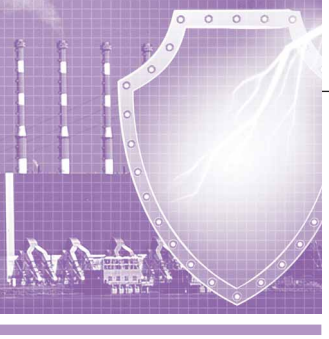

Применение специализированных вычислителей на основе ПЛИС для решения задач информационной безопасности

Артём Коновальчик

В статье поднимаются вопросы информационной безопасности в современном мире. Рассмотрены и проанализированы зарубежные решения на ПЛИС для построения суперЭВМ. Приведено описание отечественного спецвычислителя БВР-01 для применения в составе гибридных кластерных систем.

Актуальность использования специализированных вычислителей на основе ПЛИС

В настоящее время существует несколько подходов к построению вычислителей для суперкомпьютеров. Выделим два из них: первый – традиционный, то есть тот, который применяется при проектировании суперЭВМ типа представленных в TOP500 [1]; второй – предполагающий построение специализированных вычислителей на базе ПЛИС. Выбор подхода, а следовательно и архитектуры, осуществляется исходя из задач, которые необходимо решать. Традиционная модель по понятным причинам ориентирована на широкий класс задач и подразумевает использование большим количеством пользователей. Отсюда и вытекают стандартные требования к построению соответствующих высокопроизводительных систем, начиная от универсальных процессоров архитектуры x86 и заканчивая всем привычными средами программирования, в которых создаётся программа.

Нас же интересуют задачи специального класса: проблемы защиты информации, криптография, цифровая обработка сигналов, математическое моделирование, задачи с массовым параллелизмом и т.д. При определении путей решения подобных задач всегда сказывается специфика требований заказчика к вычислительной системе. Зачастую надо удовлетворить такие требования, как:

- максимально возможная производительность;
- достаточная универсальность;
- приемлемое соотношение цена/производительность;
- относительно низкое энергопотребление;
- удобство эксплуатации;
- «дружественность» системы, с точки зрения программирования задач.

Это ключевые, но далеко не все требования, которые выдвигаются заказчиком, и выступать они могут в различных комбинациях и с разными приоритетами. Кроме того, опыт построения таких систем показывает, что нередко требования противоречат друг другу. Взять хотя бы пару «производительность – универсальность». При формулировании технических требований выбирается несколько задач, на которых в итоге отлаживается, тестируется и сдаётся система. Конечно, эти задачи относятся к тому классу, для которого создаётся высокопроизводительная система, но далеко не всегда они могут выявить весь спектр проблем, с которыми столкнутся и спецвычислитель, и сам заказчик.

Предлагаю глубже окунуться в предметную область задач по защите информации и постараться ответить для себя на вопросы, насколько актуальна эта проблематика и почему здесь необходимы нетрадиционные подходы к построению спецвычислителей.

Современное общество невозможно представить без информационных и коммуникационных технологий, они присутствуют во всех сферах человеческой деятельности. Повсеместное их внедрение, с одной стороны, заметно помогает в решении многих рабочих и повседневных задач, а с другой – таит в себе множество угроз. Поэтому внедрение новых информационных технологий в системы управления и связи сопровождается разработкой и широким распространением новых способов обеспечения безопасности передачи информации и защиты данных.

Анализ развития средств защиты данных в информационных сетях показывает, что в настоящее время наблюдаются тенденции к резкому расширению использования криптографических средств в информационных инфраструктурах многих государств. Современное состояние и тенденции в развитии средств защиты (закрытия) информации неразрывно связаны с состоянием и тенденциями развития самих систем передачи информации и носят пе-

реходный характер, соответствующий сочетанию, с одной стороны, новых революционных технологий коммуникации, например связи компьютерной, мобильной, беспроводной и т.д., а с другой – эволюционного развития национальных, региональных и глобальных систем связи на базе существующей инфраструктуры. Следствием этого стало формирование двух основных направлений, по которым в последние годы развиваются криптографические средства обеспечения безопасной (закрытой) передачи информации:

- совершенствование традиционных систем шифрования, используемых в действующих каналах и сетях связи, ориентированных на использование, в первую очередь, существующей инфраструктуры, начиная от национальных систем КВ-связи и заканчивая международными и коммерческими спутниковыми системами связи;
- внедрение принципиально новых средств закрытия информации, связанное с качественной модернизацией существующих и развитием новейших систем связи и информационных технологий (для этого направления характерно бурное развитие волоконно-оптических технологий и использование глобальных компьютерных сетей в качестве коммуникационных средств).

