### 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 № 4**

1. **«Вычисление спаривания Вейля на эллиптических кривых»**
2. по дисциплине «Методы алгебраической геометрии в криптографии»
3. Выполнил
4. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Проверил:
2. старший преподаватель, к.т.н. Ярмак А.В.

<*подпись*>

1. Санкт-Петербург
2. 2023

# Цель работы

Изучение свойств спаривания Вейля и Тейта на эллиптических кривых, реализация протокола на билинейных отображениях

# Порядок выполнения работы

1. Получить у преподавателя вариант задания и разработать программу П-1, которая:

* Генерирует с помощью параметризации эллиптическую кривую E с вычислимой степенью расширения для спаривания Вейля и Тейта;
* Находит точки порядка r с координатами из простого и расширенного поля, выполняет построение подгруппы E[r] группы кручения, где r – простое число;
* Для точек из E[r] с помощью алгоритма Миллера вычисляет значения спаривания Вейля и Тейта, проверяет их свойства

2. Разработать программу П-2, которая, согласно варианту, реализует один из протоколов на билинейных отображениях (протокол трехстороннего установления ключа)

# Ход работы

Буду строить группу кручения для расширения степени k=10.

Были вычислены p- характеристика простого поля, T-след эндоморфизма Фробениуса и r- циклическая подгруппа заданного порядка.

p = 22008278923, T = 296703, r=22007982221. С помощью следа был построен дискриминант D = -445483 и вычислена функция Гильберта. Получив корни, была сгенерирована кривая с заданными характеристиками. A = 18733376401, B=19825010575. Была найдена точка порядка r, которая будет являться образующей циклической подгруппы.

Далее строю расширение степени k поля характеристики p и также нахожу образующую порядка r.

Так как r- большое, то невозможно представить группу кручения в виде полной таблицы. Поэтому была сгенерирована таблица 10x10.

