УДК 681.391.837:681.327.22

В.И. Барсов[1], В.А Краснобаев[2], А.С. Фещенко[1]

[1]*Украинская инженерно-педагогическая академия, Харьков*
[2]*Полтавский национальный технический университет им. Юрия Кондратюка, Полтава*

КОНЦЕПЦИЯ СОЗДАНИЯ СИСТЕМЫ БЫСТРОЙ И ДОСТОВЕРНОЙ ОБРАБОТКИ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ РАСПРЕДЕЛЁННЫХ ВЫЧИСЛЕНИЙ

В данной статье рассмотрена концепция создания системы криптографической обработки информации на основе использования модулярной системы счисления (МСС). Это позволит уменьшить вычислительную сложность реализации процесса криптографических преобразований, а также повысить эффективность контроля и коррекции ошибок в МСС при реализации технологии Grid вычислений.

Ключевые слова: *система обработки криптографической информации, шифрование, модулярная система счисления, криптопреобразования с открытым ключом, распределённые вычисления.*

Введение

В последнее время получила широкое распространение форма распределённых вычислений, которая, с точки зрения сетевой организации представляет собой согласованную, открытую и стандартизованную среду, обеспечивающую гибкое, скоординированное, но не всегда безопасное, разделение вычислительных ресурсов и ресурсов хранения информации, являющихся также частью этой среды, в рамках одной виртуальной организации.

Это технология Grid-вычислений, применяемая для решения научных, математических, статистических, экономических и других трудоёмких задач, требующих значительных вычислительных. Необходимо отметить, что в общем плане Grid-вычисления являются разновидностью параллельных вычислений, основывающихся на использовании обычных компьютеров подключенных к сети (локальной или глобальной) при помощи обычных протоколов, например Ethernet.

Однако, несмотря на возможную перспективу данной технологии, для её широкого распространения и применения необходимо решить целый ряд научно-технических задач.

Одна из таких актуальных задач связана с необходимость обеспечения безопасности, достоверности и аутентификации, поскольку сегодняшний Интернет и Web-технологии не рассматривают таких возможностей.

Решить данную задачу можно используя криптографические методы защиты позволяющие осуществлять как закрытие данных, хранимых в базах данных или передаваемых по каналам связи, так и контроль целостности и аутентичности данных, передаваемых по каналам связи.

Анализ содержания современных направлений развития криптографии показывает, что они связаны в первую очередь с применение криптографических преобразований, основанных на использовании открытого распределения ключей. Современные криптопреобразования с открытым ключом как правило основываются на преобразованиях проводимых на алгебраических кривых (эллиптические кривые, гиперэллиптические кривые, кривые Пикарда и суперэллиптические кривые). Небольшая длинна ключа, возможность выполнения быстрой обработки криптограммы это те достоинства которые обуславливают особый интерес к эллиптической криптографии реализуемой в телекоммуникационных системах. Результаты исследований современных тенденций реализации технологии Grid-вычислений показывают, что применение криптосистем с открытым ключом может позволить создать систему комплексного обеспечения безопасности информации в больших компьютерных сетях, информационных базах данных и аутентификацию клиента и сервера.

При проектировании криптосистемы на первый план выходит проблема безопасности, после чего решается связанная с ней проблема эффективности применения системы обработки криптографической информации (СОКИ). Проблема эффективности применения СОКИ в основном связывается с производительностью реализации криптопреобразований, т.е. со скоростью вычислений в группе точек кривой или RSA криптопреобразований.

Развитие криптографических методов направлено, в том числе на увеличения длины ключей, однако с увеличением длинны ключа (за счёт чего повышается безопасность) существенно повышается время решения задач криптопреобразований. Это определяет повышенные требования по производительности и отказоустойчивости средств обработки криптографической информации. Однако, несмотря на прогресс в индустрии микропроцессорной техники, темпы роста производительности вычислительных комплексов отстают от

темпов роста информационных потоков и сложности задач обработки информации.

Также значительные изменения произошли и в коммуникационных технологиях и организации компьютерных сетей соединяющих компьютерные центры. Наблюдается увеличение производительности сети по отношению к росту мощности СОКИ, что выдвигает дополнительные требования по производительности и надежности систем обработки криптографической информации.

