Александр Игоревич Скрипко¹, Александр Николаевич Велигура²

¹ Национальный исследовательский ядерный университет «МИФИ», Каширское шоссе, 31, г. Москва, 115409, Россия

e-mail: lifeisperfect3@gmail.com, ORCID 0000-0001-6753-8321

² Финансовый университет при Правительстве Российской Федерации, Ленинградский проспект, 49, Москва, 125993, Россия

e-mail: anveligura@fa.ru, ORCID 0000-0001-7694-7688

ОПТИМИЗАЦИОННЫЕ ЗАДАЧИ ВЫЧИСЛЕНИЙ В ЭЛЛИПТИЧЕСКИХ КРИВЫХ

DOI: <http://dx.doi.org/10.26583/bit.2017.3.08>

Аннотация. В настоящее время повсеместно применяются стандартизированные криптоалгоритмы, использующие вычисления в эллиптических кривых. В силу постоянно возрастающих требований к скорости их выполнения, становится актуальной задача оптимизации их реализации. В связи с широким использованием вычислений в группе точек эллиптической кривой на различных технических устройствах, применяемых для обеспечения безопасности информационных технологий, целесообразно сформировать оптимизационную задачу вычислений в эллиптических кривых. Решение полученной задачи позволило бы находить оптимальный в данных условиях путь вычисления. Подобный подход привёл бы к повышению быстродействия криптоалгоритмов на устройствах, обеспечивающих защиту информации. В статье представлен один из возможных подходов к оптимизации вычислений в эллиптических кривых с точки зрения математического программирования. Для формирования соответствующей оптимизационной задачи вводятся понятия композиции операций в группе точек эллиптической кривой и композиции методов вычисления произведения. Сведение оптимизации вычислений в эллиптических кривых к задачам математического программирования позволяет исследовать вопрос применимости известных методов оптимизации к вычислениям указанного типа.

Ключевые слова: эллиптическая криптография, оптимизация вычислений, математическое программирование.

Для цитирования. СКРИПКО, Александр Игоревич; ВЕЛИГУРА, Александр Николаевич. ОПТИМИЗАЦИОННЫЕ ЗАДАЧИ ВЫЧИСЛЕНИЙ В ЭЛЛИПТИЧЕСКИХ КРИВЫХ. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 67-71, July 2017. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/266>>. Дата доступа: 01 dec. 2017. doi:<http://dx.doi.org/10.26583/bit.2017.3.08>.

Alexander Igorevich Skripko¹, Alexander Nikolaevich Veligura²

¹ National Research Nuclear University MPhI, 31, Kashirskoe sh., Moscow, 115409, Russia
e-mail: lifeisperfect3@gmail.com, ORCID 0000-0001-6753-8321

² Financial University under the Government of the Russian Federation, 49, Leningradsky Prospekt, Moscow, 125993, Russia

e-mail: anveligura@fa.ru, ORCID 0000-0001-7694-7688

Application of mathematical optimization in elliptic curve arithmetic

DOI: <http://dx.doi.org/10.26583/bit.2017.3.08>

Abstract. Currently, a lot of standardized elliptic curve cryptographic algorithms are widely used. Due to the constantly increasing execution speed demands, implementation optimization problem become actual. Using elliptic curve arithmetic on a different information security devices require to form an mathematical programming problem of elliptic curves calculation. Solution of this problem allows to find optimal way of calculation in the current condition. This approach increases the speed of cryptographic algorithms on information security devices. The

paper present one of the possible ways to optimize computations in elliptic curve arithmetic by using mathematical programming. An optimization problem is formed that describes the calculation of scalar multiplication. Operations composition and multiplication methods composition are introduced to form the corresponding optimization problem. Addition of elliptic curve calculations to the mathematical programming problem allow to research applicability of known optimization methods to computations in elliptic curves.

Keywords: *elliptic curve cryptography, computation optimization, mathematical programming.*

For citation. SKRIPKO, Alexander Igorevich; VELIGURA, Alexander Nikolaevich. Application of mathematical optimization in elliptic curve arithmetic. IT Security, [S.l.], v. 24, n. 3, p. 67-71, july 2017. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/266>>. Date accessed: 01 dec. 2017. doi:<http://dx.doi.org/10.26583/bit.2017.3.08>.

