УДК 681.3.06

В.И. Долгов[1], А.В. Неласая[2], А.Н. Дорожкин[2]

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

УСКОРЕНИЕ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ НА ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ ТРЕТЬЕГО РОДА НАД МАЛЫМ ПОЛЕМ

В статье предлагаются технические решения по разработке библиотеки быстрых криптографических преобразований на гиперэллиптических кривых третьего рода, определенных над конечным полем с размером элементов 64 бита.

Ключевые слова: *гиперэллиптические кривые, библиотека криптографических преобразований, 64-разрядная платформа, модульные операции, сложение дивизоров, дублирование дивизоров.*

Введение

В Украине продолжается создание общегосударственной инфраструктуры открытых ключей, которое началось с внедрения информационной структуры поддержки электронной цифровой подписи. Современный украинский стандарт электронной цифровой подписи ДСТУ-4145, как и большинство стандартов других стран, основан на арифметике в группе точек эллиптических кривых, которые являются частным случаем более общего класса гиперэллиптических кривых (ГЭК). Особенность криптопреобразований на ГЭК состоит в том, что для достижения достаточного уровня стойкости можно определить кривую над конечным полем с элементами меньшего размера, что делает их возможной альтернативой криптопреобразованиям на эллиптических кривых. Следовательно, актуальными являются исследования, посвященные вопросам стойкости и эффективной реализации криптопреобразований на гиперэллиптических кривых.

Криптосистемы на основе арифметики якобианов гиперэллиптических кривых

Гиперэллиптические кривые различаются родом кривой. Эллиптические кривые – это кривые первого рода.

Гиперэллиптическая кривая рода $g \ge 1$ над конечным полем F_q представляет собой [1] набор решений $(x, y) \in \overline{F}_q \times \overline{F}_q$ уравнения

$$y^2 + h(x)y = f(x), \qquad (1)$$

где $h(x) \in F_q[x]$ – полином степени не более g; $f(x) \in F_q[x]$ – нормированный полином степени $2g+1$ и не существует решений $(x, y) \in \overline{F}_q \times \overline{F}_q$, которые бы одновременно удовлетворяли уравнению (1) и уравнениям с частными производными $2y + h(x) = 0$ и $h'(x)y - f'(x) = 0$.

Точки гиперэллиптической кривой не образуют группу, однако, групповую структуру имеет якобиан кривой, строящийся из классов дивизоров.

Порядок якобиана ограничен интервалом Хассе-Вейла

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

где q – характеристика поля, над которым определена кривая; g – род кривой. Как видно из (2) порядок такой группы значительно превышает количество точек кривой.

Стойкость криптографических преобразований на гиперэллиптических кривых определяется сложностью решения задачи дискретного логарифмирования на якобиане гиперэллиптической кривой.

Большинство криптографических приложений базируются на эллиптических или гиперэллиптических кривых с порядком группы не менее 2^{160}. Следовательно, для криптосистем на гиперэллиптических кривых над F_q должно выполняться как минимум условие

$$g \cdot \log_2 q \approx 160, \qquad (3)$$

где g – род кривой. В частности, для кривой рода 2, необходимо выбрать основное поле F_q с $|F_q| \approx 2^{80}$, то есть с длиной операндов 80 бит, а для кривой рода 3 – $|F_q| \approx 2^{54}$, то есть с длиной операндов 54 бита.

В отличие от эллиптических кривых, точку гиперэллиптической кривой можно факторизовать наподобие целого числа. Поэтому для ГЭК большого рода применимы атаки исчисления индексов, что исключает возможность их использования для создания криптосистем. Следовательно, практический интерес представляют только кривые малого рода.

В работах [2, 3] показано, как можно реализовать такую атаку для кривых рода 3 и 4 с использо-

ванием понятий ”больших простых” и ”двойных больших простых” дивизоров. Во избежание подобной слабости авторы этих работ рекомендуют увеличить размер группы ГЭК рода 3 на 12,5%.

Архитектура криптосистем на гиперэллиптических кривых состоит из четырех уровней (рис. 1).