Данные обстоятельства обуславливают необходимость и актуальность поиска и использования нетрадиционных методов и средств позволяющих осуществлять быструю обработку криптоалгоритмов. Один из подходов к решению рассматриваемой задачи основывается на применении методов и средств обработки криптографической информации использующих модулярную систему счисления (МСС). В литературных источниках [1 – 5] показана высокая эффективность применения МСС при решении задач обработки цифровой информации (решение задач реализации БПФ и ДПФ, задач теоретико-числовых преобразований, реализация целочисленных арифметических операций конечного поля Галуа, конечного поля комплексных чисел с целыми вещественной и мнимой частями, конечных колец и пр.).

Цель статьи – сформулировать концепцию создания быстрой и достоверной обработки криптографический информации на основе использования информационной технологии распределенных вычислений в МСС.

Основная часть

Известно, что современные системы обработки криптографической информации, функционирующие в позиционной системе счисления (ПСС) обладают существенным недостатком – наличием межразрядных связей. Данный недостаток влияет на методы реализации арифметических операций, усложняя аппаратуру, снижает достоверность вычислений и ограничивая быстродействие СОКИ.

Одним из практических направлений повышения пользовательской производительности и надёжности СОКИ (реализующих в конечном итоге совокупность целочисленных модульных операций – сложение и умножение) является внедрение нетрадиционных методов представления и параллельной обработки информации в числовых системах с параллельной структурой. В этом плане обращает на себя внимание МСС, обладающая максимальным уровнем внутреннего параллелизма в организации процесса переработки информации и способностью обнаруживать и исправлять ошибки, возникающие в динамике процесса обработки информации. Одной из главных особенностей МСС является отсутствие межразрядных связей в обрабатываемых операндах при реализации арифметических операций.

Как отмечается в литературе [1, 3], одно из свойств МСС – малоразрядность остатков, представляющих операнд. Именно это свойство дает возможность широкого выбора вариантов теоретических и системотехнических решений при реализации модульных арифметических операций и позволяет существенно повысить быстродействие выполнения арифметических операций за счет возможности применения (в отличие от ПСС) табличной арифметики, где арифметические операции сложения, вычитания и умножения выполняются практически в один такт и применении принципа кольцевого сдвига (ПКС).

Известно, что операнд в МСС представляется набором из n остатков $\{a_i\}$, образованных путем последовательного деления исходного числа A на n взаимно попарно простых чисел $\{m_i\}$, для $(i = \overline{1,n})$. В этом случае совокупность остатков $\{m_i\}$ непосредственно отождествляется с суммой n простых полей Галуа вида $\sum_{i=1}^{n} GF(m_i)$.

Для рассмотрения методов реализации арифметических операций в МСС достаточно рассмотреть вариант для произвольного конечного поля Галуа $GF(m_i)$ при i = const, т.е. для конкретной приведенной системы вычетов по модулю m_i.

Как отмечалось выше, тенденция в реализации криптографических преобразований направлена на увеличение длины разрядной сетки СОКИ. Уже сейчас предлагается к практическому использованию СОКИ для криптографических преобразований с

l = 4 и l = 8. В этом случае

$N_4 = 2^{32} \times 2^{32} = 2^{64} = 18446744073709551616$ и

$N_8 = 2^{64} \times 2^{64} = 2^{128}. \approx 3{,}4 \times 10^{38}$.

Очевидно, что табличные методы реализации арифметических операций в ПСС практически не применимы. В тоже время, при реализации криптопреобразований в МСС с l = 4 и l = 8 соответственно получим $N_{4\ МСС} = 2397$ и $N_{8\ МСС} = 13275$, что вполне приемлемо.

В общем случае таблица модульного умножения для произвольного основания m_i МСС симметрична относительно левой (главной) и правой диагоналей, а также вертикали и горизонтали. Симметричность относительно левой диагонали определяется коммутативностью операции $a_i\beta_i$ умножения, а симметричность относительно правой диагонали определяется выполнением следующего сравнения

$$(m_i - a_i)(m_i - \beta_i) \equiv a_i\beta_i (\mathrm{mod}\ m_i).$$

Симметричность относительно вертикали и горизонтали определяется из условия кратности значения модуля сумме симметричных чисел таблицы умножения

$$a_i\beta_i + a_i(m_i - \beta_i) \equiv 0(\text{mod } m_i);$$
$$a_i\beta_i + \beta_i (m_i - a_i) \equiv 0(\text{mod } m_i).$$

В этом случае очевидно, что для табличной реализации операции модульного умножения $a_i\beta_i \pmod{m_i}$ достаточно иметь числовую информацию только о ее восьмой части. Отсюда возникает возможность упростить таблицу модульного умножения.

