003.26+004.27+004.051

В.И. Долгов[1], А.В. Неласая[2]

[1]*Харьковский национальный университет радиоэлектроники, Харьков*
[2]*Запорожский национальный технический университет, Запорожье*

# ТЕОРЕТИЧЕСКАЯ И ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА СЛОЖНОСТИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ НА ЭЛЛИПТИЧЕСКИХ И ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

*В работе проводится теоретическое и экспериментальное сравнение сложности криптографических преобразований на эллиптических и гиперэллиптических кривых с учетом реализации на современной аппаратной платформе. Выполнено обобщение метрики для сравнения производительности криптосистем на кривых различного рода над $GF(2^m)$ на случай простого конечного поля. Экспериментально доказана перспективность использования арифметики гиперэллиптических кривых в протоколах асимметричной криптографии. Определены приоритетные направления дальнейших исследований в этой области.*

***Ключевые слова:*** *криптосистема, асимметричная криптография, сложность, стойкость, конечное поле, эллиптическая кривая, гиперэллиптическая кривая, дивизор, 64-разрядная платформа.*

## Введение

Асимметричные криптографические преобразования используются в системах направленного шифрования и цифровой подписи для обеспечения целостности, неотказуемости и аутентичности электронных ресурсов. В частности, задача аутентификации документов решается с помощью использования механизма электронной цифровой подписи, который реализуется методами криптографии с открытым ключом.

Для удобства использования, программная и аппаратная реализация криптографических методов должны в первую очередь обеспечивать достаточный уровень криптографической стойкости и при этом высокую скорость преобразований. Стойкость криптографических преобразований напрямую зависит от размеров значений параметров криптосистемы, главным среди которых является длина секретного ключа. Поэтому развитие математической базы алгоритмов двуключевой криптографии направлено, главным образом, на поиск компромисса между показателями «скорость-стойкость».

Программная реализация современных стандартов цифровой подписи (в частности украинского стандарта ДСТУ 4145-2002), основанных на арифметике в группах точек эллиптических кривых над конечными полями, для обеспечения достаточной стойкости требует подключения специализированных библиотек длинных чисел. Их использование связано с дополнительными накладными расходами на поддержку внутренних механизмов представления и обработки длинных чисел в форматах библиотек длинной арифметики.

Возможность уйти от этой проблемы обеспечивается использованием кривых более высокого рода. Точки таких гиперэллиптических кривых не образуют группу, однако в качестве групповой структуры используется якобиан кривой – факторгруппа дивизоров нулевой степени по подгруппе главных дивизоров.

Формула Хассе-Вейля для границ порядка группы дивизоров:

$$\left\lceil \sqrt{q}-1 \right\rceil^{2g} \le \#J/F_g \le \left\lfloor \sqrt{q}+1 \right\rfloor^{2g},$$

где q – характеристика поля, над которым определена кривая; g – род кривой, объясняет тот факт, что размер элементов основного поля уменьшается практически пропорционально роду кривой с сохранением заданного уровня криптостойкости. Однако сложность групповой операции возрастает с увеличением рода кривой. Это делает вопрос производительности криптосистем на гиперэллиптических кривых неоднозначным.

**Целью данной статьи** является проведение сравнительного анализа сложности криптографических операций на эллиптических и гиперэллиптических кривых второго и третьего рода для одинакового уровня стойкости.

## Теоретическая оценка сложности

В настоящее время в мире ведутся интенсивные работы по изучению теоретических и практических аспектов криптопреобразований на гиперэллиптических кривых. Гиперэллиптические кривые высокого рода (больше трех) не являются криптографически стойкими, поэтому для использования в практических криптосистемах, наряду с традиционными эллиптическими кривыми (первого рода), рекомендуются только гиперэллиптические кривые второго и третьего рода.

 

В табл. 1 приведено сравнение параметров различных криптографических примитивов для одинакового уровня стойкости.

До недавнего времени считалось, что криптографические преобразования на гиперэллиптических кривых настолько сложны, что их скорость не может достичь практически приемлемого уровня [1]. Однако анализ последних работ в этой области показывает, что применение современных методов вычислений позволяет значительно улучшить скоростные показатели таких преобразований.

