На правах рукописи

Шалагин Сергей Викторович

МЕТОДЫ СИНТЕЗА УСТРОЙСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ НА ОСНОВЕ НЕЛИНЕЙНЫХ ПОЛИНОМИАЛЬНЫХ ФУНКЦИЙ НАД КОНЕЧНЫМ ПОЛЕМ

05.13.05 – Элементы и устройства вычислительной техники и систем управления

Автореферат

диссертации на соискание ученой степени доктора технических наук

Казань – 2013

Работа выполнена в ФГБОУ ВПО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ».

Научный консультант - доктор технических наук, профессор
Захаров Вячеслав Михайлович

Официальные оппоненты: **Исмагилов Ильяс Идрисович**
доктор технических наук, профессор,
ФГАОУ ВПО «Казанский (Приволжский) федеральный университет»,
заведующий кафедрой

Кирьянов Борис Федорович
доктор технических наук, профессор,
ФГБОУ ВПО «Новгородский государственный университет имени Ярослава мудрого»,
профессор

Крашенинников Виктор Ростиславович
доктор технических наук, профессор
ФГБОУ ВПО «Ульяновский государственный технический университет»,
заведующий кафедрой

Ведущая организация - **ФГБОУ ВПО «МАТИ - Российский государственный технологический университет им. К.Э.Циолковского», г. Москва**

Защита состоится « ___ » _____ 20__ г. в ____ часов на заседании диссертационного совета Д 212.277.01 при Ульяновском государственном техническом университете (УлГТУ) по адресу: 432027, г. Ульяновск, ул. Северный Венец, 32 (ауд. 211, Главный корпус).

Автореферат разослан « ___ » _____ 20__ г.

Ученый секретарь
диссертационного совета,
доктор технических наук,
профессор Смирнов Виталий Иванович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. В настоящее время особую актуальность приобрела проблема, связанная с генерированием и обработкой массивов данных, представленных в цифровой форме и имеющих большую размерность, за ограниченный период времени. Один из подходов к ее разрешению – организация распределенных вычислений, под которыми будем понимать способы решения вычислительных задач с использованием двух и более вычислительных устройств с применением как распараллеливания вычислительного процесса, так и потоковой обработки данных с сохранением промежуточных результатов. Потоковой названа обработка массивов данных при использовании однотипных операций. Для решения указанного класса задач эффективны распределенные вычислительные системы с программируемой архитектурой (РВС ПА), элементами которых являются сконфигурированные программируемые логические интегральные схемы (ПЛИС) класса FPGA.

Известны результаты по представлению генераторов массивов равномерно распределенных случайных и псевдослучайных чисел большой размерности на основе полиномиальных функций над конечным полем (Алферов А.П., Винокуров В.И., Ганнтмахер В.Е., Гилл А., Кирьянов Б.Ф. Иванов М.А., Кузнецов В.М., Песошин В.А., Шнайер Б. и др.). Существует подход к представлению генераторов дискретных стохастических процессов (ДСП) из классов однородных и неоднородных цепей Маркова (ЦМ) и их функций, на основе вероятностных автоматов (ВА), в общем случае – нелинейных систем. Такие генераторы находят применение в таких областях как построение вероятностных моделей алгоритмов для решения задач защиты информации, статистическое моделирование, распознавание образов, кодирование и декодирование информации, техническая диагностика цифровых устройств, обработки сигналов в системах связи и управления. Поэтому исследование вопросов синтеза генераторов ДСП данного класса имеет важное теоретическое и прикладное значение. Указанный подход, определенный как автоматный, отражен в многочисленных публикациях (Аблаев Ф.М., Альпин Ю.А., Баканович Э.А., Бусленко Н.П., Бухараев Р.Г., Гилл А., Гиоргадзэ А.Х., Гладкий В.С., Глова В.И., Захаров В.М., Кемени Дж., Левин Б.Р., Кирьянов Б.Ф., Лоренц А.А., Нурмеев Н.Н., Нурутдинов Ш.Р., Песошин В.А., Полляк Ю.Г., Поспелов Д.А., Салимов Ф.И., Столов Е.Л., Хамитов Г.П., Ченцов В.М., Чирков М.К., Шварц В., Яковлев В.В., Paz A. и др.). Вместе с тем, реализация автоматных функций на ПЛИС/FPGA без адаптации под архитектуру ПЛИС/FPGA сопряжена с большими дополнительными затратами аппаратных ресурсов из-за неполного задействования однотипных конфигурируемых элементов ПЛИС/FPGA, реализующих любую булеву функцию (БФ) от $R \le 5$, переменных. Решение задачи адаптации более эффективно для системы БФ, пересечение по аргументам между которыми будет минимальным. Известные подходы, основанные на использовании аппарата алгебры логики, не ориентированы на базис ПЛИС/FPGA, где $R \le 5$, а декомпозиция Шеннона является нерациональной по оценкам временной и аппаратной сложности, т.к. схема имеет древовидную структуру (Баркалов А.А. и др.).

Представление генераторов ДСП класса марковских и их функций на основе однотипных операций над конечным полем позволяет производить распределенные, непересекающиеся по аргументам вычисления, что повышает эффективность реализации потоковых преобразований над *n*-разрядными двоичными векторами. Задача определения генераторов простых однородных ЦМ в базисе нелинейных полиномиальных функций (НПФ) над полем Галуа вида $GF(2^n)$, впервые решена в 1999-2001 гг. (Захаров В.М., Нурутдинов Ш.Р., Шалагин С.В.). Затем данный подход был распространен (2002-2005) на генераторы однородных α-сложных ЦМ и их детерминированных и стохастических функций, а также на генераторы неоднородных ЦМ (Захаров В.М., Нурутдинов Ш.Р., Соколов С.Ю., Шалагин С.В., Эминов Б.Ф.). В диссертации докт. физ.-мат. наук Нурутдинова Ш.Р. (2005) дано развитие конечно-автоматных преобразований на базе нелинейных полиномиальных функций от двух переменных в рамках исследования проблемы моделирования автоматов различ-

ных видов (комбинационных схем, детерминированных и вероятностных автоматов, цепей Маркова) полиномами над полем Галуа вида $GF(2^n)$. Решена задача уменьшения количества ненулевых коэффициентов НПФ путем доопределения неопределенных значений функции на заданных наборах (Нурутдинов Ш.Р., Николаев А.Г., 2005).

Развитие теоретических основ представления ВА на основе операций в конечных полях над потоками дискретных случайных величин открывает возможность для разработки эффективных методов синтеза на ПЛИС/FPGA генераторов ДСП класса марковских и их функций на основе распределенного, непересекающегося по аргументам и адаптированного под архитектуру ПЛИС/FPGA вычисления значений НПФ, определенных над конечным полем.

Известен аппарат теоретико-полиномиальных преобразований (ТПП) – дискретных преобразований, определенных на основе теории полиномиальных вычетов, ориентированный на задачи анализа и синтеза динамических систем, описываемых вещественными числами (Крот А.М., Минервина Е.Б. и др.). Частные случаи ТПП - широко применяемые на практике дискретные преобразования Фурье (ДПФ) и Хартли (ДПХ), а также алгоритмы цифровой фильтрации сигналов. В частности, получил развитие подход к синтезу устройств вычислительной техники (ВТ) для определенных алгоритмов цифровой обработки сигналов (ЦОС) – ДПФ и цифровых фильтров, на основе системы остаточных классов, обеспечивающий повышение скорости выполнения отдельных операций на уровне реализации на ПЛИС класса FPGA (Акушский И.Я., Галанина Н.А., Лебедев Е.К., Юдицкий Д.М. и др.). Дискретные функции Уолша как подкласс ТПП применимы в автоматизированных системах управления, в частности, для сжатия цифровых изображений (Исмагилов И.И. и др.) Однако, вопросы адаптации широкого класса устройств ЦОС, описываемых на основе нелинейных полиномиальных преобразований над конечным полем, под распределенную архитектуру ПЛИС/FPGA, исследованы не достаточно.

Данные обстоятельства определяют предпосылки к созданию общего метода синтеза при использовании однотипных специализированных цифровых вычислительных устройств, ориентированных на архитектуру ПЛИС/FPGA и описываемых НПФ над конечным полем, для: 1) генераторов дискретных стохастических процессов класса марковских и их функций; 2) устройств ВТ, выполняющих ЦОС. Для решения задачи синтеза (или создания прототипов) таких классов устройств ВТ как «система на кристалле», встраиваемые и портативные системы, широкое распространение получили IP-ядра (англ. Intellectual Property) – готовые блоки, применяемые для проектирования микросхем и представленные на уровне абстрактного описания, на функциональном и на физическом уровнях. При ограничениях на быстродействие и размер занимаемой площади микросхемы, IP-ядра позволяют существенно ускорить процесс синтеза устройств ВТ на микросхемах, в том числе, на ПЛИС/FPGA. При решении задач синтеза устройств ЦОС, использование подходов на базе IP-ядер позволяет синтезировать на ПЛИС цифровые сигнальные процессоры (англ. DSP, digital signal processor) как на алгоритмическом и программном уровнях, при использовании языка VHDL, так и на физическом уровне, на базе спец. DSP, встроенных в кристалл ПЛИС - XtremeDSP, PicoBlaze, MicroBlaze и т.п. (Зотов В.Ю., Шагурин И.И., B.Afra, S.Y.Kulkarni, P.Moakes, D.Pellerin, E.Young и др.). Вместе с тем, вопросы синтеза цифровых устройств, выполняющих нелинейные полиномиальные преобразования, в конечных полях на ПЛИС/FPGA при использовании IP-ядер, изучены не достаточно.

Для решения вычислительно трудоемких задач генерирования и обработки массивов данных большой размерности применимы РВС ПА. В настоящее время созданы РВС ПА различного назначения, выполненные при использовании унифицированных базовых модулей - многопроцессорных реконфигурируемых вычислителей на основе ПЛИС/FPGA (Каляев И.А., Левин И.И., Макаревич О.Б., Семерников Е.А., Шмойлов В.И. и др.). РВС ПА позволяют реализовать различные устройства ВТ, реконфигурируемые в реальном времени, что находит применение для таких областей, как символьная обработка информации,

защита компьютерных сетей, управление в реальном масштабе времени объектами энергетики, летательными и космическими аппаратами и т. п. В данной связи перспективной является задача синтеза устройств как для генерирования дискретных стохастических процессов класса марковских и их функций, так и для ЦОС, на РВС ПА при использовании однотипных IP-ядер, описываемых на основе нелинейных полиномиальных преобразований над конечным полем. В соответствии с требованиями, предьявляемыми к синтезируемым на РВС ПА устройствам по быстродействию и количеству задействованных процессорных элементов, актуальна задача адаптации указанных IP-ядер под архитектуру ПЛИС/FPGA.

Известно представление дискретных детерминированных нелинейных функций (ДДНФ) вида $\psi(x_1,...,x_m)=y$, где $x_1,...,x_m,y$ - n-разрядные двоичные числа, на основе НПФ над $GF(2^n)$ на абстрактном уровне (Лидл Р., Нидеррайтер Г. 1988). В ряде работ (Захаров В.М., Нурутдинов Ш.Р., Соколов С.Ю., Шалагин С.В. и др.) исследовано применение частных случаев НПФ, $m=1,2$, для решения задач синтеза генераторов дискретных стохастических процессов (ДСП) класса марковских и их функций. Теоретически обоснован алгоритм синтеза произвольной булевой функции (БФ) на основе НПФ над $GF(2)$ - полиномов Жегалкина И.И. (Чебурахин И.Ф.). В настоящее время существуют микросхемы ПЛИС/FPGA, количество реконфигурируемых элементов внутри которых позволяет реализовать цифровые устройства для вычисления произвольной БФ от 20-ти переменных как IP-ядро. Вместе с тем, вопросы синтеза устройств для вычисления значения $\psi(x_1,...,x_m)$, где m - произвольное, на основе системы НПФ над полем Галуа изучены не достаточно. Данное обстоятельство актуализирует исследование задач синтеза устройств ВТ для ДДНФ на основе однотипных IP-ядер, вычисляющих заданную НПФ и ориентированных на архитектуру ПЛИС/FPGA.

Для решения задачи синтеза устройств ВТ на ПЛИС/FPGA применимы однотипные функциональные модули (ФМ), описываемые нелинейными полиномиальныеми преобразованиями над конечным полем. Известно, что отдельные операции, в частности, операции умножения элементов поля вида $GF(2^n)$ и $GF((2^k)^r)$, $n=k\cdot r$, (обозначим их ОУ/$GF(2^n)$ и ОУ/$GF((2^k)^r)$, соответственно) допускают организацию распараллеливания вычислений и потоковой обработки данных (Алексеев В.Б., Лидр Р., Ниддеррайтер Г., Нурутдинов Ш.Р., Сюрин В.Н. и др.). Решены частные задачи синтеза ФМ, выполняющих ОУ/$GF(2^n)$ и ОУ/$GF((2^k)^4)$ на ПЛИС/FPGA (Захаров В.М., Нурутдинов Ш.Р., Столов Е.Л., Шалагин С.В., Fleischemann P., Orlando G., Paar C., P.Soria-Rodrigues и др.). Однако, в общем случае, вопросы, связанные с синтезом спец. ФМ, выполняющих ОУ/$GF(2^n)$ и ОУ/$GF((2^k)^r)$, $n=k\cdot r$, на основе распределенных вычислений, исследованы не достаточно. При аппаратной реализации вычислений в конечных полях, важной задачей является синтез функциональных модулей операции вычисления остатка по заданному модулю, отличного от степени числа два, над конечным полем (далее - ОВО). Однако, вопросы, связанные с синтезом функциональных модулей ОВО на основе конвейерных вычислений в конечном поле, изучены не достаточно. В данной связи, актуальна задача исследования методов синтеза модулей, определяемых как IP-ядра, ориентированных на архитектуру ПЛИС/FPGA, и реализующих как ОУ/$GF(2^n)$, ОУ/$GF((2^k)^r)$, $n=k\cdot r$, так и ОВО.

В результате, актуально создание и исследование общего метода синтеза устройств ВТ, ориентированных на архитектуру ПЛИС/FPGA, в трех направлениях: 1) разработка новых эффективных методов синтеза широкого класса устройств ВТ на основе нелинейных полиномиальных преобразований над конечным полем; 2) расширение класса процессов, представляемых нелинейными полиномиальными преобразованиями; 3) повышение эффективности методов синтеза устройств ВТ для генерирования дискретных стохастических

процессов и цифровой обработки сигналов на ПЛИС/FPGA при использовании однотипных устройств и модулей, представляемых как IP-ядра.

Объектом исследования являются методы синтеза устройств ВТ, предназначенных для генерирования дискретных стохастических процессов класса марковских и их функций и для выполнения теоретико-полиномиальных преобразований над потоками чисел в конечном поле.

Предмет исследования - методы синтеза генераторов дискретных стохастических процессов класса марковских и их функций и устройств ВТ для выполнения теоретико-полиномиальных преобразований на ПЛИС/FPGA и распределенных вычислительных системах с программируемой архитектурой, повышающие эффективность генерирования и обработки массивов цифровых данных на основе нелинейных полиномиальных функций, определенных над конечным полем.

Цель диссертационной работы - разработка общего метода для структурного, алгоритмического и функционального синтеза генераторов дискретных стохастических процессов класса марковских и их функций и устройств ВТ для выполнения теоретико-полиномиальных преобразований, повышающего эффективность реализации данных генераторов и устройств на ПЛИС/FPGA за счет применения нелинейных полиномиальных параллельных преобразований над потоками чисел в конечных полях.

Научная проблема сформулирована как разработка методов синтеза на абстрактном, структурном и функциональном уровнях устройств ВТ для обработки потоков чисел, описываемых нелинейными полиномиальными функциями над конечным полем и реализуемых в однородных вычислительных структурах по технологии ПЛИС/FPGA.

Для достижения поставленной цели диссертационной работы и разрешения научной проблемы сформулированы следующие основные задачи:

- разработка теоретических основ для общего метода структурного и функционального синтеза генераторов дискретных стохастических процессов класса марковских и их функций в базисе НПФ над конечным полем;
- разработка теоретических основ для метода синтеза цифровых вычислительных устройств, структурно ориентированных на архитектуру ПЛИС/FPGA и реализующих дискретную детерминированную нелинейную функцию общего вида на основе нелинейной полиномиальной функции или системы НПФ от многих переменных, определенных над полем Галуа;
- разработка методов алгоритмического синтеза функциональных модулей, реализующих операции умножения над элементами полей вида $GF(2^n)$ и $GF((2^k)^r)$, $n = k \cdot r$, и операцию вычисления остатка от деления по заданному модулю в конечном поле, на основе параллельных и конвейерных вычислений, выполняемых на архитектуре ПЛИС/FPGA;
- получение оценок временной и аппаратной сложности для цифровых вычислительных устройств и для функциональных модулей в базисе ПЛИС/FPGA путем проведения компьютерного моделирования разработанных устройств и модулей при использовании спец. САПР ISE 13.4 – Foundation (Xilinx Corp.) и Quartus II v. 9.0 (Altera Corp.);
- разработка методики алгоритмического и функционального синтеза генераторов дискретных стохастических процессов класса марковских и их функций, а также устройств вычислительной техники, реализующих теоретико-полиномиальные преобразования, на распределенной вычислительной системе с программируемой архитектурой при использовании однотипных IP-ядер, реализующих цифровые вычислительные устройства и функциональные модули;
- исследование повышения производительности как генераторов дискретных стохастических процессов класса марковских и их функций, так и устройств ВТ для выполнения теоретико-полиномиальных преобразований на примерах различных задач, разработка

рекомендаций по технической реализации указанных устройств на распределенных вычислительных системах с программируемой архитектурой.

Методы исследования. Для решения поставленных задач использованы методы теории вероятностей, теории вероятностных автоматов, теории графов, теории чисел, квантовой обработки информации, статистической обработки данных, схемотехники, аппарат теории конечных полей, полиномиальной алгебры и дискретной математики.

