УДК 621.391 (007.5)

05.00.00 Технические науки

КОНТРОЛЬ ОШИБОК ФУНКЦИОНИРОВАНИЯ ГЕНЕРАТОРОВ ПСП, РЕАЛИЗУЮЩИХ КРИПТОГРАФИЧЕСКИЕ ФУНКЦИИ

Углов Алексей Евгеньевич
Краснодарское высшее военное училище, Краснодар, Россия

Представлены алгоритмы и схемы построения надёжных генераторов псевдослучайных последовательностей (ГПСП) на основе многозначных кодов модулярной арифметики. Разработан алгоритм численного контроля операции арифметического сложения в Z_m, отличающийся введением различных правил выполнения операции «формирования» разряда признака переполнения и операции внесения поправки коррекции результата контроля. Построена схема локального контроля сумматора в Z_m, отличающаяся от известных введением схемы формирования разряда признака переполнения и схемы учета поправки результата контроля. Построена схема сквозного контроля модулярных сумматоров и ключевого запоминающего устройства (КЗУ) для хранения криптографических ключей остаточным кодом. От известных предложенная схема отличается введением дополнительной таблицы памяти, схем «формирования" разряда признака переполнения и учета поправки коррекции результата контроля. Приведены результаты сравнительной оценки разработанных схем локального и сквозного контроля модулярных сумматоров с методами введения аппаратной избыточности. На основании результатов сравнительной оценки подтверждена целесообразность применения метода контроля по модулю для повышения надежности ГПСП. При этом, разработанные алгоритмы и схемы сквозного контроля обеспечивают устранение участков разрыва в контроле и расширения фрагментов локального (промежуточного) контроля ГПСП при минимальной аппаратурной и временной избыточности. Областью применения разработанных алгоритмов и схем контроля являются цифровые устройства, реализующие криптографические функции

Ключевые слова: МОДУЛЯРНЫЙ КОНТРОЛЬ, СКВОЗНОЙ КОНТРОЛЬ, ФУНКЦИОНАЛЬНОЕ ДИАГНОСТИРОВАНИЕ, АППАРАТНЫЙ КОНТРОЛЬ, МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ

Doi: 10.21515/1990-4665-128-038

UDC 621.391 (007.5)

Engineering

ERROR CHECK IN OPERATING CRYPTOGRAPHICALLY SECURE PSEUDORANDOM NUMBER GENERATORS

Uglov Alexey Evgenievich
Krasnodar higher military school, Krasnodar, Russia

Algorithms and constructing schemes of trusted pseudorandom number generators (PRNG) based on multivalued codes of residue number system are presented. An algorithm for numerical control of the operation of arithmetic adder Z_m, differing by the introduction of various rules for performing the operation of "forming" of the overflow flag bit and the correction operation of the supervision data adjusting is developed. A scheme for local control of the adder Z_m, which differs from the known by introduction of the overflow flag bit generation scheme and accounting scheme of the supervision data adjusting is constructed. End-to-end monitoring scheme of modular adder control and key storage device (KSD) for holding the crypto key with residual class code is constructed. The proposed scheme differs from the known by additional memory page, overflow flag bit generation scheme and by accounting scheme of the supervision data adjusting. The results of a comparative evaluation of the developed pattern for local and end-to-end monitoring of modular adder control with hardware redundancy are provided. Based on the results of the comparative evaluation it is expedient to use the modular control method in order to increase the reliability of the PRNG. At the same time, the developed algorithms and end-to-end monitoring schemes ensure elimination of the fracture areas in the control and expansion of fragments of the local (intermediate) PRNG control with minimal hardware and time redundancy. Application field of the developed algorithms and control schemes are digital devices with cryptographic functions

Keywords: MODULAR CONTROL, END-TO-END MONITORING, ON-LINE TESTING, HARDWARE CHECK, PRODUCTIVITY IMPROVEMENT

Введение.

Рассматриваются методы повышения надежности функционирования цифровых устройств, реализующих криптографические функции. Понятие надежности цифровых устройств имеет ряд существенных особенностей, обусловленных возможностью возникновения неисправностей (отказов) и их влиянием на достоверность функционирования, достоверность обрабатываемой и получаемой на выходе информации [1, 2]. Причинами возникновения неисправностей могут быть как физические дефекты элементов интегральных микросхем и связей между ними, так и различного рода воздействия, вызывающие необратимые или временные изменения характеристик элементов интегральных микросхем. Следствием возникновения неисправностей являются ошибки функционирования.

В соответствии с положениями теории надежности известно, что для повышения надежности требуется применять методы, основанные на введении различных видов избыточности [1, 2]. Однако, при этом, как правило, кратно увеличивается объем используемого оборудования, что, в соответствии с положениями теории надежности, приводит к увеличению интенсивности отказов и, как следствие, снижению вероятности безотказного состояния [1, 2]. Поэтому, одним из перспективных направлений является применение методов избыточного кодирования, а также, средств встроенного аппаратного контроля. В частности, актуальным является метод, реализующий дифференцированный подход к синтезу алгоритмов и схем контроля. Сущность подхода заключается в разработке алгоритмических и схемотехнических решений, основанных на избыточных кодах, учитывающих специфику контроля для различных криптографических примитивов, а также, в организации участков сквозного контроля для различных сочетаний криптографических примитивов с целью устранения разрывов в контроле. Применение

дифференцированного подхода позволит обеспечить повышение надежности цифровых устройств и, как следствие, достоверности функционирования при заданных аппаратурных затратах.

Цель работы – повышение надежности и достоверности функционирования цифровых устройств, реализующих криптографические функции, путем применения дифференцированного подхода к синтезу алгоритмов и схем контроля.

Разработка алгоритмов и схемотехнических решений построения надёжных ГПСП на основе многозначных кодов модулярной арифметики. Известно, что обычно в качестве ГПСП используются линейные рекуррентные регистры с обратной связью (ЛРР с ОС). На практике для обеспечения необходимых показателей могут применяться узлы, реализующих какой-либо криптографический алгоритм блочного шифрования, например ГОСТ 34.13-2015.

