ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Дорожная карта реализации комплексного проекта по созданию в Российской Федерации технологий квантовой обработки информации

МСКФ 2014

Квантовая обработка информации

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Квантовые вычисления

2. Квантовые коммуникации, включая квантовую криптографию и синхронизацию

Цель комплексного проекта

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Координация и исключение дублирования работ, проводимых отдельными отечественными научными коллективами
2. Уточнение требований к основным прикладным результатам, запланированным к получению в итоге реализации комплекса исследований
3. Консолидация ресурсов основных государственных заказчиков работ в данной области

Квантовая вычислительная система

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Высокая производительность при решении переборных и моделирующих задач
2. Число разрядов квантового регистра: 500-1000
3. Исполнение*: стационарное, в помещении площадью до 100 м^2
4. Общая потребляемая мощность*: до 200 кВт
5. Потребляемая мощность квантовой части*: до 1 кВт

* зависит от способа физической реализации квантовых логических элементов

Некоторые задачи переборного типа

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Наименование задачи	Время вычисления на классическом компьютере эксафлопсной (10^{18} флопс) производительности	Время вычисления на квантовом компьютере мегафлопсной (10^{6} флопс) производительности
Разложение натурального числа с количеством десятичных знаков К на простые сомножители (факторизация).Алгоритм Шора	K=250 200 часов K=500 10 млн. лет K=1000 $4*10^{17}$лет	K=250 4 с K=500 18 с K=1000 84 с
Вычисление дискретного логарифма для чисел с количеством десятичных знаков К	**Ускорение сопоставимо с алгоритмом Шора**	
Быстрый поиск в большой базе данных, содержащей N элементов. Алгоритм Гровера Ускорение $\sqrt{\ }$ раз	N=10^{6}10 с N=10^{9} 3 часа N=10^{15} 4 месяца	N=10^{6} 10мс N=10^{9} 0,3 с N=10^{15} 10 с
Нахождение подстроки длины M в строке длины N (алгоритм Амбайниса), многомерного подмассива размерности M * M *… * M в массиве размерности N * N *… * N (алгоритм сопоставления шаблонов)	**Ускорение сопоставимо с алгоритмом Гровера**	

Некоторые задачи моделирования

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Наименование задачи	Время вычисления на классическом компьютере эксафлопсной (10^{18} флопс) производительности	Время вычисления на квантовом компьютере мегафлопсной (10^{6} флопс) производительности
Моделирование унитарной эволюции квантовой системы, состоящей из большого числа *N* взаимодействующих частиц		Ускорение составляет (*N*-1)! раз (алгоритм Залки-Визнера), требуется оперативная память, линейно зависящая от *N*

Квантовые коммуникации

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Средства квантового распределения криптографических ключей по незащищенным каналам связи
2. Квантовые каналы связи
3. Каналы телепортации квантового состояния и квантовые сети
4. Глобальная квантовая сеть высокоточной синхронизации абсолютно защищенных систем управления

Средства квантового распределения криптографических ключей

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Характеристика	ВОЛС	Атмосферный канал	Космический канал
Скорость распределения ключей, Мбит/с, не менее	10 000	1 000	0,001
Дальность передачи, км, не менее	200	2	1500
Криптографический протокол	BB84, B92, релятивистский или аналоги		
Исполнение	Возимое/ носимое	Возимое/носимое с внешними приемо-передающими модулями	Возимое (бортовая аппаратура), возимое/носимое (абонентская аппаратура)

Квантовый канал связи

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Размеры источника и приемника, не более: 10х10х10 $см^3$
2. Вес источника и приемника, не более: 2 кг
3. Дальность передачи информации: до 1000 км в космическом пространстве, до 200 км в плотных слоях атмосферы
4. Скорость передачи информации: не хуже 10^9 бит/с
5. Перехват информации третьей стороной исключен

Канал телепортации квантового состояния

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Размеры источника телепортируемого состояния, измерительной станции и приемной станции: не более 1 $м^3$
2. Вес: не более 10 кг
3. Дальность телепортации: до 1500 километров в космическом пространстве
4. Характерные скорости телепортации: до 10^8 кубит/сек
5. Перехват информации третьей стороной исключен

Сеть высокоточной квантовой синхронизации

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Дальность передачи информации: глобальное покрытие поверхности Земли и околоземного космического пространства
2. Стабильность частоты до 10^{-20}
3. Состав сети: 10 узлов (опорных станций) по 100 кубитов (атомов) в каждом
4. Характеристики узла: масса до 100 кг, объем до 1 $м^3$
5. Исполнение абонентских средств синхронизации: носимое, объемом до 1 $дм^3$

Отечественные центры компетенции

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

№	Наименование	Эксперимент	Теория
1	МГУ имени М.В.Ломоносова (технологическая долина)	+	+
2	Физико-технологический институт РАН	+	+
3	Институт физики полупроводников имени А.В.Ржанова СО РАН	+	
4	Институт общей физики имени А.М.Прохорова РАН	+	
5	Физический институт им. П.Н.Лебедева РАН	+	
6	Институт лазерной физики СО РАН	+	
7	Национальный исследовательский технологический университет "МИСИС"	+	
8	Институт автоматики и электрометрии СО РАН	+	
9	Физико-технический институт имени А.Ф.Иоффе	+	+
10	Институт физики твердого тела РАН	+	+
11	Институт спектроскопии РАН	+	
12	Институт прикладной физики РАН	+	
13	Санкт-Петербургский государственный политехнический университет		+
14	Новосибирский государственный университет	+	
15	Владимирский государственный университет		+
16	Институт геологии и минералогии им.В.С.Соболева СО РАН	+	
17	Математический институт имени В. А. Стеклова РАН		+
18	Казанский физико-технический институт имени Е.К.Завойского РАН		+
19	МОУ «Институт инженерной физики»	+	+