Рис. 1. Уровни криптосистемы на ГЭК

Первый уровень – это операции основного поля, над которым определена кривая. К ним относятся сложение, умножение, возведение в квадрат и редукция. Скорость реализации базовых операций критична для общей производительности всей системы. Поскольку размер основного поля уменьшается пропорционально роду кривой, скорость реализации базовых операций при этом возрастает. Однако формулы сложения и дублирования дивизоров ГЭК усложняются с повышением рода кривой, что снижает эффект от уменьшения размера основного поля.

В работе [4] рассматриваются вопросы эффективной программной реализации и сравнения криптосистем на кривых 1, 2, 3 и 4 родов. Для программной реализации использовался компьютер Pentium4@1,8GHz. Все операции были реализованы для 32-разрядной платформы с использованием языка программирования C. Также сравнивалась производительность реализаций на встроенных процессорах ARM, ColdFire, PowerPC.

Имеет смысл сравнивать производительность криптосистем с одинаковым уровнем секретности. С учетом корректирующего множителя 12,5% для кривой 3 рода имеем [4]:

Таблица 1

Сравнение производительности операций на алгебраических кривых

Род	Основное поле	Порядок группы	Сложение в группе, μc	Дублирование в группе, μc	Скалярное умножение
I	$GF(2^{163})$	2^{163}	18,3	9,4	2,60
II	$GF(2^{81})$	2^{162}	18,7	11,7	2,73
III	$GF(2^{55})$	2^{165}	25,2	9,0	2,69

Как видно из табл. 1, несмотря на усложнение формул групповых операций с увеличением рода кривой, скорость скалярного умножения для кривых рода 1,2 и 3 сравнима, а также для рода 3 выше, чем для рода 2. Это вызывает интерес к кривым третьего рода с точки зрения отыскания резервов повышения производительности криптосистем на алгебраических кривых.

Целью исследования является ускорение операций на ГЭК третьего рода за счет низкоуровневой реализации арифметики основного поля на 64-разрядном процессоре.

Предложения по разработке эффективной программной реализации криптосистемы на гиперэллиптических кривых третьего рода

Как уже упоминалось, современные стандарты, базирующиеся на эллиптических кривых, требуют использовать кривые, имеющие циклическую подгруппу простого порядка $n \geq 2^{160}$. Исходя из формул (2), (3) размер модуля основного поля должен быть не менее 160 бит.

Для обработки таких больших чисел используются специализированные библиотеки. Существует два принципиально различных подхода к представлению больших чисел в ЭВМ[5]. Первый – это создание динамических структур, занимающих пространство именно такого размера, который потребуется для представления этих чисел. Такие, экономящие оперативную память служебные средства, поддерживаются программой управления динамической памятью для больших чисел, которая по мере необходимости выделяет или освобождает память при выполнении арифметических операций. Но в этом случае управление памятью увеличивает время вычислений. Второй - определение больших чисел со статической длиной. Большие натуральные числа представляются в виде векторов, элементы которых являются каким-либо стандартным типом данных. В этом случае скорость обработки возрастает за счет увеличения объема занимаемой памяти.

В табл. 2 представлены результаты анализа нескольких наиболее известных библиотек длинных чисел. Реализация криптосистемы на ГЭК третьего рода возможна с использованием любой из рассмотренных библиотек. Однако, как было показано выше, для достижения требуемого уровня секретности, достаточно выбрать основное поле с размером модуля 55 бит, что меньше 64. Это значит, что элементы такого поля могут целиком поместиться в регистры 64-разрядного процессора. То есть при реализации арифметики основного поля не потребуется подключение специализированной библиотеки для обработки длинных чисел.

Идея заключается в том, чтобы свести опера-

ции с элементами основного поля непосредственно к регистровой арифметике 64-разрядного процессора. Измерение скорости операции умножения двух 64-разрядных чисел в пакете Microsoft Visual Studio 2005 для 64-разрядной платформы с/без подключения библиотеки NTL дало приблизительно десятикратное увеличение скорости при использовании стандартного типа __int64.

