(IV) **Mixed-Integer Upper and Lower**: If the sets of both inner and outer continuous and integer variables are nonempty, then the problem is a MIBLP of Type IV.

Advances in the solution of the mixed-integer bilevel programming problems (MIBLP) of all four types can greatly expand the scope of decision making instances that can be modeled and solved within a bilevel optimization framework. However, very little attention has been paid in the literature to both the solution and the application of BLP governing discrete variables. This is mainly because these problems pose major algorithmic challenges in the development of efficient solution strategies.

In [1]–[2], we already started considering and solving mixed-integer linear BLP of Type I. Somethimes, a BLP can be reduced to solving a multi-objective optimization problem.

The main goal of futher papers is to propose an efficient algorithm to solve the mixed-integer linear BLP of Type I, because in our bilevel portfolio optimization problem (6)–(7), the upper level variable σ can clearly treated as integer one. Knowing that this problem is hard to solve, we will propose an algorithm generating approximations that converge to a global solution. The main novelty of the presented heuristic approach lies in the combination of branch-and-bound (B&B) technique with with the simplicial subdivision algorithms. The numerical experiments demonstrate the robust performance of the developed method for instances of the small and medium size.

References:

1. S. Dempe and V. V. Kalashnikov, Discrete Bilevel Programming with Linear Lower Level Problems, Preprint, TU Bergakademie Freiberg, 2005.

2. S. Dempe, V. V. Kalashnikov, N. I. Kalashnykova and A. Arévalo Franco, A new approach to solving bi-level programming problems with integer upper level variables, ICIC Express Letters, vol. 3, no. 4 (B), pp. 1281-1286, 2009.

Бичова І.В., *студентка,*
Чередниченко В.В., *к.е.н., доцент*
кафедри менеджменту та економічної безпеки
Черкаський національний університет імені Богдана Хмельницького

ОСОБЛИВОСТІ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДІЛОВОЇ ДОКУМЕНТАЦІЇ

Розвиток нових інформаційних технологій і впровадження комп‘ютерних систем в усі сфери людської діяльності стали причиною різкого зростання інтересуширокого кола підприємців до проблеми інформаційного захисту ділової документації.

Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційнихсистемах відводиться криптографії, одними із головних задач є: забезпеченняконфіденційності, цілісність та автентичність даних, що передаються.

Криптографія – наука про математичні методи забезпечення конфіденційності(неможливості прочитання інформації сторонніми) і автентичності (цілісності і справжності автора) інформації.Криптографічні методи захисту ділової документації – це методи захисту даних із використанням шифрування. Головна мета шифрування (кодування) інформації – її захист від несанкціонованого читання.

Методи криптографічного захисту ділової документації – це системи шифрування інформації, алгоритми захисту від нав'язування фальшивої інформації (MAC-коди та алгоритми електронного цифровогопідпису) та криптографічні протоколи розподілу ключів, автентифікації тапідтвердження факту прийому(передачі) інформації.

В той же час, криптографічна стійкість методів криптографічного захисту інформації – це властивість криптографічних алгоритмів і криптографічних протоколів, що характеризує їхздатність протистояти методам дешифрування (процес несанкціонованоговідновлення оригіналу тексту повідомлення).

За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним. Апаратна реалізація криптографічного захисту – найбільш надійний спосіб, але й найдорожчий. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації.

Програмна реалізація криптографічного захисту значно дешевша та гнучкіша в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Тому, крім захисту від «вірусних» атак, потрібно вжити заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувались під час роботи програм «збирання сміття».

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів.Криптографічний алгоритм – це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв'язаного (шифрованого) тексту.Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні крипто-алгоритми мають таємний алгоритм шифрування, а загальні крипто-алгоритми характерні повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптозахисту.

Основні методи криптографічного захисту ділової документації можуть бути класифіковані різним чином, але найчастіше їх розподіляють в залежності відспособу використання та за типом ключа:

безключеві – не використовуються ключі (хеш-функції, генерація псевдовипадкових чисел, односторонні перестановки);

перетворення з таємним ключем – використовується ключовий параметр –секретний ключ (симетричне шифрування, цифровий підпис, хеш-функції,ідентифікація);

перетворення з відкритим ключем – використовують в своїх обчисленняхдва ключі – відкритий (публічний) та закритий(приватний) (асиметричнешифрування, цифровий підпис).

Усі криптографічні алгоритми можна використовувати з різними цілями, зокрема: для шифрування інформації, тобто приховування змісту повідомлень і даних;для забезпечення захисту даних і повідомлень від модифікації.

З найпоширеніших методів шифрування можна виділити американський алгоритм шифрування DES (DataEncryptionStandart, розроблений фахівцями фірми IBM і затверджений урядом США 1977 року) із довжиною ключа, що може змінюватися, та алгоритм ГОСТ 28147-89, який був розроблений та набув широкого застосування в колишньому СРСР і має ключ постійної довжини. Ці алгоритми належать до симетричних алгоритмів шифрування.

В останні роки значний інтерес викликає квантова криптографія, вагоме місце в якій займає квантовий розподіл ключів. Квантова криптографія —метод захисту комунікацій, заснований на принципах квантової фізики. Технологія квантової криптографії ґрунтується на принциповій невизначеності поведінки квантової системи — неможливо одночасно отримати координати іімпульс частинки, неможливо виміряти один параметр фотона, не спотворившиінший.

Еліптична криптографія — розділ криптографії, який вивчає асиметричні криптосистеми, засновані на еліптичних кривих над скінченними полями.Основна перевага еліптичної криптографії полягає в тому, що на сьогоднішнійдень невідомо субекспоненціальні алгоритми для вирішення задачі дискретногологарифмування в групах точок еліптичних кривих.

Отже, в ційроботібулозробленоогляднайбільшпоширених в даний час методівкриптографічногозахистуінформації та способів її реалізації.

Вибір для конкретних систем повинен бути заснований на глибокомуаналізіслабких і сильнихсторін тих абоіншихметодівзахисту. Обгрунтованийвибіртієїчиіншоїсистемизахистувзагалі ж повинен спиратися на якіськритеріїефективності. На жаль, до цихпір не розробленівідповідні методики оцінки ефективності криптографічних систем.

Список використанниходжерел:

1. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах // І.Д. Горбенко, Т.О. Гріненко. – Х. : 2004. — 222 с.

2. Юдін О.К. Захист інформації в мережах передачі даних : Підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. — К. : Видавництво «DIRECTLINE», 2009. — 714 с.