УДК 681. 142

С.О. Мартыненко, М.В. Дугин, В.А. Краснобаев

Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ БЕЗОТКАЗНОСТИ СПЕЦПРОЦЕССОРА ОБРАБОТКИ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

В статье рассмотрены варианты математических моделей надежности спецпроцессора обработки криптографической информации (СОКИ) в модулярной системы счисления (МСС). Предложенные математические модели надежности СОКИ в МСС основывается на принципе параллелизма обработки информации в непозиционной системе счисления.

Ключевые слова: *спецпроцессор обработки криптографической информации, модулярная система счисления, криптографическая обработка информации, надежность, безотказность, производительность*.

Введение

Характерным для современных технологических применений криптографических технических средств (embedded processor, processor node) реализации КП является существенное возрастание требований к скорости обработки КП и надежности (отказоустойчивости) их функционирования. Так, например, для КП в группе точек эллиптических кривых, при вычислении порядка эллиптической кривой над полем размерностью 160 бит необходимое время равно 9с. Для поля в 240 бит – 25с, для поля в 500 бит – 5 мин., для поля в 1000 бит – 1 час, для поля 2000 бит – 14 часов (вычисления КП производились с помощью процессора PENTIUM с тактовой частотой 500 МГц). При возрастание, например, порядка RSA криптосистемы или поля эллиптической кривой вычислительная сложность КП существенно возрастает, что вызывает необходимость обеспечения высокой надежности функционирования СОКИ.

В статье рассматривается возможность повышения надежности СОКИ за счет применения кодов в непозиционной модулярной системе счисления (МСС).

Таким образом, актуальна и важна задача разработка математической модели и метода повышения надежности СОКИ реального времени в МСС.

Основная часть

Рассмотрим некоторые варианты построения математических моделей СОКИ на основе использования МСС.

Первый вариант. Математическая модель безотказности СОКИ в МСС с учетом влияния надежности переключающих устройств.

Исходя из анализа литературных источников, математической моделью безотказности СОКИ в МСС целесообразно считать также модель скользящего резервирования с ненагруженным (холодным) резервом, которая используется в ПСС при динамическом резервировании с учетом надежности коммутатора [1 – 3]. При предложенном варианте математической модели надежности СОКИ в МСС содержит: основную вычислительную систему, состоящую из n информационных вычислительных трактов (ИВТ); резервную вычислительную систему, состоящую из k резервных ВТ (РВТ); дополнительную систему, состоящую из двух контрольных вычислительных трактов (КВТ); автомат надежности, выполняющий функции определения отказавших ИВТ, отключения их и подключения РВТ. Отметим, что дополнительная система органически и конструктивно входит в автомат надежности (АН). Она выделена для того, чтобы показать сущность информационного резервирования в КВ. Так, при появлении ошибок, вызванных сбоями в одном из ИВТ, они устраняются посредством КВТ известными методами. Таким образом, МСОИ, построенная в соответствии с предложенной математической моделью, является (как и троированная вычислительная система с мажоритарным органом) нечувствительной к сбоям в одном из ИВТ.

Рассмотрим, как, используя предложенный вариант математической модели (при известных до-

пущениях для ИВТ и РВТ), можно рассчитать вероятность безотказной работы СОКИ в МСС.

Пусть задана упорядоченная МСС набором взаимно попарно простых чисел: $m_1, m_2, \ldots, m_n, m_{n+1}, m_{n+2}, \ldots, m_{n+2+k}$, где n и k соответственно количество рабочих и резервных ВТ, а количество контрольных ВТ равно двум (m_{n+1}, m_{n+2}).

Получим формулу для количественной оценки показателя надежности (вероятности безотказной работы). Очевидно, СОКИ в МСС будет работать безотказно при следующих событиях:

– основная система, состоящая из m_j $(j=\overline{1, n+2})$ вычислительных трактов, в течение времени t не отказала;

– отказало не более k резервных вычислительных трактов, и АН работает безотказно.

Используя формулу вероятности безотказной работы для скользящего резервирования с ненагруженным резервом и идеальным (в смысле надежности) АН, и учитывая, что вероятность безотказной работы вычислительного тракта СОКИ в МСС равна $P_1(t)=e^{-\lambda_1 t}$, вероятность безотказной работы АН равна $P_{AH}(t)=e^{-\lambda_A t}$ и частота отказов равна $\lambda_1 e^{-\lambda_1 t}$, получим формулу для определения вероятности безотказной работы в виде

$$P_{COK}^{(k)}(t)=e^{-n\lambda_1 t}\sum_{i=1}^{k}\left(n\frac{\lambda_1}{\lambda_A}\right)^i - n\frac{\lambda_1}{\lambda_A}e^{-(\lambda_A+n\lambda_1)t}\sum_{i=0}^{k-1}\sum_{j=0}^{k-1-i}\left(n\frac{\lambda_1}{\lambda_A}\right)^j\frac{(n\lambda_1 t)^i}{i!}, \quad (1)$$

где $\lambda_1=\alpha\lambda_э=\left\{\left]\frac{1}{n+2+k}\left(\sum_{i=1}^{n+2+k}[\log_2(m_i-1)]+1\right)\right[\right\}\lambda_э^-$ – интенсивность отказов одного ВТ; $\lambda_A=\lambda'_A+2\lambda_1$ – интенсивность отказов АН (λ'_A – интенсивность отказов переключающего устройства; $2\lambda_1$ – интенсивность отказов контрольных ВТ).