В [2] введена новая метрика для сравнения производительности криптосистем на кривых различного рода над $GF(2^m)$. Поскольку для достижения одинакового уровня криптостойкости на кривых разного рода длина элементов основного поля различна, то не имеет смысла сравнивать сложность формул сложения и удвоения дивизоров просто по количеству операций умножения, возведения в квадрат и инверсий. Такой подход приемлем лишь для сравнения сложности формул для кривых одного и того же рода. Новая, более точная, метрика позволяет выразить сложность явных формул сложения и удвоения дивизоров в терминах количества процессорных инструкций, таких как сдвиг и XOR. Такое сравнение является процессорно-независимым и может быть адаптировано для любой аппаратной платформы.

Обобщение данного подхода на случай простого конечного поля заключается в выражении сложности формулы групповой операции количеством элементарных операций умножения (умножения двух операндов, по размерам не превышающих длину аккумуляторного регистра процессора). При этом допускаем, что сложности операций умножения и возведения в квадрат равны, а сложность операции инверсии определяется МИ-отношением (отношением времени одной операции инверсии к времени одной операции умножения), которое в данной работе было получено авторами экспериментальным путем для конечных полей разного размера.

Поскольку скорость операций умножения прямо зависит от размера элементов конечного поля, необходимо также введение коэффициента размера поля. Пусть отношение битовой длины элемента основного поля к длине аккумуляторного регистра процессора равно $l$, то есть, $l$ – количество регистров, необходимых для хранения одного элемента основного поля. При этом для перемножения двух операндов длины $l$ потребуется $k = l^2$ элементарных операций умножения для стандартного алгоритма умножения. Назовем k коэффициентом размера поля. Тогда для 64-разрядной платформы имеем следующие оценки сложности групповой операции (табл. 2).

Таблица 1

Сравнение параметров различных криптопреобразований с одинаковым уровнем стойкости

| Симметричные крипто-преобразования | | Криптореобразования в простом поле Галуа | | Криптореобразования на ЭК | | Криптореобразования на ГЭК второго рода | | Криптореобразования на ГЭК третьего рода | |
|---|---|---|---|---|---|---|---|---|---|
| Шифр | Длина ключа | Длина модуля | Длина ключа | Длина модуля | Длина ключа | Длина модуля | Длина ключа | Длина модуля | Длина ключа |
| DES | 56 | 384 | 384 | 112 | 112 | 56 | 112 | 39 | 112 |
| Triple DES | 168 | 4864 | 4864 | 336 | 336 | 168 | 336 | 114 | 336 |
| Rijndael | 128 | 2528 | 2528 | 256 | 256 | 128 | 256 | 87 | 256 |
| Rijndael | 192 | 6720 | 6720 | 384 | 384 | 192 | 384 | 130 | 384 |
| Rijndael | 256 | 13536 | 13536 | 512 | 512 | 256 | 512 | 173 | 512 |

Таблица 2

Сравнение сложности формул операций с дивизорами (ключ 192 бита) для 64-битной платформы

| Род кривой | Сложение | | Удвоение | | МИ-отношение | Коэффициент размера поля k |
|---|---|---|---|---|---|---|
| | Аффинные координаты | Проективные координаты | Аффинные координаты | Проективные координаты | | |
| 1 | I+2M+S<br>8M, 72T | 16M+2S<br>18M, 162T | I+2M+S<br>8M, 72T | 8M+4S<br>12M, 108T | 5 | 9 |
| 2 | I+22M+3S<br>28M, 112T | 47M+4S<br>51M, 204T | I+22M+5S<br>30M, 120T | 38M+6S<br>44M, 176T | 3 | 4 |
| 3 | I+70M+6S<br>78M, 78T | 132M+8S<br>140M,140T | I+69M+10S<br>81M, 81T | 120M+12S<br>132M, 132T | 2 | 1 |

В табл. 2 обозначены: I – количество операций инверсии, M – количество операций умножения, S – количество операций возведения в квадрат в исходной формуле сложности. Во втором ряду для каждой формулы приведены значения сложности, выраженные в соответствующем количестве операций умножения в основном поле (обозначение M) и в количестве элементарных операций умножения (обозначение T) с учетом коэффициента размера поля.

В табл. 3 приведено сравнение сложности формул групповой операции в элементарных операциях умножения для 64-разрядной платформы в случае использования стандартного алгоритма умножения.

