ФГБОУ ВО «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ имени М.В. ЛОМОНОСОВА»

На правах рукописи

Николаев Максим Владимирович

О сложности решения некоторых обобщений задачи дискретного логарифмирования

05.13.19 - Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2018

Работа выполнена на кафедре информационной безопасности факультета Вычислительной математики и кибернетики ФГБОУ ВО «Московского государственного университета имени М.В. Ломоносова».

Научный руководитель: **Матюхин Дмитрий Викторович,** кандидат физико-математических наук

Официальные оппоненты: **Гашков Сергей Борисович,** доктор физико-математических наук, МГУ имени М.В. Ломоносова, механико-математический факультет, профессор

Михайлов Владимир Гаврилович, доктор физико-математических наук, Математический институт им. В.А. Стеклова РАН, ведущий научный сотрудник

Катышев Сергей Юрьевич, кандидат физико-математических наук, Московский технологический университет (МИРЭА), доцент

Защита диссертации состоится «06» июня 2018 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.05.01 Московского государственного университета имени М.В. Ломоносова по адресу: 119234, Москва, ГСП-1, Ленинские горы, д.1, главное здание МГУ, механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на сайте ИАС «ИСТИНА»: https://istina.msu.ru/dissertations/111698314/

Автореферат разослан «03» мая 2018 г.

Ученый секретарь диссертационного совета МГУ.05.01, кандидат физико-математических наук М.А. Кривчиков

Общая характеристика работы

Актуальность темы исследования. Задача дискретного логарифмирования является одной из важнейших в области информационной безопасности. Предположение о вычислительной трудности ее решения является обоснованием стойкости большинства используемых на практике механизмов защиты информации с открытым ключом, включая различные варианты схемы (протокола) выработки общего ключа Диффи-Хеллмана[1] и схем шифрования и электронной подписи Эль-Гамаля[2]. В ряде случаев задачу определения ключа указанных схем удается свести к одному из обобщений задачи дискретного логарифмирования, которые могут быть решены с меньшей трудоемкостью. В работе рассматриваются следующие из них.

- Задача дискретного логарифмирования в интервале.
  В данном случае известно, что решение лежит в наперед заданном интервале, размер которого заведомо меньше порядка исходной группы. Необходимость решения задачи в такой формулировке естественным образом возникает в задаче нахождения c-битной экспоненты[3][4][5], атаках, использующих информацию из побочных каналов утечки[6], и атаках по маленькой подгруппе[7],

[1] Diffie W., Hellman M. New directions in cryptography // Transactions on Information Theory. – 1976. – Vol. 22, no. 6. – P. 644–654

[2] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // Transactions on Information Theory. – 1985. – Vol. 31, no. 4

[3] Gennaro R. An improved pseudo-random generator based on discrete log // Lecture Notes in Computer Science. – 2000. – Vol. 1880. – P. 469–481.

[4] Patel S., Sundaram G. S. An efficient discrete log pseudo random generator // Advances in Cryptology – CRYPTO '98: 18th Annual International Cryptology Conference Santa Barbara, California, USA August 23–27, 1998 Proceedings / Ed. by H. Krawczyk. – Berlin, Heidelberg : Springer Berlin Heidelberg, 1998. – P. 304–317

[5] Oorschot P. C. van, Wiener M. J. On Diffie-Hellman key agreement with short exponents // Lecture Notes in Computer Science. – 1996. – Vol. 1070. – P. 332–343.

[6] Gopalakrishnan K., Theriault N., Yao C. Z. Solving discrete logarithms from partial knowledge of the key // Lecture Notes in Computer Science. – 2007. – Vol. 4859. – P. 224–263.

[7] Lim C. H., Lee P. J. A key recovery attack on discrete log-based schemes using a prime order subgroup // Lecture Notes in Computer Science. – 1997. – Vol. 1294. – P. 249–263

при расшифровании в схеме гомоморфного шифрования Бонэ-Го-Ниссима[8], подсчете числа точек эллиптических кривых[9], оценке трудоемкости решения сильной задачи Диффи-Хеллмана[10][11].

- Двумерная задача дискретного логарифмирования.
  В этом случае требуется найти два неизвестных параметра, принадлежащих наперед заданным интервалам. Задача в такой формулировке возникает, например, при подсчете количества элементов многообразия Якоби, анализе трудоемкости решения классической задачи дискретного логарифмирования в случае подгруппы простого порядка группы точек эллиптической кривой, обладающей эффективным автоморфизмом, который позволяет заменять вычисление кратной точки вычислением суммы кратных точек (метод Галланта-Ламберта-Ванстоуна)[12], анализе трудоемкости решения задачи дискретного логарифмирования для экспонент ограниченной высоты[13].