Исследование возможности реализации одной модульной операции с помощью таблицы, реализующей операцию ей обратную (сложения и вычитания) позволило получить следующее аналитическое соотношение

$$\left(\gamma_a, a'_i\right) + \left(\gamma_\beta, \beta'_i\right) =$$
$$= m_i - \left\{\left[m_i - \left(\gamma_a, a'_i\right)\right] - \left(\gamma_\beta, \beta'_i\right)\right\},$$

где $a_i = \left(\gamma_a, a'_i\right)$; $\beta_i = \left(\gamma_\beta, \beta'_i\right)$ – входные операнды, представленные в коде табличного умножения.

Из полученного выражения следует, что для получения результата операции модульного сложения достаточно знать результат операции модульного вычитания. Возникает возможность эффективно, с точки зрения уменьшения количества оборудования ПЗУ, использовать табличные методы для реализации одновременно трех модульных арифметических операций: умножения, сложения и вычитания.

Несмотря на различие цифровой структуры таблиц модульных операций сложения, вычитания и умножения, предлагаемый подход к реализации арифметических операций в МСС позволяет синтезировать конструктивно простую, высоконадежную и производительную СОКИ в МСС, основу которого составляют три отдельных коммутатора, каждый из которых реализует только 0,25 части соответствующей полной таблицы модульных операций умножения и вычитания [1].

В [2] рассмотрен принцип кольцевого сдвига реализации арифметических операций в МСС, особенность которого заключается в том, что результат арифметической операции $(\alpha_i \pm \beta_i) \bmod m_i$ по произвольному модулю МСС, заданной совокупностью $\{m_j\}$ $(j = \overline{1,n})$ оснований, определяется только за счет циклических сдвигов заданной цифровой структуры. Действительно, известная теорема Кэли устанавливает изоморфизм между элементами конечной абелевой группы и элементами группы перестановок. Одним из следствий теоремы Кэли является вывод о том, что отображение элементов абелевой группы на группу всех целых чисел является гомоморфным. Это обстоятельство позволяет организовать процесс определения результата арифметических операций в МСС посредством использования ПКС.

Пусть для заданной операции модульного сложения $(\alpha_i + \beta_i) \bmod m_i$ в поле $GF(m_i)$ составлена таблица Кэли. Из существования нейтрального элемента в поле $GF(m_i)$ следует, что в таблице Кэли есть строка (столбец), в которой элементы данного поля стоят в порядке возрастания. Поскольку в поле вычетов $GF(m_i)$ указанные элементы различны (порядок группы равен m_i), следует, что в каждой строке (столбце) таблицы содержатся все элементы поля ровно по одному разу.

Использование перечисленных свойств позволяет реализовать операции модульного сложения и вычитания в МСС путем применения ПКС посредством n кольцевых $M = m_i([\log_2(m_i - 1)] + 1)$ – разрядных сдвигающих регистров. Данное обстоятельство обусловливает возможность реализации арифметической операции сложения в МСС без межразрядных переносов и вычислений промежуточных результатов сложения для одного двоичного разряда сумматора путем только кольцевого сдвига содержимого разрядов кольцевых сдвигающих регистров.

В данном случае исходная цифровая структура для каждого основания МСС представляется в виде содержимого первой строки (столбца) таблицы модульного сложения (вычитания) $(\alpha_i \pm \beta_i) \bmod m_i$ вида

$$P_0^{(m_i)} = \left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(\alpha_{m_i-1})\right],$$

где $\|$ – операция конкатенации (склеивания); $P_v(\alpha_v)$ – k-разрядный двоичный код, соответствующий значению α_v-го остатка $(\alpha_v = \overline{0, m_i - 1})$ числа по модулю m_i; $\left(k = \left[\log_2(m_i - 1) + 1\right]\right)$.

Отметим, что время реализации арифметической операции A + B в МСС будет определяться временем выполнения операции для максимального значения $(\beta_{\max i}$ $(i = \overline{1,n})$ остатка из совокупности $\{\beta_i\}$ для данного операнда $B = (\beta_1, \beta_2, \ldots, \beta_n)$, т.е. $t_\pm = \beta_{\max i}\tau$, где β_i – число разрядов кольцевого регистра сдвига.