Таблица 3

Сравнение формул групповой операции в элементарных операциях умножения для 64-разрядной платформы (стандартный алгоритм умножения)

| Длина ключа (бит) | 1 род | | | | 2 род | | | | 3 род | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Размер эл-тов поля | k | Сложение (8M) | Удвоение (8M) | Размер эл-тов поля | k | Сложение (28M) | Удвоение (30M) | Размер эл-тов поля | k | Сложение (78M) | Удвоение (81M) |
| 160 | 160 | 9 | 72 | 72 | 80 | 4 | 112 | 120 | 54 | 1 | 78 | 81 |
| 192 | 192 | 9 | 72 | 72 | 96 | 4 | 112 | 120 | 64 | 1 | 78 | 81 |
| 320 | 320 | 25 | 200 | 200 | 160 | 9 | 252 | 270 | 107 | 4 | 312 | 324 |
| 512 | 512 | 64 | 512 | 512 | 256 | 16 | 448 | 480 | 171 | 9 | 702 | 729 |
| 640 | 640 | 100 | 800 | 800 | 320 | 25 | 700 | 750 | 214 | 16 | 1248 | 1296 |

Полученные данные показывают, что наименьшей теоретической сложностью обладают все же криптографические преобразования на эллиптических кривых. Однако на длинах ключа 160-192 сложность операций на кривых третьего рода приближается к сложности операций на кривых первого рода. В то же время она является на 34 для сложения и 39 для умножения операций меньше, чем для кривых второго рода.

## Экспериментальная оценка сложности

Развитие вычислительной техники предоставляет новые возможности для повышения скорости реализации криптографических алгоритмов. В частности, переход от 32-разрядного процессора к 64-разрядным позволяет значительно повысить скорость реализации большинства алгоритмов. Компьютеры под управлением 64-битных операционных систем способны работать более чем с 4 Гбайт оперативной памяти, а также показывают большую по сравнению с 32-битными операционными системами производительность при параллельном выполнении различных приложений. Появление многоядерных архитектур позволяет говорить о «персональном суперкомпьютере». Графические ускорители GPU (Graphics Processing Unit), первоначально используемые только для ускорения трехмерной графики, стали мощными параллельными программируемыми устройствами, пригодными для решения широкого класса задач. Следовательно, актуальной является задача реализации криптографических библиотек для современных аппаратных платформ и определение степени влияния выбранного аппаратного решения на эффективность реализации.

Авторами были реализованы пакеты программ криптографических преобразований на эллиптических и гиперэллиптических кривых[3] для 64-разрядной платформы. Эксперименты были проведены на компьютере Pentium (R) Dual-Core CPU E5200 @2.50GHz 2.50GHz ОЗУ 4.00 Гб.

В табл. 4 – 6 приведено время скалярного умножения с помощью стандартного бинарного алгоритма на кривых соответственно первого, второго и третьего родов [3].

Приведенные экспериментальные данные проиллюстрированы на рис. 1.

На рис. 1 показана зависимость времени выполнения операции скалярного умножения от рода кривой для одинакового уровня стойкости (длина секретного ключа 160 бит). Каждый столбец диаграммы соответствует роду кривой. Высота столбца по оси ординат равна времени выполнения 100 операций скалярного умножения, выраженного в секундах.

Таблица 4

Время скалярного умножения на гиперэллиптической кривой второго рода

| Длина модуля кривой, бит | Длина ключа, бит | Итерационная формула Кантора, с. | Явная формула, с. | Явная формула с учетом всех частных случаев, с. |
|---|---|---|---|---|
| 80 | 160 | 0,053 | 0,229 | 0,273 |
| 120 | 240 | 0,101 | 0,262 | 0,438 |
| 160 | 320 | 0,116 | 0,344 | 0,592 |
| 200 | 400 | 0,168 | 0,433 | 0,743 |
| 240 | 480 | 0,210 | 0,794 | 0,965 |
| 280 | 560 | 0,366 | 0,902 | 1,139 |
| 320 | 640 | 0,441 | 1,061 | 1,320 |

Таблица 5

Время скалярного умножения на эллиптической кривой

| Длина модуля кривой, бит | Длина ключа, бит | Время скалярного умножения, с. | Длина модуля кривой, бит | Длина ключа, бит | Время скалярного умножения, с. |
|---|---|---|---|---|---|
| 160 | 160 | 0,01419 | 480 | 480 | 0,06147 |
| 240 | 240 | 0,02527 | 560 | 560 | 0,07581 |
| 320 | 320 | 0,03198 | 640 | 640 | 0,10265 |
| 400 | 400 | 0,04883 | | | |