Криптографические алгоритмы состоят из фиксированного набора криптографических примитивов. Одной из наиболее часто используемых операций в криптографических алгоритмах является операция арифметического сложения по модулю M ($M=2^n$, $2^n \pm 1$), реализуемая с помощью соответствующих модулярных сумматоров.

Известно, что для контроля арифметических операций наиболее часто используются контроль дублированием и метод контроля по модулю [3-5]. Классическая схема организации числового контроля по модулю m позволяет осуществлять контроль $A_i, B_i \in Z$ в кольце Z_m.

На практике для реализации аппаратного контроля модулярных сумматоров наибольшее распространение получили методы введения пространственной избыточности, в частности, дублирование и мажоритарные схемы. Однако, в соответствии с предъявляемыми к ГПСП требованиями по уменьшению аппаратурной и временной избыточности

применение методов, основанных на введении пространственной избыточности, является нецелесообразным. Альтернативным по отношению к методам ведения аппаратной избыточности вариантом повышения надежности является метод контроля по модулю. Однако, принимая во внимание, что рассматриваемый криптографический примитив реализует выполнение операций в кольце Z_M, классическая схема контроля по модулю применяться не может и требует доработки.

Предлагаемый метод локального аппаратного контроля (функциональной диагностики с целью контроля функционирования) позволяет организовать контроль арифметических двухместных $\left(\mathrm{A}_i, \mathrm{B}_i \in Z_M,\ M = 2^n, 2^n \pm 1\right)$ операций в кольце Z_m. Схемотехническое решение, реализующее предложенный метод локального контроля представлено на рисунке 1, блок-схема алгоритма функционирования данного криптографического примитива – на рисунке 2.

В контролируемую часть схемы входит двухместный *k*-разрядный сумматор, выполняющий операцию арифметического сложения по модулю M ($M = 2^n, 2^n \pm 1$). В контролирующую часть схемы контроля входят:

- СФРП, обеспечивающая, при наличии признака переполнения, коррекцию результата контроля за счет внесения поправки Δ;
- схема формирования остатка по модулю m (схема свертки – ССВ) для операндов $\mathrm{A}_i, \mathrm{B}_i$ и суммы операндов S_i;
- схема учета (формирования) поправки $\Delta = \left|-M\right|_m$ коррекции результата контроля;

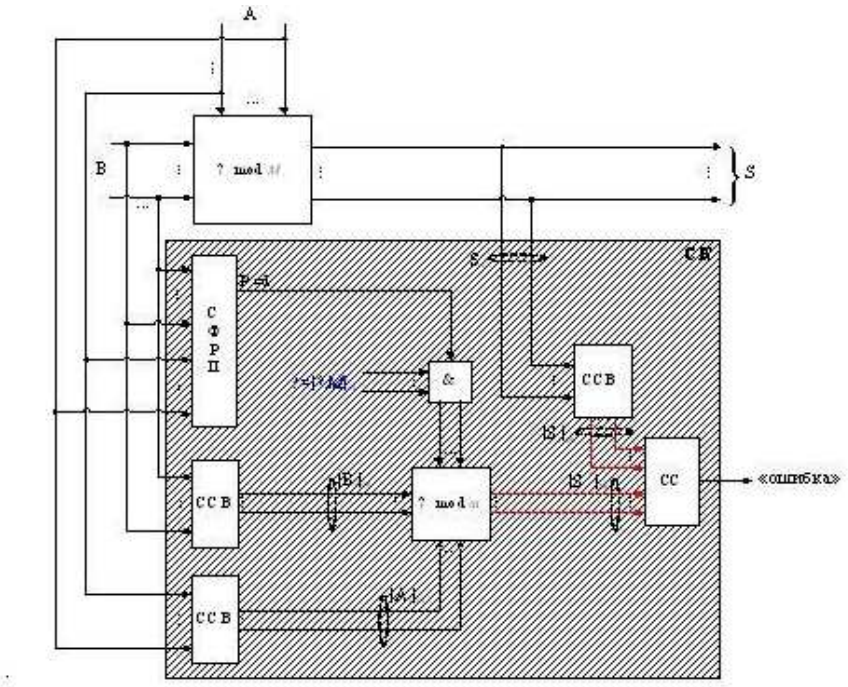


Рисунок 1 – Схема локального контроля по модулю криптографического примитива – «сумматор по модулю M »

- сумматор по модулю m для формирования общего остатка для операндов A_i, B_i с учетом возможного переполнения;
- схема сравнения (СС).

В рассматриваемом схемотехническом решении реализован классический вариант алгоритма моделирования операции ФРП, а именно, метод последовательного перебора (поразрядное, начиная с младших разрядов, суммирование k-битных операндов A_i, B_i). Блок-схема алгоритма представлена на рисунке 3. Особенностью разработанного схемотехнического решения является использование в СФРП для различных типов модулей M измененных алгоритмов ФРП. Применение данных алгоритмов позволит сократить время, затрачиваемое на формирование разряда признака переполнения, и как следствие, на выполнение операции арифметического сложения по модулю M .