Второй вариант. Совершенствование метода повышения безотказности СОКИ в МСС на основе использования принципа активной отказоустойчивости.

Совершенствованный метод повышения безотказности СОКИ в МСС основан на реализации принципа активной адаптации (с перестройкой структуры СОКИ в процессе функционирования) и предполагает использование вышеприведенной математической модели безотказности вида (1).

Однако, данная ММ не учитывает все свойства МСС. Действительно выражение (1) не учитывает влияние функционального резервирования, т.е. способность одного ИВТ взять на себя функции до r отказавших при условии $m_j \geq \prod_{i=1}^{r} m_{k_i}$. При этом в формуле (1) необходимо произвести замену $k'=k+r$.

Представленная математическая модель надежности (1) дает возможность рассчитывать безотказность СКОИ в МСС посредством простых и известных соотношений. В теоретическом плане эта математическая модель надежности позволяет исследовать и учитывать все основные виды резервирования (структурное, информационное и функциональное), обусловленные основными свойствами МСС [4].

Структурное резервирование. Математическая модель надежности СОКИ в МСС построена на основе введения вторичной структурной избыточности, т.е. применяя структурное резервирование. Информационные и контрольные вычислительные тракты играют роль основных элементов резервированной системы, а резервные вычислительные тракты - роль резервных элементов.

Информационное резервирование. Проявляется в использовании дополнительной информации, вводимой посредством использования контрольных вычислительных трактов по основаниям m_{n+1} и m_{n+2}. При возникновении ошибок, вызванных сбоями в одном из вычислительных трактов m_j $(j=\overline{1,n+2})$ СОКИ по одному из рабочих или контрольных оснований МСС, они устраняются известными методами. Таким образом, СОКИ в МСС, построенная в соответствии с разработанной математической моделью, является (как и троированная мажоритарная структура) нечувствительным к сбоям.

Функциональное резервирование. Этот вид резервирования проявляется в случае, если выполняется условие $m_j \geq \prod_{i=1}^{r} m_i$, т.е. если один вычислительный тракт СОКИ может взять на себя функции r отказавших вычислительных трактов (как указывалось выше) равноценно добавлению к k еще r резервных вычислительных трактов. В этом случае выражение (1) представится в виде

$$P_{COK}^{(k+r)}(t)=e^{-n\lambda_1 t}\sum_{i=1}^{k+r}\left(n\frac{\lambda_1}{\lambda_A}\right)^i - n\frac{\lambda_1}{\lambda_A}e^{-(\lambda_A+n\lambda_1)t}\sum_{i=0}^{k+r-1}\sum_{j=0}^{k+r-1-i}\left(n\frac{\lambda_1}{\lambda_A}\right)^j\frac{(n\lambda_1 t)}{i!}. \quad (2)$$

Суть усовершенствования предлагаемого метода состоит в повышении точности оценки вероятности безотказной работы СОКИ в МСС. Кроме этого, учет в ММ соотношения $m_j \geq \prod_{i=1}^{r} m_{k_i}$ позволяет повысить безотказность функционирования СОКИ за счет эффекта дополнительного введения к основным (рабочим) дополнительно r резервных вычислительным трактам (рис. 1).

Представление и обработка информации в алгоритме RSA	Криптографическая информация представляется и обрабатывается в МСС, путѐм формирования остатков $\{a_i\}$ чисел от деления их на выбранную систему оснований $\{m_i\}$.
Выбор оснований МСС по заданным критериям	Безотказность СОКИ повышается за счѐт исключения из структурной схемы избыточного оборудования, путем выбора по критерию минимума оборудования операционного устройства. Это снижает интенсивность отказов $\lambda_{СОКИ}$ СОКИ.
Выбор и обоснование математической модели безотказности СОКИ	Безотказность повышается за счет введения резервных вычислительных трактов. Также безотказность повышается за счѐт уменьшения интенсивности отказов $\lambda_{СОКИ}$ СОКИ. При этом используется принцип активной отказоустойчивости.
Метод повышения безотказности СОКИ основан на использовании принципа	Безотказность повышается за счѐт снижения интенсивности $\lambda_{СОКИ}$ отказов и сбоев СОКИ, путѐм использования принципа кольцевого сдвига.
Анализ и сравнительная оценка безотказности СОКИ в МСС	Посредством математических моделей безотказности СОКИ в МСС проводится расчѐт значения P(t) безотказности. Проводится сравнительный анализ безотказности СОКИ в МСС и СОКИ в ПСС. С увеличением длины l разрядной сетки СОКИ (что характерно для современной тенденции развития криптографии) эффективность использования МСС возрастает.
Повышение безотказности СОКИ	

