ЗАСТОСУВАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ ДЛЯ РОЗВ'ЯЗУВАННЯ ЗАДАЧ КРИПТОАНАЛІЗУ

Володимир Самотий[1], Уляна Дзелендзяк[1,2]

1. Львівський державний університет безпеки життєдіяльності, Львів, Україна
2. Національний університет"Львівська політехніка", Львів, Україна

Описано роботу генетичного алгоритму та наведено основні його компоненти. Обгрунтовано доцільність застосування генетичних алгоритмів для задач криптографічного аналізу симетричних алгоритмів шифрування.

Вступ. На сучасному етапі розвитку комп'ютерних технологій, що забезпечують інформаційну безпеку та захист інформації, широке застосування знаходять криптографічні методи захисту, які відносяться до *NP*-повних задач. Для їх розв'язування, сьогодні застосовують алгоритми, основані на законах природних систем. До таких алгоритмів відносяться, зокрема, генетичні алгоритми (ГА).

Основні компоненти генетичного алгоритму. У процесі розв'язування задачі генетичний алгоритм поводиться так само, як поводилися б живі організми у процесі еволюції. Потенційний розв'язок подається як певна структура-особина. Кожна особина однозначно характеризується набором хромосом, яка є унікальною характеристикою, що дозволяє врахувати властивості конкретної особини в процесі еволюції. Множина хромосом об'єднуємо в популяцію, з якою алгоритм виконує певні бінарні операції. У поняття операції входять рекомбінація, селекція і мутація особин. Суть рекомбінації полягає у створенні хромосом нових особин з хромосом батьківських особин у вже існуючій популяції. Найбільш популярним методом рекомбінації є крос-овер (cross-over), який розбиває хромосоми батьків (їх число не обов'язково дорівнює двом) на деяку кількість рівних частин. З них потім складаються хромосоми нащадків. Мутація особини – це випадкова зміна хромосом особин популяції.

Метою мутації є необхідність захистити алгоритм від розвитку в тупикові гілки еволюції, постійно вносити певний несуттєвий елемент невизначеності. Ймовірність мутації для цього повинна бути достатньо малою, щоб не допустити випадкової зміни всього генофонду. Пристосованість оцінюється кількісно за допомогою певного числового показника. Функцію, що визначає, наскільки пристосована та чи інша особина, називають цільовою функцією (fitness function), або функцією мети. Селекція описує спосіб заповнення даних про популяцію чергового покоління з великого числа батьків. Селекція виконується у віповідності до певної оцінки і її граничного значення для кожної хромосоми.

Треба відзначити, що в генетичних алгоритмах чисельність популяції зазвичай зберігається рівною наперед визначеній константі. Це дає можливість відбирати щоразу кращі особини і водночас не призводить до відхилень еволюції і тупикових гілок розвитку.

Весь генетичний алгоритм складається з таких компонент:

- подання хромосом;
- початкова популяція (стартовий набір хромосом);
- набір операторів для генерації нових рішень з попередньої популяції;
- цільова функція для оцінки пристосованості рішень;
- алгоритм оцінки пристосованості хромосом.

Реалізація криптоаналізу симетричних алгоритмів шифрування на основі ГА. Розглянемо задачу криптоаналізу симетричних алгоритмів шифрування. В [1-3] описана задача криптоаналізу і наведені результати криптоаналізу класичних криптографічних алгоритмів з використанням методів еволюційної оптимізації і генетичного пошуку для симетричних шифрів перестановок. Відомі наступні шифри перестановок: прості таблиці шифрування; таблиці шифрування з одиночною перестановкою по ключу; таблиці шифрування з подвійною перестановкою по ключу; магічні квадрати. методи шифрування за допомогою простих таблиць шифрування одиночної перестановки за ключем, двійної перестановки [1, 4].

При використанні таблиць шифрування ключем є перестановка (p_1, p_2, …, p_n), тому хромосома в ГА повинна також задавати перестановку. Основне питання при цьому – як подати окремі гени особини. У найпростішому випадку шифрування здійснюється шляхом присвоєння окремим генам відповідних елементів ключа, тобто і-м геном хромосоми P вважати елемент p_i. Незважаючи на недоліки такого підходу, відзначені в [5], (наприклад, гени виходять залежними один від одного, що приводить до можливості отримання нелегальних рішень), таке визначення генів є інтуїтивно зрозумілим і не вимагає додаткових затрат на їх формування (обчислення).

