR для пары вещественных десятичных чисел и запись результата в виде целого десятичного числа:

$$XOR[X1,X2,n1,n2]=\sum_{i=0}^{n1+n2-2}2^i\left\{\left[\left\lfloor\frac{X1}{2^i}\right\rfloor \bmod(2)+\left\lfloor\frac{X2}{2^i}\right\rfloor \bmod(2)\right]\bmod[2]\right\}; \tag{7}$$

$$AND[X1,X2,n1,n2]=\sum_{i=0}^{n1+n2-2}2^i\left\{\left[\left\lfloor\frac{X1}{2^i}\right\rfloor \bmod(2)\right]\cdot\left[\left\lfloor\frac{X2}{2^i}\right\rfloor \bmod(2)\right]\right\}; \tag{8}$$

$$OR[X1,X2,n1,n2]=\sum_{i=0}^{n1+n2-2}2^i\left\lceil\frac{\left\lfloor\frac{X1}{2^i}\right\rfloor \bmod(2)+\left\lfloor\frac{X2}{2^i}\right\rfloor \bmod(2)}{2}\right\rceil. \tag{9}$$

В составе моделей параметры $n1, n2$ – разрядность десятичных аргументов $X1, X2$. Верхний предел индексов суммирования в выражениях (7) – (9) намеренно завышен, что позволяет отказаться от решения задачи выбора максимального из двух параметров $n1$ или $n2$. В основе мини-моделей (7) – (9) использован одинаковый принцип «фильтрации» вычислением по модулю двух значений младших бит входных аргументов при организации последовательного правого сдвига делением. Деление на 2 слагаемых в выражении (9) с последующим округлением «вверх» дает арифметический эквивалент логической операции OR.

Данные мини-модели наиболее востребованы при аналитических исследованиях типовых криптографических преобразований и обладают наибольшим вычислительным выигрышем по сравнению с векторными формами последовательного вычисления побитовых логических функций.

Свопинг полубайт. Мини-модель определяет число Y, получающееся в результате обмена местами полубайт входного байтового аргумента X:

$$Y[X]=2^4\cdot(X)\bmod\left(2^4\right)+\left\lfloor X\cdot 2^{-4}\right\rfloor. \tag{10}$$

Получение байтового двоично-десятичного кода двузначного десятичного аргумента X:

$$Y[X]=(X)\bmod(10)+2^4\cdot\left\lfloor\left(\frac{X}{10}\right)\bmod(10)\right\rfloor. \tag{11}$$

Формирование десятичного представления кода Грея с порядковым номером X в лексикографически упорядоченной кодовой книге:

$$Y[X,n]=\sum_{i=0}^{1}\left\{2^i\left[\sum_{j=0}^{n-1-i}\left\lfloor\left(\frac{X}{2^{i+j}}\right)\bmod(2)\right\rfloor\right]\bmod[2]\right\}. \tag{12}$$

Извлечение порядкового номера по заданному значению кодового слова Грея. Данная мини-модель является обратной функцией к (12):

$$Y[X,n]=\sum_{i=0}^{n-1}\left\{2^i\left[\sum_{j=0}^{n-1-i}\left\lfloor\left(\frac{X}{2^{i+j}}\right)\bmod(2)\right\rfloor\right]\bmod[2]\right\}. \tag{13}$$

Выражения (12) и (13) получены на основе алгоритмов Хэмминга [6] для построения манипуляционных кодов в эффективных телекоммуникационных протоколах для использования совместно с системами многоосновных сигналов.

2. Реализации прикладных аналитических моделей на основе библиотеки мини-моделей

Рассмотрим некоторые примеры построения вычислительно эффективных аналитических моделей, предназначенных для непосредственной реализации в математических системах, реализующих концепцию WYSIWYG.

2.1. Малая аналитическая модель блочного симметричного шифра на основе структуры сети Фейстеля.

