ЗАДІРАКА
Валерій Костянтинович —
член-кореспондент НАН України,
завідувач відділу оптимізації
чисельних методів
Інституту кібернетики
ім. В.М. Глушкова НАН України

СУЧАСНІ МЕТОДИ РОЗВ'ЯЗАННЯ ЗАДАЧ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Безпеки безкоштовної не буває.
Постулат безпеки

Вельмишановний Борисе Євгеновичу!
Шановна Президіє!

Комп'ютерні технології, які зараз широко використовують не лише в інформатиці, а й у багатьох інших галузях науки, оперують з інформацією, базами даних, які мають бути захищені. Треба бути впевненим у тому, що використовувана інформація якісна і що по дорозі не була спотворена. Тому питання розроблення та впровадження методів інформаційної безпеки є актуальними не лише для криптології та стеганології, а й для майже всіх галузей науки і практики.

Розглянемо порівняльний аналіз симетричної та асиметричної криптографії. За продуктивністю асиметрична криптографія поступається симетричній на один-два порядки. Симетрична криптографія має такі вади, як проблема розповсюдження ключів, хоча вона полегшена завдяки асиметричній криптографії, і те, що її можна використовувати лише тоді, коли абоненти мережі довіряють один одному. Однак це не стосується військової справи, розвідки, забезпечення дипломатичних каналів зв'язку, фінансово-кредитної сфери, комерційної таємниці тощо. Тому в цих ситуаціях може бути застосована лише асиметрична криптографія. Крім того, задачі автентифікації інформації, застосування електронного цифрового підпису, його верифікації, розповсюдження ключів відкритими каналами зв'язку, реалізація криптографічних протоколів вирішуються лише засобами асиметричної криптографії. Те саме стосується і задач шифрування й дешифрування інформації. Безумовно, хотілося, щоб ці задачі розв'язувалися швидше, чим можна нівелювати розбіжність у продуктивності симетричної та асиметричної криптографії.

Відповідний аналіз показує, що для ефективної реалізації криптопримітивів асиметричної криптографії необхідно

розробляти швидкі алгоритми багатослівної арифметики. Багатослівну арифметику використовують для забезпечення криптостійкості алгоритмів асиметричної криптографії, щоб унеможливити використання, наприклад, таких алгоритмів, як факторизація чисел та обчислення дискретного логарифма. На сьогодні безпечний діапазон асиметричної криптографії становить не менш як 2048 двійкових розрядів для запису одного числа.

Є багато класів задач прикладної, обчислювальної та дискретної математики, для розв'язання яких потрібна техніка обчислень, що використовує алгоритми виконання різних операцій над багаторозрядними числами, — це задачі апроксимації функцій, моделювання фізичних, хімічних, біохімічних процесів, аерота гідродинаміки, інформаційної безпеки. Це зумовлює актуальність створення ефективних алгоритмів виконання операцій над багаторозрядними числами для програмної реалізації на універсальних комп'ютерах та для спеціалізованих апаратних і програмно-апаратних комплексів.

Проблема побудови ефективних алгоритмів багаторозрядної арифметики суттєво загострилася для багатопроцесорної обчислювальної техніки та грід-систем. З використанням багатопроцесорної техніки стало можливим розв'язувати задачі трансобчислювальної складності, високоточні задачі, розв'язання яких пов'язане з великим обсягом обчислювальної роботи (наприклад, 35 млн невідомих у системах лінійних алгебраїчних рівнянь) і, як наслідок, зі значним накопиченням похибки заокруглення. Це призводить до ситуацій, коли, скажімо, обраховані комп'ютерні моделі не мають нічого спільного з фізичними. Один із шляхів контролю за накопиченням похибки заокруглення — перехід до багатослівної арифметики.

Розглянемо тепер іншу задачу інформаційної безпеки — задачу приховання самого факту наявності таємного повідомлення. Якщо криптографія приховує зміст повідомлення, то стеганографія — сам факт його наявності. Стеганографія (з грец. *тайнопис*) давніша за криптографію, але активно розвиватися вона почала лише з появою комп'ютерних технологій. Саме в цей період стеганографія з мистецтва перетворилася на науку. Методи, які приховують інформацію в потоках оцифрованих сигналів і реалізуються на базі комп'ютерної техніки та програмного забезпечення в рамках окремих обчислювальних систем, корпоративних або глобальних мереж, становлять предмет вивчення досить молодої, але достатньо наукомісткої дисципліни — комп'ютерної стеганографії (рис. 1). Цей напрям наукових досліджень використовує результати з криптографії, теорії інформації, теорії складності, теорії ймовірностей і математичної статистики, загальної теорії оптимальних алгоритмів, цифрового оброблення сигналів та зображень, теорії швидких ортогональних перетворень.

Усі стеганографічні методи можна розподілити на два класи: матеріальні та інформаційні. Матеріальні — це методи, які для приховання інформації використовують певні фізичні чи хімічні властивості контейнера, наприклад невидиме чорнило, мікрокрапки тощо. Інформаційні методи для приховання інформації використовують властивості інформаційного наповнення контейнера.