Научная новизна полученных результатов. Работа является завершенным исследованием проблемы по разработке методов синтеза на уровне абстрактного описания, на структурном и на функциональном (в архитектуре ПЛИС/FPGA) уровнях генераторов дискретных стохастических процессов класса марковских и их функций, на основе предложенного принципа суперпозиции НПФ над полем Галуа, и устройств вычислительной техники для выполнения теоретико-полиномиальных преобразований.

1. Доказаны теоремы, обосновывающие предложенный в работе общий метод синтеза генераторов ДСП класса марковских и их функций: однородных цепей Маркова, их детерминированных и стохастических функций и α-сложных ЦМ, на основе введенного понятия «полиномиальная модель цепи Маркова» и реализации нелинейных полиномиальных преобразований над полями Галуа на основе предложенного принципа суперпозиции НПФ, а также систем НПФ от многих переменных. Определены структурные схемы генераторов неоднородных ЦМ и их функций, детерминированных и стохастических, на основе систем НПФ от многих переменных, определенных над полем Галуа, а также генераторов дискретных случайных величин (ДСВ) с заданным законом распределения на основе НПФ от m переменных над полем Галуа, и m генераторов равномерно распределенных ДСВ, что позволяет синтезировать указанные генераторы на распределенной вычислительной системе с программируемой архитектурой, элементами которой являются ПЛИС/FPGA.

2. Доказаны теоремы, обосновывающие предложенный метод структурного синтеза цифровых устройств для вычисления значения дискретной детерминированной нелинейной функции общего вида от m n-разрядных переменных над полями Галуа на основе представления указанной ДДНФ при использовании системы из l НПФ от $m \cdot l$ переменных над элементами полей Галуа вида $GF(2^k)$, $n = l \cdot k$. Определены структурные схемы вычисления значения указанной ДДНФ - параллельная, систолическая, последовательностная и параллельно-последовательностная, представленные на структурном уровне при использовании НПФ над $GF(2^n)$ и альтернативные по оценкам сложности.

3. Расширена область применения предложенного общего метода синтеза на устройства вычислительной техники, реализуемые на основе однотипных IP-ядер, выполняющих вычисление НПФ или операции над элементами конечных полей; разработаны методики, позволяющие решать задачи алгоритмического и функционального синтеза для устройств ВТ, предназначенных для:

- выполнения ТПП над потоками чисел (на примере ДПФ, ДПХ и цифровых фильтров с импульсной характеристикой конечной длительности (КИХ-фильтров)) при использовании системы НПФ от многих переменных согласно предложенному методу алгоритмического синтеза, причем каждая НПФ определена над полем Галуа и значения каждой НПФ системы вычисляются параллельно;
- расчета дискретной модели отображения и варьирования состояния квантово-механической системы, включающей N базисных состояний - КМС(N), а также ее частных случаев: для N=2 и N=4 на основе параллельного выполнения операций умножения элементов $GF(2^n)$ или $GF((2^k)^r)$, $n = r \cdot k$,

что позволяет синтезировать указанные устройства на распределенной вычислительной системе с программируемой архитектурой, элементами которой являются ПЛИС/FPGA.

4. Разработаны методы алгоритмического синтеза функциональных модулей, позволяющие разрешить проблему реализации ФМ для выполнения операций над элементами

конечного поля за счет применения принципов распределенных вычислений. При этом операция умножения - ОУ/$GF(2^n)$, производится на основе операций над $GF(2)$, ОУ/$GF((2^k)^r)$ - на основе операций над полем вида $GF(2^k)$, $n = r \cdot k$, а операция вычисления остатка по заданному простому модулю - на основе однотипных операций над целыми числами, выполняемых параллельно внутри каждой из ступеней конвейера. Доказаны утверждения, обосновывающие оценки сложности разработанных алгоритмов.

5. Предложена методика оценки степени соответствия ФМ, описываемых как IP-ядра и выполняющих операции над конечным полем, архитектуре ПЛИС/FPGA, которая позволяет выбрать одну из функциональных схем, описывающую данный модуль и наиболее приближенную к оптимальной по предложенным критериям.

Результаты поддержаны

- ✓ грантами РФФИ - № 99-01-00163 «Энтропийно-сложностные свойства дискретных вычислительных моделей», 03-01-00769 «Сложностные свойства классических и квантовых вычислений», 09-01-97004-Р-Поволжье 01 «Вычислительные возможности классических и квантовых моделей вычислений с ограничениями»,
- ✓ по проекту № 015-04-01-52 «Синтез и сложность детерминированных и вероятностных дискретных вычислительных моделей» программы «Университеты России»,

Практическая значимость работы в том, что предложенные теоретические основы и общий метод являются базовыми для решения задач

- анализа и синтеза генераторов ДСП класса марковских и их функций в базисе НПФ над полем $GF(2^n)$,
- синтеза устройств для вычисления теоретико-полиномиальных преобразований (на примере ДПФ, ДПХ и КИХ-фильтров).

Указанные генераторы и устройства, реализуемые на РВС ПА при использовании однотипных IP-ядер, позволяют с высокой скоростью производить и обрабатывать массивы цифровых данных большой размерности. Общий метод синтеза на ПЛИС/FPGA устройств, реализующих генераторы ДСП указанного класса и заданные алгоритмы ЦОС на основе однотипных IP-ядер, позволяет варьировать характеристики генерируемых и/или обрабатываемых последовательностей чисел за время, сопоставимое со временем вычисления значений этих чисел, путем изменения коэффициентов указанных НПФ, а также позволяет увеличивать их быстродействие за счет того, что указанные устройства адаптированы под архитектуру ПЛИС/FPGA.

Предложенные теоретические основы и общий метод синтеза обеспечивают: повышение скорости выполнения операции вычисления остатка по заданному модулю для потока чисел (получен патент [19]); повышение эффективности процесса разработки схемотехнических решений, позволяющих осуществлять распараллеливание процесса вычисления широкого класса дискретных преобразований цифровой информации, поддерживаемых специализированной прикладной программой (Свид. о гос. регистрации программы для ЭВМ № 2011610812 РФ. Вычисление коэффициентов многочлена над полем Галуа вида *GF*(2)/ Шалагин С.В.; опубл. 20.06.2011), а также решение задач:

1) синтеза генераторов дискретных стохастических процессов класса марковских и их функций на основе однотипных IP-ядер, реализуемых на ПЛИС/FPGA;
2) анализа семейства генераторов ЦМ на ПЛИС/FPGA путем отбора типичных представителей и идентификации заданных подклассов объектов данного семейства;
3) синтеза устройств анализа и фильтрации цифровых сигналов на РВС ПА.

Достоверность научных результатов определяется корректностью применяемых математических моделей и их адекватностью реальным физическим процессам, доказательством теорем и утверждений, обосновывающих предлагаемые методы, совпадением теоретических результатов с данными экспериментов, полученными на основе математического

моделирования, при использовании специализированных САПР ПЛИС класса FPGA и результатами исследований других авторов.

Результаты использованы в НИР за 2001 – 2011гг. по трем грантам РФФИ – № 99-01-00163, № 03-01-00769 и № 09-01-97004-Р-Поволжье 01, по проекту № 015-04-01-52 программы «Университеты России», в ОАО «Научно-производственное объединение «Радиоэлектроника» имени В.И. Шимко», г. Казань (далее – НПО «Радиоэлектроника»), в ОАО «Научно-производственное предприятие «Межотраслевой центр эргономических исследований и разработок», г. Тверь (далее – НПП МЦЭИР), в ООО «НПП «Измерительные технологии», г. Саров (далее – НПП «Измерительные технологии») и в учебном процессе Военной академии воздушно-космической обороны им. Маршала Советского Союза Г.К.Жукова, г. Тверь (далее – ВА ВКО) и Института технической кибернетики и информатики ФГБОУ ВПО «Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ» (далее – КНИТУ-КАИ). По тематике, представленной в диссертации, опубликовано четыре учебно-методических пособия, два из которых – с грифом УМО.

Основные положения, выносимые на защиту.

1. Теоретические основы общего метода синтеза генераторов дискретных стохастических процессов класса марковских и их функций, и устройств вычислительной техники, выполняющих теоретико-полиномиальные преобразования, (на примере дискретных преобразований Фурье, Хартли и КИХ-фильтров) при использовании однотипных IP-ядер, позволяющих выполнять распределенные вычисления над конечным полем.

2. Теоретические основы метода синтеза на структурном уровне функциональных схем цифровых устройств, реализующих вычисление дискретной детерминированной нелинейной функции общего вида при использовании системы нелинейных полиномиальных функций от многих переменных, определенных над полем Галуа.

3. Метод синтеза на алгоритмическом уровне функциональных модулей в базисе ПЛИС/FPGA, позволяющих выполнить в конечных полях при использовании распределенных вычислений операции: умножения элементов поля Галуа, его расширений и вычисления остатка по заданному модулю, отличного от степени числа два.

4. Методики, позволяющие при использовании методов многопараметрического анализа определять подмножество типичных представителей семейства генераторов ДСП класса однородных цепей Маркова, синтезируемых на РВС ПА, и идентифицировать (с определенной доверительной вероятностью) принадлежность генератора ДСП класса однородных ЦМ к одному из априори заданных подклассов путем анализа производимой им последовательности состояний конечной длины.

5. Методика оценки степени соответствия ЦВУ и ФМ архитектуре ПЛИС/FPGA на основе разработанных критериев.

Апробация работы. Основные результаты работы были доложены и обсуждались на конференциях и семинарах *международного уровня*: «Дискретная математика и её приложения» (Москва, 2001, 2007), «Проблемы теоретической кибернетики» (Москва, 2002, Пенза, 2005), «Новые информационные технологии и системы» (Пенза, 2002), «Дискретные модели в теории управляющих систем» (Дубна, 2003), «Новая геометрия природы» (Казань, 2003), «Инфокоммуникационные технологии глобального информационного общества» (Казань, 2003, 2006–2009), «Инновационное образование в техническом университете» (Казань, 2004), «Высокопроизводительные параллельные вычисления на кластерных системах» (Казань, 2008), «Проблемы техники и технологий телекоммуникации» (Казань, 2008, 2011), «Дискретные модели в теории управляющих систем» (Москва, 2009), *всероссийского уровня*: «Теория сеточных методов для нелинейных краевых задач» (Казань, 2000, 2002 и 2004), «Методы и средства обработки информации» (Москва, 2003, 2005, 2009), «Наука и профессиональная деятельность» (Казань, 2008), «Инновации РАН 2010» (Казань, 2010), «Информационные технологии в системе экономической безопасности России и ее

регионов» (Казань, 2010), «Проблемы и перспективы развития информационных технологий» (Казань, 2012), *регионального уровня*: «Методы моделирования» при Академии наук РТ (Казань, 2001-2009), *а также* Итоговой науч. конф. КФУ (КГУ) (Казань, 2001); ряде семинаров каф. Теоретической кибернетики КФУ (Казань, 2001-2007), каф. Компьютерных систем КНИТУ-КАИ (Казань, 2001 - 2013), Института информатики Академии наук РТ (Казань, 2008-2010) и др.

Публикации. Основные результаты опубликованы в 59 работах, 46 из которых представлены в автореферате: 18 статей в ведущих рецензируемых научных изданиях, патенты: два – на изобретение, один – на полезную модель, монография и 18 работ – в сборниках трудов и материалах конференций международного и всероссийского уровней.

Личный вклад автора. Выносимые на защиту результаты получены автором лично. Вклад автора в ряд совместных работ: в [2, 4, 23, 24, 28, 29, 45] – методы синтеза устройств на структурном уровне, в [1, 28, 34, 35] - методы синтеза устройств на функциональном уровне, в [3, 22, 30] - получение и анализ результатов экспериментальных данных на уровне методов, в [17] – идея создания методики анализа множества объектов на основе характеризующих их признаков, в [25, 31] – метод синтеза представленных устройств, в [10, 12, 13, 40] - основная идея, в [39] – синтез предложенных устройств на структурном уровне, в [14, 15, 18, 19] - определение предложенных устройств на функциональном уровне, а в [18, 44] – разработка метода синтеза различных устройств ВТ на РВС ПА при использовании однотипных цифровых вычислительных устройств, выполняющих вычисления в конечных полях.

Структура и объем работы: введение, шесть глав, заключение и список используемых источников, включающий 366 наименований. Объем работы - 295 стр., в т.ч., 267 стр. основного текста. Работа включает 64 рисунка и 21-ну таблицу.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационной работы и определяется ее проблематика. Дан краткий обзор исследований и актуальных проблем по теме работы. Сформулирована цель и основные задачи работы, представлены основные положения, выносимые на защиту.

Первая глава содержит обзор методов синтеза устройств ВТ, основанных на применении полиномиальных преобразований, а также основные понятия и определения, обеспечивающие разработку теоретических основ и общего метода синтеза устройств ВТ, выполняющих нелинейные полиномиальные преобразования над потоками чисел в конечных полях, путем организации распределенных вычислений при использовании однотипных цифровых устройств, адаптированных под архитектуру ПЛИС/FPGA. Пусть $G_{(v)} = GF(2^v)$ - поле Галуа. Введём в рассмотрение отображение элементов данного поля вида:

$$\varphi : \underbrace{G_{(v)} \times ... \times G_{(v)}}_{m} \to G_{(v)} . \qquad (1)$$

Любое отображение конечного поля в себя вида (1) можно задать полиномиальной функцией *f* над этим полем (Лидл Р., Нидеррайтер Г., 1988):

$$f(q_1, ..., q_m) = \sum_{i_1=0}^{w} ... \sum_{i_m=0}^{w} a_{i_1 ... i_m} q_1^{i_1} ... q_m^{i_m} ,\ w = 2^v - 1,\ a_{i_1 ... i_m}, q_1, ..., q_m \in G_{(v)} , \qquad (2)$$

получение матрицы коэффициентов НПФ (2) $A = \left(a_{i_1 ... i_m}\right)_{2^v \times .. \times 2^v}$ производится путем последовательного решения системы уравнений:

$$\begin{aligned} &V^{(1)}(*, i_2, ..., i_m) = C^{-1} V(*, i_2, ..., i_m), \quad V^{(2)}(i_1, *, ..., i_m) = C^{-1} V^{(1)}(i_1, *, ..., i_m), ..., \\ &V^{(m)}(i_1, ..., i_{m-1}, *) = C^{-1} V^{(m-1)}(i_1, ..., i_{m-1}, *), \quad A = V^{(m)}, \quad i_1 = \overline{0, w}, ..., i_m = \overline{0, w}, \end{aligned} \qquad (3)$$

где C^{-1} - матрица, определенная над полем $G_{(v)}$, размерности $2^v \times 2^v$. Существенно уменьшить количество операций, требуемых для вычисления НПФ вида (2), позволяет наличие нулевых коэффициентов, получаемых путем решения системы (3) при наличии неопреде-

ленных значений в отображении вида (1) (Нурутдинов Ш.Р., Николаев А.Г., 2005). Для решения задачи синтеза генераторов конечных простых однородных ЦМ [2, 23] и их функций [4, 24, 31, 34] применимы частные случаи НПФ вида (2) от одной и от двух переменных:

$$g(q) = \sum_{i=0}^{w} a_i q^i \ , \ a_i, q \in G_{(v)}, \tag{4}$$

$$f(q_1, q_2) = \sum_{i_1=0}^{w} \sum_{i_2=0}^{w} a_{i_1 i_2} q_1^{i_1} q_2^{i_2} \ , \ a_{i_1 i_2}, q_1, q_2 \in G_{(v)}, \ w = 2^v - 1. \tag{5}$$

На основе концептуальной модели [43] предложен общий метод синтеза, позволяющий синтезировать генераторы дискретных стохастических процессов класса марковских и их функций при использовании однотипных цифровых устройств, выполняющих вычисление дискретных детерминированных нелинейных функций, заданных произвольным отображением вида (1), на основе НПФ и/или их систем, а также функциональных модулей, выполняющих операции умножения элементов $GF(2^n)$, $GF((2^k)^r)$, где $n = k \cdot r$, и операции вычисления остатка в кольце и в конечном поле. Данный подход на основе общего метода синтеза распространяем на устройства вычисления теоретико-полиномиальных преобразований и дискретной модели отображения/варьирования состояния квантово-механической системы, включающей *N* базисных состояний, и ее частных случаев.

Предложеный общий метод синтеза (ОМС) генераторов ДСП класса марковских и их функций представлен следующими этапами. 1) определение и заданиие требуемого закона ДСП на основе одной или системы эргодических стохастических матриц (ЭСМ). 2) построение полиномиальной модели генератора (ПМГ) ДСП класса марковских и их функций на основе принципа суперпозиции полиномиальных функций – представление каждой ЭСМ (в общем случае – каждого элемента системы ЭСМ) суперпозицией НПФ над полем Галуа, включающей полиномиальную модель генератора дискретной случайной величины (ДСВ) и НПФ вида (2) от *m* переменных, *m* = 1, 2, … , над конечным полем, представляющую произвольное отображение вида (1). 3) структурный синтез ПМГ в заданном базисе однотипных цифровых устройств, анализ сложности с целью построения структурных схем ПМГ, приближенных к оптимальным по заданным критериям. 4) алгоритмический и функциональный синтез цифровых вычислительных устройств и функциональных модулей для выполнения операций в конечном поле, в базисе ПЛИС/FPGA, анализ сложности с целью синтеза устройств и модулей, приближенных к оптимальным по предложенным в работе критериям. 5) отображение схем, полученных на этапах 3) и 4), в архитектуру ПЛИС/FPGA.

В последующих главах приведены результаты по детализации этапов схемы ОМС и по распространению данной схемы на задачи синтеза устройств ЦОС.

Во второй главе представлены результаты по разработке и выполнению этапов 1) и 2) общего метода синтеза генераторов ДСП в виде разработанных **методов синтеза генераторов дискретных стохастических процессов класса марковских и их функций над полем** $GF(2^n)$**.** Показана возможность представления генераторов цепей Маркова [2, 23] и их функций [4, 24, 31, 34, 45] при использовании предложенного принципа суперпозиции НПФ, включающей полиномиальную модель генератора ДСВ, определенного на основе системы некоррелированных генераторов равномерно распределенных псевдослучайных чисел [38], и (в общем случае) суперпозицию НПФ вида (4) и/или (5) над элементами поля Галуа, каждая из которых реализует заданное отображение вида (1) [42]. Предложенный принцип суперпозиции НПФ, как совокупность сформулированных теорем, обосновывает возможность синтеза высокоскоростных генераторов ДСП указанных классов, в архитектуре ПЛИС/FPGA, с применением распределенных вычислений в конечном поле [16].