Это дает основания предполагать, что при эффективной программной реализации арифметики основного поля с длиной модуля до 64 битов можно получить выигрыш в скорости, несмотря на усложнение самой формулы групповой операции на ГЭК.

Таблица 2

Сравнение специализированных библиотек для операций над большими числами

Название библиотеки	Платформа		Организация длинного числа	Наличие криптографических функций	Язык программирования	Компилируемость в MSVC++ 2005 x64 режиме
	32-bit	64-bit				
NTL	+	+	Массив	+	C++	+
Miracl	+	+	Массив структур	+	C/C++	–
GMP	+	+	Динамический массив	–	C	–
Arageli	+	+	Структура с массивом	+	C++	+
CryptoPP	+	+	Массив	+	C++	+

Одним из основных достоинств 64-разрядных процессоров является их возможность за меньшее число тактов сложить или умножить большие числа по сравнению с 32-разрядными, а также наличие XMM-регистров с разрядностью 128 бит. Эти регистры идеально подходят для хранения результата арифметической операции, произведенной над двумя 64-разрядными числами.

Появились некоторые изменения в количестве и названия регистров для 64-разрядных процессоров. Старые регистры, расширенные до 64 бит получили названия RAX, RBX, RCX, RDX, RBP, RSI, RDI, RSP, RIP и RFLAGS, а так же появились еще 8 64-разрядных регистров от R8 до R15. Имеются так же 128-разрядные регистры XMM0-XMM15.

Отметим, что технология SSE2(Streaming SIMD Extensions 2) позволяет повысить эффективность операций с 128-разрядными данными в формате чисел с плавающей точкой двойной точности и целочисленными данными. Эта технология расширяет технологию MMX и позволяет использовать 128-разрядные операнды вместо 64, а так же использовать целочисленные данные. SSE2 команды используют регистры XMM0-XMM7 и позволяют производить арифметические действия с упакованными или скалярными целыми операндами длиной 128 бит.

Для реализации программ под управлением 64-разрядной Windows XP была выбрана среда разработки MS Visual Studio 2005. Данная среда разработки может обеспечить перенос кода с 32-разрядной платформы на 64-х разрядную.

В разрабатываемой системе для представления элементов основного поля используется тип ULONG64 объявленный как unsingned __int64() в заголовочном файле WinAPI BaseTsd.h. Для этого типа корректно определенны операции сложения и вычитания при условии контроля за битом переполнения.

Для реализации криптосистемы на гиперэллиптических кривых третьего рода, как уже упоминалось выше, базовой является арифметика основного поля, т.е модульные операции сложения, умножения, возведения в квадрат и инверсии.

Наиболее часто используется операция умножения по модулю. При этом при умножении двух 64-разрядных чисел, максимальная длина результата равна 128 битам. Результат необходимо привести по модулю длиной 64 бита. Для умножения используется SSE2 инструкция __umul128. (рис. 2)

```
ULONG64 a =0xFB579799496871C7I64;
ULONG64 b =0xFCBADD11A6F271C7I64;
ULONG64 c, d;
d = _umul128(a, b, &c);
printf_s("%#I64x * %#I64x = %#I64x%I64x\n",
a, b, c, d);
```

Рис. 2. Умножение двух 64-разрядных чисел

Эта инструкция умножает два операнда представленных 64-разрядными числами и возвращает младшие 64 бита произведения, а так же указатель на старшие биты в третьем аргументе. Недостатком этой функции является ее представление произведения в двух 64-разрядных регистрах, а не в одном 128-разрядном. Это является проблемой при приведении результата произведения по модулю основного поля, так как не получиться совершить данное

действие одной операцией.

Определяющей является операция модулярной редукции, поскольку приведение результата по модулю основного поля осуществляется после каждой операции. Основными алгоритмами модулярной редукции являются: классический алгоритм, алгоритм Барета, алгоритм Монтгомери, алгоритм модульного суммирования коэффициентов, а также недавняя разработка киевских ученых – итеративный алгоритм модулярной редукции[6], который является наиболее эффективным среди всех перечисленных при выполнении определенного условия для модуля. Этот нюанс необходимо учитывать при выборе параметров криптосистемы, а именно при задании основного поля, над которым определяется гиперэллиптическая кривая. Для практической реализации в разрабатываемой криптосистеме выбран итеративный алгоритм модулярной редукции.

