

Предисловие	7
Глава 1. Алгоритмы на эллиптических кривых	9
1.1. Алгоритм сложения и удвоения точек	9
1.1.1. Общая схема алгоритма сложения	9
1.1.2. Частные формулы для сложения и удвоения	11
1.1.3. Алгоритмы сложения и удвоения точек эллиптических кривых	17
1.2. Эллиптические кривые над $GF(2^n)$	17
1.2.1. Суперсингулярные кривые	20
1.2.2. Несуперсингулярные кривые	25
1.2.3. Стандарты о выборе кривых для реализации криптосистем на эллиптических кривых	27
1.3. Скалярное умножение на суперсингулярных кривых	31
1.3.1. Вычисление $k \cdot P$ методом аддитивных цепочек	32
1.3.2. Использование проективных координат	35
1.3.3. Метод Монтгомери	37
1.4. Скалярное умножение на несуперсингулярных кривых	39
1.4.1. Метод Монтгомери для несуперсингулярных кривых	40
1.4.2. Метод Монтгомери в проективных координатах	42
1.4.3. Метод Лопеса—Дахаба использования проективных координат	43
1.4.4. Алгоритм скалярного умножения, использующий операцию «ополовинивания»	45
1.5. Скалярное умножение на аномальных кривых	54
1.5.1. Свойства кривых Коблица	54
1.5.2. Использование модулярной редукции	64
1.6. Вычисление дискретного логарифма	72
1.6.1. Проблема дискретного логарифмирования	72
1.6.2. Алгоритм «большой шаг — малый шаг»	72
1.6.3. Алгоритм для групп составных порядков	74
Глава 2. Протоколы на эллиптических кривых	76
2.1. Выбор точки и размещение данных	76
2.1.1. Введение	76
2.1.2. Решение квадратных уравнений	76
2.1.3. Выбор точки эллиптической кривой	81
2.1.4. Размещение данных на эллиптической кривой	82

2.1.5. Определение порядка точки эллиптической кривой и нахождение образующего элемента группы точек эллиптической кривой	83
2.2. Распределение ключей	83
2.2.1. Введение	83
2.2.2. Распределение ключей для классической криптосистемы (протокол Диффи—Хеллмана)	85
2.2.3. Распределение ключей для классической криптосистемы (протокол Мессе—Омуры)	86
2.2.4. Протокол распределения ключей Менезеса—Кью—Венстоуна (MQV-протокол)	90
2.3. Криптосистемы Эль-Гамала	93
2.4. Протоколы цифровой подписи	96
2.4.1. Электронная цифровая подпись	96
2.4.2. Обобщенная схема электронной подписи Эль-Гамала	98
2.4.3. Электронная подпись Эль-Гамала с возвратом сообщения — схема Nyberg—Rueppel	102
2.5. Передача с забыванием	105
2.5.1. Введение	105
2.5.2. Схема некоторых протоколов передачи с забыванием	106
2.5.3. Некоторые частные случаи передачи с забыванием	109
2.5.4. Передача комбинации k из n сообщений с забыванием	112
2.5.5. Применение передачи k из n сообщений с забыванием	115
Глава 3. Криптосистемы на основе спариваний	120
3.1. Билинейная проблема Диффи—Хеллмана	120
3.1.1. Одноразовый протокол генерации общего секретного ключа между тремя участниками	122
3.1.2. Короткая цифровая подпись, основанная на спаривании	122
3.1.3. Криптосистема с публичным индивидуальным ключом	123
3.2. Спаривание Андре Вейля на эллиптических кривых	124
3.2.1. Дивизоры	125
3.2.2. Явное определение спаривания Вейля	128
3.2.3. Функции на гиперэллиптических кривых	130
3.3. Алгоритм вычисления спариваний Вейля и Тейта	136
3.3.1. Усовершенствования алгоритма Миллера	139
3.4. Спаривание Тейта	143
3.4.1. Применение спариваний для логарифмирования в эллиптических кривых	145
3.4.2. Кривые, удобные для спаривания	146
3.4.3. Искажающее отображение	148
3.4.4. Удобные для спаривания кривые с множителем безопасности $k \leq 2$	152
3.4.5. Удобные для спаривания поля	153

3.5. Кривые над полями характеристики три	154
3.5.1. Устранение делений	155
3.6. О больших значениях параметра безопасности	160
3.6.1. Скалярное умножение точек кривой над полем большой характеристики	162
3.6.2. Ускорение алгоритма Миллера для больших k	163
3.6.3. Итерированное удвоение в якобиевых координатах	164
3.6.4. Комбинирование с другими методами	164
3.6.5. Использование аддитивных цепочек с двойной базой	166
3.7. Алгоритм Дуурсма—Ли	168
3.7.1. Алгоритм Дуурсма—Ли над полями характеристики два	174
3.8. Некоторые алгоритмы арифметики конечных полей	176
3.8.1. Извлечение квадратных корней в полях характеристики большой двух	176
3.8.2. Извлечение корней p -й степени в полях характеристики p	177
3.8.3. Один метод компактной записи точек суперсингулярных кривых	180
3.8.4. Арифметика в полях характеристики большей двух	182
3.9. О реализации алгоритма Дуурсма—Ли	188
3.9.1. Использование нормального базиса в поле G	189
3.9.2. Умножение в поле K методом Карацубы	190
3.9.3. Умножение в поле K методом Тоома	191
3.9.4. Возведение в степень p в поле K	192

Приложение А. Алгоритмы с двоичными матрицами 196

А.1. Представление векторов и матрицы	196
А.2. Умножение матрицы на вектор	197
А.3. Алгоритм GAUS-MATRIX-TRIAN	199
А.4. Алгоритм проверки невырожденности матрицы	201
А.5. Приведение матрицы к диагональному виду	202
А.6. Обращение матрицы	204
А.7. Умножение вектор-строки на матрицу	206

Приложение В. Таблицы неприводимых многочленов 208

В.1. Неприводимые многочлены над полем $GF(2)$	208
В.1.1. Неприводимые трехчлены степени n , $2 \leq n \leq 2000$	208
В.1.2. Неприводимые трехчлены вида $1 + X^{n-1} + X^n$ степени n , $2 \leq n \leq 34\,353$	221
В.1.3. Неприводимые пятичлены степени n , $8 \leq n \leq 290$	222
В.2. Неприводимые трехчлены над полем $GF(3)$	223

Приложение С. Таблицы ОНБ	226
С.1. ОНБ размерности n , $2 \leq n \leq 30$	226
С.2. ОНБ размерности n , $30 < n < 1013$	230
С.3. Возможные размерности ОНБ n , $998 < n < 10\,000$	251
Приложение D. Примеры исполнения MQV-протокола	260
Литература	264
Предметный указатель	269
Уточнения и дополнения к первому изданию	275