- реализована возможность работы устройств (сигнального процессора и магистрали VME) независимо друг от друга, используя массив временного хранения данных в виде двухпортовой памяти;

- реализована возможность размещать контроллер в адресном пространстве магистрали VME с помощью специального внутреннего регистра.

2. Проведены исследования работоспособности контроллера в различных условиях эксплуатации путем моделирования в программной среде разработки QUARTUS II, а именно:

- определены достоверности передачи данных и величины задержки от частоты тактирования контроллера и скорости передачи данных;

- проверено, что логика работы контроллера отвечает требованиям, предъявляемым к логике работы устройств, как со стороны магистрали VME, так и со стороны сигнального процессора ADSP-21364;

- определена оптимальная частота тактирования, которая, исходя из результатов исследований, составляет 100-120 МГц.

Литература

1. Пивоваров В.В., Юминов О.Б. Проектирование контроллера обмена данных между сигнальным процессором ADSP-21364 SHARC и магистралью микропроцессорных систем VME // Сб. докладов 5-й РНТК «Приборостроение в XXI веке. Интеграция науки, образования и производства». Ижевск, 2008. – С. 321-324.
2. ГОСТ Р МЭК 821-2000. Магистраль микропроцессорных систем для обмена информацией, разрядностью от 1 до 4 байт (Магистраль VME). Госстандарт России, 2000. – 214 с.
3. ADSP-2136x SHARC Processor Hardware Reference. Analog Devices, Inc. http://www.analog.com
4. QUARTUS II handbook, Volume 1. Altera Corporation. http://www.altera.com

УДК 681.327

МНОГОАЛФАВИТНЫЙ АДАПТИВНЫЙ ШИФР, ОСНОВАННЫЙ НА ИНТЕГРАЛЬНЫХ ПРЕОБРАЗОВАНИЯХ

Алексеев А.П., Блатов И.А, Макаров М.И., Похлебаев В.А.

В статье рассматривается шифр, работа которого строится таким образом, чтобы выходное распределение элементов криптограммы имело равномерное распределение.

Постановка задачи

Одноалфавитные шифры не являются криптостойкими из-за имеющейся статистической устойчивости появления букв в открытом тексте. На рис. 1 показана гистограмма распределения частоты появления строчных русских букв в книге [1]. Гистограмма получена путем обработки текста, содержавшего 1,05 миллиона символов, среди которых было 786 тысяч русских строчных букв.

Как видно из рис. 1, абсолютная частота появления букв отличается большой неравномерностью, которая позволяет криптоаналитику успешно произвести дешифрацию длинной криптограммы, созданной методом одноалфавитной замены. Чаще всего в статистически обработанном тексте встречались строчные гласные буквы «о», «е», «и», «а». Реже других русских строчных букв попадались «ш», «э», «ъ», «е».

Распределение символов будет несколько изменяться в зависимости от предметной области, из которой берут текст, подвергаемый обработке. Так при анализе распределения заглавных букв было замечено существенное увеличение частоты появления буквы «Э». Это объяснилось тем, что книга [1] относится к области вычислительной техники, и в тексте часто встречалось слово «ЭВМ».

