ВЫСШЕЕ ОБРАЗОВАНИЕ

КРИПТОГРАФИЯ

Безопасные многосторонние вычисления

С. М. Рацеев

ЛАНЬ

E.LANBOOK.COM

Оглавление

Введение **9**

1 Базовые криптографические понятия и примитивы **11**
1.1 Вычислительная неразличимость 11
1.2 Неразличимость при повторных экспериментах 20
1.3 Семейства неоднородных схем 22
1.4 Вычислительная безопасность 23
1.5 Безопасность на примере симметричных шифров . . . 25
1.6 IND-CPA безопасность 28
1.7 IND-CCA безопасность 32
1.8 Схемы электронной подписи 34
1.9 Одноразовые коды аутентификации 36
1.10 Случайный оракул 38
1.11 Схемы обязательств 41
1.12 Подбрасывание монеты 43
1.13 Перестановки с лазейками 44
1.14 Генераторы псевдослучайных чисел 46
1.15 Псевдослучайные функции 49
1.16 Псевдослучайный синтезатор 51

2 Общие сведения по безопасным многосторонним вычислениям **54**
2.1 Многосторонние вычисления 54
2.2 Арифметические схемы на основе многочленов 58
2.3 Модели противника 60

3 Византийское соглашение и широковещательная передача **64**
3.1 Византийское соглашение 64
3.2 Широковещательная передача 67
3.3 Широковещательная передача с прерыванием 74
3.4 Протокол расширения для случая $t < n/3$ 77

3.5 Универсальная хеш-функция 82
3.6 Протоколы расширения для случая $t < n/2$ 83
3.6.1 Информационно-теоретически безопасный протокол 83
3.6.2 Криптографически безопасный протокол 88
3.7 Протоколы расширения широковещательной передачи для случая $t < n$ 90
3.7.1 Криптографически безопасный протокол 91
3.7.2 Информационно-теоретически безопасный протокол 94

4 Безопасность протоколов многосторонних вычислений 99
4.1 Основные параметры 100
4.2 Парадигма «реальный–идеальный» 103
4.3 Случай пассивного противника 107
4.4 Эквивалентное определение безопасности для случая пассивного противника 110
4.5 Случай активного противника 115
4.5.1 Случай двух участников 119
4.5.2 Произвольное число участников. Первая модель . 122
4.5.3 Произвольное число участников. Вторая модель . 125
4.6 Совершенная безопасность 126
4.7 Обобщение пассивного противника 127
4.8 Универсальная компонуемость 130
4.8.1 Безопасная *UC*-реализация функциональности . . 131
4.8.2 Безопасность протокола для случая двух участников 135
4.8.3 Универсальная композиция 138

5 Пассивный противник и честное большинство 140
5.1 Протокол BGW для случая $n \geqslant 2t+1$ 141
5.2 t-конфиденциальность протокола BGW 147
5.3 Метод t-конфиденциального вычисления произведения GRR 155
5.4 Численный пример протокола BGW 158

6 Активный противник и честное большинство 162
6.1 Проверяемые схемы разделения секрета 162
6.2 Пример на проверяемую схему разделения секрета . . 173
6.3 Протокол BGW для случая $n \geqslant 3t+1$ 174

6.4 t-безопасность протокола BGW 186
6.5 Метод t-безопасного вычисления произведения на основе протокола AAPP 190

7 Забывчивая передача 1 из 2 **194**
7.1 Определения безопасности ОТ для случая активного противника 195
7.1.1 Определение безопасности для случая активного противника 195
7.1.2 Ослабленное определение безопасности 198
7.1.3 Односторонняя имитация в определении безопасности 203
7.2 Забывчивая передача на основе асимметричных шифров 204
7.3 Протокол забывчивой передачи Белларе—Микали . . . 211
7.4 Забывчивая передача на основе перестановок с лазейками 212
7.5 Забывчивая передача Наора—Пинкаса на основе предположения DDH 214
7.6 Протокол на основе гомоморфного шифрования 215
7.7 Забывчивая передача с полной защитой от активного противника 218
7.8 Случайная забывчивая передача 219
7.9 Протокол IKNP расширения забывчивой передачи . . . 220
7.10 Стандартное и корреляционное расширения забывчивой передачи 224

8 Забывчивая передача k из n **228**
8.1 Забывчивая передача 1 из n Наора—Пинкаса 228
8.2 Забывчивая передача 1 из n на основе предположения DDH 230
8.3 Забывчивая передача k из n на основе предположения DDH 236

