Отзыв об автореферате диссертации

Николаева Максима Владимировича

«О сложности решения некоторых обобщений задачи дискретного логарифмирования»,
представленной на соискание учёной степени
кандидата физико-математических наук по специальности
05.13.19 – методы и системы защиты информации, информационная безопасность

В диссертации М. В. Николаева предложено несколько алгоритмов решения двумерной задачи дискретного логарифмирования в группе точек эллиптической кривой в предположении о наличии в группе эффективных автоморфизмов малого порядка. Кроме того, для конечных групп с быстрым инвертированием предложен новый алгоритм вычисления дискретного логарифма в заданном интервале. Согласно эвристическим оценкам средней сложности, эти алгоритмы существенно превосходят ранее известные. Этот вывод подтверждается и результатами вычислительных экспериментов.

Поиск быстрых алгоритмов дискретного логарифмирования, особенно в эллиптической криптографии – сверхактуальная задача современной прикладной математики, на решении которой сконцентрированы усилия большого числа специалистов, практиков и теоретиков, во всём мире. Получение новых результатов в этом направлении, тем более, алгоритмов с рекордными характеристиками эффективности – значительное достижение.

Поэтому представленные в диссертации результаты производят благоприятное впечатление. Автореферат содержит необходимые для квалификации работы сведения. Однако, к содержанию автореферата имеются два замечания.

1) Вместо термина сложность автор всюду использует сленговый термин «трудоёмкость». Хотя этот термин популярен в определённых кругах, с позиций русского языка и системы понятий, принятой в математике, его употребление в значении сложности неграмотно, поэтому в теоретических работах должно быть исключено. В значительной мере, указанное замечание адресовано и научному руководителю соискателя.

2) В перечне результатов автора присутствуют два внешне идентичных по формулировкам и отличающихся только оценками сложности. Имеются в виду алгоритмы дискретного логарифмирования для групп с автоморфизмами

порядка 6. То ли это разные алгоритмы (тогда какой из них лучше?), то ли это один и тот же алгоритм соответственно с менее удачным и более удачным выбором параметров, в автореферате никак не поясняется. Смысл дублирования результатов остался непонятным.

Перечисленные обстоятельства несколько снижают в остальном положительное впечатление от работы, но не отменяют значимость основных результатов.

В целом, в части, относящейся к данным, представленным в автореферате, работа удовлетворяет требованиям, предъявляемым к кандидатским диссертациям. Рекомендую присудить её автору М. В. Николаеву учёную степень кандидата физико-математических наук по специальности 05.13.19.

22.05.2018 к.ф.-м.н. И.С. Сергеев

Подпись Сергеева Игоря Сергеевича заве
Заместитель начальника отдела кадров
ФГУП «НИИ «Квант» Г.Н. Грибанова