Отчет о научной деятельности за 2014 г.

Алексеенко Екатерины Сергеевны, старшего преподавателя кафедры "Компьютерной безопасности"Института Прикладной математики и информационных технологий Балтийского Федерального университета им. И.Канта.

1. Результаты, полученные в этом году

Мною был предложен и обоснован метод для вывода уравнений оптимальной кривой рода четыре над расширением простого поля с помощью двойных накрытий рода два эллиптической кривой.

В работе я рассматриваю абсолютно неприводимые, проективные, гладкие кривые над конечным полем $\mathbb{F}_q$.

Рассмотрим H – двойное накрытие эллиптической кривой E рода два, заданное уравнением

$$z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta y.$$

Пусть P_1 и P_2 – точки кривой E, над которыми разветвляется H. В работе показано, что любое двойное накрытие H рода два имеет вид

$$z^2 = f, \text{ где } \operatorname{div}(f) = P_1 + P_2 - 2R,$$

где R – рациональная точка кривой E, а также в работе установлено следующее соответствие

$$\{\text{двойные накрытия } E \text{ рода } 2\} \longleftrightarrow \{\{P, -P\} \notin E[2]\}.$$

Если $H \to E$ соответствует $\{P, -P\}$, то с точностью до изоморфизма на кривой двойное накрытие H задано уравнением $z^2 = f$, $\operatorname{div}(f) = (R + P) + (R - P) - 2R$ для некоторой точки R.

Для двойных накрытий H_1, H_2 и H_3 эллиптической кривой E доказано соотношение $2(P_1 + P_2 + P_3) = \mathcal{O}$.

При рассмотрении эллиптической кривой E с дискриминантом $d(E) = -19$ с точностью до знака получены следующие важные условия

$$6P_1 = \mathcal{O},$$

$$6P_2 = \mathcal{O},$$

$$4P_1 + 2P_2 = \mathcal{O},$$

$$2P_1 + 4P_2 = \mathcal{O}.$$

Рассматривая кривые E и H в поле характеристики 0, можно заметить, когда эти уравнения выполняются по модулю p, и получить конечный список характеристик для дальнейшего рассмотрения.

В качестве примера рассмотрим над полем $\mathbb{F}_5$ эллиптическую кривую $E : y^2 = x^3 + 2x + 4$ и два накрытия $w^2 = x$, $z^2 = y + x^2 + +2x + 3$.

При этом многочлен Вейля композита кривых рода 4 равен $(T^2 + T + 5)^5$, а характеристический многочлен над $\mathbb{F}_{5^7}$ имеет вид $(T^2-559T+78125)^4$, и его дискриминант равен -19. Таким образом, кривая, заданная уравнением

$$z^4 + 3z^2w^4 + z^2w^2 + 4z^2 + w^8 + 3w^6 = 0,$$

является оптимальной кривой рода 4 над конечным полем с дискриминантом, равным -19.

По итогам работы, проделанной за прошедшие два года, мною была написана кандидатская диссертация. К сожалению, в связи с отменой внешнего соискательства защита диссертации (ориентировочно намеченной на конец этого года) переносится на неопределенный срок. Несмотря на это, работа над диссертацией полностью закончена.

В настоящее время я занимаюсь вопросом приложений гипербентных функций к кривым над конечными полями, а именно, вопросом применения критерия Чарпина-Гонга к числу $\mathbb{F}_{2^n}$- рациональных точек некоторых гиперэллитпических кривых.

2. Опубликованные и поданные в печать работы

1. E. Alekseenko and A. Zaytsev. «Explicit equations of optimal curves of genus 3 over certain finite fields with three parametrs». – In proceedings of AGCT-14.

2. E. Alekseenko. «A method of finding explicit equation for optimal curve of genus 4». – In proceedings of the 14th international workshop on Algebraic and Combinatorial Coding Theory. – 14–17, 2014.

3. Участие в конференциях и школах

1. XIV International Workshop on «Algebraic and Combinatorial Coding Theory». Место проведения: Россия, г. Светлогорск. Сроки: 7-13 сентября 2014 г.

2. Пятая международная конференция «Дзета-функции». Место проведения: Россия, г. Москва, НМУ, Лаборатория Понселе. Сроки: 1-5 декабря 2014 г.

4. Работа в научных центрах и международных группах

Являюсь младшим научным сотрудником лаборатории “Математические методы защиты и обработки информации” в инновационном парке БФУ им. И. Канта.

5. Педагогическая деятельность (включая научное руководство)

1. Являюсь участником семинара "Алгебраическая геометрия и ее приложения"на базе лаборатории "Математические методы защиты и обработки информации".

2. Преподаю на кафедре "Компьютерной безопасности"следующие дисциплины:

- "Прикладная алгебра";
- "Быстрые мультипликаторы";
- "Введение в алгебраическую теорию чисел и криптографию в квадратичных полях";
- "Методы вычисления дискретного логарифма";
- "Методы и алгоритмы генерации эллиптических кривых для криптографии".