

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«Российский технологический университет»**

**МИРЭА**

Институт кибернетики

**Кафедра информационной безопасности**

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

по дисциплине

«Криптографические протоколы»

На тему:

**«Реализация ЭЦП. ЭЦП ECDSA (Prime Field)»**

**Подготовил**

студент группы ККСО−01−14 А.С. Першин

**Руководитель работы**

А.П. Никитин

Москва, 2019

Оглавление

[1. Описание 3](#_Toc3061864)

[2. Рекомендации NIST по выбору эллиптических кривых 3](#_Toc3061865)

[3. Эллиптические кривые над простыми полями *GF(p)* 4](#_Toc3061866)

[4. Математические операции над эллиптическими кривыми 6](#_Toc3061867)

[5. Параметры пользователя 7](#_Toc3061868)

[6. Формирование цифровой подписи 7](#_Toc3061869)

[7. Проверка цифровой подписи 8](#_Toc3061870)

[8. Российские параметры для эллиптических кривых над *GF(p)* 8](#_Toc3061871)

[9. Результаты реализации алгоритма ECDSA 9](#_Toc3061872)

[Литература 11](#_Toc3061873)

# Описание

Стойкость алгоритма цифровой подписи (далее - ЦП) основывается на проблеме дискретного логарифма в группе точек эллиптической кривой. В отличие от проблемы простого дискретного логарифма и проблемы факторизации целого числа, не существует субэкспоненциального алгоритма для проблемы дискретного логарифма в группе точек эллиптической кривой. По этой причине «сила на один бит ключа» существенно выше в алгоритме, который использует эллиптические кривые.

Д. Брауном (Daniel R. L. Brown) было доказано, что алгоритм ECDSA не является более безопасным, чем DSA. Им было сформулировано ограничение безопасности для ECDSA, которое привело к следующему заключению:

«Если группа эллиптической кривой может быть смоделирована основной группой и её хеш-функция удовлетворяет определенному обоснованному предположению, то ECDSA устойчива к атаке на основе подобранного открытого текста с существующей фальсификацией.»

Алгоритм ECDSA в 1999 г. был принят как стандарт ANSI, в 2000 г. — как стандарт IEEE и NIST. Также в 1998 г. алгоритм был принят стандартом ISO. Несмотря на то, что стандарты ЦП созданы совсем недавно и находятся на этапе совершенствования, одним из наиболее перспективных из них на сегодняшний день является ANSI X9.62 ECDSA от 1999 — DSA для эллиптических кривых. На данный момент базовым американским стандартом, описывающим ECDSA, является стандарт от июня 2013 года NIST FIPS PUB 186-4 «Digital Signature Standard».

В Российской Федерации с 2001 года существует стандарт, описывающий процессы формирования и проверки ЭЦП, его последней редакцией является ГОСТ 34.10-2012 «Процессы формирования и проверки электронной цифровой подписи».

# Рекомендации NIST по выбору эллиптических кривых

NIST рекомендует выбирать эллиптические кривые трех видов:

- Псевдослучайная кривая над полем *GF(p)*, где *p* – простое;

- Псевдослучайная кривая над полем *GF(2m)*;

- Псевдослучайная кривая над полем *GF(2m)*, названные кривыми *Koblitz* или аномальные двоичные кривые.

Каждая эллиптическая кривая имеет базовую точку порядка *n*, где *n* – порядок подгруппы группы точек эллиптической кривой. Такая точка в стандарте NIST называется базовой точкой. Каждая кривая имеет свою базовую точку .

В реализации ЦП в данной работе будет использоваться реализация арифметики для эллиптической кривой над полем *GF(p)*.

# Эллиптические кривые над простыми полями *GF(p)*

Для каждого простого *p* существует псевдослучайная кривая



простого порядка *n*. Различные виды рекомендованных псевдослучайных кривых приведены в стандарте NIST, где для всех кривых параметр *a* (коэффициент при *x*) равен «-3».