Структура блочного симметричного шифра (БСШ), реализуемого аналитической моделью, представлена на рис.1. Схема шифрования основана на сбалансированной сети Фейстеля и содержит N раундов шифрования плайнтекста P. На каждом i-м раунде блок бит, обладающий длиной n, делится на две равные части: R_i и L_i. Все N раундовых (цикловых) функций f_i идентичны, но используют индивидуальные раундовые подключи k_i, имеющие длину $n/2$. Разворачивание раундовых подключей осуществляется по произвольному алгоритму, задаваемому словесным описанием, с использованием мастер-ключа K длиной n. Для примера рассмотрим примитивный алгоритм, в котором для получения k_i производится циклический сдвиг мастер-ключа вправо на $(i-1)$ позицию и выбор правой половины. S-блоки нелинейной замены реализуют подстановку "байт в байт" в соответствии с таблицей T, размером (16×16). Адрес строки и столбца входа определяется соответственно младшим и старшим полубайтами исходного байта. Предполагается, что все аргументы и параметры модели задаются целыми десятичными числами.

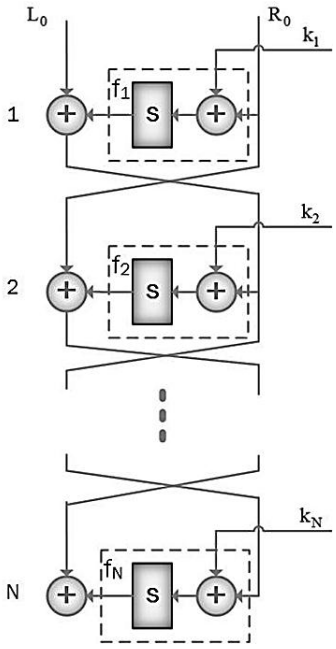

Рис. 1.Схема модели шифрования БСШ

Аналитическая реализация малой модели БСШ имеет следующий вид. Вначале производится ранжирование счетчика раундов шифрования: $i=1,2,\ldots,N$ и генерация набора раундовых подключей:

$$k_i = \left\{ 2^n \left[\left(\frac{K}{2^{(i-1)}} \right) \bmod (1) \right] + \left\lfloor \frac{K}{2^{(i-1)}} \right\rfloor \right\} \bmod \left\{ 2^{n/2} \right\}.$$

ENCRIPTION $P \to C$:

Плайнтекст задается целым числом $P \in \left[0, \left(2^n - 1 \right) \right]$.

Начальное разбиение плайнтекста:

$$R_0 = (P) \bmod \left(2^{n/2} \right), \quad L_0 = \left\lfloor P \cdot 2^{-n/2} \right\rfloor.$$

Выполнение N раундов шифрования:

$$L_i = R_{i-1}, \quad f0_i = XOR\left[R_{i-1}, k_i, \frac{n}{2}, \frac{n}{2} \right],$$

$$STR_i = (f0_i) \bmod \left(2^4 \right), \; COL_i = \left\lfloor f0_i \cdot 2^{-4} \right\rfloor,$$

$$f_i = T_{STR_i, COL_i}, \; R_i = XOR\left[L_{i-1}, f_i, \frac{n}{2}, \frac{n}{2} \right],$$

где функция $XOR[\cdots]$ задана моделью (7). Собственно, получение криптограммы:

$$C = 2^{n/2} \cdot L_N + R_N.$$

DECRIPTION $C \to P$:

Реализуется обратный порядок использования раундовых подключей: $i = N, (N-1), \ldots, 1$.

Начальное разбиение криптограммы: $R_N = (C) \bmod \left(2^{n/2} \right), \quad L_N = \left\lfloor C \cdot 2^{-n/2} \right\rfloor$. Выполнение N раундов дешифрования:

$$R_{i-1} = L_i, \quad f0_i = XOR\left[R_{i-1}, k_i, \frac{n}{2}, \frac{n}{2} \right], \; STR_i = (f0_i) \bmod \left(2^4 \right), \quad COL_i = \left\lfloor f0_i \cdot 2^{-4} \right\rfloor$$

$$f_i = T_{STR_i, COL_i}, \quad L_{i-1} = XOR\left[R_i, f_i, \frac{n}{2}, \frac{n}{2} \right].$$

Восстановление плайнтекста: $P^* = 2^{n/2} \cdot L_0 + R_0$.

2.2. Аналитическая модель генератора m-последовательностей на LFSR Фибоначчи.