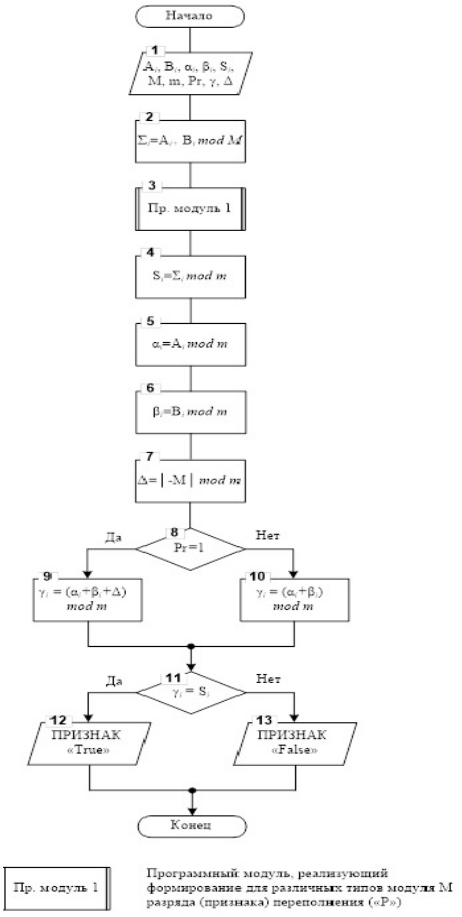


Рисунок 2 – Блок-схема алгоритма функционирования криптографического примитива

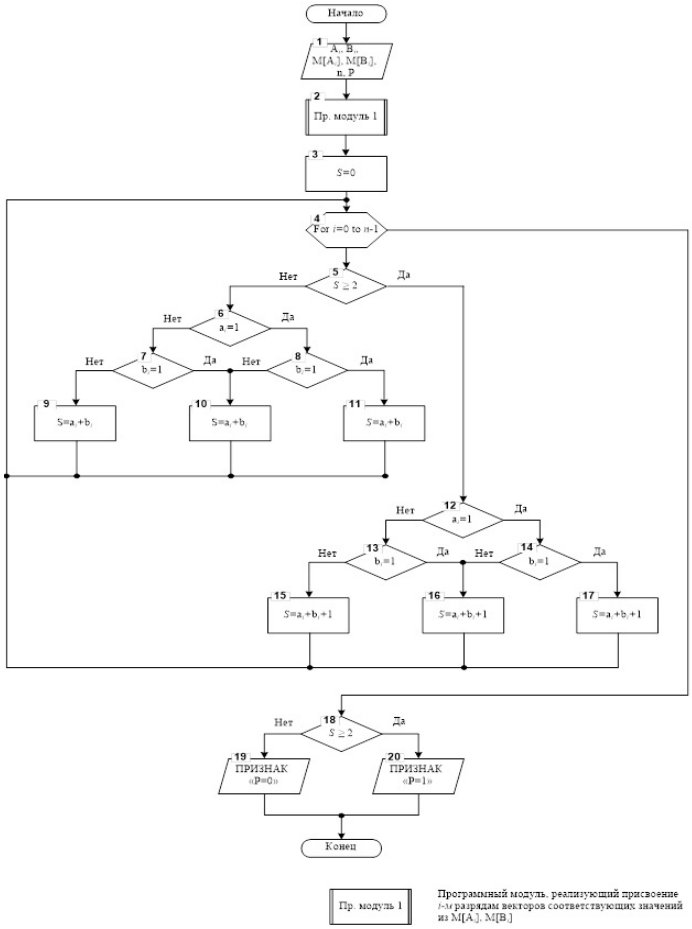
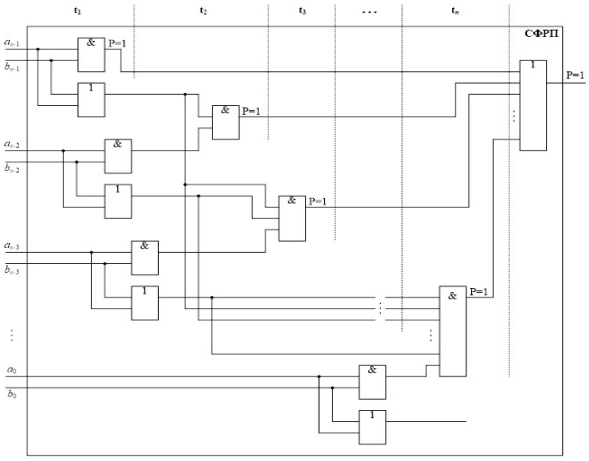


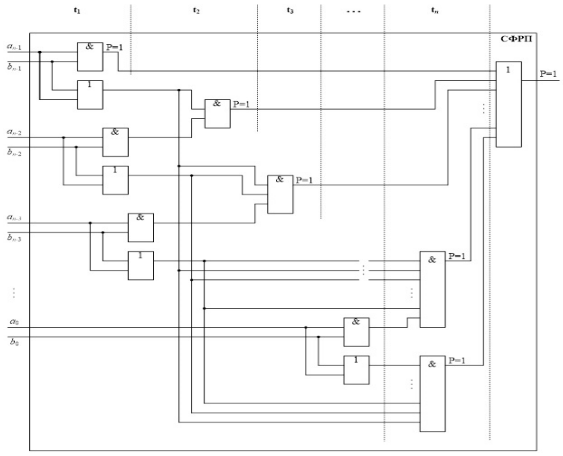
Рисунок 3 – Блок-схема алгоритма моделирования операции ФРП (классический вариант)

Разработка и оценка алгоритмов моделирования операции ФРП. На рисунках 4, 5 представлены схемы ФРП для криптографического примитива – «сумматор по модулю $M\left(M=2^n, 2^n \pm 1\right)$» с разметкой временных интервалов выполнения операции и блок-схемы алгоритмов их реализующих.

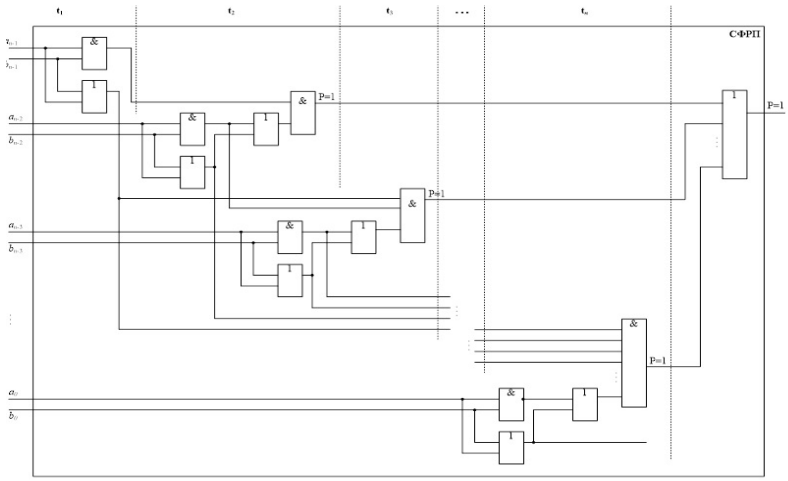
Оценка выигрыша в выполняемом количестве операций при реализации алгоритма ФРП для криптографического примитива – «сумматор по модулю $M=2^n$» по сравнению с классическим вариантом (график зависимости $N_{1шаг}/N_{об}$) представлена на рисунке 6 а [6]. На рисунке 6 б представлена оценка выигрыша в выполняемом количестве операций при реализации предложенного алгоритма ФРП по сравнению с



