

УДК 004.382
ББК 32.973-018
Г75

Граймс Р. А.
Г75 Апокалипсис криптографии / пер. с англ. В. А. Яроцкого. 2-е изд. – М.: ДМК Пресс, 2021. – 286 с.: ил.

ISBN 978-5-93700-050-7

В связи с бурным развитием технологий требования к компьютерной безопасности постоянно изменяются. Шифры, которые на сегодняшний день можно считать надежными, при использовании квантового компьютера будут легко взломать, и эта реальность уже не за горами. Вот почему необходимо уже сейчас готовиться к квантовому криптографическому прорыву, и эта книга послужит для читателя бесценным руководством к действию.

Автор, известный специалист по компьютерной безопасности, показывает, какие приложения могут оказаться самыми уязвимыми перед квантовыми вычислениями, как лучше использовать современные технологии шифрования и как внедрить новую постквантовую криптографию для обеспечения безопасности пользователей, данных и инфраструктуры.

Издание адресовано работникам служб информационной безопасности, которые принимают во внимание угрозы, возникающие с появлением квантовых вычислений, и планируют защитить свои организации от взломов информационных систем.

УДК 004.382
ББК 32.973-018

All rights reserved. This Translation publish under license with the original publisher John Wiley & Sons, Inc. Russian language edition copyright © 2020 by DMK Press. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-119-61819-5 (англ.)
ISBN 978-5-93700-050-7 (рус.)

Copyright © by John Wiley & Sons, Inc., 2020
© Оформление, издание, перевод, ДМК Пресс, 2021

Содержание

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.....	43
Теорема о запрете клонирования.....	45
Жуткая запутанность.....	45
Декогеренция	47
Квантовые примеры в современном мире.....	49
Для дополнительной информации.....	49
Резюме	50
2 Введение в квантовые компьютеры	51
В чем отличие квантовых компьютеров?	51
Традиционные компьютеры используют биты	51
Квантовые компьютеры используют кубиты.....	54
Квантовые компьютеры еще не готовы к прайм-тайму.....	58
Квант скоро будет царствовать.....	59
Квантовые компьютеры улучшают кубиты, используя исправление ошибок.....	60
Типы квантовых компьютеров	66

Сверхпроводящие квантовые компьютеры.....	67
Квантовые компьютеры на основе алгоритма отжига	68
Универсальные квантовые компьютеры	70
Топологические квантовые компьютеры	72
Компьютеры Majorana Fermion компании Microsoft.....	73
Квантовые компьютеры с ионными ловушками.....	74
Квантовые компьютеры в облаке	76
Квантовые компьютеры, произведенные не в США.....	77
Компоненты квантового компьютера	78
Квантовое программное обеспечение	79
Квантовый стек	79
Национальное руководство	80
Руководство национальной политикой.....	80
Денежные гранты и инвестиции.....	80
Другая квантовая научная информация	81
Дополнительные ресурсы	82
Резюме	82
3 Как квантовые вычисления могут взломать существующие криптокоды?	83
Основы криптографии.....	83
Шифрование	84
Хеширование.....	98
Применение криптографии.....	99
Как квантовые компьютеры могут взломать криптокоды	100
Сокращение времени.....	100
Квантовые алгоритмы.....	102
Что квант может и что не может сломать.....	106
Все еще теория	110
Резюме	111
4 Когда случится криптопрорыв?.....	112
Это вечное «лет через 10».....	112
Факторы квантового криптопрорыва	113
Квантовая механика реальна?	113
Квантовые компьютеры реальны?.....	114
Суперпозиция реальна?	115
Реален ли алгоритм Питера Шора?.....	115
Достаточно ли у нас стабильных кубитов?.....	115
Квантовые ресурсы и конкуренция	116
У нас есть постоянное улучшение?.....	117
Мнения экспертов.....	118
Когда случится квантовый киберпрорыв	118
Временные сценарии.....	118
Когда следует быть готовыми?	121
Сценарии криптопрорыва	124