Таким образом, существует обширный список задач, трудоемкость решения которых может быть оценена с помощью трудоемкости решения указанных обобщений задачи дискретного логарифмирования. Однако до настоящего времени задача поиска наилучших методов их решения относительно слабо изучена, что наделяет проводимое исследование не только теоретической, но и существенной практической значимостью. Действительно, национальные и международные стандарты, определя-

[8] Boneh D., Goh E. J., Nissim K. Evaluating 2-DNF formulas on ciphertexts // Lecture Notes in Computer Science. – 2005. – Vol. 3378. – P. 325–341

[9] Gaudry P., Schost E. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm // Lecture Notes in Computer Science. – 2004. – Vol. 3076. – P. 208–222

[10] Cheon J. H. Security analysis of the strong Diffie-Hellman problem // Lecture Notes in Computer Science. – 2006. – Vol. 4004. – P. 1–11.

[11] Jao D., Yoshida K. Boneh-Boyen signatures and the strong Diffie-Hellman problem // Lecture Notes in Computer Science. – 2009. – Vol. 5671. – P. 1–16.

[12] Gallant R., Lambert R., Vanstone S. Faster point multiplication on elliptic curves with efficient endomorphisms // Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. – CRYPTO '01. – London, UK : Springer-Verlag, 2001. – P. 190–200

[13] Blackburn S. R., Scott S. The discrete logarithm problem for exponents of bounded height // LMS Journal of Computation and Mathematics. – 2014. – no. 17. – P. 148-156

ющие рекомендации по использованию параметров механизмов защиты информации, должны в полной мере учитывать последние результаты в данной области. Огромный интерес к этому вопросу подтверждает также растущее от года к году количество публикаций по исследуемой тематике.

Степень научной разработанности темы исследования. Двумерная задача дискретного логарифмирования в конечной группе G (без ограничения общности, с аддитивной записью операции) является обобщением классической задачи дискретного логарифмирования и заключается в поиске для заданных $P_1,\ P_2,\ Q \in G,\ 0 < N_1, N_2 < \sqrt{|G|}$ значений n_1, n_2 таких, что $Q = n_1P_1 + n_2P_2$, в предположении, что при условии $-N_1 \leq n_1 \leq N_1,\ -N_2 \leq n_2 \leq N_2$ эти значения существуют. В 2004 году Годри и Шост предложили алгоритм решения этой задачи, средняя трудоемкость которого при стандартных эвристических предположениях не превосходит $(c + o(1))\sqrt{N}$ групповых операций в G, где $c \approx 2.43, N = 4N_1N_2, o(1) \to 0$ при $N \to \infty$[14]. В 2009 году Гэлбрайт и Руправи усовершенствовали алгоритм Годри-Шоста, получив $c \approx 2.36$[15].

Как и в случае классической задачи, для ускорения поиска решения двумерной задачи можно использовать наличие у группы G автоморфизма, для которого орбита любого элемента группы вычисляется существенно быстрее групповой операции (такой автоморфизм называют эффективным). Например, группа точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов

1) всегда обладает эффективным автоморфизмом порядка 2 (операция взятия обратного элемента $\varphi(x, y) = (x, -y)$);

2) если $B = 0$ и $p \equiv 1 \bmod 4$ — эффективным автоморфизмом порядка 4: $\varphi(x, y) = (-x, \alpha y)$, где α — элемент порядка 4 по модулю p;

[14] Gaudry P., Schost E. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm // Lecture Notes in Computer Science. – 2004. – Vol. 3076. – P. 208–222

[15] Galbraith S. D., Ruprai R. S. An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems // Lecture Notes in Computer Science. – 2009. – Vol. 5921, no. 10-11. – P. 368–382

3) если $A = 0$ и $p \equiv 1 \bmod 3$ — эффективным автоморфизмом порядка 6: $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p.

В 2010 году Лиу показал, что в первом случае значение c в оценке трудоемкости алгоритма Годри-Шоста может быть снижено до 1.4503, а во втором при $P_2 = \varphi(P_1)$ и $N_1 = N_2$ — до 1.0255.

