ОТЗЫВ официального оппонента
о диссертации на соискание ученой 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»
(физико-математические науки)

Предлагаемая к защите диссертация Николаева Максима Владимировича посвящена оптимизации известных методов решения некоторых обобщений задачи дискретного логарифмирования, а именно, задачи дискретного логарифмирования в интервале и двумерной задачи дискретного логарифмирования. Существует обширный список практических задач, трудоемкость которых может быть оценена с помощью оценок трудоемкости указанных обобщений.

В диссертации Николаева М.В. рассматривается известный подход к решению двумерной задачи дискретного логарифмирования, предложенный в 2009 году Гэлбрайтом и Руправи. Такой подход предполагает возможность ускорения поиска решений двумерной задачи дискретного логарифмирования методом Годри-Шоста за счет использования некоторого автоморфизма группы (такой автоморфизм называют эффективным), для которого орбита любого элемента группы вычисляется существенно быстрее групповой операции.

В 2010 году Лиу теоретически обосновал снижение значения средней трудоемкости решения двумерной задачи дискретного логарифмирования для эллиптических кривых с эффективными автоморфизмами порядка 2 и 4.

В том же году Гэлбрайту и Руправи удалось адаптировать рассматриваемый алгоритм Годри-Шоста для решения задачи дискретного логарифмирования в интервале на группе с эффективным инвертированием.

Целью диссертации Николаева М.В. является усовершенствование алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования и его модификации для решения задачи дискретного логарифмирования в интервале для групп с эффективными автоморфизмами.

Соискателю удалось распространить результаты Лиу на группы точек эллиптической кривой порядка 6 и конструктивно доказать существование оптимального (в смысле использования рассматриваемых параметров) алгоритма решения двумерной задачи дискретного логарифмирования в группе с эффективным автоморфизмом порядка 6. Продемонстрировано, как полученный результат можно обобщить для случая групп с эффективными автоморфизмами порядка 2 и 4. Разработанные алгоритмы являются в настоящее время наиболее эффективными алгоритмами решения двумерной задачи дискретного логарифмирования.

Проведено сравнение трудоемкости решения классической задачи дискретного логарифмирования методом Полларда и разработанной соискателем модификацией алгоритма Годри-Шоста в случае сведения задачи к двумерной. Найдены условия, при которых данное сведение целесообразно.

Также соискателем получено конструктивное доказательство существования оптимальной (с точки зрения используемых параметров) модификации алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале на группе с эффективным инвертированием.

Данная тематика исследований является актуальной как с практической, так и с теоретической точки зрения. Решаемые в диссертационном исследовании задачи естественным образом возникают:

– в атаках на алгоритмы открытого распределения ключей типа Диффи-Хеллмана, а именно атаках, использующих информацию из побочных каналов утечки, и атаках по маленькой подгруппе;

– при анализе трудоемкости решения классической задачи дискретного логарифмирования на группе точек эллиптической кривой, обладающей эффективным автоморфизмом;

– при подсчете числа элементов многообразия Якоби.

Отметим также, что в рассматриваемых постановках задач, алгоритмы, предложенные автором, работают на группах, размеры которых используются в настоящее время. Экспериментальные результаты в главе 4 получены на эллиптических кривых, стандартизованных NIST, SECG и ECC Brainpool.

Научная новизна полученных результатов, состоит в том, что автором предложены алгоритмы решения двумерной задачи логарифмирования и задачи дискретного логарифмирования в интервале, являющиеся на данный момент наиболее эффективными.

Автором на высоком уровне используются математические методы доказательств. Все полученные автором результаты снабжены корректными и полными доказательствами. Достоверность теоретических результатов также подтверждается проведением экспериментов на вычислительной технике.

Результаты диссертации регулярно докладывались соискателем на всероссийских и международных конференциях в области криптографии и информационной безопасности. Основные результаты с достаточной полнотой опубликованы в 3 печатных работах в рецензируемых научных изданиях, определенных в п. 2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

В качестве замечаний к диссертации и автореферату можно отметить следующее:

– при формулировке основных результатов и научной новизны в автореферате (стр. 5, 11, 13) возникает константа ε, не определенная по тексту;

– в предлагаемых автором модификациях алгоритма Годри-Шоста для хранения вычисленных элементов используется память, однако оценок на ее необходимое количество в работе не приведено;

– в оригинальной работе Лиу для решения двумерной задачи дискретного логарифмирования рассматриваются различные значения «сжатия» домашнего множества и «растяжения» дикого множества, при этом соискатель в главах 3 и 4 меняет лишь размер дикого множества, никак не комментируя фиксацию размера домашнего множества;

– лежащий в основе алгоритмов решения двумерной задачи дискретного логарифмирования алгоритм Полларда допускает эффективное распараллеливание, вопрос о возможности распараллеливания предложенных в диссертации алгоритмов остался не освещенным.

Вместе с тем, указанные замечания не влияют на общую положительную оценку диссертации оппонентом. 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. Диссертация оформлена в соответствии с приложениями №5, 6 Положения о диссертационном совете Московского государственного университета имени М.В. Ломоносова.

На основании вышеизложенного делается вывод о том, что автор диссертации Николаев Максим Владимирович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент:
кандидат физико-математических наук,
доцент базовой кафедры №252,
ФГБОУ ВО «МИРЭА – Российский технологический университет»

Катышев Сергей Юрьевич
20.05.2018

Контактные данные:
Тел.: +7 (926) 393 77 30
Специальность, по которой официальным оппонентом защищена диссертация: 20.03.04 – «Теоретическая криптография»
Адрес места работы:
119454 г. Москва, проспект Вернадского, дом 78,
МИРЭА – Российский технологический университет
базовая кафедра 252,
Тел.: +7 499 215-65-65 доб. 1140; e-mail: mirea@

Подпись Катышева С.Ю. заверяю. Начальник Управления кадр о Л.Г.