Таблица 1 – часть группы кручения

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 0P | 1P | 2P | 3P | 4P |
| 0Q | (0 : 1 : 0) | 6211720554\*a^9 + 10934984804\*a^8 + 3495644028\*a^7 + 5470476817\*a^6 + 5135484203\*a^5 + 9412348364\*a^4 + 9550385695\*a^3 + 12707671300\*a^2 + 8678213144\*a + 21688417353 : 13814923814\*a^9 + 6628670129\*a^8 + 5841984842\*a^7 + 8258607983\*a^6 + 6024419742\*a^5 + 12720170103\*a^4 + 6740441510\*a^3 + 17801889791\*a^2 + 10769854621\*a + 5408331243 : 1) | (6845569790\*a^9 + 15689741452\*a^8 + 218086034\*a^7 + 12965002890\*a^6 + 8811916966\*a^5 + 13329152100\*a^4 + 11474056744\*a^3 + 13609343294\*a^2 + 4551760600\*a + 12213516099 : 16073947093\*a^9 + 15132938833\*a^8 + 19655613421\*a^7 + 20162788763\*a^6 + 21580804538\*a^5 + 9680102320\*a^4 + 16240354380\*a^3 + 3828381248\*a^2 + 11107528194\*a + 17467995710 : 1) | (1622342517\*a^9 + 7074953152\*a^8 + 979112677\*a^7 + 6459357552\*a^6 + 9567803554\*a^5 + 8769115754\*a^4 + 14277314604\*a^3 + 14598122093\*a^2 + 16537022003\*a + 7233854735 : 13182622151\*a^9 + 18202015541\*a^8 + 13204278643\*a^7 + 5567529692\*a^6 + 4996216646\*a^5 + 19404804710\*a^4 + 18202758599\*a^3 + 21480965546\*a^2 + 17022812402\*a + 19827683486 : 1) | (14014245951\*a^9 + 5318721246\*a^8 + 17737478628\*a^7 + 18397650875\*a^6 + 18524072240\*a^5 + 19379252867\*a^4 + 11992313868\*a^3 + 16430339409\*a^2 + 6862834974\*a + 3747960574 : 6426860433\*a^9 + 21204289391\*a^8 + 15097169672\*a^7 + 16382299973\*a^6 + 21574607082\*a^5 + 17689699642\*a^4 + 18150834628\*a^3 + 9999329601\*a^2 + 3717623229\*a + 12328036461 : 1) |
| 1Q | (14922612971 : 17307217900 : 1) | (8047261055\*a^9 + 17258876752\*a^8 + 19481075569\*a^7 + 12098006647\*a^6 + 19601704515\*a^5 + 10267969836\*a^4 + 9318544569\*a^3 + 6582290962\*a^2 + 20295471404\*a + 9836344569 : 12299715905\*a^9 + 15433789810\*a^8 + 1931713068\*a^7 + 683164532\*a^6 + 5154892184\*a^5 + 20786060132\*a^4 + 5579874583\*a^3 + 20240352062\*a^2 + 5697604449\*a + 1826269443 : 1) | (17817950763\*a^9 + 13974690806\*a^8 + 3531083461\*a^7 + 18663391257\*a^6 + 3177757937\*a^5 + 12364472408\*a^4 + 19161391056\*a^3 + 7069287342\*a^2 + 17084285047\*a + 19179928718 : 19860607955\*a^9 + 9974828575\*a^8 + 8696727273\*a^7 + 3521010660\*a^6 + 5170592588\*a^5 + 14227333410\*a^4 + 16910250012\*a^3 + 2592568229\*a^2 + 15464624868\*a + 758735995 : 1) | (11292932234\*a^9 + 2555319535\*a^8 + 16179060496\*a^7 + 15929099641\*a^6 + 1263666358\*a^5 + 8790679121\*a^4 + 4156432043\*a^3 + 18199237147\*a^2 + 6752014613\*a + 5323349495 : 10232759044\*a^9 + 13401094086\*a^8 + 11994851806\*a^7 + 15239588394\*a^6 + 2304041841\*a^5 + 7612348809\*a^4 + 16158626524\*a^3 + 10039653269\*a^2 + 9931555016\*a + 2281202138 : 1) | (19448335843\*a^9 + 6866531999\*a^8 + 5440101153\*a^7 + 4076988152\*a^6 + 15718002738\*a^5 + 8081687550\*a^4 + 18201813931\*a^3 + 10695702150\*a^2 + 6263303394\*a + 20428814021 : 17773362056\*a^9 + 21934593859\*a^8 + 9498064526\*a^7 + 12954637499\*a^6 + 3651749036\*a^5 + 19394156747\*a^4 + 13302076657\*a^3 + 20091695698\*a^2 + 16228061036\*a + 10756519987 : 1) |
| 2Q | (12561331313 : 14390358538 : 1) | (16171015503\*a^9 + 3671706258\*a^8 + 855797024\*a^7 + 15048437644\*a^6 + 1816740135\*a^5 + 1495859237\*a^4 + 9041822997\*a^3 + 11211421425\*a^2 + 10871330666\*a + 17080581002 : 9355726988\*a^9 + 16615152867\*a^8 + 11409648392\*a^7 + 9271500682\*a^6 + 16974664609\*a^5 + 8709929334\*a^4 + 13631300997\*a^3 + 14898866489\*a^2 + 21539213333\*a + 19515355633 : 1) | (2456787869\*a^9 + 2354245021\*a^8 + 2460317688\*a^7 + 8623957501\*a^6 + 17714179330\*a^5 + 1318660794\*a^4 + 12154036073\*a^3 + 17818676205\*a^2 + 8393997062\*a + 20050692472 : 1726364476\*a^9 + 4847000408\*a^8 + 148076795\*a^7 + 3865746979\*a^6 + 14761076240\*a^5 + 2584512025\*a^4 + 