

УДК 004.382  
ББК 32.973-018  
Г75

Граймс Р. А.  
Г75 Апокалипсис криптографии / пер. с англ. В. А. Яроцкого. – М.: ДМК Пресс, 2020. – 290 с.: ил.

**ISBN 978-5-97060-837-1**

В связи с бурным развитием технологий требования к компьютерной безопасности постоянно изменяются. Шифры, которые на сегодняшний день можно считать надежными, при использовании квантового компьютера будет 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 978-5-97060-837-1 (рус.)

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

# Краткое содержание

<b>I Учебник по квантовым вычислениям.....</b>	<b>21</b>
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
<b>II Подготовка к квантовому взрыву .....</b>	<b>163</b>
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
<b>I Учебник по квантовым вычислениям.....</b>	<b>21</b>
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
<b>3 Как квантовые вычисления могут взломать существующие криптокоды? .....</b>	<b>85</b>
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
<b>4 Когда случится криптопрорыв?.....</b>	<b>114</b>
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
Временные 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
<b>5 Каким будет постквантовый мир? .....</b>	<b>130</b>
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
<b>II Подготовка к квантовому взрыву .....</b>	<b>163</b>
<b>6 Квантоустойчивая криптография .....</b>	<b>164</b>
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
<b>7 Квантовая криптография .....</b>	<b>208</b>
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
<b>8 Квантовые сети.....</b>	<b>233</b>
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 временная синхронизация.....	245
Предотвращение помех.....	247
Квантовый интернет.....	248
Другие квантовые сети .....	248
Где получить больше информации.....	250
Резюме .....	250
<b>9 Готовимся сейчас .....</b>	<b>251</b>
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