Одной из основных тенденций развития современных систем передачи информации продолжает оставаться увеличение удельного веса закрытых передач при одновременном росте сложности используемых криптографических и технологических методов защиты данных. Учитывая нарастающее противоборство государств в глобальном информационном пространстве, в настоящее время и в ближайшей перспективе для большей части правительственных, военных и коммерческих систем связи будет характерна устойчивая тенденция роста криптографической стойкости и сложности современных и перспективных шифраторов. При защите информации в вычислительных системах широко используются средства защиты, реализуемые программно в самих вычислительных системах. Именно для таких приложений наиболее важно быстродействие программных реализаций криптографических средств. При этом само понятие быстродействия (производительности) не сводится к абсолютной скорости работы криптографических средств, поскольку она непосредственно зависит от быстродействия вычислительной системы.

Область применения непосредственно влияет на выбор принципов синтеза криптографических алгоритмов и выбор архитектурных решений для высокопроизводительных систем, осуществляющих этот синтез. Как известно, характерными особенностями алгоритмов криптографии являются потоковый характер, большая разрядность и большой объём обрабатываемых данных, что указывает на высокую степень конвейеризации и (или) параллелизма, а наличие именно этих свойств даёт возможность наиболее эффективным образом использовать вычислители на ПЛИС и в несколько раз, по сравнению с универсальной процессорной архитектурой, увеличить производительность. Столь значительный эффект достигается за счёт того, что ПЛИС даёт возможность обеспечить соответствие между архитектурой специализированного вычислителя и структурой решаемой задачи.

Обзор решений на основе ПЛИС

Совершенно очевидно, что технология ПЛИС имеет свою нишу и заслуживает внимания производителей суперЭВМ [2]. Предлагаю остановиться на некоторых из такого рода решений, а начать с перечня основных исследовательских центров по данной тематике:

- **University of Toronto** – в Торонтском университете работает одна из наиболее активных исследовательских групп, специализирующихся в области FPGA;
- **FHPCA (FPGA High Performance Computing Alliance)** – разработанные в этом альянсе программные и аппаратные средства использованы при построении FPGA-суперкомпьютера Maxwell;
- **НИИ МВС ЮФУ (научно-исследовательский институт многопроцессорных вычислительных систем Южного федерального университета)** – здесь разрабатываются многопроцессорные системы с программируемой архитектурой, позволяющие перестраивать архитектуру системы под структуру решаемой прикладной задачи без изменения конфигурации используемого оборудования и, как следствие, обеспечивающие высокую реальную производительность и практически линейный рост производительности пропорционально задействованным аппаратным ресурсам (количеству процессоров в системе) [3];
- **NSF Center for High-Performance Reconfigurable Computing (CHREC)** – NSF-программа этого центра объединяет более 30 организаций, работающих в области реконфигурируемых вычислений.

Наиболее известные суперкомпьютеры, созданные с использованием технологий ПЛИС:

- Maxwell (University of Edinburgh) – высокопроизводительный реконфигурируемый компьютер;
- Cray XD1, использующий в многопроцессорных системах FPGA-ускорители совместно с основными процессорами;
- суперкомпьютер Cray XT5h;
- SuperQ X3.

Отдельного упоминания в связи с использованием технологий ПЛИС заслуживают говорящие сами за себя проект Adaptive Supercomputing (Cray) и направление Laptop Supercomputer, технология SGI RASC (Reconfigurable Application Specific Computing), позволяющая встраивать FPGA в серверы SGI Altix и системы визуализации Silicon Graphics Prism, а также проект RAMP (Research Accelerator for Multiple Processors), направленный на проведение исследований и развитие программного обеспечения в области многопроцессорных систем.

Даже краткий обзор решений, проектов, организаций, ориентированных на разработку суперЭВМ на базе ПЛИС, позволяет сделать вывод о насущности проблемы поиска новых архитектурных и оригинальных конструктивно-технологических решений для создания соответствующих вычислителей, которые станут базовой основой для построения кластера и позволят эффективно решать задачи предметной области.

Блок вычислительный реконфигурируемый (БВР)

ПЛИС и инструментальные средства разработки проектов на их основе представляют собой надёжную платформу для создания реконфигурируемых высокопроизводительных вычислительных систем.