9 Пассивный противник и нечестное большинство **240**
9.1 Протокол GMW для логической схемы 240
9.2 Протокол GMW для арифметической схемы 244
9.3 О схемах над кольцами 245
9.4 Метод IPS для безопасного произведения 246
9.5 Протоколы на основе искаженных схем 251

9.5.1 Искаженные схемы Яо 251
9.5.2 Пример на протокол Яо 259
9.5.3 Протокол BMR 262

10 Парадигма «офлайн–онлайн» 267
10.1 Предварительно обработанные тройки произведений . 267
10.2 Случай пассивного противника и честного большинства 270
10.3 Случай активного противника и честного большинства 277
10.4 Случай пассивного противника и нечестного большинства 286

11 Активный противник и нечестное большинство 287
11.1 Конструкция BDOZ 288
11.2 Конструкция SPDZ 291
11.2.1 Основная идея конструкции SPDZ 291
11.2.2 Операции над долями 293
11.2.3 Протокол безопасных вычислений в режиме онлайн 295

12 Активный противник и два участника 299
12.1 Протокол на основе искаженных схем 299
12.1.1 Описание протокола на высоком уровне 300
12.1.2 Проверка корректности и согласованности 302
12.1.3 Протокол для вычисления функции 307
12.2 Протокол на основе искаженных схем и задачи DDH 313
12.2.1 Обзор функциональности и конструкции 314
12.2.2 Протокол для безопасных двусторонних вычислений 317
12.3 Протокол DGNNT на основе BDOZ и OLE 322
12.3.1 Предварительные вычисления 326
12.3.2 Безопасные двусторонние вычисления 332

13 Три/четыре участника и честное большинство 334
13.1 Протокол AFLNO для случая пассивного противника . 334
13.1.1 Безопасное вычисление логических схем 335
13.1.2 Вычисление схем над кольцами вычетов по модулю 2^n и полями 340

13.1.3 Численный пример протокола AFLNO 344
13.2 Протокол FLNW для случая активного противника . . 347
13.2.1 Подпротоколы основного протокола 352
13.2.2 Безопасное вычисление функциональности 364
13.3 Протокол DEK для четырех участников и активного противника 366

14 Построение протоколов для случая активного противника и честного большинства 375
14.1 Схемы разделения секрета, используемые в протоколе 376
14.2 Сильно линейные схемы разделения секрета 378
14.3 Определение безопасности 380
14.4 Подпротоколы основного протокола 385
14.5 Конструкция основного протокола 389
14.6 Пакетная проверка корректности умножения 394
14.7 Безопасные многосторонние вычисления на основе схемы Шамира 397

15 Протоколы с прерыванием, активным противником и честным большинством 400
15.1 Протокол CGHIKLN 402
15.1.1 Подпротоколы основного протокола 405
15.1.2 Протокол для больших полей 412
15.2 Динамическое расширение поля в протоколах безопасных вычислений 421
15.2.1 Расширение поля и преобразование долей секрета 423
15.2.2 Безопасное вычисление арифметической схемы . 432
15.3 Протокол ADEN над $\mathbb{Z}_{2^m}$ 441
15.4 Протокол Фурукавы—Линделл для случая $n \geqslant 3t+1$ . . 449
15.4.1 Подпротоколы основного протокола 452
15.4.2 Протокол вычисления арифметической схемы . . 461
15.4.3 Модификация протокола Фурукавы—Линделл на основе расширения поля 463
15.5 Эффективный и масштабируемый протокол ATLAS . . 465
15.5.1 Основные идеи протокола ATLAS 465
15.5.2 Подпротоколы основного протокола 475
15.5.3 Вычисление двухуровневой схемы 484
15.5.4 Протокол ATLAS 486
15.5.5 Быстрая пакетная проверка корректности умножения 492

15.6 О проверках тройки произведения на корректность . . 503

16 Протоколы с нулевым разглашением на основе многосторонних вычислений 505

16.1 Интерактивные доказательства 505
16.2 Протоколы IKOS с нулевым разглашением на основе многосторонних вычислений 510
16.2.1 Основные идеи и определения 510
16.2.2 Нулевое разглашение на основе многосторонних вычислений для случая пассивного противника . 513
16.2.3 Нулевое разглашение на основе многосторонних вычислений для случая активного противника . . 518
16.3 Протокол с нулевым разглашением ZKBoo 519

Литература 528