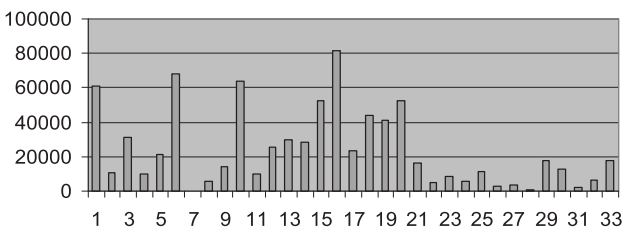
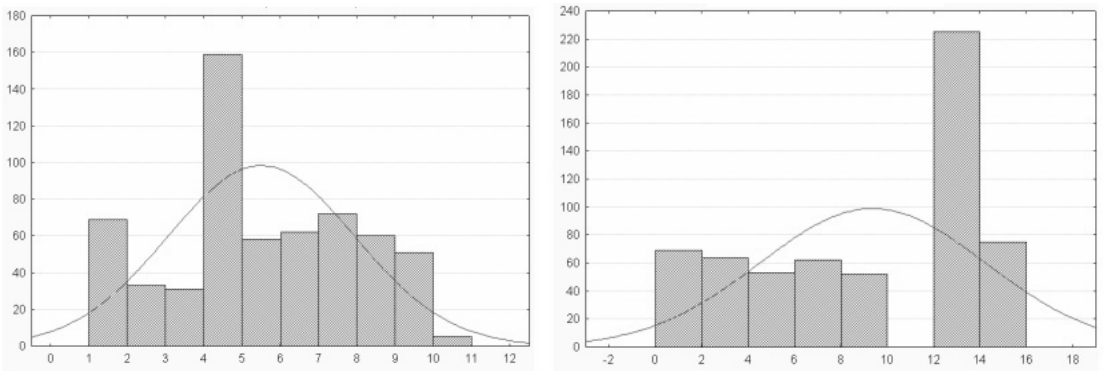


Рис. 1. Распределение строчных букв русского алфавита в открытом тексте

На рис. 1 по горизонтальной оси отложены порядковые номера букв в алфавите. По вертикальной оси отложены абсолютные частоты появления строчных букв в тексте.



а) б)

Рис. 2. Гистограммы, иллюстрирующие возможность криптоанализа

Многоалфавитные шифры замены повышают криптостойкость. Тем не менее, существует возможность взлома и многоалфавитных шифров, которые продолжают наследовать статистическую картину распределения частоты появления символов.

На рис. 2 показаны гистограммы, полученные при шифровании трехсот букв «А» (рис. 2а) и трехсот букв «Г» (рис. 2б) многоалфавитным шифром, в котором каждой букве ставится только один интервал замен, но используются интегральные преобразования [2]. Из рис. 2 видно, что распределения существенно различаются (у них разные математические ожидания и дисперсии). Это дает «зацепку» для успешного криптоанализа.

Разработка адаптивного шифра

Основная идея построения шифра заключается в формировании криптограммы в виде равномерной смеси вещественных чисел.

Равномерность распределения вещественных чисел в криптограмме достигается тем, что в процессе шифрования ведется анализ получающегося распределения чисел шифрограммы. С этой целью непрерывно строится гистограмма распределения. При этом очередные элементы шифровки формируются таким образом, чтобы они попали в те места распределения, где наблюдаются провалы. Возможность изменения (варьирования) положения очередного элемента криптограммы на числовой оси имеется благодаря тому, что при шифровании используются многоалфавитная замена и интегральное преобразование [2].

Алгоритм шифрования таков, что осуществляется непрерывный анализ выходного распределения и выполняется такая коррекция (адаптация) шифра, чтобы обеспечить приближение формируемых чисел к равномерному распределению.

Многоалфавитное шифрование предполагает, что каждый символ открытого текста многократно встречается в таблице замен на различных участках числовой оси. В таблице 1 приведен фрагмент некоторой упрощенной таблицы многоалфавитной замены. При этом считается, что буква «е» встречается в открытом тексте чаще других, а буква «д» – реже других. По этой причине для буквы «е» выделено 6 интервалов многоалфавитной замены, а для буквы «д» – только 2.