Введение

Широкое использование вычислений в группе точек эллиптической кривой в криптографических алгоритмах, растущие требования к скорости выполнения этих операций естественным образом приводит к постановке задачи минимизации времени вычислений. Стремление к повышению быстродействия работы криптоалгоритмов породило большое количество оптимизаций по архитектуре (как, например, в [1]) и по количеству операций поля, необходимых для вычисления операции в группе точек (как представлено в исследованиях [2], [3], [4], [5], [6], [7] и [8]). Вместе с тем потребность в скорости выполнения криптографических алгоритмов делает актуальной задачу разработки методов минимизации времени вычислений в группе точек эллиптической кривой, не основываясь на использовании какого-то фиксированного метода или какой-либо конкретной архитектуры устройства. Разработку подобного инструментария целесообразно проводить путем применения методов математического программирования к области вычислений в эллиптических кривых. В данной работе рассмотрен подход к оптимизации вычисления произведения точки кривой на натуральное число (скаляр).

Постановка задачи

Пусть имеется эллиптическая кривая E над полем K , натуральный множитель (скаляр) k и множество M_k методов вычисления произведения точки на скаляр $k[P]$.

Требуется сформулировать задачу оптимального в данных условиях вычисления произведения $k[P]$. Под оптимальностью будем понимать наименьшее допустимое количество операций, необходимое для проведения вычисления.

Базовые и усложнённые операции

Как известно ([7] и др.), на множестве $E(K)$ точек эллиптической кривой и еще одного элемента – бесконечно удаленной точки – можно определить операцию, по отношению к которой $E(K)$ образует абелеву группу. Эту операцию обычно называют операцией сложения точек (англ. points addition [10]) и используют аддитивную запись $A(P, Q) = P + Q$. Стоит отметить, что в случае совпадения P и Q данная операция называется удвоением точки (англ. point doubling [10]), определяется другими соотношениями и обозначается как $D(P) = P + P$. Наряду с основной операцией интерес для приложений представляют составные операции (англ. composite operation [2]), такие как, например, умножение точки кривой на число (скаляр) (англ. scalar multiplication [9]), под которым понимается k – кратное сложение:

$$[k]P = \underbrace{\quad}_{k \text{ раз}} \quad (1)$$

Помимо тривиального способа вычисления (то есть многократного сложения), существуют различные методы вычисления скалярного произведения точки на число. Среди них:

- методы, использующие представление множителя k в различных системах счисления (англ. numeral system, $NumS$, $Radix - r$, $m - ary$ [9], [10]);
- методы, использующие представление множителя k в так называемых **несмежных формах** (англ. non-adjacent form, NAF [2], [10]).

Примерами других составных операций могут послужить: операция удвоения точки и последующего сложения $DA^Q(P) = 2P + Q$ (англ. doubling-addition operation [2]); операция утроения точки и последующего сложения $TA^Q(P) = 3P + Q$ операция произведения точки на простое число d (англ. composite operation dP [2]); операция произведения точки на простое число с последующим сложением $dP + Q$ (англ. composite operation $dP + Q$ [2]).

Выполнение различных операций в группе точек кривой требует различного количества операций поля K , над которым рассматривается кривая. Так, операция удвоения точки в аффинных координатах требует 2 умножения, 2 возведения в квадрат и 1 инверсию, а для сложения двух точек, представленных в координатах Якоби, с совпадающими z -координатами понадобится 5 умножений и 2 возведения в квадрат. **Стоимостью** операции θ в группе точек будем называть количество операций поля (умножений, возведений в квадрат и обращений), необходимое для выполнения операции θ и обозначать $c_\theta = n_M M + n_S S + n_I I$. Таким образом, для указанных выше операций можно записать: $c_{DAff} = 2M + 2S + 1I$, $c_{Az} = 5M + 2S$.

Композиция операций в группе точек

В силу замкнутости основной и составных операций мы можем определить композицию подобных операций на множестве точек кривой. Пусть P — точка кривой, θ_1 и θ_2 — замкнутые операции на множестве таких точек. **Композицией операций** θ_1 и θ_2 будем называть последовательное применение θ_1 и θ_2 к точке P , то есть $\theta_1(\theta_2(P))$, и обозначать $\theta_1 \circ \theta_2(P)$.