С учётом выше рассмотренного общую структуру реализующую предлагаемую концепцию обработки криптографической информации в МСС расширенного поля Галуа $GF(2^v)$ можно представить следующим образом (рис. 1). На основе анализа основных характеристик и принципов построения СОКИ, а также требований, предъявляемых к качеству решения прикладной задачи, осуществляется выбор единственно оптимального решения по организации процесса обработки криптоинформации

$W = \{w_1, w_2, \ldots, w_E\}$, при котором организация вычислений $P(w_e)$ полностью соответствует параллельно-конвейерной структуре СОКИ P(D). В этом случае математическая постановка задачи формулируется следующим образом

$$w_{опт} \in W\left[w_e = w_{опт} \to P(w_e) \leftrightarrow P(D)\right].$$

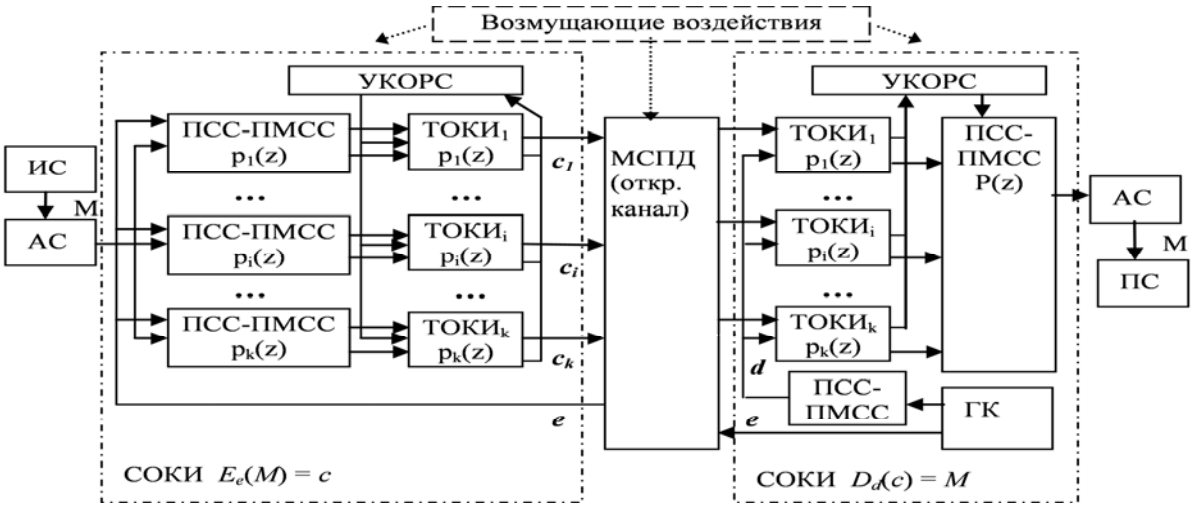

Рис. 1. Общая структура системы обработки криптографической информации, функционирующей в ПМСС

Данные системы, выполняется реконфигурация структуры СОКИ.

Полученное, с использованием СОКИ, криптографическое сообщение, представленное в коде ПМСС, передаётся по каждому модулю, в параллельном избыточном модулярном коде (R-коде), в n-канальную систему передачи данных.

Применение, в рассматриваемом случае, избыточного модулярного кода позволяет обеспечить обнаружение и исправление однократных и многократных ошибок, возникающих при обработке и передаче криптограмм в результате воздействия помех различного происхождения, вмешательства злоумышленников и пр.

Поскольку векторам L нелинейного R-кода соответствуют числа, представленные в ПМСС с взаимно простыми основаниями $m_1, m_2, ..., m_n$., эти коды могут иметь любое минимальное кодовое расстояние d_{min} в зависимости от степени избыточности, причем для любой заданной МСС величина R однозначно определяет корректирующие возможности R-кода.

Легко показать, что R-код имеет минимальное кодовое расстояние d_{min} только в том случае, если степень избыточности не меньше произведения любых $d_{min} - 1$ оснований заданной МСС, т.е.

$$R \geq \prod_{i=1}^{d-1} m_{q_i},$$

где $q_i = 1, 2, ..., n$.

