Я посвящаю эту книгу моей жене Трише,
женщине замужем в полном смысле этого слова

Краткое содержание

I **Учебник по квантовым вычислениям** 21

1 Введение в квантовую механику 22

2 Введение в квантовые компьютеры 52

3 Как квантовые вычисления могут взломать существующие криптокоды? 85

4 Когда случится криптопрорыв? 114

5 Каким будет постквантовый мир? 130

II **Подготовка к квантовому взрыву** 163

6 Квантовоустойчивая криптография 164

7 Квантовая криптография 208

8 Квантовые сети 233

9 Готовимся сейчас 251

Содержание

Содержание ... 6
Краткое содержание ... 6
Об авторе ... 12
Благодарности ... 13
Предисловие ... 15

I **Учебник по квантовым вычислениям** ... 21

1 Введение в квантовую механику ... 22
Что такое квантовая механика? ... 22
Квант противоречит интуиции ... 23
Квантовая механика реальна ... 24
Основные свойства квантовой механики ... 27
Фотоны и квантовая механика ... 28
Фотоэлектрический эффект ... 28
Двойственность волна–частица ... 29
Принцип вероятности ... 34
Принцип неопределенности ... 38
Спиновые состояния и заряды ... 40
Квантовое туннелирование ... 41
Суперпозиция ... 42
Эффект наблюдателя ... 44
Теорема об отсутствии клонирования ... 45
Жуткая запутанность ... 46
Декогеренция ... 47
Квантовые примеры в современном мире ... 49
Для дополнительной информации ... 50
Резюме ... 51

2 Введение в квантовые компьютеры ... 52
В чем отличие квантовых компьютеров? ... 52
Традиционные компьютеры используют биты ... 52
Квантовые компьютеры используют кубиты ... 55
Квантовые компьютеры еще не готовы к прайм-тайму ... 59
Квант скоро будет царствовать ... 60

Квантовые компьютеры улучшают кубиты, используя исправление ошибок ... 61
Типы квантовых компьютеров ... 67
Сверхпроводящие квантовые компьютеры ... 68
Квантовые компьютеры на основе алгоритма отжига ... 69
Универсальные квантовые компьютеры ... 71
Топологические квантовые компьютеры ... 73
Компьютеры Majorana Fermion компании Microsoft ... 74
Квантовые компьютеры с ионными ловушками ... 75
Квантовые компьютеры в облаке ... 77
Квантовые компьютеры, произведенные не в США ... 78
Компоненты квантового компьютера ... 79
Квантовое программное обеспечение ... 80
Квантовый стек ... 81
Национальное руководство ... 81
Руководство национальной политикой ... 81
Денежные гранты и инвестиции ... 82
Другая квантовая научная информация ... 82
Дополнительные ресурсы ... 83
Резюме ... 83

3 Как квантовые вычисления могут взломать существующие криптокоды? ... 85
Основы криптографии ... 85
Шифрование ... 86
Хеширование ... 100
Применение криптографии ... 101
Как квантовые компьютеры могут взломать криптокоды ... 102
Сокращение времени ... 102
Квантовые алгоритмы ... 104
Что квант может и что не может сломать ... 108
Все еще теория ... 112
Резюме ... 113

4 Когда случится криптопрорыв? ... 114
Это вечное «лет через 10» ... 114
Факторы квантового криптопрорыва ... 115
Квантовая механика реальна? ... 115
Квантовые компьютеры реальны? ... 116
Суперпозиция реальна? ... 117
Реален ли алгоритм Питера Шора? ... 117
Достаточно ли у нас стабильных кубитов? ... 117
Квантовые ресурсы и конкуренция ... 118
У нас есть постоянное улучшение? ... 119
Мнения экспертов ... 120
Когда случится квантовый киберпрорыв ... 120
Временны́е сценарии ... 120

Когда следует быть готовыми? ... 123
Сценарии криптопрорыва ... 125
Новая технология надолго останется в распоряжении национальных государств ... 126
Применение крупнейшими компаниями ... 127
Массовое распространение ... 128
Наиболее вероятный сценарий прорыва ... 128
Резюме ... 129