5118399646\*a^3 + 6930694979\*a^2 + 14769041724\*a + 15619153092 : 1) | (21405717753\*a^9 + 21036727510\*a^8 + 20144849330\*a^7 + 21091173653\*a^6 + 20520619522\*a^5 + 16111925073\*a^4 + 4433333140\*a^3 + 16523750727\*a^2 + 16188082367\*a + 16582568327 : 17444834151\*a^9 + 16242898933\*a^8 + 20171041826\*a^7 + 16952391300\*a^6 + 6879769159\*a^5 + 3096052589\*a^4 + 7319228188\*a^3 + 20679572440\*a^2 + 10623499711\*a + 15590764658 : 1) | (15181878644\*a^9 + 542018857\*a^8 + 2359367340\*a^7 + 20368659187\*a^6 + 11849171086\*a^5 + 18963757675\*a^4 + 6830347211\*a^3 + 4258914713\*a^2 + 19495085786\*a + 17019964306 : 5814536121\*a^9 + 4244402512\*a^8 + 1395998575\*a^7 + 21636685606\*a^6 + 3478711227\*a^5 + 11326131185\*a^4 + 17434146876\*a^3 + 4589855778\*a^2 + 881276563\*a + 18642273167 : 1) |
| 3Q | (9784727779 : 18922318180 : 1) | (14043875349\*a^9 + 2887787131\*a^8 + 14652522204\*a^7 + 7656348366\*a^6 + 11467176049\*a^5 + 17866738971\*a^4 + 3255176709\*a^3 + 8068672916\*a^2 + 59528980\*a + 6904209851 : 17276710546\*a^9 + 18474574684\*a^8 + 8532860925\*a^7 + 6998236918\*a^6 + 18738289891\*a^5 + 4072787764\*a^4 + 8473756313\*a^3 + 3647446485\*a^2 + 14142834508\*a + 17429905720 : 1) | (9829517621\*a^9 + 14927716455\*a^8 + 14552222797\*a^7 + 8889671833\*a^6 + 9068994227\*a^5 + 7054633005\*a^4 + 13431748845\*a^3 + 1395185665\*a^2 + 18011932734\*a + 13685212077 : 15841308618\*a^9 + 9734821075\*a^8 + 6370236866\*a^7 + 13836281878\*a^6 + 13714044247\*a^5 + 4794951007\*a^4 + 789940165\*a^3 + 15160129760\*a^2 + 8491754673\*a + 6780478086 : 1) | (6146907393\*a^9 + 18752113302\*a^8 + 6831419257\*a^7 + 17640516166\*a^6 + 16998802816\*a^5 + 2643430162\*a^4 + 8846257904\*a^3 + 10915004631\*a^2 + 13425748147\*a + 4121478405 : 17125772443\*a^9 + 4265101651\*a^8 + 19234426614\*a^7 + 15010761442\*a^6 + 19322998099\*a^5 + 21647542256\*a^4 + 2057123532\*a^3 + 12632212553\*a^2 + 21292105144\*a + 6430490655 : 1) | (6293055662\*a^9 + 13554325771\*a^8 + 21709232654\*a^7 + 19678038426\*a^6 + 19045488760\*a^5 + 14938079807\*a^4 + 3234987054\*a^3 + 6572172776\*a^2 + 2675789885\*a + 5329425743 : 5057770397\*a^9 + 9585278837\*a^8 + 17724779221\*a^7 + 2248514265\*a^6 + 21163014172\*a^5 + 13881427193\*a^4 + 4629941319\*a^3 + 10211460647\*a^2 + 6365156724\*a + 2418747564 : 1) |
| 4Q | (18214324769 : 131770217 : 1) | (16456508070\*a^9 + 794646798\*a^8 + 18781811498\*a^7 + 12859865885\*a^6 + 8621926957\*a^5 + 9038850654\*a^4 + 2259893887\*a^3 + 4847610830\*a^2 + 6318898073\*a + 2453214349 : 7385035626\*a^9 + 8822668311\*a^8 + 6792682320\*a^7 + 14634645305\*a^6 + 11642567210\*a^5 + 3738002895\*a^4 + 11046911026\*a^3 + 17513373656\*a^2 + 16111921549\*a + 11871887465 : 1) | (9418477475\*a^9 + 14870970698\*a^8 + 21936580109\*a^7 + 18857544222\*a^6 + 18064318026\*a^5 + 9782857665\*a^4 + 9235032080\*a^3 + 2338715136\*a^2 + 15113967756\*a + 17137416957 : 4267016641\*a^9 + 19999501448\*a^8 + 20208298982\*a^7 + 861590144\*a^6 + 18497112943\*a^5 + 21245918059\*a^4 + 2212076897\*a^3 + 17035236194\*a^2 + 7812968498\*a + 14608981670 : 1) | (21950026254\*a^9 + 9847068930\*a^8 + 2496652466\*a^7 + 11314870027\*a^6 + 20289886572\*a^5 + 1983825530\*a^4 + 5040070590\*a^3 + 12771667645\*a^2 + 869878096\*a + 14100982748 : 18202008169\*a^9 + 19473991477\*a^8 + 5303793383\*a^7 + 19455919317\*a^6 + 2937509786\*a^5 + 3582377202\*a^4 + 16268495133\*a^3 + 18945112494\*a^2 + 18634350171\*a + 16809684685 : 1) | (3127454678\*a^9 + 3452189678\*a^8 + 12485616904\*a^7 + 8458749090\*a^6 + 3422486274\*a^5 + 13361659479\*a^4 + 2719144323\*a^3 + 11905086009\*a^2 + 17782617802\*a + 19034441530 : 7724081537\*a^9 + 4376569919\*a^8 + 5979883812\*a^7 + 10970897298\*a^6 + 13161520538\*a^5 + 8203487569\*a^4 + 10439571000\*a^3 + 10932330541\*a^2 + 2643964279\*a + 14365042722 : 1) |

