Криптография на эллиптических кривых для разработчиков

Майкл Розинг

MANNING

ДМК ПРЕСС

Оглавление

1 Спаривание эллиптических кривых в криптографии 25

Часть I ОСНОВЫ 37

2 Математика конечных полей 39

3 Основы математики эллиптических кривых 53

4 Обмен ключами с применением эллиптических кривых 71

5 Цифровые подписи с применением эллиптических кривых над простым полем 90

6 Нахождение криптографически хороших эллиптических кривых 103

Часть II ИНТЕРЛЮДИЯ 116

7 Математика полиномов над конечными полями 118

8 Умножение полиномов 126

9 Вычисление степеней полиномов 140

10 Деление полиномов по алгоритму Евклида 148

11 Создание неприводимых полиномов 161

12 Извлечение квадратных корней из полиномов 168

Часть III СПАРИВАНИЕ 184

13 Кривые над расширением конечного поля 186

14 Нахождение эллиптических кривых с малой степенью вложения 207

15 Общие правила спаривания эллиптических кривых 235

16 Спаривание Вейля 249

17 Спаривание Тейта 261

18 Мультиподписи BLS 271

19 Доказательство знания и хранение секретов: нулевое разглашение с применением спариваний 312

Содержание

Предисловие ... 13
Благодарности ... 16
Об этой книге ... 18
Об авторе ... 23
Об иллюстрации на обложке ... 24

1 ***Спаривание эллиптических кривых в криптографии*** ... 25
1.1 Что такое криптография на эллиптических кривых? ... 26
1.2 Зачем использовать криптографию на эллиптических кривых? ... 27
1.3 Эллиптические кривые приходят в криптографию ... 29
1.3.1 Общее описание обмена ключами ... 30
1.3.2 Объяснение алгоритмов цифровой подписи ... 31
1.3.3 Как несколько человек могут подписать один и тот же документ ... 32
1.3.4 Нулевое разглашение, или Как сохранить секрет и доказать, что вы его знаете ... 33
1.4 Для кого написана эта книга ... 35
Резюме ... 35

Часть I ОСНОВЫ ... 37

2 ***Математика конечных полей*** ... 39
2.1 Основы математики конечных полей ... 40
2.2 Эллиптические кривые образуют группы точек над конечным полем ... 41
2.3 Базовые подпрограммы для арифметики на конечном поле ... 42
2.4 Вычисление квадратичных вычетов над простым полем ... 46
2.5 Вычисление квадратного корня по модулю p ... 47
Ответы к упражнениям ... 52
Резюме ... 52

3 ***Основы математики эллиптических кривых*** ... 53
3.1 Алгебра эллиптических кривых ... 53
3.1.1 Представление точки ... 54
3.1.2 Эллиптические кривые над конечными полями ... 55

3.1.3 Сложение точек ... 57
3.1.4 Умножение точки на число ... 58
3.1.5 Вложение данных в кривую ... 59
3.2 Подпрограммы для работы с эллиптическими кривыми ... 62
3.2.1 Представление кривых и точек ... 62
3.2.2 Сложение точек ... 63
3.2.3 Умножение точки на число ... 65
3.3 Вложение данных в кривую ... 66
3.4 Разные функции ... 68
Ответы к упражнениям ... 69
Резюме ... 69

4 ***Обмен ключами с применением эллиптических кривых*** ... 71
4.1 Описание алгоритма Диффи–Хеллмана ... 72
4.1.1 Математика эллиптических кривых ... 72
4.1.2 Хеш-функция ... 74
4.1.3 Генерирование ключа ... 76
4.1.4 Вычисление разделяемых ключей ... 77
4.2 Алгоритм MQV ... 78
4.2.1 Математика эллиптических кривых для алгоритма MQV ... 78
4.2.2 Код MQV ... 80
4.3 Пример кода ... 82
4.3.1 Тестовые кривые ... 83
4.3.2 Функции для тестирования алгоритма Диффи–Хеллмана ... 87
4.3.3 Функция для тестирования алгоритма MQV ... 88
Ответы к упражнениям ... 89
Резюме ... 89