5 Каким будет постквантовый мир? ... 130
Взломанные приложения ... 130
Ослабленные хеши и симметричные шифры ... 131
Взломанные асимметричные шифры ... 134
Ослабленные и взломанные генераторы случайных чисел ... 135
Слабые, или взломанные, зависимые приложения ... 136
Квантовые вычисления ... 147
Квантовые компьютеры ... 147
Квантовые процессоры ... 149
Квантовые облачные вычисления ... 150
Будет использоваться квантовая криптография ... 150
Квантовая идеальная конфиденциальность ... 150
Появляется квантовая сеть ... 151
Квантовые приложения ... 152
Улучшение химикатов и лекарств ... 152
Лучшие аккумуляторы электроэнергии ... 153
Настоящий искусственный интеллект ... 154
Управление цепочками поставок ... 155
Квантовые финансы ... 155
Улучшенное управление рисками ... 156
Квантовый маркетинг ... 156
Более точный прогноз погоды ... 156
Квантовые деньги ... 156
Квантовое моделирование ... 157
Более совершенное вооружение и точное оружие ... 157
Квантовая телепортация ... 157
Резюме ... 162

II **Подготовка к квантовому взрыву** ... 163

6 Квантовоустойчивая криптография ... 164
Постквантовый конкурс NIST ... 164
Классификация уровня безопасности ... 167
PKE против KEM ... 169
Формальные гарантии неразличимости ... 169
Размеры ключа и шифрованного текста ... 171
Типы постквантовых алгоритмов ... 172
Криптография на основе кода ... 172

Криптография на основе хеша ... 173
Решетчатая криптография ... 175
Многомерная криптография ... 177
Криптография изогенной сверхсингулярной эллиптической кривой ... 177
Доказательство нулевого знания ... 178
Квантовая устойчивость симметричного ключа ... 180
Квантовоустойчивые асимметричные шифры ... 181
BIKE ... 182
Classic McEliece ... 183
CRYSTALS-Kyber ... 184
FrodoKEM ... 184
HQC ... 185
LAC ... 186
LEDAcrypt ... 187
NewHope ... 187
NTRU ... 188
NTRU Prime ... 188
NTS-KEM ... 189
ROLLO ... 189
Round5 ... 190
RQC ... 190
SABER ... 191
SIKE ... 191
ThreeBears ... 192
Общие замечания по размерам ключей PKE, KEM и шифротекста ... 193
Квантовоустойчивые схемы цифровой подписи ... 195
CRYSTALS-Dilithium ... 196
FALCON ... 197
GeMSS ... 198
LUOV ... 199
MQDSS ... 199
Picnic ... 200
qTESLA ... 200
Rainbow ... 201
SPHINCS+ ... 201
Общие замечания о ключе и размерах подписи ... 204
Рекомендуемые предостережения ... 204
Недостаток стандартов ... 205
Проблемы производительности ... 206
Отсутствие проверенной защиты ... 206
Для дополнительной информации ... 207
Резюме ... 207

7 Квантовая криптография ... 208
Квантовые RNG ... 209
Случайное не всегда случайное ... 209
Почему истинная случайность так важна? ... 211

Квантовые RNG ... 213
Квантовые хеши и подписи ... 219
Квантовые хеши ... 219
Квантовые цифровые подписи ... 221
Квантовые шифры ... 223
Распределение квантовых ключей ... 224
Резюме ... 231

8 Квантовые сети ... 233
Компоненты квантовой сети ... 233
Среда передачи ... 233
Расстояние против скорости ... 235
Точка–точка ... 236
Доверенные повторители ... 237
Квантовые повторители ... 239
Квантовые сетевые протоколы ... 241
Квантовые сетевые приложения ... 244
Более безопасные сети ... 245
Облако квантовых вычислений ... 245
Лучшая временна́я синхронизация ... 245
Предотвращение помех ... 247
Квантовый интернет ... 248
Другие квантовые сети ... 248
Где получить больше информации ... 250
Резюме ... 250