а) для модуля $M = 2^n$

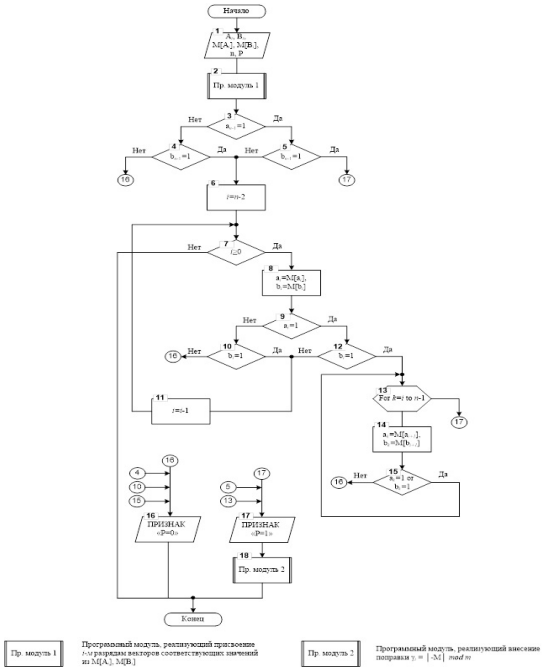


б) для модуля $M = 2^n - 1$

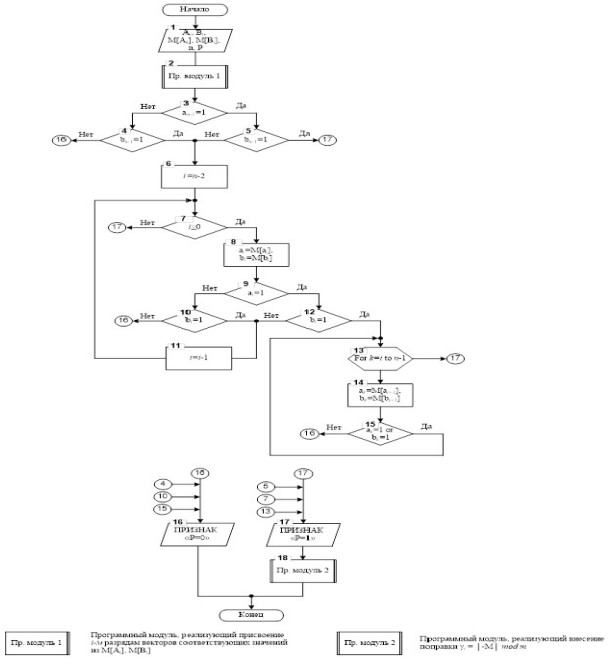


в) для модуля $M = 2^n + 1$

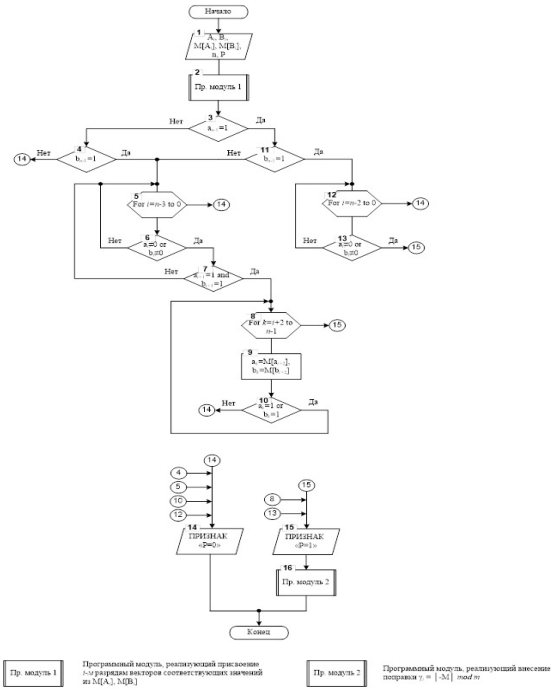
Рисунок 4 – Схема ФРП для криптографического примитива – «сумматор по модулю M $\left(M = 2^n, 2^n \pm 1\right)$» с разметкой временных интервалов выполнения операции