5 ***Цифровые подписи с применением эллиптических кривых над простым полем*** ... 90
5.1 Цифровая подпись Шнорра ... 91
5.1.1 Математические основы алгоритма Шнорра на эллиптической кривой ... 91
5.1.2 Функция вычисления подписи в алгоритме Шнорра ... 93
5.1.3 Функция проверки подписи в алгоритме Шнорра ... 94
5.1.4 Тест алгоритма Шнорра ... 95
5.2 Алгоритм NIST цифровой подписи с применением эллиптических кривых ... 97
5.2.1 Функция вычисления подписи в алгоритме ECDSA ... 99
5.2.2 Функция проверки подписи в алгоритме ECDSA ... 100
5.2.3 Тест алгоритма ECDSA ... 101
Ответы к упражнениям ... 101
Резюме ... 101

6 ***Нахождение криптографически хороших эллиптических кривых*** ... 103
6.1 PARI/gp для эллиптических кривых ... 104

6.1.1 Запуск PARI/gp 104
6.1.2 Эллиптические кривые над конечными полями в PARI/gp 105
6.1.3 Эллиптические кривые в библиотеке libpari 106
6.2 Обыкновенные кривые общего вида 107
6.2.1 Переменные и инициализация 110
6.2.2 Главный цикл 111
6.3 Плохие кривые 113
Ответы к упражнениям 114
Резюме 115

Часть II ИНТЕРЛЮДИЯ 116

7 *Математика полиномов над конечными полями* 118
7.1 Расширение поля 119
7.2 Представление полинома 120
7.3 Сложение полиномов 121
7.4 Служебные функции 123
Ответ к упражнению 125
Резюме 125

8 *Умножение полиномов* 126
8.1 Определение неприводимых полиномов 127
8.2 Неприводимый полином как модуль 128
8.3 Построение матрицы 130
8.4 Код умножения 131
8.4.1 Создание таблицы умножения 131
8.4.2 Умножение полиномов 133
8.5 Разные функции, связанные с умножением 135
Ответы к упражнениям 138
Резюме 138

9 *Вычисление степеней полиномов* 140
9.1 Метод возведения в квадрат и умножения для быстрого вычисления степеней 141
9.2 Код возведения полинома в степень в общем случае 142
9.3 Конкретный пример 144
9.4 Степени простого порядка поля 145
Ответ к упражнению 147
Резюме 147

10 *Деление полиномов по алгоритму Евклида* 148
10.1 Алгоритм Евклида и НОД 149
10.2 Обращение и деление полиномов 152
10.3 Реализация алгоритма Евклида 155
10.4 Код нахождения НОД 156
10.5 Обращение по модулю неприводимого полинома 157

10.6 Деление по модулю простого полинома 159
Ответы к упражнениям 160
Резюме 160

11 *Создание неприводимых полиномов* 161
11.1 Основы теории неприводимых полиномов 162
11.2 Код для нахождения неприводимых полиномов 164
Ответ к упражнению 167
Резюме 167

12 *Извлечение квадратных корней из полиномов* 168
12.1 Математика квадратных корней по модулю неприводимого полинома 169
12.2 Код извлечения квадратных корней по модулю неприводимого полинома 173
12.2.1 Вычисление содержания полинома 174
12.2.2 Функция псевдоделения 174
12.2.3 Вычисление результанта 176
12.2.4 Проверка на квадратичный вычет 178
12.2.5 Функция извлечения квадратного корня из полинома 179
Ответ к упражнению 183
Резюме 183

