ОТЗЫВ официального оппонента
о диссертации на соискание учёной степени
кандидата физико-математических наук
Николаева Максима Владимировича
на тему: «О сложности решения некоторых
обобщений задачи дискретного логарифмирования»
по специальности 05.13.19 — «Методы и системы защиты
информации, информационная безопасность»

Диссертационная работа М. В. Николаева посвящена усовершенствованию и разработке методов оценивания трудоемкости дискретного логарифмирования на группах точек эллиптических кривых. Эти задачи привлекают внимание многих математиков в связи с их особой ролью при разработке методов шифрования с открытым ключом.

Двумерная задача дискретного логарифмирования в конечной группе является обобщением классической задачи дискретного логарифмирования и состоит в следующем. Для заданных элементов P_1, P_2, Q группы G и чисел N_i, $1 \leq N_i < \sqrt{|G|}$, $i = 1, 2$, требуется найти числа n_i, $-N_i \leq n_i \leq N_i$, $i = 1, 2$, что $Q = n_1 P_1 + n_2 P_2$ (при условии, что такие n_1, n_2 существуют).

Алгоритм решения этой задачи в 2004 году предложили П. Годри и Э. Шост. Трудоемкость этого алгоритма была оценена как $(c + o(1))\sqrt{N}$, где $N = 2N_1N_2$, $c \approx 2.43$, а $N \to \infty$ (в 2009 С. Д. Гэлбрайт и Р. С. Рупраи усовершенствовали этот алгоритм, получив $c \approx 2.36$). Как и в классической задаче, для ускорения поиска решения двумерной задачи можно использовать наличие у группы автоморфизма, для которого орбита любого элемента группы вычисляется существенно быстрее групповой операции (такой автоморфизм называют эффективным). Имеются три случая, когда группа точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p \geq 5$ элементов обладает эффективным автоморфизмом:

1) эллиптическая кривая $y^2 = x^3 + Ax + B$, $A, B \neq 0$ (эффективный автоморфизм порядка 2 — операция взятия обратного элемента);

2) эллиптическая кривая $y^2 = x^3 + Ax$, $A \neq 0$, $p \equiv 1 \mod 4$ (эффективный автоморфизм порядка 4);

3) эллиптическая кривая $y^2 = x^3 + B$, $B \neq 0, p \equiv 1 \mod 3$ (эффективный автоморфизм порядка 6).

В 2010 году В. Лиу показал, что в случае 1) величина коэффициента в главном члене асимптотической оценки трудоемкости алгоритма Годри-Шоста может быть снижена до 1.4503, а во втором случае (при некотором

дополнительном ограничении) — до 1.0255. Аналогичных результатов для случая 3) в этом исследовании получено не было.

Теперь о результатах диссертации. В диссертации автор, опираясь на разработанные ранее подходы, модифицирует несколькими способами алгоритм Годри–Шоста. Главной целью при этом является максимально возможное в рассматриваемых обстоятельствах снижение трудоемкости алгоритма. Важную роль в этих исследованиях играет разработанная автором методика рационального выбора параметров алгоритма Годри–Шоста.

В силу того, что для двумерной задачи дискретного логарифмирования ранее были получены модификации алгоритма Годри–Шоста лишь для эллиптических кривых, обладающих эффективными автоморфизмами порядков 2 и 4 (случаи 1) и 2)), естественно было начать с соответствующего исследования для подгрупп группы точек эллиптической кривой с автоморфизмом порядка 6 (случай 3)).

Этой задаче посвящена глава 2 диссертации. В ней построена модификация алгоритма Годри–Шоста для подгрупп простого порядка группы точек эллиптической кривой $y^2 = x^3 + B$, $B \neq 0$, над конечным простым полем из $p \equiv 1 \mod 3$ элементов, имеющей эффективный автоморфизм порядка 6. Удачно используя теоретико-вероятностные методы, автор предложил более простой (по сравнению с ранее использованными в литературе) способ вывода верхней оценки средней трудоемкости разработанного алгоритма. При $N_1 = N_2$ коэффициент в полученной оценке $c \approx 0.978$, что меньше, чем в упомянутых выше оценках. Результаты главы 2 существенно дополняют результаты В. Лиу и, некоторым образом, завершают определенный этап модифицирования алгоритма Годри–Шоста применительно к рассматриваемым задачам.

Принципиально новый шаг делается в главе 3, где предложены способы оптимизации алгоритма Годри–Шоста, использующего эффективный автоморфизм. Алгоритм Годри-Шоста и его различные модификации оперируют так называемыми «диким» и «домашним» множествами, из которых поочередно выбираются элементы до тех пор, пока не будут найдены совпадающие. Диссертантом предложена удачная параметризация «дикого» множества, связывающая его размер со значением оценки средней трудоемкости алгоритма. Используя эту связь и варьируя размер «дикого» множества, диссертант построил менее трудоемкие алгоритмы (являющиеся модификациями алгоритма Годри–Шоста) и обосновал оценки их средней трудоемкости при $N_1 = N_2$:

а) для подгрупп простого порядка группы точек эллиптической кривой $y^2 = x^3 + Ax + B$, $A, B \neq 0$, над конечным простым полем из $p \geq 5$ элементов

оценка имеет вид $(1+\varepsilon)\sqrt{\frac{\pi N}{2}}$ групповых операций (константа ε в оценке зависит от введенной диссертантом параметризации и может быть выбрана сколь угодно близкой к нулю: так при $\varepsilon \approx 0.01$ получаем $c \approx 1.266$);