а) для модуля $M = 2^n$



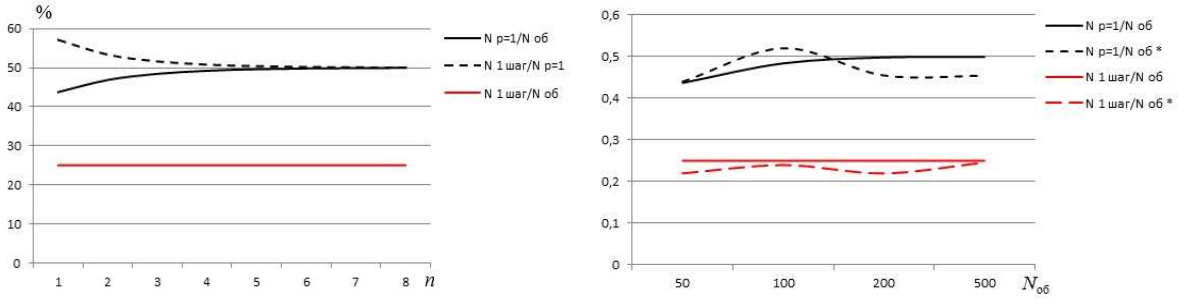
б) для модуля $M = 2^n - 1$



в) для модуля $M = 2^n + 1$

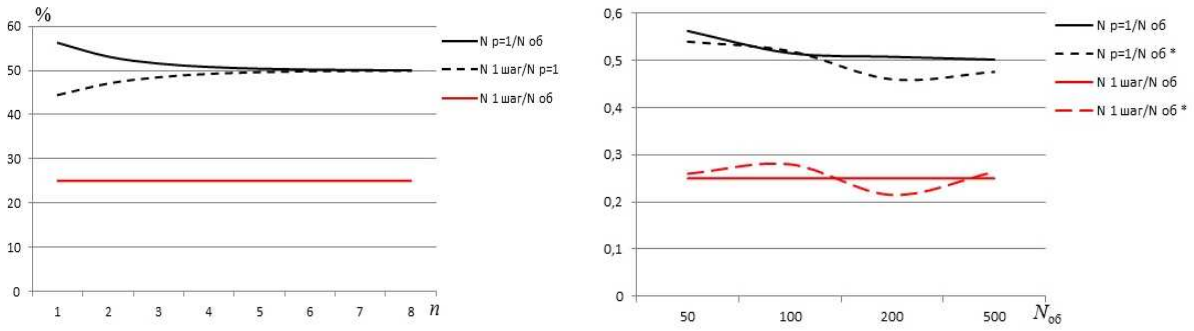
Рисунок 5 – Блок – схема алгоритма моделирования операции ФРП для криптографического примитива – «сумматор по модулю $M\left(M = 2^n, 2^n \pm 1\right)$»

классическим вариантом по результатам проведенного имитационного моделирования. Моделирование процесса формирования разряда признака переполнения проводилось на ЭВМ (CPU: Intel Core *i*7–3630QM, RAM: DDRIII 8GB) с помощью разработанной программы. Аналогично, на рисунках 7, 8 представлены оценки выигрыша в выполняемом количестве операций при реализации алгоритма ФРП для криптографического примитива – «сумматор по модулю $M\left(M=2^n-1, 2^n+1\right)$» по результатам проведенных теоретических расчетов и имитационного моделирования.



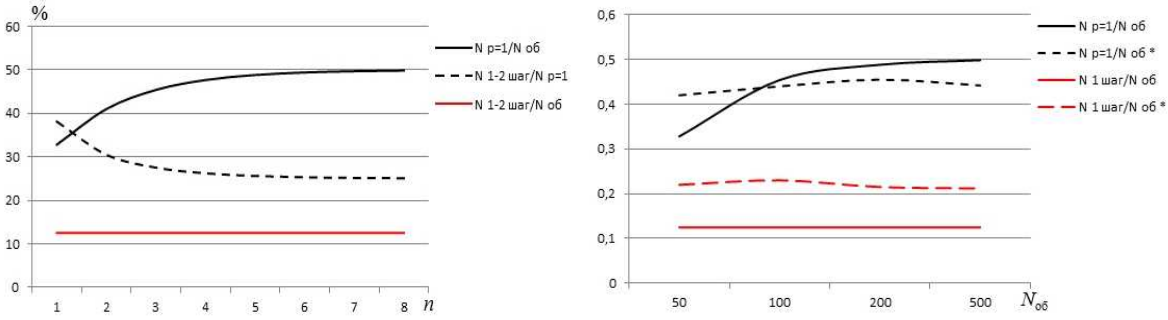
а) теория б) моделирование

Рисунок 6 – Оценка выигрыша в выполняемом количестве операций (для криптопримитива – «сумматор по модулю $M=2^n$»)



а) теория б) моделирование

Рисунок 7 – Оценка выигрыша в выполняемом количестве операций (для криптопримитива – «сумматор по модулю $M=2^n-1$»)



а) теория

б) моделирование

Рисунок 8 – Оценка выигрыша в выполняемом количестве операций (для криптопримитива – «сумматор по модулю $M = 2^n + 1$»)

Результаты моделирования, отражающие зависимость времени выполнения $T_{вып}$ для усовершенствованных алгоритмов ФРП и классического алгоритма от общего числа возможных комбинаций ($N_{об}$) представлены в таблице .1. В ходе моделирования использовались комбинации размерностью 32 бита. Моделирование проводилось с помощью разработанной программы. Оценка выигрыша по длительности выполнения операции ФРП алгоритма ФРП для модуля $M = 2^n - 1$ по отношению к классическому алгоритму представлена на рисунке 9.

Таблица. 1 – Результаты моделирования, отражающие зависимость времени выполнения $T_{вып}$ алгоритмов ФРП от $N_{об}$ для модулей $M = 2^n, 2^n \pm 1$

Тип модуля	**Значение $N_{об}$ (при $N_{повт}$=5)**						
	$5x10^3$	$1x10^4$	$15x10^3$	$2x10^4$	$35x10^3$	$5x10^4$	$1x10^5$
$T_{вып}$ ($M=2^n$), (с)	2,158	4,374	6,534	8,696	15,278	21,596	42,888
$T_{вып}$ ($M=2^n-1$), (с)	2,171	4,33	6,598	8,56	14,722	21,524	42,228
$T_{вып}$ ($M=2^n+1$), (с)	2,182	4,4	6,444	8,762	15,11	22,464	42,638
$T_{вып}$ (классический вариант), (с)	2,32	4,432	6,74	8,624	15,124	21,968	42,692