Часть III СПАРИВАНИЕ 184

13 *Кривые над расширением конечного поля* 186
13.1 Свойства расширения поля 187
13.2 Функции для работы с эллиптическими кривыми 189
13.2.1 Инициализация полиномиальной кривой 190
13.2.2 Служебные функции 191
13.2.3 Вложение точки на полиномиальную кривую 192
13.2.4 Случайная точка на полиномиальной кривой 194
13.2.5 Сложение точек на полиномиальной эллиптической кривой 195
13.2.6 Умножение точки полиномиальной эллиптической кривой 197
13.3 Модельный пример 198
13.3.1 Описание переменных 198
13.3.2 Базовая кривая в модельном примере 200
13.3.3 Кривая над расширением поля в модельном примере 202
Ответ к упражнению 205
Резюме 205

14 *Нахождение эллиптических кривых с малой степенью вложения* 207
14.1 Безопасность расширения полей для спаривания эллиптических кривых 208
14.2 Низкая степень вложения 210

14.3 Комплексное умножение 212
14.4 Факторизация гильбертова полинома класса 213
14.5 Код поиска кривых, пригодных для спаривания 215
14.5.1 Перебор спариваний 215
14.5.2 Нахождение кривой 223
Ответ к упражнению 234
Резюме 234

15 *Общие правила спаривания эллиптических кривых* 235
15.1 Математические правила спаривания эллиптических кривых 236
15.1.1 Правило билинейности для спаривания точек на эллиптической кривой 238
15.1.2 Правило невырожденности в случае бесконечно удаленной точки 239
15.2 Алгоритмы спаривания 240
15.2.1 Функция $h_{PQ}(R)$ 240
15.2.2 Алгоритм Миллера 243
15.3 Подпрограмма, вычисляющая функцию $h_{P,Q}$ 244
15.4 Код алгоритма Миллера 246
Ответы к упражнениям 247
Резюме 248

16 *Спаривание Вейля* 249
16.1 Формула спаривания Вейля 250
16.2 Функции для вычисления спаривания 252
16.3 Демонстрация на примере модельных кривых 255
Ответ к упражнению 260
Резюме 260

17 *Спаривание Тейта* 261
17.1 Математика спаривания Тейта 262
17.2 Реализация спаривания Тейта 263
17.3 Тестирование спаривания Тейта на модельном примере 265
Ответ к упражнению 270
Резюме 270

18 *Мультиподписи BLS* 271
18.1 Введение в мультиподписи 271
18.2 Мультиподписи с агрегированием ключей 273
18.2.1 Хеш-функции, применяемые в алгоритмах агрегирования 274
18.2.2 Алгоритм агрегирования ключей для мультиподписей 276
18.2.3 Математика цифровой мультиподписи и алгоритм проверки 277
18.3 Описание кода мультиподписи 279
18.3.1 Код генерирования ключей 280
18.3.2 Хеш-функции 281
18.3.3 Вычисление хеша открытых ключей a_i 283
18.3.4 Мультиподпись и подпрограммы проверки 286

18.4 Контролируемые подгрупповые мультиподписи 289
18.5 Код подгрупповых мультиподписей 292
18.6 Пример использования множественных подписей BLS 297
18.6.1 Тестовые параметры 297
18.6.2 Генерирование ключей в программе тестирования мультиподписей 299
18.6.3 Моделирование подписания и проверки подписи 302
18.6.4 Программа моделирования создания подгрупповой мультиподписи 306
Ответы к упражнениям 310
Резюме 310

19 *Доказательство знания и хранение секретов: нулевое разглашение с применением спариваний* 312
19.1 Определение SNARK 313
19.2 Что такое квадратичная арифметическая программа 315
19.3 Интерполяционный полином Лагранжа 317
19.4 Главная ссылочная строка 321
19.5 Пример кода zk-SNARK 325
19.5.1 Общие функции в файле snarkbase.c 326
19.5.2 Программа вычисления параметров QAP 336
19.5.3 Создание главной ссылочной строки 338
19.5.4 Построение доказательства знания медицинской карты 343
19.5.5 Проверка медкарты с нулевым разглашением 351
Ответы к упражнениям 353
Резюме 354

Приложение A. Код и инструменты 356
Приложение B. Гильбертовы полиномы классов 361
Литература 365
Предметный указатель 367