В п. 2.1 представлены результаты по разработке и выполнению этапов 1) и 2) ОМС для решения задач синтеза и анализа генераторов однородных ЦМ вида

$$(S, P_{(m)}, \pi_0), \tag{6}$$

где $S=\{s_1, s_2,..., s_m\}$ - конечное множество ее состояний, $P_{(m)}$ - эргодическая стохастическая матрица размера $m \times m$, $\pi_0=\{\pi_i\}$, $i=\overline{1, m}$ - m-разрядный стохастический вектор, задающий начальное распределение вероятностей состояний.

Однородная ЦМ представима на основе автономного вероятностного автомата (ВА), определяемого системой:

$$A(1)=(\hat{\mu}, S, \delta(x, s)), \tag{7}$$

где S - тот же объект, что и в (6), $\hat{\mu}$ - ДСВ, принимающая конечное число значений $\mu_1, \mu_2,..., \mu_l$ на входе $A(1)$ с вероятностями $p_1, p_2,..., p_l$, $\overline{P}=(p_1, p_2, \ldots, p_l)$ - стохастический вектор, $0 \le p_i \le 1$, $\sum_{i=1}^{l} p_i = 1$. $\delta(x, s)$ - функция переходов, однозначно ставящая в соответствие паре (x, s) новое состояние $s' \in S$ и для которой множество значений $\{x_i\}=X=\{\mu_i\}$, $i=\overline{1, l}$, $l \le (m^2-m+1)$ (Поспелов Д.А., 1970). Рассмотрим предлагаемый метод реализации этапа 2) ОМС – метод полиномиального представления генератора однородной ЦМ на базе автономного ВА, определенного согласно (7), над $G_{(n)}$. Имеет место

Теорема 2.1.1 (синтеза) [2]. Для системы вида (6) можно вычислить дискретную случайную величину $\hat{\mu}$ и полином $f(x, q)$ вида (5), $x, q, f(x, q) \in GF(2^n)$, минимальная степень которого определена из условия $2^n-1=r \ge \max(m, l)$, $l \le (m^2-m+1)$, с коэффициентами $a_{ij} \in GF(2^n)$, $i, j=\overline{0, r}$, и случайным начальным значением x, такие, что $f(x, q)$ преобразует $\hat{\mu}$ в последовательность состояний заданной цепи Маркова.

ДСВ $\hat{\mu}$, в свою очередь, реализуема на основе НПФ $g(z)$ вида (4) над $G_{(n)}$, задаваемой отображением элементов множества значений n-разрядной дискретной случайной величины $\hat{z}$, $\hat{z} \in \hat{Z}$, распределенной по равновероятному закону, $|\hat{Z}|=2^n$, во множество $\mu_1, \mu_2,..., \mu_l$, $l \le 2^n$, согласно (1) для $m=1$. Теорема 2.1.1 устанавливает возможность представления стохастической матрицы $P_{(m)}$ суперпозицией двух НПФ вида (4) и (5). Согласно теореме 2.1.1, задание ЦМ в виде системы

$$(\hat{\mu}, f(x, q), \pi_0) \equiv (g(\hat{z}), f(x, q), \pi_0), \tag{8}$$

эквивалентно заданию системы (6).

Определение 2.1 [2]. Систему (8) будем называть полиномиальной моделью конечной однородной цепи Маркова над полем Галуа – полиномиальной марковской моделью (ПММ).

Теорема 2.1.1 *обосновывает метод синтеза генераторов однородных ЦМ* вида (6) *на базе ПММ* вида (8), заданной путем представления ЭСМ вида $P_{(m)}$ при использовании суперпозиции НПФ вида (4) и (5) над $G_{(n)}$, в соответствии с этапом 2) ОМС [2]: 1) представление ЭСМ линейной стохастической комбинацией простых матриц - $P_{(m)}=\sum_{i=1}^{l} p_i M_i$, где p_i - элементы стохастического вектора $\overline{P}$, M_i - простые матрицы. 2) определение функции переходов конечного детерминированного автомата (КДА) - $\delta(x, s)$, и закона распределения ДСВ $\hat{\mu}$, на основе полученной линейной комбинации. 3) представление $\hat{\mu}$ и $\delta(x, s)$ НПФ $g(\hat{z})$ и $f(x, q)$ над $G_{(n)}$ вида (4) и (5), соответственно, где задание коэффициентов указанных НПФ производится согласно (3) на основе отображений вида (1) для $m=1, 2$, соответственно. Схема генератора однородной ЦМ представлена на рис. 2.1.1, где модуль «*D*» есть набор *D*-триггеров, составляющих регистр памяти.

Для системы (8) справедлива теорема 2.1.2, обратная теореме 2.1.1, позволяющая решать задачу анализа ПММ - определение ЭСМ по заданной суперпозиции НПФ вида (4) и (5) [2].

Теорема 2.1.2 (анализа). Для заданного полинома $f(x,q)$ вида (5), $x, q, f(x,q) \in GF(2^n)$, с коэффициентами $a_{ij} \in GF(2^n)$, $i,j = \overline{0,r}$, $r = 2^n - 1$, с множеством $\{x_k\}$, $k = \overline{1,l}$ значений переменной x и множеством $\{q_t\}$, $t = \overline{1,m}$ значений переменной q, для дискретной случайной величины $\hat{\mu}$ с множеством значений $\{\mu_k\} = \{x_k\}$, заданной вектором $\overline{P}$ и для вектора π_0 последовательность вычисленных значений $f(x,q)$ является реализацией простой однородной цепи Маркова вида (6), для которой $S = \{q_t\}$, а элементы $P_{(m)}$, $m = |\{q_t\}|$, однозначно определены $\overline{P}$ и $f(x,q)$.

Теорема 2.1.2 *обосновывает метод определения ЭСМ* $P_{(m)}$ *по заданным НПФ* над $G_{(n)}$ - $f(x,q)$ вида (5) и $g(\hat{z})$ вида (4) [2]. 1) определение функции переходов КДА - $\delta(x,s)$, на основе НПФ $f(x,q)$ и закона распределения ДСВ $\hat{\mu}$ на основе НПФ $g(\hat{z})$, путем вычисления отображений вида (1) - $\varphi_2 : G_{(n)} \times G_{(n)} \to G_{(n)}$, реализуемого $f(x,q)$ и $\varphi_1 : G_{(n)} \to G_{(n)}$, реализуемого $g(\hat{z})$. 2) на основе $\delta(x,s)$ и $\hat{\mu}$ определение множества простых матриц - $\{M_i\}$, $i = \overline{1,l}$, и стохастического вектора $\overline{P}$. 3) на основе $\{M_i\}$, $i = \overline{1,l}$, и $\overline{P}$ вычисление ЭСМ, определяющей (6), на основе линейной стохастической комбинации простых матриц - $P_{(m)} = \sum_{i=1}^{l} p_i M_i$.

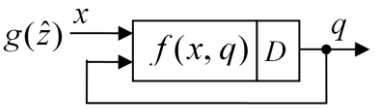

Рис. 2.1.1. Схема генератора однородной ЦМ

Генератор α-связной (α-сложной, $\alpha > 1$) ЦМ, схема которого приведена на рис. 2.1.2, определяем на основе ЭСМ P_α размера $d^\alpha \times d^\alpha$, где d^α - число состояний данной цепи. На множестве состояний α-связной ЦМ Z^α в соответствии с различающимися распределениями, представленными в матрице P_α, зададим разбиение вида

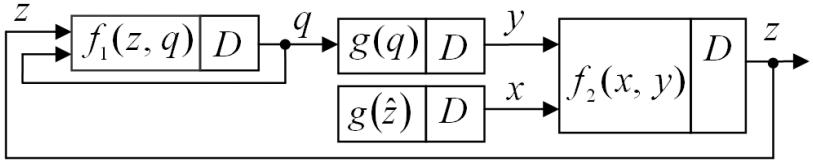

Рис. 2.1.2 Схема генератора α-сложной ЦМ

$$y_1, y_2, ..., y_k,\ y_i \cap y_j = 0,\ y_i \cup y_j = z \text{ при } i \neq j,\ i,j = \overline{1,k},\ k < d^\alpha. \qquad (9)$$

Тогда ЭСМ P_α представима как разложение вида $\sum_{i=1}^{l_3} p_i M(x_i)$, где $l_3 \le (k \cdot d - k + 1)$ (Бухараев Р.Г., Захаров В.М., 1978). Справедлива

Теорема 2.1.3 [4]. Для α-связной цепи Маркова, $\alpha > 1$, заданной стохастической матрицей P_α размера $d^\alpha \times d^\alpha$ и разбиением над Z^α вида (9), последовательность ее состояний представима последовательностью значений функции $\psi_1 = f_1(z,q) \bullet g(q) \bullet f_2(x,y)$ - суперпозицией трех полиномиальных функций над полем $GF(2^n)$, где $2^n \ge \max(h, l_3, d)$, $k \le h \le d^\alpha$, а начальное состояние данной цепи определяется начальным значением переменной полинома q.

В п. 2.2 приведены результаты по разработке и выполнению этапов 1) и 2) ОМС для решения задач ***синтеза генераторов детерминированных и стохастических функций однородных ЦМ*** - $\{Y_t\}$ и $\{Z_t\}$, которые применимы на практике при решении широкого круга задач [4, 24, 34, 39, 41]. Схема генератора ДСП $\{Y_t\}$ представлена на рис. 2.2. Метод синтеза указанных генераторов, представленных на основе НПФ вида (4) и (5), обоснован

рядом теорем [4, 39]. Разобьем множество *S* в системе (6) на непересекающиеся подмножества A_1, A_2, …, A_k:

$$\bigcup_{i=1}^{k} A_i = S, \quad A_i \cap A_j = 0, \text{ при } i \neq j. \tag{10}$$

Теорема 2.2.1 [4]. Для цепи Маркова, заданной согласно (6), последовательность состояний процесса $\{Y_t\}$, заданного разбиением (9) на множестве *S*, представима последовательностью значений функции $\psi_2 = g(q) \bullet f(x,q)$ - суперпозицией двух полиномиальных функций над полем $GF(2^n)$, минимальная степень которого удовлетворяет условию $2^n \geq l$, где $l \leq \left(m^2 - m + 1\right)$, $m = |S|$, а начальное значение q в $f(x,q)$ определяется распределением π_0.

Пусть задано множество *Z*, $|Z| = d$, и $\mu(z/s)$ - стохастическая функция, определяемая ЭСМ $P_{(z/s)}$ размера $m \times d$, и имеющая вид: $P_{(z/s)} = \left(p_{ij}\right)_{m\times d} = \left(p\left(z_j / s_i\right)\right)_{m\times d}$, где p_{ij}, $i = \overline{1,m}$, $j = \overline{1,d}$ определяет вероятность появления буквы z_j при условии, что автономный ВА вида (7) находится в состоянии s_i. Схема генератора ДСП $\{Z_t\}$ представлена на рис. 2.2, $\hat{\mu}'$ есть ДСВ, принимающая l_1 всевозможных значений переменной x', $l_1 \leq \left(md - m + 1\right)$. Имеет место

Теорема 2.2.2 [2]. Последовательность состояний процесса $\{Z_t\}$, заданного системой (10) и функцией $\mu(z/s)$, представима последовательностью значений функции $\psi_3 = f\left(x,q\right) \bullet f_1\left(x',q\right)$ - суперпозицией двух полиномиальных функций над полем $GF(2^n)$, минимальная степень которого удовлетворяет условию $2^n \geq \max(l, l_1)$, где $l \leq \left(m^2 - m + 1\right)$, $l_1 \leq \left(md - m + 1\right)$.

Разложение ЭСМ $P(z/y)_{kxd}$, участвующей в определении ДСП $\{Z'_t\}$, имеет вид $\sum_{i=1}^{l_2} p_i M(x''_i)$, где $l_2 \leq k \cdot d - k + 1$, а $\left\{M(x''_i)\right\}_{i=\overline{1,l_2}}$ определяет НПФ $f_2\left(x'', y\right)$ (рис. 2.2) [4]. Схема генератора ДСП $\{Z'_t\}$ представлена на рис. 2.2, $\hat{\mu}''$ есть ДСВ, принимающая l_2 всевозможных значений x''. Справедливо

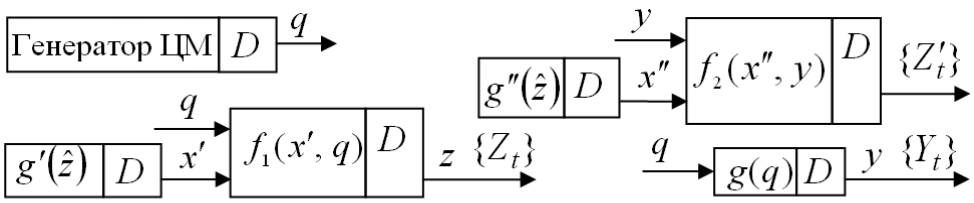

Рис. 2.2. Схемы генераторов ДСП $\{Y_t\}$, $\{Z_t\}$ и $\{Z'_t\}$

Следствие теоремы 2.2.2 [4]. Последовательность состояний процесса $\{Z'_t\}$, заданного системой (10), разбиением (9) на множестве *S* и функцией $\mu(z/y)$, представима последовательностью значений функции $\psi_4 = f_1\left(x', q\right) \bullet g(q) \bullet f_2\left(x'', y\right)$- суперпозицией трех полиномиальных функций над $GF(2^n)$, где $2^n \geq \max(l, l_2)$.

На основе теорем, представленных в п. 2.2, и в соответсвии с этапом 2) общего метода синтеза предложен *метод синтеза генераторов ДСП из классов* $\{Y_t\}$ *и* $\{Z_t\}$ *на основе суперпозиции НПФ вида* (*4*) *и* (5). [4, 24, 34, 41], включающий три этапа. 1) определение каждой из стохастических функций, представленных при использовании ЭСМ, на основе генератора дискретных случайных величин и КДА. 2) кодирование множеств входных и выходных переменных каждой из детерминированных функций, определяющих заданный ДСП, элементами $G_{(n)}$ с целью представления данных детерминированных функций на основе отображений вида (1). 3) определение многочленов вида (4) и/или (5) над $G_{(n)}$ на ос-

нове дискретных детерминированных нелинейных функций, заданных отображениями вида (1).

Представление генераторов ДСП из классов $\{Y_t\}$ и $\{Z_t\}$ на основе нелинейных полиномиальных преобразований над полем Галуа (рис. 2.2) позволяет получать элементы указанных последовательностей путем организации конвейерной обработки данных с сохранением промежуточных результатов, полученных при вычислении значений НПФ вида (4) и/или (5) [39]. При этом законы распределения ДСВ $\hat{\mu}'$ и $\hat{\mu}''$ заданы на основе НПФ $g'(\hat{z})$ и $g''(\hat{z})$, каждая из которых определена над $G_{(n)}$ путем отображения элементов множества $\hat{Z}$ во множества всевозможных значений переменных x' и x'', соответственно.

В п. 2.3 приведены результаты по разработке и выполнению этапа 2) ОМС как ***метода синтеза генератора дискретных случайных величин с заданным законом распределения*** на основе системы, включающей генератор равномерно распределенных дискретных случайных величин (ГРДСВ) на *n* разрядов, и НПФ (от одной или от множества из *m* переменных) над полем Галуа. Метод синтеза генераторов ДСП, определенных в пп. 2.1 и 2.2, основан на описании их вероятностной и детерминированной частей на основе нелинейных полиномиальных преобразований над полем Галуа. Основу вероятностной части указанных генераторов составляет генератор дискретных случайных величин, метод синтеза которого описан в данном разделе [38].

С целью увеличения точности представления вероятности формирования значений ДСВ, требуется увеличивать количество разрядов чисел, снимаемых с выхода ГРДСВ - *n*. Следствие этого – увеличение сложности как ГРДСВ, так и НПФ вида (4) за счет увеличения размерности $G_{(n)}$ [33]. *Предложенный* в [38] *метод*, основан на распределенном представлении генератора ДСВ $\hat{\mu}$ как композиции *m* некоррелированных *v*-разрядных ГРДСВ $\hat{\mu}_1, \ldots, \hat{\mu}_m$ и НПФ от *m* переменных над $G_{(v)}$ вида (2). При этом $2^v \geq 2^{n/m}$ и $2^v \geq l$, где l – количество значений $\hat{\mu}$. Схема данного генератора ДСВ приведена на рис. 2.3. [20].

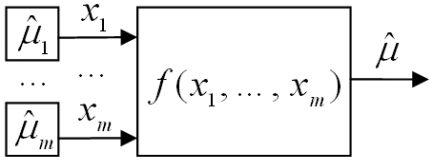

Рис. 2.3. Схема генератора ДСВ

Согласно [38], в качестве меры оценок временной и аппаратной сложности для *m* некоррелированных ГРДСВ на *v* разрядов, определены операции над полем Галуа вида $GF(2)$, позволяющие вычислить произвольную булеву функцию от двух переменных (Ахо А. и др., 1979). Данные оценки ограничены сверху величинами $\lceil \log_2 v \rceil$ и $mv(v-1)$. Предложенный метод позволяет представить вероятности формирования значений $\hat{\mu}$ с дискретностью, равной 2^{-vm}, что обеспечивает абсолютную погрешность представления указанных вероятностей $\varepsilon \leq 2^{-vm-1}$, без увеличения разрядности чисел - *v*, формируемых ГРДСВ, $n = m \cdot v$, (по сравнению с представлением генератора ДСВ $\hat{\mu}$ системой из НПФ вида (4) над $G_{(n)}$ и ГРДСВ на *n* разрядов) [38].