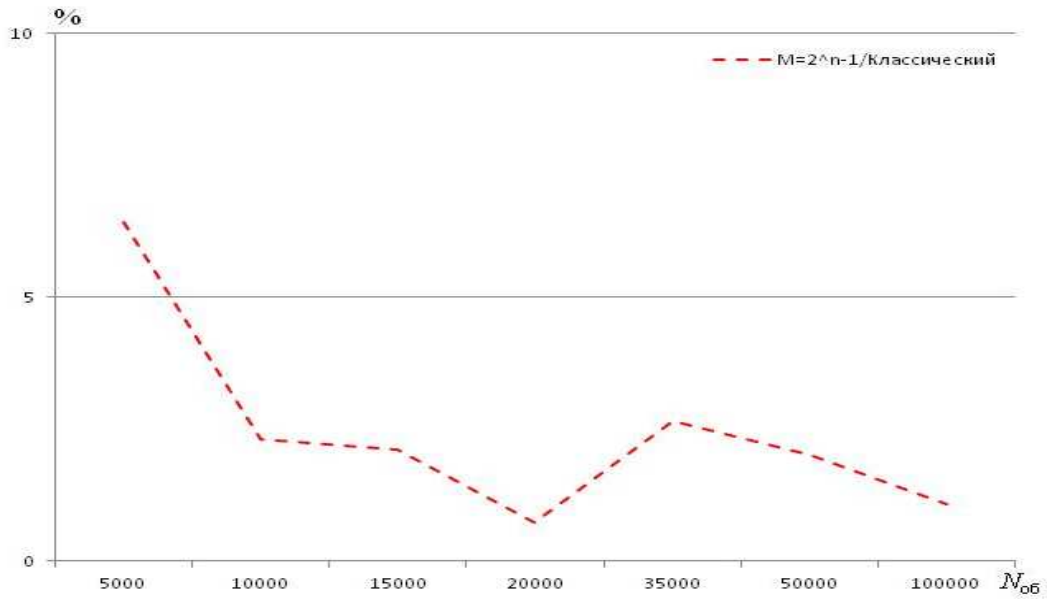


Рисунок 9 – Оценка выигрыша по длительности выполнения операции ФРП алгоритма ФРП по модулю $M = 2^n - 1$ по отношению к классическому алгоритму

Оценка разработанного схемотехнического решения для реализации локального контроля модулярных сумматоров ГПСП. Сравнительная оценка разработанной схемы локального модулярного контроля криптографического примитива – «сумматор по модулю M» с применяемыми на практике методами аппаратного резервирования (дублирование, троирование) проводилась по критерию суммарных затрат на реализацию аппаратного контроля, выраженных через сложность схемы. В качестве показателя для измерения сложности схем (элементов) использовалось число входов логических элементов – $L_{\text{вх.л.э.}}$. Оценка сложности схемной реализации модулярных сумматоров проводилась по методу Лупанова [7–9].

Сравнительная оценка предложенного схемотехнического решения локального аппаратного контроля модулярных сумматоров по сравнению с классическими методами повышения надежности представлена на рисунке 10.

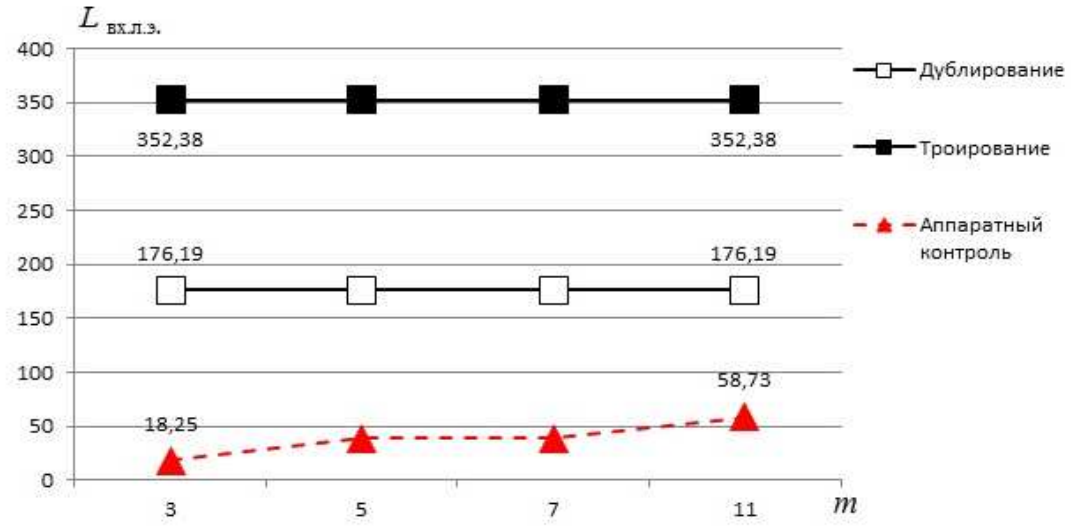


Рисунок 10 – Семейство графиков, отражающих зависимость объема аппаратных затрат на реализацию СК по отношению к исходной схеме в зависимости от величины используемого модуля контроля

Анализ графиков показал, что предложенное схемотехническое решение локального аппаратного контроля криптографического примитива – «сумматор по модулю M» имеет меньший объем суммарных аппаратных затрат на реализацию схемы контроля по сравнению с классическими методами. Суммарные затраты на реализацию схемы локального аппаратного контроля составляют (для значений модуля $m=3...11$) от 18% до 59% от затрат на реализацию исходной схемы криптографического примитива. Таким образом, коэффициент избыточного оборудования k_u составляет от 1,18 до 1,59. При этом, суммарные затраты на реализацию схемы контроля (для значений модуля $m=3...11$) снижены по сравнению с методами дублирования и троирования на 42,5–57% и 65–73,8% соответственно.

Разработка алгоритмов и схемотехнических решений сквозного контроля модулярных сумматоров и ключевого запоминающего устройства остаточным кодом. На практике для реализации сквозного контроля наибольшее распространение получили методы введения

пространственной избыточности, в частности, дублирование и мажоритарные схемы. Предлагаемое схемотехническое решение позволяет за счет применения метода модулярного контроля, использования особенностей криптографических примитивов и построения криптографических алгоритмов получить улучшения в контроле, а именно, реализовать сквозной контроль различных криптографических примитивов (блоков) на единых принципах (в алгебре конечного кольца) одним устройством контроля при снижении объема аппаратных затрат (по сравнению с методами аппаратного резервирования).

Прежде чем перейти к рассмотрению разработанных решений дадим определение понятиям модулярный (остаточный) и многомодульный (многоостаточный) код.

ОПРЕДЕЛЕНИЕ 1. Пусть информационные слова N образуют множество элементов кольца $Z_m \left(m > 1, m \in Z^+\right)$. Тогда арифметическим многомодульным (многоостаточным) кодом называется множество $C(m; m_1, \ldots, m_l)$ слов вида:

$$\overline{N}\{N; c_1(N), \ldots, c_l(N)\},$$

где $N \in Z_m$, $c_i(N) \in Z_{m_i}$, $c_i(N) \equiv N \left(\mathrm{mod}\, m_i\right)$, $i = 1, \ldots, l$; $m_1, \ldots, m_l \in Z^+$.

