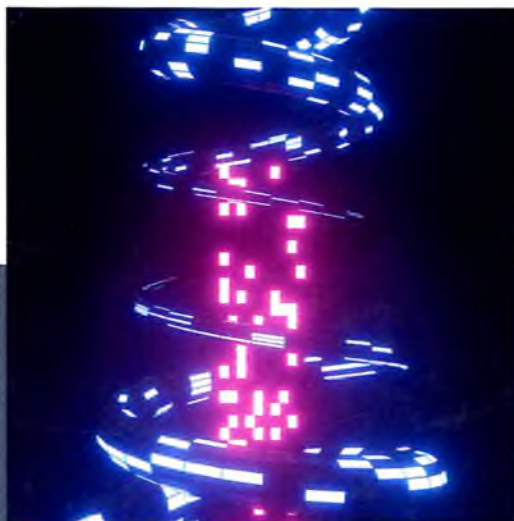


ВЫСШЕЕ ОБРАЗОВАНИЕ

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Схемы разделения секрета



С. М. Рацеев



E.LANBOOK.COM

Оглавление

Введение	6
1 Пороговые схемы разделения секрета	7
1.1 Основные определения и обозначения	7
1.2 Аддитивная схема разделения секрета	13
1.3 Схема разделения секрета Шамира	15
1.4 Свойство совершенности схемы Шамира	20
1.5 Проверяемая схема Фельдмана—Шамира	25
1.6 Совершенная проверяемая схема Педерсена—Шамира .	27
1.7 Схема разделения секрета Блэкли	30
1.8 Реплицированная схема разделения секрета	33
1.9 Схемы разделения секрета на основе ортогональных таблиц	37
1.10 Схема Миньотта	39
1.11 Схема Асмута—Блума	40
1.12 Пороговая модулярная схема разделения секрета в кольце многочленов	42
1.13 Пороговая схема разделения мультисекрета	43
1.14 Рамп-схемы разделения секрета	45
1.15 Расширение схемы Шамира	47
2 Схемы разделения секрета для произвольных структур доступа	53
2.1 Основные определения и обозначения	53
2.2 Структуры доступа, связанные с разбиением множества участников	55
2.3 Схемы разделения секрета для некоторых частных случаев	56
2.4 Схема Ито—Сайто—Нишизеки	57
2.5 Схема Бенало—Лейхтера	61
2.6 Схема Бенало—Рудича	62
2.7 Схема Брикелла	64

2.8	Схема разделения секрета на основе определителей матриц	67
2.9	Схема разделения секрета с заданным на множестве участников отношением порядка	69
2.10	Иерархические схемы разделения секрета	72
2.10.1	Схемы для конъюнктивных иерархических структур доступа	73
2.10.2	Схемы для дизъюнктивных иерархических структур доступа	76
2.11	Монотонные программные линейные оболочки	80
3	Схемы разделения секрета на основе линейных кодов	84
3.1	Историческая справка	84
3.2	Обобщение схемы Шамира с помощью кодов Рида—Соломона	85
3.3	Пороговые схемы разделения секрета на основе кодов МДР	88
3.4	Минимальные кодовые векторы и их свойства	89
3.5	Построение структуры доступа на основе линейных кодов	93
3.6	Структура доступа, связанная с разбиением множества участников	96
3.7	Построение линейного кода, реализующего структуру доступа	99
3.8	Построение линейных кодов на основе некоторых структур доступа	105
3.9	Критерий максимальной неправомерной коалиции	109
3.10	Совершенные проверяемые схемы разделения секрета на основе линейных кодов	111
3.11	Совершенная и идеальная иерархическая схема разделения секрета на основе кодов МДР	112
4	Безопасные многосторонние вычисления	116
4.1	Безопасные многосторонние вычисления	116
4.2	Широковещательная передача	126
4.3	Протокол BGW	133
4.3.1	Случай пассивного противника	134
4.3.2	Метод t -конфиденциального вычисления произведения GRR	140
4.3.3	Случай активного противника	142

4.3.4	Метод t -безопасного вычисления произведения на основе протокола AAPP	152
4.4	Протокол забывчивой передачи	155
4.5	Протокол GMW	156
4.6	Предварительно обработанные тройки произведений	161
4.6.1	Случай пассивного противника	163
4.6.2	Случай активного противника	166
4.6.3	Случай нечестного большинства	174
4.7	Случай активного противника и нечестного большинства	174
4.7.1	Конструкция BDOZ	175
4.7.2	Конструкция SPDZ	179
5	Синхронные проверяемые схемы разделения секрета	186
5.1	Проверяемые схемы разделения секрета	186
5.2	Синхронные схемы разделения секрета	189
5.3	Многочлены от двух переменных	193
5.4	7-раундовый протокол разделения секрета 7BGW	203
5.5	6-раундовый протокол разделения секрета 6KK	209
5.6	5-раундовый протокол разделения секрета 5BGW	212
5.7	4-раундовый протокол разделения секрета 4GIKR	215
5.8	3-раундовый протокол разделения секрета 3GIKR	217
5.9	3-раундовый протокол разделения секрета 3FGGRS-W	220
5.10	3-раундовый протокол разделения секрета 3FGGRS	224
5.11	3-раундовый протокол разделения секрета 3KKK-W	229
5.12	3-раундовый протокол разделения секрета 3KKK	232
5.13	3-раундовый протокол разделения секрета 3AKP	236
5.14	2-раундовый протокол 2GIKR для случая $n > 4t$	238
5.15	1-раундовый протокол 1GIKR-W для случая $n = 5, t = 1$	243
5.16	Протокол разделения мультисекрета AAPP	244
6	Асинхронные и гибридные проверяемые схемы разделения секрета	248
6.1	Асинхронные протоколы разделения секрета	248
6.2	Асинхронный протокол разделения секрета BCG	252
6.3	Асинхронный протокол разделения секрета PCR	256
6.4	Гибридные протоколы разделения секрета	260
6.5	Гибридный протокол разделения секрета PR	262
	Литература	269