Содержание:

1) Симметричная и асимметричная криптография, ЭЦП. Проблемы дискретного логарифмирования и Диффи-Хеллмана. Протокол Диффи-Хеллмана, схема Эль-Гамаля (шифрование и подпись).

2) Алгоритмы дискретного логарифмирования: Полига-Хеллмана, ро-метод и лямбда-метод Полларда, метод исчисления индексов.

3) Плоские особые и неособые (т. е. эллиптические) кубические кривые. Нормальная форма Вейерштрасса, дискриминант, j-инвариант, групповой закон.

4) Взвешенные проективные пространства. Координаты Лопеса-Дахаба, Якоби, братьев Чудновских. Формулы сложения и удвоения в данных координатах и сравнение их сложности.

5) Сжатия точек эллиптических кривых. Псевдогрупповой закон на куммеровой кривой (т. е. на P^1), алгоритм возведения в степень Монтгомери (так называемая лестница Монтгомери). Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG).

6) Формы эллиптических кривых: Лежандра, Гессе, Эдвардса, Хаффа, Якоби (особая квартика в P^2 и пересечение двух квадрик в P^3). Формулы сложения и удвоения на данных формах и сравнение их сложности.

7) Суперсингулярные и обыкновенные эллиптические кривые.

8) Классификация групп E(Fq), алгоритм Миллера, аномальные кривые.

9) Число Fq-точек эллиптических кривых: неравенство Хассе, теорема Ватерхауза. Многочлены деления, алгоритм Шуфа и Шуфа-Элкиса-Аткина (SEA).

10) Изогении: теорема Тэйта, формулы Велу, кольца эндоморфизмов, GLV(Gallant-Lambert-Vanstone)-декомпозиция.

Литература:

1) Silverman J. H. The Arithmetic of Elliptic Curves. Second Edition, 2009.

2) Cohen H., Frey G., Avanzi R., Doche C., Lange T., Nguyen K., Vercauteren F. Handbook of elliptic and hyperelliptic curve cryptography, 2006.

3) Galbraith S. D. Mathematics of public key cryptography, 2012.