Число m является информационным модулем, числа $m_1, \ldots, m_l$ – проверочными модулями [10].

ОПРЕДЕЛЕНИЕ 2. Арифметический модулярный (остаточный) код – частный случай многомодульного (многоостаточного) кода, в котором используется один проверочный модуль [10].

Разработанное схемотехническое решение сквозного контроля фрагментов СГ ПСП, реализованного на основе типовых элементов криптографических алгоритмов, представлено на рисунке 11, блок-схема алгоритма сквозного контроля – на рисунке 12. В качестве типовых элементов в рассматриваемом схемотехническом решении выступают

модулярные сумматоры и запоминающее устройство для хранения криптографических ключей. Особенностью предлагаемого схемотехнического решения является:

- организация сквозного контроля различных криптографических примитивов (блоков) на единых принципах;
- возможность обеспечения требуемой сложности схемы контроля и снижения суммарного объема оборудования в зависимости от выбранной элементной базы;
- повышение надежности и достоверности функционирования при снижении объема аппаратных затрат по сравнению с методами введения аппаратной избыточности;
- возможность обнаружения симметричных ошибок.

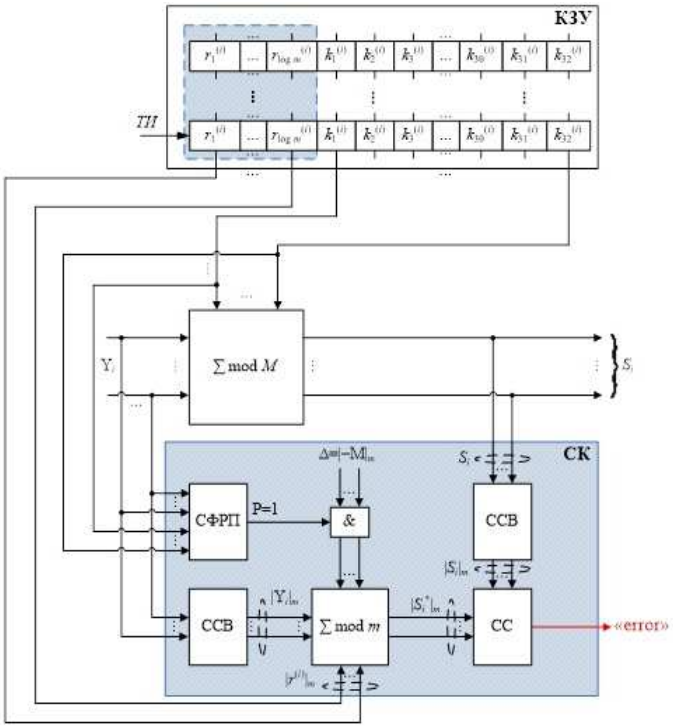


Рисунок 11 – Схема сквозного контроля модулярных сумматоров и КЗУ остаточным кодом

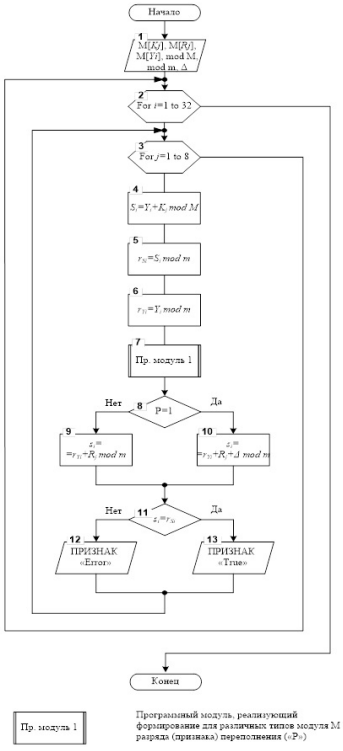


Рисунок 12 – Блок-схема алгоритма сквозного контроля фрагментов СГ ПСП остаточным кодом

Сравнительная оценка разработанной схемы сквозного контроля модулярных сумматоров и КЗУ с применяемыми на практике методами аппаратного резервирования (дублирование, троирование) проводилась по критерию суммарных затрат на реализацию аппаратного контроля, выраженных через сложность схемы. В качестве показателя для измерения сложности схем (элементов) использовалось число входов логических элементов – $L_{\text{вх.л.э.}}$. Оценка сложности схемной реализации модулярных сумматоров проводилась по методу Лупанова [7–9].

Сравнительная оценка предложенного схемотехнического решения по реализации сквозного контроля модулярных сумматоров и КЗУ остаточным кодом по сравнению с классическими методами повышения надежности представлена на рисунке 13.

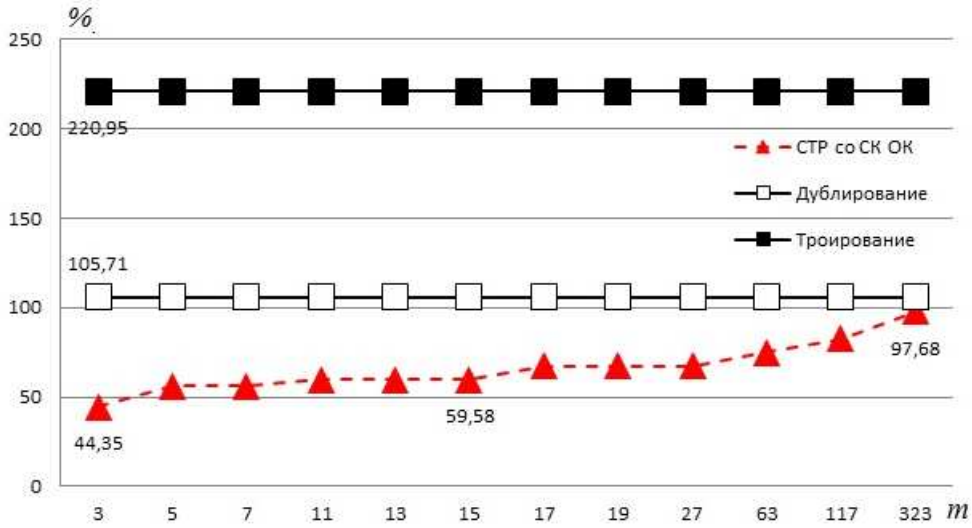


Рисунок 13 – Семейство графиков, отражающих зависимость увеличения объема аппаратных затрат на реализацию СК по отношению к исходной схеме в зависимости от величины модуля контроля