В третьей главе приведены результаты по разработке и детализации этапа 3) ОМС в виде предложенных теоретических основ синтеза на структурном уровне **устройств для вычисления значений дискретных детерминированных нелинейных функций** (ДДНФ) **на основе нелинейных полиномиальных преобразований над полем Галуа**. Актуальность полученных результатов обоснована тем, что генераторы дискретных стохастических процессов класса марковских и их функций (пп. 2.1 – 2.3) в общем случае реализуемы в архитектуре ПЛИС/FPGA на основе системы НПФ, определенных над полем Галуа [41, 43]. Снижение оценок временной сложности для схем устройств вычисления значений ДДНФ, реализованных на ПЛИС/FPGA как IP-ядер, влечет за собой повышение быстродействия устройств ВТ - как генерирующих элементы последовательностей из класса марковских и их функций, так и выполняющих ЦОС. В данной связи, определены как перспективные

следующие подходы к синтезу цифровых устройств вычисления ДДНФ от *m* *n*-разрядных переменных:

- подход на основе системы из *l* многочленов от $m \cdot l$ переменных над полем Галуа вида $GF(2^k)$, $n = k \cdot l$ [11, 41];
- подход с использованием схем, позволяющих вычислить НПФ от многих переменных над $GF(2^n)$, альтернативных по оценкам временной и аппаратной сложности - параллельной, систолической и последовательностной [38].

В п. 3.1 дано представление структурных ***схем устройств для вычисления значений ДДНФ на основе операций над элементами поля Галуа*** вида $G_{(v)}$, в виде определений. Устройства, позволяющие вычислить НПФ вида (2), представляющую заданную ДДНФ от *m* переменных, реализуемы на основе схем, альтернативных по оценкам временной и аппаратной сложности, которые получены на основе количества операций над $G_{(n)}$: параллельной, систолической, последовательностной [38] и параллельно-последовательностной [46].

Определение 3.1.1. Параллельная схема есть схема вычисления значения НПФ вида (2) от *m* переменных над $GF(2^n)$ путем параллельного вычисления значений слагаемых $a_{i_1 \ldots i_m} q_1^{i_1} \ldots q_m^{i_m}$ и их поразрядного сложения по модулю два.

Определение 3.1.2. Систолическая схема есть схема вычисления значения НПФ вида (2) от *m* переменных над $GF(2^n)$ на базе выражения вида

$$f(q_1, ..., q_m) = \sum_{i_m=0}^{w} a_{i_m}\left(q_1^{i_1} \ldots q_{m-1}^{i_{m-1}}\right) q_m^{i_m}, \; w = 2^n - 1, \qquad (11)$$

согласно схеме Горнера: $f(q_1, ..., q_m) =$ $= \left(\ldots\left(a_w\left(q_1^{i_1} \ldots q_{m-1}^{i_{m-1}}\right) q_m + a_{(w-1)}\left(q_1^{i_1} \ldots q_{m-1}^{i_{m-1}}\right)\right) + \ldots + a_1\left(q_1^{i_1} \ldots q_{m-1}^{i_{m-1}}\right)\right) q_m + a_0\left(q_1^{i_1} \ldots q_{m-1}^{i_{m-1}}\right)$, где $a_{i_m}\left(q_1^{i_1} \ldots q_{m-1}^{i_{m-1}}\right) =$ $= \sum_{i_{m-1}=0}^{w} a_{i_{m-1} i_m}\left(q_1^{i_1} \ldots q_{m-2}^{i_{m-2}}\right) q_{m-1}^{i_{m-1}}$, …, $a_{i_3 \ldots i_m}\left(q_1^{i_1}, q_2^{i_2}\right) = \sum_{i_2=0}^{w} a_{i_2 \ldots i_m}\left(q_1^{i_1}\right) q_2^{i_2}$, $a_{i_2 \ldots i_m}\left(q_1^{i_1}\right) = \sum_{i_1=0}^{w} a_{i_1 \ldots i_m} q_1^{i_1}$, значения которых вычисляются по схеме Горнера.

Определение 3.1.3. Последовательностная схема есть схема вычисления значения НПФ вида (2) от *m* переменных над $GF(2^n)$, путем последовательного выполнения операций вида $a_{i+1} q + a_i$, $i = \overline{0, (w-1)}$, над $GF(2^n)$ в выражении (11), вычисляемого по схеме Горнера с сохранением результатов выполнения данной операции.

На основе анализа достоинств и недостатков параллельной, систолической и последовательностной схем цифровых вычислительных устройств значений ДДНФ *предложена параллельно-последовательностная схема* (*ППС*) [46].

Определение 3.1.4. Параллельно-последовательная схема есть схема вычисления значения НПФ вида (2) от *m* переменных над $GF(2^n)$ путем последовательного выполнения групп из *d* операций над $GF(2^n)$, выполняемых параллельно, вида: а) $a_{i_1 \ldots i_m} q_1^{i_1} \ldots q_m^{i_m}$ в (2) для $d \in [2, w/2]$, либо б) $a_{i+1} q + a_i$, $i = \overline{0, (w-1)}$, в (11) для $d > 1$, НОД$(w, (d+1)) = 1$.

Оценки временной и аппаратной сложности для ППС занимают промежуточное положение между соответствующими оценками для параллельной (вариант а)) и систолической (вариант б)) схем с одной стороны и последовательностной схемой с др. стороны [46]. Примем в качестве меры сложности операции над элементами $GF(2)$. Тогда, согласно [38], для параллельной, систолической и последовательностной схем порядки оценок временной и аппаратной сложности равны, соответсвенно,

$$\mathrm{O}_t^{(Par.)}\left(n \log n + (\log m) \log n + m \cdot n\right) \text{ для } n > 1 \text{ и } \mathrm{O}_q^{(Par.)}\left(m^2 \cdot n^2 \cdot 2^{mn}\right), \qquad (12)$$

$$\mathrm{O}_t^{(Sist.)}\left(m \cdot 2^n \cdot \log m\right) \text{ и } \mathrm{O}_q^{(Sist.)}\left(2^{m \cdot n} \cdot n^2\right), \qquad (13)$$

$$\mathrm{O}_t^{(Sec.)}\left(2^{n \cdot m} \cdot \log n\right) \text{ и } \mathrm{O}_q^{(Sec.)}\left(n^2\right). \qquad (14)$$

В п. 3.2 предложен ***метод синтеза устройств для вычисления ДДНФ от m переменных***, представимой НПФ над $G_{(n)} = GF(2^n)$, ***на основе системы из l НПФ от*** $m \cdot l$ ***переменных*** каждая над полем $G_{(k)}$, $n = k \cdot l$ [11, 42]. Определим частный случай НПФ вида (2), $k = 2$, от $p = m \cdot n/2$ переменных над $G_{(2)}$ В [43] показана возможность представления ДДНФ, заданной произвольным отображением вида (1), системой из *n*/2 полиномов вида:

$$\varphi_q(t_1,...,t_p) = \sum_{i_1=0}^{1} ... \sum_{i_p=0}^{1} b_{i_1...i_p} t_1^{i_1} ... t_p^{i_p},\ b_{i_1...i_p}, t_1, ..., t_p \in G_{(2)},\ q = \overline{1,(n/2)}, \qquad (15)$$

выбранной из-за высокой степени соответствия ОУ/$G_{(2)}$ базису ПЛИС/FPGA для большого числа семейств: Virtex-4 (Xilinx, Inc), Stratix (Altera, Inc) и др.

С целью решения задачи синтеза устройств для вычисления значений дискретных детерминированных нелинейных функций от *m* переменных на основе системы НПФ вида (15), обозначим: $U(\psi(x_1, ..., x_m))$- множество всевозможных значений ДДНФ $\psi(x_1, ..., x_m)$; $I(x_j)$ - множество всевозможных значений переменной x_j, $j = \overline{1, m}$, на входе ДДНФ $\psi(x_1, ..., x_m)$. Сформулированы и доказаны теоремы [11], обосновывающие оценки сложности вычисления НПФ вида (2) от *m* переменных над элементами $G_{(n)}$, принадлежащего к классам $A(k)$, $k = \overline{1, n}$, $|U(\psi(x_1, ..., x_m))| \in (2^{k-1}, 2^k]$ и $B(d_1;\ d_2;\ ...\ ; d_m)$, $d_j \in [1, n]$, $j = \overline{1, m}$, ($|I(x_1)| \in (2^{d_1-1}, 2^{d_1}]$, …, $|I(x_m)| \in (2^{d_m-1}, 2^{d_m}]$) на основе системы НПФ вида (15). В качестве меры сложности принято количество операций над элементами $GF(2)$. Определим НПФ вида (2) в виде:

$$y = \psi(x_1, ..., x_m),\ y, x_1, ... x_m \in GF(2^n) \qquad (16)$$

Представив величины *y* и $x_1, ... x_m$, определенные как *n*-разрядные векторы, на основе множества *l* *k*-разрядных векторов, $n = k \cdot l$ - $\{y^{(1)}, ..., y^{(l)}\}$, $\{x_t^{(1)}, ..., x_t^{(l)}\}$, $t = \overline{1, m}$, выражение (16) определяется как система НПФ вида:

$$\{y^{(p)} = \psi_p(x_1^{(1)}, ..., x_1^{(l)}, ..., x_m^{(1)}, ..., x_m^{(l)})\}_p,\ p = \overline{1, l}, \qquad (17)$$

где $y^{(p)}$, $x_t^{(p)} \in GF(2^k)$, $t = \overline{1, m}$. Согласно (16) и (17), обоснована возможность представления НПФ вида (2) над $GF(2^n)$ на основе системы полиномов над $GF(2^k)$. Справедлива

Теорема 3.2.1 [43]. Оценки временной и аппаратной сложности вычисления полиномиальной функции вида (2) от *m* переменных над $GF(2^n)$, на основе системы из *l* полиномиальных функций вида (2) над $GF(2^k)$ от $m \cdot l$ переменных, принадлежащих к классам $A_z(p)$ и $B_z(d_1^{(z)} ... d_{m \cdot l}^{(z)})$, $z = \overline{1, l}$, равны $T_s = \max_{z=\overline{1,l}} \lceil \log_2 \sum_{j=1}^{m \cdot l} d_j^{(z)} \rceil$ и $Q_s = l \cdot \sum_{z=1}^{l} (\sum_{j=1}^{m \cdot l} d_j^{(z)} - 1)$, соответственно.

Предлагаемый в данном пункте *метод синтеза цифровых устройств для вычисления дискретной детерминированной нелинейной функции*, принадлежащей классам $A(n)$ и $B(d_1;\ ...\ ; d_m)$, $d_j = n$, $j = \overline{1, m}$, *на основе системы из l НПФ*, включает три этапа [43]. 1) представление множества значений и *m* множеств значений переменных ДДНФ *l* *k*-разрядными векторами, $n = k \cdot l$. 2) определение *l* ДДНФ, принадлежащих классам $A(k)$ и $B(d_1;\ ...\ ; d_{m \cdot l})$, $d_j = k$, $j = \overline{1, m \cdot l}$, на основе отображений (1) для $m \cdot l$ множеств элементов $G_{(k)}$ в одно множество элементов $G_{(k)}$. 3) вычисление коэффициентов для *l* НПФ от $m \cdot l$ переменных каждая, определенных над $G_{(k)}$, которые соответствуют отображениям вида (1), полученным на этапе 2).

Порядки оценок временной и аппаратной сложности цифровых устройств для вычисления ДДНФ, представленной системой НПФ вида (17) над $G_{(2)}$ на основе параллельной

реализации каждая, вычислены на основе операций над $GF(2)$ и составляют $\mathrm{O}_t\left(\log_2(m\cdot n)\right)$ и $\mathrm{O}_q\left(m\cdot n\cdot l^2\right)$, $l=n/k$, соответственно. Это определяет *преимущество данных устройств по порядкам оценок временной сложности в сравнении с оценками* (*12*) – (*14*) *для устройств, определенных на основе схем, представленных в п. 3.1*: примерно в $n\cdot(m+\log_2 n)/\log_2(m\cdot n)$ раз для параллельной и примерно в $\left(m\cdot 2^n\cdot\log_2 m\right)/\log_2(m\cdot n)$ раз - для систолической, соответственно [43].

В п. 3.3 предложены результаты по разработке и выполнению этапа 3) ОМС как ***метода синтеза генераторов неоднородных цепей Маркова*** (НЦМ) ***и их функций на основе цифровых устройств для вычисления ДДНФ*** [35, 41], определяемых на основе НПФ от многих переменных: как НПФ вида (2) над полем $G_{(n)}$ [2, 4] (п. 3.1), так и системы многочленов вида (15) над $G_{(2)}$ (см. п. 3.2) [11, 43]. Метод является развитием подхода к представлению однородных ЦМ и их функций на основе принципа суперпозиции нелинейных полиномиальных преобразований в конечных полях [2, 4, 23, 31]. НЦМ задается как последовательность состояний ВА вида $A_{НЦМ}=\left(V, S, \mu(s'/s, v)\right)$, где $\mu(s'/s, v)$ - функция переходов, задаваемая системой стохастических матриц размерности $m\times m$ вида $\left\{P_{(s),i}, i=\overline{1,h}\right\}$, $V=\{v_1 \quad v_2 \quad \ldots \quad v_h\}$ - входной алфавит, $S=\{s_1 \quad s_2 \quad \ldots \quad s_m\}$ - множество состояний. Функция НЦМ задана последовательностью букв выходного алфавита ВА общего вида $A_{ФНЦМ}=\left(V, S, Z, \mu(s', z/s, v)\right)$, где $Z=\{z_1 \quad z_2 \quad \ldots \quad z_d\}$ - выходной алфавит, $\mu(s', z/s, v)$ задается двумя системами ЭСМ: $\left\{P_{(s),i}, i=\overline{1,h}\right\}$ - $m\times m$-матрицы, определенные аналогично $A_{НЦМ}$ и $\left\{P_{(z),i}, i=\overline{1,h}\right\}$ $m\times d$-матрицы, определяющие вероятностный закон последовательности выходных букв. На основе $\left\{P_{(s),i}, i=\overline{1,h}\right\}$ и $\left\{P_{(z),i}, i=\overline{1,h}\right\}$ образуем ЭСМ $P_{(s,h)}$ и $P_{(z,h)}$ размерности $h\cdot m\times m$ и $h\cdot m\times d$ соответственно. Определены разложения $P_{(s,h)}=\sum_{i=1}^{l_s} p_i M_i$ и $P_{(z,h)}=\sum_{i=1}^{l_z} p_i M_i$, где M_i - простая матрица. Величины $p_i^{(s)}, p_i^{(z)}\in[0,1]$, $\sum_{i=1}^{l_s} p_i^{(s)}=1$ и $\sum_{i=1}^{l_z} p_i^{(z)}=1$, $l_s\le hm^2-m+1$, $l_z\le hmd-d+1$. На основе полученных систем простых матриц для каждого разложения строим конечный детерминированный автомат, основываясь на НПФ вида (4) и (5) [23, 31]. В [35] теоретически обоснована возможность представления генераторов, задаваемых $A_{НЦМ}$ и $A_{ФНЦМ}$, на основе суперпозиции НПФ над $GF(2^n)$.

Схема генератора, задаваемого $A_{ФНЦМ}$, как общий случай рассматриваемых генераторов ДСП класса марковских и их функций на основе нелинейных полиномиальных преобразований [42] приведена на рис. 3.3, где $|\hat{Z}|=2^n$ - разрядность равномерно распределенных случайных чисел, применяемых в генераторах дискретных случайных величин (ГДСВ1 и ГДСВ2), $|X'|=l_S$, $|X''|=l_Z$, $|V|=h$, $|S|=m$ и $|Z|=d$. При задании ограничения на НПФ f_2 ($|X''|=0$) получаем последовательность элементов *y* как детерминированную функцию ЦМ (п. 2.2), однородных и неоднородных. При ограничении на НПФ f_1 ($|V|=0$) получаемая последовательность элементов *q* есть однородная ЦМ (п. 2.1).

Предложен метод синтеза генератора неоднородных цепей Маркова и их функций, включающий два этапа: 1) синтез цифровых устройств для вычисления НПФ, заданных в блоках 1 и 2 на рис. 3.3, на основе их представления системами НПФ от многих переменных над $G_{(2)}$ вида (15) согласно методу, предложенному в п. 3.2 [42]; 2) синтез ГДСВ 1 и ГДСВ 2, определяющих ДСВ x' и x'', соответственно, с заданным законом распределения: ГДСВ*i* реализуем системой из η_i *n*-разрядных равномерно распределенных некоррелиро-

ванных дискретных случайных величин и НПФ от η_i переменных согласно методу, предложенному в п. 2.3 [38], $i = 1, 2$.

Представление генератора, задаваемого $A_{ФНЦМ}$ и приведенного на рис. 3.3, на основе нелинейных полиномиальных преобразований над полем Галуа позволяет получать элементы указанных последовательностей путем организации конвейерной обработки данных с сохранением промежуточных результатов [43]; вычисление значений НПФ $f_1(v, x', q) = q$ и $f_2(x'', q) = z$ производится при использовании устройств, определенных как на основе предложенных структурных схем (п. 3.1), так и систем НПФ над $G_{(2)}$ (п. 3.2) [43]. Данное обстоятельство создает предпосылки для представления генератора, задаваемого произвольным $A_{ФНЦМ}$, на основе однотипных IP-ядер, адаптированных под однородную архитектуру ПЛИС/FPGA определенных семейств за счет организации распределенных вычислений в конечном поле [16, 18, 46].