9 Готовимся сейчас ... 251
Четыре основных этапа смягчения последствий постквантового прорыва ... 251
Этап 1. Укрепление существующих решений ... 251
Этап 2. Переход к квантовоустойчивым решениям ... 255
Этап 3. Применение квантово-гибридных решений ... 258
Этап 4. Применение полностью квантовых решений ... 259
Шесть основных шагов проекта смягчения последствий постквантового прорыва ... 260
Шаг 1. Обучение ... 261
Шаг 2. Создание плана ... 265
Шаг 3. Сбор данных ... 270
Шаг 4. Анализ ... 272
Шаг 5. Принять меры / исправить ... 274
Шаг 6. Обзор и улучшение ... 276
Резюме ... 276

Приложение. Дополнительные источники по квантам ... 278

Именной указатель ... 285

Предметный указатель ... 286

Об авторе

Роджер А. Граймс борется с хакерами более трех десятилетий (с 1987 года). Он получил десятки компьютерных сертификатов (включая CISSP, CISA, MCSE, CEH и Security+) и даже сдал очень жесткий экзамен на сертифицированного общественного бухгалтера (Certified Public Accountant, CPA), хотя это не имеет никакого отношения к компьютерной безопасности, и он худший из когда-либо существовавших бухгалтеров. Ему платили как профессиональному тестировщику компьютерной безопасности компаний и их веб-сайтов более 20 лет, и процесс тестирования никогда не занимал у него более трех часов. Он создал и обновил классы компьютерной безопасности, был инструктором и учил тысячи студентов, как взламывать или защищать криптокоды. Роджер – частый докладчик на национальных конференциях по компьютерной безопасности. Он написал сам и в соавторстве десять книг по компьютерной безопасности и более тысячи журнальных статей. С августа 2005 года ведет колонку обозревателя компьютерной безопасности в журналах InfoWorld и CSO (www.infoworld.com/blog/security-adviser/) и более двух десятилетий работает консультантом по компьютерной безопасности. Роджер часто дает интервью в журнальной прессе, на радио и телевидении (в том числе для журнала Newsweek и программы All Things Considered на радиостанции NPR). В настоящее время он консультирует большие и малые компании по всему миру, объясняя, как остановить злоумышленников и вредоносные программы в кратчайшие сроки и наиболее эффективным способом. Он следит за литературой и изучает квантовую физику с 1983 года.

Вы можете связаться с Роджером и подробнее узнать о его деятельности:

- E-mail: roger@banneretcs.com
- LinkedIn: www.linkedin.com/in/rogeragrimes/
- Twitter: @rogeragrimes
- CSOOnline: www.csoonline.com/author/Roger-A.-Grimes/

Благодарности

Я хотел бы поблагодарить издательство Wiley и Джима Минтеля (Jim Mintel) за то, что они дали этой книге зеленый свет. Я более года делал презентации для энтузиастов по теме данной книги, не имея возможности видеть их лица. Спасибо моему работодателю – компании KnowBe4, Inc., и ее замечательному генеральному директору Стью Сьюверману (Stu Sjouwerman), а также Кэти Уоттман (Kathy Wattman), Кендре Ирми (Kendra Irmie) и Мэри Оуэнс (Mary Owens), которые позволили мне разработать оригинальную презентацию и представить ее в различных организациях графства. Спасибо моей основной команде поддержки этих квантовых презентаций в компании KnowBe4: Эми Митчелл (Amy Mitchell), Джессике Шелтон (Jessica Shelton) и Энди Риду (Andy Reed). Я хочу поблагодарить всех, у кого брал интервью и с кем обменивался электронными письмами в стремлении лучше понять, как квантовые компьютеры повлияют на наш мир, включая криптографию. Не думаю, что моя голова когда-либо болела сильнее, чем когда я придумывал, как представить очень сложные понятия, пытаясь донести их до аудитории наиболее доходчивым способом. Эту задачу усложняло то обстоятельство, что большая часть квантовой физики и криптографии определена в терминах современной математики. В нескольких разделах я сдался и просто процитировал то, что написали или сказали эксперты. В качестве характерного примера приведу цитату из главы 6, где я пытаюсь описать один из квантовоустойчивых шифров: «команда NTRU Prime описывает свой шифр как “эффективную реализацию высоконадежной криптографии на идеальной решетке с инертным модулем группы Галуа”... другие же используют определения вроде “неприводимые, нециклотомические полиномы”». Всякий раз, видя это описание, я не могу удержаться от улыбки, поскольку, не понимая, что оно значит (как и вся терминология передовой современной математики), я должен был бы отделываться примерно такими общими фразами: «Это по-настоящему сложная математическая задача».