Анализ зависимостей показал, что предложенное схемотехническое решение реализации сквозного контроля различных криптографических примитивов остаточным кодом имеет более низкий объем аппаратных затрат на реализацию схемы контроля (по сравнению с методами

дублирования и троирования). При этом, суммарные затраты на реализацию схем сквозного контроля фрагментов криптографического алгоритма составляют (для значений модуля $m = 3 \ldots 27$) от 44% до 67% от затрат на реализацию исходной схемы соответствующих фрагментов криптографического алгоритма. Таким образом, коэффициент избыточного оборудования k_u составляет от 1,44 до 1,67.

Выводы.

В настоящем исследовании были представлены разработанные алгоритмы численного контроля операции арифметического сложения в Z_m и моделирования операции ФРП, схема локального контроля сумматора в Z_m, а также схема сквозного контроля модулярных сумматоров и ключевого запоминающего устройства остаточным кодом. На основании результатов проведенного моделирования и оценки сложности схемной реализации разработанных схемотехнических решений была подтверждена целесообразность применения метода контроля по модулю для повышения надежности ГПСП, реализующих криптографические функции.

Список литературы:

1. Хетагуров, Я.А. Повышение надежности цифровых устройств методами избыточного кодирования / Я.А.Хетагуров, Ю.П. Руднев. – М.: Энергия, 1974. – 272 с.

2. Щербаков, Н.С. Достоверность работы цифровых устройств / Н.С. Щербаков. – М.: Машиностроение, 1989. – 224 с.: ил.

3. Савельев, А.Я. Арифметические и логические основы цифровых автоматов: учебник для вузов по специальности Электронные вычислительные машины / А.Я. Савельев.– М: Высшая школа, 1980. – 255 с.

4. Надежность и эффективность в технике: справочник в 10 т. / Ред. совет: В.С. Авдуевский (пред.) и др. – М.: Машиностроение, 1987. – (В пер.). Т.9.: Техническая диагностика / Под общ. ред. В.В. Клюева, П.П. Пархоменко. – 352 с.: ил.

5. Огнев, И.В. Надежность запоминающих устройств / И.В. Огнев, К.Ф. Сарычев. – М.: Издательство «Радио и связь», 1988. – 224 с.

6. Гладков, Л.А. Дискретная математика: учебник / Л.А. Гладков, В.В. Курейчик, В.М. Курейчик, под ред. В.М. Курейчика. – Таганрог: Издательство ТТИ ЮФУ, 2011. – 312 с.

7. Введение в математическую логику: конспект лекций / О.Б. Лупанов, под ред. А.Б. Угольникова. – М.: Издательство ЦПИ при МГУ имени М.В.Ломоносова, 2007. – 192 с.

8. Лупанов, О.Б. Асимптотические оценки сложности управляющих систем / О.Б. Лупанов. – М.: Издательство МГУ, 198. – 137 с.

9. Гашков, С.Б. Схемная сложность некоторых задач анализа и алгебры / С.Б. Гашков // Современные проблемы математики и механики. – 2009. – №3. – С. 7.

10. Бояринов, И.М. Помехоустойчивое кодирование числовой информации / И.М. Бояринов. – М.: Наука, 1983. – 195 с.

References

1. Hetagurov, Ja.A. Povyshenie nadezhnosti cifrovyh ustrojstv metodami izbytochnogo kodirovanija / Ja.A.Hetagurov, Ju.P. Rudnev. – M.: Jenergija, 1974. – 272 s.

2. Shherbakov, N.S. Dostovernost' raboty cifrovyh ustrojstv / N.S. Shherbakov. – M.: Mashinostroenie, 1989. – 224 s.: il.

3. Savel'ev, A.Ja. Arifmeticheskie i logicheskie osnovy cifrovyh avtomatov: uchebnik dlja vuzov po special'nosti Jelektronnye vychislitel'nye mashiny / A.Ja. Savel'ev.– M: Vysshaja shkola, 1980. – 255 s.

4. Nadezhnost' i jeffektivnost' v tehnike: spravochnik v 10 t. / Red. sovet: V.S. Avduevskij (pred.) i dr. – M.: Mashinostroenie, 1987. – (V per.). T.9.: Tehnicheskaja diagnostika / Pod obshh. red. V.V. Kljueva, P.P. Parhomenko. – 352 s.: il.

5. Ognev, I.V. Nadezhnost' zapominajushhih ustrojstv / I.V. Ognev, K.F. Sarychev. – M.: Izdatel'stvo «Radio i svjaz'», 1988. – 224 s.

6. Gladkov, L.A. Diskretnaja matematika: uchebnik / L.A. Gladkov, V.V. Kurejchik, V.M. Kurejchik, pod red. V.M. Kurejchika. – Taganrog: Izdatel'stvo TTI JuFU, 2011. – 312 s.

7. Vvedenie v matematicheskuju logiku: konspekt lekcij / O.B. Lupanov, pod red. A.B. Ugol'nikova. – M.: Izdatel'stvo CPI pri MGU imeni M.V.Lomonosova, 2007. – 192 s.

8. Lupanov, O.B. Asimptoticheskie ocenki slozhnosti upravljajushhih sistem / O.B. Lupanov. – M.: Izdatel'stvo MGU, 198. – 137 s.

9. Gashkov, S.B. Shemnaja slozhnost' nekotoryh zadach analiza i algebry / S.B. Gashkov // Sovremennye problemy matematiki i mehaniki. – 2009. – №3. – S. 7.

10. Bojarinov, I.M. Pomehoustojchivoe kodirovanie chislovoj informacii / I.M. Bojarinov. – M.: Nauka, 1983. – 195 s.