Більшість цифрових методів ґрунтуються, з одного боку, на тому, що файли, які не потребують абсолютної точності, можна дещо видозмінювати без втрати функціональності, а з іншого — на відсутності спеціального інструментарію або нездатності органів чуття людини надійно розрізняти незначні зміни в таких файлах.

Загалом під стеганографічною системою розуміють сукупність пустих контейнерів X повідомлень M ключів K, заповнених контейнерів і перетворень E і D, що їх пов'язують. Цифровим контейнером може слугувати будь-який файл чи потік даних. Через свою надлишковість найчастіше цифровими контейнерами виступають зображення, аудіо- чи відеосигнали. Контейнер, який не містить додаткового повідомлення, називають пустим, а той, що містить, — заповненим, або стеганоконтейнером. Таємний ключ, який застосовується при

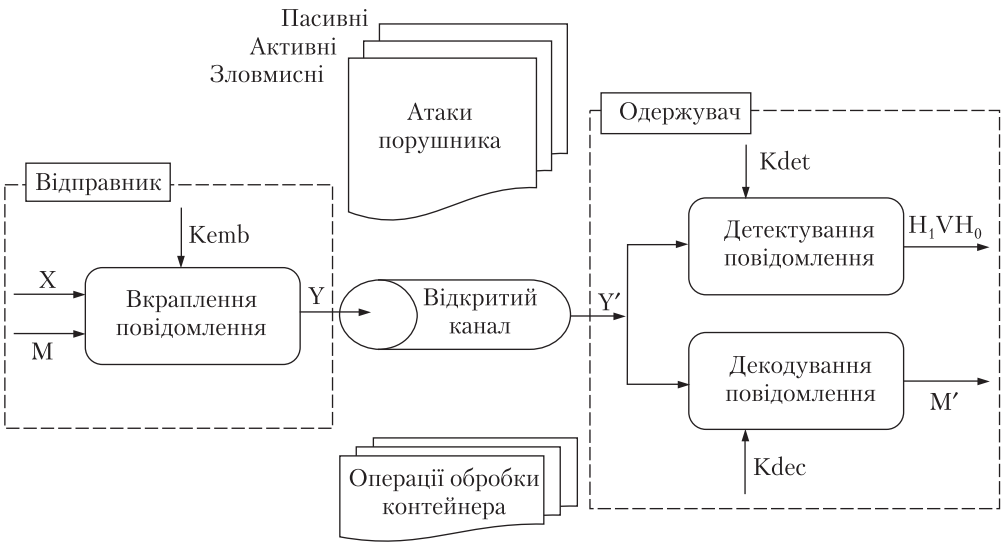

Рис. 1. Узагальнена модель стеганографічної системи

вкрапленні та подальшому вилученні повідомлення з контейнера, називається стеганоключем. У загальному випадку інформація, що передається стеганоканалом, може бути спотворена операціями обробки контейнера — так званими ненавмисними атаками. Слід також врахувати, що крім легальних користувачів (відправника та одержувача) при експлуатації стеганосистеми можлива наявність третього учасника інформаційної взаємодії — порушника, який здійснює навмисні атаки. Порушник може мати можливість лише спостерігати за інформацією в каналі зв'язку без можливості її змінювати, в такому разі його називають пасивним. Порушник може впливати на стеганоконтейнер з метою знищення вкрапленого повідомлення, тоді він зветься активним. Порушник, мета якого достовірно оцінити таємний ключ і тим самим отримати можливість виконувати функції легального спостерігача, тобто створювати фальшиві контейнери, є зловмисним.

Комп'ютерна стеганографія розвивається в кількох напрямах. Так, серед стеганосистем виділяють системи прихованого передавання даних, цифрових водяних знаків, ідентифікаційних номерів («відбитків пальців»). Завдання будь-якої стеганографічної системи — розмістити певне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити різниці між модифікованим контейнером та оригінальним методами візуального або статистичного аналізу.

Системи цифрових водяних знаків (ЦВЗ) актуальні для низки практичних застосувань, таких як завадостійка автентифікація аудіо- та візуальних даних (зокрема, контроль цілісності знімків камер спостереження, записів телефонних розмов, фотознімків як доказів у суді), автентифікації джерела даних (захист авторських прав і прав власності), контроль телевізійного та радіомовлення, копіювання тощо. Основна мета ЦВЗ — зберегти цілісність вкрапленого повідомлення після певного ряду можливих модифікацій стеганоконтейнера. Характерними є активні та зловмисні атаки порушника, а також ненавмисні атаки, спричинені обробкою контейнера. Водяний знак має порівняно невеликий розмір, що дозволяє вкрапити його так, щоб забезпечити стійкість до ненавмисних і активних атак.

Розроблено низку принципово нових стійких стеганоалгоритмів для прихованого передавання повідомлень. Один із них ґрунтується на приховуванні повідомлення в спектрі шумів на рівні похибки заокруглення алгоритму.

