МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

МОРОЗ

Екатерина Александровна

Методы разделения секрета

Дипломная работа

Научный руководитель:

доктор физ.-мат. наук,
профессор В.В. Беняш-Кривец

Допущена к защите

«26» мая 2017 г.

Зав. кафедрой высшей алгебры и защиты информации

доктор физ.-мат. наук, профессор В.В. Беняш-Кривец

Минск, 2017

Аннотация

Дипломная работа содержит 43страницы и 5 литературных источников.

Ключевые слова: *схемы разделения секрета (СРС), схема Шамира, схема Блейкли, частичный секрет, схема Миньотта, пороговые схемы, схема Асмута-Блума, модулярная схема разделения секрета, кольцо многочленов от нескольких переменных, структура доступа, структура отказа.*

Цель работы заключается в изучении различных схем разделения секрета.

Первая глава посвящена общей постановке задачи разделения секрета и наиболее известным схемам его разделения.

В первом параграфе данаобщая постановка задачи и критерии качества схем разделения секрета.

Во втором параграфе представлены схема Шамира, линейное разделение секрета и модулярный подход.

В третьем параграфе рассмотренырпороговые схемы над кольцом многочленов и генерация модулей для пороговых схем в кольце целых чисел.

В четвертом параграфе описываютсясовершенные модулярные схемы и модулярная реализация произвольных структур доступа.

Вторая глава посвящена схемам разделения секрета в кольцах от нескольких переменных.

В первом параграфе рассматривается разделение секрета в кольце многочленов о нескольких переменных и реализации произвольных структур доступа.

Во втором параграфе представлены максимальные идеалы одинаковых степеней, нульмерные радикальные идеалы и идеальные схемы в кольце многочленов от нескольких переменных.

Анатацыя

Дыпломнаяпрацазмяшчае 43старонкі і 5 літаратурныхкрыніц.

Ключавыясловы: схемы падзелусакрэту (СРС), схема Шаміра, схема Блейкли, частковысакрэт, схема Миньотта, парогавыя схемы, схема Асмута-Блюма, мадулярная схема падзелусакрэту, кольца мнагачлена ад некалькіхзменных, структура доступу, структура адмовы.

Мэта работы заключаецца ў вывучэнні розных схем падзелусакрэту.

Першаячасткапрысвечанаагульнайпастаноўцызадачыпадзелусакрэту і найбольшвядомым схемах ягопадзелу.

У першымпараграфедадзенаагульнаяпастаноўказадачы і крытэрыіякасці схем падзелусакрэту.

Удругім параграфе прадстаўлены схема Шаміра, лінейнаепадзелсакрэту і модулярный падыход.

У трэцімпараграферазгледжаныпарогавыя схемы над кальцоммнагачлена і генерацыямодуляў для парогавых схем у кольцыцэлыхлікаў.

У чацвёртымпараграфеапісваюццадасканалыямадулярнае схемы і мадулярнаерэалізацыяадвольных структур доступу.

Другаячасткапрысвечана схемах падзелусакрэту ў кольцах ад некалькіхзменных.

У першымпараграферазглядаеццападзелсакрэту ў коле мнагачленаабнекалькіхзменных і рэалізацыіадвольных структур доступу.

У другімпараграфепрадстаўленымаксімальныяідэалыаднолькавыхступеняў, нульмерныерадыкальныяідэалы і ідэальныя схемы ў коле мнагачлена ад некалькіхзменных.

Abstract

The thesis contains 43 pages and 5 literary sources.

Key words: Secret division scheme, Shamir scheme, Blakely scheme, partial secret, Minott scheme, threshold schemes, Asmut-Bloom scheme, modular secret sharing scheme, polynomial ring of several variables, access structure, fault structure.

The aim of the work is to study various schemes of secretion.

The first chapter is devoted to a general formulation of the problem of separation of secret and the most well-known schemes for its separation.

In the first section we give a general statement of the problem and the criteria for the quality of the secret separation schemes.

In the second section Shamir's scheme is presented, the linear separation of the secret and the modular approach.

In the third section we consider threshold schemes over the ring of polynomials and generation of modules for threshold schemes in the ring of integers.

In the fourth section, we describe perfect modular schemes and the modular realization of arbitrary access structures.

The second chapter is devoted to schemes for separating secret in rings from several variables.

In the first section we consider the separation of a secret in the polynomial ring of several variables and the realization of arbitrary access structures.

In the second section we present maximal ideals of the same degree, zero-dimensional radical ideals and ideal schemes in the ring of polynomials in several variables.