### Министерство науки и высшего образования Российской Федерации

1. Санкт-Петербургский политехнический университет Петра Великого
2. —
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 1**

1. **«ГЕНЕРАЦИЯ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ С ЗАДАННЫМ ЧИСЛОМ ТОЧЕК»**
2. по дисциплине «Методы алгебраической геометрии в криптографии»
3. Выполнил
4. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Проверил:
2. старший преподаватель Ярмак А.В.

<*подпись*>

1. Санкт-Петербург
2. 2023

# Цель работы

Изучение способов генерации эллиптической кривой для стандарта электронной цифровой подписи ГОСТ 34.10-2018.

# Порядок выполнения работы

1. Получить у преподавателя задание, содержащее требования к размеру задачи и числу классов . Разработать программу П-1, моделирующую алгоритм генерации эллиптической кривой, параметры которой удовлетворяют требованиям ГОСТ 34.10-2018. Найти образующую циклической подгруппы группы точек эллиптической кривой большого простого порядка *r*.

2. Выбрать две стандартизированные эллиптические кривые и провести их анализ (форму кривой и ее преимущества, длину характеристики поля, число точек, число классов, применение в известных библиотеках, программных решениях, платформах).

# Ход работы

Был выбран дискриминант D = -20330567. Он удовлетворяет условиям . Был реализован алгоритм 1.1 и найдена группа классов {()}, *i = 1,2,…,.* Число классов =3703.

Были найдены *a, b* такие, что – простое число. *a* = 1122163254750825614190870165471914037080, *b* = 163837269953416404312883646079501012881, *p* = 10683863876144140607596037180633903641062677122953791254380615843457373831710272591247, *m* = 10683863876144140607596037180633903641062677121831627999629790229266503666238358554168

С помощью выданного скрипта на Wolfram Mathematica был посчитан полином Вебера и вычислены по его корням j-инварианты в . Среди множества не было j-инвариантов равных 0 и 1728. Выбранный j-инвариант

*j*=2822285505244240609064881573451638766679524945491308869709840817974058286278389768242.

По *j*-инварианту были вычислены коэффициенты *A, B* эллиптической кривой. Уравнение эллиптической кривой выглядит следующим образом:

Далее был подобрана точка, образующая циклическую подгруппу порядка *r*. Вычислена она была следующим образом: выбирается случайная точка на кривой, проверяется ее порядок. Если порядок равен заданному, то вернуть точку, иначе пусть у точки порядок k, домножим точку на , где *r* – нужный нам порядок, *m* – порядок группы точек эллиптической кривой, соответственно, точка выглядит как , тогда точка имеет порядок *r*, вернуть *Q.* Точка имеет координаты (8389710613803362588873720479438378981370144694110365712593180666191521639932692322818 : 9702765860223458806634239656267150970951408754898442490451198392795073710056650211626 : 1)

Далее описаны две выбранные стандартизированные кривые.

Эллиптическая кривая E-382 – скрученная кривая в форме Эдвардса, задающаяся уравнением . Преимуществом кривых в форме Эдвардса является однородный закон сложения. В общем виде он представлен на рисунке 1. Тем самым, кривые в такой форме защищены от атаки по побочным каналам.

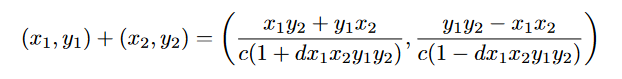


Рисунок 1 – закон сложения для кривой в форме Эдвардса

Характеристика поля p = 2^382 – 105. Число точек 9850501549098619803069760025035903451269934817616361666982952138230652218258596685050637306732978417384336324189284. Циклическая подгруппа простого порядка r = 2462625387274654950767440006258975862817483704404090416745738034557663054564649171262659326683244604346084081047321. Используется в протоколе TLS. Реализацию также можно найти в RELIC Toolkit.

Эллиптическая кривая M-511 – кривая в форме Монтгомери, задающаяся уравнением . Характеристика поля p = 2^511 – 187, число точек 6703903964971298549787012499102923063739682910296196688861780721860882015036859286439014235064444070097128474067979591479896420070205009299687445903538392, циклическая подгруппа простого порядка r = 8379879956214123187233765623878653829674603637870245861077225902

32610251879607410804876779383055508762141059258497448934987052508775626162460930737942299. Используется также в TLS. В форме Монтгомери есть возможность выполнять умножение точки на число за фиксированное время, благодаря лестнице Монтгомери. Так как умножение происходит за фиксированное число операций, то кривые в такой форме также защищены от атак по побочным каналам.

# Ответы на контрольные вопросы

1. Что такое группа классов? Как задается поле классов мнимого квадратичного порядка?

Группа классов мнимого квадратичного порядка – конечная абелева группа, заданная на эквивалентности моноидов идеалов мнимого квадратичного порядка. Поле классов мнимого квадратичного порядка — это квадратное расширение исходного поля с помощью корня где *D*<0, *D*-свободное от квадратов. *D* называют дискриминантом квадратичного поля.

2. Как выполняется переход к скрученной кривой?

Переход с скрученной кривой происходит с помощью домножения коэффициентов кривой на квадратичный невычет *t:*

3. Найти мнимый квадратичный порядок с числом классов не менее 10 и вычислить для него полином .

D = -191, h=13

x^13 + 7178874489555770070\*x^12 - 14412129900790076822258611\*x^11 + 51536266750679803854633551771840260203\*x^10 - 103386239396269087020741974285554789917453508\*x^9 + 199518440359885837424153227327826660336955370546108\*x^8 - 14768638405830894134972427622171024141266129942650181658\*x^7 + 541808230910284083390456000848314355028531599104942728173485\*x^6 - 832818220571586800392164744000358270319532131590078379471735694\*x^5 + 15253788701960481284921391493158919700255797559466559311296323232498\*x^4 - 49375911707911743432917242207615322174325427611237741682026488846612521\*x^3 + 14061234326903814621176226216076159779271092623995827091347309743554898127\*x^2 + 42312753036411362230230450305478672870803475782951657706005442304434341869586\*x + 58256749348304523248144969888837463340160093969294532742146556156000521034802783

# Выводы

В результате работы была написана программа, генерирующая параметры эллиптической кривой для стандарта электронной цифровой подписи ГОСТ Р 34.10–2018. Также был проведен анализ двух эллиптических кривых: M-511 и E-382.