Задача дискретного логарифмирования в интервале заключается в поиске для заданной конечной группы G (с аддитивной записью операции), заданных $P, Q \in G, N < |G| - 1$ такого значения n (в предположении, что оно существует), что $Q = nP, 0 \leq n \leq N$. В 2010 году Гэлбрайт и Рупраи адаптировали алгоритм Годри-Шоста к решению указанной задачи для групп с эффективным инвертированием. Оценка средней трудоемкости решения задачи составила $(1.36 + o(1))\sqrt{N}$ групповых операций в G при $N \to \infty$.

Целью исследования является усовершенствование известных методов решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале для групп с эффективными автоморфизмами.

Основные задачи исследования.

- Разработать алгоритм решения двумерной задачи дискретного логарифмирования в подгруппе группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6. Оценить среднюю трудоемкость полученного алгоритма.

- Провести анализ возможности оптимизации наилучших известных методов решения двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами, а именно для подгрупп группы точек эллиптической кривой

$y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов в перечисленных ранее случаях 1), 2), 3).

- Провести анализ возможности оптимизации наилучших известных методов решения задачи дискретного логарифмирования в интервале для групп с эффективным инвертированием.

Научная новизна полученных результатов.

- Автором впервые предложена модификация алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6. Автором получена также оценка средней трудоемкости разработанного алгоритма, составляющая $(c+o(1))\sqrt{N}$ групповых операций, где $c \approx 0.9781$, что меньше, чем в случае эллиптической кривой общего вида.

- Автором разработаны модификации алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования и получены оценки средней трудоемкости:

  – для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов при $N_1 = N_2$ с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;

  – для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 4, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;

  – для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$

элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций.

С помощью разработанной программной реализации алгоритмов продемонстрирована также согласованность теоретических оценок средней трудоемкости с экспериментальными. Таким образом, получены наиболее эффективные в настоящее время алгоритмы решения указанных задач.

- Автором предложена модификация алгоритма Годри-Шоста для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, и получена оценка средней трудоемкости, составляющая $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций в G. Разработанный алгоритм в настоящее время является наиболее эффективным алгоритмом решения указанной задачи.

Теоретическая и практическая значимость работы. Получены наиболее эффективные (на момент написания работы) алгоритмы решения некоторых обобщений задачи дискретного логарифмирования. Работа имеет теоретический характер, однако полученные результаты могут применяться для обоснования стойкости конкретных реализаций математических методов защиты информации, что указывает на практическую значимость.

Методология и методы исследования. Проводимые исследования базируются на известных теоретических положениях алгебраической геометрии, дискретной математики, теории вероятностей, математического анализа, вычислительной математики. Достоверность полученных результатов обоснована строгими математическими доказательствами.

Положения, выносимые на защиту.

- Модификация алгоритма Годри-Шоста решения двумерной задачи

дискретного логарифмирования при $P_2 = \varphi(P_1)$ и $N_1 = N_2$ в случае эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов, где φ — эффективный автоморфизм порядка 6. Оценка средней трудоемкости нового алгоритма.

- Оптимальные (с точки зрения используемых параметров алгоритма Годри-Шоста) оценки средней трудоемкости решения двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами, а именно для подгрупп группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов в рассмотренных ранее случаях 1), 2), 3).

- Модификация алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, а также оценка средней трудоемкости нового алгоритма.

Апробация результатов. Результаты работы докладывались на семинарах, всероссийских и международных конференциях:

1) на XV международной научно-практической конференции «РусКрипто», 2013 год, с 27 по 30 марта, с.п. Смирновское, Солнечногорский район, Московская область;

2) на III симпозиуме «Современные тенденции в криптографии» (CTCrypt' 2014), 2014 год, с 5 по 6 июня, Москва;

3) на XVI международной научно-практической конференции «РусКрипто», 2014 год, с 25 по 28 марта, с.п. Смирновское, Солнечногорский район, Московская область;

4) на XIV всероссийской конференции «Сибирская научная школа-семинар с международным участием Компьютерная безопасность и криптография» (SIBECRYPT'15), 2015 год, с 7 по 12 сентября, Новосибирск;

5) на семинаре «Арифметические вопросы криптографии» под руководством д.ф.-м.н., проф. В.Н. Чубарикова (Механико-математический факультет Московского государственного университета имени М.В. Ломоносова, г. Москва), 2017 год.

Содержание работы

Первая глава является введением в проблематику дискретного логарифмирования и содержит обзор наиболее значимых в настоящее время результатов по теме исследования.

В параграфе 1 рассматривается классическая задача дискретного логарифмирования.

Определение 1. *Задача дискретного логарифмирования.*
Дано: группа $G = \langle P \rangle$, $Q \in G$.
Найти: $n \in \{0, \ldots, |G| - 1\}$ *такое, что* $Q = nP$.