ПЛИС – высокоинтегрированные гибкие универсальные устройства с мощной логикой, памятью и возможностью внутрисистемного перепрограммирования. Расширение сферы применения ПЛИС определяется рас-

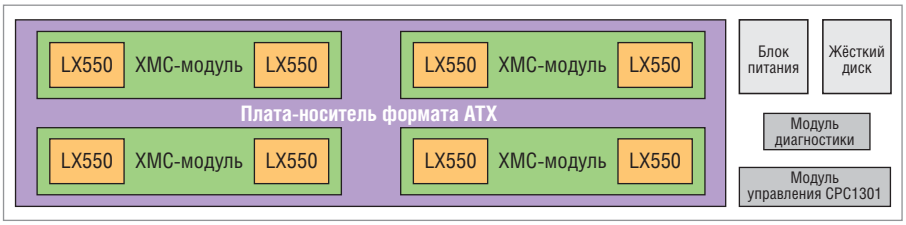

Рис. 1. Состав БВР-01

тущим спросом на устройства с быстрой перестройкой выполняемых функций, сокращением проектно-технологического цикла новых или модифицируемых изделий, востребованностью режимов изменения внутренней структуры в реальном масштабе времени, повышением быстродействия, снижением потребляемой мощности, а также снижением цен на эти устройства.

Идея о создании проблемно-ориентированных вычислителей (в том числе, «заточенных» на решение задач информационной безопасности) нового поколения на базе реконфигурируемых систем, основанных на ПЛИС-технологии, и была положена в основу разработки блока вычислительного реконфигурируемого БВР-01 [4]. При этом были учтены основные недостатки современных ПЛИС-систем:

1) большинство таких систем являются продукцией иностранного производства, что накладывает серьёзные ограничения на их применение при решении специальных задач, в том числе задач военного назначения;
2) использование различных интерконнектов (RapidIO, LVDS и др.) создаёт для программиста существенные трудности, так как бóльшую часть времени приходится тратить на согласование входных/выходных интерфейсов и данных для передачи из одного узла суперЭВМ в другой;
3) при проектировании суперЭВМ с входящими в его состав вычислителями на основе ПЛИС у разработчика нет возможности включать в вычислительный контур высокопроизводительные серверы другой архитектуры (например, CUDA или Xeon Phi) ввиду отсутствия стандартного интерфейса передачи данных, способного обеспечить полнодоступную информационную связь между всеми элементами кластера.

Преодоление перечисленных недостатков позволило создать систему с динамически перестраиваемой архитектурой, обеспечивающей полнодоступную информационную связь между всеми элементами кластера. Вычислитель нового поколения БВР-01 (рис. 1) использует самые мощные на сегодняшний день кристаллы Virtex-6 (LX550, SX475). С помощью оригинальных и передовых технических решений в нём реализован интерконнект PCI-E, позволяющий вести интенсивный обмен данными не только между кристаллами внутри одного блока, но и обеспечивать информационную связь между любыми элементами кластера. В состав решения уже входят предустановленные ядра PCI-E, что позволяет разработчикам не ломать голову над тем, как выгрузить данные из одного узла и передать в другой; обеспечена возможность организации вычислений таким образом, что данные, например из графической карты Nvidia, можно передать напрямую в конкретный кристалл ПЛИС.

Вычислитель является полностью отечественной разработкой. XMC-модуль, плата-носитель формата ATX, конструктив, модуль диагностики, управляющий модуль CPC1301 изготавливаются на производственных мощностях ЗАО «НПФ «ДОЛОМАНТ». Всё системное и специальное программное обеспечение БВР разработано специалистами дизайн-центра ЗАО «НПФ «ДОЛОМАНТ».

Основным вычислительным элементом БВР выступает XMC-модуль с двумя кристаллами ПЛИС (рис. 2). Отличительной особенностью является использование модельного ряда ПЛИС серии Virtex-6. На модуле установлены две пользовательские ПЛИС (X1 и X2). Каждая из пользовательских ПЛИС симметрично подключена к слоту расширения для установки в него различных мезонинных модулей, на которых могут располагаться несколько микросхем памяти, адаптеры различных интерфейсов, внешние каналы передачи данных. Внутренняя логика работы модуля организуется посредством системной ПЛИС, которая обеспечивает ввод/вывод информации, конфигурирование пользовательских ПЛИС X1 и X2 и управление ими. Конфигурирование пользовательских ПЛИС может быть выполнено с управляющей машины через интерфейс PCI-E.

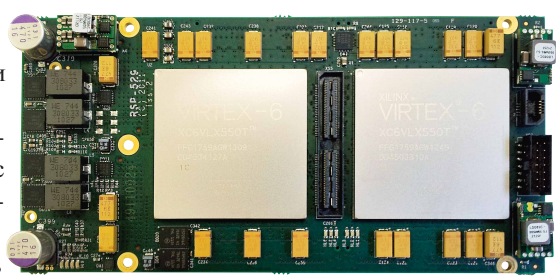

Рис. 2. XMC-модуль с кристаллами LX550

Область применения БВР – это задачи линейной алгебры, цифровой обработки сигналов, математической физики, символьной обработки. Вычислитель может быть использован во многих встраиваемых решениях, в том числе и военного назначения, в системах обеспечения информационной безопасности, в мобильных транспортных системах. И уже есть прецеденты таких применений. Главные его особенности – возможность гибкого конфигурирования собственной структуры и возможность объединения с другими аналогичными устройствами для создания кластерных структур с выполнением функции основного вычислительного элемента (рис. 3).