С учетом сказанного любые фактические ошибки, допущенные в этой книге, принадлежат только мне. Я приложил все силы, чтобы убедиться, что ни одна ошибка не попала в книгу. И горжусь тем, что старался быть абсолютно корректным в передаче фактов. В книге, которая охватывает так много сложных тем, возможно, я допустил ошибки. По-видимому, найдутся эксперты по квантовой криптографии, которые будут осуждать меня за то, что я не упомянул какие-то ключевые понятия. Пожалуйста, учтите, что я всего лишь человек, который изо всех сил старался быть максимально точным. Я заранее прошу прощения за любые ошибки. Хочу поблагодарить всех великих учителей и писателей, которые пытались более доступно объяснить квантовую механику и вычислительную технику и мне, и всем остальным. В этой книге я часто привожу примеры и аналогии, к которым прибегали другие авторы,

тексты и выступления которых я читал, слушал и смотрел в течение последних 20 лет. Иногда я понимал вещи, трудные для понимания, только потому, что эти люди проложили мне дорогу. Я старался отдать должное автору любых примеров или объяснений и сослаться на него, если мог вспомнить или найти этого автора. Прошу прощения у всех, кого я не упомянул. Мне будет стыдно за это. Я хочу поблагодарить все команды, которые ответили на мой призыв, за помощь в исправлении и уточнении моего обзора представленных ими в NIST алгоритмов (глава 6). Они стремились объяснить мне суть своих криптографических решений. Не все команды ответили (или ответили вовремя) на мои вопросы. Вот те, кто сделал это: Питер Швабе (Peter Schwabe) из CRYSTAL-Kyber; Томас Прест (Thomas Prest) из FALCON; Дуглас Стебила (Douglas Stebila) из FrodoKEM; Филипп Габори (Philippe Gaborit) из HQC, ROLLO и RQC; Вадим Любашевский из Dilithium; Сяньхуэй Лу (Xianhui Lu) из LAC; Марко Балди (Marco Baldi) из LEDCrypt; Уорд Бьюлленс (Ward Beullens) из LUOV; Йост Райневельд (Joost Rijneveld) из MQDSS & SPHINCS+; Симона Самардзиска (Simona Samardziska) из MQDSS; Томас Пеппельман (Thomas Poeppelmann) из NewHope; Джон Шанк (John Schanck) из NTRU; Нина Биндель (Nina Bindel) из qTESLA; Скотт Флюрер (Scott Fluhrer) из SPHINCS+ и Майк Гамбург (Mike Hamburg) из ThreeBears. Спасибо всем!

Я хотел бы выразить особую благодарность профессору Техасского университета в Остине, исследователю квантовых процессов Скотту Ааронсону (Scott Aaronson); физику, писателю Филипу Беллу (Philip Bell); Кену Мафли (Ken Mafli) из Townsend Security и Даниэлю Бургарту (Daniel Burgarth). Наконец, большое спасибо сотрудникам издательства Wiley, которые терпели мои вечные переработки текста, – это Ким Уимпсетт (Kim Wimpsett), Пит Гоган (Pete Gaughan) и Атияппан Лалиткумар (Athiyappan Lalitkumar). В конце концов, им пришлось меня остановить и наконец-то отправить книгу в печать.

Примечание Я часто намеренно или непреднамеренно использовал слово «шифр» для описания любого криптографического алгоритма. Технически шифр относится только к алгоритмам кодирования, а алгоритмы цифровой подписи являются схемами. Иногда я использовал слово «шифр», чтобы было проще писать о криптографии во всех девяти главах. Пожалуйста, извините меня за любое злоупотребление техническими терминами.