Заметим, что каждому фиксированному множителю и фиксированному методу вычисления произведения соответствует некоторая композиция операций в группе точек кривой. Указанная композиция при этом осуществляет преобразование исходной точки P в точку $k[P]$. Обозначим вычисление произведения методом m с множителем k через (m, k) , а через $\varphi(m, k)$ — оператор получения композиции операций, соответствующей (m, k) . Заметим, что $\varphi(m, k)$ не зависит от точки P , при этом φ не инъективен, а потому не является биекцией.

Композиция методов вычисления произведения точки на скаляр

Пусть P — точка кривой, (m_1, k_1) и (m_2, k_2) — некоторые методы вычисления произведения. **Композицией методов** вычисления произведения (m_1, k_1) и (m_2, k_2) будем называть последовательное применение композиций операций $\varphi(m_1, k_1)$ и $\varphi(m_2, k_2)$ к точке P , то есть

$$(m_1, k_1) \circ (m_2, k_2) = \varphi(m_1, k_1) \circ \varphi(m_2, k_2) \quad (2)$$

Другими словами, композицией методов вычисления произведения называется композиция композиций операций, соответствующих каждому из методов.

Пример. Пусть $k_1 = 13$ и $m_1 = NumS_2$. Тогда для любой точки $P \in E(K)$ верно:

$$\varphi(NumS_2, 13)(P) = DA \circ \circ \circ = 2(2(2P + P)) + P = [13]P. \quad (3)$$

Пусть $k_2 = 23$ и $m_2 = NumS_3$. Тогда для любой точки $P \in E(K)$ верно:

$$\varphi(NumS_3, 23)(P) = TA^{2P} \circ \circ \circ = 3(3(2P) + P) + 2P = [23]P. \quad (4)$$

Композицией $(NumS_2, 13)$ и $(NumS_3, 23)$ для некоторой точки P будет композиция композиций из (2) и (3):

[illegible]

Заметим, что композицию, введённую таким образом, можно использовать только для вычислений с совпадающими точками P . Отметим также, что композиция методов, вообще говоря, не является коммутативной.

Под **стоимостью вычисления** F некоторой композиции операций $\Theta = \theta_1 \circ \dots \circ \theta_n$ будем понимать сумму стоимостей всех операций, то есть $F(\Theta) = c_{\theta_1} + \dots + c_{\theta_n}$.

Оптимизационная задача вычисления произведения точки на скаляр

Теперь, введя понятия композиции операций в группе точек, композиции методов вычисления произведения и приняв функцию F за функцию стоимостей из [11] и [12], мы можем сформировать **оптимизационную задачу вычисления произведения точки на скаляр** $[k]P$, где $k = k_1 \cdot \dots \cdot k_n$, путем последовательного умножения:

$$\min_{k_1, \dots, k_n} F(\varphi(m_1, k_1) \circ \dots \circ \varphi(m_n, k_n)),$$

при условиях

$$m_i \in M_k, i = \overline{1, n}, \quad (6)$$

$$\varphi(m_1, k_1) \circ \dots \circ \varphi(m_k, k_k)(P) = [k]P.$$

Как видно из (6), задача поиска наименьшей стоимости вычисления произведения путем последовательного умножения сводится к поиску некоторой композиции методов из M_k , осуществляющей преобразование вида $P \rightarrow [k]P$, на которой функция стоимости принимает минимальное значение. Задача (6) является задачей дискретной оптимизации, для большинства из которых не найдено алгоритмов решения полиномиальной сложности [12]. Исходя из вида задачи (6), можно предположить, что для ее решения могут быть использованы методы динамического программирования [11,13,14].

Заключение

В статье предложен подход к оптимизации вычислений в группе точек эллиптической кривой путем использования методов математического программирования. Представлена оптимизационная задача, соответствующая указанному подходу. Практическая ценность предложенного подхода заключается в том, что он даёт возможность перейти к исследованию полученной задачи математического программирования уже разработанными в этой области методами. Подобный подход может поспособствовать увеличению быстродействия работы криптографических алгоритмов на устройствах, обеспечивающих защиту информации, с различным количеством имеющихся ресурсов.