Рассмотрим вариант вычислительно эффективной в системах WYSIWYG аналитической модели процесса получения двоичных псевдослучайных последовательностей линейными регистрами сдвига с обратными связями (LFSR). Структура примитивного неприводимого многочлена задается в модели вектором S, размерность которого $m > 2$ определяется числом ненулевых обратных связей LFSR, а значения элементов равны степеням присутствующих в многочлене слагаемых. Например, для многочлена $P(x) = x^{11} + x^9 + 1$ вектор параметров имеет вид $S = \{0, 9, 11\}$. Для любого вида $P(x)$: $S_0 = 0$, $S_{m-1} = n$, где n – степень многочлена. В соответствии с методологией построения рассматриваемых аналитических моделей состояние LFSR для произвольного i-го такта генерации характеризуется целым положительным числом R_i, при этом, поскольку период m-последовательности равен $2^n - 1$, имеет смысл рассмотрение тактов генерации с номерами из диапазона $\left[0, 1, \ldots, 2^n - 2 \right]$.

Инициализация LFSR для генерации производится n-элементной единичной последовательностью: $R_0 = 2^n - 1$. Модификация LFSR на i-м такте описывается суммой вида:

$$R_i = ASL(R_{i-1}) + F\_XOR(R_{i-1}, S),$$

где $ASL(R_{i-1})$ – мини-модель арифметического сдвига влево с потерей бита переноса

$$ASL(R_{i-1}) = (2 \cdot R_{i-1}) \bmod (2^n);$$

$F\_XOR(R_{i-1}, S)$ – функция вычисления нового значения младшего бита LFSR, основанная на $(m-1)$-кратном вычислении XOR, аргументы которого определяются элементами вектора S: $F\_XOR(R_{i-1}, S) = \left\{ \sum_{j=1}^{m-1} \left[\left(\left\lfloor \frac{R_{i-1}}{2^{S_j - 1}} \right\rfloor \right) \bmod (2) \right] \right\} \bmod \{2\}$.

В итоге формируется собственно двоичная m-последовательность M при помощи извлечения значений старших бит из чисел с десятичным эквивалентом R_i: $M_i = \left(\left\lfloor \frac{R_i}{2^{n-1}} \right\rfloor \right) \bmod (2)$.

2.3. Аналитическая модель физического протокола формирования и обработки сложного узкополосного сигнала АФМ-16

Данная модель воспроизводит процесс формирования и обработки сложных сигналов объемной укладки в протоколах беспроводного доступа. Ансамбль содержит 16 сигнальных точек, расположение и кодирование которых на фазовой плоскости показано на рис. 2.

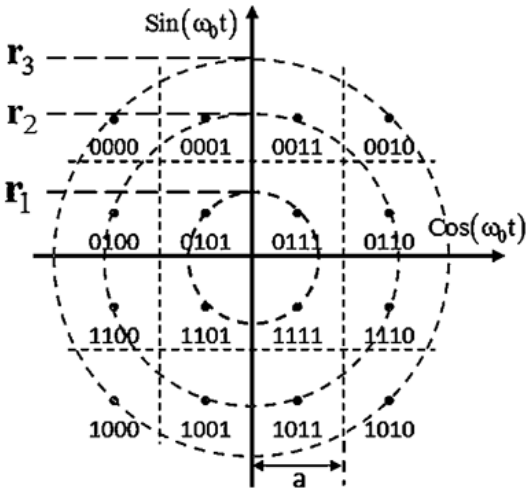

Рис. 2. Структура и кодирование АФМ-16

Все сигнальные точки лежат на поверхности трех концентрических окружностей различных радиусов r_1, r_2, r_3. Для построения аналитической модели необходимо определение параметра решетки (длины ребра a) на основе ограничения бюджета мощности Pw, предусмотренного для передачи 1 бита данных. В рассматриваемом случае один сигнал на интервале модуляции передает значения $k = 4$ бит. 4 точки ансамбля лежат на поверхности окружности радиуса r_1, 8 точек – на поверхности окружности радиуса r_2 и 4 точки – на поверхности окружности радиуса r_3. Полагая равновероятное использование всех сигнальных точек и усредняя на объем ансамбля, можно составить уравнение для нахождения параметра решетки:

$$\frac{1}{16}\left(4r_1^2 + 8r_2^2 + 4r_3^2\right) = k \cdot Pw. \qquad (14)$$

Левая часть уравнения определяет среднюю мощность сигнала на произвольном интервале модуляции, а правая – бюджет мощности с учетом количества бит, передаваемых одним сигналом. Используя формулы геометрии, выразим значения радиусов через параметр решетки:

$$r_1 = \sqrt{\frac{a^2}{4} + \frac{a^2}{4}} = \frac{a}{\sqrt{2}}, \quad r_2 = \sqrt{9\frac{a^2}{4} + \frac{a^2}{4}} = a\sqrt{\frac{5}{2}}, \quad r_3 = \sqrt{9\frac{a^2}{4} + 9\frac{a^2}{4}} = a\frac{3}{\sqrt{2}}.$$