Основания МСС $m_1, ..., m_n$. являются информационными, а основания $m_{n+1}, ..., m_{n+k}$ – контрольными. Если МСС упорядочена $(m_k < m_{k+1})$, то $d_{min} = k + 1$, и если МСС расширяется путем добавления k оснований и каждое основание больше любого информационного основания, то минимальное расстояние кода автоматически увеличивается на величину k. Увеличить d_{min} можно также за счет уменьшения числа информационных оснований, т.е. за счет перехода к вычислениям с меньшей точностью.

Таким образом, между корректирующими возможностями R-кодов и точностью вычислений существует обратно пропорциональная зависимость. Одна и та же СОКИ может выполнять арифметические операции с высокой точностью, но небольшой надежностью или с меньшей точностью, но с более высокой надежностью и скоростью.

На приёмной стороне в СОКИ выполняются следующие операции: контроль наличия и исправление ошибок в криптограмме, представленной в коде ПМСС с использованием известных апробированных методов; дешифрование кодограммы СОКИ в ПМСС; представление исходного сообщения в ПСС.

Процесс обнаружения ошибок в ПМСС с одним контрольным m_{n+1} основанием заключается в следующем. Пусть задана упорядоченная ПМСС основаниями $m_1, m_2, ..., m_n$.. Рабочий диапазон определится величиной $M = \prod_{i=1}^{n} m_i$.

Введем одно контрольное основание $m_{n+1} > m_n$ взаимно простое с любым из информационных оснований. В этом случае полный диапазон ПМСС определится как произведение $M_1 = Mm_{n+1}$. Принцип контроля и коррекции ошибок в МСС основан на результата доказательства такой теоремы.

Теорема. Если ПМСС упорядочена, то искаженное число $\tilde{A} = (a_1, a_2, ..., \tilde{a}_i, ..., a_{n+1})$ является

неправильным при условии, что $A=(a_1,a_2,...,a_i,...,a_{n+1})$ правильное.

Таким образом, чтобы обнаружить факт искажения числа $\tilde{A}=(a_1,a_2,...,\tilde{a}_i,...,a_{n+1})$ необходимо сравнить его с рабочим диапазоном M. Если $A<M$, то либо ошибки нет, либо она имеет более сложный характер.

Для определения и исправления ошибок в криптограмме введем еще одно контрольное основание $m_{n+2}>m_{n+1}$. В этом случае полный диапазон ПМСС определяется как $M_2=M_1m_{n+2}$. В этом случае алгоритм определения и исправления ошибочного остатка в ПМСС представится следующим образом.

1. Вычисляются все проекции числа

$$\tilde{A}=(a_1,a_2,\dots,a_n,a_{n+1},a_{n+2})$$

по всем основаниям ПМСС

$$\tilde{A}_1=(a_2,a_3,\dots,a_n,a_{n+1},a_{n+2});$$

$$\tilde{A}_2=(a_1,a_3,\dots,a_n,a_{n+1},a_{n+2});$$

$$\dots\dots\dots\dots\dots\dots$$

$$\tilde{A}_{n+1}=(a_1,a_2,\dots,a_n,a_{n+2});$$

$$\tilde{A}_{n+2}=(a_1,a_2,\dots,a_n,a_{n+1}).$$

2. Полученные проекции $\tilde{A}_i\left(i=\overline{1,n+2}\right)$ сравниваются с рабочим диапазоном M.

3. Определяем проекцию числа, для которой $\tilde{A}_i<M,$ и исправляем ошибочный остаток:

$$a_i=\tilde{a}_i+\left[\frac{m_i(1+jm_{n+1})}{m_{n+1}m_i}-\frac{\tilde{A}}{B_i}\right],$$

где $B_i=\bar{m}_iM/m_i$ ортогональный базис ПМСС;

$j=0,1,2,\dots;$ m_i – вес ортогонального базиса.

Из характера рассмотренного R-кода видна его полная арифметичность. Введенные основания включены в общую систему оснований ПМСС и коды, содержащие цифры по всем как основным, так и контрольным разрядам участвуют в любой операции операционного устройства СОКИ. Обработка основных и дополнительных цифр производится совершенно одинаково, без какого-либо различия. Это позволяет считать, что обработка информации в ПМСС может вестись без контроля каждого полученного промежуточного результата. Величина (длина) этапа контроля определяется в каждом отдельном случае либо по законченному циклу обработки массива информации, либо в соответствии с вероятностью возникновения одиночной ошибки. Конечный результат вычислений каждого этапа может быть подвергнут контролю и его правильность подтверждает правильность проведения всех операций данного этапа. Отметим, что введение только одного контрольного основания позволяет обнаружить не только любую одиночную ошибку, как и в позиционной системе счисления, но и большую часть двойных.