Предисловие

В конце 1990-х годов мир был озадачен компьютерной проблемой, известной под аббревиатурой Y2K, которую предстояло решить с наступлением 2000 года. Она заключалась в том, что к этому моменту большинство устройств, компьютеров и программ в мире записывали даты с использованием только двух последних цифр года и потому на программном уровне разницы между 1850, 1950 и 2050 годами для них не существовало. Когда 1999 год превратился в 2000-й, многие из этих компьютеров и программ не могли правильно обрабатывать данные с использованием двузначных дат в новом столетии, и прогнозировалось много отказов программ и устройств, которые уже использовали даты в будущем (например, программ планирования и гарантий). Симптомы неисправных устройств и программ варьировались от заметных ошибок до ошибок, наличие которых непросто обнаружить (что может быть чрезвычайно опасным), и полной неработоспособности устройств и программ.

Трудность заключалась и в том, что хотя было известно, что значительный процент устройств и программ подвержен влиянию этой проблемы, никто не знал, что оставалось правильным и не требовало обновления, а что необходимо было обновить или заменить до 1 января 2000 года. Оставалось два-три года, чтобы найти, что необходимо исправить, а что нет. Как и в случае многих медленно, но неизбежно надвигающихся катастроф глобального масштаба, большинство людей вплоть до последних нескольких месяцев мало что предпринимало для решения проблемы. Запоздалые попытки предотвратить то, что произойдет, когда часы переместятся в новый век, вызвали в мире накануне этой даты некоторую панику. В 1999 году даже был создан фантастически плохой фильм-катастрофа (www.imdb.com/title/tt0215370), в котором показаны падающие с неба самолеты и прочие приметы наступившего хаоса.

В конце концов, едва ли кто-либо хотел, чтобы с приходом Y2K настоящая жизнь была похожа на кино. Проблемы были, но по большей части мир продолжал жить обычной жизнью. Были устройства и программы, которые не могли обработать новые даты должным образом, но большинство основных систем работали правильно. Не было ни падающих самолетов, ни пожаров, ни прорванных дамб. Многих людей, ожидавших катастрофы, результаты даже несколько разочаровывали, так что со временем аббревиатурой Y2K стали обозначать события, по поводу которых поднимают слишком много шума, создавая преждевременную панику, притом что реальный ущерб оказывается незначительным.

Большинство людей сегодня не осознают, что «катастрофическая» Y2K всех разочаровала именно потому, что у нас были годы для подготовки и предупреждения последствий. Большинство основных систем были про-

верены на наличие проблем 2000 года и по мере необходимости заменены или обновлены. Если бы мир не осознал проблемы Y2K и вообще ничего бы не сделал, ее последствия наверняка были бы намного, намного хуже (хотя я все же не уверен, что самолеты стали бы падать). Нельзя сказать, что Y2K демонстрирует эффект неразорвавшейся бомбы. Благополучный переход к новой дате явился предсказуемым результатом многолетней подготовки, демонстрирующей успех того, что человечество может сделать, столкнувшись с надвигающейся цифровой проблемой.

Грядущий квантовый судный день

Большая часть мира этого еще не осознает, но мы приближаемся к еще более весомому, по сравнению с Y2K, моменту, который, вероятно, уже и теперь вызывает серьезные проблемы и наносит ущерб. Хуже того, мы не можем исключить весь ущерб, даже если начнем готовиться заранее. Сегодня существуют организации, уже наносящие вред программам, избежать которого системы не могут. Государства и конкурирующие компании, должно быть, уже извлекают для себя преимущества из этого обстоятельства.

Квантовые компьютеры, вероятно, в ближайшем будущем взломают традиционные криптокоды с открытым ключом, в том числе шифры, защищающие большинство цифровых секретов мира. Эти протоколы и компоненты включают HTTPS, TLS, SSH, PKI, цифровые сертификаты, RSA, DH, ECC, большинство сетей Wi-Fi, многие сети VPN, смарт-карт, HSM, большинство криптовалют и большинство устройств многофакторной аутентификации, которые полагаются на криптографию с открытым ключом. Даже если бы список содержал только HTTPS и TLS, то он уже охватывал бы бóльшую часть интернета. В тот день, когда квантовые вычисления нарушат традиционную публичную криптографию, все секреты, защищенные этими протоколами и механизмами, выйдут наружу.