Структура дорожной карты комплексного проекта

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Технологические задачи (разработка отдельных технологий в области квантовой обработки информации)
2. Прикладные задачи (стадии ЖЦ создания изделий)
3. Задачи в области подготовки научных и инженерных кадров

Технологические задачи в области квантовых вычислений

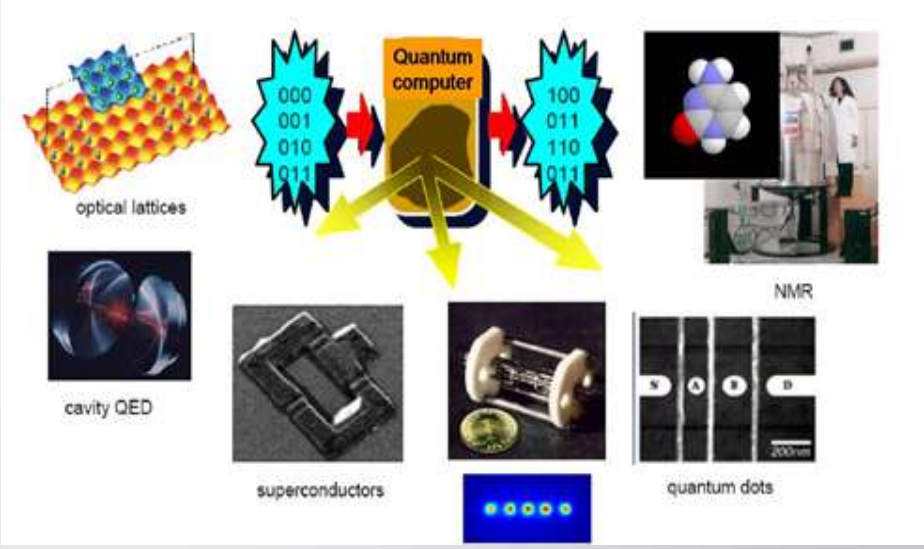
ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Проведение поисковых исследований
2. Создание элементной базы
3. Создание алгоритмов исправления квантовых ошибок
4. Задачи в теоретической области (разработка алгоритмов квантовых вычислений для различных типовых задач; квантового моделирования и квантовой томографии; оценки точности)

Варианты физической реализации квантовых элементов (поисковый этап)

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. На основе нейтральных атомов и молекул
2. На основе линейно-оптических и нелинейно-оптических систем
3. На основе полупроводниковых структур
4. На основе сверхпроводящих структур, включая квантовый отжиг
5. На основе примесных спинов в твердотельных структурах
6. …



Технологические задачи в области квантовых коммуникаций

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Эффективные интерфейсы «свет-вещество»
2. Источники одно-, двух- и N-фотонных состояний, включая источники перепутанных состояний
3. Приемники одно-, двух- и N-фотонных состояний
4. Методы передачи квантовых состояний между наземными и космическими станциями
5. Методы передачи квантовых состояний
6. Эффективные методы реализации протоколов квантовой коммуникации, таких как квантовая телепортация и обмен перепутыванием

Подготовка научных и инженерных кадров

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

1. Квантовая механика (2 семестра)
2. Квантовая оптика (2 семестра)
3. Статистическая физика (2 семестра)
4. Квантовые обработка информации и квантовые вычисления (2 семестра)
5. Квантовые алгоритмы (1 семестр)
6. Квантовая электроника (1 семестр)
7. Квантовая коммуникация (1 семестр)
8. Суперкомпьютерное моделирование и технологии программирования (1 семестр)
9. Параллельные вычисления (1 семестр) и др.

Технологические задачи

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Планируемые результаты	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Технологические задачи																
Оптимальные способы физической реализации квантовых логических элементов																
Одно- и двухкубитовые логические элементы																
Квантовые регистры																
Алгоритмы коррекции квантовых ошибок																
Алгоритмы квантовых вычислений для различных типовых задач																
Методы квантового моделирования и квантовой томографии																
Методы и алгоритмы оценки точности																
Интерфейсы «свет – вещество»																
Источники одно-, двух- и N-фотонных состояний																
Приемники одно-, двух- и N-фотонных состояний																
Квантовые генераторы криптографических ключей																
Квантовые криптографические протоколы																
Методы передачи квантовых состояний																

Прикладные задачи

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Планируемые результаты	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Прикладные задачи																
Квантовый компьютер																
Распределенная система квантовых вычислений																
Система квантового распределения криптографических ключей по ВОЛС																
Система квантового распределения криптографических ключей по атмосферному каналу связи																
Система квантового распределения криптографических ключей с использованием космических ретрансляторов																
Квантовый канал связи на основе спутанных состояний																
Средства телепортации квантовых состояний																
Национальная квантовая сеть																
Глобальная система высокоточной синхронизации																

Прикладные результаты

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Системы засекреченной связи

- перехват информации
- исключение несанкционированного доступа к информации

Big Data

- поиск в БД и распознавание изображений
- выявление латентных зависимостей
- задачи биоинформатики (секвенирование ДНК)
- сигнатурный и эвристический анализ компьютерных атак

Моделирование сложных систем

- прямое моделирование квантово-механических систем
- моделирование физико-химических процессов
- моделирование социальных процессов
- моделирование когнитивных процессов

Средства синхронизации и позиционирования

- радионавигационные системы
- системы единого времени
- синхронизация в системах связи, в том числе, на основе сверхширокополосных и шумоподобных сигналов

ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ

Спасибо за внимание

Гарбук Сергей Владимирович

Garbuk@FPI.gov.ru