Рассмотрим, как осуществляется шифрование с помощью таблицы многоалфавитной замены. Предположим, что нужно зашифровать фразу «где абба». Шифровку можно создать бесконечным числом способов. При этом каждую букву допустимо заменять любым вещественным

Таблица 1. Фрагмент многоалфавитного шифра

	Алфавит открытого текста					
Интервалы замены	а	б	в	г	д	е
	[5…6)	[2…3)	[4…5)	[3…4)	[1…2)	[6…7)
	[8…9)	[10…11)	[11…12)	[7…8)	[9…10)	[12…13)
	[13…14)	[14…15)	[17…18)	[15…16)	–	[16…17)
	[18…19)	–	[21….22)	[20…21)	–	[19…20)
	[23…24)	–	–	–	–	[22…23)
	–	–	–	–	–	[24…25)

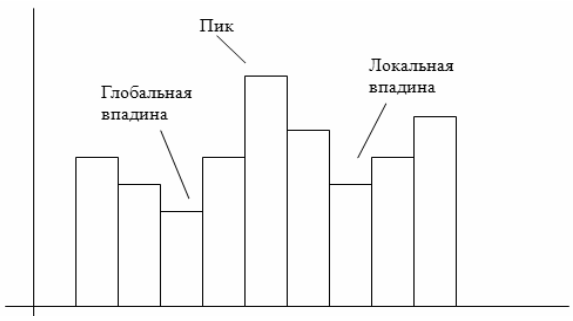


Рис. 3. Гистограмма выходного распределения с обозначением введенных понятий

числом из указанных интервалов. Приведем две криптограммы для указанной фразы:

1) 15,33 – 9,101 – 22,99 – 18,06 – 14,57 – 2,331 – 5,064 ;

2) 7,105 – 1,102 – 12,98 – 8,473 – 10,16 – 14,91 – 23,26 .

В предлагаемом шифре после многоалфавитной замены осуществляется интегральное преобразование полученного числа. Это дает возможность один из пределов интегрирования выбирать по случайному закону [2]. При этом нужно находить очередной предел интегрирования таким образом, чтобы формируемое число криптограммы попало в зону наибольшего провала (в зону глобальной впадины) на гистограмме.

Для шифрования адаптивным (подстраиваемым) шифром необходимо постоянно решать обратную задачу шифрования: по найденному числу в выходном распределении (находящегося в зоне глобальной впадины) выбирать такое значение предела интегрирования, которое обязательно попадет в заданный интервал гистограммы. Следующий рисунок иллюстрирует эту идею. После зашифрования очередного символа гистограмма достраивается (пополняется). На гистограмме выделяется максимальное значение (пик), минимальное значение (глобальная впадина) и провалы (локальные впадины). Формирование криптограммы ведется таким образом, чтобы с максимально возможной степенью выровнять имеющееся выходное распределение.

Предположим, что наибольший провал на гистограмме наблюдается в интервале чисел $[c_i, c_{i+1}]$. Пусть при этом для интегрального преобразования используется некоторая подынтегральная функция $f(x)$: $I = \int_a^b f(x)dx$.

Для того чтобы уменьшить глубину глобальной впадины, генерируется случайное число a из интервала $[c_i, c_{i+1}]$. По таблице многоалфавитной замены определяется значение интеграла I, которое соответствует шифруемому символу. По известному значению нижнего предела интегрирования a и величине интеграла I, находят значение верхнего предела интегрирования b: $b = \varphi(a, I)$.

Полученные числа a и b передают в линию. Эти числа являются элементами криптограммы (шифровкой). Заметим, что пределы интегрирования можно формировать и в обратном порядке: сначала выбирать b, а потом вычислять a.

На приемной стороне известны вид использованного интегрального преобразования (подынтегральная функция) и конфигурация таблицы многоалфавитной замены (ТМЗ). Эти два элемента определяются секретным сеансовым ключом. Поэтому процесс дешифрации криптограммы не вызывает затруднений. Он сводится к вычислению определенного интеграла по известным значениям нижнего и верхнего пределов интегрирования и определению принятого символа по таблице многоалфавитной замены.

Таким образом, сформированная величина a обязательно попадет в зону наибольшего провала, а верхний предел интегрирования b случайно окажется в одной из зон гистограммы.

Величину b также можно приблизить к одной из локальных впадин на гистограмме (эта величина даже может попасть в зону глобальной впадины). Для этого нужно произвести расчеты верхнего предела интегрирования b при имеющемся значении нижнего предела интегрирования a, поочередно выбирая допустимые значения интеграла I из таблицы многоалфавитной замены. При расчете верхнего предела интегрирования b желательно не допустить попадание этого числа в зону пика гистограммы. Все другие результаты расчетов являются приемлемыми.