Рис. 1. Метод повышения безотказности СОКИ в МСС

Выводы

1. Совершенствована математическая модель и метод повышения безотказности СОКИ в МСС, основанные на принципе активной отказоустойчивости и на использовании методов динамического резервирования с учетом свойств, правил и принципов представления и обработки информации в модулярной арифметике. Получено аналитические соотношение для оценки безотказности и проведения сравнительного анализа надежности СОИ различных типов. Суть рассмотренного метода состоит в повышении точности оценки вероятности безотказной работы СОКИ в МСС. Это достигается путем учета в математической модели безотказности СОКИ соотношения $m_j \geq \prod_{i=1}^{r} m_{k_i}$. Учет данного обстоятельства позволяет повысить безотказность функционирования СОКИ за счет дополнительного введения к n основным (рабочим) r резервных вычислительных трактов. При этом структура СОКИ в МСС практически соответствует мультимикропроцессорной (кластерной) системы обработки информации в ПСС. Это дало возможность применить известные теоретические и практические положения теории надежности и теории помехоустойчивого кодирования для анализа и синтеза структуры СОК в МСС. Отметим, что СОКИ в МСС, построенная в соответствии с предложенной в статье математической моделью, является (как и троированная вычислительная система в ПСС с мажоритарным органом) нечувствительной к сбоям в одном из ИВТ.

2. На основе исследований разработанной математической модели безотказности СОКИ в МСС, в работе научно обоснованы основные направления в создании отказоустойчивых структур спецпроцессоров в МСС: применение метода замены и метода постепенной деградации. В качестве базовой структуры предлогается разработанная архитектура СОКИ в МСС, основанная на применении комбинированного метода адаптации: последовательного применения методов замены и методов постепенной деградации. Данная структура объединяет положительные свойства обоих методов повышения безотказности СОКИ.

Список литературы

1. Краснобаев В.А. Методы повышения надежности специализированных ЭВМ систем и средств связи / В.А. Краснобаев. – Х.: МО СССР, 1990. – 172 с.

2. ДСТУ 2606-94. Средства вычислительной техники. Отказоустойчивость и живучесть. Общие технические требования.

3. Барсов В.И. Методология параллельной обработки информации в модулярной системе счисления: монография / В.И. Барсов, Л.С. Сорока, В.А. Краснобаев. – Х.: МОН, УИПА, 2009. – 268 с.

4. Сиора А.А. Отказоустойчивые системы с версионно-информационной избыточностью в АСУ ТП: монография / А.А. Сиора, В.А. Краснобаев, В.С. Харченко. – Х.: МОН, НАКУ им. Н.Е. Жуковского «ХАИ», 2009. – 320 с.

Поступила в редколлегию 2.08.2010

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского “ХАИ”, Харьков.

МАТЕМАТИЧНА МОДЕЛЬ БЕЗВІДМОВНОСТІ СПЕЦПРОЦЕСОРА ОБРОБКИ КРИПТОГРАФІЧНОЇ ІНФОРМАЦІЇ В МОДУЛЯРНІЙ СИСТЕМІ ЧИСЛЕННЯ

С.О. Мартиненко, М.В. Дугін, В.А. Краснобаєв

У статті розглянуті варіанти математичних моделей надійності спецпроцесора обробки криптографічної інформації (СОКІ) в модулярній системи числення (МСЧ). Запропоновані математичні моделі надійності СОКІ в МСЧ грунтується на принципі паралелізму обробки інформації в непозиційній системі числення.

Ключові слова: *спецпроцесор обробки криптографічної інформації, модулярна система числення, криптографічна обробка інформації, надійність, безвідмовність, продуктивність.*

MATHEMATICAL MODEL OF FAULTLESSNESS OF THE SPECIAL PROCESSOR OF TREATMENT OF CRYPTOGRAPHIC INFORMATION IN MODULYARNOY TO NUMBER SYSTEM

S.O. Martynenko, M.V. Dugin, V.A. Krasnobaev

In the article the variants of mathematical models of reliability of the special processor of treatment of cryptographic information (STCS) are considered in the modular number systems (MNS). Offered mathematical models of reliability STCSin MNS based on principle of parallelism of treatment of information in the unposition number system.

Keywords: *special processor of treatment of cryptographic information, modular number system, cryptographic treatment of information, reliability, faultlessness, productivity.*