СПИСОК ЛИТЕРАТУРЫ

- 1 Bluhm M. Software optimization of binary elliptic curves arithmetic using modern processor architectures. 2013. 210 pp. URL (дата обращения: 11.06.2017): https://www.emsec.rub.de/media/attachments/files/2014/11/MA_Bluhm.pdf
- 2 Longa, P. Accelerating the scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields : for the degree of Master of Applied Science 2007. — 173 pp.
- 3 Gueron S., Krasnov V. Fast Prime Field Elliptic Curve Cryptography with 256 Bit Primes. 2014. 17 pp. URL (дата обращения: 11.06.2017): <https://eprint.iacr.org/2013/816.pdf>
- 4 Bernstein D., Lange T. Analysis and optimization of elliptic-curve single-scalar multiplication. 2008. 19 pp. URL (дата обращения: 11.06.2017): <http://www.hyperelliptic.org/EFD/precomp.pdf>
- 5 Feng M., Zhu B., Xu M., Li S. Efficient Comb Elliptic Curve Multiplication Methods Resistant to Power Analysis. 2005. 31 pp. URL (дата обращения: 11.06.2017): <https://eprint.iacr.org/2005/222.pdf>

- 6 Cohen H., Miyaji A., Ono T. Efficient Elliptic Curve Exponentiation Using Mixed Coordinates. 2002. 14 pp.
- 7 Болотов А. А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. 2006. 280 с.
- 8 Giorgia P., Imberta L., Izarda T. Optimizing Elliptic Curve Scalar Multiplication for small scalars. 2009. 10 pp.
- 9 Blake I. F., Seroussi G, Smart N. P. Elliptic Curves In Cryptography. 1999. 217 pp.
- 10 Hankeron D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. 2004. 331 pp.
- 11 Мину М. Математическое программирование. Теория и алгоритмы. 1990. 488 с.
- 12 Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. 1982, 416 с.
- 13 Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. Алгоритмы и сложность. 1985. 512 с.
- 14 Jiang Y., Jiang Z. Robust Adaptive Dynamic Programming. 2017. 216 pp.

REFERENCES

- [1] Bluhm M. Software optimization of binary elliptic curves arithmetic using modern processor architectures. 2013. 210 pp. URL (date of reference: 11.06.2017): https://www.emsec.rub.de/media/attachments/files/2014/11/MA_Bluhm.pdf
- [2] Longa, P. Accelerating the scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields : for the degree of Master of Applied Science 2007. — 173 pp.
- [3] Gueron S., Krasnov V. Fast Prime Field Elliptic Curve Cryptography with 256 Bit Primes. 2014. 17 pp. URL (date of reference: 11.06.2017): <https://eprint.iacr.org/2013/816.pdf>
- [4] Bernstein D., Lange T. Analysis and optimization of elliptic-curve single-scalar multiplication. 2008. 19 pp. URL (date of reference: 11.06.2017): <http://www.hyperelliptic.org/EFD/precomp.pdf>
- [5] Feng M., Zhu B., Xu M., Li S. Efficient Comb Elliptic Curve Multiplication Methods Resistant to Power Analysis. 2005. 31 pp. URL (date of reference: 11.06.2017): <https://eprint.iacr.org/2005/222.pdf>
- [6] Cohen H., Miyaji A., Ono T. Efficient Elliptic Curve Exponentiation Using Mixed Coordinates. 2002. 14 pp.
- [7] Bolotov A. A., Gashkov C.Б., Frolov. A.Б An elementary introduction in elliptic cryptography: Protokoly kriptografii na ellipticheskikh krivykh. 2006. 280 pp. (in Russian).
- [8] Giorgia P., Imberta L., Izarda T. Optimizing Elliptic Curve Scalar Multiplication for small scalars. 2009. 10 pp.
- [9] Blake I. F., Seroussi G, Smart N. P. Elliptic Curves In Cryptography. 1999. 217 pp.
- [10] Hankeron D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. 2004. 331 pp.
- [11] Minoux M Mathematical programming: theory and algorithms. 1986. 489 p. (in Russian).
- [12] Garey. M, Johnson. D. Computers and Intractability. 1979. 338 pp. (in Russian).
- [13] Papadimitriou H., Steiglitz K. Combinatorial Optimization: Algorithms and Complexity. 1982. 496 pp. (in Russian).
- [14] Jiang Y., Jiang Z. Robust Adaptive Dynamic Programming. 2017. 216 pp.