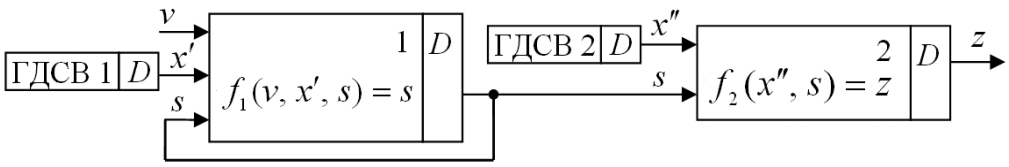

Рис. 3.3. Схема генератора стохастической функции НЦМ

В четвертой главе, как детализация результатов этапа 4) ОМС (см. главу 1), предложены **схемы функциональных модулей** (ФМ) **операций** умножения и вычисления остатка по заданному модулю **в конечных полях**, определенные на структурном и алгоритмическом уровнях. Данные ФМ являются базовыми для реализации цифровых устройств для генерирования дискретных стохастических процессов класса марковских и их функций (пп. 2.1 – 2.3, 3.3) и для вычисления дискретных детерминированных нелинейных функций, заданных произвольным отображением вида (1) (пп. 3.1 и 3.2), на основе НПФ вида (2) [43]. Проблемный вопрос - синтез ФМ операций над элементами конечных полей большой размерности при ограничениях на оценки временной сложности данных операций. Подходы к разрешению данной проблемы основаны на организации распределенных вычислений при обработке потоков однотипных данных. В частности, при выполнении операции умножения элементов поля Галуа вида $G_{(n)}$ - ОУ/$G_{(n)}$, распределенные вычисления организованы на основе перехода к ОУ элементов расширения поля Галуа вида $G_{(k)}^{(r)} = GF((2^k)^r)$ - ОУ/$G_{(k)}^{(r)}$, $k \cdot r = n$. ФМ, выполняющий ОУ/$G_{(n)}$, определен как IP-ядро на структурном уровне на основе операций над элементами поля $G_{(k)}$, размерность которого – в 2^{n-k} раз меньше, чем $G_{(n)}$ [9, 26, 36]. Что касается операции вычисления остатка от деления по заданному модулю, то ФМ, ее реализующий, определен как IP-ядро на структурном уровне при использовании конвейерной схемы [12, 14, 40].

В п. 4.1 предложены ***функциональные модули ОУ/$G_{(n)}$ как IP-ядра***, определение которых на структурном и алгоритмическом уровне допускает возможность распараллеливания вычислений отдельных двоичных разрядов произведения. Согласно [9, 26], оценки временной сложности данного ФМ при определенных образующих многочленах поля $G_{(n)}$ меньше, чем для ФМ ОУ/$G_{(n)}$, определенной в [1, 29]. Пусть $\alpha, \beta \in G_{(n)}$, $\alpha = (\alpha_0 \quad ... \quad \alpha_{n-1})^T$ и $\beta = (\beta_0 \quad ... \quad \beta_{n-1})^T$, где $\alpha_i, \beta_i \in GF(2)$. Возможность создания ФМ ОУ/$G_{(n)}$ на основе распределенных вычислений обосновывает

Утверждение 4.1 [9, 26]. Вычисление разрядов произведения c элементов α и β, $\alpha, \beta, c \in G_{(n)}$ производится параллельно согласно формуле:

$$c_i = (\alpha_0 \quad ... \quad \alpha_i)\cdot(\beta_i \quad ... \quad \beta_0)^T + \sum_{j=1}^{n-1}\left((\alpha_j \quad ... \quad \alpha_{n-1})\cdot(\beta_{n-1} \quad ... \quad \beta_j)^T \xi_i^{j+n-1}\right), \qquad (18)$$

где $i = \overline{0, n-1}$, $\xi^m = \left(\xi_0^m \quad \xi_1^m \quad ... \quad \xi_{n-1}^m\right)^T$, $\alpha_i, \beta_i, c_i, \xi_i^m \in GF(2)$, ξ^m - степени примитивного элемента, корня образующего многочлена $G_{(n)}$: $P(\xi) = 0$, $m = \overline{n, (2n-2)}$.

На основе операций над элементами $GF(2)$, принятых в качестве меры сложности, для функционального модуля ОУ/$G_{(n)}$, определенного на основе выражения (18), вычислены оценки временной и аппаратной сложности: $T\left(G_{(n)}\right) = \left]\log_2 2n\right[$ и $Q\left(G_{(n)}\right) = \sum_{i=0}^{n-1}(2n-1) = n(2n-1)$, соответственно [9, 26].

В п. 4.2 предложены ***функциональные модули ОУ/$G_{(k)}^{(r)}$ на основе IP-ядер***, определенные на структурном и алгоритмическом уровне согласно [9, 26, 36] (рис. 4.2). Элементы $G_{(k)}^{(r)}$ представимы как $n = k \cdot r$ - разрядные векторы, то есть как r векторов размерности k: $\alpha = (\alpha_0 \quad ... \quad \alpha_{r-1})^T$ и $\beta = (\beta_0 \quad ... \quad \beta_{r-1})^T$, $\alpha_i, \beta_i, c_i \in GF(2^k)$, $\alpha, \beta \in G_{(k)}^{(r)}$. Справедливо обобщение утверждения 4.1 –

Утверждение 4.2 [9, 26]. Вычисление элементов произведения α и β, $\alpha, \beta \in G_{(k)}^{(r)}$ - c_i производится согласно (18) для $n = r$, $i = \overline{0, r-1}$, где $\xi^m \in G_{(k)}^{(r)}$, $m = \overline{r, (2r-2)}$, - степени примитивного элемента, корня образующего многочлена $G_{(k)}^{(r)}$: $P(\xi) = 0$.

На основе утверждения 4.2 *предложен алгоритм конвейерного вычисления ОУ/$G_{(k)}^{(r)}$:* 1) вычисление множества ОУ/$G_{(k)}$ и 2) вычисление множества ОУ на константу и операций поразрядного сложения по модулю два над элементами поля $G_{(k)}$. Для

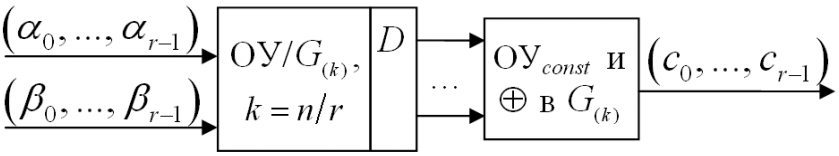

Рис. 4.2. Схема функционального модуля ОУ/$G_{(k)}^{(r)}$

определенных $G_{(n)}$ и $G_{(k)}^{(r)}$ на структурном уровне *представляется возможным уменьшить оценки временной сложности функциональных модулей ОУ/$G_{(k)}^{(r)}$, по сравнению с ФМ ОУ/$G_{(n)}$, $n = k \cdot r$, $k > 1$, примерно в* $1 + \log_2(n/k)/(\log_2 2k)$ *раз* за счет организации распределенных вычислений [9, 26, 43]. В частности, для $k = 2$ (см. п. 3.2), - примерно в $1 + 0{,}5 \cdot \log_2(n/2)$ раза.

В п. 4.3 предложены две альтернативные ***схемы функциональных модулей операции вычисления остатка от деления по заданному модулю для потока чисел*** (ОВО), определенные как IP-ядра на структурном и алгоритмическом уровне. *Особенность данных ФМ – уменьшение оценок временной сложности вычисления ОВО за счет сохранения промежуточных результатов, получаемых на каждой ступени конвейера* (см. рис. 4.3). Пример эффективного использования указанных ФМ - синтез генератора Смита из класса конгруэнтных генераторов равномерно распределенных псевдослучайных чисел над конечным полем [12, 19, 40]. В зависимости от того, какие логические операции реализуют программируемые элементы заданной ПЛИС/FPGA, производится выбор одного из двух предложенных IP-ядер ФМ для операции вычисления остатка от деления по заданному модулю, в наибольшей степени соответствующего предъявляемым требованиям к оценкам временной и/или аппаратной сложности. Обозначим как $T_{cm}(c)$, $T_{sb}(c)$ и T_{mx} - оценки временной сложности для операций сравнения и вычитания с константой c, а также для операции мультиплексирования n-разрядных чисел, а $T_{\otimes}(q)$ - оценку временной сложности операций умножения на константу q разрядности l. Оценки аппаратной сложности указанных элементов

обозначим как $Q_{cm}(c)$, $Q_{sb}(c)$, Q_{mx} и $Q_{\otimes}(q)$, соответственно. Общая структурная схема ФМ ОВО приведена на рис. 4.3.

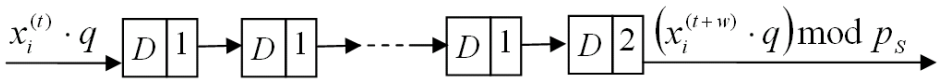

Рис. 4.3. Общая схема функционального модуля операции вычисления остатка по заданному модулю

Для первого варианта IP-ядра функционального модуля, определенной на основе операций вычисления частичных остатков от деления при заданных постоянных величинах q и p_s (l- и k-разрядных, соответственно) на каждом этапе конвейера [40], справедливы

Утверждение 4.3.1 [40]. Оценки временной сложности функционального модуля операции вычисления остатка по заданному модулю для потока чисел на основе вычисления частичных остатков, будут меньше, чем для функционального модуля, заданного на основе схемы операции вычисления остатка по заданному модулю без использования конвейера, в $l+1+T_{\otimes}(q)/T'$ раз, если $T' \geq T_{\otimes}(q)$, и в $1+(l+1)(T'/T_{\otimes}(q))$ раз – если $T' < T_{\otimes}(q)$, где $T' = \max\left(T_{cm}(p_s),\ T_{cm}(2p_s),\ T_{sb}(p_s),\ T_{sb}(2p_s)\right)+T_{mx}$.

Утверждение 4.3.2 [40]. Оценка аппаратной сложности функционального модуля операции вычисления остатка по заданному модулю на основе вычисления частичных остатков сотавляет $Q(x_{i+1}) = Q_{\otimes}(q) + (l+1)\cdot\left(Q_{cm}(p_s)+Q_{cm}(2p_s)+Q_{sb}(p_s)+Q_{sb}(2p_s)+Q_{mx}\right)$, как и для функционального модуля, заданного на основе схемы операции вычисления остатка по заданному модулю без использования конвейера.

Однако, для ФМ операции вычисления остатка по заданному модулю на основе вычисления частичных остатков требуется $k(l+1)$ D-триггеров, применяемых для сохранения промежуточных сезультатов на каждой ступени конвейера [40].

Второй вариант IP-ядра ФМ операции вычисления остатка по заданному модулю определяет T-кратное выполнение функции вида [14, 19]:

$$G(A) = a_{n-1}b_{n-1} + \ldots + a_{k+1}b_{k+1} + a_k 2^k + \ldots + a_1 2 + a_0, \qquad (19)$$

где $A = (a_{n-1}, \ldots, a_0)$ - n-разрядное двоичное число, $b_i = 2^i$ для $i = \overline{0,k}$ и $b_j = 2^j \bmod p_s$ для $j = \overline{k+1, n-1}$, k – разрядность p_s. Значение T устанавливается эмпирически для заданного p_s согласно методике, предложенной в [14]. Обозначим T_{RG}, T_B и T_{Σ} - оценки временной сложности для параллельного регистра, буферного элемента и сумматора на $n-k$ входов. Согласно [14] справедливо следующее

Утверждение 4.3.3. Для функционального модуля операции вычисления остатка по заданному модулю, заданного на основе однотипных операций вида (19), величина оценок временной сложности, по сравнению с функциональным модулем, заданным на основе указанной схемы операции вычисления остатка по заданному модулю без использования конвейера, уменьшена в

$$(l+1)\cdot\left(\max\left(T_{cm}(p_s), T_{cm}(2p_s), T_{sb}(p_s), T_{sb}(2p_s)\right)+T_{mx}\right)/T'' \text{ раз,}$$

где $T'' = T_{RG} + \max\left(T_B + T_{\Sigma}, \max\left(T_{cm}(p_s), T_{sb}(p_s)\right)+T_{mx}\right)$.

При этом для ФМ ОВО, определенного на основе операций вида (19), требуется $\left(T\cdot\left(n(k+2)-(k+1)^2\right)+2k+3\right)$ D-триггеров.

<u>В пятой главе</u>, как развитие п. 5) ОМС, предложена **«Методология реализации устройств**, описанных в главах 3 – 5 и позволящих выполнить операции над конечным полем, **на основе однотипных IP-ядер, представленных на ПЛИС/FPGA»**. Методология включает ряд методик синтеза и анализа, основанных на предложенном ОМС. Методики представлены в пп. 5.1 – 5.3. Показано, что общий метод синтеза устройств ВТ для генерирования дискретных стохастических процессов класса марковских и их функций (пп. 2.1-2.3, 3.3) на РВС ПА сводится к методике синтеза однотипных IP-ядер, реализующих цифровые

устройства для вычисления ДДНФ от многих переменных (пп. 3.1, 3.2), а также ФМ для вычисления операций умножения элементов $G_{(n)}$ или $G_{(k)}^{(r)}$ (пп. 4.1 и 4.2) и операции вычисления остатка по заданному модулю (п. 4.3), на ПЛИС/FPGA [16]. Указанный общий метод применим и к синтезу устройств для вычисления теоретико-полиномиальных преобразований [21, 27, 43] и отображения/варьирования состояния КМС(N) [6 – 8, 21, 27, 32]. При синтезе однотипных IP-ядер использован подход, предполагающий предварительную структурную и функциональную проработку описывающих их схем на предмет возможности организации распределенных вычислений [1]. Подход, основанный на применении ОМС, включает в качестве важнейших задачи оценки: 1) количества и эффективности задействования конфигурируемых ресурсов ПЛИС/FPGA для синтеза IP-ядер [1, 5, 9, 10, 25, 26]; 2) количества корпусов ПЛИС/FPGA, требуемых для реализации устройства ВТ, и времени задержки его (устройства) работы [16].

Решена задача выбора реализации для заданного функционального модуля, представленного как IP-ядро, приближенное к оптимальному по предложенным критериям [1, 5, 9, 10, 25, 26]. Причем одной структурной схеме заданного ФМ, определяемой как IP-ядро на алгоритмическом уровне, может быть поставлено в соответствие множество *FS* - функциональных схем в базисе ПЛИС/FPGA, определяемых как IP-ядра на уровне физической реализации и удовлетворяющих ограничениям по указанным критериям. Синтез ФМ в базисе ПЛИС/FPGA выполнен путем создания принципиальной схемы IP-ядра, его описывающего, при использовании спец. САПР: ISE 13.4 – Foundation (Xilinx Corp.) и Quartus II v. 9.0 (Altera Corp.). Принципиальные схемы включают в себя элементы, определяющие арифметические и логические операции над двоичными числами заданной разрядности, а также связи между указанными элементами. Порядок ввода принципиальной схемы ФМ в САПР выполнен в зависимости от разрядности n обрабатываемых операндов - двоичных векторов. Если n относительно небольшое (например, не превышает 16 - 20 для операции умножения элементов $G_{(n)}$ или $G_{(k)}^{(r)}$ (пп. 4.1 и 4.2) и 12 – для операции вычисления остатка по заданному модулю (п. 4.3)), ФМ представим в САПР при использовании схемотехнического редактора; иначе - использование схемотехнического редактора сопряжено с большими затратами труда и для описания модуля в САПР применен HDL-код.

Предложен двухэтапный метод синтеза [16] устройств ВТ на РВС ПА, элементами которой являются ПЛИС/FPGA, на основе IP-ядер, представленных пп. 3.1, 3.2, 4.1 – 4.3. При этом на одном корпусе ПЛИС/FPGA размещается как минимум одно IP-ядро, являющееся составной частью синтезируемого устройства.

Для обеспечения синтеза на ПЛИС/FPGA семейства генераторов, описываемых полиномиальной марковской моделью (определение 2.1), путем выделения из данного семейства k типичных представителей, и распознавания принадлежности данных генераторов к одному из заданных подклассов, решены задачи классификации [3, 17, 22, 30, 37] и идентификации [13, 15] при использовании методов многопараметрической статистики. Методика классификации позволяет в Q/k раз уменьшить суммарный объем файлов конфигурации ПЛИС/FPGA, реализующих семейство из Q генераторов конечных простых однородных цепей Маркова, $k << Q$. Методика идентификации генераторов ОЦМ, заданных стохастическими матрицами из определенных подклассов, позволяет существенно уменьшить длину ОЦМ, требуемую для идентификации данных генераторов с доверительной вероятностью 0,95: в 1,4 – 64 раза. Представленные методики внедрены в НПО «Радиоэлектроника» (г. Казань), в ВА ВКО (г. Тверь) и в НПП МЦЭИР (г. Тверь).

В п. 5.1 предложена ***методика оценки степени соответствия функционального модуля архитектуре ПЛИС/FPGA*** [10]. Методика позволяет оценить степень соответствия для ФМ, описываемых в пп. 4.1 – 4.3, при использовании критериев, характеризующих: 1) долю ресурсов взаимосвязи в общих затратах логических ресурсов ПЛИС - K_{PT} [1, 5]; 2) вклад задержки межсоединений (МС) в общую оценку времени задержки функциониро-

вания - K_t [1, 5, 9]; 3) оценку времени прохождения сигнала внутри логических элементов ПЛИС в пересчете на один уровень ЭС - $t_{з\,ЭС}$ [10]; 4) эффективность задействования ГФ внутри конфигурируемых логических элементов (ЛЭ) - $K_з$ [25].

Замечание 5.1. Если для синтеза ФМ сконфигурировано не более 50% ЛЭ и не более 50% блоков ввода-вывода (БВВ), то, согласно опыту синтеза ФМ различного назначения на ПЛИС/FPGA (Норенков И.П., Пономарёв В.И., Шабалин Л.А. и др.), существуют реализации функциональных схем, в большой степени соответствующие архитектуре ПЛИС/FPGA по заданным критериям.