Остается добавить, что использование проективных координат исключает надобность в ресурсоемкой операции инверсии в конечном поле.

Вывод

Таким образом, реализация криптографической системы с использованием арифметики якобиана гиперэллиптической кривой третьего рода не может быть эффективно реализована путем подключения специализированных библиотек для обработки больших чисел.

Поскольку достаточная криптографическая стойкость обеспечивается при малом размере элементов основного поля (длиной до 64 бита), авторы предлагают реализовать арифметику основного поля на 64-разрядном процессоре с использованием среды разработки MS Visual Studio 2005. Элементы основного поля в этом случае не являются большими числами, а представляются стандартным типом ULONG64, что открывает скрытые резервы производительности.

Следующим шагом в данном направлении является детальная проработка явных формул сложения и дублирования дивизоров с учетом всех возможных вариантов видов входных дивизоров по аналогии с [7].

Список литературы

1. Menezes A. An Elementary Introduction to Hyperelliptic Curves / A. Menezes, Y. Wu, R. Zuccherato // Published as Technical Report CORR 96-19 Department of C&O University of Waterloo. – Ontario, Canada, 1996. – P. 1-35. – [Электронный ресурс]. – Режим доступа: www.cacr.math.uwaterloo.ca/techreports/1997/corr96-19.ps.

2. Thériault N. Index calculus attack for hyperelliptic curves of small genus / N. Thériault. – 2003. – 17 с. – [Электронный ресурс]. – Режим доступа: //http://www.math.uwaterloo.ca/~ntheriau/.

3. Gaudry P. A double large prime variation for small genus hyperelliptic index calculus / P. Gaudry, E. Thomé, N. Thériault – 2005. – 16 с. – [Электронный ресурс]. – Режим доступа: //http://www.math.uwaterloo.ca/~ntheriau/.

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

5. Вельшенбах М. Криптография на C и C++ в действии: учебное пособие / М. Вельшенбах. – М.: Триумф, 2004. – 464 с.

6. Мекуш О.Г. Алгоритми модулярної арифметики великих чисел : автореф. дис. ... канд. фіз.-мат. наук : спец. 01.05.01 „Теоретичні основи інформатики та кібернетики” / О.Г. Мекуш. – К.: Лотос, 2005. – 17 с.

7. Долгов В.И. Геометрический подход к сложению дивизоров гиперэллиптической кривой / В.И. Долгов, А.В. Неласая // Радіоелектроніка. Інформатика. Управління. – 2007. – № 2 (18) . – С. 44-50.

Поступила в редколлегию 25.03.2009

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

ПРИСКОРЕННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ НА ГІПЕРЕЛІПТИЧНИХ КРИВИХ ТРЕТЬОГО РОДУ НАД МАЛИМ ПОЛЕМ

В.І. Долгов, Г.В. Неласая, О.М. Дорожкін

В статті пропонуються технічні рішення по розробці бібліотеки швидких криптографічних перетворень на гіпереліптичних кривих третього роду, визначених над скінченим полем з розміром елементів 64 біта.

Ключові слова: *гіпереліптичні криві, бібліотека криптографічних перетворень, 64-розрядна платформа, модульні операції, додавання дивізорів, дублювання дивізорів.*

SPEEDING-UP OF CRYPTOGRAPHIC TRANSFORMATION ON HYPERELLIPTIC CURVES OF GENUS THREE OVER SMALL FIELD

V.I. Dolgov, G.V. Nelasaya, O.M. Dorogkin

In this article the technology for design of fast cryptography library on hyperelliptic curves of genus three over finite field with 64 bit size elements is proposed.

Keywords: *curves, library of the cryptographic transformations, 64-class platform, module operations, duplication.*