Таблица 2. Зависимость числа интервалов от числа символов

n	100	1000	10000	100000	1000000
k	7,64	10,96	14,28	17,60	20,92

Оценка числа интервалов на гистограмме выходного распределения

Число интервалов k на гистограмме, предназначенной для контроля выходного распределения, можно оценить по формуле Стержесса [3]:

$$k \approx 1 + 3{,}32 \lg n \ , \qquad (1)$$

где n – число элементов (вещественных чисел) в криптограмме. Таблица 2 позволяет наглядно представить оценку числа интервалов в гистограмме k в зависимости от длины (числа символов) зашифрованного текста n. С учетом того, что при шифровании каждый символ открытого текста s заменяется двумя вещественными числами ($n = 2 \cdot s$), то при длине открытого текста (сообщения) s = 500 символов число интервалов k на гистограмме оценивается числом 10,96.

Порядок формирования таблицы многоалфавитной замены

Таблица многоалфавитной замены служит на передающей стороне для замены символа открытого текста на некоторое вещественное число. Это число эквивалентно значению определенного интеграла, для которого определяются значения верхнего и нижнего пределов интегрирования. На приемной стороне таблица многоалфавитной замены используется для определения значения принятого символа по величине определенного интеграла, вычисленного с помощью полученных значений верхнего и нижнего пределов интегрирования. Таблица является элементом секретного ключа.

Рассмотрим порядок формирования таблицы многоалфавитной замены.

1. Вначале нужно задаться длиной открытого текста, подлежащего шифрованию. Пусть $s_{\max} = 50000$ символов. Тогда число вещественных чисел, из которых будет состоять криптограмма, n = 100000.

2. По формуле (1) следует оценить число необходимых интервалов на гистограмме. Для выбранного значения $s_{\max}$ число интервалов k = 17,6.

3. Определить общее число интервалов в таблице многоалфавитной замены t, которое должно быть на один – два порядка больше числа k. Кроме того, число интервалов в ТМЗ должно быть в 3…4 раза больше числа символов в алфавите открытого текста. Таким образом, число интервалов в таблице многоалфавитной замены лежит в пределах 176…1760. Примем t = 1000.

4. Найти сумму нормированных частот символов открытого текста

$$sg = \sum_{i=1}^{r} g_i \ ,$$

где r – число символов в алфавите открытого текста (r = 256 при использовании всех символов таблицы СР-1251 и r = 33 при использовании только русских строчных или заглавных букв); g_i – нормированная частота.

Нормированные частоты появления символов в открытом тексте g_i получают путем деления абсолютных частот на наименьшее значение абсолютной частоты.

5. Вычислить число интервалов замен для каждого i-го символа алфавита открытого текста:

$$t_i = \frac{g_i \cdot t}{\sum_{i=1}^{r} g_i} \ .$$

Для примера вычислим число интервалов замен для букв «а» и «б»:

$$t_a = \frac{619 \cdot 1000}{7939} = 78 \ , \ t_б = \frac{105 \cdot 1000}{7939} = 13 \ .$$

6. Задать диапазон (ширину) гистограммы и ее положение на числовой оси. Это означает, что задаются значения $a_{\min}$ и $b_{\max}$ (это для случаев, когда определенный интеграл принимает только положительные значения). Задать ширину и положение на числовой оси таблицы многоалфавитной замены, то есть определить значения $I_{\min}$ и $I_{\max}$. Перечисленные величины связаны между собой и соотношения между ними зависят от вида подынтегральной функции:

$$I_{\max} = \varphi(a_{\min}, b_{\max}) \text{, а } I_{\min} \approx 0 \ .$$

Например, для подынтегральной функции правая граница для таблицы многоалфавитной замены вычисляется по формуле:

$$I_{\max} = \frac{b_{\max}^5 - a_{\min}^5}{5} \ .$$

Вычислить ширину одного интервала замен:

$$\Delta = \frac{I_{\max} - I_{\min}}{t} \ .$$

7. Пусть $\Delta = 0{,}1$. Требуется составить таблицу многоалфавитной замены, в которой ширина каждого интервала замен равна Δ, а общее число интервалов замен равно t. Все интервалы замен образуют непрерывный интервал чисел шириной Δt. Для рассматриваемого случая $\Delta t = 0{,}1 \cdot 1000 = 100$. Каждому интервалу замен ставят в соответствие один из символов алфавита открытого текста. При этом число интервалов замен для буквы «а» равно t_a, для буквы «б» равно $t_б$ и т.д. Интервалы замен для каждого символа располагаются на числовой оси в случайном порядке.

Конфигурация таблицы многоалфавитной замены является одним из элементов секретного ключа. Вторым элементом ключа является вид подынтегральной функции.

Примеры шифрования с помощью адаптивного многоалфавитного шифра

Пример 1. Предположим, что в текущий момент времени необходимо зашифровать букву «в». В качестве первого ключевого элемента используется таблица 1. Вторым элементом секретного ключа является вид подынтегральной функции. Пусть $f(x) = x^4$.

Предположим, что на гистограмме, составленной на предыдущих шагах шифрования, наблюдается глобальная впадина в диапазоне чисел [6…10).

Для зашифрования буквы «в» по случайному закону из таблицы 1 выбирается один из четырех интервалов замен. Допустим, что выбран интервал 3, то есть (17…18]. Из этого интервала генерируется случайное число, например, $I = 17{,}58$.

Для заполнения провала на гистограмме генерируется случайное число a из интервала [7…9). Пусть $a = 8{,}02$. С учетом формулы Ньютона-Лейбница для выбранной подынтегральной функции получаем:

$$b = \sqrt[5]{5 \cdot I + a^5}$$

Расчет верхнего предела интегрирования дает значение: $b = 8{,}0242448$. Таким образом, оба числа a и b попали в зону глобальной впадины. «Рассеяние» (отличие, отклонение) пределов интегрирования небольшое.

Пример 2. Используем в качестве исходных данных числа, приведенные в предыдущем примере, но другую подынтегральную функцию:

$$f(x) = \frac{1}{x} .$$

Для этой функции верхний предел интегрирования вычисляется по формуле:

$$b = \exp(I + \ln| a |);$$

$$b = 3{,}46 \cdot 10^8 .$$

Приведенные примеры показывают, что при одних видах подынтегральной функции рассеяние чисел малое, а при других – большое.

Выбор вида подынтегральной функции

В качестве подынтегральной функции желательно подобрать функцию, у которой с изменением аргумента меняются амплитуда и частота колебаний. График подобной функции приведен на следующем рисунке.

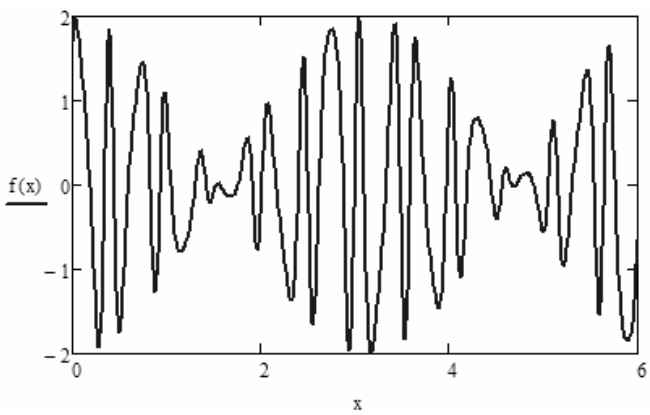


Рис. 4. График подынтегральной функции

При выборе вида подынтегральной функции $f(x)$ и нахождении первообразной $F(x)$ можно воспользоваться следующими соображениями.