Новая технология надолго останется в распоряжении государств	124
Применение крупнейшими компаниями	125
Массовое распространение.....	126
Наиболее вероятный сценарий прорыва.....	126
Резюме	127
5 Каким будет постквантовый мир?.....	128
Взломанные приложения.....	128
Ослабленные хеши и симметричные шифры	129
Взломанные асимметричные шифры.....	132
Ослабленные и взломанные генераторы случайных чисел.....	133
Слабые, или взломанные, зависимые приложения	134
Квантовые вычисления.....	145
Квантовые компьютеры	145
Квантовые процессоры	146
Квантовые облачные вычисления.....	147
Будет использоваться квантовая криптография.....	148
Квантовая идеальная конфиденциальность.....	148
Появляется квантовая сеть.....	149
Квантовые приложения	150
Улучшение химикатов и лекарств.....	150
Лучшие аккумуляторы электроэнергии.....	151
Настоящий искусственный интеллект	152
Управление цепочками поставок.....	153
Квантовые финансы	153
Улучшенное управление рисками.....	153
Квантовый маркетинг.....	154
Более точный прогноз погоды	154
Квантовые деньги.....	154
Квантовое моделирование.....	155
Более совершенное вооружение и точное оружие.....	155
Квантовая телепортация	155
Резюме	159
II Подготовка к квантовому взрыву	161
6 Квантовоустойчивая криптография	162
Постквантовый конкурс NIST	162
Классификация уровня безопасности.....	165
PKE против KEM	167
Формальные гарантии неразличимости	167
Размеры ключа и зашифрованного текста	168
Типы постквантовых алгоритмов	170
Криптография на основе кода	170
Криптография на основе хеша	171
Решетчатая криптография.....	173

Многомерная криптография	174
Криптография изогенной сверхсингулярной эллиптической кривой	175
Доказательство нулевого знания	176
Квантовая устойчивость симметричного ключа	177
Квантовоустойчивые асимметричные шифры	179
BIKE.....	180
Classic McEliece.....	181
CRYSTALS-Kyber.....	182
FrodoKEM	182
HQC.....	183
LAC.....	184
LEDACrypt.....	185
NewHope.....	185
NTRU	185
NTRU Prime.....	186
NTS-KEM.....	187
ROLLO.....	187
Round5	187
RQC.....	188
SABER.....	188
SIKE.....	189
ThreeBears.....	189
Общие замечания по размерам ключей PKE, KEM и шифротекста	191
Квантовоустойчивые схемы цифровой подписи	193
CRYSTALS-Dilithium.....	193
FALCON.....	195
GeMSS.....	196
LUOV.....	196
MQDSS	197
Picnic	197
qTESLA.....	198
Rainbow.....	198
SPHINCS+	199
Общие замечания о ключе и размерах подписи	200
Рекомендуемые предостережения	202
Недостаток стандартов.....	203
Проблемы производительности	203
Отсутствие проверенной защиты.....	204
Для дополнительной информации.....	205
Резюме	205
7 Квантовая криптография	206
Квантовые RNG.....	207
Случайное не всегда случайное	207
Почему истинная случайность так важна?.....	209
Квантовые RNG.....	211

Квантовые хеши и подписи	217
Квантовые хеши	217
Квантовые цифровые подписи	219
Квантовые шифры.....	221
Распределение квантовых ключей.....	222
Резюме	229
8 Квантовые сети.....	231
Компоненты квантовой сети.....	231
Среда передачи	231
Расстояние против скорости	233
Точка–точка.....	234
Доверенные повторители.....	235
Квантовые повторители.....	237
Квантовые сетевые протоколы	239
Квантовые сетевые приложения.....	242
Более безопасные сети	243
Облако квантовых вычислений	243
Лучшая временная синхронизация.....	243
Предотвращение помех.....	245
Квантовый интернет	246
Другие квантовые сети	246
Где получить больше информации.....	248
Резюме	248
9 Готовимся сейчас	249
Четыре основных этапа смягчения последствий постквантового прорыва.....	249
Этап 1. Укрепление существующих решений.....	249
Этап 2. Переход к квантовоустойчивым решениям.....	253
Этап 3. Применение квантово-гибридных решений.....	256
Этап 4. Применение полностью квантовых решений.....	257
Шесть основных шагов проекта по смягчению последствий постквантового прорыва.....	258
Шаг 1. Обучение	259
Шаг 2. Создание плана.....	263
Шаг 3. Сбор данных.....	268
Шаг 4. Анализ	270
Шаг 5. Принять меры / исправить	272
Шаг 6. Обзор и улучшение	274
Резюме	274
Приложение. Дополнительные источники по квантам	276
Предметный указатель	283