Далее был реализован трехсторонний протокол установления ключа на основе спаривания Вейля. Общеизвестными являются E-эллиптическая кривая, отображение спаривания, точки P и Q, а также передаваемые по каналу связи списки [aP, aQ], [bP, bQ], [cP, cQ], где a, b, c- секретные данные пользователя.

Реализуется протокол следующим образом. Есть три пользователя A, B, C. Каждый выбирает случайное число и умножает на него точки P и Q. Далее каждый отправляет эти точки соседям по каналу связи. После этого этапа у каждого пользователя есть свое случайное число и по паре точек от 2 других пользователей. Общий секрет пользователь A вычисляет по следующей формуле

Аналогично для пользователей B и C.

На рисунке 1 представлена схема с передачей только одной точки вместо двух.

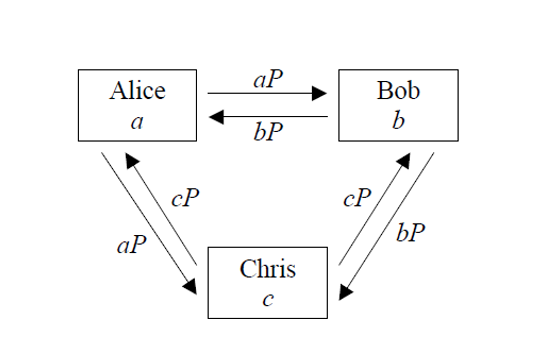


Рисунок 1 – схема трехстороннего протокола установления ключа

Были попытки протестировать написанный протокол на сертифицированной эллиптической кривой. Удалось проверить только на кривой mnt1. На остальных не получилось, так как не удавалось найти образуюшую точку порядка r в расширении поля, необходимую для спаривания Вейля. Были попытки построить кривую семейства BN для заданного параметра z. Для z длины 20 бит удалось построить кривую и проверить на ней работоспособность протокола, на остальных столкнулся с той же проблемой поиска образующей.

# Ответы на контрольные вопросы

1. Что такое спаривание Вейля и как оно вычисляется?

Спаривание Вейля это отображение *-*корень степени m из 1 в поле расширения.

На практике оно вычисляется как *, где S и T-* точки кручения кривой *E(L), –* функции на кривой с дивизором

2. Какие эллиптические кривые используются для эффективного вычисления билинейных отображений?

Эллиптические кривые, для которых размер k в расширенного поля достаточно мало. На практике рассматривают значения k меньше 100.

3. Почему для спаривания Тейта не выполняется свойство знакопеременности?

-

4. Что такое параметр безопасности? Каким требованиям он должен удовлетворять для эллиптических кривых, используемых в криптосистемах на основе задачи дискретного логарифмирования?

Чтобы уровень безопасности в группе точек и в был одинаковый, размер расширенного поля должен быть значительно больше r. Отношение этих размеров определяет параметр безопасности k и отношение . Параметр безопасности рассматривается по отношению к атаке -методом Полларда.

# Выводы

В данной лабораторной работе была построена группа кручения порядка и на ее основе проверены свойства спаривания Вейля и Тейта. Также был реализован протокол установления ключа с помощью спаривания Вейля.