Альтернативним підходом є використання певного проміжного подання, при якому набір генів задає певне правило або об'єкт, за допомогою якого формується ключ [1, 5]. При цьому основною задачею є знаходження проміжного розв'язку, що задається у вигляді бітового рядка для застосування стандартних генетичних операторів. При реалізації ГА криптографічного аналізу використовувався перший підхід, тобто в якості генів особини розглядаються елементи ключа. Для запобігання отримання нелегальних розв'язків при десятковому кодуванні хромосом використовується правило: при появі в хромосомі однакових генів другий повторюваний ген замінюється на відсутній. В якості функції пристосованості особин використовується факт збігу відкритого тексту і шифротексту при реалізації криптографічного аналізу другого типу для визначення секретного ключа. В [5, 7] в якості цільової функції пропонується використовувати функцію Якобсена про розподіл частот у відкритих текстах. В [1-3] наведені результати експерименту при реалізації криптографічного аналізу другого типу при бінарному і десятковому кодуванні хромосом методом одиночної і подвійної перестановки по ключу, а також простої перестановки, в якому ключем служить розмір таблиці. Отримані результати свідчать про можливість застосування еволюційних методів для криптографічного аналізу шифрів, що використовують таблиці шифрування для перестановок стовпцями і стрічками.

Поряд з використанням таблиць шифрування, широке поширення для шифрування отримали шифри маршрутної перестановки. В [1, 6] розглядаються методи шифрування перестановками, що використовують магічні квадрати. Наводиться ГА їх побудови і результати експерименту, які свідчать про можливість застосування ГА для вирішення задач криптографічного аналізу даних шифрів перестановки при розробці систем забезпечення інформаційної безпеки і захисту інформації. Відзначається, що суттєвим відмінним моментом являється наявність випадкового пошуку, що дозволяє отримувати нові результати при кожній реалізації ГА.

В [1, 6, 8] розглядається застосування даних підходів для реалізації шифрів простої і багатоалфавітної заміни. Суть методів простої заміни зводиться до заміни символів шифрованого тексту символами того ж або іншого алфавіту із заздалегідь встановленим правилом заміни. Розглядається реалізація криптографічного аналізу шифрів одноалфавітної заміни на прикладі афінного шифру Цезаря та системи Цезаря з ключовим словом при відомій і невідомій довжині ключа, шифрів блокової заміни на прикладі шифру Плейфера і шифру «двійний квадрат» Уітстона при відомій і невідомій довжині кодового слова, а також шифру багатоалфавітної заміни на прикладі шифру Віжинера.

Таким чином, вищенаведені основні особливості застосування генетичних алгоритмів, які імітують процеси еволюції живої природи, для розв'язування задачі криптографічного аналізу класичних алгоритмів шифрування свідчать про ефективність застосування даних методів для розв'язування задач криптографічного аналізу.

Література

1. Чернышев Ю.О, Сергеев А.С., Дубров Е.О., Крупенин А.В., Третьяков О.П. Криптографические методы и генетические алгоритмы решения задач криптоанализа: монография. – Краснодар : ФВАС, 2013. – 138 с.
2. Чернышев Ю.О., Сергеев А.С., Дубров Е.О. Применение биоинспирированных методов оптимизации для реализации криптоанализа классических и блочных криптосистем // Теоретические и прикладные вопросы современных информационных технологий: Материалы 11 Всероссийской научно-технической конференции. – Улан-Удэ : Изд-во ВСГТУ, 2012. – С. 121–131.

3. Чернышев Ю.О., Сергеев А.С., Дубров Е.О. Применение биоинспирированных методов оптимизации для реализации криптоанализа классических симметричных и асимметричных криптосистем // Системный анализ в проектировании и управлении: Сборник научных трудов 16-й Международной научно-практической конференции. С-Пб. : Изд-во Политехн. Ун-та, 2012. – С. 112–122.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М. : Радио и связь, 1999. – 328 с.
5. Городилов А.Ю. Криптоанализ перестановочного шифра с помощью генетического алгоритма // Вестник пермского университета. Серия: математика, механика, информатика, 2007, № 7. – С. 44–49.
6. Дубров Е.О., Рязанов А.Н., Сергеев А.С., Чернышев Ю.О. Разработка методов криптоанализа шифров перестановок и замены в системах защиты информации на основе эволюционно-оптимизационных методов // Радиоэлектронные устройства и системы для инфокоммуникационных технологий: научная конференция, посвященная дню радио. – Москва, 2013. – С. 220–224.
7. Морозенко В.В., Елисеев Г.О. Генетический алгоритм для криптоанализа шифра Вижинера //Вестник пермского университета. Серия: математика, механика, информатика, 2010, № 1. – С. 75–80.

Чернышев Ю.О., Сергеев А.С., Дубров Е.О., Рязанов А.Н. Применение эволюционных методов оптимизации для реализации криптоанализа классических шифров замены // Информатика: проблемы, методология, технологии: материалы XIII междунар. науч.-метод. конф. / ВГУ. – Воронеж, 2013, С. 415–418.