Еще более важно, что любой, кто сейчас перехватит и сохранит эти защищенные в настоящее время секреты, после квантового криптографического взлома будет иметь возможность вернуться и раскрыть секреты. Сколько у вас или вашей организации есть секретов, которыми вы готовы поделиться с миром через несколько лет? Это новая проблема Y2K, с которой мы имеем дело уже сегодня.

Есть много выполнимых решений, которые можно реализовать сегодня, хотя некоторые из них либо выходят за рамки имеющихся возможностей средней компании, либо, если их преждевременно реализовать, могут привести к значительным нарушениям ведущихся работ. Подготовка к грядущему квантовому взрыву требует образования, критичного выбора и планирования. Люди и организации, которые четко понимают, что нас ждет впереди, могут предпринять правильные шаги уже сейчас, чтобы быть как можно более подготовленными. Они могут остановить сегодня необоснованное подслушивание и начать переводить свои управляемые активы в более устойчивую среду. Данная книга содержит необходимые для этого знания и дает вам план, помогающий минимизировать риски вашей организации от прихода

квантового криптовзлома. Если достаточное количество организаций будут готовиться к этому уже сейчас, мы можем избежать квантовых проблем и сделать их столь же малосущественными, как это было с проблемой Y2K.

Для кого эта книга

Эта книга в первую очередь предназначена для тех, кто отвечает за управление безопасностью компьютерной техники своей организации и, в частности, компьютерную криптографию. Это люди, которые, разрабатывая проекты, будут отвечать на вызовы постквантовой миграции. Данная книга также для менеджеров и других лидеров, понимающих важность хорошей криптографии и ее влияние на их организацию. Наконец, любой, интересующийся квантовой механикой, квантовыми компьютерами и квантовой криптографией, найдет здесь много неизвестных ему фактов, делающих эту книгу достойной прочтения.

Что вы найдете в этой книге

Книга «Апокалипсис криптографии» подготавливает читателя к квантовому прорыву в вычислениях. Она состоит из девяти глав, разделенных на две части.

Часть I «Учебник по квантовым вычислениям» – это базовый учебник по квантовой механике и вычислениям, рассказывающий о том, как можно взломать сегодняшнюю криптографическую защиту.

Глава 1 «Введение в квантовую механику»

Если вы не понимали квантовую механику, читая о ней впервые, не расстраивайтесь – квантовая механика досаждала самым блестящим умам, которые украшали нашу планету за последнее столетие. Нас, простых смертных, можно простить за то, что мы не сразу усваиваем ее основные идеи. Глава 1 объясняет свойства, наиболее важные для понимания того, как квантовая механика влияет на наш цифровой мир. Если я проделал свою работу хорошо и правильно, вы поймете это лучше, чем 99 % других представителей нашей компьютерной цивилизации.

Глава 2 «Введение в квантовые компьютеры»

Квантовые компьютеры используют квантовые свойства и обеспечивают возможности, логические и арифметические результаты, которых просто невозможно достигнуть с помощью традиционных бинарных компьютеров. Глава 2 охватывает различные типы квантовых компьютеров, которые, скорее всего, станут окружать нас в следующем десятилетии и будут поддерживать различные квантовые свойства.

Глава 3 «Как квантовые вычисления могут взломать существующие криптокоды?»

Наиболее распространенный вопрос, который задают, когда человеку говорят, что квантовые компьютеры, вероятно, взломают традиционные

криптокоды с открытым ключом, – каким образом? В главе 3 рассказывается, почему традиционным бинарным компьютерам нелегко взломать большинство шифров с открытым ключом и что позволит квантовым компьютерам легче справиться с задачей. Здесь показано, что квантовые компьютеры, скорее всего, будут иметь возможность взломать, а также что будет устойчивым к квантовым вычислительным мощностям.

Глава 4 «Когда случится криптопрорыв?»