Заключение

Безопасность является одной из базовых потребностей человека, без реального ощущения безопасности в социальном и экономическом аспектах люди чувствуют себя крайне уязвимыми. В то же время минимальные требования к безопасности растут в соответствии с эволюцией вероятных угроз, в том числе в области безопасности личных и деловых коммуникаций, а значит и в сфере ИТ. Сегодня общество уязвимо перед угрозами, исходящими из этой сферы, более чем когда-либо, так как более чем когда-либо зависит от надлежащего функционирования информационных и коммуникационных технологий, которые в настоящее время проходят тест на доверие всего мирового сообщества. Именно поэтому новые подходы и технологии в области защиты информации ныне настолько актуальны и востребованны, ведь они решают самую насущную задачу – сделать мир более безопасным. Индустрия спецвычислителей адекватно и своевременно реагирует на запросы информационного общества и за последние годы прошла огромный путь, найдя своё место в решении задач обеспечения информационной безопасности. Наблюдается

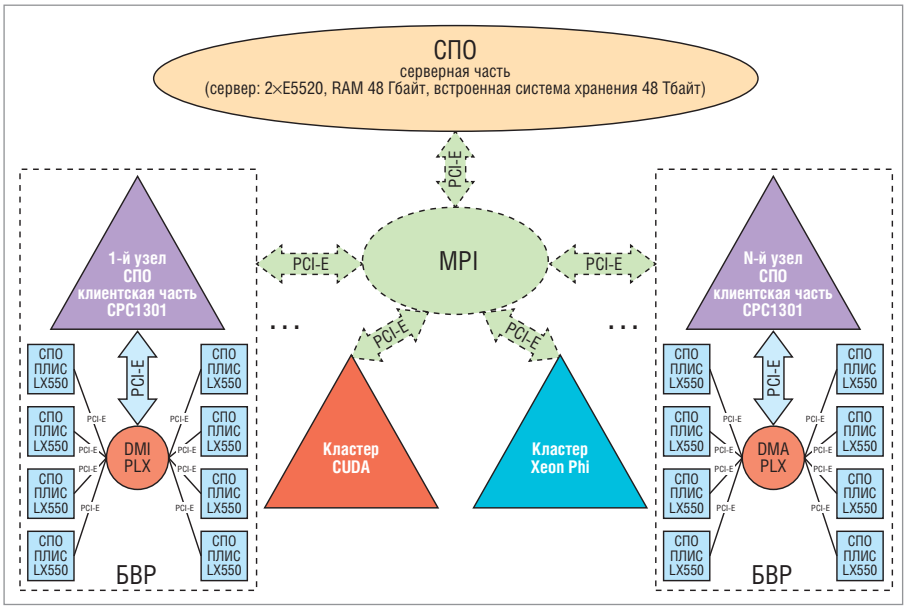

Рис. 3. Применение БВР в гибридном кластере: распределение специального программного обеспечения (СПО)

тенденция к поиску и применению специализированных решений, способных многократно превзойти традиционные архитектурные методы построения высокопроизводительных серверов и вычислителей, предназначенных для решения задач защиты информации.

Отечественные разработки, воплощённые в БВР-01, дают потребителям возможность получить современный универсальный высокопроизводительный вычислитель, способный обеспечить соответствие между его архитектурой и структурой решаемых задач, и на его основе создавать гибридные кластерные системы, заметно превосходящие по своим характеристикам зарубежные аналоги в сегменте рынка информационной безопасности и супер-ЭВМ. БВР-01 создан российскими инженерами и программистами и поэтому представляет большой интерес для встраиваемых систем военного назначения, что подтверждается успешными результатами внедрений и возрастающим спросом. ●

Литература

1. TOP 10 Sites for June 2013 [Электронный ресурс]. – Режим доступа : http://www.top500.org/lists/2013/06/.
2. Суперкомпьютеры на основе ПЛИС [Электронный ресурс]. – Режим доступа : http://www.parallel.ru/fpga/supercomputers.html.
3. Каляев А.В., Левин И.И. Модульно-наращиваемые многопроцессорные системы со структурно-процедурной организацией вычислений. – М. : Янус-К, 2003. – 380 с.
4. Коновальчик А. Высокопроизводительные вычислительные системы с реконфигурируемой архитектурой, построенной на ПЛИС // Современные технологии автоматизации. – 2013. – № 3.

Автор – сотрудник фирмы FASTWEL
Телефон: (495) 234-0639
E-mail: info@fastwel.ru