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

Стойкость алгоритма шифрования 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 ЭЦП 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».

2. 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 $GF(2^m)$;

- Псевдослучайная кривая над полем $GF(2^m)$, 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 $G = (G_x, G_y)$.

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

3. Эллиптические кривые над простыми полями *GF(p)*

Для каждого простого *p* существует псевдослучайная кривая

$$E:\ y^2 \equiv x^3 - 3x + b \pmod{p}$$

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 *p*;

- порядком подгруппы точек эллиптической кривой *n*;

- коэффициентом *b*, таким, что:

$$4a^3 + 27b^2 \neq 0 \pmod{p}$$

- координатой *x* базовой точки G_x;

- координатой *y* базовой точки G_y;

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

$p =$ 6277101735386680763835789423207666416083908700390324961279

$n =$ 6277101735386680763835789423176059013767194773182842284081

$b =$ 64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1

$G_x =$ 188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012

$G_y =$ 07192b95 ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811

Кривая NIST P-224

$p =$ 26959946667150639794667015087019630673557916260026308143510066298881

$n =$ 26959946667150639794667015087019625940457807714424391721682722368061

$b =$ b4050a85 0c04b3ab f5413256 5044b0b7 d7bfd8ba 270b3943 2355ffb4

$G_x =$ b70e0cbd 6bb4bf7f 321390b9 4a03c1d3 56c21122 343280d6 115c1d21

$G_y =$ bd376388 b5f723fb 4c22dfe6 cd4375a0 5a074764 44d58199 85007e34

Кривая NIST P-256

$p =$ 115792089210356248762697446949407573530086143415290314195533631308867097853951

$n =$ 115792089210356248762697446949407573529996955224135760342422259061068512044369

$b =$ 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

$G_x =$ 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

$G_y =$ 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

Кривая NIST P-384

$p =$ 39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

$n =$ 39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

$b =$ b3312fa7 e23ee7e4 988e056b e3f82d19 181d9c6e fe814112 0314088f 5013875a c656398d 8a2ed19d 2a85c8ed d3ec2aef

$G_x =$ aa87ca22 be8b0537 8eb1c71e f320ad74 6e1d3b62 8ba79b98 59f741e0 82542a38 5502f25d bf55296c 3a545e38 72760ab7

$G_y =$ 3617de4a 96262c6f 5d9e98bf 9292dc29 f8f41dbd 289a147c e9da3113 b5f0b8c0 0a60b1ce 1d7e819d 7a431d7c 90ea0e5f

Кривая NIST P-521

$p =$ 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

$n =$ 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

$b =$ 051 953eb961 8e1c9a1f 929a21a0 b68540ee a2da725b
99b315f3 b8b48991 8ef109e1 56193951 ec7e937b 1652c0bd
3bb1bf07 3573df88 3d2c34f1 ef451fd4 6b503f00

$G_x =$ c6 858e06b7 0404e9cd 9e3ecb66 2395b442 9c648139
053fb521 f828af60 6b4d3dba a14b5e77 efe75928 fe1dc127
a2ffa8de 3348b3c1 856a429b f97e7e31 c2e5bd66

$G_y =$ 118 39296a78 9a3bc004 5c8a5fb4 2c7d1bd9 98f54449
579b4468 17afbd17 273e662c 97ee7299 5ef42640 c550b901
3fad0761 353c7086 a272c240 88be9476 9fd16650

4. 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 $C_1(x_1, y_1)$ и $C_2(x_2, y_2)$ равны, если равны их соответствующие координаты ($C_1 = C_2$, если $x_1 = x_2$ и $y_1 = y_2$).

На множестве точек эллиптической кривой E операцию сложения обозначают знаком «+». Для двух произвольных точек $C_1(x_1, y_1)$ и $C_2(x_2, y_2)$ эллиптической кривой E рассматривают несколько случаев:

1. Для точек $C_1(x_1, y_1)$ и $C_2(x_2, y_2)$, координаты которых удовлетворяют условию $x_1 \neq x_2$, их суммой называется точка $C_3(x_3, y_3)$, координаты которой определяются сравнениями:

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p, \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod p, \end{cases}$$

Где:

$$\lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} \pmod p.$$

2. Для точек $C_1(x_1, y_1)$ и $C_2(x_2, y_2)$, координаты которых удовлетворяют условию $x_1 = x_2$ и $y_1 = y_2 \neq 0$, их суммой называется точка $C_3(x_3, y_3)$, координаты которой определяются сравнениями:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 \pmod p, \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod p, \end{cases}$$

Где:

$$\lambda \equiv \frac{3x_1^2 + a}{2y_1} \pmod p.$$

3. Для точек $C_1(x_1, y_1)$ и $C_2(x_2, y_2)$, координаты которых удовлетворяют условию $x_1 = x_2$ и $y_1 = y_2(mod\ p)$, их суммой называется точка $C_3(x_3, y_3) = O$ – нулевой точкой без определения её x и y координат. В этом случае точка C_2 называется отрицанием точки C_1. Для нулевой точки O выполнены равенства:

$$C + O = O + C = C,$$

Где:

C – 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:

$$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p}.$$

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

$$C = \underbrace{P + \ldots + P}_{k} = kP$$

5. Параметры пользователя

Каждый пользователь схемы ЭЦП должен обладать личными параметрами:

- ключом подписи – целым числом d, удовлетворяющим неравенству:

$$0 < d < n$$

- ключом проверки подписи – точкой эллиптической кривой Q с координатами (x_Q, y_Q) удовлетворяющая равенству:

$$dG = Q$$

6. Формирование цифровой подписи

Для получения цифровой подписи под сообщением M необходимо выполнить следующие шаги:

1) Вычислить хеш-значение сообщения M:
$$h = HASH(M)$$
2) Вычислить целое число e:
$$e \equiv h(\mathrm{mod}\, n)$$
Если $e = 0$, то определить $e = 1$.
3) Получить случайное (псевдослучайное) целое число k, удовлетворяющее неравенству:
$$0 < k < n$$
4) Вычислить точку эллиптической кривой $C = kG$ и определить:
$$r = x_C(\mathrm{mod}\, n),$$
Где: x_C – x координата точки C.
Если $r = 0$, то вернуться к шагу 3).

5) Вычислить значение:

$$s \equiv (rd + ke) (\mathrm{mod}\, n)$$

Если $s = 0$, то вернуться к шагу 3).

6) Определить цифровую подпись: как два выходных параметра r и s.

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

7. Проверка цифровой подписи

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

1) Получение параметров r и s – цифровой подписи сообщения M. Если выполнены неравенства $0 < r < n$ и $0 < s < n$, то перейти к следующему шагу. В противном случае подпись неверна.
2) Вычислить хеш-значение полученного сообщения M:

$$h = HASH(M)$$

3) Вычислить целое значение e:

$$e \equiv h (\mathrm{mod}\, n)$$

Если $e = 0$, то определить $e = 1$.

4) Вычислить значение:

$$v \equiv e^{-1} (\mathrm{mod}\, n)$$

5) Вычислить значения:

$$z_1 \equiv sv (\mathrm{mod}\, n)$$
$$z_2 \equiv -rv (\mathrm{mod}\, n)$$

6) Вычислить точку эллиптической кривой $C = z_1 G + z_2 Q$ и определить:

$$R \equiv x_C (\mathrm{mod}\, n)$$

Где: x_C – x координата точки C.

7) Если выполнено равенство $R = r$, то подпись принимается, в противном случае – подпись неверна.

Исходными данными этого процесса являются подписанное сообщение M, 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.

8. Российские параметры для эллиптических кривых над *GF(p)*

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

G_x = 2

G_y = 40189740565390375033354494229370597756357393899055450806909793652134315662 80

Кривая ГОСТ Р-512

a = 7

p = 3623986102229003635907788753683874306021320925534678605086546150450856166624002482588482022271496854025090823603058735163734263 8223719649872258290737240 3

n = 3623986102229003635907788753683874306021320925534678605086546150450856166623969164898305032863068499961404079437936585455865192212970734808812618120619743

b = 1518655069210828534508950034714043154928747527740206436194018823352809982443793732829756914785974674866041605397883677596626326413990136959047435811826396

G_x = 1928356944067022849399309401243137598997786635459507974357075491307766592685835441065557681003184874819658004903212332884252335830250729527632383493573274

G_y = 2288728693371972859970012155529478416353562327329506180314497425931102860301572814141997072271708807066593850650334152381857347798885864807605098724013854

9. 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 ЭЦП 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 ЭЦП на различных видах кривых NIST и GOST, а также фиксация времени выполнения отдельных элементов в процессе ЭЦП (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.

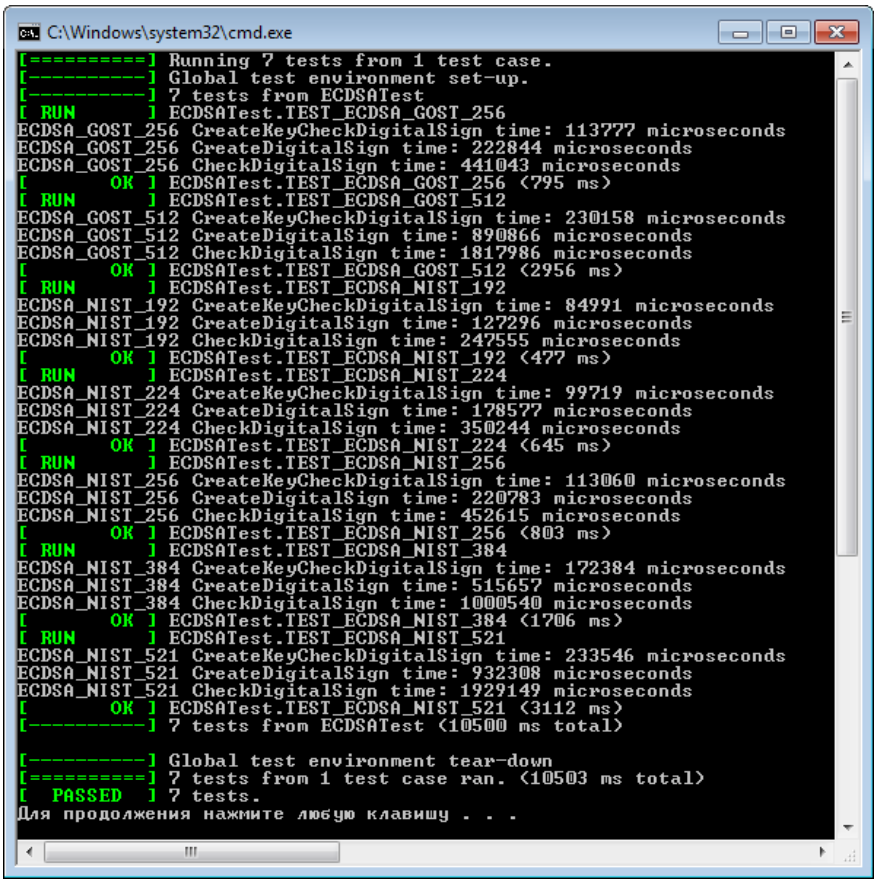

Рис. 1. Результат тестирования реализованного алгоритма ECDSA

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

- время выработки ключа проверки ЭЦП (*Q*);
- время создания ЭЦП;
- время проверки ЭЦП.

для данного ЦП. Данные приведены в Табл. 1.

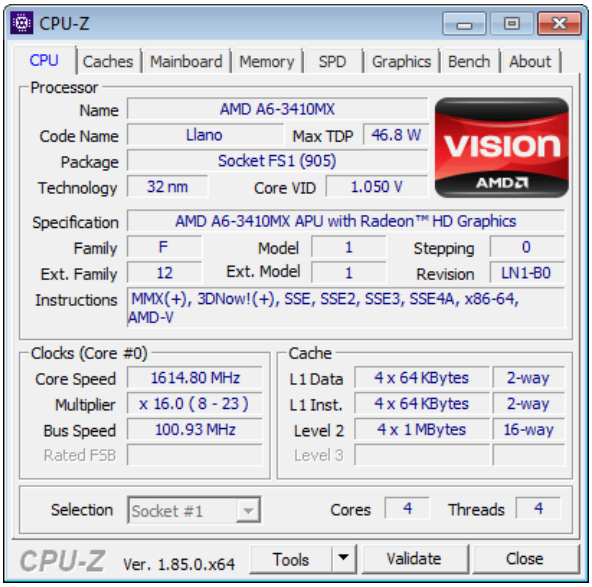

Рис. 2. ЦП AMD A6-3410MX (4 ядра, 4 потока)

Табл. 1. Скорость выполнения операций ЭЦП

Используемая хеш-функция	Выработка ключа проверки ЭЦП / Создание ЭЦП/ Проверка ЭЦП	Скорость [микросекунд]
Кривая ГОСТ Р-256		
SHA-512	Выработка ключа проверки ЭЦП	113777
SHA-512	Создание ЭЦП	222844
SHA-512	Проверка ЭЦП	441043
Кривая ГОСТ Р-512		
SHA-512	Выработка ключа проверки ЭЦП	230158
SHA-512	Создание ЭЦП	890866
SHA-512	Проверка ЭЦП	1817986
Кривая NIST P-192		
SHA-512	Выработка ключа проверки ЭЦП	84991
SHA-512	Создание ЭЦП	127296
SHA-512	Проверка ЭЦП	247555
Кривая NIST P-224		
SHA-512	Выработка ключа проверки ЭЦП	99719
SHA-512	Создание ЭЦП	178577
SHA-512	Проверка ЭЦП	350244
Кривая NIST P-256		
SHA-512	Выработка ключа проверки ЭЦП	113060
SHA-512	Создание ЭЦП	220783
SHA-512	Проверка ЭЦП	452615
Кривая NIST P-384		
SHA-512	Выработка ключа проверки ЭЦП	172384
SHA-512	Создание ЭЦП	515657
SHA-512	Проверка ЭЦП	1000540
Кривая NIST P-521		
SHA-512	Выработка ключа проверки ЭЦП	233546
SHA-512	Создание ЭЦП	932308
SHA-512	Проверка ЭЦП	1929149

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