Каждая кривая описывается параметрами:

- простым модулем *р*;

- порядком подгруппы точек эллиптической кривой *n*;

- коэффициентом *b*, таким, что:



- координатой *x* базовой точки ;

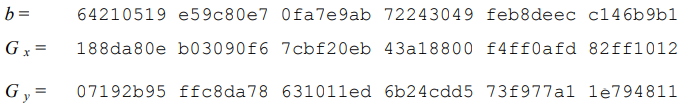
- координатой *y* базовой точки ;

Параметр *n* обладает следующим свойством: *nG = O* (нулевая точка). Описание операций над точками эллиптической кривой приведены в следующем разделе.

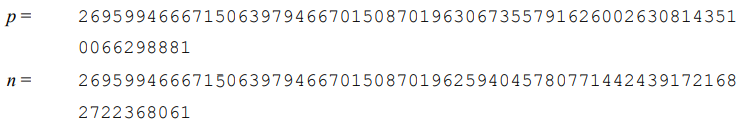
Параметры *p* и *n* представлены в стандарте в десятичной форме, остальные представляются в шестнадцатеричной системе счисления.

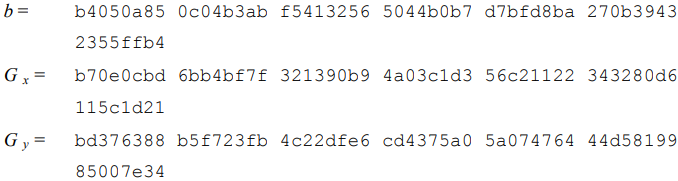
*Кривая NIST P-192*



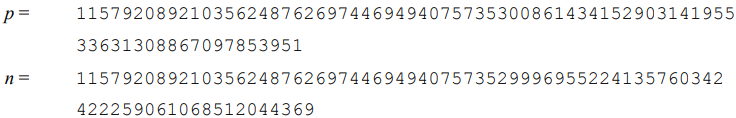


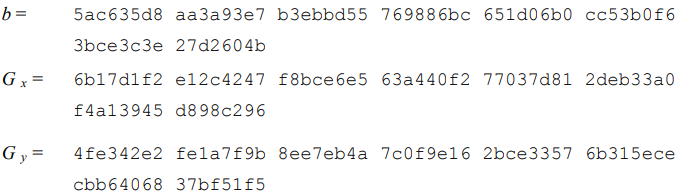
*Кривая NIST Р-224*



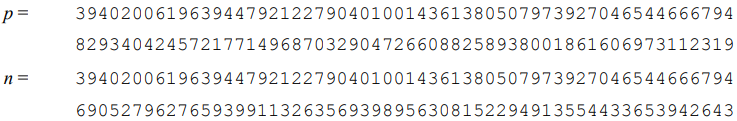


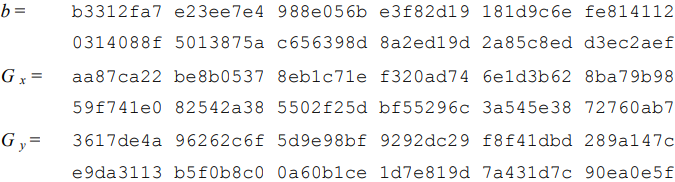
*Кривая NIST Р-256*



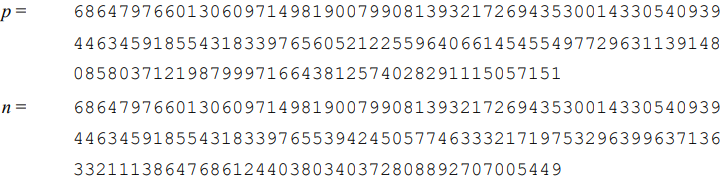


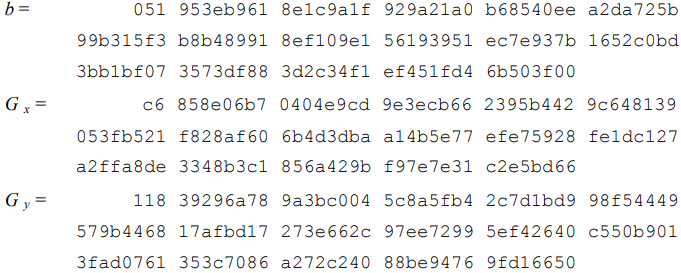
*Кривая NIST Р-384*





*Кривая NIST Р-521*

**



В стандарте ГОСТ Р 34.10-2012 приведены два типа эллиптических кривых Р-256 и Р-512, которые задаются следующими параметрами, представленными в десятичной системе счисления:

*Кривая ГОСТ Р-256*

*a =* 7

*p =* 57896044618658097711785492504343953926634992332820282019728792003956564821041

*n* = 57896044618658097711785492504343953927082934583725450622380973592137631069619

*b* = 43308876546767276905765904595650931995942111794451039583252968842033849580414

*Gx* = 2

*Gy* = 4018974056539037503335449422937059775635739389905545080690979365213431566280

*Кривая ГОСТ Р-512*

*a =* 7

*p =* 36239861022290036359077887536838743060213209255346786050865

46150450856166624002482588482022271496854025090823603058735

1637342638 22371964987228582907372403

*n* = 36239861022290036359077887536838743060213209255346786050865

46150450856166623969164898305032863068499961404079437936585

455865192212970734808812618120619743

*b* = 15186550692108285345089500347140431549287475277402064361940

18823352809982443793732829756914785974674866041605397883677

596626326413990136959047435811826396

*Gx* = 1928356944067022849399309401243137598997786635459507974357

0754913077665926858354410655576810031848748196580049032123

32884252335830250729527632383493573274

*Gy* = 22887286933719728599700121555294784163535623273295061803  
 14497425931102860301572814141997072271708807066593850650

334152381857347798885864807605098724013854

# Математические операции над эллиптическими кривыми

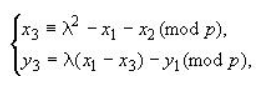
Парой (*x*, *y*), где *x* и *y* – элементы поля *GF(p)* и удовлетворяющие уравнению эллиптической кривой *E* называются точками эллиптической кривой *E*, а *x* и *y* координатами этой точки.

Точка эллиптической кривой обозначается как *C*(*x, y*) или просто *C*.

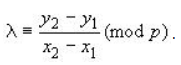
Две точки эллиптической кривой *С1*(*x1, y1*) и *С2*(*x2, y2*) равны, если равны их соответствующие координаты (*С1* = *С2*, если *x1* = *x2* и *y1* = *y2*).

На множестве точек эллиптической кривой *E* операцию сложения обозначают знаком «+». Для двух произвольных точек *С1*(*x1, y1*) и *С2*(*x2, y2*) эллиптической кривой *Е* рассматривают несколько случаев:

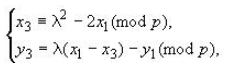
1. Для точек *С1*(*x1, y1*) и *С2*(*x2, y2*), координаты которых удовлетворяют условию *x1* ≠ *x2*, их суммой называется точка *С3*(*x3, y3*), координаты которой определяются сравнениями:



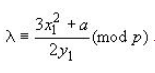
Где:



1. Для точек *С1*(*x1, y1*) и *С2*(*x2, y2*), координаты которых удовлетворяют условию *x1* = *x2* и *y1* = *y2* ≠ 0, их суммой называется точка *С3*(*x3, y3*), координаты которой определяются сравнениями:



Где:



1. Для точек *С1*(*x1, y1*) и *С2*(*x2, y2*), координаты которых удовлетворяют условию *x1* = *x2* и *y1* = *y2*(*mod p*), их суммой называется точка *С3*(*x3, y3*) = *O* – нулевой точкой без определения её *х* и *у* координат. В этом случае точка *С2* называется отрицанием точки *С1*. Для нулевой точки *O* выполнены равенства:

*С* + *О* = *О + С = С*,

Где:

*С* – произвольная точка эллиптической кривой *E*.

Относительно введенной операции сложения множество точек эллиптической кривой *E* вместе с нулевой точкой образуют конечную абелевую (коммутативную) группу порядка *m*, для которого выполнено неравенство:



Точка *C* называется точкой кратности *k* или просто кратной точкой эллиптической кривой *E*, если для некоторой точки *Р* выполнено равенство:



# Параметры пользователя

Каждый пользователь схемы ЦП должен обладать личными параметрами:

- ключом подписи – целым числом *d*, удовлетворяющим неравенству:



- ключом проверки подписи – точкой эллиптической кривой *Q* с координатами (*xQ*, *yQ*) удовлетворяющая равенству:



# Формирование цифровой подписи

Для получения цифровой подписи под сообщением *М* необходимо выполнить следующие шаги:

1. Вычислить хеш-значение сообщения *М*:



1. Вычислить целое число *e*:



Если *e* = 0, то определить *e* = 1.

1. Получить случайное (псевдослучайное) целое число *k*, удовлетворяющее неравенству:



1. Вычислить точку эллиптической кривой *С = kG* и определить:

,

Где: *xC*– *x* координата точки *С*.

Если *r* = 0, то вернуться к шагу 3).

1. Вычислить значение:



Если *s* = 0, то вернуться к шагу 3).

1. Определить цифровую подпись: как два выходных параметра *r* и *s*.

Исходными данными данного процесса являются ключ подписи *d* и подписываемое сообщение *М*, а выходным результатом – цифровая подпись в виде двух параметров *r* и *s*.

# Проверка цифровой подписи

Для проверки цифровой подписи под полученным сообщением *M* необходимо выполнить следующие шаги:

1. Получение параметров *r* и *s* – цифровой подписи сообщения *М*. Если выполнены неравенства  и , то перейти к следующему шагу. В противном случае подпись неверна.
2. Вычислить хеш-значение полученного сообщения *М*:



1. Вычислить целое значение *е*:



Если *e* = 0, то определить *e* = 1.

1. Вычислить значение:



1. Вычислить значения:



1. Вычислить точку эллиптической кривой  и определить:



Где: *xC*– *x* координата точки *С*.

1. Если выполнено равенство , то подпись принимается, в противном случае – подпись неверна.

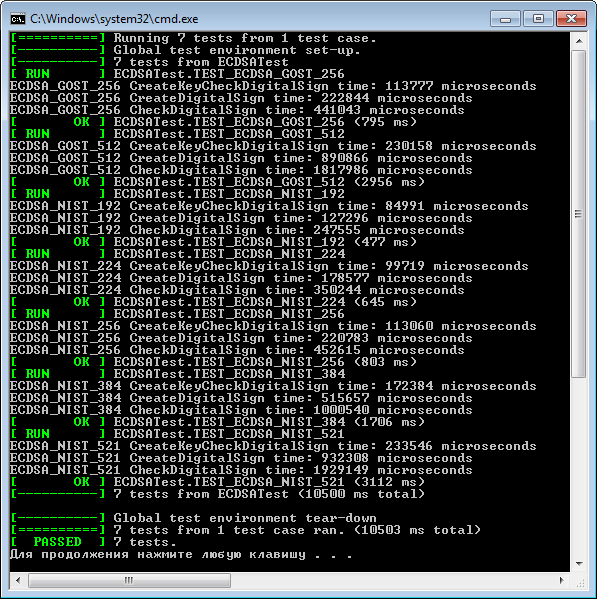
Исходными данными этого процесса являются подписанное сообщение *М*, цифровая подпись в виде двух параметров *r* и *s*, а также ключ проверки подписи *Q*, а выходным результатом – свидетельство о достоверности или ошибочности данной подписи.

# Результаты реализации алгоритма ECDSA

Разработка производилась в IDE Microsoft Visual Studio 15 Pro. Для реализации задания лабораторной работы было создано общее решение с именем CryptoProtocols. Реализация алгоритма ЦП ECDSA входит в проект ECDSA решения CryptoProtocols.

Для тестирования корректности разрабатываемых проектов в решении CryptoProtocols был создан отдельный проект GoogleTestingSolutionProject модульного тестирования gtest (для unit testing) и gmock (для проверки корректности вызовов методов). Данные пакеты устанавливались через менеджер пакетов NuGet для Visual Studio.

Результат выполнения тест кейсов для проверки корректности работы формирования и проверки ЦП на различных видах кривых NIST и GOST, а также фиксация времени выполнения отдельных элементов в процессе ЦП (т.к. gtest замеряет работу вызовов кейсов в микросекундах, то для повышения точности была использована библиотека <chrono> c++11 с точностью до микросекунд) приведены на Рис. 1.



**Рис. 1.** Результат тестирования реализованного алгоритма ECDSA

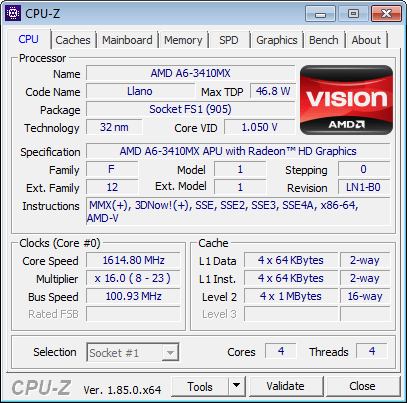
Запускался тест на ЦП AMD A6-3410MX (4 ядра, 4 потока) на Рис.2. По полученным данным увидим:

- время выработки ключа проверки ЦП (*Q*);

- время создания ЦП;

- время проверки ЦП.

для данного ЦП. Данные приведены в Табл. 1.



**Рис. 2.** ЦП AMD A6-3410MX (4 ядра, 4 потока)

**Табл. 1.** Скорость выполнения операций ЦП

|  |  |  |  |
| --- | --- | --- | --- |
| Используемая хеш-функция | | Выработка ключа проверки ЦП / Создание ЦП/ Проверка ЦП | Скорость  [секунд] |
| *Кривая ГОСТ Р-256* | | | |
| SHA-512 | Выработка ключа проверки ЦП | | 0,114 |
| SHA-512 | Создание ЦП | | 0,223 |
| SHA-512 | Проверка ЦП | | 0,441 |
| *Кривая ГОСТ Р-512* | | | |
| SHA-512 | Выработка ключа проверки ЦП | | 0,230 |
| SHA-512 | Создание ЦП | | 0,891 |
| SHA-512 | Проверка ЦП | | 1,818 |
| *Кривая NIST P-192* | | | |
| SHA-512 | Выработка ключа проверки ЦП | | 0,085 |
| SHA-512 | Создание ЦП | | 0,127 |
| SHA-512 | Проверка ЦП | | 0,248 |
| *Кривая NIST P-224* | | | |
| SHA-512 | Выработка ключа проверки ЦП | | 0,100 |
| SHA-512 | Создание ЦП | | 0,179 |
| SHA-512 | Проверка ЦП | | 0,350 |
| *Кривая NIST P-256* | | | |
| SHA-512 | Выработка ключа проверки ЦП | | 0,113 |
| SHA-512 | Создание ЦП | | 0,221 |
| SHA-512 | Проверка ЦП | | 0,453 |
| *Кривая NIST P-384* | | | |
| SHA-512 | Выработка ключа проверки ЦП | | 0,172 |
| SHA-512 | Создание ЦП | | 0,516 |
| SHA-512 | Проверка ЦП | | 1,001 |
| *Кривая NIST P-521* | | | |
| SHA-512 | Выработка ключа проверки ЦП | | 0,234 |
| SHA-512 | Создание ЦП | | 0,932 |
| SHA-512 | Проверка ЦП | | 1,929 |

# Литература

1. NIST FIPS PUB 186-4 «Digital Signature Standard (DSS)» [Интернет ресурс], ссылка: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
2. ГОСТ Р 34.10-2012 «Процессы формирования и проверки электронной цифровой подписи» [Интернет ресурс], ссылка: http://docs.cntd.ru/document/gost-r-34-10-2012