В п. 5.2 предложена, как составная часть п. 5) ОМС (глава 1), ***методика оценки сложности синтеза устройств ВТ на основе IP-ядер на распределенных вычислительных системах с программируемой архитектурой*** [16]. ПЛИС/FPGA включает такие виды программируемых ресурсов как МС, ЛЭ и БВВ. Количество ЛЭ и БВВ, в большей степени определяет возможности ПЛИС по реализации множества IP-ядер в одном её корпусе. Каждое из устройств ВТ описывается на основе графа алгоритма вычислений (Каляев И.А., Левин И.И. и др.). Вершинам данного графа соответствуют однотипные цифровые вычислительные устройства (или функциональные модули), описываемые как IP-ядра, общее количество которых равно $\sum_{i=1}^{m} n_i$, где n_i - количество ядер *i*-го типа, *m* – количество типов IP-ядер. Для синтеза IP-ядер *i*-го типа на ПЛИС/ FPGA требуется $q_{\mathrm{LE}}^{(i)}$ ЛЭ и $q_{\mathrm{IOB}}^{(i)}$ БВВ. При этом общее количество ЛЭ и БВВ, задействуемых под логические входы или выходы, внутри одного корпуса ПЛИС/FPGA определено как Q_{LE} и Q_{IOB}, соответственно. Задача оценки сложности синтеза определенного устройства (или модуля) по количеству корпусов ПЛИС определенного типа (N_{FPGA}) и по времени задержки его функционирования (T_{FPGA}) сводится к решению двумерной задачи об упаковке в контейнеры. Первое измерение - количество ЛЭ, а второе – количество БВВ. IP-ядра (с параметрами $q_{\mathrm{LE}}^{(i)}$ и $q_{\mathrm{IOB}}^{(i)}$) выступают в качестве объектов упаковки, а корпусы ПЛИС (с параметрами $\gamma \cdot Q_{\mathrm{LE}}$ и Q_{IOB}) – как контейнеры, где γ – коэффициент задействования ЛЭ ПЛИС, $0 < \gamma < 1$, определяемый проектировщиком. Эмпирически установлено, что для приближенного к оптимальному (для обеспечения $T_{\mathrm{FPGA}} \to \min$) размещения ЛЭ, используемых для реализации на ПЛИС IP-ядер, значения $\gamma \in [0{,}5;\ 0{,}7]$ (Норенков И.П., Пономарёв В.И., Шабалин Л.А.).

На ПЛИС семейства Virtex-4 - XC4VLX200 FF1513-11 реализованы IP-ядра, позволяющие вычислить элементы системы вида (15) - НПФ вида (2) от *m* переменных (НПФ(*m*)), определенных над полем $G_{(2)} = GF(2^2)$. Данные НПФ определены на основе следующих структурных схем (см. п. 3.1): параллельной (ПарС) и параллельно-последовательностной (ППС).

На одной ПЛИС заданного типа (при условии, что $\gamma \le 0{,}5$) на основе ПарС реализуемы IP-ядра для реализации НПФ(*m*), $m \le 7$: до двух IP-ядер для НПФ(7) (общее время задержки функционирования – $T_з$ = 30,9 нс., критерий 2) (см. п. 5.1) – K_t = 76,4 %) и до 11-ти IP-ядер для НПФ(6) ($T_з$ = 26,4 нс., K_t = 74,5 %). Что касается реализации НПФ(*m*) на основе ППС, то на указанной ПЛИС синтезированы IP-ядра, реализующие вычисление значения $\sum_f a_{i_1 \ldots i_m} q_1^{i_1} \ldots q_m^{i_m} \in G_{(2)}$, $f = 16$, – частичных сумм (ЧС(*f*, *m*)). Количество IP-ядер, реализуемых на одной ПЛИС XC4VLX200 FF1513-11 с применением ПСС, определено не по количеству задействованных ЛЭ, а по числу задействованных блоков ввода-вывода (БВВ) ПЛИС, т.к. доля задействованных БВВ для указанных устройств будет выше, чем доля задействованных ЛЭ. На одной ПЛИС реализуемы до десяти ЧС(16, 6) ($T_з$ = 8,81 нс., K_t = 59,2 %) и до четырех ЧС(16, 34) ($T_з$ = 13,5 нс., K_t = 60,3 %).

Предложен метод оценки параметров N_{FPGA} *и* T_{FPGA} *для устройств ВТ на РВС ПА*, реализующих как произвольную дискретную детерминированную нелинейную функцию (пп. 3.1 – 3.2), так и теоретико-полиномиальные преобразования (п. 5.1) и генераторы дискретных стохастических процессов класса марковских и их функций (пп. 2.1 – 2.3, 3.3), при использовании ДДНФ. Метод позволяет выполнить предварительный анализ характеристик реконфигурируемых ресурсов, требуемых для реализации широкого класса устройств ВТ, синтезируемых на основе однотипных цифровых устройств (функциональных модулей), на РВС ПА [16, 18, 44] и включает два этапа: 1) оценка количества ЛЭ и БВВ, требуемых для реализации одного IP-ядра *i*-го типа, $i=\overline{1,m}$, - $q_{\text{LE}}^{(i)}$ и $q_{\text{IOB}}^{(i)}$, на одной ПЛИС/FPGA (с заданными параметрами $k\cdot Q_{\text{LE}}$ и Q_{IOB}) при использовании специализированной САПР; 2) на основе результатов решения двумерной задачи об упаковке в контейнеры вычисление значений параметров T_{FPGA} и N_{FPGA}.

Предложенный метод открывает возможности для предварительного анализа характеристик реконфигурируемых ресурсов, требуемых для реализации широкого класса устройств ВТ, синтезируемых на основе однотипных цифровых устройств (или функциональных модулей), на РВС ПА [16, 18, 55, 56, 58].

В п. 5.3 предложены ***методики синтеза и идентификации семейства генераторов, описываемых полиномиальными марковскими моделями*** (ПММ). При реализации семейства генераторов дискретных стохастических процессов, задаваемых ПММ вида (8), на ПЛИС/FPGA, существует проблема хранения массивов исходных данных большей размерности. Указанная проблема разрешена путем многопараметрической классификации множества стохастических матриц класса эргодических *P*, задающих указанные ПММ, мощности *Q* методами многомерной математической статистики, с последующим выделением представителей *k* получаемых групп (кластеров) – задачи типизации, $k<<Q$. Задача решена при использовании метода кластерного анализа (КА) для ЭСМ из подклассов положительных, дважды стохастических и с локальными переходами [22, 30, 37]. Предложено множество признаков, $\left\{c_j,\ j=\overline{1,10}\right\}$, отражающее свойства ЭСМ *P*, существенные для многопараметрической классификации [22, 30, 37]. *Методика многопараметрической классификации ЭСМ* включает два этапа [17, 22, 30]: 1) КА множества объектов - ЭСМ *P* с применением разработанного множества признаков $\left\{c_j,\ j=\overline{1,10}\right\}$; 2) оценка качества результатов КА: оценки адекватности кластеризации и коррекция результатов КА при использовании метода дискриминантного анализа [3, 37], а также оценка корреляции между признаками $\left\{c_j,\ j=\overline{1,10}\right\}$ методом факторного анализа.

С целью распознавания принадлежности семейства генераторов, задаваемых ПММ вида (8), определенных на основе ЭСМ размерности $m\times m$, к одному из конечного множества подклассов, *предложена методика многопараметрической идентификации ЦМ*, порождаемых указанными генераторами. Идентификация производится на основе предложенного множества признаков (МнП) $\tilde{h}\in\left\{\tilde{v}_g\quad \tilde{w}_g\quad \tilde{f}_k\right\}$, $k=\overline{1-m,m-1}$, $g=\overline{1,4}$, вычисляемых непосредственно по ЦМ ограниченной длины *N*, с заданной доверительной вероятностью *p*. Подклассы ЭСМ из множества - треугольные (верхние и нижние) и блочно-сообщающиеся (правые и левые), имеют различную степень сходства/различия структур [13, 15]. Показано, что *для идентификации генератора ЦМ*, заданного на основе ЭСМ размерности $m\times m$ (биграмм), элементы которой варьируются с дискретностью $D=5\cdot10^{-2}$, с вероятностью $p=0{,}95$, требуется *N* = 386 элементов ЦМ, причем *N* практически не зависит от значения *n*. Тогда как для идентификации аналогичного объекта с $p=0{,}95$ *на основе предложенного МнП*, требуется *N* = 284 элемента ЦМ для *n* = 6 и *N* = 6 для *n* = 256, то есть *требуется элементов ЦМ в 1,4 - 64 раза меньше*, соответственно [15]. Данное обстоятель-

ство позволяет существенно уменьшить время идентификации генераторов ЦМ, определенных на основе ЭСМ заданных подклассов.

<u>В шестой главе</u>, «Техническая реализация и применение устройств ВТ на основе нелинейных полиномиальных преобразований над конечным полем», представлены результаты по применению предложенных теоретических основ общего метода синтеза (гл. 1) как в задачах реализации генераторов ДСП класса марковских и их функций, так и в задачах создания специализированных устройств ВТ ЦОС, как существующих, так и перспективных. Во-первых, в направлении синтеза устройств ВТ для теоретико-полиномиальных преобразований на примере ДПФ, ДПХ и алгоритмов цифровой фильтрации с импульсной характеристикой конечной длительности (КИХ-ф.) на основе систем НПФ в поле Галуа (п. 3.2), причем каждая НПФ реализуема одним из однотипных функциональных модулей [43]. Во-вторых, на применение ФМ операции умножения элементов полей вида $G_{(n)}$ и $G_{(k)}^{(r)}$ (пп. 4.1 и 4.2) для синтеза устройства ВТ, применяемого для отображения/варьирования состояния дискретной модели квантово-механической системы с N базисными состояниями - КМС(N) [8] а также ее частных случаев: КМС(2) (кубит) [6, 32] и КМС(4) (простейший регистр с двумя взаимосвязанными кубитами) [7].

Для решения задачи синтеза устройств ВТ, применяемых для отображения/варьирования состояния КМС(N), в соответствии с предложенной методикой (п. 5.1), синтезированы ФМ, реализующие операции умножения (ОУ) элементов $G_{(n)}$ и $G_{(k)}^{(r)}$ (пп. 4.1 и 4.2). Функциональные схемы реализации ОУ в базисе ПЛИС/FPGA получены при использовании спец. САПР (см. введение к гл. 5).

Для уствойств ВТ, синтезируемых при использовании цифровых устройств для вычисления дискретных детерминированных нелинейных функций, за счет параллельного вычисления системы НПФ над полем $GF(2^2)$ (п 3.2) на РВС ПА «Медведь» (НИИ многопроцессорных вычислительных систем им. А.В. Каляева Южного федерального университета (НИИ МВС ЮжнФУ), г. Таганрог), *увеличена скорость выполнения алгоритмов ЦОС* по сравнению с реализациями на ПЛИС EP2C5T144C6 (семейство Cyclone II) в системе остаточных классов (СОК) (Галанина Н.А., 2011) и на спец. процессорах ADSP-TS001 (Analog Devices, Inc., 2010) и AM1808 ARM Microprocessor (Texas Instrument, Inc., 2011) в позиционной системе счисления (ПСС) *в 1,2 – 2,6 раза*. Достигнутое преимущество позволило внедрить устройства, реализующие ДПФ и КИХ-ф. на основе предложенной общей структурной схемы, ориентированной на архитектуру ПЛИС/FPGA, в НПП «Измерительные технологии» (г. Саров).

Реализуемые на РВС ПА «Медведь» генераторы ОЦМ (рис. 2.1.1, $|Q| \le 2^3 \div 2^6$, $|X| \le 2^8 \div 2^9$, $|Z| \le 2^{14}$) и стохастической функции НЦМ (рис. 3.3, $|Z|, |S| \le 2^6$, $|V| \le 2^4$, $|X'|, |X''| \le 2^8$ и $|\hat{Z}| \le 2^{12}$), генерирующие элементы с частотой до 37,9 МГц, внедрены в НПО «Радиоэлектроника» (г. Казань) и в НПП МЦЭИР (г. Тверь).

<u>В п. 6.1</u> представлен подход к решению задач синтеза ***генераторов ДСП класса марковских и их функций на РВС ПА «Медведь»*** с применением предложенного ОМС (см. гл. 1). На основе IP-ядер, реализующих систему НПФ над $G_{(2)}$ вида (15) согласно методу, приведенному в п. 3.2, выполнен синтез генераторов как однородных цепей Маркова, заданных ПММ вида (8) (см. п. 2.1), так и стохастической функции неоднородных ЦМ, заданных ВА $A_{ФНЦМ} = (V, S, Z, \mu(s', z/s, v))$ (п. 3.3). Генераторы ОЦМ общего вида, представленные НПФ $g(\hat{z})$ и $f(x, q)$ над $GF(2^2)$, реализуемы при использовании IP-ядер на основе ПарС и ППС (см. п. 5.2). В первом случае *обеспечивается высокая частота генерирования элементов* ОЦМ – *37,9 МГц* для $|Q| \le 2^3 \div 2^6$, $|X| \le 2^8 \div 2^9$, $|\hat{Z}| \le 2^{12}$, *примерно в 2*

раза большая, чем на современных спец. процессорах, за счет распределенного вычисления НПФ в архитектуре ПЛИС/FPGA. Из-за характеристик современных ОЗУ (полное время цикла чтения – не менее 50 нс.) вычисление функции перехода ОЦМ на спец. процессорах производится с частотой не более 20 МГц (В.П.Афанасьев, 2013).

Генераторы стохастической функции НЦМ общего вида, реализуемы на основе предложенной структурной схемы (рис. 3.3) при использовании IP-ядер, из которых $n_S/2 = \rceil \log_2 l_S [$ позволяют вычислить НПФ вида (15) от $(\eta_1 \cdot n/2)$ переменных, $n_Z/2 = \rceil \log_2 l_Z [/2$ - от $(\eta_2 \cdot n/2)$, $n_m/2 = \rceil \log_2 m [/2$ - от $((] \log_2 h [+ n_S + n_m)/2)$, а $\rceil \log_2 d [/2$ - от $((n_Z + n_m)/2)$ переменных, соответственно. Для $|Z| \le 2^{14}$, $|\hat{Z}| \le 2^6$, $|V| \le 2^3$, $|S| \le 2^6$ и $|X'|, |X''| \le 2^8$ данный генератор реализуем на 30-ти ПЛИС 4VLX200FF1513-11 в составе РВС ПА «Медведь» при использовании 59-ти IP-ядер, реализующих НПФ(7) либо на 32-х корпусах указанных ПЛИС при использовании 212-ти IP-ядер, реализующих НПФ(6). Оценки периода и частоты генерирования элементов СФ НЦМ равны: в первом случае - 30,9 нс. и 32,4 МГц, во втором случае – 26,4 нс. и 37,9 МГц.

В п. 6.2 представлены результаты по применению метода синтеза цифровых устройств для вычисления дискретной детерминированной нелинейной функции общего вида (см. п. 3.2) для задачи реализации ***устройств ВТ определенных подклассов теоретико-полиномиальных преобразований***, применяемых для анализа и фильтрации потоков *n*-разрядных двоичных чисел, на примерах ДПФ, ДПХ, а также КИХ-ф., описываемых на основе систем НПФ над полем Галуа [43].

Предложена общая структурная схема (ОбСС) для устройств ВТ, выполняющих заданные подклассы ТПП – ДПФ, ДПХ и КИХ-ф., ***на РВС ПА «Медведь»***, которая включает в себя однотипные элементы, например, ПЛИС XC4VLX200FF1513-11. ОбСС указанных устройств приведена на рис. 6.2. Определены оценки аппаратной сложности предложенной ОбСС, как на основе ЛЭ ПЛИС/FPGA, так и по количеству *D*-триггеров:

$$Q_{\text{ОСС}} = t \cdot \left(S \cdot Q(\otimes_C) + \sum_{j=0}^{u-2} \left(Q(\Sigma_{f+j}) \cdot 2^{u-2-j} \right) \right), \tag{20}$$

где $Q(\otimes_C) = f \cdot Q(\text{БФ}(n))$, $Q(\Sigma_{f+j}) = (f + j)$ (по количеству ЛЭ).

$$Q_{\text{ОСС}}^{(\text{D})} = n \cdot S + t \cdot \sum_{j=0}^{u-1} \left((f + j) \cdot 2^{u-1-j} \right). \tag{21}$$

Оценки аппаратной сложности вычислимы согласно (20) и (21) для устройств ВТ, обрабатывающих двоичные числа разрядности *n* и реализующих: 1) ДПФ для $S = N$ и $t = 2 \cdot N$; 2) ДПХ для $S = N$ и $t = N$; 3) КИХ-ф. для $S = M + 1$ и $t = 1$, где N – количество отсчетов дискретного сигнала, подвергаемого ДПФ или ДПХ, M – порядок КИХ-ф.

Оценка значения временного интервала между синхроимпульсами, общая для всех схем устройств ВТ указанного класса, составляет:

$$T_{\text{ОСС}} = \max\left(T(\otimes_C),\ \ T(\Sigma_{(f+u-2)}),\ \ T_{IOB}^{(in)},\ \ T_{IOB}^{(out)} \right) + T_D \ , \tag{22}$$

где $T(\otimes_C)$, $T(\Sigma_{(f+u-2)})$, $T_{IOB}^{(in)}$, $T_{IOB}^{(out)}$ и T_D - оценки времени задержки схемы умножения на константу, сумматора для двух $(f+u-2)$-разрядных двоичных чисел, блоков ввода-вывода, сконфигурированных на вход и выход, а также *D*-триггера, соответственно. Оценка частоты работы каждого из устройств указанного класса - $F = T_{\text{ОСС}}^{-1}$, получена на основе (22).

Устройства ВТ для КИХ-ф. реализуемы на одной ПЛИС 4VLX200FF1513-11 при $M \le 255$, $n \le 8$, а для ДПФ и ДПХ – на одной РВС ПА «Медведь» при обработке чисел разрядности $n \le 8$, при $N \le 128$, а также когда $n \le 6$, при $N \le 256$.

Для предложеных устройств ВТ, реализующих заданные подклассы теоретико-полиномиальных преобразований - ДПФ, ДПХ и КИХ-ф., оценки времени задержки функционирования снижены в 2,4 – 2,6 раз, в 1,2 – 1,3 раза и в 1,6 – 2,4 раза, соответственно, по сравнению с устройствами ВТ, реализующими указанные ТПП на основе операций над числами, представленными в СОК и в ПСС (см. табл. 6.2), *за счет организации распределенных вычислений при использовании однотипных IP-ядер*. В результате, увеличено быстродействие устройств ВТ указанного класса при обработке векторов размерности n, $n \le 8$.