Приводится оценка средней трудоемкости наиболее эффективного в общем случае метода ее решения — параллельного метода Полларда.

Параграф 2 содержит описание классического алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования.

Определение 2. *Двумерная задача дискретного логарифмирования.*
Дано: группа G; $P_1, P_2, Q \in G$, $N_1, N_2 \in \mathbb{N}$, $Q = n_1 P_1 + n_2 P_2$ *для некоторых (неизвестных)* $n_1 \in \{-N_1, \ldots, N_1\}$, $n_2 \in \{-N_2, \ldots, N_2\}$.
Найти: $n_1', n_2' \in \mathbb{Z}$ *такие, что* $Q = n_1' P_1 + n_2' P_2$.

В общем случае наиболее эффективным алгоритмом решения двумерной задачи дискретного логарифмирования является алгоритм Годри-Шоста[16]. Основная идея алгоритма может быть сформулирована следующим образом. Сначала выбираются так называемые «домашнее»

[16] Gaudry P., Schost E. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm // Lecture Notes in Computer Science. – 2004. – Vol. 3076. – P. 208–222

(tame) и «дикое» (wild) множества:

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

Затем параллельно вычисляются псевдослучайные последовательности

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \tag{1}$$

$$Q + z_j P_1 + w_j P_2, (n_1 + z_j, n_2 + w_j) \in W, j = 1, 2, \ldots \tag{2}$$

до тех пор, пока в них не найдутся два одинаковых элемента:

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \tag{3}$$

откуда находим $n'_1 = x_k - z_l, n'_2 = y_k - w_l$.

Пусть группа G — циклическая простого порядка и обладает эффективным автоморфизмом φ, действующим в группе G как умножение на $\lambda \in \{1, \ldots, |G| - 1\}$. Тогда можно ускорить алгоритм, если искать не совпадающие элементы последовательностей (1) и (2), а совпадающие классы эквивалентности этих элементов. Действительно, в этом случае вместо равенства (3) имеем равенство

$$\varphi^s(x_k P_1 + y_k P_2) = Q + z_l P_1 + w_l P_2, \tag{4}$$

для некоторого s, откуда

$$Q = (\lambda^s x_k - z_l) P_1 + (\lambda^s y_k - w_l) P_2,$$

т. е. $n'_1 = \lambda^s x_k - z_l, n'_2 = \lambda^s y_k - w_l$.

Далее приводится теорема Гэлбрайта-Холмса, используемая для оценки среднего количества шагов, выполняемых алгоритмом. Описываются основные идеи использования эффективных автоморфизмов для оптимизации алгоритма Годри-Шоста в случае решения двумерной задачи дискретного логарифимирвания. И, наконец, приводятся наилучшие известные оценки средней трудоемкости решения двумерной задачи дискретного логарифмирования в случае групп с эффективными автоморфизмами порядка 2 и 4.

В параграфе 3 рассматривается задача дискретного логарифмирования в интервале. Приводятся наилучшие известные оценки средней трудоемкости решения задачи дискретного логарифмирования в интервале в случае групп с эффективным инвертированием.

Параграф 4 содержит анализ возможности достижения теоретических оценок средней трудоемкости алгоритмов решения обобщений задачи дискретного логарифмирования на практике с учетом принятых допущений при их получении.

Во **второй главе** конструктивно доказывается возможность снижения трудоемкости решения двумерной задачи дискретного логарифмирования для класса эллиптических кривых, обладающих эффективным автоморфизмом порядка 6, а также приводится оценка средней трудоемкости соответствующего алгоритма, разработанного автором.

Теорема 1. *Пусть G — подгруппа простого порядка q группы точек эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$, $q^2 \nmid \#E$; φ — автоморфизм группы G, $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p; λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod q$ такой, что $\varphi(x, y) = \lambda(x, y)$. Тогда средняя трудоемкость решения двумерной задачи дискретного логарифмирования в группе G при $N_1 = N_2$, $P_2 = \varphi(P_1)$ и случайном равновероятном выборе (n_1, n_2) не превосходит $(0.97811 + o(1))\sqrt{N}$ групповых операций, где $N = 4N_1N_2, N \to \infty$.*

Третья глава посвящена исследованию возможностей оптимизации алгоритма Годри-Шоста для решения некоторых обобщений задачи дискретного логарифмирования.