Отличительной особенностью ПМСС, как отмечалось выше, является существенное проявление первичной информационной избыточности при введении вторичной $Q(l)$ (за счет наличия контрольных оснований ПМСС). Можно показать, что R-код может (в некоторых случаях) обнаруживать некоторое число ошибок более высокой кратности, чем та, которая допускается общей теорией кодирования, т.е. значением d_{min}. Пусть для МСС минимальное кодовое расстояние определяется значением d_{min}. Предположим, что в МСС имеются такие основания, число которых $l\ge d_{min}$, при этом

$$Q(l)=\prod_{j=1}^{l}m_{Z_j}<R=M_1/M.$$

Тогда у вектора ошибки $\Delta A=\tilde{A}-A$ должно быть не менее $n-l$ нулевых компонент. Представим вектор ΔA в виде

$$\Delta A=(O,O,\dots\Delta a_{Z1}\dots,O,\Delta A\,a_{Z_1},\dots,O).$$

В позиционной системе счисления ΔA определяется как

$$\Delta A=B_{Z_1}a_{Z_1}+\dots+B_{Zl}a_{Z_l}.$$

Учитывая, что $B_{Z_1}=\bar{m}_{Z_1}M_1/m_{Z_1}$, где $\bar{m}_{Z_1}$ – вес l-ортогонального базиса, запишем

$$\Delta A=\frac{\bar{m}_{Z_1}M_1}{m_{Z_1}}a_{Z_1}+\dots+\frac{\bar{m}_{Z_l}M_1}{m_{Z_l}}a_{Z_l}=R\Delta R\cdot Z,\quad(1)$$

где $R\cdot\Delta R=\frac{M_1}{Q(l)};Z=\sum_{j=1}^{l}\bar{m}_{Z_j}Q_j(l)$ и

$$Q_j(l)=\frac{Q(l)}{m_{Z_j}}\left(M_1=R\cdot\Delta R\cdot Q_j(l)\cdot m_{Z_j}\right).$$

Из (1) очевидно, что $\Delta A=O\left[\mathrm{mod}\,M_1/a(l)\right]$,

тогда $\Delta A/Z_O=R\Delta R=M_1/Q(l)\ge M_1/R=M,$ (2)

где $Z_O=1,2,\dots.$

Из (2) следует, что $\Delta A\ge M$, и, таким образом,

$$\tilde{A}=A-\Delta A\ge M \qquad (3)$$

Неравенство (3) показывает, что сумма любого числа A и числа соответствующего вектору ошибки ΔA, не могут принадлежать множеству M, т.е. подобную ошибку можно обнаружить. Отметим, что даже в тех случаях, когда $Q(l)>R$, среди ошибок ΔA найдутся такие, которые удовлетворяют неравенству (3). Это возможно за счет наличия вторичной информационной избыточности. Специфика представления чисел в ПМСС позволяет в ряде случаев не только обнаружить ошибку, но и найти место ее возникновения, используя только контрольное основание, что невозможно при существующих методах контроля и коррекции в ПСС, например, при контроле по модулю. Осуществить коррекцию ошибок при $d_{min}=2$ можно либо способом

проекций, либо используя понятие альтернативной совокупности (АС) чисел [1, 3].

На последнем этапе конвейерной обработки криптографической информации осуществляется обратное преобразование полученного информационного продукта из модулярного кода ПМСС в позиционный двоичный код.

В итоге математическая модель реализуемая СОКИ реального времени в ПМСС, при заданной системе ограничений имеет следующий вид:

$$P\left(A,\left\{p^{п}(z),p^{к+г}(z)\right\},s_j,u_l,f_d,o_a,\hat{u}_в,t\right)\to\max,$$

$$T_{рек}\left(\left\{p^{п}(z),p^{к+г}(z)\right\},s_j,u_l,f_d,o_a,\hat{u}_в\right)\le T_{доп},$$

$$Q_{рек}\left(\left\{p^{п}(z),p^{к+г}(z)\right\},s_j,u_l,f_d,o_a,\hat{u}_в\right)\ge Q_{доп},$$