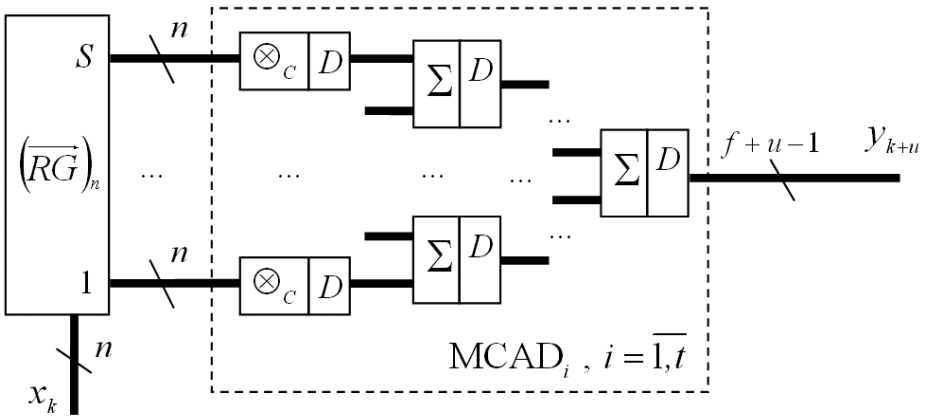

Рис. 6.2. Общая структурная схема устройств ВТ, реализующих ДПФ, ДПХ и КИХ-ф.

Таблица 6.2. Оценки сложности устройств ВТ для ДПФ, ДПХ и КИХ-ф.

Тип устройства ВТ	ПЛИС EP2C5T144C6 (одни корпус), в СОК, *t*з	Спец. процессоры в ПСС		РВС ПА «Медведь», система НПФ над $GF(2^2)$ (п. 3.2)	
		TS001, *t*з (мкс.)	AM1808, *t*з (мкс.)	*t*з (мкс.) / число корпусов	**Выигрыш по *t*з (раз)**
ДПФ, *N*=128	~ 19 мкс.	--	--	~ 1,35 / 22	**~ 14**
ДПФ, *N*=256	~ 43 мкс.	~ 7,3	~ 6,8	~ 2,86 / 47	**~ 2,4 – 2,6**
ДПХ, *N*=128	--	--	--	~ 1,35 / 11	--
ДПХ, *N*=256	--	~ 3,7	~ 3,4	~ 2,86 / 24	**~ 1,2– 1,3**
КИХ-ф., *M*=255	--	~ 6,9	~ 4,5	~ 2,86 / (1/11)	**~ 1,6 – 2,4**

В п. 6.3 решена задача ***анализа степени соответствия архитектуре ПЛИС/ FPGA схем функциональных модулей операции умножения элементов полей вида*** $G_{(n)}$ ***и*** $G_{(k)}^{(r)}$ - ОУ/$G_{(n)}$ и ОУ/$G_{(k)}^{(r)}$, определенных в пп. 4.1 и 4.2, соответственно.В качестве примера на рис. 6.3.1 приведены оценки общего и приведенного (критерий $t_{з\,ЭС}$, п. 5.1) времени задержки функционирования для модулей, реализующих ОУ/$G_{(n)}$ на ПЛИС серии EP1S10B672C6 для двоичных векторов размерности 8, 16, 32 и 64. При отображении данных модулей в базис ПЛИС выполнено сопоставление их теоретических оценок сложности с оценками реальных затрат программируемых элементов ПЛИС: ЛЭ с программируемыми ГФ и *D*-триггерами, а также МС, согласно критериям, определенным в п. 5.1 (для указанных функциональных модулей (ФМ) значения критериев $K_{РТ}$, K_t и $K_з$ (см. п. 5.1) приведены на рис. 6.3.2).

Критерий K_t позволяет оценить возможность снижения *T* для ФМ за счет реконфигурирования МС ПЛИС, а критерии $K_{РТ}$ и $K_з$ – оценить возможность более эффективного задействования ЛЭ и ГФ ПЛИС. Степень соответствия ФМ ОУ/$G_{(n)}$ и ОУ/$G_{(k)}^{(r)}$, архитектуре ПЛИС семейств XC4000E, Spartan и XC5200 (Xilinx Corp.) и EP1S10B672C6 (Altera Corp.), в частности, при условии, что $r \cdot k = n$, определена по методике и согласно критериям, описанным в п. 5.1 [1, 9, 10, 25, 35].

В п. 6.4. решена задача ***синтеза схем функциональных модулей операции вычисления остатка от деления по заданному модулю***, определенной на основе конвейерных вычислений (п. 4.3), ***для потока чисел на ПЛИС/FPGA*** [14, 19]. Представлена реализация на ПЛИС/FPGA Stratix II GX (Altera Corp.) типа EP2SGX30CF780C3 и Virtex 4 (Xilinx Corp.) типа 4VLX160FF1148-11 генератора равномерно распределенной дискретной случайной величины Смита, заданного при использовании первого варианта схемы операции вычисления остатка по заданному простому модулю (рис. 4.3) [12, 40].

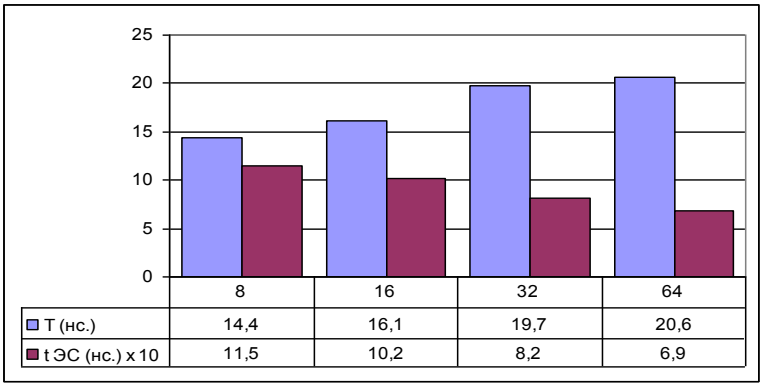

Рис. 6.3.1. Общее и приведенное время задержки функционирования ФМ ОУ/$G_{(n)}$ на ПЛИС EP1S10B672C6, n = 8, 16, 32 и 64

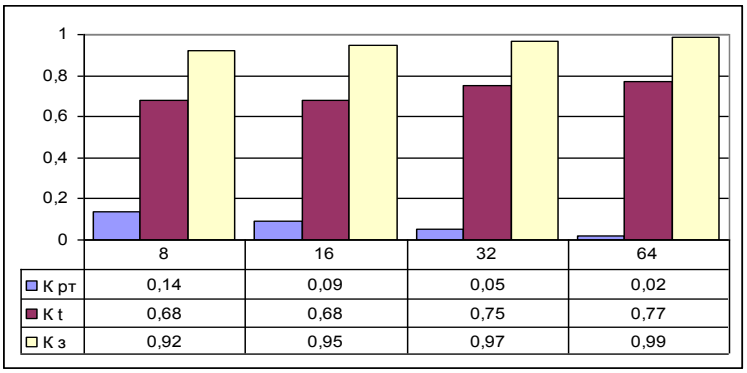

Рис. 6.3.2. Доля ресурсов взаимосвязи в ФМ ОУ/$G_{(n)}$ на ПЛИС EP1S10B672C6, n = 8, 16, 32 и 64

Данные семейства ПЛИС сопоставимы по таким характеристикам, как оценка временной сложности, количество конфигурируемых логических ресурсов и наличию специализированных вычислителей (ядер XtremeDSP). Различие данных семейств - в структуре их логических ресурсов. Сопоставление оценок времени задержки функционирования (T) ФМ, реализующего операцию вычисления остатка от деления по заданному модулю, на ПЛИС 4VLX160FF1148-12 для потока чисел разрядности 8, 16 и 24, приведено на рис. 6.4. За счет выбора оптимальной конфигурации программируемых элементов ПЛИС, параметр T для ФМ, реализованных без использования ядер XtremeDSP, определяется только задержкой блоков ввода-вывода, частота функционирования которых для ПЛИС данного типа – примерно 283 МГц). Если ФМ операции вычисления остатка от деления по заданному модулю реализуемы на ПЛИС без использования ядер XtremeDSP, то ГФ и логические элементы задействованы не более чем на 50 и 75%, соответственно. Для ФМ операции вычисления остатка по заданному модулю характерна большая доля логических ресурсов, задействованных для пе-

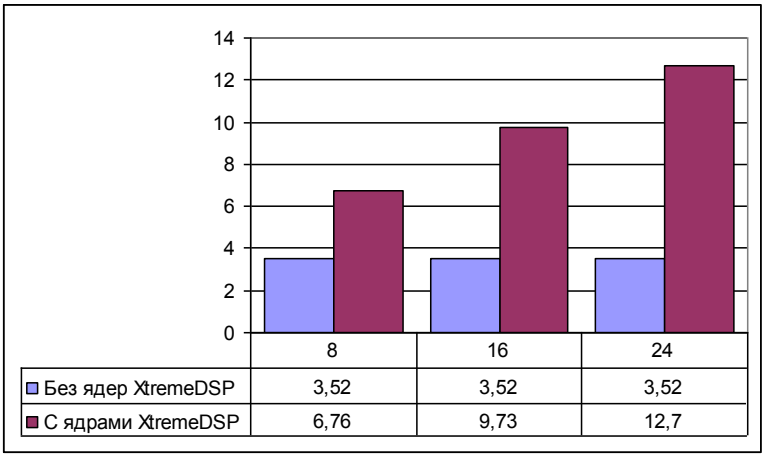

Рис. 6.4. Время задержки функционирования (нс.) модуля, реализующего ОВО, на ПЛИС 4VLX160FF1148-12, n = 8, 16 и 24

редачи сигналов внутри ПЛИС, а не для синтеза логических функций. Что касается ФМ ОВО на ПЛИС Virtex 4 LX с использованием ядер XtremeDSP, то ГФ задействованы на 80-100%, а ЛЭ – на 50-56%, соответственно [14]. Степень соответствия ФМ ОВО (п. 4.3), архитектуре ПЛИС/FPGA определена по методике и согласно предложенным критериям (п. 5.1) [1, 9, 10, 25, 35].

В результате, при распределенной реализации ФМ, определенных в пп. 4.1 – 4.3, увеличение быстродействия достигается за счет снижения степени задействования ГФ, применяемых для синтеза логических функций.

В п. 6.5 предложены ***схемы устройств ВТ для отображения и варьирования состояния дискретной модели*** **КМС(*N*)** для произвольного числа базисных состояний N [8], а также **ее частных случаев**: КМС(2) – квантового бита (кубита) [6, 32] и КМС(4) – простого квантового регистра [7]. Данное устройство представимо при использовании однотипных ФМ операции умножения (ОУ) элементов полей $GF(2^n)$ и $GF((2^k)^r)$, $k \cdot r = n$, (см. пп. 4.1 и 4.2), функционирующих параллельно, что обосновано соответствующими теоремами [8]. Состояние КМС(N) описывается как

$$|\psi\rangle = (r_0 e^{i\phi_0} \quad ... \quad r_{N-1} e^{i\phi_{N-1}})^T, \ \sum_{j=0}^{N-1} r_j^2 = 1. \qquad (23)$$

Дискретная модель (ДМ) КМС(N) описывается при использовании графовой модели - двоичного (бинарного) дерева T. Число его вершин, являющихся листьями, равно числу базисных состояний КМС(N), а число вершин, которые не являются листьями, $(N-1)$, определяет количество параметров, описывающих амплитудные и фазовые составляющие данной модели - $2(N-1)$ [8]. Варьирование состояния ДМ КМС(N), описываемое системой (23), задано квантовым вентилем, унитарной матрицей размерности $N \times N$, вида $G = G_\phi G_A$, где матрицы G_ϕ и G_A размерности $N \times N$ определяют варьирование фазовой и амплитудной составляющей ДМ КМС(N), соответственно [8]. *Верхняя оценка аппаратной сложности устройства ВТ для расчета предложенной ДМ отображения и варьирования КМС*(N)*, а также ее частных случаев* $(N = 2, 4)$, *определена как для* $2(N-1)$ *функциональных модулей ОУ/*$GF(2^n)$ *или ОУ/*$GF((2^k)^r)$, $k \cdot r = n$ (пп. 4.1 и 4.2); *нижняя оценка временной сложности для указанного устройства ВТ определена как для одного функционального модуля ОУ/*$GF(2^n)$ *или ОУ/*$GF((2^k)^r)$ [6 - 8, 32].

В заключении сформулированы основные результаты работы.

ЗАКЛЮЧЕНИЕ

Главным результатом данной работы является достижение ее цели - разработка теоретических основ общего метода структурного, алгоритмического и функционального синтеза генераторов дискретных стохастических процессов класса марковских и их функций и устройств вычислительной техники для выполнения теоретико-полиномиальных преобразований, повышающего эффективность реализации данных генераторов и устройств на ПЛИС/FPGA за счет применения нелинейных полиномиальных параллельных преобразований над потоками чисел в конечных полях. Достижению цели способствовало получение следующих основных научных результатов.

1. Предложен общий метод структурного синтеза классов устройств вычислительной техники и разработаны теоретические положения его реализации на основе предложенного принципа суперпозиции нелинейных полиномиальных функций (НПФ) над полем Галуа; принцип суперпозиции определяется рядом теорем и позволяет отобразить на распределенных вычислительных системах с программируемой архитектурой, элементами которой являются ПЛИС/FPGA
   - разработанные структурные схемы генераторов ДСП класса марковских и их функций - однородных ЦМ, определенных на основе введенного понятия «полиномиальная модель цепи Маркова», их детерминированных и стохастических функций, α-сложных ЦМ, неоднородных ЦМ и их функций, детерминированных и сто-

хастических, дискретных случайных величин с заданным законом распределения; реализация применяемого принципа суперпозиции основана на предложенном методе представления стохастических матриц нелинейными полиномиальными функциями от многих переменных над полем Галуа, что позволяет уменьшить время генерирования элементов однородных ЦМ примерно в 2,0 раза, по сравнению с минимальным временем генерирования указанных процессов на основе известных методов (табличный, на основе функций алгебры логики) при использовании современных спец. процессоров;

- разработанную общую структурную схему устройств ВТ в архитектуре ПЛИС/ FPGA, выполняющих теоретико-полиномиальные преобразования на примере ДПФ, ДПХ и цифровых фильтров с импульсной характеристикой конечной длительности (КИХ-ф.), что позволяет получить выигрыш по быстродействию при реализации указанных устройств на распределенной вычислительной системе с программируемой архитектурой «Медведь»: для ДПФ и ДПХ (при $n \le 8$ и $N \le 256$) – примерно в 1,2 – 2,6 раз, а для КИХ-ф. порядка 255 (при $n \le 8$) – примерно в 1,6 – 2,4 раза, за счет организации распределенного вычисления дискретной детерминированной нелинейной функции на основе системы из l НПФ, определенных над $GF(2^k)$, $n = k \cdot l$;
- разработанные структурные схемы устройств ВТ, позволяющих моделировать отображение и варьирование состояния квантово-механической системы общего вида с N базисными состояниями и ее частных случаев для $N = 2$ и $N = 4$ при использовании предложенной дискретной модели, за счет параллельного выполнения $2(N-1)$ операций умножения над полем $GF(2^n)$ или $GF((2^k)^r)$, $n = k \cdot r$.

2. Разработаны теоретические основы для предложенного метода синтеза ЦВУ ДДНФ от m n-разрядных переменных на основе распределенных вычислений при использовании системы из l НПФ от $l \cdot m$ переменных, определенных над $GF(2^k)$, $n = k \cdot l$, а также для схем вычисления НПФ от m переменных над $GF(2^n)$, альтернативных по оценкам сложности: параллельной, систолической, последовательностной и параллельно-последовательностной. Метод позволяет уменьшить оценки временной сложности для ЦВУ ДДНФ, синтезируемых на основе системы НПФ над $GF(2^k)$, $k = 2$, примерно в $1 + \left(n \cdot \log_2 n + (\log_2 m)\log_2 n\right)/(m \cdot n)$ раз по сравнению с ЦВУ указанной ДДНФ на основе параллельной схемы ($n \le 6, m \le 7$) и примерно в $\left(2^n \cdot \log_2 m\right)/n$ раз – по сравнению с ЦВУ ДДНФ, определенным при использовании систолической схемы ($n, m \le 7$).
3. Разработаны методы синтеза функциональных модулей на структурном и алгоритмическом уровнях при использовании распределенных вычислений для операций в конечных полях. Указанные ФМ синтезированы на основе предложенных
   - схем ОУ n-разрядных элементов расширений поля Галуа вида $GF((2^k)^r)$, при использовании операций над элементами $GF(2^k)$, $n = k \cdot r$, что позволяет уменьшить оценки временной сложности примерно в $1 + \log_2(n/k)/(\log_2 2k)$ раз, $k \le 4$, $n \le 64$, по сравнению со схемой ОУ элементов $GF(2^n)$, на основе операций над полем $GF(2)$;
   - двух альтернативных схем операции вычисления остатка по заданному простому n-разрядному модулю, $n \le 24$, что позволяет уменьшить оценки временной сложности выполнения ОВО примерно в w раз по сравнению с существующими методами вычисления остатка по заданному простому модулю, где w – количество ступеней конвейера в предложенных схемах ОВО.

Работоспособность разработанных ФМ, определяемых как на основе схем операции умножения элементов $GF(2^n)$ и $GF((2^k)^r)$, так и схем ОВО, и синтезированных на ПЛИС/FPGA, подтверждена моделированием функциональных схем указанных модулей при использовании специализированных САПР ISE 13.4 (Xilinx Corp.) и Quartus II v. 9.0 (Altera Corp.).