Представим подынтегральную функцию в виде:

$$f(x) = w'(x)\sin w(x) \ . \qquad (2)$$

Тогда с учетом $F'(x) = f(x)$ для подынтегральной функции (2) получим:

$$F(x) = -\cos w(x) .$$

В качестве $w(x)$ можно использовать большой класс функций, например

$$w(x) = Ax + C\sin Bx .$$

Тогда

$$f(x) = (A + BC\cos Bx)\sin(Ax + C\sin Bx) .$$

В этом случае первообразная определяется выражением

$$F(x) = -\cos(Ax + C\sin Bx) .$$

Понятно, что первообразная должна быть использована при вычислении нижнего и верхнего

пределов интегрирования, которые являются элементами шифра. Коэффициенты A, B и C можно использовать в качестве элементов ключа рассмотренного шифра.

Выводы

Рассмотренный в статье адаптивный многоалфавитный шифр целесообразно использовать при шифровании объемных текстов. Криптоанализ данного шифра осложнен тем, что элементы криптограммы представляют собой вещественные числа, распределенные по равномерному закону.

Литература

1. Алексеев А.П. Информатика 2007. М.: СОЛОН-ПРЕСС, 2007. – 608 с.
2. Алексеев А.П. Математические методы формирования многоалфавитных шифров замены // ИКТ. Т.7, № 2, 2009. – С. 21-25.
3. Алексеев А.П., Камышенков Г.Е. Использование ЭВМ для математических расчетов. Самара: Парус, 1998. – 190 с.

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 658.512.22

СТРУКТУРА ФОРМАЛЬНОГО ПРЕДСТАВЛЕНИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ В ФУНКЦИОНАЛЬНО АДАПТИРОВАННОЙ САПР

Горбачев И.В., Похилько А.Ф.

В статье рассматривается структура функционально адаптированной САПР и принципы работы с ней. Описывается структура формального описания объектов информационного пространства функционально адаптированной САПР и принципы формирования условий.

Введение

Проблема обмена решениями между различными САПР, на сегодняшний день, остается не решенной. Разработанный формат ISO 10303 STEP позволяет передать геометрическую модель объекта из одной системы в другую, но передается только геометрия модели. Логику (дерево) построения модели передать из одной геометрической среды в другую без искажений практически невозможно. Внесение в существующие модели изменений является необходимым элементом инфокоммуникационного взаимодействия в проектной деятельности с использованием современных информационных технологий, так как по существу означает невозможность использования «опыта со стороны» [1].

Сложность проблемы достижения интероперабельности в данном контексте является принципиальной. CAD-системы от различных производителей проектирования никогда не будут иметь в точности одинаковый набор операций, так как потеряют свои конкурентные преимущества; так же как невозможно в рыночных условиях заставить всех пользоваться только одной и той же САПР [2].

Предлагается передавать геометрическую модель проектируемого объекта вместе с функционалом, который позволяет ее построить – то есть в виде небольшого программного модуля, содержащего только необходимый для решения текущей задачи набор функциональности – функционально адаптированной САПР (ФА САПР).

За счет включения в ФА САПР конвертора STEP, модель можно передать в любую другую систему. Если возникает необходимость внести в модель изменения, то ФА САПР обладает достаточным функционалом для этого.

Структура функционально адаптированной САПР

В состав ФА САПР входят три модуля:

- исполняемый модуль, который представляет собой графический интерфейс пользователя с процедурами вызова функций графического ядра, областью моделирования (отображения) трехмерной модели проектируемого объекта, и деревом построения объекта, средствами редактирования прочих проектных операций (выбора табличных данных, математических расчетов и др.);
- библиотеки графического ядра: набор перекомпилированных библиотек, из состава которых удалена избыточная функциональность. Для построения ФА САПР требуется ядро геометрического моделирования. Для проведения программного эксперимента используется геометрическое ядро Open CASCADE. Исследо-