где $T_{рек}\left(\left\{p^{п}(z),p^{к+г}(z)\right\},u_l,o_a,\hat{u}_в\right)$ – время выполнения задания СОКИ; $Q_{рек}\left(\left\{p^{п}(z),p^{к+г}(z)\right\},u_l,f_d,o_a,\hat{u}_в\right)$ – точность выполнения задания СОКИ; A – исходное задание, представляющее набор процедур реализуемых СОКИ в процессе обработки информации; $\hat{u}_в\in\hat{U}=[\hat{u}_1,\hat{u}_2,...,\hat{u}_m]$ – совокупность методов и алгоритмов выполнения обменных операций; $o_a\in O=\left[o_1,o_2,...,o_п\right]$ – совокупность возможных методов реконфигурации; $f_d\in F=\left[f_1,f_2,...,f_M\right]$ – совокупность возможных алгоритмов обнаружения и исправления ошибок в кодах ПМСС.

Выводы

В статье рассмотрена концепция создания СОКИ, обладающей повышенными характеристиками по быстродействию обработки модульных операций. Основное преимущество предложенного подхода состоит в возможности достижения высокой производительности обработки криптографической информации, а также в создании уникальной системе контроля и коррекции ошибок данных. При этом процедуру контроля и коррекции данных, возможно, проводить как в процессе передачи информации по каналу связи, так и при обработки информации без останова вычислений. Последнее обстоятельство особенно важно для СОКИ, функционирующей в реальном времени.

Полученные результаты исследований, проведенных в статье, также целесообразно использовать в системах и устройствах обработки больших массивов цифровой информации реального времени, представленной в целочисленном виде.

Список литературы

1. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.

2. Методы многоверсионной обработки информации в модулярной арифметике: моногр. / [В.И. Барсов, В.А. Краснобаев, А.А. Сиора, И.В. Авдеев]. – Х.: МОН, УИПА, 2008. – 460 с.

3. Барсов В.И. Методология параллельной обработки информации в модулярной системе счисления: моногр. / В.И. Барсов, Л.С. Сорока, В.А. Краснобаев. – Х.: МОН, УИПА, 2009. – 288 с.

4. Метод повышения производительности и отказоустойчивости нейрокомпьютеров обработки криптографической информации автоматизированных систем управления специального назначения на основе модулярной арифметики / В.И. Барсов, В.А. Краснобаев, А.А. Замула, О.В. Зефирова // Прикладная радиоэлектроника. Научн.-техн. ж. – Х.: ХНУРЭ, 2007. – Вип. 2, т. 6. – С. 282-287.

5. Барсов В.И. Устройства обработки информации в МСС на основе применения метода унитарного кодирования / В.И. Барсов, В.О. Жадан, В.А. Краснобаев, Е.А. Сотник // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 8 (98). – С. 25-28.

Поступила в редколлегию 5.01.2012

Рецензент: д-р техн. наук, проф. И.О. Фурман, Харьковский национальный технический университет сельского хозяйства им. Петра Василенка, Харьков.

КОНЦЕПЦІЯ СТВОРЕННЯ СИСТЕМИ ШВИДКОЇ ТА ДОСТОВІРНОЇ ОБРОБКИ КРИПТОРГАФІЧНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ РОЗПОДІЛЕННИХ ОБЧИСЛЕНЬ

В.І. Барсов, В.О Краснобаєв, А.С. Фещенко

У даній статті розглянута концепція створення системи криптографічної обробки інформації на основі використання модулярної системи числення (МСЧ). Це дозволить зменшити обчислювальну складність реалізації процесу криптографічних перетворень, а також підвищити ефективність контролю і корекції помилок в МСЧ при реалізації технології Grid обчислень.

Ключові слова: *система обробки криптографічної інформації, шифрування, модулярна система числення, криптоперетворення з відкритим ключем, розподілені обчислення.*

CONCEPT DEVELOPMENT SYSTEM QUICKLY AND RELIABLY CRYPTOGRAPHIC INFORMATION TREATMENT BASED ON THE USE OF INFORMATION TECHNOLOGY DISTRIBUTED COMPUTING

V.I. Barsov, V.O. Krasnobayev, A.S. Feschenko

In this article the concept of creating a system of cryptographic information processing based on the use of a modular number system (MNS). This will reduce the computational complexity of the process of cryptographic transformations, as well as increase the efficiency of monitoring and correction of errors in the MNS in the implementation of Grid computing technologies.

Keywords: *cryptographic information processing system, encryption, modular number system, cryptographic transformation of public-key, distributed computing.*