Рис. 2. Модель обчислень в «хмарі»

Тому невідомо, чи сталися спотворення в шумі через те, що приховали повідомлення, чи через похибку заокруглення алгоритму. Другий алгоритм оснований на використанні дискретної згортки повідомлення, що приховується, з пустим контейнером, параметри якого засекречені. Авторам невідомі зарубіжні аналоги таких алгоритмів.

Цікавий підхід, який також не має аналогів у літературі, полягає у створенні криптостеганоалгоритмів. Криптостеганографічна система — складний комплекс, загальна стійкість якого не визначається лише стійкістю використаного криптографічного чи стеганографічного перетворення. Стійкість усієї системи залежатиме від правильного узгодження криптографічної і стеганографічної складових системи.

Як правило, бітова послідовність контейнера, в яку вкраплюється повідомлення, не відповідає за своїм характером випадковій послідовності з рівномірним розподілом. Вкраплення інформації в такий контейнер демаскуватиме її за допомогою візуального аналізу бітових зрізів. Виходом у цьому випадку може бути підбір контейнера з розподілом, який збігається з розподілом повідомлення, що вкраплюється. Однак такий підбір робить стеганографічну систему непрактичною.

Етап шифрування дає змогу досягти рівномірності розподілу повідомлення по контейнеру. У цьому разі відрізнити контейнер з вкрапленою інформацією від сканованого або отриманого з цифрової камери зображення стає складніше. Проте залишається відкритим питання стійкості всієї криптостеганографічної системи до статистичних атак. Правильне узгодження криптографічної і стеганографічної складових системи дозволить вирішити цю проблему. Ключову роль при цьому відіграють алгоритми узгодження, які дають змогу перетворити рівномірно розподілені бітові послідовності, отримані на виході криптографічних алгоритмів, на бітові послідовності, аналогічні тим, що використовуються для вкраплення стеганографічними алгоритмами в пусті контейнери. Вимогою, яку висувають до алгоритмів узгодження, що застосовуються у криптостеганографічних системах, є точна статистична відповідність вхідних і вихідних даних.

Інтеграція криптографії і стеганографії дасть можливість позбутися вразливих сторін відомих методів захисту інформації та розробити ефективніші з позицій обчислювальної складності і стійкості до зламу нові методи розв'язання задач інформаційної безпеки.

Розглянемо застосування технологій «хмарних обчислень» у стеганографії. За міжнародними даними, трафік, який обробляється центрами обробки даних, побудованими за «хмарними» технологіями, вперше перевищив трафік, що обробляється за традиційними технологіями. За прогнозом на 2017 р., частка «хмарних» систем у загальному трафіку перевищить 2/3.

«Хмарні» технології — одна з реалізацій теоретичної концепції розподілених обчислювальних технологій, при використанні яких сумісні комп'ютерні ресурси, програмне забезпечення та дані надаються користувачам на замовлення, як послуги через Інтернет (рис. 2). Обчислення у «хмарі» — це спосіб надання клієнту через Інтернет ресурсів як послуг, за якого засоби підтримки цих послуг приховані від нього, а власне ресурси оплачуються клієнтом у міру їх використання.

«Хмарні» обчислення мають такі переваги: зниження вимог до обчислювальних потужностей комп'ютерів; віддалений доступ до даних у «хмарі»; забезпечення високої швидкості обробки даних; економія на придбанні, підтримці, модернізації програмного забезпечення та обладнання; можливість обслуговувати велику кількість користувачів; оплата послуги користувачем лише тоді, коли вона йому необхідна.

Недоліки «хмарних» обчислень: користувач не є власником і не має доступу до внутрішньої «хмарної» інфраструктури; користувач отримує такий рівень безпеки у «хмарі», який може надати провайдер; для отримання якісних послуг користувачеві необхідно мати надійний та швидкий доступ до Інтернету.

При формуванні контейнерів стеганосистем у «хмарних» системах необхідно комплексно використовувати всі види надлишковості систем: у базах даних, інформаційних сховищах, збитковість кодування тощо.

Нові властивості «хмарних» обчислень зумовлюють нові постановки задач у галузі захисту інформації. Розроблена модель стеганосистем на основі загальної теорії оптимальних алгоритмів дозволила запропонувати точні методи оцінювання стійкості стеганографічного перетворення. Основні з наведених результатів уже впроваджено в Головному управлінні розвідки Міністерства оборони України, а також у Службі безпеки України.

Коротко розглянемо деякі проблеми, які чекають на своє розв'язання:

1. Розроблення стандартів на криптопримітиви.

2. Створення теоретичних засад для розроблення нових криптографічних перетворень, а саме нових односторонніх функцій та односторонніх функцій з «лазівкою».

3. Упровадження технологій «хмарних» обчислень у криптографії та стеганографії.

4. Удосконалення криптографічних протоколів з розділення секрету.

5. Отримання оцінок знизу стійкості до криптоаналізу та стеганоаналізу криптографічних і стеганографічних систем.

6. Упровадження алгоритмів паралельної математики при розв'язанні задач інформаційної безпеки.

7. Упровадження нових криптографічних протоколів електронних платежів та електронної комерції.

8. Модернізація і розроблення національної системи закритого зв'язку (в тому числі рухомої та мобільної компоненти).

Дякую за увагу.