**Николаев, Максим Владимирович О сложности решения некоторых обобщений задачи дискретного логарифмирования**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Николаев, Максим Владимирович

трудоемкости ....................................... 41

2.3 Выводы.............................................. 54

3 О сложности решения двумерной задачи дискретного ло-

гарифмирования и задачи дискретного логарифмирования в интервале 55

2

3.1 О сложности решения двумерной задачи дискретного ло-

гарифмирования в конечной циклической группе с эффективным автоморфизмом ............................ 56

3.1.1 Оценка средней трудоемкости для некоторых значений параметров алгоритма ................. 57

3.1.2 Алгоритм и оценка средней трудоемкости..... 59

3.1.3 Двумерная и классическая задачи дискретного логарифмирования ............................. 70

3.2 О сложности решения задачи дискретного логарифмирова-

ния в интервале в группе с эффективным инвертированием 73

3.3 Выводв1.......................................... 79

4 Численный эксперимент 82

4.1 Общая методика проведения численных экспериментов . . 83

4.2 Двумерная задача в конечных циклических группах с эффективным автоморфизмом порядка 2 ............... 85

4.3 Двумерная задача в конечных циклических группах с эффективным автоморфизмом порядка 4 ............... 90

4.4 Двумерная задача в конечных циклических группах с эффективным автоморфизмом порядка 6 ............... 94

4.5 Задача дискретного логарифмирования в интервале .... 100

4.6 Выводы...........................................104

Заключение 106

Список сокращений и обозначений 108

A Оценка средней трудоемкости для некоторых значений параметров алгоритма Годри-Шоста 109

B Программная реализация алгоритма Годри-Шоста 113

Список литературы 121

3