После вопроса о том, как квантовые компьютеры могут сломать традиционные криптокоды с открытым ключом, второй наиболее часто задаваемый вопрос, – когда это произойдет. Хотя этого никто (достоверно) не знает, предположительный ответ таков: скорее раньше, чем позже. В главе 4 обсуждаются различные сроки и их вероятность.

Глава 5 «Каким будет постквантовый мир?»

Как и изобретение интернета, квантовое доминирование разделит мир на «до» и «после». Квант решит проблемы, которые мучили нас на протяжении веков, и даст нам новые проблемы, и это в будущем начнет раздражать нас. Глава 5 опишет постквантовый мир и как он будет влиять на нас.

Часть II «Подготовка к квантовому взрыву» поможет вам и вашей организации наиболее эффективно подготовиться к грядущему квантовому доминированию.

Глава 6 «Квантовоустойчивая криптография»

Глава 6 охватывает более двух десятков квантовоустойчивых шифров и схем, которые Национальный институт стандартов и технологий (NIST) рассматривает во втором туре своего постквантового конкурса. Два или более из этих квантовоустойчивых алгоритмов станут следующими национальными стандартами криптографии. Вы узнаете о конкурентах, их сильных и слабых сторонах.

Глава 7 «Квантовая криптография»

Глава 7 посвящена традиционной бинарной квантовоустойчивой криптографии, которая не использует квантовые защитные свойства. Глава 7 охватывает шифры и схемы, которые квантовые свойства используют, чтобы обеспечить их криптографическую устойчивость. В долгосрочной перспективе вы, вероятно, будете использовать криптографию на основе квантов, а не только квантовоустойчивую криптографию. Узнайте, как это выглядит.

Глава 8 «Квантовые сети»

Глава 8 охватывает квантовые сетевые устройства, такие как квантовые повторители и приложения, которые ищут квантовую защиту сети. Она описывает текущее состояние квантовых сетей и как это, вероятно, будет выглядеть в ближайшем и долгосрочном будущем. Скорее всего, настанет время, когда весь интернет будет основан на квантах. Читайте о таких сетях и их компонентах и о том, как мы к ним придем.

Глава 9 «Готовимся сейчас»

Ради одной только этой главы книга заслуживает внимания. Здесь будет показано, как уже сегодня организации любого рода могут начать подготовку к грядущему квантовому криптографическому взрыву. Из главы 9 вы узнаете, что можно сделать сегодня, чтобы защитить ваши наиболее важные долгосрочные секреты, какие размеры криптографических ключей нужно увеличить, что и когда должно быть заменено. Обобщенный план, применявшийся ранее для глобальных обновлений криптографии, может быть использован и для преодоления апокалипсиса криптографии.

В приложении перечислены десятки ссылок на квантовые информационные ресурсы, в том числе книги, видео, блоги, официальные документы и веб-сайты.

Если я хорошо справился со своей работой, к концу этой книги вы лучше, чем прежде, поймете квантовую физику, поймете, как она сломает сегодняшнюю традиционную криптографию с открытым ключом, и будете в состоянии надлежащим образом подготовить и лучше защитить ваши важные цифровые секреты.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в тексте, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Wiley очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Учебник по квантовым вычислениям

Глава 1 Введение в квантовую механику
Глава 2 Введение в квантовые компьютеры
Глава 3 Как квантовые вычисления могут взломать существующие криптокоды?
Глава 4 Когда случится криптопрорыв?
Глава 5 Каким будет постквантовый мир?

1 Введение в квантовую механику

Ничего удивительного в том, что те, кто впервые встречается с квантовой механикой, не могут понять ее.

Нильс Бор, квантовый физик,
лауреат Нобелевской премии 1922 года

Любая достаточно развитая технология неотличима от магии.