Таблица 6

Время скалярного умножения на гиперэллиптической кривой третьего рода

| Длина модуля кривой, бит | Длина ключа, бит | Итерац. формула Кантора, с. | Явные формулы, с. |
|---|---|---|---|
| 56 | 168 | 1,60E-01 | 4,46E-03 |
| 58 | 174 | 1,65E-01 | 4,62E-03 |
| 60 | 180 | 1,72E-01 | 4,79E-03 |
| 62 | 186 | 1,78E-01 | 4,98E-03 |
| 64 | 192 | 1,84E-01 | 5,26E-03 |

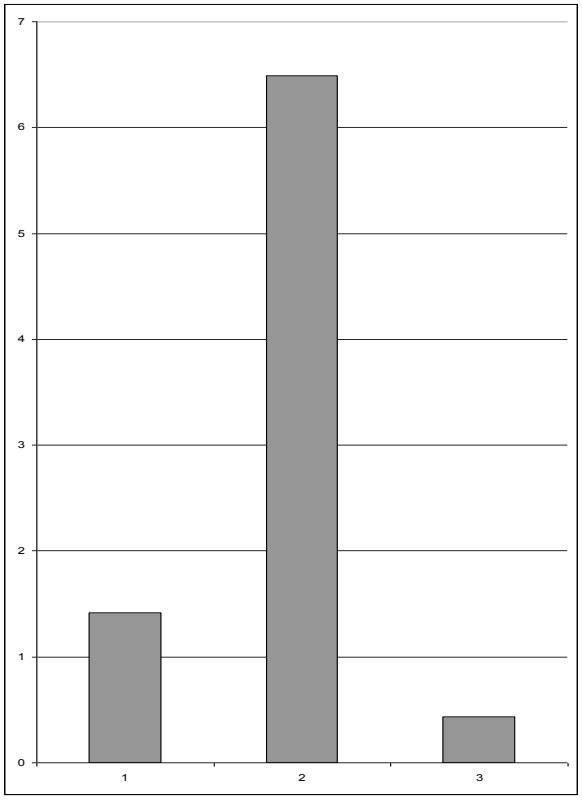


Рис. 1. Сравнение скорости криптографических преобразований на кривых 1, 2 и 3 родов

Судя по экспериментальным данным, скорость операции скалярного умножения на гиперэллиптических кривых третьего рода в приблизительно в 3,5 раза превышает скорость выполнения аналогичной операции на эллиптической кривой для уровней стойкости до 192 бит секретного ключа.

Объяснить причину расхождения теоретических результатов с экспериментальными достаточно просто. В предложенной теоретической модели не учтены накладные расходы на обслуживание внутренних механизмов библиотеки длинной арифметики, которые составляют существенный процент от полезной работы.

Громоздкая на первый взгляд формула групповой операции с дивизорами гиперэллиптической кривой хорошо поддается распараллеливанию. В совокупности с отказом от использования библиотек длинной арифметики и использования современных аппаратных платформ это дает неожиданно высокое увеличение скорости криптографических операций, несмотря на достаточно пессимистические теоретические оценки.

Следовательно, особенности программирования современных средств вычислительной техники требуют разработки нового подхода к формированию критериев оценки сложности вычислительных алгоритмов.

## Кривые над векторными полями

Если, следуя закону Мура, предположить, что в скором времени широкое распространение получат 128-разрядные процессоры, то можно будет реализовать криптосистему на гиперэллиптических кривых второго рода без использования библиотеки длинных чисел с длиной ключа до 256 бит. При этом можно ожидать достижения высоких скоростных характеристик.

Избежать использования библиотек длинной арифметики при реализации криптосистемы на гиперэллиптических кривых второго рода можно также, если использовать в качестве основного поля конечное векторное поле [4 – 6].

Конечное векторное поле задается вектором коэффициентов длины $n$, являющихся элементами конечного поля GF(p), при соответствующих базисных векторах. При этом операция умножения двух векторов выполняется по принципу умножения многочленов с последующим приведением подобных членов, определяемым таблицей умножения базисных векторов.

Определение гиперэллиптической кривой второго рода над векторным полем длины 2 позволяет на нижнем уровне криптографической системы использовать арифметику основного поля с длиной операндов до 64 бит, вместо 128 бит в случае простого поля. В этом случае, как и в описанной реали-

зации криптографической системы на гиперэллиптических кривых третьего рода, можно отказаться от использования библиотек длинных чисел.