Решая уравнение (14) при $k = 4$, получим взаимосвязь параметра решетки с бюджетом мощности: $a = \sqrt{8Pw/5}$. Значения модулирующих коэффициентов по обеим осям фазовой плоскости, в силу симметричности поля сигнальных точек, могут принимать одинаковые значения:

$$\{-3a/2, -a/2, a/2, 3a/2\}. \quad (15)$$

Рассмотрим реализацию модели. Пусть определены следующие параметры модели: несущая частота f_0 [Hz]; скорость модуляции V [Бод]; интервал дискретности $T = 1/V$ [c], массив данных, предназначенных для передачи, $P = \{p_0, \ldots, p_{q-1}\}$ содержащий q байтовых целых чисел.

Аналитическая модель формирования сигнала. Вначале производится формирование вектора полубайт из $2q$ элементов для определения координат сигнальных точек на фазовой плоскости (рис. 2):

$$j = 0 \ldots q-1; \quad X_{2j} = \left\lfloor \frac{p_j}{2^4} \right\rfloor; \quad X_{2j+1} = (p_j) \bmod (2^4).$$

На основе X можно получить два вектора XH и XL такой же размерности, содержащие старший и младший дибиты полубайт: $i = 0 \ldots 2q-1; \; XH_i = \left\lfloor \frac{p_i}{2^2} \right\rfloor; \; XL_i = (X_i) \bmod (2^2)$.

Каждая пара элементов (XH_i, XL_i) содержит, при их конкатенации, код Грея, соответствующий определенной сигнальной точке на фазовой плоскости. Для перехода к порядковым лексикографическим номерам значений амплитудных модуляционных коэффициентов (15) в соответствии с мини-моделью (13) используется следующая пара преобразований:

$$H_i = 2\left\lfloor \frac{XH_i}{2} \right\rfloor + \left[\left\lfloor \frac{XH_i}{2} \right\rfloor + (XH_i) \bmod (2) \right] \bmod [2];$$

$$L_i = 2\left\lfloor \frac{XL_i}{2} \right\rfloor + \left[\left\lfloor \frac{XL_i}{2} \right\rfloor + (XL_i) \bmod (2) \right] \bmod [2].$$

Элементы полученных векторов H и L представляют собой лексикографические номера координат точек ансамбля АФМ-16, соответствующие содержимому полубайт исходного массива данных, и представлены числами в системе счисления с основанием $Q = 2^2$. Тогда, на основе геометрии размещения сигнальных точек можно записать окончательную аналитическую модель сигнала, определенного на интервале времени $t \in [0, 2 \cdot q \cdot T]$

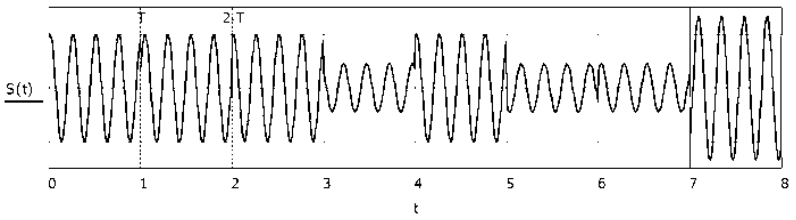

Рис. 3. Реализация модели АФМ-16

$$S(t) = a\left\{ \left(\frac{3}{2} - H_{\left\lfloor \frac{t}{T} \right\rfloor} \right) \sin[\omega_0 t] + \left(\frac{-3}{2} + L_{\left\lfloor \frac{t}{T} \right\rfloor} \right) \cos[\omega_0 t] \right\},$$

где $\omega_0 = 2\pi f_0$ [рад/с] – круговая частота. Пример реализация модели $S(t)$ на восьми интервалах T при произвольно выбранных параметрах представлен на рис. 3.

