**Абу Усбах Олексій Нідалійович. Методи синтезу та спосіб обчислення булевих функцій спеціального класу для засобів захисту інформації: дис... канд. техн. наук: 05.13.21 / НАН України; Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова. - К., 2004**

|  |  |
| --- | --- |
| |  | | --- | | **Абу Усбах Олексій Нідалійович.** Методи синтезу та спосіб обчислення булевих функцій спеціального класу для засобів захисту інформації. – Рукопис.  Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України, Київ, 2004.  Дисертація присвячена дослідженню шляхів підвищення ефективності засобів захисту даних за рахунок використання булевих функціональних перетворень, основаних на функціях спеціального класу.  Запропоновано новий клас булевих функцій, який характеризується інваріантністю до лінійних перетворень та має властивості важливі для його використання в булевих функціональних перетвореннях засобів захисту даних.  Запропоновано новий метод синтезу нелінійних балансних булевих функцій, що задовольняють критерію чіткого лавинного ефекту, а також каскадний метод побудови булевих функціональних перетворень на основі таких функцій.  Запропоновано новий таблично-паралельний спосіб обчислення булевих функціональних перетворень для блокових засобів захисту інформації. Спосіб має лінійну обчислювальну складність і дозволяє підвищити ефективність засобів захисту даних шляхом використання в них перетворень великої розрядності.  Ключові слова: булеві функції, булеві функціональні перетворення, чіткий лавинний ефект, нелінійність, захист інформації, блокові засоби захисту інформації. | |
| |  | | --- | | В дисертаційній роботі здійснено теоретичне обґрунтування і отримано нове вирішення наукових задач синтезу і організації обчислення булевих функцій спеціального класу та перетворень на їх основі для блокових засобів захисту інформації. Результати проведеного дослідження дозволяють підвищити ефективність проектування нових і модифікації існуючих засобів захисту інформації.  *Основні наукові і практичні результати полягають у наступному:*   1. Проведено аналіз існуючих підходів до побудови булевих функціональних перетворень для засобів захисту інформації. Показані технологічні обмеження відомих методів, які зумовлені експоненціальною складністю використаних в них операцій. 2. Для підвищення ефективності булевих функціональних перетворень було запропоновано використовувати класи булевих функцій, які інваріантні до лінійних перетворень та мають певні властивості, важливі для їх застосування у засобах захисту інформації. Основним ефектом такого застосування є стабільність характеристик будь-яких лінійних комбінацій функцій, що складають перетворення. Додатковим ефектом використання функцій детермінованого класу, що мають однакову структуру є можливість ефективної організації їх обчислення за рахунок уніфікації операцій. 3. Виділено замкнений відносно лінійних операцій клас булевих функцій, чіткий лавинний ефект котрих досягається шляхом кон’юнктивної суперпозиції елементів лінійного базису. Доведено, що на основі булевих функцій виділеного класу можливо будувати ортогональні системи, що мають якісні лінійні та диференційні профілі. 4. Запропоновано формалізований метод синтезу нелінійних булевих функцій виділеного класу. Реалізація методу має лінійну обчислювальну складність, що підвищує ефективність процесів проектування булевих функціональних перетворень для блокових засобів захисту інформації. 5. Запропоновано каскадний метод побудови бієктивних функціональних перетворень на основі ортогональних систем булевих функцій виділеного класу. Синтезовані запропонованим методом перетворення характеризуються стійкістю до лінійного та диференційного аналізу. На відміну від відомих, запропонований метод дозволяє гнучко змінювати нелінійність синтезованих перетворень та обчислювальну складність їх реалізації шляхом варіювання кількості каскадів. 6. Розроблено таблично-паралельний спосіб організації обчислення функціональних перетворень, що базуються на булевих функціях виділеного класу. Цей спосіб забезпечує лінійну складність обчислення таких перетворень. 7. Запропоновані методи синтезу та спосіб організації обчислення булевих функціональних перетворень доведені до рівня готових до використання програмних модулів, що пройшли апробацію в ході експериментальних досліджень. | |