Поскольку в векторных конечных полях операция умножения является распараллеливаемой по определению, целесообразным является определение гиперэллиптической кривой второго рода над векторным полем длины 4. Тогда арифметика основного поля будет включать лишь 32-битные целочисленные операции, для выполнения которых удобно использовать архитектуру XMM-расширения процессора и внутренних параллельных команд группы SSE2.

Дополнительных исследований на данном этапе требуют вопросы стойкости криптографических операций на гиперэллиптических кривых, определенных над векторными конечными полями.

## Заключение

Основным результатом данного исследования является экспериментально подтвержденное доказательство перспективности направления исследования, связанного с криптографическими преобразованиями на гиперэллиптических кривых.

Внедрение технологии использования гиперэллиптических кривых в асимметричных криптографических алгоритмах в рамках проведения работ по созданию Национальной PKI в Украине является актуальной и своевременной задачей.

Появление современных мощных аппаратных платформ с нестандартной архитектурой открывает широкие возможности перед гиперэллиптической криптографией.

При этом важной задачей исследования является формирование критериев оценки сложности вычислительных алгоритмов с учетом особенностей аппаратных платформ.

## Список литературы

*1. Smart N. On the Performance of Hyperelliptic Cryptosystems / N. Smart // Advances in Cryptology – EUROCRYPT '99, LNCS 1592. – Springer-Verlag, 1999. – P. 165-175.*

*2. Wollinger T. Software and Hardware Implementation of Hyperelliptic Curve Cryptosystem : Dissertation for the Degree of Doctor-Ingenious / T. Wollinger. – Bochum. – Germany, 2004. – 201 p.*

*3. Неласа Г.В. Удосконалення методів перетворень в якобіанах гіпереліптичних кривих для криптографічних додатків : автореф. дис. … канд. техн. наук : спец. 05.13.21 / Г.В. Неласа. – Х., 2010. – 22 с.*

*4. Молдовян Н.А. Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах / Н.А. Молдовян // Автоматика и телемеханика. – 2008. – № 12. – С. 163-177.*

*5. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи / Н.А. Молдовян. – СПб.: БХВ – Петербург, 2010. – 304 с.*

*6. Козіна Г.Л. Еліптичні криві над скінченим векторним полем / Г.Л. Козіна, Г.І. Нікуліщев // Системи обробки інформації. Безпека та захист інформації в інформаційних і телекомунікаційних системах. – 2010. – Вип. 3 (84). - С. 126.*

*Поступила в редколлегию 14.09.2010*

**Рецензент:** д-р техн. наук, проф. Л.М. Карпуков, Запорожский национальный технический университет, Запорожье.

### ТЕОРЕТИЧНА ТА ЕКСПЕРИМЕНТАЛЬНА ОЦІНКА СКЛАДНОСТІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ НА ЕЛІПТИЧНИХ ТА ГІПЕРЕЛІПТИЧНИХ КРИВИХ

В.І. Долгов, Г.В. Неласа

*В роботі проводиться теоретичне та експериментальне порівняння складності криптографічних перетворень на еліптичних та гіпереліптичних кривих з урахуванням реалізації на сучасній апаратній платформі. Виконано узагальнення метрики для порівняння продуктивності криптосистем на кривих різного роду над $GF(2^m)$ на випадок простого скінченого поля. Експериментально доказана перспективність використання арифметики гіпереліптичних кривих в протоколах асиметричної криптографії. Визначені пріоритетні напрямки подальших досліджень в цій області.*

***Ключові слова:*** *криптосистема, асиметрична криптографія, складність, стійкість, скінчене поле ,еліптична крива, гіпереліптична крива, дивізор, 64-розрядна платформа.*

### THEORETICAL AND PRACTICAL ESTIMATE OF CRYPTOGRAPHIC OPERATIONS ON ELLIPTIC AND HYPERELLIPTIC CURVES COMPLEXITY

V.I. Dolgov, G.V. Nelasa

*Theoretical and practical estimate of cryptographic operations on elliptic and hyperelliptic curves complexity with taking into account realization on modern hardware is carried out. Generalization of metric for comparing performance crypto transformations on different genus curves over $GF(2^m)$ to prime finite field case is carried out. The availability of using of hyperelliptic curves arithmetic in asymmetric cryptography protocols is confirmed by experiments. The foreground tasks for future research in this area are determined.*

***Keywords:*** *cryptosystem, open key cryptography, complexity, resistance, finite field, elliptic curve, hyperelliptic curve, divisor, 64-bit hardware.*