Аналитическая модель когерентной обработки сигнала. Используем определенные ранее ранжированные счетчики i и j, при этом значение i – определяет порядковый номер обрабатываемого интервала T, а значение j – порядковый номер байта исходного массива данных. Вычисление пары корреляционных интегралов дает амплитудные коэффициенты квадратур несущей частоты на i-м канальном интервале времени:

$$\alpha_i = \frac{2}{aT} \int_{i \cdot T}^{(i+1) \cdot T} S(t) \sin(\omega_0 t) dt; \qquad \beta_i = \frac{2}{aT} \int_{i \cdot T}^{(i+1) \cdot T} S(t) \cos(\omega_0 t) dt. \quad (16)$$

Тогда, в соответствии с правилом максимального правдоподобия, оценки координат сигнальных точек в виде соответствующих значений дибит определяются:

$$H^*_i = \mathrm{round}\left(\frac{3}{2} - \alpha_i\right), \quad L^*_i = \mathrm{round}\left(\frac{3}{2} + \beta_i\right), \tag{17}$$

где $\mathrm{round}(\cdots)$ – функция целочисленного округления.

Переход от координат (17) к оценке истинных значений дибит, составляющих полубайт, производится на основе мини-модели (12), которая для дибит при $n = 2$ эквивалентна по виду модели обратного преобразования (13):

$$XH^*_i = 2\left\lfloor \frac{H^*_i}{2} \right\rfloor + \left\lfloor \left\lfloor \frac{H^*_i}{2} \right\rfloor + \left(H^*_i\right) \bmod (2) \right\rfloor \bmod [2];$$

$$XL^*_i = 2\left\lfloor \frac{L^*_i}{2} \right\rfloor + \left\lfloor \left\lfloor \frac{L^*_i}{2} \right\rfloor + \left(L^*_i\right) \bmod (2) \right\rfloor \bmod [2].$$

На заключительном шаге обработки оценки значений дибит объединяются в полубайты $X^*_i = XH^*_i \cdot 2^2 + XL^*_i$, а полубайты – в оценки байт исходного массива данных:

$$P^*_j = X^*_{2\cdot j} \cdot 2^4 + X^*_{2\cdot j+1}.$$

Рассмотренная аналитическая модель формирования и обработки сложных сигналов технологична для применения в задачах статистических исследований помехоустойчивости различных ансамблей сигналов, которые реализуются при введении заданных моделей помех перед обработкой. Для случая некогерентной обработки аналитическая модель может быть дополнена произвольным фазовым сдвигом на несущей частоте. Ошибки, порождаемые неточной тактовой синхронизацией, легко моделируются путем введения детерминированного или случайного временного сдвига при определении границ интервалов T_i в корреляционных интегралах (16).

Выводы

Рассмотренные компоненты библиотеки аналитических мини-моделей стандартных преобразований представляют собой реализацию концепции оптимизированных вычислений, ориентированных на возможности низкоуровневых машинных языков. При этом оперативное построение и отладка алгоритмов моделирования комфортно производятся в среде высокоуровневых интерпретаторов WYSIWYG. Методология целочисленных вычислений, использованная в мини-моделях библиотеки, значительно сокращает временные затраты и обеспечивает экономию задействованной памяти.

Список литературы: 1. *Морозов В.К.* Моделирование информационных и динамических систем / В.К. Морозов, Г.Н. Рогачев. – М. : Изд. центр «Академия», 2011. – 384 с. 2. *Абель П.Т.* Язык Ассемблера для IBM PC и программирования. Избранные главы ; пер. с англ. – М. : Высш. шк., 1992. – 477 с. 3. *Кирьянов Д.* Mathcad-12. – С-Петербург : БХВ-Петербург, 2005. – 576 с. 4. *http://freeanalogs.ru.* 5. *Долгов В.И.* Стойкость блочных шифров к дифференциальному и линейному криптоанализу / В.И. Долгов, И.В. Лисицкая // Lambert Academic Publishing, 2013. – 498 с. 6. *Хэмминг Р.В.* Теория кодирования и теория информации ; пер. с англ. – М. : Радио и связь, 1983. – 176 с.

Харьковский национальный университет имени В.Н. Каразина

Поступила в редколлегию 11.03.2015