РЕФЕРАТ

Дипломну роботу виконано на 56 аркушах, вона містить 2 додатки та перелік посилань на використані джерела з 29 найменувань. У роботі наведено 6 рисунків та 3 таблиці.

Метою даної дипломної роботи є виконання алгоритмів дискретного логарифмування для мультиплікативних груп простих полів $GF(p)$ у хмарній моделі обчислень та оцінка дійсного розміру проблеми, яку можливо розв'язати з їх використанням за певний період часу та матеріальних витрат на цей розв'язок.

Об'єктом дослідження є проблема дискретного логарифму у скінченних полях виду $GF(p)$.

Предметом дослідження є процес виконання конкретних алгоритмів дискретного логарифмування у заданих полях на хмарних платформах.

Проведено аналіз існуючих рішень проблеми дискретного логарифму, виконано їх порівняння з погляду швидкодії та легкості реалізації для паралельної моделі. Також проведено огляд існуючих систем хмарних обчислень та обрано ту, що дозволяє точніший контроль за загальною обчислювальною потужністю системи вузлів, з меншою ціною за рівних інших показниках.

Був реалізований обраний алгоритм у паралельній моделі та проведено його виконання на обраній платформі. З результатів виконання зроблено аналіз оптимальних параметрів алгоритму та орієнтовного розміру модуля, розв'язок проблеми дискретного логарифму для якого можна отримати за календарний рік.

Результати роботи можуть бути використані для оцінки вартості атаки на популярні асиметричні криптосистеми.

ДИСКРЕТНИЙ ЛОГАРИФМ, INDEX-CALCULUS, ПАРАЛЕЛЬНІ ОБЧИСЛЕННЯ, ХМАРНІ СИСТЕМИ

РЕФЕРАТ

Дипломная работа выполнена на 56 листах, она содержит 2 приложения и список ссылок на использованные источники с 29 наименований. В работе приведены 6 рисунков и 3 таблицы.

Целью данной дипломной работы является выполнение алгоритмов дискретного логарифмирования для мультипликативных групп простых полей $GF(p)$ в облачной модели вычислений и оценка действительного размера проблемы, которую можно решить с их использованием за определенный период времени и материальных затрат на это решение.

Объектом исследования является проблема дискретного логарифма в конечных полях вида $GF(p)$.

Предметом исследования является процесс выполнения конкретных алгоритмов дискретного логарифмирования в заданных полях на облачных платформах.

Проведен анализ существующих решений проблемы дискретного логарифма, выполнено их сравнение с точки зрения быстродействия и легкости реализации для параллельной модели. Также проведен осмотр существующих систем облачных вычислений и избран ту, что позволяет точнее контроль за общей вычислительной мощностью системы узлов, с меньшей ценой за равных других показателях.

Был реализован выбранный алгоритм в параллельной модели и проведено его выполнения на избранной платформе. С результатов выполнения сделано анализ оптимальных параметров алгоритма и ориентировочно размера модуля, решение проблемы дискретного логарифма для которого можно получить за календарный год.

Результаты работы могут быть использованы для оценки стоимости атаки на популярные асимметричные криптосистемы.

ДИСКРЕТНЫЙ ЛОГАРИФМ, INDEX-CALCULUS, ПАРАЛЛЕЛЬНЫЕ ВЫЧИСЛЕНИЯ, ОБЛАЧНЫЕ СИСТЕМЫ

ABSTRACT

The thesis is presented in 56 pages. It contains 2 appendixes and bibliography of 29 references. Six figures and 3 tables are given in the thesis.

The goal of the thesis is to implement algorithms of discrete logarithm for multiplicative groups of fields of the form $GF(p)$ in the cloud computational model and to estimate the actual problem size which is possible to solve during some predefined period of time and to estimate the costs for such solution.

The object is discrete logarithm problem in the finite fields of the form $GF(p)$.

The subject is the process of some discrete logarithm algorithms execution on cloud platforms.

In the thesis, existing solutions to the discrete logarithm problem are analyzed. They are compared in terms of performance and ease of use in parallel computational models. Also existing cloud systems are analyzed and the one is chosen based on more granular control over the whole computational power with other things equal.

The selected algoritm is implemented in parallel computation model and is executed on the selected platform. From the results of this execution analysis of optimal algorithm parameters and approximate problem size solvable in the span of one calendar year were made.

The results could be used for estimating attack cost on popular asymmetric cryptosystems.

DISCRETE LOGARITHM, INDEX-CALCULUS, PARALLEL COMPUTATION, CLOUD SYSTEMS