В параграфе 1 рассматривается двумерная задача дискретного логарифмирования в конечных циклических группах с эффективным автоморфизмом. Для оптимизации алгоритма Годри-Шоста можно варьировать размеры «домашнего» и «дикого» множеств. В целях определения характера влияния размера и формы этих множеств на константу при главном члене в оценке средней трудоемкости рассматриваются случаи групп с эффективными автоморфизмами порядка 2, 4 и 6: в каждом

из них используются «дикие» и «домашние» множества, однако размер «дикого» множества варьируется. Приводятся описание разработанного автором программного средства и результаты выполненных с помощью этого средства расчетов константы при главном члене в оценке средней трудоемкости решения задачи алгоритмом Годри-Шоста для различных значений параметров алгоритма.

Далее приводится конструктивное доказательство существования оптимального (в смысле использования рассматриваемых параметров) алгоритма решения двумерной задачи дискретного логарифмирования в группе с эффективным автоморфизмом порядка 6.

Теорема 2. *Пусть G — подгруппа простого порядка q группы точек эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$, $q^2 \nmid \#E$; φ — автоморфизм группы G, $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p; λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod q$ такой, что $\varphi(x, y) = \lambda(x, y)$. Тогда для любого $\varepsilon > 0$ существует такой алгоритм решения двумерной задачи дискретного логарифмирования (см. определение 2) в группе G, что при $N_1 = N_2$, $P_2 = \varphi(P_1)$ и случайном равновероятном выборе (n_1, n_2), его средняя трудоемкость не превосходит $(1 + \varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций[17], где $N = 4N_1N_2, N \to \infty$.*

Демонстрируется, как полученный результат можно обобщить для случаев групп с эффективными автоморфизмами порядка 2 и 4. В параграфе сравнивается трудоемкость решения классической задачи дискретного логарифмирования модифицированным алгоритмом Полларда и разработанной автором модификацией алгоритма Годри-Шоста в случае сведения задачи к двумерной, анализируются условия, при которых такое сведение целесообразно.

В параграфе 2 результаты, полученные в первом параграфе, используются для конструктивного доказательства существования оптимальной (с точки зрения рассматриваемых параметров) модификации алго-

[17] запись O_ε означает, что константа, скрывающаяся под символом O, зависит от ε

ритма Годри-Шоста решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием.

Четвертая глава содержит описание и результаты численных экспериментов для вариантов алгоритма Годри-Шоста, изложенных в главе 3, а именно, алгоритмов решения двумерной задачи дискретного логарифмирования в конечных циклических группах с эффективными автоморфизмами (параграф 1), а также задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием (параграф 2). Выполнено сравнение теоретических и экспериментальных результатов, полученных реализациями алгоритма Годри-Шоста, для ряда эллиптических кривых, стандартизованных NIST, SECG и ECC Brainpool.

Заключение содержит краткий перечень полученных результатов, а также описание возможных перспектив дальнейшей разработки темы.

Заключение

В работе получены следующие результаты.

- Разработана модификация алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6. Оценка средней трудоемкости разработанного алгоритма составляет $(0.978 + o(1))\sqrt{N}$ групповых операций.

- Разработаны наиболее эффективные в настоящее время алгоритмы решения двумерной задачи дискретного логарифмирования, которые являются модификациями алгоритма Годри-Шоста:

  – для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$

элементов при $N_1 = N_2$ с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;

- для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 4, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;
- для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций.

- Разработана модификация алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, и получена оценка средней трудоемкости, составляющая $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций в G. Разработанный алгоритм в настоящее время является наиболее эффективным алгоритмом решения указанной задачи.

Благодарности

Автор выражает искреннюю благодарность своему научному руководителю кандидату физико-математических наук Матюхину Дмитрию Викторовичу за постановку задач, постоянное внимание к работе и ценные советы. Автор выражает признательность коллективу кафедры информационной безопасности факультета ВМК МГУ имени М.В. Ломоносова.

Публикации автора по теме исследования

Научные статьи, опубликованные в рецензируемых научных изданиях, определенных п.2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова

1. М. В. Николаев, Д. В. Матюхин. О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6. Дискретная математика, том 25 (2013), стр. 54–65.

2. М. В. Николаев. On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism. Математические вопросы криптографии, том 6 выпуск 2 (2015), стр. 45–57.

3. М. В. Николаев. О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием. Прикладная дискретная математика, №2 (2015), стр. 97–102.

Первая работа выполнена в соавторстве с научным руководителем. Д. В. Матюхину принадлежит постановка задачи; решение поставленной задачи полностью принадлежит М. В. Николаеву.