б) для подгрупп простого порядка группы точек эллиптической кривой $y^2 = x^3 + Ax$, $A \neq 0$, над конечным простым полем из $p \equiv 1 \mod 4$ элементов при наличии эффективного автоморфизма порядка 4 оценка имеет вид $(1+\varepsilon)\sqrt{\frac{\pi N}{4}}$ групповых операций (при $\varepsilon \approx 0.01$ получаем $c \approx 0.895$);

в) для подгрупп простого порядка группы точек эллиптической кривой $y^2 = x^3 + B$, $B \neq 0$, над конечным простым полем из $p \equiv 1 \mod 3$ элементов при наличии эффективного автоморфизма порядка 6 (алгоритм отличается от алгоритма главы 2 параметризацией и имеет меньшую оценку средней трудоемкости) оценка имеет вид $(1+\varepsilon)\sqrt{\frac{\pi N}{4}}$ групповых операций (при $\varepsilon \approx 0.01$ получаем $c \approx 0.895$);

г) для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием.

В последнем случае оценка средней трудоемкости имеет вид $(1+\varepsilon)\sqrt{\frac{\pi N}{2}}$ групповых операций (при $\varepsilon \approx 0.01$ получаем $c \approx 1.266$).

Полученные автором оценки трудоемкости показывают, что построенные для перечисленных задач алгоритмы главы 3 являются наиболее эффективными среди известных в настоящее время.

Кроме этого, в диссертации (глава 4) приведены описание и результаты численных экспериментов для вариантов алгоритма Годри–Шоста, построенных в главе 3. Экспериментальные данные хорошо согласуются с главными членами полученных в главе 3 оценок трудоемкости.

Диссертация написана на высоком научном уровне и представляет собой законченную научно-квалификационную работу, все части которой объединены единым планом, кругом рассматриваемых задач и методикой исследования. Основные результаты диссертации являются новыми и строго обоснованными. Результаты диссертации своевременно опубликованы в изданиях, определенных п.2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Автореферат правильно отражает содержание диссертации.

В изложении материала имеются следующие недостатки.

В диссертации используется позаимствованное у зарубежных авторов неудачное определение «дикого» множества. В нем используется выражение, не согласующееся с традиционными математическими представлениями. Это в определенной степени затрудняет ознакомление с материалом.

Приведенное в разделе 1.1 описание свойств группы точек эллиптиче-

ской кривой недостаточно полно, в частности, в нем не указано такое основное свойство, как коммутативность группы. Не приведено никаких сведений о величине порядка группы.

Название раздела 1.4 «О достижимости теоретических оценок средней трудоемкости» дезориентирует читателя. На самом деле, основная часть раздела посвящена вопросу о том, почему в диссертации в качестве оценки трудоемкости взято число выполняемых алгоритмом групповых операций.

В теоремах 3–6 (глава 3 диссертации) оценки средней трудоемкости выписаны в форме, отличной от формы, приведенной в работах С.Д. Гэлбрайта, Р.С. Руправи. Поэтому автору надо было дополнить теоремы главы 3 наглядной демонстрацией преимущества построенных алгоритмов.

Формулировки теорем глав 2 и 3 полезно было сопроводить обсуждениями, в которых говорилось бы о том, насколько условия этих теорем совпадают с условиями аналогичных утверждений предшествующих авторов, какие именно подгруппы для каждой теоремы рассматриваются в четвертой главе диссертации и т. п.

В «Заключении» отмечены две модификации алгоритма Годри–Шоста решения двумерной задачи дискретного логарифмирования в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$, $B \neq 0$, без указания на то, чем они различаются.

В работе имеется некоторое количество опечаток. Одна из них содержится в формуле. А именно, на странице 72 в выносной формуле в строке 12 вместо неравенства должно стоять равенство.

Считаю, что в диссертации содержится решение актуальной задачи построения эффективного метода оценивания трудоемкости дискретного логарифмирования на эллиптических кривых. Результаты диссертации вносят важный вклад в это научное направление и имеют существенное значение для обоснования ряда современных математических методов защиты информации.

Все отмеченные выше недостатки не имеют принципиального характера, а сделанные замечания не умаляют значимости диссертационного исследования. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к работам подобного рода. Содержание диссертации соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова, а также оформлена согласно приложениям № 5, 6 Положения о диссертационном со-

вете Московского государственного университета имени М.В.Ломоносова.

Таким образом, соискатель Николаев Максим Владимирович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
доктор физико-математических наук,
ведущий научный сотрудник
отдела дискретной математики
ФГБУН «Математический институт им. В.А. Стеклова
Российской академии наук»
Михайлов Владимир Гаврилович

21 мая 2018 г.

Контактные данные:
тел.: 8(499)941-01-84, e-mail: mikhail@mi.ras.ru
Специальность, по которой официальным оппонентом
защищена диссертация:
01.01.09 – Дискретная математика и математическая кибернетика

Адрес места работы:
119991, г. Москва, ул. Губкина, д. 8
ФГБУН «Математический институт им. В.А. Стеклова
Российской академии наук»,
отдел дискретной математики
Тел.: +7(495)984-81-41; e-mail: steklov@mi.ras.ru

Подпись Михайлова Владимира Гавриловича заверяю.
Ученый секретарь МИ

Яськов Павел Андреев
ученый секретарь, старший научный сотрудник
Математический институт им. В.А. Стеклова
Российской академии наук,
ул. Губкина, д. 8, 119991, Москва, Россия