Артур Чарльз Кларк, писатель-фантаст

В главе 1 будут обсуждаться основы квантовой механики, особенно аспекты, касающиеся квантовых вычислений. Данная глава намеренно не охватывает все аспекты полностью, поскольку для этого потребовалась бы целая книга, а не просто глава на эту тему. Не будет описана каждая частица, ее свойства или возможное взаимодействие, и будут опущены все сложные математические уравнения. Эта глава даст вам понимание квантовой физики, достаточное, чтобы объяснить, как квантовые компьютеры способны быстро решать считавшиеся ранее нерешаемыми математические задачи, на которых основаны многие распространенные, обеспечивающие защиту, типы шифрования. Понимание квантовой механики и квантовых вычислений совершенно не требуется для подготовки к грядущей эпохе криптографических взломов, но оно поможет вам усвоить самые азы для обсуждения соответствующих проблем.

Что такое квантовая механика?

В этом разделе я буду объяснять квантовую механику, но если это ваша первая встреча с данной темой, отнеситесь к ней с некоторой осторожностью. Квантовая механика невероятно крута, и иногда мы не способны полностью понять, что происходит. Многое в ней кажется таким странным для нашего нынешнего понимания того, как устроен мир, что большинству людей, которые впервые сталкиваются с квантовой механикой, понять ее очень нелегко. Даже после почти 30 лет попыток полностью осознать сущность этой области знаний и ее значение мой мозг психологически все еще не готов к этому. Я не одинок. Приятно снисходительно сказать, что только на первый взгляд квантовая механика противоречит интуиции и выглядит неестественно, но часто это совсем не так. Это идет вразрез со многим, чему нас учили ранее об устройстве нашего мира и Вселенной. Один плюс один

не всегда равняется двум. Это идет также вразрез с тем, что мы можем легко увидеть, потрогать и почувствовать, хотя вся наша реальность возможна именно благодаря этому.

Хотя лучшие умы нашей цивилизации неоднократно доказывали, что в существовании квантовой механики нет ни тени сомнения, то, что она влечет за собой, звучит так странно для обычного человека, что часто остается для него невероятным и волшебным. Понимание значения квантовой механики даже впервые ставит вопрос о существовании реальности.

Довольно распространенная реакция на квантовую теорию заключается в предположении, что все, кто проповедует ее, должно быть, находятся под воздействием какой-то научной фантастики, что это результат массового заблуждения, потому что речь идет о том, чего быть не может. Как однажды сказала мне одна моя подруга, после того как я попытался (явно неудачно) объяснить ей квантовую механику: «Ты можешь верить во все, что хочешь, но это просто чушь собачья»... правда, слова «собачья» она не произнесла.

Даже Альберт Эйнштейн, который помогал открытию некоторых из наиболее важных принципов, лежащих в основе квантовой механики, не вполне верил в некоторые ее другие принципы. Он потратил десятилетия, пытаясь понять их, и понял их лучше, чем многие другие. Это его глубокое понимание ее основ создавало для него проблемы. Он даже ставил эксперименты, пытаясь доказать или опровергнуть их. Он не мог логически проверить или объяснить многие странные свойства квантовой механики и «пугающие при взгляде с расстояния» результаты. После десятилетий ожидания экспериментального подтверждения своих предположений он просто перешел к изучению других научных областей. Видимо, его мозг просто устал постоянно думать об этом. Так что не столь великие умы вполне можно извинить.

С учетом сказанного я написал эту главу учебника по квантовой механике так, как хотел бы, чтобы это было объяснено мне самому, когда я впервые начал изучать ее. Я надеюсь, что данная глава поможет сократить вам время обучения.

Квант противоречит интуиции

Хотя квантовая механика лежит в основе всей реальности, она не всегда выглядит так, как то, что мы наблюдаем в нашей повседневной жизни. Например, собака одной масти не может быть белой и черной масти в одно и то же время; белая собака, находящаяся в комнате, не становится черной, когда выходит из нее, и собака не может разделиться на две собаки прямо на ваших глазах, а затем снова слиться воедино. Но на атомном и субатомном уровнях особенности квантовой механики состоят как раз в подобных странностях. Какие же свойства квантов, о которых я говорю, столь странные? Вот некоторые примеры:

- одна квантовая частица может находиться в двух местах и быть одновременно двумя совершенно разными частицами;
- одна квантовая частица может разделиться на две, а позже столкнуться или смешаться и восстановиться или исчезнуть;

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru