Криптография с открытым ключом

Владислав Ковтун

Владислав Ковтун

Оглавление

Владислав Ковтун

Принципы построения криптосистем с открытым ключом

От истоков криптографии до самых современных времен, криптосистемы строились на основе элементарных преобразований: подстановки и перестановки. Ручной труд, на протяжении тысяч лет, был сменен механическими, а далее и электромеханическими шифровальными и дешифровальными машинами, которые открыли новую эру в области защиты информации. Дальнейшее изобретение компьютеров, послужило новым толчком, развитию средств не только шифрования, но и криптоанализа. Одним из таких достижений, является алгоритм LUCIFER компании IBM, который был положен в основу всем хорошо известного алгоритма DES. Однако, основу всех алгоритмов продолжали составлять, все те же, подстановки и перестановки, которые производились как отправителем, так и получателем. Другими словами, отправитель и получатель обязаны обладать одним и тем же ключом, отсюда вытекает одно из ограничений симметричных криптосистем – распространение (распределение) ключей.

Указанный недостаток послужил толчком к поиску подходов к построению криптосистем способных исключить защищенный канал передачи ключей и обеспечивая защиту передаваемых сообщений по незащищенному каналу, без дополнительных преобразований. На рис. 1, показан процесс двустороннего обмена между отправителем и получателем (абонентами), при этом злоумышленник выполняет пассивную роль слушателя. В отличие от обычных систем (с секретным ключом), системы, допускающие открытую передачу (открытой) части ключа по незащищенному каналу связи, называют системами с открытым ключом. В таких системах открытый ключ (ключ шифрования), отличается от личного ключа (ключа расшифровывания), поэтому их иногда называют ассиметричными системами или двуключевыми системами.

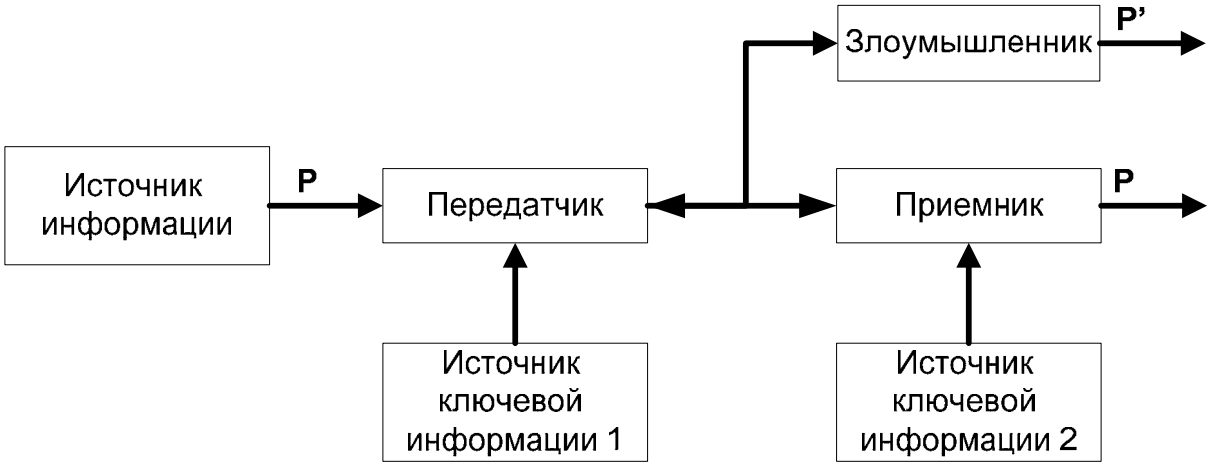


Рис. 1. Информационные потоки в криптографической системе с открытым ключом

Впервые, публично, Диффи и Хеллман в 1976 году изложили идею разработанного метода на национальной компьютерной конференции [0] и опубликована в том же году в основополагающей работе "Новые направления в криптографии" [1]. Предложеный метод решает задачу: распределения ключей и цифровой подписи. Она радикально отличалась от известных ранее подходов, за всю историю криптографии.

К числу отцов-основателей следует отнести также и Ральфа Меркля, который независимо от Диффи и Хеллмана пришел к тем же конструкциям, однако опубликовал свои результаты только в 1978 году [69].

Криптография с открытм ключем. Текущее состояние

Однако, истинную точку отсчета криптографии с открытым ключом, следует отнести к более раннему времени. Известно несколько независимых источников, которые отдают пальму первенства, в разработке криптографии с открытым ключем, Агентству национальной безопасности США (National Security Agency - NSA).

По словам адмирала Бобби Инман (Bobby Inmann), занимал пост главы Агентства, метод криптографических преобразований с открытым ключом разработан NSA еще в середине 60-х годов. Первое документальное подтверждение этому, появилось в 1970 году в закрытом отчете Джеймса Эллиса (James Ellis) из Группы защиты электронных коммуникаций Службы безопасности Великобритании [73].

В статье энциклопедии "Британника" директор NSA Симмонс заявляет, что "двухключевая криптография была известна в Агентстве за 10 лет до публикации Диффи и Хеллмана" [70].

В опубликованной статье покойного военного криптоаналитика Джеймса Эллиса (James Ellis) из Великобритании утверждается, что ему и Клиффорду Коксу (Clifford Cocks) удалось получить работающую схему, близкую к RSA [2], за несколько лет до этого [73]. К сожалению, отсутствуют независимые подтверждения этому.

И так, в основе преобразований с открытым ключом лежит теоретико-числовой подход к определению стойкости криптоанализа, т.е. проблема обоснования стойкости криптографической схемы свелась к доказательству отсутствия полиномиального алгоритма, который решает задачу, стоящую перед злоумышленником. Из этого следует, что на данный момент стойкость криптографических схем может быть установлена лишь с привлечением каких-либо недоказуемых предположений. Поэтому, основное направление исследований состоит в поиске наиболее слабых достаточных условий для существования стойких схем каждого типа. В основном рассматриваются предположения двух типов – общие (или теоретико-сложностные) и теоретико-числовые, т.е. предположения о сложности конкретных теоретико-числовых задач [0, 1].

В работах [0, 1] показано предположение о существовании односторонних функций. Там, же дается доказательство того факта, что существование односторонних функций является необходимым и достаточным условием существования стойких криптосистем с секретным, открытым ключом и криптографических протоколов нескольких типов. В 1978 г. [2] был предложен пример такой односторонней функции $f(x)$, обладающей рядом свойств [71]:

а) существует достаточно быстрый (полиномиальный) алгоритм вычисления значений $f(x)$;

б) существует достаточно быстрый (полиномиальный) алгоритм вычисления значений обратной функции $f^{-1}(x)$;

в) функция $f(x)$ обладает некоторым «секретом», знание которого позволяет быстро вычислять значение $f^{-1}(x)$; в противном случае вычисление $f^{-1}(x)$ становится трудно разрешимой в вычислительном отношении задачей, требующей для своего решения столь много времени, что по его прошествии зашифрованная информация перестанет быть актуальной для лиц, использовавших $f(x)$ в качестве шифра.

На основе указанных принципов была предложена трудноразрешимая задача факторизации большого числа, которая была положена в основу первой, реально используемой, системы шифрования – RSA [2].

Далее рассмотрим основные направления применения криптосистем с открытым ключом.

Применение криптосистем с открытым ключом

Двигателем данного направления криптографии является, в первую очередь, практика. Стремительное развитие информационных систем ставит все новые и новые задачи перед разработчиками криптографических алгоритмов (протоколов). Классифицируем наиболее существенные побудительные мотивы развития криптографии с открытым ключом (не претендует быть исчерпывающей):

- Развитие телекоммуникационных систем и сетей различного назначения.
- Развитие глобальной сети Интернет.
- Развитие банковских систем, в том числе и пластиковых карт.
- Потребность мыслящего человека к познанию.

Выделяют следующие основные (глобальные, в самом широком смысле) направления применения криптографических преобразований с открытым ключом:

- зашифровывание и расшифровывание;
- выработка общего секрета или обмен ключами;
- наложение и проверка электронной цифровой подписи;
- аутентификация;
- «электронные деньги».

Каждому, из перечисленных направлений, присуща собственная процедура применения открытого или личного кличей.

В современных условиях, для решения задач защиты информации могут применяться криптографические алгоритмы, которые могут решать как одну, так и несколько задач (из выше перечисленных). Алгоритм RSA [2], например, с успехом позволяет решать задачи шифрования, обмена ключами и цифровой подписи. Однако все универсальное не лишено недостатков. Для успешного противостояния криптоаналитикам и повышения эффективности алгоритма, были предложены различные модификации RSA [ ], решающие указанные задачи по отдельности.

Условия применения криптосистем с открытым ключом

В свое время Диффи и Хеллманом предложили, что существуют криптосистемы, которые содержат два более ключа (с открытым ключом), без предоставления доказательств. Однако или были указаны условия, которым следует удовлетворять таким криптосистемам:

1. Для стороны A (или B) процесс генерации ключевых пар: Pb_A и Pt_A (или Pb_B и Pt_B), не вызывает вычислительных трудностей.

2. Для отправителя A (или B), процесс зашифровывания не вызывает вычислительных трудностей, при наличии открытого ключа Pb_B и сообщения M: $C = E_{Pb_B}(M)$.

3. Для получателя B (или A), процесс расшифровывания не вызывает вычислительных трудностей, при наличии личного ключа Pt_B и полученного зашифрованного сообщения C': $M = D_{Pt_B}(C') = D_{Pt_B}\left[E_{Pb_B}(M)\right]$.

4. Для злоумышленника, процесс восстановления личного ключа Pt_B из открытого ключа Pb_B, является вычислительно неосуществимым.

5. Для злоумышленника, процесс восстановления оригинального сообщения M из имеющегося зашифрованного текста C открытого ключа Pb_B, является вычислительно неосуществимым.

6. Функции зашифровывания и расшифровывания, могут применяться в произвольном порядке: $M = E_{Pb_B}\left[D_{Pt_B}(M)\right]$. Данное условие не является необходимым.

Обзор теоретико-числовых задач

Сегодня широко известны и получили применение в криптографических приложениях целый ряд теоретико-числовые задачи, которые позволяют строить односторонние функции с «секретом», их классификация приведена на рис. 2. Далее, в работе, постараемся детально остановиться на описании наиболее известных задачах в следующей последовательности:

1. Краткое описание задачи.

2. Оценка вычислительной и пространственной сложности криптоанализа.

3. Производительность/вычислительная сложность программной реализации.

Далее, в работе, под сложностью будет пониматься именно вычислительная сложность.

Отметим, что при оценке сложности решения той или иной задачи, по возможности, будет указываться сложность ее решения с использованием квантового компьютера. Данное замечание становиться достаточно существенным в свете последней презентации канадской компании D-Wave Systems в 2007 году реально действующего квантового компьютера [72]. Разработчиками было отмечено, что криптоанализ является одним из основных направлений его применения.

При описании практической реализации, сделаем следующее предположение: оценка производится с учетом реализации на W-разрядном процессоре, при этом операции присвоения и управления потоком выполнения команд – не учитываются.

Постоянное развитие вычислительной техники и увеличение ее производительности, что подтверждается законом Мура, а также совершенствованию математических методов криптоанализа влечет периодическому пересмотру размеров ключевой информации.

На рис. 2 используются следующие аббревиатуры:

- ЦП – цифровая подпись.

Владислав Ковтун

- АСШ – асимметричное шифрование.
- ОК – обмен ключами.

Криптография с открытм ключем. Текущее состояние

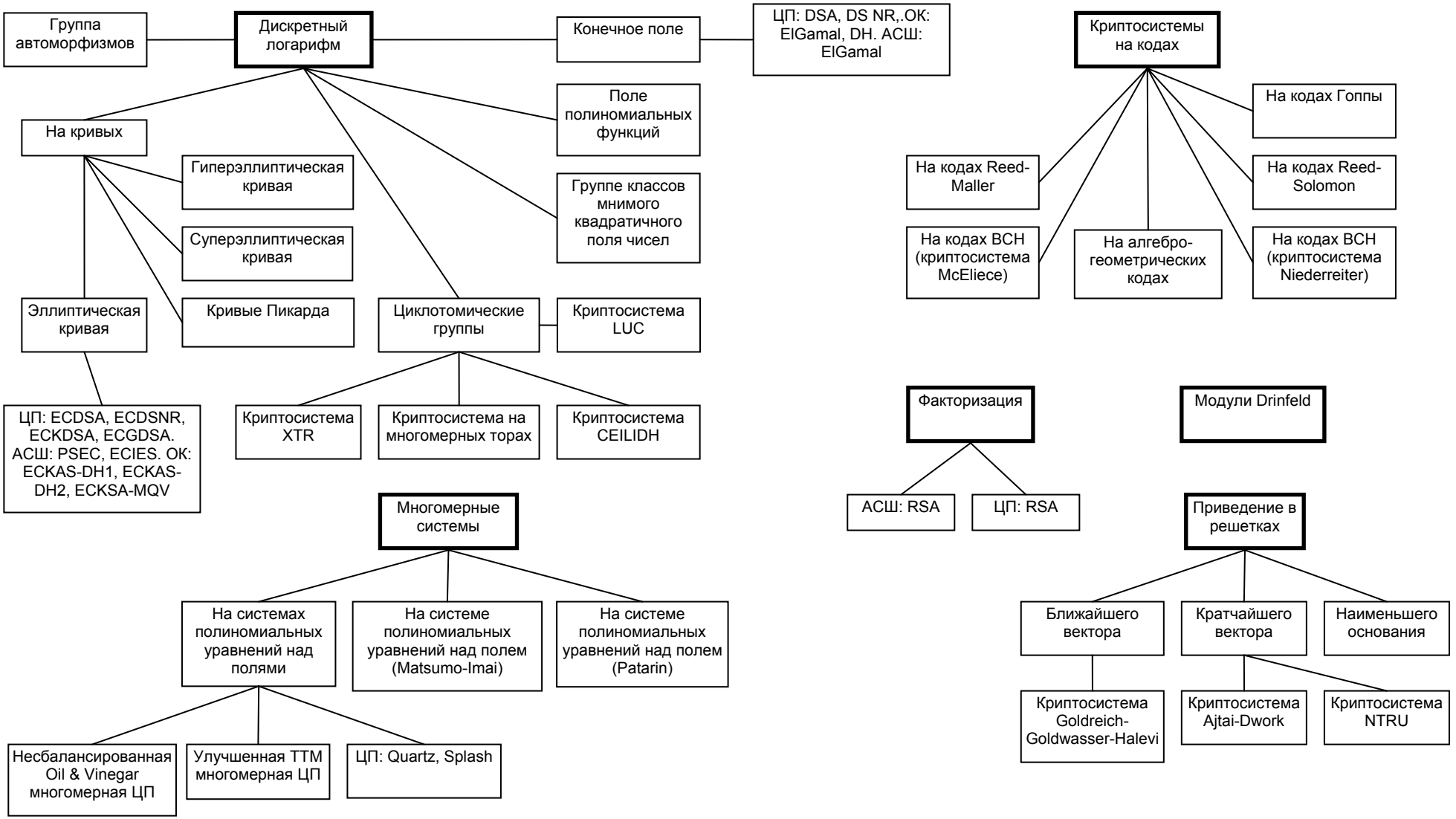


Рис. 2. Классификация теоретико-числовых задач, а также криптосистем на их основе

Владислав Ковтун

Факторизация большого целого числа

Описание задачи

Пусть дан целое число $N > 1$, которое не является простым, тогда существует целое число a, такое, что $1 < a < N$ и $a \mid N$. Задача состоит в том, что бы найти такое a или доказать, что оно равно 1. В криптографических приложениях используют число N, состоящее из двух простых множителей соизмеримой величины, другими словами они имеют соизмеримые двоичные длины.

Сложность криптоанализа

Задача факторизации большого целого числа N на множители принадлежит к классу субэкспоненциальных алгоритмов, сложность которых составляет $L_N(\alpha, \beta) = \exp\left((\beta + o(1))(\log N)^{\alpha} (\log\log N)^{1-\alpha}\right)$.

Сложность алгоритма GNFS (General Number Field Sieve) - решета поля чисел общего вида составит $L_N\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right)$ [15].

Сложность алгоритма SNFS (Special Number Field Sieve) - решета поля чисел специального вида $N = a^b + c$ составит $L_N\left(\frac{1}{3}, \sqrt[3]{\frac{32}{9}}\right)$ [15].

Сложность решения задачи с использованием квантового компьютера с количеством $O(\log N)$ кубитов составит $O(\log N)$ [56].

Известно, что для факторизации чисел двоичной длины до 1024 бит, наиболее приемлемым считается алгоритм ECM (Elliptic Curve Method) […] с использованием эллиптических кривых, для чисел большего размера принято использовать GNFS алгоритм [56].

Производительность/сложность реализации

Примитив RSA. Данный примитив является первым среди реализованных. Пусть k является секретным и пусть $N = pq$ является произведением двух больших простых множителей двоичной длиной $\frac{k}{2}$. Пусть также открытый параметр – показатель e, такое, что $\gcd(e, (p-1)(q-1)) = 1$ и соответствующий личный параметр $d \equiv e^{-1} \pmod{\lambda(N)}$, где $\lambda(x)$ - функция Карлмайкла, $\lambda(N) = \operatorname{lcm}(p-1, q-1)$.

Как видно из описания данного примитива, основными операциями в кольце целых чисел являются:

- сложение/вычитание;
- умножение;
- возведение в квадрат;
- мультипликативное инвертирование;
- приведение по модулю;
- возведение в степень, базируется на операциях умножения и возведения в квадрат.

Известно, что в данной ситуации наиболее целесообразным является использование арифметики Montgomery [16]. Основу указанных преобразований

составляет операция умножения. Известно несколько модификаций умножения методом Montgomery [16]:

- SOS: separated operand scanning;
- CIOS: coarsely integrated operand scanning;
- FIOS: finely integrated operand scanning;
- CIHS: coarsely integrated hybrid scanning.

Согласно исследованиям [16], алгоритм CIOS является наиболее приемлемым для реализации на процессорах общего назначения, с точки зрения производительности.

В таблице 1 приведем сложности операций в кольце целых чисел, выраженные в операциях процессора [16].

Таблица 1. Сложности операций в кольце целых чисел, выраженные в операциях процессора [16]

№	Название	Предвычисления	Сложность
1	Классическое приведение по модулю*		$k(k+2)M_{CPU} + kD_{CPU}$
2	Приведение по модулю, метод Barret*		$k(k+4)M_{CPU}$
3	Приведение по модулю, метод Montgomery*		$k(k+1)M_{CPU}$
4	Сложение, без приведения по модулю		kA_{CPU}
5	Вычитание, без приведения по модулю		kA_{CPU}
6	Умножение Montgomery умножение методом CIOS [17], без приведения по модулю		$(2k^3+2k)M_{CPU} + (4k^2+6k+2)A_{CPU}$
7	Умножение KCM (Karatrsuba-Comba-Montgomery) [17], без приведения по модулю		$(k^2+k+X_1)M_{CPU} + (2k^2+4k+1+X_2)A_{CPU}$
8	Умножение KCM с приведением по модулю псевдо-Мерсенова числа [17]		$(\frac{3}{4}k^2+k+1)M_{CPU} + (4k^2+2k+2)A_{CPU}$
9	Возведение в степень, метод «возвести в квадрат, и умножить» [17]		$\frac{1}{2}lM_{Z_N} + lS_{Z_N}$
10	Возведение в степень, промежуточные умножения выполнены методом Montgomery [17]		$(2+\frac{3}{2}l)MM_{Z_N}$, $k(2k+1)(2+\frac{3}{2}l)M_{CPU}$
11	Возведение в степень, метод Lim-Lee, сложность предвычислений $(v+b+h-1+v(2^h-2)(v+b))S_{Z_N} + vh2^{h-1}M_{Z_N}$ [18]	$v(2^h-1)$	$(\frac{2^h-1}{2^h}a-2)M_{Z_N} + bS_{Z_N}$
12	Возведение в степень на стороне владельца личной информации, промежуточные умножения выполнены методом Montgomery, с некоторыми допущениями из [16], $\log_2 p = \log_2 q = \log_2 d_p = \log_2 d_q = \frac{1}{2}l$		$(7+\frac{3}{2}l)MM_{Z_p}$, $\frac{1}{4}k[(k+1)(14+3l)+k]M_{CPU}$

* - в данных работах отсутствует ссылка на количество

l - двоичная длина показателя. M_{Z_N} - операция умножения в кольце чисел Z_N. S_{Z_N} - операция возведения в квадрат в кольце чисел Z_N. MM_{Z_N} - операция умножения методом Montgomery в кольце чисел Z_N. $k = \lceil l/W \rceil$ - количество машинных слов двоичной длиной W, необходимых для хранения в памяти число двоичной длины l.

h - число блоков, на которые разбивается показатель в алгоритме Lim-Lee [19], $a = \lceil \frac{l}{h} \rceil$ - размер блока, v - число подблоков, на которые разбивается каждый блок, размер блока $b = \lceil \frac{a}{v} \rceil$. Варьируя значениями h и v можно достигнуть требуемой производительности при известных ограничениях на размер памяти для хранения предвычислений. Оптимальные значения для современных персональных компьютеров составляют $h = 8$ и $v = 3$ (или $v = 4$) [18]. В работе [20] были предложены параметры $h = 4$ и $v = 1$, которые позволяют эффективно реализовать алгоритм Lim-Lee.

Зашифровывание. На этом этапе производится возведение в степень чисел длиной k машинных слов посредством одного из методов указанных в строках 7-9 таблицы 1. Аналитически данное преобразование выглядит как:

$$y = x^e \pmod N,$$

где y - зашифрованное сообщение, x - исходное сообщение, N - составной модуль, e - ключ зашифровывания.

Количество операций процессора необходимых для выполнения зашифровывания информационного блока соответствует суммарной сложности операции возведения в степень и приведения по модулю.

Расшифровывание. На этом этапе происходит процесс аналогичный предыдущему.

$$x = y^d \pmod N,$$

где y - зашифрованное сообщение, x - исходное сообщение, N - составной модуль, d - ключ расшифровывания.

Для возведения в степень $y^d \bmod N$ на стороне обладателя личной информации, следует воспользоваться Китайской теоремой об остатках (CRT-Chinese Remainder Theorem). Зная разложение $N = pq$, значение $y^d \bmod N$ может быть получено как $y^d \bmod N = s_q + q\left(i_q\left(s_p - q_q\right) \bmod p\right)$, $s_p = y^{d_p} \bmod p$, $s_q = y^{d_q} \bmod q$, $d_p = d \bmod (p-1)$, $d_q = d \bmod (q-1)$, $i_q = q^{-1} \bmod p$.

Предположив, что двоичная длина $\log_2 p = \log_2 q = \log_2 d_p = \log_2 d_q = \tfrac{1}{2}l$, это позволяет снизить нагрузку на процессор, т.к. длина операндов, с которыми ему придется оперировать составит $\frac{1}{2}l$ бит, что позволяет получить вычислительную сложность, приведенную в таблице, строка 10.

Существуют также и другие варианты реализации описанных алгоритмов, которые обладают немного большей производительность чем приведенные, но и более сложной логикой и требующие значительных предвычислений.

Таблица 2. Сложность криптопримитива RSA выраженная в количестве операций в кольце целых чисел и количестве операций процессора

Сложность	Зашифровывание	Расшифровывание
Операции в кольце	$\left(2+\tfrac{3}{2}l\right)MM_{Z_N}$	$\left(7+\tfrac{3}{2}l\right)MM_{Z_p}$
Операций процессора	$k(2k+1)\left(2+\tfrac{3}{2}l\right)M_{CPU}$	$\tfrac{1}{4}k\left[(k+1)(14+3l)+k\right]M_{CPU}$
Операции в кольце, при наличии предвычислений	$\left(\frac{2^h-1}{2^h}a+b\right)MM_{Z_N}$	$\left(\frac{2^h-1}{2^{h+1}}a+5+\frac{b}{2}\right)MM_{Z_N}$
Операций процессора, при наличии предвычислений	$\left(\frac{2^h-1}{2^h}a+b\right)\left(\left(\frac{3}{4}k^2+k+1\right)M_{CPU}+\right.$ $\left.+\left(4k^2+2k+2\right)A_{CPU}\right)$	$\left(\frac{2^h-1}{2^h}a+5+b\right)\left(\left(\frac{3}{4}k^2+k+1\right)M_{CPU}+\right.$ $\left.+\left(4k^2+2k+2\right)A_{CPU}\right)$

MM_{Z_N} - операция умножения методом Montgomery в кольце чисел Z_N. M_{Z_N} - операция умножения в кольце чисел Z_N.

При получении результатов приведенных в таблице 2, авторами было сделано предположение о равенстве сложности операций умножения и возведения в квадрат в кольце целых чисел.

Владислав Ковтун

Дискретный логарифм

В данном случае под задачей дискретного логарифма подразумевается целый класс задач, которые отличаются друг от друга лишь алгебраическими структурами, образующими группы. Далее дадим наиболее общее определение данной задачи. Пусть дана конечная циклическая группа $\langle G \rangle$ порядка n, образующий элемент P и произвольный элемент группы Q. Задача нахождения дискретного логарифма состоит в поиске такого целого числа x, что $Q = xP$. Отметим, что это число приведено по модулю n. Рассмотрим задачи дискретного логарифмирования (DLP) на конкретных алгебраических структурах, которые образуют группы.

Дискретный логарифм в мультипликативной группе конечного поля (чисел, полиномов)

Описание задачи

Пусть даны групповые элементы g (генератор поля) и h, тогда под **решением DLP** будем понимать решение уравнения $h = g^l$ относительно l или доказательство того, что решения не существует. Необходимым условием является $h \in \langle g \rangle$, т.е. $l \in [0, \mathrm{ord}(g) - 1]$ и $h^{\mathrm{ord}(g)} = 1$, где $g, h \in \mathbf{GF}(q)$, n - порядок элемента образующего группу $n = \mathrm{ord}(g)$, l - секретный ключ, h - открытый ключ.

Сложность криптоанализа

В таблице 3 приведем оценки сложности решения DLP в поле по результатам обзора [21].

Таблица 3. Оценки сложность решения DLP в поле [21]

№	Название алгоритмов	Поле	Сложность	Тип
1	Обобщенное решето поля чисел	$\mathbf{GF}(p)$	Требуется $O\left(\exp\left((64/9)^{1/3} + o(1)\right)(\ln p)^{1/3}(\ln\ln p)^{2/3}\right)$ групповых операций.	Д
2	Обобщенное решето поля чисел	$\mathbf{GF}(2^m)$	Требуется $O\left(\exp\left(1.587 m^{1/3}(\ln m)^{2/3}\right)\right)$ групповых операций.	Д
3	Алгоритм Adleman-Coppersmith	$\mathbf{GF}(2^m)$	Требуется $O\left(\exp\left((c + o(1)) m^{1/3}(\log m)^{2/3}\right)\right)$ групповых операций, где $c \approx 1.4$.	Д

Д – детерминированный алгоритм, дающий точное решение.

Сложность/производительность реализации

В криптографии широкое распространение получили поля $\mathbf{GF}(p)$, p - простое и их расширения $\mathbf{GF}(p^m)$. Расширенные поля в свою очередь делятся по характеристике на $\mathbf{GF}(2^m)$ и $\mathbf{GF}\left((2^m - c)^n\right)$ с характеристикой в виде псевдо Мерсеновых чисел. По степени расширения: на $\mathbf{GF}(2^m)$, m - простое и композитные $\mathbf{GF}\left((2^m)^n\right)$. Также следует выделить простые поля с характеристикой в виде псевдо Мерсеновых чисел и обобщенных Мерсеновых чисел. Каждый из приведенных полей нашли свое применение в криптографии, т.к. являются предпочтительными при реализации на различных платформах.

Одним из наиболее интересных полей, считается Optimal Extension Field (OEF), по причине высокопроизводительной арифметики. На рис. 3 приводится, некоторая, классификация [18].

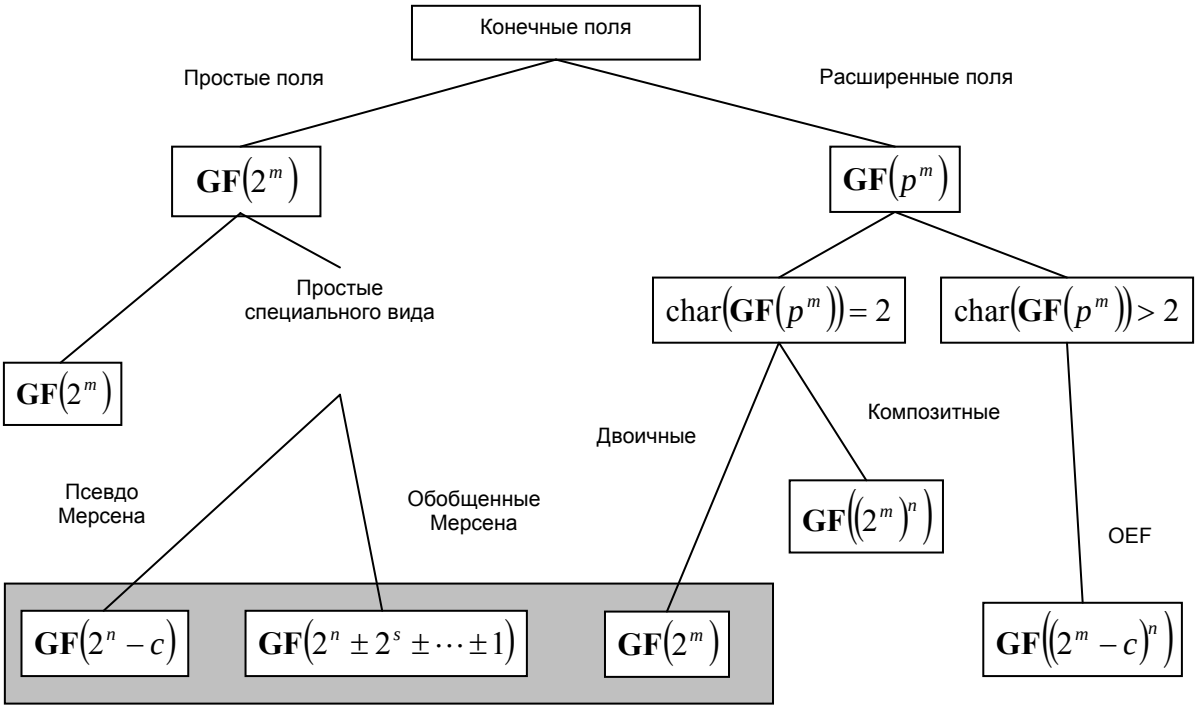


Рис. 3. Конечные поля, которые предлагаются для использования в криптографических приложениях

В работе нами будет уделено основное внимание полям, выделенным на рис. 3. Рассмотрение остальных полей выходит за рамки данной работы, существует достаточно большое количество публикаций касательно реализации арифметики в этих полях.

Простые поля. Рассмотрение начнем с простых полей, модуль которых является псевдо-Мерсеновыми и обобщенными Мерсеновыми числами вида $p=\beta^t-c$, где c - небольшое целое.

В таблице 4 приведем сложности операции приведения по известным простым модулям в операциях процессора.

Таблица 4. Теоретические оценки сложности операции приведения по известным простым модулям в операциях процессора

№	Модуль	Сложность в полевых операциях	Сложность в операциях процессора
1	Псевдо-Мерсеново число общего вида, $p=\beta^t-c$		$(tl+l^2)M_{CPU}$, t - двоичная длина модуля p, причем $l=\log_2 c\le\frac{t}{2}$, k - двоичная длина числа, которое приводится
2	Псевдо-Мерсеново число общего вида, $p=\beta^t-c$, когда c размещается в одном машинном слове		$(t+1)M_{CPU}$, t - двоичная длина модуля p, причем $l=\log_2 c\le\frac{t}{2}$, k - двоичная длина числа, которое приводится
3	Псевдо-Мерсеново число $p=2^{192}-2^{64}-1$	$2A_{F_p}$	$12A_{CPU}$, $W=32$
4	Псевдо-Мерсеново число $p=2^{224}-2^{96}+1$	$7A_{F_p}$	$49A_{CPU}$, $W=32$
5	Псевдо-Мерсеново число	$15A_{F_p}$	$120A_{CPU}$, $W=32$

	$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$		
6	Псевдо-Мерсеново число $p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$	$15A_{F_p}$	$180A_{CPU}$, $W = 32$
7	Псевдо-Мерсеново число $p = 2^{521} - 1$	$\frac{3}{2}A_{F_p} + 17X_{CPU} + 33Sh_{CPU}$	$25{,}5A_{CPU} + 17X_{CPU} + 33Sh_{CPU}$, $W = 32$
8	Сложение, без приведения по модулю		kA_{CPU}
9	Вычитание, без приведения по модулю		kA_{CPU}
10	Умножение Montgomery [17], без приведения по модулю		$(2k^3 + 2k)M_{CPU} + (4k^2 + 6k + 2)A_{CPU}$
11	Умножение КСМ [17], без приведения по модулю		$(k^2 + k + X_1)M_{CPU} + (2k^2 + 4k + 1 + X_2)A_{CPU}$
12	Умножение [22], без приведения по модулю		$(k(k-1) + t)(3A_{CPU} + M_{CPU})$
13	Возведение в квадрат [22], без приведения по модулю		$(k(2k-1) + t)(4A_{CPU} + \frac{1}{2}M_{CPU})$

Далее рассмотрим сложность операции возведения в степень, в таблице 5 приведены интересующие нас аналитические выражения.

Таблица 5. Теоретические оценки сложности операции возведения в степень в полевых операциях

№	Название	Размер пред-вычислений	Средняя сложность
1	Метод «Возведение в квадрат и умножение»	-	$\frac{1}{2}lM_{F_p} + lS_{F_p}$
2	Метод с фиксированной шириной окна предвычислений	2^{w-1}	$\left(\left\lfloor\frac{l-1}{w}\right\rfloor(w + 1 - 2^{-w}) + 1 - 2^{-((l-1) \bmod w)}\right)M_{F_p}$
3	Метод с адаптируемой шириной окна (скользяще окно) предвычислений	2^{w-1}	$\left(2^{w-1} + \frac{l}{w+1} + l - w\right)M_{F_p}$
4	Метод Lim-Lee	$v(2^h - 1)$	$\left(\frac{2^h - 1}{2^h}a - 2\right)M_{F_p} + bS_{F_p}$

Окончательный выбор того или иного алгоритма будет производиться на основе не только теоретической оценки сложности, но и экспериментальной оценки. Ниже, в таблице 6 приведем условия эксперимента проведенного авторами данной работы, а также опубликованными в [22].

Таблица 6. Условия проведения экспериментальных оценок времени выполнения алгоритмов, реализующих операции в простом поле

Колонка	Источник	Процессор	Операционная система	Компилятор	Особенности реализации
1	[22]	Intel, Pentium II 400 MHz	MS Windows 2000	MS Visual C++ 6.0	С ассемблером
2	авторы	AMD, Athlon XP 2500+ MHz	MS Windows XP	MS Visual C++ 2005	Без ассемблера

Непосредственно результаты эксперимента сведены в таблице 7, там же приведены результаты опубликованные в [22].

Таблица 7. Экспериментальные оценки времени выполнения алгоритмов, реализующих операции в простом поле

Условия	$\log_2 p = 192$		$\log_2 p = 224$		$\log_2 p = 256$		$\log_2 p = 384$		$\log_2 p = 521$	
Операция	1	2	1	2	1	2	1	2	1	2
Сложение	0,097	0,045	0,114	0,048	0,123	0,058	0,169	0,081	0,162	0,081
Вычитание	0,094	0,047	0,112	0,06	0,125	0,073	0,158	0,087	0,15	0,093
Умножение,	0,823	3,44	1,074	5	1,568	7,03	2,884	17,18	4,771	34,38

метод Comb										
Умножение, метод Карацубы	1,758	-	2,347	-	2,844	-		-		-
Приведение, классический метод	0,203	0,142	0,261	0,218	0,522	0,632	0,728	0,742	0,15	0,12
Возведение в квадрат	0,823	2,34	1,074	3,28	1,358	4,84	2,438	11,41	3,864	21,25
Инвертирование, расширенный алгоритм Эвклида	66.30	50,62	88,26	64,22	115,9	82,19	249,6	172,6	423,2	281,1

Двоичные поля. Элементы двоичных полей могут быть представлены как в полиномиальном базисе, так и в нормальном базисе. В данной работе будет рассматриваться только полиномиальное представление. В таблице 8 приведем вычислительные сложности операций в двоичном поле.

Таблица 8. Теоретические оценки сложности полевых операций в операциях процессора

№	Название	Предвычисления	Сложность
1	Приведение по модулю (полином общего вида), количество предвычислений $W(k+1)Sh_{CPU}$	W элементов поля	$(l-1)(k+1)X_{CPU}$
2	Приведение по модулю $p(x)=x^{163}+x^7+x^6+x^3+1$		$43X_{CPU}+34Sh_{CPU}$, $W=32$
3	Приведение по модулю $p(x)=x^{233}+x^9+x^4+x^1+1$		$55X_{CPU}+45Sh_{CPU}$, $W=32$
4	Приведение по модулю $p(x)=x^{233}+x^{74}+1$		$33X_{CPU}+31Sh_{CPU}$, $W=32$
5	Приведение по модулю $p(x)=x^{283}+x^{12}+x^7+x^5+1$		$70X_{CPU}+68Sh_{CPU}$, $W=32$
6	Приведение по модулю $p(x)=x^{307}+x^8+x^5+x^2+1$		$86X_{CPU}+84Sh_{CPU}$, $W=32$
7	Приведение по модулю $p(x)=x^{367}+x^{21}+1$		$45X_{CPU}+43Sh_{CPU}$, $W=32$
8	Приведение по модулю $p(x)=x^{409}+x^{87}+1$		$53X_{CPU}+51Sh_{CPU}$, $W=32$
9	Приведение по модулю $p(x)=x^{431}+x^5+x^3+x^1+1$		$102X_{CPU}+100Sh_{CPU}$, $W=32$
10	Приведение по модулю $p(x)=x^{571}+x^{10}+x^5+x^2+1$		$150X_{CPU}+148Sh_{CPU}$, $W=32$
11	Сложение		kX_{CPU}
12	Умножение, метод Comba, количество предвычислений [20, 23]: $\lceil\frac{l+w}{W}\rceil(2^w-w-3)X_{CPU}+(w-1)Sh_{CPU}$	2^w-1 элементов поля, как правило $w=4$	$\lceil\frac{l}{w}\rceil\lceil\frac{l+w}{W}\rceil X_{CPU}+2k(\frac{W}{w}-1)Sh_{CPU}$
13	Умножение, метод Comba [24]	2^w-1 элементов поля, как правило $w=4$	$k(\frac{l}{w}+2^w-w-1)X_{CPU}+$ $+(w-1+2(\frac{W}{w}-1))Sh_{CPU}$
14	Умножение, метод Карацубы, рассматривались такие поля, что двоичная длина элемента поля $l=2^i$, $i\in N$		$10(3^h-2^h)X_{CPU}+3^hM_{W\times W}$, где $h=\log_2\lvert\frac{l}{Wq}\rvert$, причем $q\cdot 2^h\cdot W\ge l$

15	Умножение, метод Карацубы [17]		Представлены в таблице для различного числа k машинных слов длиной $W = 32$ k | $M_{W\times W}$ 2 | 3 3 | 6 4 | 9 5 | 15 6 | 18 7 | 24 8 | 27
16	Возведение в квадрат, [20 (algorithm 7)]	512 байт	$2k\left(X_{CPU}+4Sh_{CPU}\right)$
17	Возведение в степень, методом «возведение в квадрат и умножение» (умножение методом Comba, возведение в квадрат [20 (algorithm 7)])		$\frac{1}{2}l\left(\left\lceil\frac{l}{w}\right\rceil\left\lceil\frac{l+w}{W}\right\rceil X_{CPU}+2k\left(\frac{W}{w}-1\right)Sh_{CPU}\right)+$ $+l2k\left(X_{CPU}+4Sh_{CPU}\right)$
18	Возведение в степень, методом Lim-Lee [19], умножение методом Comba, возведение в квадрат [20 (algorithm 7)]	$v\left(2^h-1\right)$	$\left(\frac{2^h-1}{2^h}a-2\right)\left(\left\lceil\frac{l}{w}\right\rceil\left\lceil\frac{l+w}{W}\right\rceil X_{CPU}+\right.$ $+2k\left(\frac{W}{w}-1\right)Sh_{CPU}\Big)$ $+2bk\left(X_{CPU}+4Sh_{CPU}\right)$

l - двоичная длина показателя. $M_{W\times W}$ - операция умножения в двух машинных слов. X_{CPU} - операция XOR процессора. Sh_{CPU} - операция сдвига процессора. $k=\lceil l/W\rceil$ - количество машинных слов двоичной длиной W, необходимых для хранения в памяти числа двоичной длины l. h - число блоков, на которые разбивается показатель в алгоритме Lim-Lee [19], $a=\left\lceil\frac{l}{h}\right\rceil$ - размер блока, v - число подблоков, на которые разбивается каждый блок, размер блока $b=\left\lceil\frac{a}{v}\right\rceil$. Варьируя значениями h и v можно достигнуть требуемой производительности при известных ограничениях на размер памяти для хранения предвычислений. Оптимальные значения для современных персональных компьютеров составляют $h=8$ и $v=3$ (или $v=4$) [18]. В работе [20] были предложены параметры $h=4$ и $v=1$, которые позволяют эффективно реализовать алгоритм Lim-Lee.

Проведем экспериментальную оценку сложности преобразований в двоичном поле. В таблице 9 приведены условия проведения экспериментов, результаты которых использовались далее для сравнения.

Таблица 9. Условия проведения экспериментов

Кол.	Источник	Процессор	Компилятор	Операционная система	Особенности реализации
1	[17]	Sun, UltraSPARC III 900 MHz	Sun Solaris 9	GNU gcc 3.1	Без ассемблера, производилась эмуляция 32-разрядного режима на 64-разрядной архитектуре
2	[17]	Sun, UltraSPARC III 900 MHz	Sun Solaris 9	gcc 3.1	Без ассемблера, оптимизация с учетом 64-разрядной архитектуры на уровне компилятора
3	[17]	Intel, Pentium III 1 GHz	Linux	gcc 2.95.3	Без ассемблера
4	[20]	Intel, Pentium II 400 MHz	MS Windows 2000	MS Visual C++ 6.0	С ассемблером
5	Авторы	AMD, AthlonXP 2500+ MHz	MS Windows XP	MS Visual C++ 2005	Без ассемблера

В таблице 10 сведем результаты экспериментальных оценок сложности операций в двоичном поле.

Таблица 10. Экспериментальные оценки времени выполнения полевых операций

	Операция	1, μs	2, μs	3, μs	4, μs	5, μs
163	Сложение				0,10	0.022

	Умножение, метод Comb	3,9	3,4	2,8	3,0	2.35
	Умножение, метод Карацубы	2,3	1,3	1,9	3,92	-
	Приведение по модулю	0,7	0,4	0,4	0,18	0.039
	Возведение в квадрат	0,8	0,5	0,5	0,4	0.089
	Инвертирование, расширенный алгоритм Эвклида				30,99	44.53
233	Сложение				0,12	0.026
	Умножение, метод Comb	5,8	4,8	3,8	5,07	3.56
	Умножение, метод Карацубы	2,8	1,5	2,9	7,04	-
	Приведение по модулю	0,3	0,2	0,3	0,22	0.034
	Возведение в квадрат	0,5	0,4	0,4	0,55	0.097
	Инвертирование, расширенный алгоритм Эвклида				53,22	76,25
283	Сложение				0,13	0,031
	Умножение, метод Comb	6,6	5,8	4,5	6,23	4,281
	Умножение, метод Карацубы	4,5	3,3	4,4	8,01	-
	Приведение по модулю	0,7	0,5	0,5	0,35	0,144
	Возведение в квадрат	1,0	0,8	0,6	0,75	0,207
	Инвертирование, расширенный алгоритм Эвклида				70,32	92,34
409	Сложение					0,046
	Умножение, метод Comb	10,7	8,9	6,9		6,907
	Умножение, метод Карацубы	8,5	4,7	8,1		-
	Приведение по модулю	0,5	0,3	0,4		0,146
	Возведение в квадрат	0,8	0,6	0,6		0,261
	Инвертирование, расширенный алгоритм Эвклида					163,29
571	Сложение					0,060
	Умножение, метод Comb	17,7	12,8	10,6		11,07
	Умножение, метод Карацубы	16,4	7,0	13,4		-
	Приведение по модулю	1,3	0,9	0,9		0,236
	Возведение в квадрат	1,8	1,2	1,2		0,382
	Инвертирование, расширенный алгоритм Эвклида					265,94

Кроме непосредственного представления элемента поля в качестве элемента группы, рассмотрим альтернативные подходы к представлению групповых элементов. Одним из таких представлений, является XTR, название происходит от аббревиатуры ECSTR (Efficient and Compact Subgroup Trace Representation).

Представление XTR

Описание задачи

Пусть даны простые числа p и q, такие, что $p \equiv 2 \bmod 3$ и $q \mid (p^2 - p + 1)$, причем частное является небольшим. Пусть g образует подгруппу G_{p^2-p+1} в $F_{p^6}^{\times}$ порядка q. Подгруппа G_{p^2-p+1} в $F_{p^6}^{\times}$ (далее $\langle g \rangle$) представляет интересн, с криптографической точки зрения, т.к. она не может быть внедрена в собственное подполе поля F_{p^6}. Для p и q, соответствующего размера, задача дискретного логарифма в $\langle g \rangle$, является такой же сложной, как и для $F_{p^6}^{\times}$ [25].

Сложность криптоанализа

Сложность решения задачи дискретного логарифмирования при XTR представлении элементов группы эквивалентно сложности решения задачи дискретного логарифма в поле. Согласно исследованиям [25], эвристическая асимптотическая оценка времени выполнения алгоритма NFS решета поля чисел составит $L\left[p^s, \frac{1}{3}, 1.923\right]$, где $L[n, v, u] = \exp\left((u + o(1))(\ln n)^v (\ln \ln n)^{1-v}\right)$, в случае характеристики поля $p = 2$, константу $u = 1.923$ следует заменить на $u = 1.53$. В качестве альтернативы, можно рассматривать алгоритм ρ-Pollard, но он не является таким эффективным, как алгоритм, указанный ранее.

Известно, что в данном случае, сложность задачи дискретного логарифмирования зависит от размера минимального «внешнее», содержащего рассматриваемую группу, $\mathbf{GF}(p^t)$. Другими словами, решение задачи дискретного логарифма в XTR представлении сводится к решению задачи дискретного логарифма в поле $\mathbf{GF}(p^t)$, а это в свою очередь соответствует решению задачи факторизации с размером модуля преобразований $t \cdot \log_2 p$ бит. Параметры XTR подбираются таким образом, что бы минимальное «внешнее», которое содержит группу, в которой решается задача, должно быть равным $\mathbf{GF}(p^6)$, при достаточно большом простом p. Проведенные исследования [25] показали, что сложность данной задачи может быть сведена к задаче дискретного логарифма в поле $\mathbf{GF}(p^6)$. Другими словами сложность составит $L[p^6, \frac{1}{3}, 1.923]$. Таким образом, сложность решения задачи XTR в группе рассматриваемой в поле $\mathbf{GF}(p^6)$ будет соизмерима с решением задачи факторизации при двоичной длине модуля $6 \cdot \log_2 p$, т.е. $6 \cdot 170 = 1020$ битный модуль RSA соответствует 170 битному модулю XTR преобразований.

Сложность/производительность реализации

Согласно [26], в таблице 11 приведем сложность преобразований в поле $\mathbf{GF}(p^6)$, где $p \equiv 2 \bmod 9$, в операциях в поле $\mathbf{GF}(p)$.

Таблица 11. Сложность операций в поле $\mathbf{GF}(p^6)$ в операциях в поле $\mathbf{GF}(p)$

№	Операция в поле $GF(p^6)$	Сложность
1	Вычисление a^p или a^{p^5}	$1A_{F_p}$
2	Вычисление a^{p^2}, a^{p^3} или a^{p^4}	$2A_{F_p}$
3	Вычисление a^2	$12M_{F_p}$
4	Вычисление $a \cdot b$	$18M_{F_p}$
5	Возведение в степень, метод «возвести в квадрат и умножить» [16]	$8lM_{F_p}$
6	Возведение в степень, метод «возвести в квадрат и умножить» с представлением показателя в JSF виде [16]	$\approx 6.62lM_{F_p}$
7	Возведение в степень, метод «возвести в квадрат и умножить»	$12 + 6lM_{F_p}$
8	Одновременное возведение в степень, метод «возвести в квадрат и умножить» $a^m b^n$, следует хранить 31 элемент $\mathbf{GF}(p^6)$, вычисленные алгоритма Пиппенгера для $w = \frac{l}{10}$, $t = 5$ [26]	$2.93(l-10)M_{F_p}$
9	Возведение в степень, метод с адаптируемой шириной окна (скользяще окно) предвычислений, следует хранить 2^{w-1} элементов $\mathbf{GF}(p^6)$	$\left(2^{w-1} + \frac{l}{w+1} + l - w\right)18M_{F_p}$
10	Возведение в степень, метод Lim-Lee, следует хранить $v(2^h - 1)$ элементов поля $\mathbf{GF}(p^6)$	$\left(\frac{2^h-1}{2^h}a - 2\right)18M_{F_p} + b12M_{F_p}$

M_{F_p} - операция умножения в поле $\mathbf{GF}(p)$, $A_{\mathbf{GF}(p)}$ - операция сложения в поле $\mathbf{GF}(p)$. l двоичная длина показателя. JSF – joint sparse form [26]

Таблица 12. Условия проведения экспериментальных оценок времени выполнения RSA, XTR DSA [25], ECDSA [22]

Криптосистема	Источник	Процессор	Операционная система	Компилятор	Особенности реализации
ECDSA	[22]	Intel, Pentium II 400 MHz	MS Windows 2000	MS Visual C++ 6.0	С ассемблером
RSA, XTRDSA	[25]	Intel, Pentium II 450 MHz		C	

Приведем в таблице 12 результаты сравнения экспериментальных оценок времени формирования и проверки цифровой подписи посредством RSA, XTR DSA [25], ECDSA [22].

Таблица 13. Экспериментальные оценки времени выполнения RSA, XTR DSA [25], ECDSA [22]

Преобразования	Длина ключа	Время формирования ключа, мс	Формирование подписи	Проверка подписи
RSA	1020	1224	5	40 (w/ CRT: 123)
XTRDSA	170	73	23	11
ECDSA	192		0,681	3,94

В таблице 13 приведем теоретическую оценку сложности преобразований XTRDSA, ECDSA.

Таблица 14. Теоретическая оценка числа операций умножения в поле $\mathbf{GF}(p)$ для XTR, EC [25], $\log_2 p = 170$

Название примитива	Формирование	Проверка
XTRDSA	1700	2575
ECDSA	1360	2754

Другим альтернативным представлением алгебраической структуры является CEILIDH представление, которое расшифровывается как Compact, Efficient, Improves on LUC, and Improves on Diffie-Hellman [16, 26]. Остановимся на нем более подробно.

Представление CEILIDH

Описание задачи

Данное представление является механизмом для сжатия/ разворачивания элементов циклотомической группы $G_{p^2-p+1} \subset \mathbf{F}_{p^6}^{\times}$, оно основывается на наблюдении, что элементы поля $\mathbf{GF}(p^6)$ лежат в этой подгруппе и выглядят как $\mathbf{GF}(p)$-рациональные точки на алгебраическом торе $\mathbf{T}_6$.

Сложность криптоанализа

Сложность решения задачи дискретного логарифма в группе представленной в виде CEILIDH, аналогична решению задачи дискретного логарифма для простого поля, в котором длина двоичного представления элемента равна $6 \cdot \log_2 p$. Это позволяет говорить о достаточно высокой степени стойкости.

Сложность/производительность реализации

Таблица 15. Теоретическая оценка сложности преобразований в CEILIDH представлении группы [16, 26]

№	Операция	Сложность
1	Умножение	$18M_{F_p} + 53A_{F_p}$
2	Возведение в квадрат	$6M_{F_p} + 21A_{F_p}$
3	Инвертирование	$12A_{F_p}$

4	Фробениус	$1A_{F_p}$
5	Сжатие	$15M_{F_p}+31A_{F_p}+1I_{F_p}$
6	Разворачивание	$27M_{F_p}+52A_{F_p}+1I_{F_p}$
7	Возведение в степень двоичной длины l в JSF (Joint Sparse Form)	$\frac{l}{2}\left(6M_{F_p}+21A_{F_p}\right)+\frac{l}{4}\left(18M_{F_p}+53A_{F_p}\right)$
8	Возведение в степень, метод «возведение в квадрат умножение»	$\frac{l}{2}\left(18M_{F_p}+53A_{F_p}\right)+l\left(6M_{F_p}+21A_{F_p}\right)$
9	Возведение в степень, метод с фиксированной шириной окна предвычислений, следует хранить 2^{w-1} элементов $\mathbf{GF}\left(p^6\right)$	$\left(\left\lfloor\frac{l-1}{w}\right\rfloor\left(w+1-2^{-w}\right)+1-2^{-((l-1)\bmod w)}\right)\times$ $\times\left(18M_{F_p}+53A_{F_p}\right)$
10	Возведение в степень, метод Lim-Lee, следует хранить $v\left(2^h-1\right)$ элементов $\mathbf{GF}\left(p^6\right)$	$\left(\frac{2^h-1}{2^h}a-2\right)\left(18M_{F_p}+53A_{F_p}\right)+$ $+b\left(6M_{F_p}+21A_{F_p}\right)$

Количество операций процессора для основных криптографических примитивов, получаются посредством подстановки выражений из таблиц 4, 11 и 14.

Таблица 16. Теоретическая оценка сложности, в полевых операциях, криптопримитивов основанных на задаче дискретного логарифмирования в различных представлениях элементов группы

Представление		Обычное представление	XTR	CEILIDH
Diffie-Hellman		$2E_{F_p} + 2R_{F_p}$	$\left(\frac{2^h-1}{2^h}a-2\right)36M_{F_p} + b24M_{F_p}$	$2\left(\frac{2^h-1}{2^h}a-2\right)\left(18M_{F_p}+53A_{F_p}\right)+2b\left(6M_{F_p}+21A_{F_p}\right)$
ElGamal	Зашифровывание	$2E_{F_p} + 2R_{F_p}$	$\left(\frac{2^h-1}{2^h}a-2\right)36M_{F_p} + b24M_{F_p}$	$2\left(\frac{2^h-1}{2^h}a-2\right)\left(18M_{F_p}+53A_{F_p}\right)+2b\left(6M_{F_p}+21A_{F_p}\right)$
	Расшифровывание	$1E_{F_p}$	$12 + 6lM_{F_p}$	$\frac{l}{2}\left(18M_{F_p}+53A_{F_p}\right)+l\left(6M_{F_p}+21A_{F_p}\right)$
DSA	Формирование	$1E_{F_p} + 5R_{F_p} +$ $+1I_{F_p} + 2M_{F_p} + 1A_{F_p}$	$\left(\frac{2^h-1}{2^h}a-2\right)18M_{F_p} + b12M_{F_p} +$ $1I_{F_p} + 2M_{F_p} + 1A_{F_p}$	$\left(\frac{2^h-1}{2^h}a-2\right)\left(18M_{F_p}+53A_{F_p}\right)+b\left(6M_{F_p}+21A_{F_p}\right)+$ $1I_{F_p} + 2M_{F_p} + 1A_{F_p}$
	Проверка	$2E_{F_p} + 5R_{F_p} +$ $+1I_{F_p} + 3M_{F_p}$	$\left(\frac{2^h-1}{2^h}a-2\right)18M_{F_p} + b12M_{F_p} + 12 + 6lM_{F_p} +$ $1I_{F_p} + 3M_{F_p}$	$\left(\frac{2^h-1}{2^h}a-2\right)\left(18M_{F_p}+53A_{F_p}\right)+b\left(6M_{F_p}+21A_{F_p}\right)+$ $\frac{l}{2}\left(18M_{F_p}+53A_{F_p}\right)+l\left(6M_{F_p}+21A_{F_p}\right)+1I_{F_p}+3M_{F_p}$

E_{F_p} - операция экспоненцирования в поле, l - двоичная длина показателя, R_{F_p} - операция приведения по модулю, M_{F_p} - операция умножения, A_{F_p} - операция сложения.

Известно, что элементы группы могут быть также представлены точками эллиптической кривой, что позволяет уже говорить о ECDLP – задаче дискретного логарифма в группе точек эллиптической кривой. Остановимся на этой задаче детальнее.

Владислав Ковтун

Дискретный логарифм в группе точек эллиптической кривой над конечным полем

Описание задачи

Пусть даны точки $P, Q \in E(\mathbf{GF}(q))$, тогда **решением ECDLP** будем понимать решение уравнение $Q = lP$ относительно l или доказательстве того, что решение не существует. Необходимым условием является $Q \in \langle P \rangle$, т.е. $l \in [0, \mathrm{ord}(P) - 1]$, причем $\mathrm{ord}(P) \cdot Q = O$, где P - базовая точка, образующая группу, - порядок базовой точки $n = \mathrm{ord}(P)$, l - секретный ключ, Q - открытый ключ, O - точка на бесконечности.

Проведем краткий теоретический экскурс.

Эллиптической кривой E над полем k называется гладкая кривая, которая описывается множеством решений $(x, y) \in k^2$ уравнения в обобщенной форме Вейерштрасса [43, 44]:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_1, a_2, a_3, a_4, a_6 \in k,$$

и находится в аффинной плоскости $\mathbf{A}^2(\bar{k}) = \bar{k} \times \bar{k}$ с точкой O на ∞.

Альтернативным, является следующее определение. Эллиптическая кривая – гладкая кривая E из $\mathbf{P}^2$ над полем k из семейства кривых из $\mathbf{P}^2$ над полем k, образованных двумя кубиками $x_0x_1x_2 = 0$ и $x_0^3 + x_1^3 + x_2^3 = 0$ в форме Хассе [74]:

$$E_{(a,b)} : ax_0x_1x_2 + b\left(x_0^3 + x_1^3 + x_2^3\right) = 0,\ (a, b) \in \mathbf{P}^1.$$

С точки зрения практической реализации, следует рассматривать конкретные кривые, заданные над полями четной и нечетной характеристики.

Далее рассмотрим более специфичные представления эллиптической кривой над различными полями:

- Поле нечетной характеристики:
  - Представление Дочи-Икарт-Кохеля (Doche-Icart-Kohel)

$$E_{(a)} : y^2 = x^3 + ax^2 + 16ax,\ a \in k,\ a(a - 64) \neq 0.$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$. Впервые представлено [103] и развито в работе [104].

  - Представление Дочи-Икарт-Кохеля (Doche-Icart-Kohel) орентированное на утроение точек:

$$E_{(a)} : y^2 = x^3 + 3x^2 + 3a(x + 1)^2,\ a \in k,\ a \neq 0,\ a \neq \tfrac{9}{4}.$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$. Впервые представлено [103] и развито в работе [104].

  - Представление Эдвардса (Edwards)

$$E_{(c,d)} : x^2 + y^2 = c^2\left(1 + dx^2y^2\right),\ c, d \in k, d = 1.$$

Технически, кривая Эдвардса не является эллиптической, т.к. является сингулярной. Нейтральным элементом, в этом случае, является точка O на ∞ в координатах $(0, c)$. Отметим, что точка $(0, -c)$ обладет порядком 2, в то время как точки $(c, 0)$ и $(-c, 0)$ обладают порядком 4. Впервые представлено в работе [141].

- Представление Хассе (Hasse) - кубическая кривая в аффинных координатах:

$$E_{(d)} : x^3 + y^3 + 1 = 3dxy,\ d \in k.$$

или в стандартных проективных координатах:

$$E_{(d)} : X^3 + Y^3 + Z^3 = 3dXYZ,\ d \in k,\ d^3 \neq 1.$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(1:-1:0)$. Над полем с нетривиальным кубическим корем w из 1, существует две дургие точки на бесконечности $(1:-w:0)$ и $(1:-w^2:0)$. Впервые представление Хассе было представлено в [74, 142] и получило дальнейшее развитие в [108].

- Представление скрещивание Якоби (Jacobi intersection)

$$E_{(a)} : s^2 + c^2 = 1,\ as^2 + d^2 = 1,\ a \in k, a \neq 0 \text{ и } a \neq 1.$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:1)$ [111, 110].

- Представление в форме уравнения Якоби 4-ой степени (Jacobi quartics) ориентированное на удвоение

$$E_{(a)} : y^2 = x^4 + 2ax^2 + 1,\ a \in k,\ \mathrm{char}(k) \neq 2, 3,\ a^2 \neq 1.$$

Также может быть представлено в следующем частном виде:

$$E_{(a)} : y^2 = (1 - x^2)(1 - a^2x^2),\ a \in k,\ a^2 \neq 1.$$

Нейтральным элементом, в этом случае, является точка O на ∞ с координатами $(0, 1)$ [111, 112].

- Представление Монтгомери (Montgomery)

$$E_{(a,b)} : by^2 = x^3 + ax^2 + x,\ a, b \in k.$$

Нейтральным элементом, в этом случае, является точка O на ∞ в координатах $(0, 1)$ [101].

- Представление Вейерштрасса (Weierstrass)

$$E_{(a,b)} : y^2 = x^3 + ax^2 + b,\ a, b \in k,\ b \neq 0 \text{ и } a^3 + 27b^3 \neq 0$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$.

- Поле четной характеристики:
  - Двоичное представление Эдвардса (Edwards)

$$E_{(d_1,d_2)}: d_1(x+y)+d_2(x^2+y^2)=(x+x^2)(y+y^2),\ d_1, d_2 \in k.$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$ [141].

- Представление Вейерштрасса (Weierstrass)

$$E_{(a,b)}: y^2 + xy = x^3 + ax^2 + b,\ a, b \in k,$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0, 0)$ для случая $b \neq 0$, в противном случае $(0, 1)$.

Сложность криптоанализа

Детальное исследование вопроса криптоанализа ECDLP проводится в работе [21]. Согласно приведенных в [21] результатов, сложность решения ECDLP для стандартизированных кривых [12, 35], посредством метода ρ-Pollard, составляет $O\left(\left(\ln^c h\right)\sqrt{\pi\, h/2}\right)$ групповых операций, где h - наибольший простой делитель $\mathrm{ord}(P)$, c - небольшая константа.

Таблица 17. Соответствие двоичной длины ключей симметричных шифров, RSA и криптосистем построенных на эллиптических кривых над простыми и двоичными полями [21, 22]

Двоичная длина ключа симметричного алгоритма шифрования	Название симметричного алгоритма	Двоичная длина ключа RSA	Двоичная длина простого числа p для базового поля $\mathbf{GF}(p)$	Степень расширения m для базового поля $\mathbf{GF}(2^m)$
80	SKIPJACK	1248	192	163
112	Triple-DES	2432	244	233
128	AES Small	3248	256	283
192	AES Medium	7936	384	409
256	AES Large	15424	521	571

Сейчас, наиболее активные исследования производятся в области криптоанализа, которая позволит существенно снизить объемы вычислений для взлома конкретной криптосистемы (программно и/или аппаратно реализованной), посредством анализа информации полученной косвенным путем (Side Channel Attacks):

- Потребляемой энергии (Differential power analysis).
- Времени отклика (Time analysis).

К сожалению, данные исследования выходят за рамки данной работы.

Сложность/производительность реализации

Известно, что во всех криптографических примитивах на эллиптической кривой, основной операцией является операция скалярного умножения. В свою очередь, скалярное умножение может быть представлено в виде иерархии, рис. 4.

Рис. 4. Обобщенная иерархия операций при скалярном умножении в группе точек эллиптической кривой

Более подробная иерархия операций при скалярном умножении может быть представлена виде рис. 4.

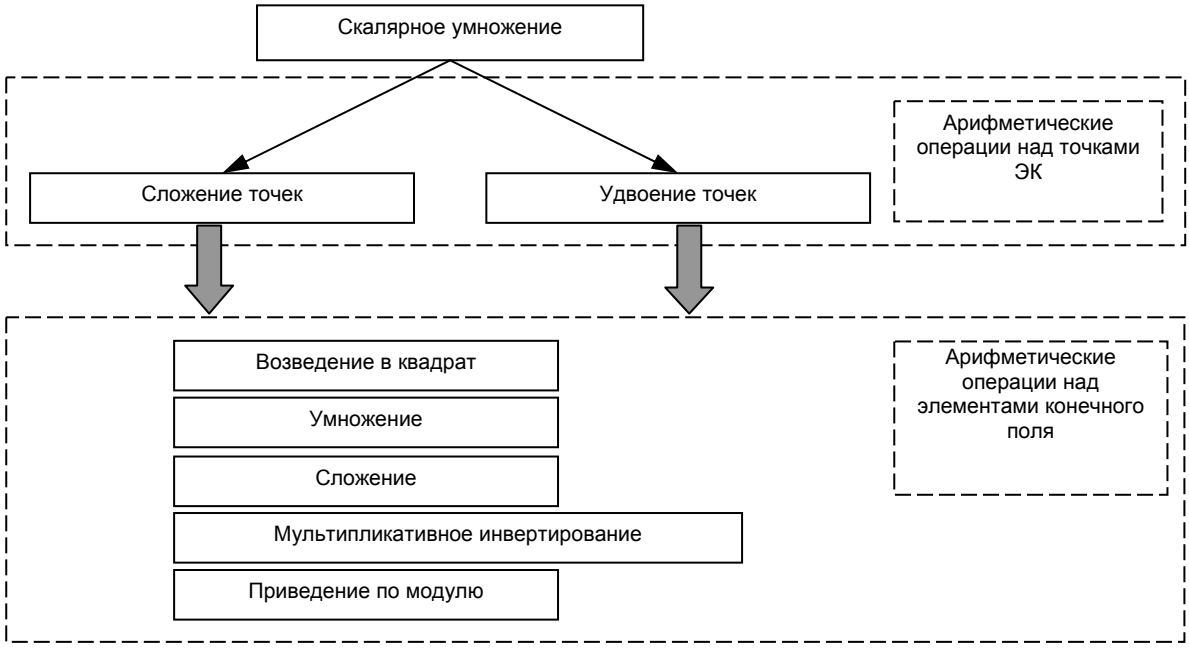


Рис. 5. Иерархия операций используемых для скалярного умножения точек эллиптической кривой

Рассмотрим сложности арифметики точек ЭК в различных формах и представлениях. В основу обзора, положена классификация и результаты опубликованные в работе [28] и БД арифметик в группе точек ЭК созданной Т. Ланге и опубликованной в сети Интернет по адресу: http://www.hyperelliptic.org/EFD.

Поле нечетной характеристики

Кривая в форме Вейерштраса (Weierstrass)

Арифметика для в стандартном проективном представлении $[X:Y:Z]$, таком, что $(x,y)\mapsto(X/Z,\ Y/Z)$ [138], для уравнения Вейрештрасса в общем виде изложена в работах [102, 104, 111, 144].

Таблица 18. Оценка сложности арифметики точек ЭК в форме Вейерштрасса в стандртном проективном представлении над полем нечетной характеристики [102, 104, 111, 144, 138]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 2S	5M + 2S
Сложение	Z2=1	9M + 2S	9M + 2S
Сложение		12M + 2S	12M + 2S

Сложение		11M + 6S + 1*a	11M + 6S + 1*a
Сложение		12M + 5S + 1*a	12M + 5S + 1*a
Сложение		10M + 4S + 1^3	10M + 4S + 1^3
Сложение		16M + 3S + 3^3	16M + 3S + 3^3
Удвоение	Z1=1	3M + 5S	
Удвоение		5M + 6S + 1*a	
Удвоение		6M + 5S + 1*a	
Удвоение		6M + 5S + 1^3 + 1*a	
Scale		1I + 2M	

В работе Кохен, Мияджи и Оно (Cohen–Miyaji–Ono) [102], предлагают использовать стандартное проективное представление $[X:Y:Z]$, такое, что $(x,y)\mapsto(X/Z,Y/Z)$, а также смешанной арифметики: слагаемые представлены в различных координатах. Введение допущения $a_4=-1$ в уравнении Вейрештрасса в общем виде (для сокращенного уравнения кривой $a=-1$) [136], позволяет повысить эффективность арифметики по сравнению с арифметикой для уравнения в общем виде.

Таблица 19. Оценка сложности арифметики точек ЭК в форме Вейерштрасса с $a_4=-1$ в стандртном проективном представлении над полем нечетной характеристики [102, 136]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 2S	5M + 2S
Сложение	Z2=1	9M + 2S	9M + 2S
Сложение		12M + 2S	12M + 2S
Сложение		13M + 3S	13M + 3S
Сложение		11M + 6S + 1*a	11M + 6S + 1*a
Сложение		12M + 5S + 1*a	12M + 5S + 1*a
Сложение		10M + 4S + 1^3	10M + 4S + 1^3
Сложение		16M + 3S + 3^3	16M + 3S + 3^3
Удвоение	Z1=1	3M + 5S	
Удвоение		5M + 6S + 1*a	
Удвоение		6M + 5S + 1*a	
Удвоение		6M + 5S + 1^3 + 1*a	
Scale		1I + 2M	

Альтернативное предположение в уравнении Вейрештрасса общем виде $a_4=-3$ (для сокращенного уравнения $a=-3$) для стандартного проективного представления $[X:Y:Z]$, такого, что $(x,y)\mapsto(X/Z,Y/Z)$ [137], позволяет достигнуть аналогичных результатов [102, 104, 111, 144].

Таблица 20. Оценка сложности арифметики точек ЭК в форме Вейерштрасса с $a_4=-3$ в стандртном проективном представлении над полем нечетной характеристики [102, 104, 111, 144, 137]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 2S	5M + 2S
Сложение	Z2=1	9M + 2S	9M + 2S
Сложение		12M + 2S	12M + 2S
Сложение		11M + 6S + 1*a	11M + 6S + 1*a
Сложение		12M + 5S + 1*a	12M + 5S + 1*a
Сложение		10M + 4S + 1^3	10M + 4S + 1^3
Сложение		16M + 3S + 3^3	16M + 3S + 3^3
Удвоение	Z1=1	3M + 5S	
Удвоение		7M + 3S	
Удвоение		5M + 6S + 1*a	
Удвоение		6M + 5S + 1*a	

Удвоение		6M + 5S + 1^3 + 1*a	
Scale		1I + 2M	

В работе [111] было предложено проективное представление Якоби (Jacobi) $[X:Y:Z]$, такое, что $(x, y)\mapsto (X/Z^2, Y/Z^3)$, причем сделаем следующее допущение в уравнении Вейрештрасса в общем виде $a_4=-3$ (для сокращенного уравнения $a=-3$) [134]. Дальнейшее развитие предложенного подхода было предложено авторами работ [102, 104, 115, 116, 117, 118, 119].

Таблица 21. Оценка сложности арифметики точек ЭК в форме Вейрштрасса в проективном представлении Якоби над полем нечетной характеристики [102, 104, 111, 115, 116, 117, 118, 119, 134]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	4M + 2S	4M + 2S
Сложение	Z2=1	7M + 4S	7M + 4S
Сложение	Z2=1	8M + 3S	8M + 3S
Сложение	Z2=1	8M + 3S	8M + 3S
Сложение	Z2=1	8M + 3S	8M + 3S
Сложение		11M + 5S	10M + 4S
Сложение		12M + 4S	11M + 3S
Сложение		12M + 4S	11M + 3S
Сложение	half*2=1	12M + 4S + 1*half	11M + 3S + 1*half
Сложение		8M + 6S + 2^3	8M + 5S + 1^3
Сложение		10M + 5S + 3^3	10M + 4S + 2^3
Сложение		10M + 5S + 4^3	10M + 4S + 3^3
Удвоение	Z1=1	1M + 5S	
Удвоение		3M + 5S	
Удвоение	2*half=1	4M + 4S + 1*half	
Удвоение	2*half=1	4M + 4S + 1*half	
Удвоение		1M + 8S + 1*a	
Удвоение		3M + 6S + 1*a	
Удвоение	half*2=1	3M + 6S + 1*a + 1*half	
Удвоение		4M + 4S + 1^4	
Удвоение		3M + 3S + 2^4 + 1*a	
Удвоение		3M + 3S + 2^4 + 1*a	
Утроение		7M + 7S	
Утроение		5M + 10S + 1*a	
Утроение		8M + 7S + 1*a	
Утроение		9M + 5S + 1^3 + 2^4 + 1*a	
Преобрзование		1I + 3M + 1S	

Казалось бы, проективное представление Якоби (Jacobi) известно достаточно давно, однако в работе [145] было предложена следующая модикация $[X:Y:Z^2:Z^3]$, такая, что $(x, y)\mapsto (X/Z^2, Y/Z^3)$, с допущением $a_4=-3$ в уравнении Вейрештрасса в общем виде (для сокращенного уравнения $a=-3$) [139].

Таблица 22. Оценка сложности арифметики точек ЭК в форме Вейерштрасса с $a_4=-3$ в модифицированном проективном представлении Якоби над полем нечетной характеристики [145, 139]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	ZZ1=1 и ZZZ1=1 и ZZ2=1 и ZZZ2=1	4M + 2S	4M + 2S
Сложение	ZZ2=1 и ZZZ2=1	8M + 2S	8M + 2S
Сложение		12M + 2S	12M + 2S
Удвоение	ZZ1=1 и ZZZ1=1	4M + 3S	
Удвоение	ZZ1=1 и ZZZ1=1	4M + 3S	

Удвоение		7M + 2S	
Удвоение		6M + 4S + 1*a	
Scale		1I + 3M + 1S	

В работе [145] также рассматривается обобщенная арифметика в модифицированном проективном представлении Якоби (Jacobi) $\left[X:Y:Z^2:Z^3\right]$, $(x,y)\mapsto\left(X/Z^2,Y/Z^3\right)$, для уравнения Вейрештрасса [140].

Таблица 23. Оценка сложности арифметики точек ЭК в форме Вейерштрасса в модифицированном проективном представлении Якоби над полем нечетной характеристики [145, 140]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	ZZ1=1 и ZZZ1=1 и ZZ2=1 и ZZZ2=1	4M + 2S	4M + 2S
Сложение	ZZ2=1 и ZZZ2=1	8M + 2S	8M + 2S
Сложение		12M + 2S	12M + 2S
Удвоение	ZZ1=1 и ZZZ1=1	4M + 3S	
Удвоение		6M + 4S + 1*a	
Scale		1I + 3M + 1S	

В 2007 году Т. Ланге и Д. Бернштейном были полученые оптимизированные формулы для групповой арифметики в проективных координатах Якоби [104, 135].

Таблица 24. Оценка сложности арифметики точек ЭК в форме Вейерштрасса в проективном представлении Якоби над полем нечетной характеристики [102, 104, 111, 115, 116, 117, 118, 119, 135]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	4M + 2S	4M + 2S
Сложение	Z2=1	7M + 4S	7M + 4S
Сложение	Z2=1	8M + 3S	8M + 3S
Сложение	Z2=1	8M + 3S	8M + 3S
Сложение	Z2=1	8M + 3S	8M + 3S
Сложение		11M + 5S	10M + 4S
Сложение		12M + 4S	11M + 3S
Сложение		12M + 4S	11M + 3S
Сложение	half*2=1	12M + 4S + 1*half	11M + 3S + 1*half
Сложение		8M + 6S + 2^3	8M + 5S + 1^3
Сложение		10M + 5S + 3^3	10M + 4S + 2^3
Сложение		10M + 5S + 4^3	10M + 4S + 3^3
Удвоение	Z1=1	1M + 5S	
Удвоение		1M + 8S + 1*a	
Удвоение		3M + 6S + 1*a	
Удвоение	half*2=1	3M + 6S + 1*a + 1*half	
Удвоение		3M + 3S + 2^4 + 1*a	
Удвоение		3M + 3S + 2^4 + 1*a	
Утроение		5M + 10S + 1*a	
Утроение		8M + 7S + 1*a	
Утроение		9M + 5S + 1^3 + 2^4 + 1*a	
Scale		1I + 3M + 1S	

Кривая в форме уравнения Якоби (Jacobi) 4-ой степени (quartics)

Впервые арифметика для такой формы кривой была описана [111] в проективном представлении. Дальнейшее развитие подхода [111], для более быстрого вычисления удвоение, предлагается использовать следующее расширенное проективное представление $\left[X:X^2:Y:Z:Z^2\right]$ [107, 109, 113], такое, что $(x,y)\mapsto\left(X/Z,Y/Z\right)$ [127]. Основу предложенного представления составляет следующее предположение

$a^2 + c^2 = 1$, а также дополнительные предвычисления, которые хранятся как дополнительные координаты точки.

Таблица 25. Оценка сложности арифметики точек ЭК в форме Якоби – уравнения 4-ой степени (ориентированной на удвоения) в расширенном проективном представлении над полем нечетной характеристики [107, 109, 113, 127]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1 и k=a-1	6M + 3S + 1*k	6M + 3S + 1*k
Сложение	k=a-1	7M + 4S + 1*k	7M + 3S + 1*k
Удвоение	Z1=1	1M + 5S	
Удвоение		3M + 4S	
Удвоение		8S + 1*a + 2*c	
Удвоение		1M + 8S + 1*a	
Удвоение	a2=2*a	3M + 8S + 1*a2 + 1*a	
Удвоение	a2=2*a	2M + 7S + 1^4 + 1*a2 + 2*c	
Утроение		8M + 6S + 1*a	
Утроение	b=a^2-1	4M + 11S + 1*a + 1*b	
Scale		1I + 2M + 2S	

Альтернативной к стандартному проективному представлению является проективное представление $[X : Y : Z]$ [104, 109, 112, 113, 114], такое, что $(x, y) \mapsto (X/Z, Y/Z^2)$ [132]. По сути, оно является аналогий проективному представлению Лопеса-Дахаба для двоичных кривых [30].

Таблица 26. Оценка сложности арифметики точек ЭК в форме Якоби – уравнения 4-ой степени в проективном представлении Лопеса-Дахаба над полем нечетной характеристики [104, 109, 112, 113, 114, 132]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 2S + 1*a	5M + 2S + 1*a
Сложение	Z2=1	8M + 3S + 1*a	8M + 3S + 1*a
Сложение		10M + 3S + 1*a	9M + 3S + 1*a
Сложение		8M + 6S + 1*a	8M + 3S + 1*a
Сложение		10M + 4S + 1*a	9M + 2S + 1*a
Сложение	b=-2*a	10M + 4S + 1*b	9M + 2S + 1*b
Сложение		19M + 8S + 1*a	18M + 6S + 1*a
Сложение	Z1=1 и Z2=1	2I + 11M + 5S + 1*a	2I + 11M + 4S + 1*a
Удвоение	a2=2*a и Z1=1	1M + 4S + 1*a2	
Удвоение	b=4-4*a^2	2M + 6S + 1*a + 1*b	
Удвоение	a2=2*a	2M + 6S + 1*a2	
Удвоение	a2=2*a	3M + 6S + 2*a2	
Удвоение		1M + 9S + 1*a	
Удвоение		19M + 8S + 1*a	
Удвоение		19M + 8S + 1*a	
Scale		1I + 2M + 1S	

Для предложенного проективного представления Лопеса-Дахаба $[X : Y : Z]$, такого, что $(x, y) \mapsto (X/Z, Y/Z^2)$ [129]. За счет введения дополнительного предположения $a^2 + c^2 = 1$, достигается повышение производительности операции удвоения [104, 109, 112, 113, 114].

Таблица 27. Оценка сложности арифметики точек ЭК в форме Якоби – уравнения 4-ой степени (ориентированной на удвоения) в проективном представлении Лопеса-Дахаба над полем нечетной характеристики [104, 109, 112, 113, 114, 129]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 2S + 1*a	5M + 2S + 1*a

Сложение	Z2=1	8M + 3S + 1*a	8M + 3S + 1*a
Сложение		10M + 3S + 1*a	9M + 3S + 1*a
Сложение		8M + 6S + 1*a	8M + 3S + 1*a
Сложение		10M + 4S + 1*a	9M + 2S + 1*a
Сложение	b=-2*a	10M + 4S + 1*b	9M + 2S + 1*b
Сложение		19M + 8S + 1*a	18M + 6S + 1*a
Сложение	Z1=1 и Z2=1	2I + 11M + 5S + 1*a	2I + 11M + 4S + 1*a
Удвоение	a2=2*a и Z1=1	1M + 4S + 1*a2	
Удвоение	a2=2*a и c2=2*c	1M + 7S + 1*a2 + 1*c + 1*c2	
Удвоение	b=4-4*a^2	2M + 6S + 1*a + 1*b	
Удвоение	a2=2*a	2M + 6S + 1*a2	
Удвоение	a2=2*a	3M + 6S + 2*a2	
Удвоение		1M + 9S + 1*a	
Удвоение	a2=2*a	2M + 5S + 1^4 + 1*a2 + 2*c	
Удвоение		19M + 8S + 1*a	
Удвоение		19M + 8S + 1*a	
Scale		1I + 2M + 1S	

Дальнейшего повышения производительности достигается посредством введения дополнительных предвычислений в качестве координат к проективному представлению Лопеса-Дахаба $\left[X : X^2 : Y : Z : Z^2\right]$ [107, 109, 113], такому, что $(x, y) \mapsto \left(X/Z, Y/Z^2\right)$ [130].

Таблица 28. Оценка сложности арифметики точек ЭК в форме Якоби – уравнения 4-ой степени в расширенном проективном представлении Лопеса-Дахаба над полем нечетной характеристики [107, 109, 113, 130]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1 и k=a-1	6M + 3S + 1*k	6M + 3S + 1*k
Сложение	k=a-1	7M + 4S + 1*k	7M + 3S + 1*k
Удвоение	Z1=1	1M + 5S	
Удвоение		3M + 4S	
Удвоение		1M + 8S + 1*a	
Удвоение	a2=2*a	3M + 8S + 1*a2 + 1*a	
Утроение		8M + 6S + 1*a	
Утроение	b=a^2-1	4M + 11S + 1*a + 1*b	
Scale		1I + 2M + 2S	

Дальнейшее введение предвычислений в расширенное представление Лопеса-Дахаба $\left[X : X^2 : Y : Z : Z^2 : R\right]$, такое, что $(x, y) \mapsto \left(X/Z, Y/Z^2\right)$ и $R = 2XZ$ [104, 107, 109, 113, 114, 131], позволяет уменьшить сложность арифметики на одну операцию умножения.

Таблица 29. Оценка сложности арифметики точек ЭК в форме Якоби – уравнения 4-ой степени в модифицированном расширенном проективном представлении Допеса-Дахаба над полем нечетной характеристики [104, 107, 109, 113, 114, 131]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 4S + 1*a	5M + 4S + 1*a
Сложение	Z2=1 и k=a-1	6M + 3S + 1*k	6M + 3S + 1*k
Сложение	Z2=1	7M + 3S + 1*a	7M + 3S + 1*a
Сложение	k=a-1	7M + 3S + 1*k	7M + 3S + 1*k
Сложение		8M + 3S + 1*a	8M + 3S + 1*a
Сложение	b=-2*a и half*2=1	9M + 2S + 2*half + 1*b	9M + 2S + 1*half + 1*b
Удвоение	Z1=1	1M + 6S	
Удвоение		3M + 4S	
Удвоение		1M + 8S + 1*a	
Удвоение	a2=2*a	3M + 9S + 2*a2	
Утроение	b=a^2-1	4M + 11S + 1*a + 1*b	

Утроение		8M + 7S + 1*a	
Scale		1I + 2M + 1S	

Добавление дополнительной координаты к расширенному проективному представлению, позволяет говорить о модифицированном расширенном проективном представлении $[X : X^2 : Y : Z : Z^2 : R]$ [104, 107, 109, 113, 114], такое, что $(x, y) \mapsto (X/Z, Y/Z^2)$ и $R = 2XZ$ [128] с предположением $a^2 + c^2 = 1$. Такой подход позволяет снизить сложность операций удвоения в группе.

Таблица 30. Оценка сложности арифметики точек ЭК в форме Якоби – уравнения 4-ой степени (ориентированной на удвоения) с предположением $a^2 + c^2 = 1$ в модифицированном расширенном проективном представлении Лопеса-Дахаба над полем нечетной характеристики [104, 107, 109, 113, 114, 128]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 4S + 1*a	5M + 4S + 1*a
Сложение	Z2=1 и k=a-1	6M + 3S + 1*k	6M + 3S + 1*k
Сложение	Z2=1	7M + 3S + 1*a	7M + 3S + 1*a
Сложение	k=a-1	7M + 3S + 1*k	7M + 3S + 1*k
Сложение		8M + 3S + 1*a	8M + 3S + 1*a
Сложение	b=-2*a и half*2=1	9M + 2S + 2*half + 1*b	9M + 2S + 1*half + 1*b
Удвоение	Z1=1	1M + 6S	
Удвоение		3M + 4S	
Удвоение		8S + 1*a + 2*c	
Удвоение		1M + 8S + 1*a	
Удвоение	a2=2*a	3M + 9S + 2*a2	
Удвоение		2M + 8S + 1^4 + 1*a + 2*c	
Утроение	b=a^2-1	4M + 11S + 1*a + 1*b	
Утроение		8M + 7S + 1*a	
Scale		1I + 2M + 1S	

Кривая в форме скрещивания Якоби (Jacobi)

Применение ЭК в форме скрещивания Якоби для повышения производительности метода ECM факторизации упоминается в работе [111]. Предложенные в работе [111] идеи, активно эксплуатируются многими учеными и по сей день [106, 107, 109, 110], что и послужило использованию стандартного проективного представления $[S : C : D : Z]$, такого, что $(s, c, d) \mapsto (S/Z, C/Z, D/Z)$ [126].

Таблица 31. Оценка сложности арифметики точек ЭК в форме скрещивания Якоби в проективном представлении над полем нечетной характеристики [106, 107, 109, 110, 111, 126]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	8M + 2S + 1*a	8M + 1S + 1*a
Сложение	Z2=1	11M + 1S + 2*a	10M + 1S + 2*a
Сложение	Z2=1	11M + 2S + 1*a	10M + 2S + 1*a
Сложение	S2=1	11M + 2S + 1*a	10M + 2S + 1*a
Сложение		13M + 1S + 2*a	11M + 1S + 2*a
Сложение		13M + 2S + 1*a	11M + 2S + 1*a
Сложение		14M + 2S + 1*a	12M + 2S + 1*a
Сложение		20M + 2S + 1*a	18M + 2S + 1*a
Удвоение	Z1=1	2M + 4S	
Удвоение		2M + 5S + 1*a	
Удвоение		3M + 4S	
Удвоение		4M + 3S	

Удвоение		5M + 3S	
Удвоение		12M + 9S	
Утроение	b=a-1 и b2=2*b и b3=3*b и bb2=2*b*b	4M + 10S + 2*a + 1*b2 + 1*b3 + 1*bb2	
Утроение	b=a-1 и b2=2*b и bb2=2*b*b и b3=3*b	4M + 10S + 2*a + 1*b2 + 1*b3 + 1*bb2	
Утроение	b=a-1	7M + 7S + 3*b	
Утроение	b=a-1	7M + 7S + 5*b	
Scale		1I + 3M	

Дальнейшего увеличения производительности от предложенного подхода, позволяет добиться посредлством внесения дополнительных предвычислений в проективное представление. Следующее расширенное проективное представление $[S:C:D:Z:SC:DZ]$ [143], такое, что $(s, c, d) \mapsto (S/Z, C/Z, D/Z)$, $SC = SC$ и $DZ = DZ$, было предложено в работе [107] авторами Х. Хисли, К. Вонг, Г. Картером и Э. Доусоном.

Таблица 32. Оценка сложности арифметики точек ЭК в форме скрещивания Якоби в раширенном представлении над полем нечетной характеристики [106, 107, 109, 110, 143]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1	10M + 1S + 2*a	10M + 1S + 2*a
Сложение	Z1=1 и Z2=1	10M + 2S + 1*a	10M + 1S + 1*a
Сложение		11M + 1S + 2*a	11M + 1S + 2*a
Сложение	Z2=1	13M + 2S + 1*a	12M + 2S + 1*a
Сложение	S2=1	13M + 2S + 1*a	12M + 2S + 1*a
Сложение		15M + 2S + 1*a	13M + 2S + 1*a
Сложение		16M + 2S + 1*a	14M + 2S + 1*a
Сложение		22M + 2S + 1*a	20M + 2S + 1*a
Удвоение		2M + 5S + 1*a	
Удвоение	Z1=1	4M + 4S	
Удвоение		5M + 4S	
Удвоение		6M + 3S	
Удвоение		7M + 3S	
Удвоение		14M + 9S	
Утроение	b=a-1 и b2=2*b и b3=3*b и bb2=2*b*b	6M + 10S + 2*a + 1*b2 + 1*b3 + 1*bb2	
Утроение	b=a-1 и b2=2*b и bb2=2*b*b и b3=3*b	6M + 10S + 2*a + 1*b2 + 1*b3 + 1*bb2	
Утроение	b=a-1	9M + 7S + 3*b	
Утроение	b=a-1	9M + 7S + 5*b	
Scale		1I + 4M	

Кривая в форме Монтгомери (Montgomery)

В 1987 году Монтгомери описал такую форму ЭК кривой, для которой предложил дифференциальную формулу сложения точек кривой (вычисляются лишь X-координаты точки при сложении и удвоении, без необходимости вычисления Y-координаты) [101]. На основе описанного подхода, исключение операции мультипликативного инвертирования посредством проективного представления $[X:Z]$, такое, что $(x, y) \mapsto (X/Z, Y/Z)$ [133], позволило существенно повысить производительность арифметики в группе.

Таблица 33. Оценка сложности арифметики точек ЭК в форме Монтгомери в проективном представлении над полем нечетной характеристики [101, 133]

Операция	Условие	Сложность	Сложность при повторном сложении
Удвоение	4*a24=a+2	2M + 2S + 1*a24	
Удвоение	4*a24=a+2	4M + 3S + 1*a24	

Удвоение		3M + 5S + 1*a	
diffadd	Z1=1	3M + 2S	
diffadd		4M + 2S	
diffadd		6M + 2S	
diffadd		6M + 2S	
ladder	Z1=1 и 4*a24=a+2	5M + 4S + 1*a24	
ladder	4*a24=a+2	6M + 4S + 1*a24	
ladder	4*a24=a+2	10M + 5S + 1*a24	
ladder		9M + 7S + 1*a	
Scale		1I + 1M	

Кривая в форме Хассе (Hesse)

Применение ЭК в форме Хассе для повышения производительности метода ECM факторизации упоминается еще в работе [111], дальнейшее развитие арифметики в группе ЭК в форме Хассе описывается в работах [74, 108]. Стандартное проективное представление $[X:Y:Z]$ для ЭК форме Хассе было предложено в работе [111], такое, что $(x, y)\mapsto(X/Z, Y/Z)$ [125], дальнейшее развитие предложенного подхода изложено в [109].

Таблица 34. Оценка сложности арифметики точек ЭК в форме Хассе в стандартном проективном представлении над полем нечетной характеристики [107, 108, 109, 125]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	8M	7M
Сложение	Z2=1	10M	10M
Сложение		12M	12M
Сложение		12M	12M
Сложение	X2=1	5M + 9S	5M + 6S
Сложение		6M + 12S	6M + 6S
Сложение		12M + 6S	9M + 3S
Удвоение	Z1=1	3M + 3S	
Удвоение		7M + 1S	
Удвоение		7M + 1S	
Удвоение		3M + 6S	
Удвоение		3M + 6S	
Удвоение		6M + 3S	
Удвоение		12M	
Удвоение		3M + 6^3	
Утроение	3*b*d=1	8M + 6S + 1*b	
Утроение	a=3*d	11M + 4S + 2*a	
Утроение		10M + 1S + 29^3 + 2*d	
Scale		1I + 2M	

Развитием идеи [111] стали публикации [108, 109], что позволило повысить эффективность арифметики в группе точек ЭК. Так, в [107], авторы Х. Хисли, К. Вонг, Г. Картер и Э.Доусон предлагают расширенное стандартное проективное представление точек $[X:Y:Z:X^2:Y^2:Z^2:XY:XZ:YZ]$, такое, что $(x, y)\mapsto(X/Z, Y/Z)$, $XY=2XY$, $XZ=2XZ$ и $YZ=2YZ$ [124], в котором за счет введения предвычислений в координаты проективного представления, позволяет уменьшить сложность арифметики.

Таблица 35. Оценка сложности арифметики точек ЭК в форме Хассе в расширенном проективном представлении над полем нечетной характеристики [107, 124]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1	5M + 6S	5M + 6S

Сложение		6M + 6S	6M + 6S
Удвоение		3M + 6S	
Удвоение		3M + 6S	
Scale		1I + 3M + 2S	

Кривая в форме Эдвардса (Edwards)

Активное исследование арифметики в группе точек ЭК в форме Эдвардса началось с публикации [141] группой ученых Т. Ланге и Д. Бернштейн с целью эффективной реализации групповых операций для применения в криптографических целях. Результаты были представлены 2007 году в работе [104].

В 2007 году Т. Ланге, П.Биркнер и Д. Бернштейн в их совместной работе [105], предлагают использовать стандартное проективное представление $[X:Y:Z]$, такое, что $(x, y)\mapsto(X/Z, Y/Z)$ [123].

Таблица 36. Оценка сложности арифметики точек ЭК в форме Эдвардса в стандартных проективной представлении над полем нечетной характеристики [105, 106, 107, 123]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	6M + 1S + 1*c + 1*d	6M + 1S + 1*c + 1*d
Сложение	k*c=1 и Z2=1	9M + 1*k	9M + 1*k
Сложение	X2=1	9M + 1S + 1*c + 1*d	9M + 1S + 1*c + 1*d
Сложение	Z2=1	9M + 1S + 1*c + 1*d	9M + 1S + 1*c + 1*d
Сложение	Z2=1	9M + 1S + 1*c + 1*d	9M + 1S + 1*c + 1*d
Сложение	c2=2*c и Z2=1	6M + 5S + 1*d + 1*c2	6M + 5S + 1*d + 1*c2
Сложение		10M + 1S + 1*c + 1*d	10M + 1S + 1*c + 1*d
Сложение		10M + 1S + 1*c + 1*d	10M + 1S + 1*c + 1*d
Сложение	i^2=-1	10M + 1S + 1*c + 1*d + 3*i	10M + 1S + 1*c + 1*d + 2*i
Сложение	k*c=1	11M + 1*k	11M + 1*k
Сложение	c2=2*c	7M + 5S + 1*d + 1*c2	7M + 5S + 1*d + 1*c2
Удвоение	cc2=2*c*c и Z1=1	3M + 3S + 2*c	
Удвоение		3M + 4S + 3*c	
Удвоение		3M + 4S + 3*c	
Удвоение		3M + 4S + 3*c	
Утроение	c2=2*c	9M + 4S + 1*c2	
Утроение		9M + 4S + 1*c	
Утроение	c=1	7M + 7S	
Утроение	cc4=4*c*c	7M + 7S + 1*cc4	
Scale		1I + 2M	

Т. Ланге и Д. Бернштейн в 2007 году совместно предложили инвертированное проективное представлении точек $[X:Y:Z]$, такое, что $(x, y)\mapsto(Z/X, Z/Y)$ [106, 107], которое позволило уменьшить сложность операций в группе.

Таблица 37. Оценка сложности арифметики точек ЭК в форме Эдвардса в инвертированном проективнм представлении над полем нечетной характеристики [106, 107, 122]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	7M + 2*c	7M + 2*c
Сложение	X2=1	8M + 1S + 2*c + 1*d	8M + 1S + 2*c + 1*d
Сложение	Z2=1	8M + 1S + 2*c + 1*d	8M + 1S + 2*c + 1*d
Сложение	Z2=1	9M + 1*c	9M + 1*c
Сложение		9M + 1S + 2*c + 1*d	9M + 1S + 2*c + 1*d
Сложение		11M + 1*c	11M + 1*c
Удвоение	ccd2=2*c*c*d и Z1=1	3M + 3S + 1*c	
Удвоение	ccd2=2*c*c*d	3M + 4S + 1*ccd2 + 1*c	

Утроение		9M + 4S + 1*c + 1*d	
Утроение	ccd=c*c*d	7M + 7S + 1*ccd	
Scale		1I + 2M	

Кривая в форме Дочи-Икарт-Кохеля (Doche-Icart-Kohel) ориентированная на удвоения

Авторами работы [120], в 2007 году, было предложено использовать ЭК определнной формы, которая в дальнейшем получила название Дочи-Икарт-Кохеля. Такая форма позволила в кооперации с предложенным проективным представлением $\left[X:Y:Z:Z^2\right]$, такое, что $(x,\,y)\mapsto\left(X/Z\,,Y/Z^2\right)$, существенно повысить производительность операции удвоения в группе точек ЭК. Проективное представление напоминает представление Лопеса-Дахаба для двоичных кривых [30]. В таблице 18, приведем сложности операций в группе.

Таблица 38. Оценка сложности арифметики точек ЭК в форме Doche-Icart-Kohel (ориентированной на удвоения) над полем нечетной характеристики [103, 104, 120]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	4M + 4S + 1*a	4M + 4S + 1*a
Сложение	Z1=1 и Z2=1	4M + 4S + 1*a	4M + 4S + 1*a
Сложение	Z1=1 и Z2=1	6M + 3S + 1*a	6M + 3S + 1*a
Сложение	Z2=1	8M + 4S + 1*a	8M + 4S + 1*a
Сложение	Z2=1	9M + 3S + 1*a	9M + 3S + 1*a
Сложение		12M + 5S + 1*a	12M + 5S + 1*a
Сложение		21M + 15S + 2^4 + 1*a	21M + 11S + 1^4 + 1*a
Сложение		7I + 12M + 9S + 1^4 + 1*a	4I + 9M + 8S + 1^4 + 1*a
Удвоение	a2=2*a и a16=16*a и Z1=1	1M + 5S + 1*a2 + 1*a	
Удвоение	a2=2*a	2M + 5S + 1*a2 + 1*a	
Удвоение	a4=4*a	3M + 4S + 1*a + 1*a4	
Удвоение	a16=16*a	3M + 8S + 1*a16 + 2*a	
Scale		1I + 2M + 1S	

Кривая в форме Дочи-Икарт-Кохеля (Doche-Icart-Kohel) ориентированная на утроения

В отличие от формы кривой, предложенной в работе [120] и в [121], в 2007 году была предложена другая форма кривой и соответствующее модифицированное проективное представление Якоби для точек ЭК $\left[X:Y:Z:Z^2\right]$, такое, что $(x,\,y)\mapsto\left(X/Z^2\,,Y/Z^3\right)$ [111, 104, 105]. Предложенный подход, в значительной мере, позволил повысить производительность операции утроения в группе.

Таблица 39. Оценка сложности арифметики точек ЭК в форме Doche-Icart-Kohel (ориентированной для утроений) над полем нечетной характеристики [104, 105, 121]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	a3=3*a и Z1=1 и Z2=1	4M + 2S + 1*a3	4M + 2S + 1*a3
Сложение	a3=3*a и Z1=1 и Z2=1	4M + 3S + 1*a3	4M + 3S + 1*a3
Сложение	a3=3*a и Z2=1	7M + 4S + 1*a3	7M + 4S + 1*a3
Сложение	a3=3*a и Z2=1	8M + 3S + 1*a3	8M + 3S + 1*a3
Сложение	a3=3*a	11M + 6S + 1*a3	10M + 6S + 1*a3
Сложение	a3=3*a	13M + 4S + 1*a3	12M + 4S + 1*a3
Сложение		15M + 11S + 5^3 + 1*a	15M + 7S + 3^3 + 1*a
Сложение		7I + 11M + 9S + 5^3 + 1*a	5I + 9M + 8S + 4^3 + 1*a
Удвоение	a2=2*a и a3=3*a и Z1=1	1M + 5S + 1*a2 + 1*a3	
Удвоение	a2=2*a и a3=3*a	2M + 7S + 1*a2 + 1*a3	

Удвоение	a3=3*a	4M + 5S + 1*a + 1*a3	
Удвоение	a3=3*a	4M + 5S + 1^4 + 2*a + 1*a3	
Утроение		6M + 6S + 2*a	
Утроение	b=4*a-9 и c=-3*a	6M + 7S + 1*a + 1*b + 1*c	
Scale		1I + 3M + 1S	

Сложность операций в группе

В таблицах 41-42 обобщается сложность выполнения восьми различных операций в группе. Далее воспользуемся следующими сокращениями:

- DBL: Удвоение $P_1 \mapsto P_1 + P_1$.
- ADD: Сложение $P_1, P_2 \mapsto P_1 + P_2$.
- reADD: Повторное сложение; т.е., сложение точек, при котором сложение произойдет, перед тем как все повторноиспользуемые промежуточные результаты будут закэшированы. $P_1, P_2 \mapsto P_1 + P_2$, когда все результаты зависящие исключительно от P_2 уже закешированы. Классическим примером может быть формула для вычисления $[X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]$ в представлении Якоби начинается с вычисления Z_1^2, Z_1^3, Z_2^2 и Z_2^3; кеширование Z_2^2 и Z_2^3 позволяет избежать следующего набора операций 1M+1S при повторном сложении с точкой $[X_1 : Y_1 : Z_1]$.
- preADD: Предварительное сложение; т.е., сложение точек, при котором сложение совместимо с наиболее быстрым повторным сложением. Иногда ADD является быстрее, чем reADD, т.к. существуют формулы более быстрого сложения обеспечивающее наиболее медленное последующее сложение.
- mADD: Смешанное сложение;т.е., сложение входных значений, при котором одна из точек обладает Z-координаты равной 1. $P_1, P_2 \mapsto P_1 + P_2$, когда $Z_2 = 1$.
- mreADD: Смешанное последующее сложение.
- mpreADD: Смещанное предварительное сложение.
- mDBL: Смешанное удвоение; т.е., удвоение точки с Z-координатой равной 1. $P_1 \mapsto P_1 + P_1$, когда $Z_1 = 1$.
- mmADD: Смешанное сложение;т.е., сложение точек обладающих Z-координатами равными 1. $P_1, P_2 \mapsto P_1 + P_2$, когда $Z_1 = 1$ и $Z_2 = 1$.
- mmreADD: Сложение точек обладающих Z-координатами равными 1, причем когда творая точка учавствовала в ложении ранее.
- mmpreADD.
- SUNI: Строго унифицированное сложение; т.е., сложение, которое выполняется без учета особенностей удвоение (нет необходимости сравнивать точки на равенство перед сложением).
- TPL: Утроение. $P_1 \mapsto P_1 + P_1 + P_1$.
- DADD: Дифференциальное сложение, т.е., сложение точек, чьи разницы известны заранее. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2$.
- mDADD: Смешанное дифференциальное сложение, т.е., сложение точек, чьи разницы известны заранее, причем Z-координата разницы равна 1. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2$, когда $Z(P_3 - P_2) = 1$.
- LADD: Лестничное сложение; т.е., дифференциальное сложение и удвоение одного из слагаемых. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2, P_2 + P_2$.

Криптография с открытм ключем. Текущее состояние

- mLADD: Смешанное лесничное сложение; т.е., смешанное дифференциальное сложение и удвоение одного из слагаемых. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2, P_2 + P_2$, когда $Z(P_3 - P_2) = 1$.
- SCALE: Преобразование точки из проективного представления к аффинному, когда Z-координата равна 1.

Содержимое таблиц отсортировано в порядке уменьшения сложности операции DBL; потом по уменьшению сложности операции ADD; и наконец, по уменьшению сложности операции reADD и т.д.

Владислав Ковтун

Для оценки вычислительной сложности, каждого метода сложения точек для различных форм описания уравнения эллиптической кривой для различных представлений, сделаем следующие предположения:

- Сложность операции мультипликативного инвертирования в поле I соответствует 100M операциям умножения в поле.
- Операция возведения в квадрат в поле S соответствует 0M операциям умножения в поле.
- Операция умножения на параметр кривой *param соответствует 1M операциям умножения в поле.
- Операция сложения в поле add соответствет 0M операциям умножения в поле.
- Операция умножения на константу *const соответствует 0M операциям умножения в поле.

В таблице 40-42 рассмотрим сложность всех описанных ранее операций для различных форм кривых и предствлений точек для указанного условия.

Таблица 40. Оценка сложности арифметики точек ЭК над полем нечетной характеристики

Уравнение кривой, представление	DBL	ADD	reADD	preADD	mADD	mreADD	mpreADD	mDBL	mmADD	mmreADD	mmpreADD	SUNI	TPL	DADD	mDADD	LADD	mLADD	SCALE
Short Weierstrass, projective	11	14	14	14	11	11	11	8	7	7	7	17						102
Short Weierstrass, projective with a4=-1	11	14	14	14	11	11	11	8	7	7	7	16						102
Short Weierstrass, XYZZ	10	14	14	14	14	14	14	10	14	14	14							104
Short Weierstrass, projective with a4=-3	10	14	14	14	11	11	11	8	7	7	7	17						102
Tripling-oriented Doche–Icart–Kohel, standard	9	17	16	17	11	11	11	6	6	6	6		12					104
Short Weierstrass, Jacobian	9	16	14	16	11	11	11	6	6	6	6		15					104
Short Weierstrass, XYZZ with a4=-3	9	14	14	14	14	14	14	9	14	14	14							104
Hessian, extended	9	12	12	12	11	11	11	9	11	11	11							105
Short Weierstrass, Jacobian with a4=-3	8	16	14	16	11	11	11	6	6	6	6		14					104
Jacobi quartic, doubling-oriented XYZ	8	13	11	14	11	11	11	5	7	7	7	13						103
Jacobi quartic, XYZ	8	13	11	14	11	11	11	5	7	7	7	13						103
Hessian, projective	8	12	12	12	10	10	10	6	8	7	8		14					102
Doubling-oriented Doche–Icart–Kohel, standard	7	17	17	17	12	12	12	6	8	8	8							103
Jacobi intersection, projective	7	14	12	14	12	11	12	6	10	9	10	14	14					103
Jacobi intersection, extended	7	12	12	12	11	11	11	7	11	11	11	12	16					104
Edwards, projective	7	11	11	11	9	9	9	6	7	7	7	11	13					102
Jacobi quartic, doubling-oriented XXYZZ	7	11	10	11	9	9	9	6	9	9	9	11	14					104
Jacobi quartic, XXYZZ	7	11	10	11	9	9	9	6	9	9	9	11	14					104
Jacobi quartic, XXYZZR	7	10	10	10	9	9	9	7	9	9	9	10	15					103
Jacobi quartic, doubling-oriented XXYZZR	7	10	10	10	9	9	9	7	9	9	9	10	15					103
Edwards, inverted	7	10	10	10	9	9	9	6	7	7	7	10	13					102
Montgomery, XZ	4							4						6	5	10	9	101

Рассмотрим оценки вычислительной сложности, каждого метода сложения точек для различных форм описания уравнения эллиптической кривой для различных представлений, со следующими допущениями:

- Сложность операции мультипликативного инвертирования в поле I соответствует 100M операциям умножения в поле.
- Операция возведения в квадрат в поле S соответствует 0M операциям умножения в поле.
- Операция умножения на параметр кривой *param соответствует 0,8M операциям умножения в поле.
- Операция сложения в поле add соответствет 0M операциям умножения в поле.
- Операция умножения на константу *const соответствует 0M операциям умножения в поле.

Таблица 41. Оценка сложности арифметики точек ЭК над полем нечетной характеристики

Уравнение кривой, представление	DBL	ADD	reADD	preADD	mADD	mreADD	mpreADD	mDBL	mmADD	mmreADD	mmpreADD	SUNI	TPL	DADD	mDADD	LADD	mLADD	SCALE
Short Weierstrass, projective	9.8	13.6	13.6	13.6	10.6	10.6	10.6	7.0	6.6	6.6	6.6	15.8						102.0
Short Weierstrass, projective with a4=-1	9.8	13.6	13.6	13.6	10.6	10.6	10.6	7.0	6.6	6.6	6.6	15.4						102.0
Short Weierstrass, projective with a4=-3	9.4	13.6	13.6	13.6	10.6	10.6	10.6	7.0	6.6	6.6	6.6	15.8						102.0
Short Weierstrass, XYZZ	9.2	13.6	13.6	13.6	13.6	13.6	13.6	9.2	13.6	13.6	13.6							103.8
Short Weierstrass, XYZZ with a4=-3	8.6	13.6	13.6	13.6	13.6	13.6	13.6	8.6	13.6	13.6	13.6							103.8
Hessian, projective	7.8	12.0	10.8	15.6	10.0	10.0	10.0	5.4	8.0	7.0	8.0		12.8					102.0
Hessian, extended	7.8	10.8	10.8	10.8	9.8	9.8	9.8	7.8	9.8	9.8	9.8							104.6
Tripling-oriented Doche–Icart–Kohel, standard	7.6	15.8	14.8	15.8	10.2	10.2	10.2	5.0	5.6	5.6	5.6		10.8					103.8
Short Weierstrass, Jacobian	7.4	15.0	13.2	15.0	10.2	10.2	10.2	5.0	5.6	5.6	5.6		13.0					103.8
Short Weierstrass, Jacobian with a4=-3	7.0	15.0	13.2	15.0	10.2	10.2	10.2	5.0	5.6	5.6	5.6		12.6					103.8
Jacobi quartic, XYZ	6.8	12.4	10.4	12.8	10.4	10.4	10.4	4.2	6.6	6.6	6.6	12.4						102.8
Jacobi quartic, doubling-oriented XYZ	6.6	12.4	10.4	12.8	10.4	10.4	10.4	4.2	6.6	6.6	6.6	12.4						102.8
Edwards, projective	6.2	10.8	10.8	10.8	9.0	9.0	9.0	5.4	6.8	6.8	6.8	10.8	12.2					102.0
Jacobi quartic, doubling-oriented XXYZZ	6.2	10.2	9.4	10.2	8.4	8.4	8.4	5.0	8.4	8.4	8.4	10.2	12.8					103.6
Jacobi quartic, XXYZZ	6.2	10.2	9.4	10.2	8.4	8.4	8.4	5.0	8.4	8.4	8.4	10.2	12.8					103.6
Edwards, inverted	6.2	9.8	9.8	9.8	8.8	8.8	8.8	5.4	7.0	7.0	7.0	9.8	12.2					102.0
Jacobi quartic, XXYZZR	6.2	9.4	9.4	9.4	8.4	8.4	8.4	5.8	8.2	8.2	8.2	9.4	12.8					102.8
Jacobi quartic, doubling-oriented XXYZZR	6.2	9.4	9.4	9.4	8.4	8.4	8.4	5.8	8.2	8.2	8.2	9.4	12.8					102.8
Doubling-oriented Doche–Icart–Kohel, standard	6.0	16.0	16.0	16.0	11.2	11.2	11.2	5.0	7.2	7.2	7.2							102.8
Jacobi intersection, projective	6.0	13.8	11.8	13.8	11.8	10.8	11.8	5.2	9.6	8.8	9.6	13.8	12.0					103.0
Jacobi intersection, extended	6.0	11.8	11.8	11.8	10.8	10.8	10.8	6.0	10.8	10.8	10.8	11.8	14.0					104.0
Montgomery, XZ	3.6							3.6						5.6	4.6	9.2	8.2	101.0

Таблица 42. Оценка сложности арифметики точек ЭК над полем нечетной характеристики

Curve shape, representation	DBL	ADD	reADD	preADD	mADD	mreADD	mpreADD	mDBL	mmADD	mmreADD	mmpreADD	SUNI	TPL	DADD	mDADD	LADD	mLADD	SCALE
Short Weierstrass, projective	9.02	13.34	13.34	13.34	10.34	10.34	10.34	6.35	6.34	6.34	6.34	15.02						102.00
Short Weierstrass, projective with a4=-1	9.02	13.34	13.34	13.34	10.34	10.34	10.34	6.35	6.34	6.34	6.34	15.01						102.00
Short Weierstrass, projective with a4=-3	9.01	13.34	13.34	13.34	10.34	10.34	10.34	6.35	6.34	6.34	6.34	15.02						102.00
Short Weierstrass, XYZZ	8.68	13.34	13.34	13.34	13.34	13.34	13.34	8.68	13.34	13.34	13.34							103.67
Short Weierstrass, XYZZ with a4=-3	8.34	13.34	13.34	13.34	13.34	13.34	13.34	8.34	13.34	13.34	13.34							103.67
Hessian, projective	7.02	12.00	10.02	14.04	10.00	10.00	10.00	5.01	8.00	7.00	8.00		12.02					102.00
Hessian, extended	7.02	10.02	10.02	10.02	9.02	9.02	9.02	7.02	9.02	9.02	9.02							104.34
Tripling-oriented Doche–Icart–Kohel, standard	6.69	15.02	14.02	15.02	9.68	9.68	9.68	4.35	5.34	5.34	5.34		10.02					103.67
Short Weierstrass, Jacobian	6.36	14.35	12.68	14.35	9.68	9.68	9.68	4.35	5.34	5.34	5.34		11.70					103.67
Short Weierstrass, Jacobian with a4=-3	6.35	14.35	12.68	14.35	9.68	9.68	9.68	4.35	5.34	5.34	5.34		11.69					103.67
Jacobi quartic, XYZ	6.02	12.01	10.01	12.02	10.01	10.01	10.01	3.68	6.34	6.34	6.34	12.01						102.67
Jacobi quartic, doubling-oriented XYZ	5.69	12.01	10.01	12.02	10.01	10.01	10.01	3.68	6.34	6.34	6.34	12.01						102.67
Edwards, projective	5.68	10.35	10.35	10.35	9.00	9.00	9.00	5.01	6.67	6.67	6.67	10.35	11.68					102.00
Jacobi quartic, XXYZZ	5.68	9.68	9.01	9.68	8.01	8.01	8.01	4.35	8.01	8.01	8.01	9.68	11.37					103.34
Edwards, inverted	5.68	9.67	9.67	9.67	8.67	8.67	8.67	5.01	7.00	7.00	7.00	9.67	11.68					102.00
Jacobi quartic, XXYZZR	5.68	9.01	9.01	9.01	8.01	8.01	8.01	5.02	7.68	7.68	7.68	9.01	11.37					102.67
Jacobi quartic, doubling-oriented XXYZZ	5.36	9.68	9.01	9.68	8.01	8.01	8.01	4.35	8.01	8.01	8.01	9.68	11.37					103.34
Jacobi quartic, doubling-oriented XXYZZR	5.36	9.01	9.01	9.01	8.01	8.01	8.01	5.02	7.68	7.68	7.68	9.01	11.37					102.67
Doubling-oriented Doche–Icart–Kohel, standard	5.35	15.35	15.35	15.35	10.68	10.68	10.68	4.35	6.68	6.68	6.68							102.67
Jacobi intersection, projective	5.35	13.67	11.67	13.67	11.67	10.67	11.67	4.68	9.34	8.67	9.34	13.67	10.70					103.00
Jacobi intersection, extended	5.35	11.67	11.67	11.67	10.67	10.67	10.67	5.35	10.67	10.67	10.67	11.67	12.70					104.00
Montgomery, XZ	3.34							3.34						5.34	4.34	8.68	7.68	101.00

Владислав Ковтун

В таблице 42 оценки вычислительной сложности, каждого метода сложения точек для различных форм описания уравнения эллиптической кривой для различных представлений, приведены со следующими допущениями:

- Сложность операции мультипликативного инвертирования в поле I соответствует 100M операциям умножения в поле.
- Операция возведения в квадрат в поле S соответствует 0M операциям умножения в поле.
- Операция умножения на параметр кривой *param соответствует 0,67M операциям умножения в поле.
- Операция сложения в поле add соответствет 0M операциям умножения в поле.
- Операция умножения на константу *const соответствует 0M операциям умножения в поле.

Поле четной характеристики

Кривая в форме Вейерштрасса (Weierstrass)

Исторически сложилось, что публикации Н. Коблица [168] и Миллера [169] базировались на аффинном представлении ЭК и ее точек (x, y) [154].

Таблица 43. Оценка сложности арифметики точек ЭК в форме Вейерштрасса (Weierstrass) в аффином представлении над полем четной характеристики [154]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение		1I + 2M + 1S	1I + 2M + 1S
Удвоение		1I + 2M + 1S	
Scale		0M	

Известно, что наиболее вычислительно сложной операцией в двоичном поле является мультипликативное инвертирование, избавиться от него при промежуточных вычислениях в скалярном умножении возможно посредством проективного представления. Исторически первыми было предложено стандартное проективное представление $[X : Y : Z]$, такое, что $(x, y) \mapsto (X/Z, Y/Z)$ [28, 161]. Арифметика в стандартном проективном представлении была усовершенствована в совместной работе Дочи иТ. Ланге в 2005 году [163], в 2008 году в работе Д. Бернштейна и Т. Ланге [162] предложенная идея была развита.

Таблица 44. Оценка сложности арифметики точек ЭК в форме Вейерштрасса в стандартном проективном представлении над полем четной характеристики [28, 161, 162, 163]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	7M + 1S + 1*a2	7M + 1S + 1*a2
Сложение	Z2=1	11M + 1S + 1*a2	11M + 1S + 1*a2
Сложение	Z2=1	11M + 2S + 1*a2	11M + 2S + 1*a2
Сложение		14M + 1S + 1*a2	14M + 1S + 1*a2
Сложение		15M + 2S + 1*a2	15M + 2S + 1*a2
Сложение		15M + 2S + 1^3 + 1*a2	15M + 2S + 1^3 + 1*a2
Удвоение	Z1=1	5M + 3S + 1*a2	
Удвоение		7M + 3S + 1*a2	
Удвоение		7M + 4S + 1*a2	
Scale		1I + 2M	

Проективное представление Якоби $[X : Y : Z]$, такое, что $(x, y) \mapsto (X/Z^2, Y/Z^3)$ было известно еще с момента публикации [111], однако С. Дочи и Т. Ланге в работе [163],

предложили подход, который был развит далее Д. Берштейна и Т. Ланге [162], который уменьшить количество полевых операций.

Таблица 45. Оценка сложности арифметики точек ЭК в форме Вейерштрасса в проективном представлении Якоби над полем четной характеристики [20, 28, 157, 162, 163]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1	10M + 3S + 1*a2	10M + 3S + 1*a2
Сложение		14M + 5S + 1*a2	13M + 4S + 1*a2
Удвоение	Z1=1	1M + 2S + 1*a6	
Удвоение		4M + 5S + 1*a6	
Scale		1I + 3M + 1S	

Развитие идеи изменения проективного представления $[X:Y:Z]$ точек кривой, такого, что $(x, y)\mapsto (X/Z, Y/Z^2)$, в 1998 году было предложено Д. Лопесом и Р. Дахабом в работе [30]. Развитие арифметики в проективном представлении Лопеса-Дахаба было изложено в работах [29, 30, 31, 163, 164, 165].

Таблица 46. Оценка сложности арифметики точек ЭК в форме Вейерштрасса в проективном представлении Лопеса-Дахаба над полем четной характеристики [29, 30, 31, 160, 163, 164, 165]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 3S + 1*a2	5M + 3S + 1*a2
Сложение	Z2=1	8M + 5S + 1*a2	8M + 5S + 1*a2
Сложение		13M + 4S	13M + 3S
Удвоение	Z1=1	1M + 3S + 1*a2 + 1*a6	
Удвоение		3M + 5S + 1*a2 + 1*a6	
Удвоение		4M + 4S + 1*a2	

Дальнейшего уменьшения количества полевых операций в проективной арифметике Лопеса-Дахаба $[X:Y:Z]$, $(x, y)\mapsto (X/Z, Y/Z^2)$, было достигнуто посредством рассмотрения особого класса кривых, для которых $a_2=1$ (или $a=1$) [29, 31, 32, 163, 164, 165].

Таблица 47. Оценка сложности арифметики точек ЭК в форме Вейерштрасса с $a_2=1$ в проективном представлении Лопеса-Дахаба над полем четной характеристики [29, 31, 32, 159, 163, 164, 165]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 3S + 1*a2	5M + 3S + 1*a2
Сложение	Z2=1	8M + 5S + 1*a2	8M + 5S + 1*a2
Сложение		13M + 4S	13M + 3S
Удвоение	Z1=1	1M + 3S + 1*a2 + 1*a6	
Удвоение	sqrt(a6)^2=a6	3M + 5S + 1*sqrta6	
Удвоение		3M + 5S + 1*a2 + 1*a6	
Удвоение		4M + 4S + 1*a2	

По аналогии с ранее изложенным подходом, в проективной арифметике Лопеса-Дахаба $[X:Y:Z]$, $(x, y)\mapsto (X/Z, Y/Z^2)$, были предложены особые кривые с $a_2=0$ (или $a=0$) [29, 31, 32, 163, 164, 165], что также позволило добиться уменьшения количества полевых операций.

Таблица 48. Оценка сложности арифметики точек ЭК в форме Вейерштрасса с $a_2=0$ в проективном представлении Лопеса-Дахаба над полем четной характеристики [29, 31, 32, 158, 163, 164, 165]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z1=1 и Z2=1	5M + 3S + 1*a2	5M + 3S + 1*a2
Сложение	Z2=1	8M + 5S + 1*a2	8M + 5S + 1*a2
Сложение		13M + 4S	13M + 3S
Удвоение	Z1=1	1M + 3S + 1*a2 + 1*a6	
Удвоение	sqrt(a6)^2=a6	3M + 5S + 1*sqrta6	
Удвоение		3M + 5S + 1*a2 + 1*a6	
Удвоение		4M + 4S + 1*a2	

Дальнейшего сокращения количества полевых операций, предлагается за счет внесения предвычисленных значений, например Z^2 в проективное представление, и использования кривых особого вида с $a_2 = 1$ (или $a = 1$) [31, 32, 163, 164, 166, 167]. После такого изменения, представление стало именоваться как расширенное проективное представление Лопеса-Дахаба $\left[X : Y : Z : Z^2\right]$, $(x, y) \mapsto \left(X/Z, Y/Z^2\right)$.

Таблица 49. Оценка сложности арифметики точек ЭК в форме Вейерштрасса с $a_2 = 1$ в расширенном проективном представлении Лопеса-Дахаба над полем четной характеристики [156, 31 32, 163, 164, 166, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1	8M + 4S	8M + 4S
Сложение	Z2=1	8M + 4S + 1*a2	8M + 4S + 1*a2
Сложение		13M + 3S	13M + 3S
Удвоение	sqrt(a6)^2=a6	2M + 4S + 1*a6 + 1*sqrta6	
Удвоение		2M + 5S + 2*a6	

По аналогии с рассмотренным выше подходом, авторами [163, 164, 167] было предложено расширить представление за счет дополнительных предвычислений и использовать кривые особого вида с $a_2 = 0$ (или $a = 0$). Полученное представление получило назнвание модифицированного расширенного проективного представления Лопеса-Дахаба $\left[X : Y : Z : Z^2 : XZ\right]$, $(x, y) \mapsto \left(X/Z, Y/Z^2\right)$.

Таблица 50. Оценка сложности арифметики точек ЭК в форме Вейерштрасса с $a_2 = 0$ в расширенном проективном представлении Лопеса-Дахаба над полем четной характеристики [155, 163, 164, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1	9M + 4S + 1*a2	9M + 4S + 1*a2
Сложение		14M + 3S	14M + 3S
Удвоение	Z1=1	2M + 3S + 1*a6	
Удвоение	sqrt(a6)^2=a6	2M + 5S + 1*a6 + 1*sqrta6	

Далее рассмотрим сводные таблицы, в которых приводится наименьшая сложность, среди известных представлений.

Кривая в форме Эдвардса (Edwards)

Применение кривых Эдвардса в криптографических целях начались после публикации Т. Ланге и Д. Бернштейна [104]. За основу, авторами было взято аффинное представление, которое является наиболее распространенным и удобным при первичном рассмотрении кривых. На сегоднешний день, наиболее эффективная арифметика для аффинного представления (x, y) опубликована в работе [167].

Таблица 51. Оценка сложности арифметики точек ЭК в форме Эдварса в аффинном представлении над полем четной характеристики [151, 167]

Операция	Условие	Сложность	Сложность при повторном сложении

Владислав Ковтун

Сложение		2I + 8M + 2S + 2*d1 + 1*d2	2I + 7M + 2S + 2*d1 + 1*d2
Удвоение	d2d1=d2/d1	1I + 2M + 4S + 1*d2d1 + 1*d2	
Удвоение		4I + 4M + 10S + 6^4 + 4*d2	
Scale		0M	

Рассмотрение более узкого класса кривых Эдвардса, для которых $d_1 = d_2$, в аффинном представлении (x, y), позволяет сократить количество полевых операций [167].

Таблица 52. Оценка сложности арифметики точек ЭК в форме Эдварса с $d_1 = d_2$ в аффинном представлении над полем четной характеристики [150, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение		2I + 8M + 2S + 2*d1 + 1*d2	2I + 7M + 2S + 2*d1 + 1*d2
Удвоение		1I + 1M + 4S + 2*d1	
Удвоение	d2d1=d2/d1	1I + 2M + 4S + 1*d2d1 + 1*d2	
Удвоение		4I + 4M + 10S + 6^4 + 4*d2	
Scale		0M	

Дальнейшее развитие описанного похода было предложено Т. Ланге и Р.Р. Фарашахи: использовать такое аффинное представление W, что паре (x, y) соответствует $W = x + y$ для уравнения кривой Эдвардса, было опубликовано в работе [167].

Таблица 53. Оценка сложности арифметики точек ЭК в форме Эдварса в аффинном W представлении над полем четной характеристики [147, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Удвоение	d2overd1plus1=d2/d1+1	1I + 1M + 2S + 1*d2overd1plus1	
diffadd	d2overd1plus1=d2/d1+1	1I + 3M + 1S + 1*d2overd1plus1	
ladder	d2overd1plus1=d2/d1+1	2I + 4M + 3S + 2*d2overd1plus1	
Scale		0M	

Введение дополнительного ограничения $d_1 = d_2$ на уравнение кривой (использование ограниченного класса кривых), в предложенную идею [167], позволило сократить количество полевых операций.

Таблица 54. Оценка сложности арифметики точек ЭК в форме Эдварса с $d_1 = d_2$ в аффинном W представлении над полем четной характеристики [146, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Удвоение		1I + 2S + 1*d1	
Удвоение	d2overd1plus1=d2/d1+1	1I + 1M + 2S + 1*d2overd1plus1	
diffadd		1I + 1M + 2S + 1*d1	
diffadd	d2overd1plus1=d2/d1+1	1I + 3M + 1S + 1*d2overd1plus1	
ladder		2I + 1M + 3S + 2*d1	
ladder	d2overd1plus1=d2/d1+1	2I + 4M + 3S + 2*d2overd1plus1	
Scale		0M	

Введение в аффинное W представление Z-координаты, с целью избавиться от операции мультипликативного инвертирования в промежуточных вычислениях, в работе [167], привело к появлению нового проективного WZ представления: паре (x, y) соответствует $x + y = W/Z$.

Таблица 55. Оценка сложности арифметики точек ЭК в форме Эдварса в проективном WZ представлении над полем четной характеристики [149, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Удвоение	e^4=d1 и f^4=d2/d1+1	1M + 3S + 1*e + 1*f	
diffadd	e^2=d1 и f^2=d2/d1+1 and Z1=1	6M + 1S + 1*e + 1*f	

diffadd	e^2=d1 и f^2=d2/d1+1	6M + 2S + 1*e + 1*f + 1*d1	
diffadd	e^2=d1 и f^2=d2/d1+1	8M + 1S + 1*e + 1*f	
ladder	Z1=1 и e^4=d1 и f^4=d2/d1+1 и ee=e*e и ff=f*f	6M + 4S + 1*ee + 1*ff + 1*e + 1*f	
ladder	e^4=d1 и f^4=d2/d1+1 и ee=e*e и ff=f*f	8M + 4S + 1*ee + 1*ff + 1*e + 1*f	
Scale		1I + 1M	

Введение дополнительного ограничения $d_1 = d_2$ на уравнение кривой (использование ограниченного класса кривых), в предложенную в работе [167] идею: использовать проективное WZ представление, позволило сократить количество полевых операций.

Таблица 56. Оценка сложности арифметики точек ЭК в форме Эдварса с $d_1 = d_2$ в проективном WZ представлении над полем четной характеристики [148, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Удвоение		1M + 3S + 1*d1	
Удвоение	e^4=d1 и f^4=d2/d1+1	1M + 3S + 1*e + 1*f	
diffadd	Z1=1	5M + 1S + 1*d1	
diffadd	e^2=d1 и f^2=d2/d1+1 и Z1=1	6M + 1S + 1*e + 1*f	
diffadd		6M + 2S + 2*d1	
diffadd	e^2=d1 и f^2=d2/d1+1	6M + 2S + 1*e + 1*f + 1*d1	
diffadd		7M + 1S + 1*d1	
diffadd	e^2=d1 и f^2=d2/d1+1	8M + 1S + 1*e + 1*f	
ladder	Z1=1	5M + 4S + 2*d1	
ladder	Z1=1 и e^4=d1 и f^4=d2/d1+1 и ee=e*e и ff=f*f	6M + 4S + 1*ee + 1*ff + 1*e + 1*f	
ladder		7M + 4S + 2*d1	
ladder	e^4=d1 и f^4=d2/d1+1 и ee=e*e и ff=f*f	8M + 4S + 1*ee + 1*ff + 1*e + 1*f	
Scale		1I + 1M	

В качестве альтернативы, Т. Ланге и Р.Р. Фарашахи в [167], было рассмотрено стандартное проективное представление $[X : Y : Z]$, такое что $(x, y) \mapsto [X/Z, Y/Z]$, которое позволило уйти от мультипликативного представления в классическом аффинном представлении и повысило эффективность операций а группе.

Таблица 57. Оценка сложности арифметики точек ЭК в форме Эдварса в стандартном проективном представлении над полем четной характеристики [153, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1	13M + 3S + 2*d1 + 1*d2	13M + 1S + 2*d1 + 1*d2
Сложение	d2plusd1=d2+d1 и d1d1=d1^2	18M + 2S + 1*d1d1 + 2*d2plusd1 + 3*d1 + 1*d2	18M + 2S + 1*d1d1 + 2*d2plusd1 + 3*d1 + 1*d2
Сложение	d2plusd1=d2+d1 и d1d1=d1^2	18M + 3S + 2*d2plusd1 + 3*d1 + 1*d2	18M + 3S + 2*d2plusd1 + 3*d1 + 1*d2
Сложение		21M + 1S + 3*d1 + 1*d2	20M + 1S + 2*d1
Удвоение	d2d1=d2/d1	2M + 6S + 1*d2d1 + 1*d1 + 1*d2	
Scale		1I + 2M	

Введение дополнительного ограничения $d_1 = d_2$ на уравнение кривой (использование ограниченного класса кривых), в предложенную в работе [167] идею: использовать стандартное проективное представление $[X : Y : Z]$, позволило сократить количество полевых операций.

Таблица 58. Оценка сложности арифметики точек ЭК в форме Эдварса с $d_1 = d_2$ в стандартном проективном представлении над полем четной характеристики [152, 167]

Операция	Условие	Сложность	Сложность при повторном сложении
Сложение	Z2=1	13M + 3S + 2*d1 + 1*d2	13M + 1S + 2*d1 + 1*d2
Сложение	d1d1=d1^2	16M + 1S + 1*d1d1 + 3*d1	16M + 1S + 1*d1d1 + 3*d1
Сложение	d1d1=d1^2	16M + 2S + 3*d1	16M + 2S + 3*d1

Владислав Ковтун

Сложение	d2plusd1=d2+d1 и d1d1=d1^2	18M + 2S + 1*d1d1 + 2*d2plusd1 + 3*d1 + 1*d2	18M + 2S + 1*d1d1 + 2*d2plusd1 + 3*d1 + 1*d2
Сложение	d2plusd1=d2+d1 и d1d1=d1^2	18M + 3S + 2*d2plusd1 + 3*d1 + 1*d2	18M + 3S + 2*d2plusd1 + 3*d1 + 1*d2
Сложение		21M + 1S + 3*d1 + 1*d2	20M + 1S + 2*d1
Удвоение	sqrtd1^2=d1	2M + 5S + 1*d1 + 1*sqrtd1	
Удвоение	d2d1=d2/d1	2M + 6S + 1*d2d1 + 1*d1 + 1*d2	
Scale		1I + 2M	

Сложность операций в группе

В таблицах 59 и 60 указывается сложность выполнения восьми различных операций в группе. Далее воспользуемся следующими сокращениями:

- DBL: Удвоение $P_1 \mapsto P_1 + P_1$.
- ADD: Сложение $P_1, P_2 \mapsto P_1 + P_2$.
- reADD: Повторное сложение; т.е., сложение точек, при котором сложение произойдет, перед тем как все повторноиспользуемые промежуточные результаты будут закэшированы. $P_1, P_2 \mapsto P_1 + P_2$, когда все результаты зависящие исключительно от P_2 уже закешированы.
- preADD: Предварительное сложение; т.е., сложение точек, при котором сложение совместимо с наиболее быстрым повторным сложением. Иногда ADD является быстрее, чем reADD, т.к. существуют формулы более быстрого сложения обеспечивающее наиболее медленное последующее сложение.
- mADD: Смешанное сложение;т.е., сложение входных значений, при котором одна из точек обладает Z-координаты равной 1. $P_1, P_2 \mapsto P_1 + P_2$, когда $Z_2 = 1$.
- mreADD: Смешанное последующее сложение.
- mpreADD: Смещанное предварительное сложение.
- mDBL: Смешанное удвоение; т.е., удвоение точки с Z-координатой равной 1. $P_1 \mapsto P_1 + P_1$, когда $Z_1 = 1$.
- mmADD: Смешанное сложение;т.е., сложение точек обладающих Z-координатами равными 1. $P_1, P_2 \mapsto P_1 + P_2$, когда $Z_1 = 1$ и $Z_2 = 1$.
- mmreADD: Сложение точек обладающих Z-координатами равными 1, причем когда творая точка учавствовала в ложении ранее.
- mmpreADD.
- SUNI: Строго унифицированное сложение; т.е., сложение, которое выполняется без учета особенностей удвоение (нет необходимости сравнивать точки на равенство перед сложением).
- TPL: Утроение. $P_1 \mapsto P_1 + P_1 + P_1$.
- DADD: Дифференциальное сложение, т.е., сложение точек, чьи разницы известны заранее. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2$.
- mDADD: Смешанное дифференциальное сложение, т.е., сложение точек, чьи разницы известны заранее, причем Z-координата разницы равна 1. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2$, когда $Z(P_3 - P_2) = 1$.
- LADD: Лестничное сложение; т.е., дифференциальное сложение и удвоение одного из слагаемых. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2, P_2 + P_2$.
- mLADD: Смешанное лесничное сложение; т.е., смешанное дифференциальное сложение и удвоение одного из слагаемых. $P_3 - P_2, P_2, P_3 \mapsto P_3 + P_2, P_2 + P_2$, когда $Z(P_3 - P_2) = 1$.

- SCALE: Преобразование точки из проективного представления к аффинному, когда Z -координата равна 1.

Владислав Ковтун

Содержимое таблиц отсортировано в порядке уменьшения сложности операции DBL; потом по уменьшению сложности операции ADD; и наконец, по уменьшению сложности операции reADD и т.д.
Для оценки вычислительной сложности, каждого метода сложения точек для различных форм описания уравнения эллиптической кривой для различных представлений, сделаем следующие предположения:

- Сложность операции мультипликативного инвертирования в поле I соответствует 10M операциям умножения в поле.
- Операция возведения в квадрат в поле S соответствует 0M операциям умножения в поле.
- Операция умножения на параметр кривой *param соответствует 0M операциям умножения в поле.
- Операция сложения в поле add соответствет 0M операциям умножения в поле.
- Операция умножения на константу *const соответствует 0M операциям умножения в поле.

Таблица 59. Оценка сложности арифметики точек ЭК над полем четной характеристики

Уравнение кривой, представление	DBL	ADD	reADD	preADD	mADD	mreADD	mpreADD	mDBL	mmADD	mmreADD	mmpreADD	SUNI	DADD	mDADD	LADD	mLADD	SCALE
Binary Edwards, affine	12	28	27	28	28	27	28	12	28	27	28	28					0
Short Weierstrass, affine	12	12	12	12	12	12	12	12	12	12	12						0
Binary Edwards, affine with d1=d2	11	28	27	28	28	27	28	11	28	27	28	28					0
Binary Edwards, w	11							11					13	13	24	24	0
Binary Edwards, w with d1=d2	10							10					11	11	21	21	0
Short Weierstrass, projective	7	14	14	14	11	11	11	5	7	7	7						12
Short Weierstrass, Jacobian	4	14	13	14	10	10	10	1	10	10	10						13
Short Weierstrass, Lopez-Dahab with a2=1	3	13	13	13	8	8	8	1	5	5	5						
Short Weierstrass, Lopez-Dahab with a2=0	3	13	13	13	8	8	8	1	5	5	5						
Short Weierstrass, Lopez-Dahab	3	13	13	13	8	8	8	1	5	5	5						
Binary Edwards, projective	2	18	18	18	13	13	13	2	13	13	13	18					12
Binary Edwards, projective with d1=d2	2	16	16	16	13	13	13	2	13	13	13	16					12
Short Weierstrass, extended Lopez-Dahab with a2=0	2	14	14	14	9	9	9	2	9	9	9						
Short Weierstrass, extended Lopez-Dahab with a2=1	2	13	13	13	8	8	8	2	8	8	8						
Binary Edwards, WZ	1							1					6	6	8	6	11
Binary Edwards, WZ with d1=d2	1							1					6	5	7	5	11

Таблица 60. Оценка сложности арифметики точек ЭК над полем четной характеристики

Уравнение кривой, представление	DBL	ADD	reADD	preADD	mADD	mreADD	mpreADD	mDBL	mmADD	mmreADD	mmpreADD	SUNI	DADD	mDADD	LADD	mLADD	SCALE
Binary Edwards, affine	12.8	28.4	27.4	28.4	28.4	27.4	28.4	12.8	28.4	27.4	28.4	28.4					0.0
Short Weierstrass, affine	12.2	12.2	12.2	12.2	12.2	12.2	12.2	12.2	12.2	12.2	12.2						0.0
Binary Edwards, affine with d1=d2	11.8	28.4	27.4	28.4	28.4	27.4	28.4	11.8	28.4	27.4	28.4	28.4					0.0
Binary Edwards, w	11.4							11.4					13.2	13.2	24.6	24.6	0.0
Binary Edwards, w with d1=d2	10.4							10.4					11.4	11.4	21.6	21.6	0.0
Short Weierstrass, projective	7.6	14.2	14.2	14.2	11.2	11.2	11.2	5.6	7.2	7.2	7.2						12.0
Short Weierstrass, Jacobian	5.0	15.0	13.8	15.0	10.6	10.6	10.6	1.4	10.6	10.6	10.6						13.2
Short Weierstrass, Lopez-Dahab with a2=1	4.0	13.8	13.6	13.8	9.0	9.0	9.0	1.6	5.6	5.6	5.6						
Short Weierstrass, Lopez-Dahab with a2=0	4.0	13.8	13.6	13.8	9.0	9.0	9.0	1.6	5.6	5.6	5.6						
Short Weierstrass, Lopez-Dahab	4.0	13.8	13.6	13.8	9.0	9.0	9.0	1.6	5.6	5.6	5.6						
Binary Edwards, projective	3.2	18.4	18.4	18.4	13.6	13.2	13.6	3.2	13.6	13.2	13.6	18.4					12.0
Binary Edwards, projective with d1=d2	3.0	16.2	16.2	16.2	13.6	13.2	13.6	3.0	13.6	13.2	13.6	16.2					12.0
Short Weierstrass, extended Lopez-Dahab with a2=0	3.0	14.6	14.6	14.6	9.8	9.8	9.8	2.6	9.8	9.8	9.8						
Short Weierstrass, extended Lopez-Dahab with a2=1	2.8	13.6	13.6	13.6	8.8	8.8	8.8	2.8	8.8	8.8	8.8						
Binary Edwards, WZ	1.6							1.6					6.4	6.2	8.8	6.8	11.0
Binary Edwards, WZ with d1=d2	1.6							1.6					6.4	5.2	7.8	5.8	11.0

Криптография с открытм ключем. Текущее состояние

В таблице 60, оценки вычислительной сложности, каждого метода сложения точек для различных форм описания уравнения эллиптической кривой для различных представлений, были выполнены со следующими предположениями:

- Сложность операции мультипликативного инвертирования в поле I соответствует 10M операциям умножения в поле.
- Операция возведения в квадрат в поле S соответствует 0,2M операциям умножения в поле.
- Операция умножения на параметр кривой *param соответствует 0M операциям умножения в поле.
- Операция сложения в поле add соответствет 0M операциям умножения в поле.
- Операция умножения на константу *const соответствует 0M операциям умножения в поле.

Использование цепочки преобразований из одной системы координат в другую во время выполнения скалярного умножения позволяет сэкономить несколько операций умножения и возведения в квадрат [102].

Далее приведем экспериментальные оценки времени выполнения операций над точками ЭК над простыми и двоичными полями. При проведении эксперимента, авторами использовались кривые рекомендованные NIST [35], а также результатами [29]. В таблице 61 указаны условия проведения эксперимента, результаты которого приведены в таблице 62.

Таблица 61. Условия проведения экспериментальных оценок времени выполнения алгоритмов

№	Процессор	Операционная система	Компилятор	Особенности реализации
1	AMD, Athlon XP 2500+ MHz	MS Windows XP	MS Visual C++ 2005	Без использования ассемблера

Таблица 62. Экспериментальные оценки времени выполнения преобразования в группе точек эллиптической кривой

Операция	B-163	B-233	B-283	B-409	B-571	P-192	P-224	P-256	P-384	P-521
Скалярное умножение, метод Leem-Lee	0,36	0,41	0,92	1,54	2,78	0,92	1,67	1,59	4,51	7,67
Скалярное умножение, метод «возвести в квадрат и умножить», промежуточные вычисления в проективных координатах Lopez-Dahab	1,79	4,0	5,20	12,91	28,61					
Скалярное умножение, метод «возвести в квадрат и умножить», промежуточные вычисления в проективных координатах Jacobi						4,56	13,56	4,29	10,21	19,67
Скалярное умножение, метод «возвести в квадрат и умножить» в аффинных координатах	12,11	29,14	43,45	110,407	250,45	9,25	26,01	7,23	15,42	26,62

Результаты, полученные авторами, отличаются от результатов [20] и [22], это свидетельствует о различных условиях проведения экспериментов, а также особенностях программной реализации авторов [20, 22].

Эксперименты, проведенные авторами, свидетельствуют о превосходстве производительности в группе $EC(\mathbf{GF}(2^m))$ над преобразованиями в группе $EC(GF(p))$ на величину $2{,}5 \div 3$.

Таблица 63. Описание криптопримитивов, которые рассматривались в эксперименте

Криптография с открытм ключем. Текущее состояние

Номер колонки	Назначение	Название криптопримитива	Название стандарта
1	Цифровая подпись	ECDSA	IEEE P1363-2000, ANSI X9.62–1998 [6, 7, 8]
2	Цифровая подпись	ECGDSA	ISO/IEC FCD 15946 [6]
3	Цифровая подпись	ECKDSA	ISO/IEC FCD 15946 [6]
4	Цифровая подпись	GOST 34.10-20001	GOST R 34.10-20001 [11]
5	Цифровая подпись	DSTU4145-2002	DSTU 4145-2002 [12]
6	Обмен ключами	ECKAS-DH1	IEEE P1363-2000, ANSI X9.63–1999 [7, 10]
7	Обмен ключами	ECKAS-DH1	IEEE P1363-2000, ANSI X9.63–1999 [7 10]
8	Обмен ключами	ECKAS-MQV	IEEE P1363-2000, ANSI X9.63–1999 [7 10]

Далее, в таблице 64 приведем экспериментальную оценку времени выполнения основных криптопримитивов, выполненные авторами. В эксперименте рассматривались кривые, описанные в [12, 35].

Таблица 64. Экспериментальные оценки времени выполнения криптопримитивов основанных на преобразованиях в группе точек эллиптической кривой

Кривая	1, μs			2, μs			3, μs			4, μs				5, μs			6, μs		7, μs		8, μs	
	Pre	G	V	Pre	G	V	Pre	G	V	Pre	PG	G	V	Pre	G	V	Pre	G	Pre	G	Pre	G
B-163	468,0	0,69	3,94	468,0	0,66	3,86	468,0	0,61	3,81	468,0	0,57	0,016	4,00	468,0	0,65	3,82	468,0	3,07	922,0	6,41	468,0	6,20
B-233	963,0	1,41	8,97	963,0	1,34	8,74	963,0	1,28	8,59	963,0	1,20	0,31	8,90	963,0	1,32	8,71	963,0	7,03	1890	13,98	963,0	10,98
B-283	1281,0	1,89	13,39	1281,0	1,81	13,03	1281,0	1,70	12,29	1281,0	1,62	0,032	12,39	1281,0	1,76	12,87	1281,0	10,62	2546,0	19,41	1281,0	17,03
B-409	2828,0	4,27	28,91	2828,0	4,09	28,12	2828,0	3,89	29,17	2828,0	3,71	0,047	28,25	2828,0	3,98	29,59	2828,0	23,84	5672,0	47,45	2828,0	38,54
B-571	6188,0	4,27	28,91	6188,0	8,98	63,20	6188,0	8,65	64,59	6188,0	8,31	0,078	63,57	6188,0	8,78	65,34	6188,0	53,61	12422,0	103,04	6188,0	84,14
P-192	1500,0	1,35	10,57	1516,0	1,30	10,00	1516,0	1,25	10,98					1516,0	1,28	10,37	1516,0	8,84	3016,0	16,41	1516,0	13,97
P-224	2390,0	2,11	17,07	2390,0	2,03	16,33	2390,0	1,97	16,78					2390,0	2,03	16,50	2390,0	14,58	4797,0	28,26	2390,0	22,29
P-256	3843,0	3,32	27,84	3843,0	3,25	28,91	3843,0	3,15	26,94					3843,0	3,21	26,86	3843,0	23,92	7688,0	46,92	3843,0	36,03
P-384	12906,0	11,22	98,37	12953,0	11,05	95,20	12953,0	10,87	95,89					12953,0	10,95	97,51	12953,0	83,93	25797,0	165,23	12953,0	130,34
P-521	32093,0	28,25	253,89	32093,0	27,94	250,92	32093,0	27,65	255,72					32093,0	27,78	255,06	32093,0	215,41	64187,0	445,79	32093,0	344,56
DB-163										468,0	0,57	0,016	3,76									
DB-167										484,0	0,59	0,016	3,91									
DB-173										485,0	0,59	0,016	3,91									
DB-179										500,0	0,59	0,016	4,46									
DB-191										484,0	0,61	0,016	5,12									
DB-233										1015,0	1,25	0,016	9,23									
DB-257										1125,0	1,34	0,016	11,32									
DB-307										1625,0	2,06	0,031	15,72									
DB-367										2375,0	3,12	0,031	23,34									
DB-431										3391,0	4,45	0,047	34,51									

Следует отметить, что в случае формирования подписи или формировании общего ключа, происходит умножение базовой точки, заранее известной, на случайное число. В этом случае применяется алгоритм Lim-Lee с параметрами $h = 8$, $v = 4$, согласно результатам, приведенным в диссертации [18]. При проверке подписи осуществляется два скалярных умножения на базовую точку, заранее известную и произвольную точку, заранее неизвестную. В первом случае применяется алгоритм Lim-Lee, как и для формирования подписи, во втором случае производится умножение классическим алгоритмом «возвести в квадрат и умножить». На этапе предвычислений, а также во время выполнения скалярных умножений обеими методами, все промежуточные вычисления выполняются в смешанных координатах, согласно результатам исследований приведенных в таблицах 59, 60.

Дискретный логарифм в якобиане гиперэллиптической кривой над конечными полями (чисел, полиномов)

Описание задачи

Впервые использование гиперэллиптических кривых было предложено в работе [36] Пусть дана гиперэллиптическая кривая $C(\mathbf{GF}(q))$ рода g и приведенные дивизоры $D_1, D_2 \in \mathbf{J}(\mathbf{GF}(q))$, под **решением HCDLP** будем понимать решение уравнения $D_2 = lD_1$ относительно l или доказательстве, что решение не существует, где $\mathbf{J}(\mathbf{GF}(q)) = D^0/\mathrm{P}$ - якобиан, P - множество основных дивизоров, D^0 - множество дивизоров степени 0, n - порядок дивизора D_1, т.е. $n = \mathrm{ord}(D_1)$, l - секретный ключ, D_2- открытый ключ [21, 37].

Сложность криптоанализа

Наиболее удачным для решения HECDLP считается алгоритм Index-calculus. Некоторые идеи, при решении DLP, могут быть применимы и для вычисления HECDLP в якобиане $\mathbf{J}_C(k)$ гиперэллиптической кривой C, рода g над полем $k = \mathbf{F}_q$ в мнимой квадратичной форме. Если род g значительно больше по сравнению с q, тогда субэкспоненциальное временем работы вероятностного алгоритма с известным $n = q^g$ обозначают $O(L_n[c])$, где $L_{q^g}[c] = \exp\left((c + o(1)\sqrt{g \log q \log g \log q}\right)$ для некоторой положительной константы c.

Наиболее эффективным алгоритмом решения задачи дискретного логарифма в Якобиане ГЭК принято считать алгоритм Theriault [21, 37] . Различные его варианты позволяют получить сложности $O\left(g^5 q^{2-2/(g+1)+\varepsilon}\right)$ и $O\left(g^5 q^{2-4/(2g+1)+\varepsilon}\right)$ [21, 37].

Производительность/сложность реализации

Известно, что во всех криптографических примитивах на гиперэллиптической кривой, основной операцией является операция скалярного умножения в якобиане. В свою очередь, скалярное умножение может быть представлено в виде иерархии, рис. 6.

Рис. 6. Обобщенная иерархия операций при скалярном умножении дивизоров в якобиане ГЭК

Более подробная иерархия операций при скалярном умножении может быть представлена виде рис. 7.

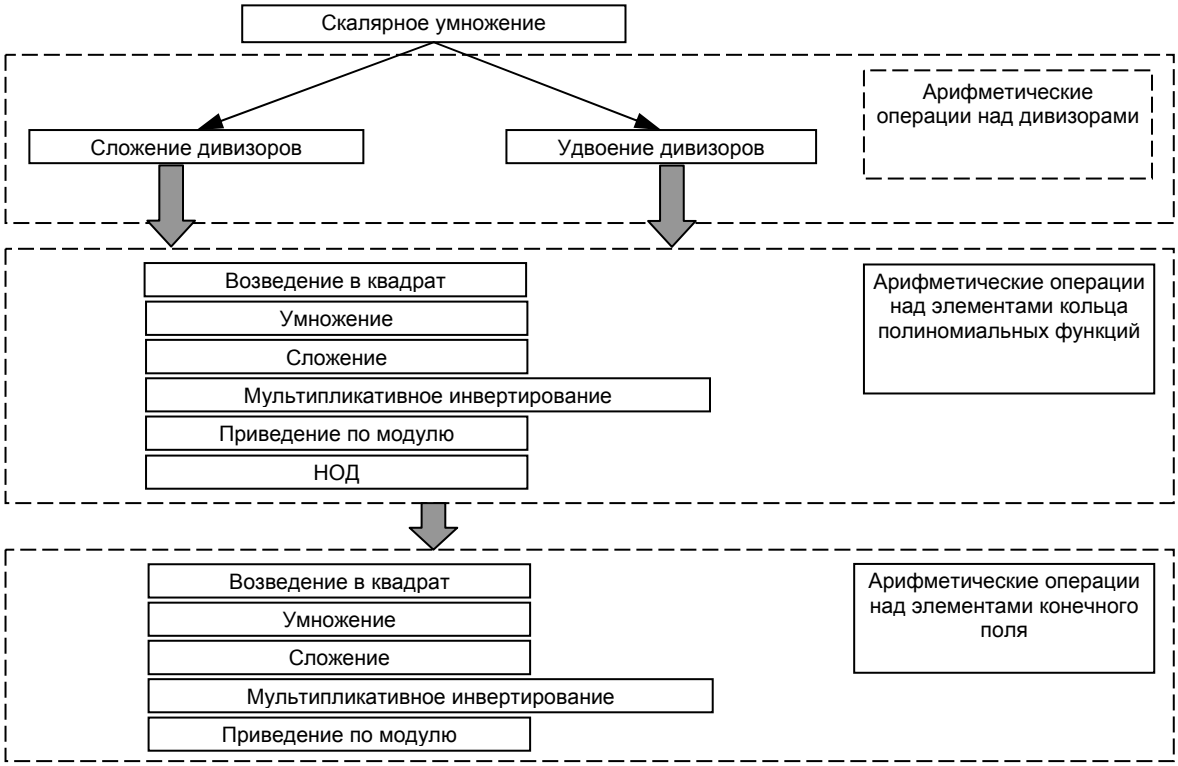


Рис. 7. Иерархия операций используемых для скалярного умножения дивизоров ГЭК

Известно, что в основу группового закона в Якобиане ГЭК положен алгоритм Кантора, который получил развитие в работе [39]. Оценки его сложности были проведены A. Enge и опубликованы в работе [38], и приведены в таблице 65.

Таблица 65. Теоретические оценки сложности преобразований в Якобиане ГЭК зависимости от рода кривой g в полевых операциях [38]

Якобиан	Сложение		Удвоение	
	*	$()^{-1}$	*	$()^{-1}$
$\mathbf{J}_C(\mathbf{F}_p),\ g \equiv 0 \bmod 2$	$17g^2+3g-3$	$\frac{3}{2}g+3$	$\frac{33}{2}g^2+\frac{11}{2}g-1$	$\frac{3}{2}g+2$
$\mathbf{J}_C(\mathbf{F}_p),\ g \equiv 1 \bmod 2$	$17g^2+4g-2$	$\frac{3}{2}g+\frac{7}{2}$	$\frac{33}{2}g^2+\frac{13}{2}g$	$\frac{3}{2}g+\frac{5}{2}$
$\mathbf{J}_C(\mathbf{F}_{2^m}),\ g \equiv 0 \bmod 2$	$14g^2+5g-1$	$\frac{3}{2}g+2$	$7g^2+g+1$	$\frac{1}{2}g+2$
$\mathbf{J}_C(\mathbf{F}_{2^m}),\ g \equiv 1 \bmod 2$	$14g^2+5g$	$\frac{3}{2}g+\frac{5}{2}$	$7g^2+2g+2$	$\frac{3}{2}g+\frac{5}{2}$

Непосредственное количество операций в поле, необходимых для реализации группового закона в Якобиане, приведены в таблице 66.

Таблица 66. Средняя оценка сложности, согласно оценкам из таблицы 65 [38]

g	$\mathbf{J}_C(\mathbf{F}_q)$	Сложение		Удвоение		160-разрядный скалярный множитель	
		*	$()^{-1}$	*	$()^{-1}$	*	$()^{-1}$
3	$\mathbf{J}_C(\mathbf{F}_p)$	163	8	168	7	39920	1760
	$\mathbf{J}_C(\mathbf{F}_{2^m})$	137	7	44	5	18000	1360
4	$\mathbf{J}_C(\mathbf{F}_p)$	281	9	285	8	68080	2000
	$\mathbf{J}_C(\mathbf{F}_{2^m})$	239	8	117	4	37840	1280
5	$\mathbf{J}_C(\mathbf{F}_p)$	443	9.5	445	8.5	106640	2120
	$\mathbf{J}_C(\mathbf{F}_{2^m})$	375	10	187	5	59920	1600
6	$\mathbf{J}_C(\mathbf{F}_p)$	627	12	628	11	15064	2720

	$\mathbf{J}_C(\mathbf{F}_{2^m})$	527	11	259	5	83600	1680

Дальнейшее развитие арифметических преобразований в Якобиане ГЭК пошло по пути фиксации рода кривой, т.е. перехода от операций над полиномиальными функциями непосредственно к операциям над элементами базового поля. В таблице 67 приведем сложности операций в Якобиане, методом Кантора, в полевых операциях, для кривых, обладающих достаточной для криптографических приложений стойкостью к криптоанализу [21, 37].

Таблица 67. Сложность операций в якобиане ГЭК 2-4 рода в полевых операциях методом Cantor

Род	Условия	Сложение			Смешанное сложение			Удвоение			Смешанное удвоение		
		()-1	^2	*	()-1	^2	*	()-1	^2	*	()-1	^2	*
Поле нечетной характеристики $\mathrm{char}(\mathbf{F}_q) = p$													
2	Кантор [40]*	3		70				3		76			
	$h_i \in F_2,\ f_4 = 0$ [41]	2	4	44				2	8	42			
Поле четной характеристики $\mathrm{char}(\mathbf{F}_q) = 2$													
2	$h(x) = 0,\ f_i = F_2$ [40]*	2		52				2		49			
	$h_i \in F_2,\ f_4 = 0$ [41]	2	4	42				2	8	40			
	$h(x) = x,\ f_4 = 0$ [41]	2	4	42				1	6	23			
Поле нечетной характеристики $\mathrm{char}(\mathbf{F}_q) = p$													
3	Кантор [Nag00]*	4		200				4		207			
	$h_i \in F_2,\ f_6 = 0$ [41]	2	4	118				2	19	106			
Поле четной характеристики $\mathrm{char}(\mathbf{F}_q) = 2$													
3	$h(x) = 0,\ f_i = F_2$ [40]*	2		154				2		132			
	$h_i \in F_2,\ f_6 = 0$ [41]	2	4	110				2	13	98			
	$h(x) = 1,\ f_6 = 0$ [41]	2	4	110				1	11	14			
Поле нечетной характеристики $\mathrm{char}(\mathbf{F}_q) = p$													
4	Кантор [40]*	6		386				6		359			
	$h_i \in F_2,\ f_8 = 0$ [41]	3	6	222				3	17	206			
Поле четной характеристики $\mathrm{char}(\mathbf{F}_q) = 2$													
4	$h(x) = 0,\ f_i = F_2$ [40]*	3		286				3		260			
	$h_i \in F_2,\ f_6 = 0$ [41]	3	6	204				3	14	181			
	$h(x) = 1,\ f_6 = 0$ [41]	3	6	204				2	13	76			

* - в указанных работах авторы не различают операции умножения и возведения в квадрат.

После публикации работы [42], начали различать методы, посредством которых выполняются операции в Якобиане, предложенный метод является модификацией метода Кантора и получил название в честь своего создателя – Harley. В таблице 67 приведем сложности операций в Якобиане методом Harley.

Таблица 68. Сложность операций в якобиане ГЭК 2-4 рода в полевых операциях методом Harley

Род	Условия	Сложение			Смешанное сложение			Удвоение			Смешанное удвоение		
		()-1	^2	*	()-1	^2	*	()-1	^2	*	()-1	^2	*

Владислав Ковтун

Поле нечетной характеристики $\mathrm{char}(\mathbf{F}_q) = p$													
2	Аффинные координаты												
	$h(x) = 0$ [42]*	2		27				2		30			
	$h_2 = 1$ [43]	2	3	24				2	6	26			
	$h(x) = 0$ [50]*	2		25				2		27			
	$h(x) = 0,\ f_4 = 0$ [51]*	1		26				1		27			
	$h(x) = 0$ [52]*	1		25				1		29			
	$f_4 = 0$ [43]	1	3	22				1	5	22			
	Проективные координаты $[U_1, U_0, V_1, V_0, Z]$												
	$\deg(h) = 2,\ h_i \in \mathbf{F}_2$ [44]		4	47		3	40		6	40		5	25
	$\deg(h) = 2,\ h_i \in \mathbf{F}_2$ [45]		4	46		4	39		6	39		5	25
	$h(x) = 0,\ f_4 = 0$ [46]		4	46		4	39		6	33		5	24
	Взвешенные координаты $[U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2]$												
	$h(x) = 0,\ f_4 = 0$ [48]		7	47		5	36		7	34		5	21
Поле четной характеристики $\mathrm{char}(\mathbf{F}_q) = 2$													
2	Аффинные координаты												
	$h_i \in F_2$ [53]	1	2	25				1	1	27			
	$f_4 = 0$ [43]	1	3	21				1	5	20			
	$h_2 = 0,\ f_4 = 0$ [43]	1	3	21				1	5	17			
	$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [41]							1	6	9			
	$h(x) = x,\ f(x) = x^5 + f_3 x^3 + \varepsilon x^2 + f_0,\ \varepsilon \in \mathbf{F}_2$ [47]	1		24				1	5	13			
	$\deg(h) = 2,\quad h_0 = 0,\quad h_1 \in \mathbf{F}_q,\quad f(x) = x^5 + \varepsilon x^4 + f_1 x + f_0,\ \varepsilon \in \mathbf{F}_2$ [47]	1		25				1	4	22			
	$h_1 \in \mathbf{F}_q,\ h_2 = h_0 = 0,\ f_4 = f_1 = 0$ [49]							1	5	9			
	$h_1 = 1,\ h_2 = h_0 = 0,\ f_4 = f_1 = 0$ [49]							1	6	5			
	$\deg(h) = 2,\ h_0 = 0,\ h_1 \in \mathbf{F}_q,\ f_3 = f_2 = 0$ [49]							1	5	17			
	$\deg(h) = 2,\ h_0 = 0,\ h_1 \in \mathbf{F}_2,\ f_3 = f_2 = 0$ [49]							1	6	12			
2	Аффинные координаты												
	$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [41]							1	6	9			
	Проективные координаты $[U_1, U_0, V_1, V_0, Z]$												
	$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [41]		5	45		5	38		6	31		5	18
	$h_2 = 0,\ f_4 = 0$ [43]		4	49		4	39		7	38			
	$\deg(h) = 2,\ h_i \in \mathbf{F}_q,\ f_4 = 0$ [47]									45		6	39
	$\deg(h) = 2,\quad h_0 = 0,\quad h_1 \in \mathbf{F}_q,\quad f(x) = x^5 + \varepsilon x^4 + f_1 x + f_0,\ \varepsilon \in \mathbf{F}_2$ [47]								3	39		6	38
	$h(x) = x,\ f(x) = x^5 + f_3 x^3 + \varepsilon x^2 + f_0,\ \varepsilon \in \mathbf{F}_2$ [47]											5	26
	$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [45]		4	44		5	37		7	29		4	17
	Взвешенные координаты $[U_1, U_0, V_1, V_0, Z_1, Z_2, Z_1^2, Z_2^2, Z_1 Z_2, Z_1^3 Z_2]$												
	$\deg(h) = 2,\ f_4 = 0$ [48]		4	46		5	35		6	35		5	20
	$h(x) = x,\ f_4 = 0$ [48]		6	44		6	34		6	29		6	19
Поле нечетной характеристики $\mathrm{char}(\mathbf{F}_q) = p$													

3	Аффинные координаты												
	$h(x)=0,\ f_6=0$ [54]*	1		81				1		74			
	$h(x)=0,\ f_6=0$ [55]*	1		70				1		71			
	$h_i \in \mathbf{F}_2,\ f_6=0$ [41]	1	6	70				1	10	62			
Поле четной характеристики $\mathrm{char}(\mathbf{F}_q)=2$													
3	Аффинные координаты												
	$h_i \in \mathbf{F}_2,\ f_6=0$ [41]	1	6	65				1	10	53			
	$h(x)=1,\ f_6=0$ [41]	1	6	65				1	7	22			
Поле нечетной характеристики $\mathrm{char}(\mathbf{F}_q)=p$													
4	Аффинные координаты												
	$h_i \in \mathbf{F}_2,\ f_8=0$ [41]	2	6	158				2	17	193			
Поле четной характеристики $\mathrm{char}(\mathbf{F}_q)=2$													
4	Аффинные координаты												
	$h_i \in \mathbf{F}_2,\ f_8=0$ [41]	2	6	146				2	17	144			
	$h(x)=1,\ f_8=0$ [41]	2	6	146				2	13	72			

С точки зрения практического применения, наибольший интерес представляют преобразования в Якобиане кривых рода 2 и 3. Далее, в работе, будут рассматриваться кривые только второго рода.

Анализ результатов оценок сложности, приведенных в таблице 67, позволяет сделать вывод, что на сегодняшний день наиболее эффективными являются преобразования:

- В аффинном представлении: Byramjee, Duquesne [47] и Lange [43].
- В проективном представлении: Ковтун [45, 46].
- Во взвешенном представлении: Lange [48].

Авторами была проведена экспериментальная оценка времени выполнения основных операций в якобиане ГЭК.

Таблица 69. Условия проведения экспериментальных оценок времени выполнения алгоритмов, реализующих операции в простом поле

№	Процессор	Операционная система	Компилятор	Особенности реализации
1	AMD, Athlon XP 2500+ MHz	MS Windows XP	MS Visual C++ 2005	Без ассемблера

В данном эксперименте была использована ГЭК из работы Lange [57, page 83]:

- Род кривой: 2.
- Кривая: $y^2+\left(x^2+x+1\right)y=x^5+x^4+1$, которая является кривой Коблица.
- Базовое поле: $\mathbf{GF}\left(2^{89}\right),\ p(t)=t^{89}+t^{38}+1$.
- Порядок якобиана: 2 * 191 561 942 608 242 456 073 498 418 252 108 663 615 312 031 512 914 969.
- Порядок базового дивизора: 191 561 942 608 242 456 073 498 418 252 108 663 615 312 031 512 914 969.

Таблица 70. Экспериментальные оценки времени выполнения операций в якобиане ГЭК в аффинном представлении дивизоров

№	Операция	Время, мс
1	Сложение дивизоров веса 2, $D_1=P_1+P_2-2\inf$, $D_2=P_3+P_4-2\inf$, точки из носителей	0,125

	дивизоров - различные	
2	Сложение дивизоров веса 2, $D_1 = 2P_1 - 2\inf$, $D_2 = 2P_2 - 2\inf$, точки из носителей дивизоров - различные	0,11
3	Сложение дивизоров веса 1, $D_1 = P_1 - \inf$, $D_2 = P_2 - \inf$, точки из носителей дивизоров - различные	0,047
4	Удвоение дивизора веса 2, $D_1 = P_1 + P_2 - 2\inf$, точки из носителя дивизора - различные	0,125
5	Удвоение дивизора веса 2, $D_1 = 2P_1 - 2\inf$, точки из носителя дивизора - различные	0,125
6	Удвоение дивизора веса 1, $D_1 = P_1 - \inf$, точки из носителя дивизора - различные	0,047
8	Скалярное умножение дивизора веса 2, посредством метода «сложить и удвоить, слева – направо»	7,984

Из приведенной таблицы следует, что для повышения производительности преобразований, следует воспользоваться в качестве базового дивизора, образующего группу, деградирующим дивизором, т.е. обладающим весом 1.

Авторами была проведена подмена группы точек ЭК на якобиан ГЭК второго рода при реализации схемы ECDSA, что позволило получить HECDSA. Результаты экспериментальной оценки времени данной реализации приведены в таблице 67.

В данном эксперименте была использована ГЭК из работы Lange [57, page 83]:

- Род кривой: 2.
- Кривая: $y^2 + \left(x^2 + x + 1\right)y = x^5 + x^4 + 1$, которая является кривой Коблица.
- Базовое поле: $\mathbf{GF}\left(2^{89}\right)$, $p(t) = t^{89} + t^{38} + 1$.
- Порядок якобиана: 2 * 191 561 942 608 242 456 073 498 418 252 108 663 615 312 031 512 914 969.
- Порядок базового дивизора: 191 561 942 608 242 456 073 498 418 252 108 663 615 312 031 512 914 969.
- Базовый дивизор веса 2.

Таблица 71. Экспериментальные оценки времени выполнения формирования и проверки цифровой подписи согласно схемы HECDSA

№	Операция	Время, мс
1	Формирование цифровой подписи	33,42
2	Проверка цифровой подписи	67,75

В данном случае, для скалярного умножения использовался алгоритм «сложить и удвоить, слева - направо», о чем свидетельствует достаточно большое время выполнения операций.

В дальнейшем, авторами планируется для промежуточных вычислений использовать проективное и взвешенное представление дивизоров, а также алгоритма Lim-Lee для скалярного умножения базового дивизора.

Следующим шагом в использовании алгебраических кривых в криптографических приложениях является переход к более сложным кривым, от эллиптических к гиперэллиптическим, от гиперэллиптических к суперэллиптическим.

Дискретный логарифм в якобиане суперэллиптической кривой над конечными полями

Описание задачи

Впервые использование кривых суперэллиптических кривых (СЭК) было предложено в работе [58] Пусть дана суперэллиптическая кривая $y^k = x^m + f_{m-1}x^{m-1} + \cdots + f_1 x + f_0$ над полем $\mathbf{GF}(q)$, рода $g = \frac{1}{2}(k-1)(m-1)$, отметим, что $k, m \geq 3$, и приведенные дивизоры $D_1, D_2 \in \mathbf{J}(\mathbf{GF}(q))$. Под **решением SCDLP** будем понимать решение уравнения $D_2 = lD_1$ относительно l или доказательстве, что решение не существует, где $\mathbf{J}(\mathbf{GF}(q)) = \mathbf{D}^0/\mathbf{P}$ - якобиан, $\mathbf{P}$ - множество основных дивизоров, $\mathbf{D}^0$ - множество дивизоров степени 0, n - порядок дивизора D_1, т.е. $n = \mathrm{ord}(D_1)$, l - секретный ключ, D_2 - открытый ключ [58].

Сложность криптоанализа

Согласно результатам исследований приведенных в работе [58], сложность субэкспоненциального алгоритма решения SCDLP составляет $O(L_N(\alpha, \beta))$, причем $L_N(\alpha, \beta) = \exp\left(\beta(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right)$, где $N = p^{2g+1}$, $\alpha = \frac{1}{2}$, $\beta = c$, c - некоторая константа. По оценкам авторов [58] $c = \max\left(\sqrt{2\log q} + o(1), s\sqrt{\frac{\log q}{2}}\right)$, где параметр s определяется степенью разреженности матрицы. Для разреженной матрицы $s = 2$, и следовательно $c = \sqrt{2\log q} + o(1)$.

Производительность/сложность реализации

Оценка сложности композиции дивизоров в якобиане СЭК над полем $\mathbf{GF}(q)$ составляет $O(k^6 m^2 g^2)$. Результаты теоретической оценки сложности групповой операции в якобиане СЭК, опубликованные [59], приведены в таблице 67.

Таблица 72. Оценка сложности преобразований в якобиане СЭК

Название шага	[59]		[58]
	C_{ab}	СЭК	СЭК
Шаг 1: (произведение идеала)	$O(a^4 g^2 \log^2 q)$	$O(a^4 g^2 \log^2 q)$	$O(a^4 g^2 \log^2 q)$
Шаг 2: (инверсия идеала)	$O(a^8 g^2 \log^2 q)$	$O(a^4 g^2 \log^2 q)$	$O(a^7 g^2 \log^2 q)$ или $O(a^9 g^2 \log^2 q)$
Шаг 3: (поиск минимального элемента)	$O(a^7 g^2 \log^2 q)$	$O(a^3 g^2 \log^2 q)$	$O(a^7 g^2 \log^2 q)$
Шаг 4: (произведение идеала)	$O(a^7 g^2 \log^2 q)$	$O(a^4 g^2 \log^2 q)$	$O(a^4 g^2 \log^2 q)$
Групповая операция в целом	$O(a^8 g^2 \log^2 q)$	$O(a^4 g^2 \log^2 q)$	$O(a^7 g^2 \log^2 q)$ или $O(a^9 g^2 \log^2 q)$

К сожалению, на сегодняшний день, практической реализации криптосистемы на СЭК отсутствует, в печати даются лишь теоретические оценки, что свидетельствует о недостаточной разработке данного направления. Частным случаем СЭК являются кривые Пикарда.

Владислав Ковтун

Дискретный логарифм в якобиане кривой Пикарда над конечными полями (чисел, полиномов)

Описание задачи

Впервые, использование кривых Пикарда было предложено в работах [60, 61]. Пусть дана кривая Пикарда кривая третьего рода $y^3 = x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ над полем $\mathbf{GF}(q)$, $\mathrm{char}(\mathbf{GF}(q)) \neq 3$, и приведенные дивизоры $D_1, D_2 \in \mathbf{J}(\mathbf{GF}(q))$, под **решением PCDLP** будем понимать решение уравнения $D_2 = lD_1$ относительно l или доказательстве, что решение не существует, где $\mathbf{J}(\mathbf{GF}(q)) = \mathbf{D}^0/\mathbf{P}$ - якобиан, $\mathbf{P}$ - множество основных дивизоров, $\mathbf{D}^0$ - множество дивизоров степени 0, n - порядок дивизора D_1, т.е. $n = \mathrm{ord}(D_1)$, l - секретный ключ, D_2 - открытый ключ [60, 61, 62, 63].

Сложность криптоанализа

Согласно результатам исследований приведенных в работе [58], сложность субэкспоненциального алгоритма решения PCDLP составляет $O(L_N(\alpha, \beta))$, причем $L_N(\alpha, \beta) = \exp\left(\beta(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right)$, где $N = p^{2g+1}$, $\alpha = \frac{1}{2}$, $\beta = c$, c - некоторая константа. По оценкам авторов [58] $c = \max\left(\sqrt{2\log q} + o(1), s\sqrt{\frac{\log q}{2}}\right)$, где параметр s определяется степенью разреженности матрицы. Для разреженной матрицы $s = 2$, и следовательно $c = \sqrt{2\log q} + o(1)$.

Производительность/сложность реализации

Таблица 73. Оценки сложности групповых операций в Якобиане ГЭК, кривых Пикарда и СЭК кривых над простыми полями [63]

Условия	Сложение			Удвоение		
	()-1	^2	*	()-1	^2	*
Гиперэллиптические кривые 3 рода $h_i \in \mathbf{F}_2$, $f_6 = 0$ [41]	1	6	70	71	10	62
Кривая Пикарда	2		130	2		152
$C_{3,4}$, $\deg(h_2) = 1$	2		138	2		160
$C_{3,4}$, $\deg(h_2) = 2$	2		145	2		167
$C_{3,4}$, $\deg(h_2) = 3$	2		163	2		185

К сожалению, на сегодняшний день, практической реализации криптосистемы на кривых Пикарда отсутствует, в печати даются лишь теоретические оценки, что свидетельствует о не достаточной разработке данного направления.

Сравнение

Приведем результаты сравнения стойкости к криптоанализу криптопреобразований в основу, которой положены преобразования в поле, в группе точек эллиптической кривой и якобиане гиперэллиптической кривой [21]. Данную оценку стойкости криптопреобразований следует проводить при фиксированной длине ключа относительно стойкости к криптоанализу алгоритма AES.

Стойкость криптопреобразований, напрямую связанны с порядком группы, которая образуется базовым элементом:

- - для криптографических преобразований в поле $\mathbf{GF}(q)$, $q = 2^m$, известным наилучшим алгоритмом криптоанализа DLP является алгоритм A. 5 [21],

сложность которого, составляет $O\left(\exp\left((1.4+o(1))m^{1/3}(\log m)^{2/3}\right)\right)$ групповых операций;

- - для криптографических преобразований в группе точек эллиптической кривой, как и для гиперэллиптических кривых, рода $g=1$, порядок равен $\#E(\mathbf{GF}(q))=O\left(4N^{1/2}\right)$. Причем точка $P\in E(\mathbf{GF}(q))$ должна иметь порядок $\mathrm{ord}(P)\approx q-2\sqrt{q}$ [21]. Наилучшим универсальным алгоритмом криптоанализа является алгоритм A. 4.5 [21], сложность которого составляет $O\left(\left(\ln^c h\right)\sqrt{\pi\, h/2}\right)$ групповых операций, где h - наибольший простой делитель $\mathrm{ord}(P)$, c - небольшая константа [21];
- - для криптографических преобразований в якобиане гиперэллиптической кривой порядок произвольного абелевого многообразия A над $\mathbf{GF}(q)$ рода g, лежит в интервале $\left(q^{1/2}-1\right)^{2g}\le\#A(\mathbf{GF}(q))\le\left(q^{1/2}+1\right)^{2g}$, количество изогенных классов якобиановых многообразий рода g, чей порядок равен $\#\mathbf{J}\left(\mathbf{F}_q\right)=O\left(q^g\right)=O(N)$, соответственно равен $\#\mathbf{J}(\mathbf{GF}(q))=O\left(4gN^{1-1/2g}\right)$ [21]. Приведенный дивизор D якобиана гиперэллиптической кривой $\mathbf{J}_C(\mathbf{GF}(q))$ рода g, имеет простой порядок $\mathrm{ord}(D)\approx q^g$ [21]. Сложность наиболее эффективного алгоритма криптоанализа составляет $O\left(g^5 q^{2-4/(2g+1)+\varepsilon}\right)$.

На основе приведенных данных в таблице 74 представлены необходимые размеры полей (длины ключей) для фиксированного уровня стойкости.

Таблица 74. Длины ключей симметричного шифра AES и криптопсистем построенных на основе преобразований в поле, в группе точек ЭК и якобиане ГЭК, согласно результатов [21, 38]

Название задачи	m_1	m_2	m_3	m_4	m_5
AES	-	-	(80)	128	256
DLP, $\mathbf{GF}\left(2^m\right)$, A3	256	512	1024	3072	15360
ECDLP, $E\left(\mathbf{GF}\left(2^m\right)\right)$, A4.5	71	109	147	235	453
HECDLP, $g=2$, $C\left(\mathbf{GF}\left(2^m\right)\right)$, A7.1	26	42	58	95	186
HECDLP, $g=3$, $C\left(\mathbf{GF}\left(2^m\right)\right)$, A7.1	20	33	46	77	153
HECDLP, $g=4$, $C\left(\mathbf{GF}\left(2^m\right)\right)$, A7.1	17	29	41	69	139

Как видно из представленной таблицы, ГЭК обеспечивает соизмеримую стойкость с AES и ЭК при гораздо меньшей длине ключа. Преобразования в поле, при той же стойкости, требуют наибольшей длины ключа.

Владислав Ковтун

Приведение в решетках

NTRU

Описание

Данная криптосистема была впервые представлена на конференции CRYPTO'96 и опубликована в [64], 24 июля 2000 года на нее был получен патент США (U.S. Patent No. 6,801,597). Следует отметить, что наличие патента накладывает свой отпечаток на данную криптосистему – менее интенсивное исследование [65].

NTRU основана на алгебраической структуре некоторого полиномиального кольца. Трудноразрешимой задачей является поиск кратчайшего вектора в заданной решетке. Процедура шифрования основывается на смешанных операциях: полиномиальной алгебре и приведении по модулю двух чисел. Детальнее остановимся на процедурах формирования ключа и шифрования [65].

Пусть дано полиномиальное кольцо $\mathbf{\Gamma}$ с неприводимым полиномом $X^N - 1$, т.е. $\mathbf{\Gamma} = \mathbf{Z}[X]/(X^N - 1)$.

Формирование ключа

Вход: два числа p и q

Выход: открытый ключ h, личный ключ f, инверсия личного ключа I_{fp}.

1. Выбор случайным образом два полинома $f, g \in \mathbf{\Gamma}$, причем $\exists I_{fq} \equiv f^{-1} \bmod q$ и $\exists I_{fp} \equiv f^{-1} \bmod p$.
2. Вычисление $h \equiv I_{fq} \otimes g \bmod q$.
3. Return h, f, I_{fp}.

Зашифровывание

Вход: открытый текст $m \in \mathbf{\Gamma}$ (с коэффициентами, приведенными по модулю q), открытый ключ h

Выход: шифротекст e

1. Выбор случайным образом полинома $\phi \in \mathbf{\Gamma}$.
2. Вычисление шифротекста $e \equiv (p\phi \otimes h + m) \bmod q$.
3. Return e.

Расшифровывание

Вход: шифротекст e, личный ключ f

Выход: открытый текст m

1. Вычисление $a \equiv (f \otimes e) \bmod q$, где выбираются коэффициенты полинома a из $\left(-\frac{q}{2}, \frac{q}{2}\right)$.
2. Вычисление $m = (I_{fp} \otimes a) \bmod p$.

3. Return m.

Как стало видно из процедуры расшифровывания, криптосистема NTRU является вероятностной, что позволяет получить неправильное исходное сообщение на этапе расшифровывания при тех же значениях параметров f, g, ϕ. Вероятность ошибки ничтожно мала, и она напрямую зависит от корректного выбора f, g, ϕ, детальное описание их выбора рассматривается в [64].

Сложность криптоанализа

На сегодняшний день известно несколько атак: прямой перебор, встреча посредине, мультипликативное пропускание и атаки, основанные на решетках [64]. Приведем результаты сравнения длин ключей RSA и NTRU при соизмеримой стойкости в таблице 75.

Таблица 75. Соответствие длин ключей криптосистем RSA и NTRU [64]

Длина ключа RSA	512	1024	2048
Длина ключа NTRU	167	263	503

Производительность/сложность реализации

Данная криптосистема является достаточно молодой, и нельзя заявить о большом интересе к ней со стороны ученых, о чем свидетельствует небольшое количество публикаций. Однако авторам удалось найти несколько работ посвященных практической реализации, кроме начальной [64]. В таблице 76 укажем условия проведения экспериментальных оценок.

Таблица 76. Условия проведения экспериментальных оценок времени выполнения алгоритмов [65, 66]

№	Процессор	Операционная система	Компилятор	Особенности реализации
1	Intel, Celeron 500 MHz	Linux	gcc C++	?
2	Intel, Pentium II 266	MS Windows 98 SW	MS Visul C++	
3	ARM7TDMI 50 MHz		ARM Developmental Suite	

В таблице 77 сведем экспериментальные оценки сложности формирования ключей, а также шифрования.

Таблица 77. Экспериментальные оценки времени выполнения преобразований посредством NTRU [65, 66]

№	Операция	167			263	503		
		1	2	3	1	1	2	3
1	Формирования ключа	8,3	16,2	91,4	19,8	71,2	699,5	2412,1
2	Зашифровывание	0,8	0,6	4,9	1,9	6,6	15,0	110,9
3	Расшифровывание	1,4	1,4	5,7	3,5	12,7	29,4	163,1

Оценить производительность NTRU и другие, хорошо зарекомендовавшие себя криптосистемы, при соизмеримом уровне стойкости позволяю данные приведенные в таблице 78.

Таблица 78. Соответствие длин ключей криптосистем на ЭК, NTRU, RSA и косах обеспечивающий соизмеримый уровень безопасности [65]

	RSA	ECC	NTRU	Группа кос
Длина личного ключа, бит	1024	168	263	$p = 2,\ q = 2,\ n = 48$
Длин блока текста, бит	1024	160	416	1088
Длина открытого ключа, бит	1024	169	1841	1000
Время формирования ключа, мс	1432	65	19,8	8,5
Зашифровывание, мс	4,28	140	1,9	29,8

Расшифровывание, мс	48,5	67	3,5	14,9

Преобразования на ЭК были выполнены над OEF полем $\mathbf{GF}\left(\left(2^{14}-3\right)^{12}\right)$ [65].

Группа кос

Описание

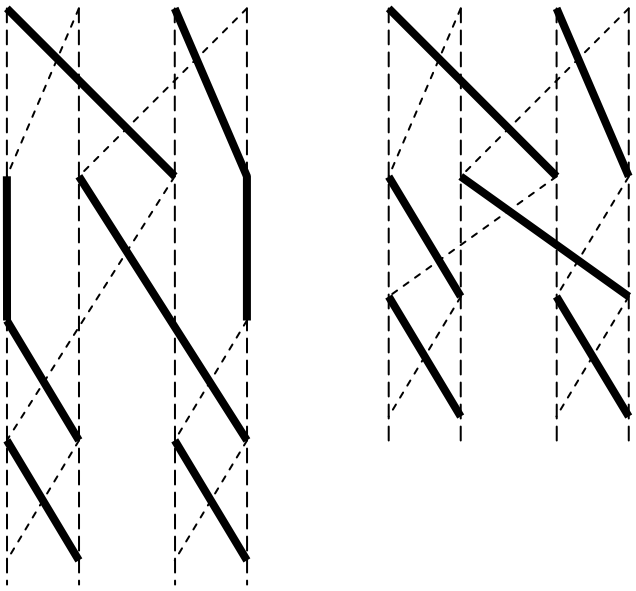
Произведем краткий экскурс в данную криптосистему [65]. n-коса – множество из n непересекающихся прядей, каждая из которых является соединенной с двумя горизонтальными полосками сверху и снизу. Между полосками одна прядь может пересекать одну горизонтальную линию - единожды. Когда генератор n, обозначенный как σ_n применен к n-косе, конечные токи «шнурков», что заканчиваются на позиции n и $n+1$ нижней полоски являются перекрученными слева направо. Соответственно σ_n^{-1} является аналогичным преобразованием, но «шнурки» являются перекрученными справа налево. Каждая n-коса может быть представлена словом (генератором примененным одним за другим) положительного и отрицательного генераторов.

Индекс косы n означает количество «шнурков» в косе.

Единичная коса – коса с некоторым индексом, в котором каждый «шнурок» прямо следует к нижней полоске. Фундаментальная коса содержит положительную экспоненту, каждое пересечение является положительным, что значит, когда два «шнурка» пересекаются слева направо проходят над остальными. Если фундаментальная коса имеет отрицательную экспоненту, то пересечения являются отрицательными. Группа n-косы обозначается через B_n и является множеством множеств n-кос. Каждая коса в группе косы может быть преобразована в любую другую косу в группе косы посредством формирования уравнения как указанное ниже:

$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$, если $|i-j|=1$ или $\sigma_j\sigma_i = \sigma_i\sigma_j$, если $|i-j|>1$.

Две косы являются эквивалентными если они принадлежат одной и той же группе. Каждая группа B_n может быть представлена в канонической форме, которая является уникальной для каждой B_n. Каноническая форма группы косы может быть представлена посредством фундаментальной косы и числом перестановок. Перестановки являются представлением одного из возможных вариантов упорядочивания множества. Количество перестановок в представлении посредством канонической формы обозначается как каноническая длина. Перестановки являются влевовзвешенной форме, т.е. если пересечения пройденными от одной перестановки к следующей, перестановки уже не могут представлять сформированною косу. На рис. 8 представлена каноническая форма.



а) б)

Рис. 8. а) Коса перед применение алгоритма эквивалентности. б) Коса после применения алгоритма эквивалентности [65]

Задача «слова» - задача преобразования косы из группы косы к ее уникальному каноническому представлению – канонической форме. Произведением ab двух кос является коса, полученная посредством размещения косы a поверх b.

Криптосистема, основанная на косах - частный случай более общего подхода впервые предложенного в [67]. Ключевым моментов в этой криптосистеме является задача эквивалентности. Существует алгоритм решения этой задачи за полиномиальное время. Результатом его является каноническая форма n-косы, которая соответствует уникальной группе косы. Если мы получили произведение трех кос axa^{-1} и преобразуем произведение в его каноническую форму, то исходные косы – множители найти достаточно сложная задача. Известные алгоритмы факторизации обладают экспоненциальной сложностью.

Следовательно, мы можем воспользоваться косами для реализации быстрой ассиметричной криптосистемы. Другим ключевым моментом такой криптосистемы, является свойство коммутативности кос построенных в LB_l (группа n-кос образованная генератором, который меньше некоторого целого d) и RB_r (группа n-кос образованная генератором, который большего некоторого целого d).

Кратко опишем процессы формирования ключа и шифрования [65].

Формирование ключа

Вход: числа l и r

Выход: открытый ключ (x, y) и личный ключ a

1. Выбирается достаточно сложная $(l+r)$-коса $x \in B_{l+r}$.
2. Выбирается коса $a \in LB_l$.
3. Вычисляется $y = axa^{-1}$.
4. Return (x, y) и a.

Владислав Ковтун

Зашифровывание

Вход: Сообщение m длиной k бит, открытый ключ (x, y)

Выход: Шифротекст (c, d)

1. Выбирается коса $b \in RB_r$ случайным образом.
2. Вычисляется $c = bxb^{-1}$.
3. Вычисляется $d = \mathbf{H}(byb^{-1}) \oplus m$, где $\mathbf{H}(t)$. – хэш-функция.
4. Return (c, d).

Расшифровывание

Вход: Шифротекст (c, d), личный ключ a

Выход: Открытый текст m

1. Вычисляется $m = \mathbf{H}(aca^{-1}) \oplus d$.
2. Return m.

Корректность алгоритма зашифровывания и расшифровывания легко доказать через свойство коммутативности кос a и b: $aca^{-1} = a(bxb^{-1})a^{-1} = b(axa^{-1})b^{-1} = byb^{-1}$

Сложность криптоанализа

Сложность криптоанализа определяется сложногстью задачи полного перебора ключей и составляет $O(\exp(\frac{1}{2} pn \log n))$, где p - каноническая длина и n - индекс косы.

Также следует отметить, что согласно исследованиям [68], на задачу эквивалентности в группе кос было предложено несколько вариантов алгебраической атаки. На сегодняшний день нет однозначного толкования в применимости данного подхода в криптографических целях, в тоже время, в работе [68] показано, что возможен такой выбор группы, в которой будет реально решить задачу эквивалентности, но невозможно решить задачу сопряженности, что позволяет говорить о необходимости дальнейшего изучения данного направления.

Производительность/сложность реализации

Данная криптосистема не получила широкого распространения по причине своей новизны и явными уязвимостями, которые были обнаружены в первичной публикации. В связи с этим, теоретические и экспериментальные оценки сложности реализации были опубликованы не так давно [65], которые приведены в таблице 79.

Таблица 79. Теоретическая оценка сложности преобразований в группе кос [65]

Операция	Зашифровывание	Расшифровывание
Сложность	$O(p^2 n \log n)$	$O(p^2 n \log n)$

p - каноническая длина, n - индекс косы, q - каноническая длина косы x - первый параметр в открытом ключе.

В таблице 80, приведена зависимость длин блоков открытого и зашифрованного текстов, а также открытого и личного ключа от параметров криптосистемы.

Таблица 80. Зависимость длины ключей, а также блоков открытого и зашифрованного текстов от параметров криптосистемы основанной на преобразовании в группе кос [65]

Криптография с открытм ключем. Текущее состояние

	Открытый текст	Зашифрованный текст	Личный ключ	Открытый ключ
Длина, бит	$O(pq\log n)$	$O(4pq\log n)$	$O(\frac{1}{2}pq\log n)$	$O(3pq\log n)$

p - каноническая длина косы, n - индекс косы, q - каноническая длина косы x - первый параметр в открытом ключе.

Условия проведения экспериментальных оценок приведены в таблице 81.

Таблица 81. Условия проведения экспериментальных оценок времени выполнения преобразований [65]

№	Процессор	Операционная система	Компилятор	Особенности реализации
1	Intel, Celeron 500 MHz	Linux	gcc C++	?

Согласно исследованиям, проведенным в работе [65], соотнесем длины ключей криптосистем при их соизмеримой стойкости к криптоанализу в таблице 82.

Таблица 82. Соответствие длин ключей криптосистем на ЭК, NTRU, RSA и косах обеспечивающий соизмеримый уровень безопасности [65]

Параметр, метрика	RSA	ECC	NTRU	Группа кос
Длина личного ключа, бит	1024	168	263	$p=2,\ q=2,\ n=48$
Длин блока текста, бит	1024	160	416	1088
Длина открытого ключа, бит	1024	169	1841	1000
Время формирования ключа, мс	1432	65	19,8	8,5
Зашифровывание, мс	4,28	140	1,9	29,8
Расшифровывание, мс	48,5	67	3,5	14,9

Преобразования на ЭК были выполнены над OEF полем $\mathbf{GF}\left(\left(2^{14}-3\right)^{12}\right)$ [65].

Владислав Ковтун

Криптосистемы на кодах

Литература

0. Diffie W., Hellman M. E. "Multi-user Cryptographic Techniques", Proceedings of AFIPS National Computer Conference. -1976. -pp.109-112.

1. Diffie W., Hellman M. New directions in cryptography // IEEE Transactions on information theory. -1976. -pp. 644–654. URL: http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf.

2. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. -Vol. 21 (2). -1978. -pp.120–126.

3.

4.

5.

6. ISO/IEC FCD 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves, Final Committee Draft. -2001.

7. IEEE P1363–2000: Standard Specifications for Public Key Cryptography. -2000. -206p. URL: http://www.ieee.org.

8. ANSI X9.62–1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). –1998. -192p.

9. ANSI X9.42–1998: Public Key Cryptography for The Financial Service Industry: Agreement of Symmetric Keys on Using Diffie–Hellman and MQV Algorithms. –1998. –93p.

10. ANSI X9.63–1999 Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. –1999. –207p.

11. ГОСТ Р 34.10–2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. –М.: Госстандарт России, 2001. –24с.

12. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. –К.: Держстандарт України, 2002. –40с.

13.

14.

15. Aori A., Kida Y., Shimoyama T., Sonoda Y., Ueda H., SNFS-248, E-mail announcement, 2004. URL: http://www.crypto-world.com/annoncements/SNFS248.txt

16. Avanzi R., Batina L., Chevallier-Mames B. etc. D.VAM.1 Performance Benchmarks. Revision 1.1 / In: M. Joye ed. // ECRYPT Research report IST-2002-507932. European Network of Excellence in Cryptology. August 3, 2005. –87 p.

17. Weimerskirch A., Stebila D., Chang Shantz Sh., Generic $\mathbf{GF}(2^m)$ Arithmetic in Software and its Application to ECC ECC // The 8th Australasian conference on information security and privacy (9-11 July 2003). –ACISP`2003. –Australia: Wollongong, 2003. –14p.

18. Ковтун В.Ю. Методы и алгоритмы арифметических преобразований с уменьшенной вычислительной сложностью на алгебраических кривых для криптографических приложений: Диссертация кандидата технических наук: Системы защиты информации. – Харьковский университет Воздушных Сил.– Украина: Харьков, 2005. –249 с.

19. C. Lim, P. Lee. More flexible exponentiation with precomputation. Advances in Cryptology – Crypto'94, LNCS 839, Springer-Verlag, 1994. -pp. 95-107.

20. Hankerson D., Lopez J., Menezes A. Software implementation of elliptic curve cryptography over binary fields / In Cetin K. Koc and C. Paar editors // Workshop and embedded systems. –CHES'99. –LNCS 1717. –Berlin: Springer–Verlag, 2000. –pp.1–24.

21. Ковтун В.Ю., Збитнев С.И., Шевченко Д.В., Гиневский А.М. Исследование алгоритмов решения задачи дискретного логарифма на эллиптической и гиперэллиптической кривых // Восточно–Европейский журнал передовых технологий. – 2004. –Вып. №6 (12). –С. 155–167. URL: http://www.nrjetix.com/r-and-d/publications/

22. Brown M., Hankerson D., Lopez J., Menezes A. Software implementation of the NIST elliptic curves over prime fields // Research Report CORR 2000–56. Department of Combinatorics and Optimization, University of Waterloo. –Canada: Waterloo, Ontario, 2000. –21p.

23. Стасев Ю.В., Головашич С.А., Ковтун В.Ю. Сравнительный анализ алгоритмов умножения и приведения по модулю в поле GF(2^m) // Радиотехника: Всеукраинский межведомственный научно–технический сборник. –2003. –Вып. №135. –С. 129–141. URL: http://www.nrjetix.com/r-and-d/publications/

24. OpenSSL Library, URL: www.openssl.org

25. Lenstra A.K., Verheul E.R.. The XTR public key system // Advances in Cryptology. – Crypto'2000. –LNCS 1880. –Berlin. –Springer, 2001.

26. Avanzi R., Bockle G., Breaken A. etc. D.AZTEC. 2-1.2 Alternatives to RSA (Lightweight Asymmetric Cryptography and Alternatives to RSA). Revision 1.2 / In: R. Avanzi ed. // ECRYPT Research report IST-2002-507932. European Network of Excellence in Cryptology. July, 27 2005. Revised August 17, 2005. –138 p.

27.

28. Збитнев С.И., Ковтун В.Ю., Илясова О.Е. Арифметические операции на эллиптической кривой над двоичным полем в проективных координатах // Радиотехника: Всеукраинский межведомственный научно–технический сборник. –2005. –Вып. №141. –С. 97–107. URL: http://www.nrjetix.com/r-and-d/publications/

29. Ковтун В.Ю. Метод сложения точек эллиптической кривой в проективных координатах Лопеса–Дахаба // Системы обработки информации. –2004. –Вып. №12 (40). –С. 83–88. http://www.nrjetix.com/r-and-d/publications/

30. Lopez J., Dahab R. Improved algorithms for elliptic curve arithmetic's in GF(2^n) // Selected Areas in Cryptography. –SAC'98. –LNCS 1556. –Berlin: Springer–Verlag, 1999. -pp.201–212.

31. Lange T. A notes on Lopez-Dahab coordinates. Cryptology ePrint Archive, report 2002/323, 2002. URL: http://eprint.iacr.org.

32. Higuchi A., Takagi N. A fast addition algorithm for elliptic curve arithmetic in GF(2^m) using projective coordinates // Information Processing Letters, 76. -2000. -pp. 101-103.

35. National Institute of Standards and Technology, Recommended Elliptic Curves for Federal Government Use, Appendix to FIPS 186-2, 2000. -43p.

36. Koblitz N. Hyperelliptic cryptosystems // Journal of cryptology. –1989. –No.1. -pp.139–150.

37. Ковтун В.Ю., Збитнев С.И., Шевченко Д.В. Исследование алгоритмов решения задачи дискретного логарифма в якобиане гиперэллиптической кривой // Радиотехника: Всеукраинский межведомственный научно–технический сборник. –2005. –Вып. №141. -С. 116–132. http://www.nrjetix.com/r-and-d/publications/

38. Enge A. The extended Euclidean algorithm on polynomials, and the efficiency of hyperelliptic cryptosystems // Designs, Codes and Cryptography. –Vol. 23. –No. 1. -pp.53–74.

39. Menezes A.J., Wu Y., Zuccherrato R.J. An elementary introduction to hyperelliptic curves // Technical report CORR96-19, Department of combinatorics and optimization, University of Waterloo, Waterloo, Ontario, 1996. In: Koblitz, N.: Algebraic aspects of cryptography, Springer-Verlag, Berlin Heidelberg New York. 1998.

40. Nagao K. Improving Group Law Algorithms for Jacobians of Hyperelliptic Curves // In W. Bosma, editor, ANTS IV, LNCS 1838. –Berlin. –Springer-Verlag. -pp. 439–448.

41. Wollinger T. Software and hardware implementation of hyperelliptic curve cryptosystems. PhD dissertation: Electronics and informatics. –Worchester Polytecnic Institute. –Germany: Bochum, 2004. –218 p.

42. Harley R. Fast arithmetic on genius two curves. –2000. URL: http://cristal.inria.fr/harley/hyper/, adding.txt and doubling.c.

43. Lange T. Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae // Cryptology ePrint Archive. –Report 2002/121. –2002. –13 p. URL: http://eprint.iacr.org.

44. Lange E. Inversion-free arithmetic on genus 2 hyperelliptic curves // Cryptology ePrint Archive. –Report 2002/147. –2002. -7 p. URL: http://eprint.iacr.org.

45. Ковтун В. Ю., Збитнев С. И. Арифметические операции в якобиане гиперэллиптической кривой рода 2 в проективных координатах с уменьшенной вычислительной сложностью // Восточно-Европейский журнал передовых технологий. -2004. –Вып. №½ (13). –С. 14–22. http://www.nrjetix.com/r-and-d/publications/

46. Ковтун В.Ю. Преобразования в якобиане гиперэллиптической кривой рода 2 в проективных координатах над полем нечетной характеристики // Радиотехника: Всеукраинский межведомственный научно-технический сборник. -2006. -Вып. №144. -Харьков. –С. 102–110. http://www.nrjetix.com/r-and-d/publications/

47. Byramjee B., Duquesne S. Classification of genus 2 curves over F2 and optimization of their arithmetic // Cryptology ePrint Archive. -Report 2004/107. -2004. URL: http://eprint.iacr.org

48. Lange T. Weighted coordinates on genius 2 hyperelliptic curves // Cryptology ePrint Archive. –Report 2002/153. –2002. –20p. URL: http://eprint.iacr.org.

49. Lange T., Stevens M. Efficient Doubling on Genus Two Curves over Binary Fields // Selected Areas in Cryptography. -Springer-Verlag. -LNCS 3357. -2004, –pp. 170–181.

50. Matsuo K., Chao J., Tsujii S. Fast genius two hyperelliptic curve cryptosystem // Technical report IEICE. –ISEC2001–31. –IEICE`2001. –2001. –8p.

51. Miyamoto Y., Doi H., Matsuo K., Chao J., Tsujii S. A fast addition algorithm of genius two hyperelliptic curve // In the 2002 Symposium on cryptography and information security. –SCIS`2002. Japan: IEICE, 2002. –pp.497–502. (In Japanese).

52. Takahashi M. Improving Harley algorithms for jacobians of genius 2 hyperelliptic curves // In the 2002 Symposium on cryptography and information security. –SCIS`2002. Japan: IEICE, 2002. –pp. 155–160. (In Japanese).

53. Sugizaki H., Matsuo K., Chao J., Tsujii S. An extension of Harley addition algorithm for hyperelliptic curves over finite fields of characteristic two // Technical report IEICE. –ISEC2002–09. –IEICE`2002. –2002. –8 p.

54. Kuroki J., Gonda M., Matsuo K., Chao J., Tsujii J. Fast genius three hyperelliptic curve cryptosystems // In The 2002 symposium on cryptography and information security (January 29 – February 1). –SCIS'2002. –Japan, 2002. –pp. 17–23.

55. Goda M., Matsuo K., Aoki K., Chao J., Tsujii S. Improvements of Addition Algorithm on Genus 3 Hyperelliptic Curves and their Implementations // In The 2004 Symposium on Cryptography and Information Security. –SCIS 2004. –Japan.

56. Augot D., Enge A., Girault M. etc. D.AZTEC.4-1.1 Hardness of the Main Computational Problems Used in Cryptography. Revision 1.1 / In: J.-S. Coron and B. de Weger ed. // ECRYPT Research report IST-2002-507932. European Network of Excellence in Cryptology. November 10, 2005. –62 p.

57. Lange T. Efficient arithmetic on hyperelliptic curves. PhD dissertation: Mathematics and informatics. –Germany: Essen, 2001. –122 p. URL: http://www.exp-mayh.uni-essen.de/~lange/KoblitzC.html

58. Galbraith S.D., Paulus S. and Smart N.P. Arithmetic on superelliptic curves. Math. Comp. 71(237). –2002. –pp. 393–405.

59. Harasawa R., Suzuki J. Fast Jacobian Group Arithmetic on C_{ab} Curves.

60. Volcheck. Computing in the Jacobian of plane algebraic curve // ANTS-I (Adleman, ed.). –LNCS 877. –Springer-Verlag. –1994. –pp. 221–223.

61. Huang M-D., Ierardi D. Efficient algorithms for the Rieman-Roch problem and for addition in the Jacobian of a curve // Journal of symbolic computation. –No.18. –1994. -pp. 519–539.

62. Flon S., Oyno R. Fast Arithmetic on Jacobians of Picard curves // In Public Key Cryptography. –PKC'2004. –LNCS 2947. –Springer. –2004. –pp. 55–68.

63. Flon S., Oyono R., Ritzentailer C. Fast addition on non-hyperelliptic genus 3 curve // Cryptology ePrint Archive. –Report 2004/118. –2004. –13 p. URL: http://eprint.iacr.org.

64. Hoffstein J., Pipher J., Silverman J. NTRU: A ring based public key cryptosystem // Algorithmic Number Theory. ANTS III. –Portland. –LNCS 1423. –Springer-Verlag. –1998. –pp. 267–288.

65. Karu P., Loikkanen J. Practical Comparison of Fast Public-key Cryptosystems.

66. O'Rourke C.M. Efficient NTRU Implementation. Master thesis: Electrical and Computer Engineering. –Worchester Polytechnic Institute. –2002. –99 p.

67. Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography // Mathematical Research Letters. –No.6. –1999. –pp.287–291.

68. Shpilrain V. Assessing security of some group based cryptosystems // Cryptology ePrint Archive. –Report 2003/123. –2003. –10 p. URL: http://eprint.iacr.org.

69. Merkle R. C. "Secure Communication Over Insecure Channels", Communications of the ACM, v.21, n.4, 1978, pp.294-299.

70. Simmons G. I. "Cryptology", Encyclopedia Britannica, 16th edition, 1986, pp.913-924B.

71. Варновский Н.П. Криптография и теория сложности // Математическое просвещение. –Сер. 3. –Вып. №2, –1998. –С. 71–86.

72. Press release of D-Wave Systems Company. URL: www.dwavesys.com

73. Журнал Компьютерра, #1, 1998, с. 6.

74. Frium H.R. The group law on elliptic curves on Hesse form // Research Report CORR 2001–09, Department of Combinatorics and Optimization, University of Waterloo. – Canada: Waterloo, Ontario, 2001. –February 1. –41p.

101. Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization// Mathematics of Computation 48. -1987. -pp. 243-264. URL: http://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3. ISSN 0025-5718. MR 88e:11130

102. Henri Cohen, Atsuko Miyaji, Takatoshi Ono. Efficient elliptic curve exponentiation using mixed coordinates// Kazuo Ohta, Dingyi Pei ed. Advances in cryptology-ASIACRYPT '98. LNCS 1514. -Springer. -1998. –pp. 51-65. ISBN 3-540-65109-8. MR 2000h:94002. URL: www.math.u-bordeaux.fr/~cohen/asiacrypt98.dvi.

103. Christophe Doche, Thomas Icart, David R. Kohel. Efficient scalar multiplication by isogeny decompositions/ Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, Tal Malkin ed.// 9th international conference on theory and practice in public-key cryptography, New York, NY, USA, April 24-26, 2006, proceedings. LNCS 3958, Springer. -2006. –pp. 191-206. ISBN 978-3-540-33851-2.

104. Daniel J. Bernstein, Tanja Lange. Faster addition and doubling on elliptic curves// Kaoru Kurosawa ed. Advances in Cryptology - ASIACRYPT 2007. LNCS 4833 Springer. -2007. -pp. 29-50. URL: http://eprint.iacr.org/2007/286.

105. Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters. Optimizing double-base elliptic-curve single-scalar multiplication/ Kannan Srinathan, Chandrasekaran Pandu Rangan, Moti Yung ed.// Progress in Cryptology - INDOCRYPT 2007. LNCS 4859, Springer. -2007. –pp. 167-182. ISBN 978-3-540-77025-1. URL: eprint.iacr.org/2007/410.

106. Daniel J. Bernstein, Tanja Lange. Inverted Edwards coordinates/ Serdar Boztas, Hsiao-feng Lu ed.// Applied algebra, algebraic algorithms and error-correcting codes, 17th international symposium, AAECC-17, Bangalore, India, December 16-20, 2007, proceedings. LNCS 4851, Springer. -2007. –pp. 20-27. ISBN 978-3-540-77223-1. URL: eprint.iacr.org/2007/410.

107. Huseyin Hisil, Kenneth Wong, Gary Carter, Ed Dawson. Faster group operations on elliptic curves. URL: eprint.iacr.org/2007/441.

108. Marc Joye, Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks/ Cetin Kaya Koc, David Naccache, Christof Paar ed.// Cryptographic hardware and embedded systems – CHES 2001. LNCS 2162, Springer, 2001. –pp. 402-410. ISBN 3-540-42521-7. URL: www.geocities.com/MarcJoye/publications.html.

109. Huseyin Hisil, Gary Carter, Ed Dawson. New formulae for efficient elliptic curve arithmetic/Kannan Srinathan, Chandrasekaran Pandu Rangan, Moti Yung ed.// Progress in Cryptology: INDOCRYPT 2007. LNCS 4859, Springer. -2007. –pp. 138-151. ISBN 978-3-540-77025-1.

110. Pierre-Yvan Liardet, Nigel P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form/ Cetin Kaya Koc, David Naccache, Christof Paar ed. // Cryptographic hardware

and embedded systems - CHES 2001. LNCS 2162, Springer. -2001. -pp. 391-401. ISBN 3-540-42521-7.

111. David V. Chudnovsky, Gregory V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests// Advances in Applied Mathematics 7. -1986. -pp. 385-434.

112. Olivier Billet, Marc Joye. The Jacobi model of an elliptic curve and side-channel analysis/ Marc Fossorier, Tom Hoeholdt, Alain Poli ed.// Applied algebra, algebraic algorithms and error-correcting codes. LNCS 2643, Springer. -2003. –pp. 34-42. ISBN 3-540-40111-3. URL: eprint.iacr.org/2002/125.

113. Rongquan Feng, Hongfeng Wu. Fast Point Multiplication on Elliptic Curves of Even Order // Cryptology ePrint Archive. –Report 2007/377. –2007. –15 p. URL: eprint.iacr.org/2007/377

114. Sylvain Duquesne. Improving the arithmetic of elliptic curves in the Jacobi model// Information Processing Letters 104. -2007. –pp. 101-105.

115. D. Hankerson, A. Menezes, S. Vanstone. Guide to Elliptic Curve Cryptography// Springer-Verlag, New York, 2004. URL: www.springeronline.com/sgw/cda/frontpage/0,10735,5-102-22-8685189-0,00.html

116. 2008 Giessmann

117. Daniel J. Bernstein. A software implementation of NIST P-224// The 5th Workshop on Elliptic Curve Cryptography - ECC 2001. URL: cr.yp.to/talks.html#2001.10.29, cr.yp.to/nistp224.html File: opt-idea53.c: ecadd function.

118. Toshio Hasegawa, Junko Nakajima, Mitsuru Matsui A Practical Implementation of Elliptic Curve Cryptosystems over GF(p) on a 16-bit Microcomputer//Proceedings of the First International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography. LNCS 1431. -1998. Springer-Verlag London. -pp. 182–194.

119. V. S. Dimitrov and L. Imbert and P. K. Mishra. Fast Elliptic Curve Point Multiplication using Double120.-Base Chains// Cryptology ePrint Archive, Report 2005/069. -2005.

120. Арифметика на кривой Дочи-Икарт-Кохеля (Doche-Icart-Kohel) ориентированной на удвоения в проективных координатах $\left[X:Y:Z:Z^2\right]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-2dik.html

121. Арифметика на кривой Дочи-Икарт-Кохеля (Doche-Icart-Kohel) ориентированной на утроения в стандартных проективных координатах $\left[X:Y:Z:Z^2\right]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-3dik-standard.html

122. Арифметика на кривой Эдвардса (Edwards) в инвертированных проективных координатах. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-edwards-inverted.html

123. Арифметика на кривой Эдвардса (Edwards) в стандартных проективных координатах $\left[X:Y:Z\right]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-edwards.html

124. Арифметика на кривой Хассе (Hesse) в расширенных стандартных проективных координатах $\left[X:Y:Z:X^2:Y^2:Z^2:XY:XZ:YZ\right]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-hessian-extended.html

125. Арифметика на кривой Хассе (Hesse) в стандартных проективных координатах $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-hessian-standard.html

126. Арифметика на кривой в форме скрещивания Якоби (Jacobi) в стандартных проективных координатах $[S:C:D:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-jintersect-standard.html

127. Арифметика на кривой в форме уравнения Якоби (Jacobi) 4-ой степени ориентированной на удвоения в проективных координатах $[X:X^2:Y:Z:Z^2]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-jquartic-2xxyzz.html

128. Арифметика на кривой в форме уравнения Якоби (Jacobi) 4-ой степени ориентированной на удвоения в проективных координатах $[X:X^2:Y:Z:Z^2:R]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-jquartic-2xxyzzr.html

129. Арифметика на кривой в форме уравнения Якоби (Jacobi) 4-ой степени ориентированной на удвоения в проективных координатах $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-jquartic-2xyz.html

130. Арифметика на кривой в форме уравнения Якоби (Jacobi) 4-ой степени в проективных координатах $[X:X^2:Y:Z:Z^2]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-jquartic-xxyzz.html

131. Арифметика на кривой в форме уравнения Якоби (Jacobi) 4-ой степени в проективных координатах $[X:X^2:Y:Z:Z^2:R]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-jquartic-xxyzzr.html

132. Арифметика на кривой в форме уравнения Якоби (Jacobi) 4-ой степени в проективных координатах $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-jquartic-xyz.html

133. Арифметика на кривой в форме Монтгомери (Montgomery) в проективных координатах $[X:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-montgom-xz.html

134. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в проективных координатах Якоби $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-shortw-jacobian-3.html

135. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в оптимизированных проективных координатах Якоби $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-shortw-jacobian.html

136. Арифметика на кривой в форме Вейерштрасса (Weierstrass) с $a_4=-1$ в стандартных проективных координатах $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-shortw-projective-1.html

137. Арифметика на кривой в форме Вейерштрасса (Weierstrass) с $a_4=-3$ в стандартных проективных координатах $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-shortw-projective-3.html

138. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в стандартных проективных координатах Якоби $[X:Y:Z]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-shortw-projective.html

139. Арифметика на кривой в форме Вейерштрасса (Weierstrass) с $a_4=-3$ в модифицированных проективных координатах Якоби $[X:Y:Z^2:Z^3]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-shortw-xyzz-3.html

140. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в общем виде в модифицированных проективных координатах Якоби $[X:Y:Z^2:Z^3]$. Поле нечетной характеристики. URL: http://www.hyperelliptic.org/EFD/g1p/auto-shortw-xyzz.html

141. Harold M. Edwards. A normal form for elliptic curves// Bulletin of the American Mathematical Society 44 (July 2007). -pp. 393-422. URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html

142. Nigel P. Smart. The Hessian form of an elliptic curve/Cetin Kaya Koc, David Naccache, Christof Paar ed.// Cryptographic hardware and embedded systems - CHES 2001. LNCS 2162, Springer, 2001. –pp. 118-125. ISBN 3-540-42521-7.

143. Арифметика на кривой в форме скрещивания Якоби (Jacobi) в расширеных проективных координатах $[S:C:D:Z]$. Поле нечетной характеристики.URL: http://www.hyperelliptic.org/EFD/g1p/auto-jintersect-extended.html

144. Eric Brier, Marc Joye. Weierstrass elliptic curves and side-channel attacks/ David Naccache, Pascal Paillier ed. // Public key cryptography. LNCS 2274, Springer. -2002. -pp. 335-345. ISBN 3-540-43168-3. URL: http://www.geocities.com/MarcJoye/publications.html

145. Andrew V. Sutherland. Constructing elliptic curves with prescribed torsion over finite fields. Preprint. -2008.

146. Арифметика на кривой в форме Эдвардса (Edwards) с $d_1=d_2$ в аффинных W координатах. Поле четной характеристики. URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-w-1.html

147. Арифметика на кривой в форме Эдвардса (Edwards) в аффинных W координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-w.html

148. Арифметика на кривой в форме Эдвардса (Edwards) с $d_1=d_2$ в проективных WZ координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-wz-1.html

149. Арифметика на кривой в форме Эдвардса (Edwards) в проективных WZ координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-wz.html

150. Арифметика на кривой в форме Эдвардса (Edwards) с $d_1=d_2$ в аффинных координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-xy-1.html

151. Арифметика на кривой в форме Эдвардса (Edwards) с $d_1=d_2$ в аффинных координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-xy.html

152. Арифметика на кривой в форме Эдвардса (Edwards) с $d_1=d_2$ в стандартных проективных координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-xyz-1.html

153. Арифметика на кривой в форме Эдвардса (Edwards) в стандартных проективных координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-edwards-xyz.html
154. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в аффинных координатах. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-affine.html
155. Арифметика на кривой в форме Вейерштрасса (Weierstrass) с $a_2 = 0$ в расширенных проективных координатах Лопеса-Дахаба. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-extended-0.html
156. Арифметика на кривой в форме Вейерштрасса (Weierstrass) с $a_2 = 1$ в расширенных проективных координатах Лопеса-Дахаба. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-extended-1.html
157. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в проективных координатах Якоби. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-jacobian.html
158. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в проективных координатах Лопеса-Дахаба. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-lopezdahab-0.html
159. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в проективных координатах Лопеса-Дахаба. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-lopezdahab-1.html
160. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в проективных координатах Лопеса-Дахаба. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-lopezdahab.html
161. Арифметика на кривой в форме Вейерштрасса (Weierstrass) в проективных координатах Лопеса-Дахаба. Поле четной характеристики URL: http://www.hyperelliptic.org/EFD/g12o/auto-shortw-projective.html
162. Bernstein, D.J., Lange, T. Analysis and optimization of elliptic-curve single-scalar multiplication/ G.L. Mullen, D. Panario, I.E. Shparlinski Ed.// Finite Fields and Applications (Proceedings 8th International Conference, Fq8, Melbourne, Australia, July 9-13, 2007). Contemporary Mathematics Series. -Vol. 461. -pp. 1-20.
163. Doche, C., Lange, T. Arithmetic of Elliptic Curves. CRC Press, Boca Raton, USA (2005). Chapter 13. -pp. 267–302.
164. Al-Daoud, E., and et al. A New Addition Formula For Elliptic Curves Over GF(2^n). IEEE Transactions on Computers. –Vol. 51. –Num. 8. -2002. -pp 972-975.
165. 2005 Lange
166. Kwang Ho Kim and So In Kim. A New Method for Speeding Up Arithmetic on Elliptic Curves over Binary Fields// Cryptology ePrint Archive, Report 2007/181. -2007. URL: eprint.iacr.org/2007/181
167. Tanja Lange, Reza Rezaeian Farashahi. Binary Edwards curves// Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008, Proceedings. Elisabeth Oswald and Pankaj Rohatgi ed. LNCS 5154, Springer, 2008. -pp. 244-265. ISBN 978-3-540-85052-6. URL: cr.yp.to/newelliptic/edwards2-20080611.pdf
168. N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, 1987, pp. 203–209
169. V. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985.