4. Предложены методики многопараметрического анализа, позволяющие:
   - определять подмножество из k типичных представителей семейства генераторов ДСП класса однородных ЦМ, заданных на основе Q эргодических стохастических матриц, описывающих указанные генераторы, с целью уменьшения в Q/k раз объема массивов исходных данных большой размерности, определяющих реализацию генераторов однородных ЦМ на ПЛИС/FPGA, на основе разработанного множества признаков, а также
   - идентифицировать принадлежность дискретных простых конечных однородных ЦМ конечной длины N к одному из априори заданных подклассов с определенной доверительной вероятностью (0,95) на основе разработанного множества признаков, для N в 1,4 – 64 раза меньшей, чем на основе статистической обработки биграмм.
5. Разработана методика оценки степени соответствия цифровых вычислительных устройств и функциональных модулей архитектуре ПЛИС/FPGA, позволяющая выбрать из множества реализаций указанных устройств или модулей наиболее приближенную к оптимальной по предложенным критериям. Высокая степень соответствия данных устройств и модулей архитектуре ПЛИС/FPGA достигается путем организации распределенного вычисления как значений нелинейной полиномиальных функций от многих переменных, определенных над полем $GF(2^k)$, так и результатов операций, выполняемых в конечных полях: ОУ элементов $GF(2^n)$, ОУ элементов $GF((2^k)^r)$, $n = k \cdot r$, и вычисления остатка по заданному модулю.
6. Разработаны на основе САПР ISE 13.4 (Xilinx Corp.) и Quartus II v. 9.0 (Altera Corp.) и внедрены устройства ВТ для теоретико-полиномиальных преобразований и генераторы дискретных стохастических процессов из класса стохастических функций неоднородных ЦМ (СФ НЦМ), реализуемые на распределенной вычислительной системе с программируемой архитектурой (РВС ПА) «Медведь» (НИИ МВС ЮжнФУ , г.Таганрог) при использовании однотипных IP-ядер, синтезируемых на ПЛИС/FPGA. Основным объектом внедрения являются устройства ВТ ДПФ и КИХ-ф. (НПП «Измерительные технологии», г. Саров) и генератор СФ НЦМ, представленных двоичными числами (НПО «Радиоэлектроника», г. Казань и в НПП МЦЭИР, г. Тверь). За счет организации распараллеливания процесса вычислений и потоковой обработки данных в архитектуре ПЛИС/FPGA время вычисления на указанной РВС ПА: 1) Фурье-образа для устройства ВТ ДПФ уменьшено примерно в 2,4 раза по сравнению с устройсвами ВТ для быстрых ДПФ, реализованных на спец. процессорах AM1808 (Texas Instrument, Inc.); 2) значений, снимаемых с выхода устройства ВТ КИХ-ф., уменьшено примерно в 1,6 раз по сравнению с аналогичными устройствами, реализованными на AM1808. Показана принципиальная возможность синтеза высокопроизводительных генераторов (частота – до 37,9 МГц) однородных ЦМ и СФ НЦМ на основе однотипных IP-ядер, определенных на основе операций в конечном поле и синтезируемых на ПЛИС/FPGA, включенных в состав РВС ПА «Медведь». Теоретические основы и методы анализа и синтеза для генераторов ДСП класса марковских и их функций и для устройств ВТ ТПП на основе НПФ над конечным полем использованы при выполнении грантов РФФИ - № 99-01-00163, № 03-01-00769 и № 09-01-97004-Р-Поволжье 01, в проекте № 015-04-01-52 программы «Университеты России» и внедрены в учебный процесс КНИТУ-КАИ и в ВА ВКО. По результатам работы в ФГБУ ФИПС получены три патента РФ: два – на изобретение, один – на полезную модель, и зарегистрирована одна программа для ЭВМ.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в ведущих рецензируемых научных изданиях.

1. Захаров, В.М. Аппаратная реализация умножения элементов поля Галуа на программируемых микросхемах архитектуры FPGA/ В.М.Захаров, Ш.Р. Нурутдинов, С.В.Шалагин// Вестник КГТУ им.А.Н.Туполева. – 2001.- № 1.- С.36 – 47. (л. вк. 30%).

2. Захаров, В.М. Полиномиальное представление цепей Маркова над полем Галуа/ В.М.Захаров, Ш.Р.Нурутдинов, С.В.Шалагин// Вестник КГТУ им. А.Н.Туполева. – 2001. - № 3. – С. 27-31. (л. вк. 30%).
3. Захаров, В.М. К задаче дискриминантного анализа автоматных марковских моделей/ В.М. Захаров, Н.Н. Нурмеев, Ф.И. Салимов и др. // Вестник КГТУ им.А.Н. Туполева. – 2001. – № 3. – С. 37–39. (л. вк. 20%).
4. Захаров, В.М. Полиномиальное представление конечноавтоматных случайных последовательностей над полем Галуа/ В.М. Захаров, Ш.Р. Нурутдинов, С.Ю. Соколов и др.// Вестник КГТУ им. А.Н. Туполева. – 2003. – № 2. – С.24–28. (л. вк. 25%).
5. Шалагин, С.В. Экспериментальное исследование методики синтеза комбинационных схем на программируемых микросхемах класса FPGA / С.В. Шалагин // Микроэлектроника. – 2004. – Т. 33; № 1. – С. 56–67; Shalagin, S.V. Computer Evaluation of a Method for Combinational-Circuit Synthesis in FPGAs / S.V. Shalagin // Russian Microelectronics. – 2004. – Vol. 33; № 1. – P. 46–54.
6. Шалагин, С.В. Дискретная модель квантового вычислителя/ С.В.Шалагин// Вестник КГТУ им. А.Н.Туполева. – 2005. - № 1. - С. 35 – 39.
7. Шалагин, С.В. Моделирование квантового регистра, включающего два квантовых бита/ С.В.Шалагин // Вестник КГТУ им. А.Н. Туполева. – 2006. - № 1. - С. 35 - 38.
8. Шалагин, С.В. Дискретная модель квантовой системы обработки информации/ С.В.Шалагин// Вестник КГТУ им. А.Н. Туполева. – 2007. - № 4. - С.22-27.
9. Шалагин, С.В. Умножение элементов расширений полей Галуа в базисе ПЛИС/FPGA/ С.В.Шалагин//Информационные технологии. – 2007. -№ 12.-С.22-27.
10. Кайбушев, Ф.Х. Реализация схем умножения элементов поля Галуа в базисе ПЛИС класса FPGA семейства Stratix/ Ф.Х.Кайбушев, С.В.Шалагин // Информационные технологии. – 2008. - № 11. - С. 51 – 55 (л. вк. 60%).
11. Шалагин, С.В. О представлении нелинейных полиномов над конечным полем распределенной вычислительной системой/ С.В.Шалагин// Нелинейный мир.– 2009.- № 5. - С.376–379.
12. Зелинский, Р.В. Реализация на ПЛИС генераторов псевдослучайных последовательностей и средств их CRC-контроля/ Р.В.Зелинский, Ф.Х.Кайбушев, С.В.Шалагин// Вестник КГТУ им. А.Н.Туполева. – 2009. - № 2. - С. 57 – 61 (л. вк. 40%).
13. Нурутдинова, А.Р. Методика идентификации автоматных марковских моделей на основе порождаемых ими последовательностей/ А.Р.Нурутдинова, С.В.Шалагин// Вестник КГТУ им. А.Н.Туполева. – 2010. - № 1. - С. 94 – 99 (л. вк. 60%).
14. Захаров, В.М. Алгоритм вычисления остатка по модулю и оценки его сложности/ В.М.Захаров, Е.Л.Столов, С.В.Шалагин// Информационные технологии. – 2010. – № 11. – С. 32 – 36. (л. вк. 30%).
15. Нурутдинова, А.Р. Многопараметрическая классификация автоматных марковских моделей на основе генерируемых ими последовательностей состояний/ А.Р. Нурутдинова, С.В.Шалагин // Прикладная дискретная математика.– 2010.- № 4. – С. 41–54 (л. вк. 60%).
16. Шалагин, С.В. Реализация устройств вычислительной техники на многопроцессорных системах с программируемой архитектурой/ С.В.Шалагин// Вестник МарГТУ. – 2011. – № 1 (11). – С. 38 – 46.
17. Барковский, С.С. Многопараметрический анализ и ранжирование предложений НИОКР отраслевой программы/ С.С.Барковский, А.Р.Нурутдинова, С.В.Шалагин// Вестник КГТУ им. А.Н.Туполева. – 2011. - № 2. - С. 115 – 122 (л. вк. 40%).
18. Захаров, В.М. Вычисление нелинейных полиномиальных функций на многопроцессорной системе с программируемой архитектурой/В.М.Захаров, С.В.Шалагин// Информационные технологии. - 2012. - №5. - С. 6 – 11. (л. вк. 50%).

Патенты на изобретение.

19. Пат. 2421781 РФ МПК[8] G06F 7/72, H03M 7/18. Устройство для формирования остатка по заданному модулю/ В.М.Захаров, Е.Л.Столов, С.В.Шалагин; заявитель и патентообладатель ГОУ ВПО Казан. гос. техн. ун-т. - № 2009138613/08; заявл. 19.10.2009; опубл. 20.06.2011, Бюл. № 17. - 12 с.: ил. (л. вк. 30%).
20. Пат. 2446444 РФ МПК G06F 7/58 (2006.01). Генератор псевдослучайных последовательностей / В.М.Захаров, Р.В.Зелинский, С.В.Шалагин; заявитель и патентообладатель

ГОУ ВПО Казан. гос. техн. ун-т. - № 2010146202/08; заявл. 12.11.2010; опубл. 27.03.2012, Бюл. № 9. – 14 с.: ил. (л. вк. 30%).

Монография.

21. Шалагин, С.В. Представимость дискретных детерминированных нелинейных функций на основе многочленов над полем Галуа в базисе ПЛИС класса FPGA/ С.В.Шалагин. – Казань: изд-во КГТУ им. А.Н.Туполева, 2010. - 184 с.

Публикации в прочих научных изданиях.

22. Захаров, В.М. Классификация стохастических эргодических матриц методами кластерного и дискриминантного анализа / В.М. Захаров, Н.Н. Нурмеев, Ф.И. Салимов и др.// Исследования по информатике. – 2000. – Вып. 2. – С. 91–106. (л. вк. 25%).
23. Захаров, В.М. Синтез автономных вероятностных автоматов на основе полей Галуа/ В.М.Захаров, Ш.Р.Нурутдинов, С.В.Шалагин// Исследования по информатике. – 2000. – Вып. 2. - С. 107 – 116 (л. вк. 30%).
24. Захаров, В.М. Полиномиальное представление автоматных моделей марковских функций над полем Галуа / В.М. Захаров, Ш.Р. Нурутдинов, С.Ю. Соколов и др.// Исследования по информатике. – 2003. – Вып. 5. – С. 45–56. (л. вк. 25%).
25. Саси, С.А. Оценки сложности архитектур умножителей в базисе ПЛИС/FPGA/ С.А.Саси, С.В.Шалагин, Л.М.Шарнин // Исследования по информатике. – Казань, 2005. – Вып. 9. – С. 71 – 80 (л. вк. 40%).
26. Шалагин, С.В. Реализация умножения элементов расширений поля Галуа в базисе ПЛИС/ FPGA/ С.В. Шалагин// Методы моделирования: сб. тр. Казанского научного семинара. – Казань: Изд-во КГТУ им. А.Н. Туполева, 2007. – Вып. 3. – С. 297–314.
27. Шалагин, С.В. Представление нелинейных полиномиальных функций над полем Галуа в базисе ПЛИС/FPGA / С.В. Шалагин. – Saarbrücken Germany: LAP Lambert Academic Publishing GmbH & Co. KG, 2012. – 188 с.
28. Пат. на пол. модель 131886 РФ МПК G06F 17/14 (2006.01). Устройство для вычисления дискретных полиномиальных преобразований / В.М.Захаров, С.В.Шалагин; заявитель и патентообладатель КНИТУ-КАИ - № 2012148954/08 заявл. 16.11.2012; опубл. 27.08.2013, Бюл. № 24. – 3 с.: ил. (л. вк. 50%)

Публикации в сборниках трудов и материалов конференций и семинаров.

29. Захаров, В.М. Построение модели умножителя в полях Галуа/ В.М. Захаров, Ш.Р. Нурутдинов, С.В. Шалагин // Дискретная математика и ее приложения: материалы 7-го Междунар. семинара 29 янв.–2 февр. 2001. – В 3 ч. Ч. I. – М.: Изд-во центра прикладных исследований при механико-матем. факультете МГУ, 2001. – С. 62–65. (л. вк. 30%).
30. Захаров, В.М. Анализ стохастических матриц методами многомерной классификации / В.М. Захаров, Н.Н. Нурмеев, Ф.И. Салимов и др. // Дискретная математика и ее приложения: материалы 7-го Междунар. семинара 29 янв.–2 февр. 2001. – В 3 ч. Ч. II. – М.: МГУ, 2001. – С. 156–159. (л. вк. 25%).
31. Нурутдинов, Ш.Р. Синтез автоматных моделей цепей Маркова и их функций в конечных полях / Ш.Р. Нурутдинов, С.Ю. Соколов, С.В. Шалагин // Новые информационные технологии и системы: сб. тр. 5-й Междунар. науч.-техн. конф. 14–15 нояб. 2002. – Пенза: Изд-во Пенз. гос. ун-та, 2002. – С. 211– 213. (л. вк. 30%).
32. Шалагин, С.В. Дискретная модель квантового бита / С.В. Шалагин /// Методы и средства обработки информации: тр. 1-й Всерос. науч. конф. 1–3 окт. 2003. – М.: МГУ, 2003. – С. 572– 577.
33. Шалагин, С.В. Синтез генераторов дискретной случайной величины над полем GF(2^n)/ С.В. Шалагин // Сеточные методы для краевых задач и приложения: материалы 5-го Всерос. семинара 17–21 сент. 2004. – Казань: Изд-во КГУ, 2004. – С. 236–240.
34. Захаров, В.М. Метод моделирования и преобразования функций цепей Маркова в полях Галуа и его реализация в базисе ПЛИС/ В.М. Захаров, Ш.Р. Нурутдинов, С.В. Шалагин // Методы и средства обработки информации: тез. докл. 2-й Всерос. науч. конф. 5-7 окт. 2005.– М.: МГУ, 2005. – С. 256–262. (л. вк. 30%).
35. Захаров, В.М. Реализация полиномиальных моделей над полем *GF*(2^n) неоднородных цепей Маркова и их функций в базисе ПЛИС/FPGA/ В.М. Захаров, Ш.Р. Нурутдинов, С.В. Шалагин // Инфокоммуникационные технологии глобального информационного

общества: тез. докл. 4-й ежегодной Междунар. науч.-практ. конф. 5-8 сент. 2006. – Казань: Центр инновационных технологий, 2006. – С. 62–66. (л. вк. 40%).

36. Шалагин, С.В. Операция умножения элементов полей Галуа вида $GF((2^k)^l)$ / С.В. Шалагин // Дискретная математика и ее приложения: материалы 9-го Междунар. науч. семинара 18–22 июня 2007. – М.: Изд-во механико-матем. ф-та МГУ, 2007. – С. 136–139.
37. Шалагин, С.В. Многопараметрическая классификация устройств на базе марковских моделей / С.В. Шалагин // Инфокоммуникационные технологии глобального информационного общества: сб. тр. 5-й Междунар. науч.-практ. конф. 5–6 сент. 2007. – Казань: Изд-во «Фолиантъ», 2007. – С. 62–65.
38. Шалагин, С.В. Полиномиальные модели генераторов дискретных случайных величин / С.В. Шалагин // Инфокоммуникационные технологии Глобального информационного общества: сб. тр. 6-й ежегодной Междунар. науч.-практ. конф. 4–5 сент. 2008. – Казань: Центр Оперативной Печати, 2008. – С. 159–171.
39. Захаров, В.М. Параллельные марковские модели над полем $GF(2^n)$ / В.М. Захаров, С.В. Шалагин // Высокопроизводительные параллельные вычисления на кластерных системах: тез. докл. 8-й Междунар. конф. 17 – 21 нояб. 2008. – Казань: Изд-во КГТУ им. А.Н. Туполева, 2008. – С. 155–160. (л. вк. 40%).
40. Шалагин, С.В. Оценки сложности конгруэнтных псевдослучайных последовательностей по простому модулю на ПЛИС/FPGA/ С.В. Шалагин, Ф.Х. Кайбушев, Р.В. Зелинский // Методы и средства обработки информации (МСО-2009): тр. 3-й Всерос. науч. конф. 6–8 окт. 2009. – М.: Издат. отд. ф-та ВМиК МГУ; МАКС Пресс, 2009. – С. 173–179. (л. вк. 40%).
41. Шалагин, С.В. Представимость марковских моделей системой полиномов над полем Галуа вида $GF(2)$ / С.В.Шалагин // Методы и средства обработки информации: сб. тр. 3-й Всерос. науч. конф. 6–8 окт. 2009. – М.: МГУ, 2009. – С. 167–172.
42. Шалагин, С.В. Представимость неоднородных цепей Маркова и их стохастических функций полиномами от нескольких переменных над полем Галуа / С.В. Шалагин// Инфокоммуникационные технологии Глобального информационного общества: сб. тр. 7-й ежегодной Междунар. науч.-практ. конф. 10–11 сент. 2009. – Казань: Центр оперативной печати, 2009. – С. 134–139.
43. Шалагин, С.В. Обобщенная распределенная полиномиальная модель нелинейных преобразований над потоками чисел в конечных полях/ С.В. Шалагин// Информационные технологии в системе экономической безопасности России и ее регионов: сб. тр. III Всерос. науч. конф. 19-22 окт. 2010. – Казань: ИГМА-пресс, 2010. – С. 186–192.
44. Шалагин, С.В. Реализация многоканальных корреляционных измерителей на многопроцессорной вычислительной системе с программируемой архитектурой/ С.В. Шалагин, Ю.К. Евдокимов// Проблемы техники и технологий телекоммуникаций ПТиТТ-2011: материалы XII Междунар. науч.-техн. конф. Оптические технологии в телекоммуникациях ОТТ-2011: материалы IX Междунар. науч.-техн. конф. 21–24 ноября 2011. – Казань: Изд-во Казан. гос. техн. ун-та. 2011. – С. 163–164. (л. вк. 50%).
45. Песошин, В.А. Аппаратно-программные системы статистического моделирования и защиты информации / В.А. Песошин, В.М. Захаров, В.М. Кузнецов и др. // Проблемы и перспективы развития информационных технологий: материалы докл. Всерос. науч.-техн. конф. 10 февр. 2012. – Казань: Изд-во Казан. гос. техн. ун-та, 2012. – С. 8–21. (л. вк. 20%).
46. Шалагин, С.В. Цифровые вычислительные устройства полиномиальной функции на основе однотипных операций над полем Галуа/ С.В. Шалагин // Проблемы и перспективы развития информационных технологий: материалы Всерос. науч.-техн. конф. 10 февр. 2012. – Казань: Изд-во Казан. гос. техн. ун-та, 2012. – С. 63–73.