УДК 003.26.09:004.032.24-004.272.3

А.М. Луцків, С.А. Лупенко
Тернопільський національний технічний університет імені Івана Пулюя
кафедра комп'ютерних систем та мереж

ОСОБЛИВОСТІ КРИПТОАНАЛІЗУ У ГРІД-СЕРЕДОВИЩІ

Розглянуто ГРІД-орієнтоване програмне забезпечення для здійснення криптоаналізу. Проаналізовано аспекти розробки ГРІД-орієнтованого програмного забезпечення для криптоаналізу. Розглянуто архітектуру та компоненти грід-орієнтованого програмного забезпечення для криптоаналізу.

Ключові слова: віртуальна лабораторія, криптоаналіз, алгебраїчний, криптоаналіз, "сендвіч-атака", обчислювальні кластери, грід-обчислення.

The paper examines grid-oriented software for cryptanalysis. Aspects of cryptanalysis grid-oriented software development are analysed. The architecture and components of grid-oriented cryptanalysis software are described.

Key words: virtual laboratory, cryptanalysis, algebraic cryptanalysis, sandwich attack, computation cluster, grid computing

Вступ

Одним із найважливіших завдань, яке необхідно розв'язувати, розробляючи нові та впроваджуючи існуючі системи криптографічного захисту, є їх верифікація. Оскільки криптостійкість більшості сучасних шифрів ґрунтується на просторовій (вимоги до об'єму пам'яті) та часовій (вимоги до процесорного часу виконання) складностях, відповідно, неможливо розв'язати задачі криптоаналізу за розумний час за допомогою доступних обчислювальних засобів. Тому актуальною є проблема адаптації існуючого криптоаналітичного алгоритмічного забезпечення для його використання на високопродуктивних обчислювальних системах: векторних, паралельних та гібридних. Водночас відповідне криптоаналітичне алгоритмічне забезпечення доцільно реалізувати у вигляді програм, орієнтованих на вчених-криптологів. Особливістю програмних засобів для верифікації створюваних та досліджуваних криптографічних алгоритмів шифрування є можливість їх виконання на доступній обчислювальній базі [1]. Серед таких високопродуктивних обчислювальних систем особливе місце посідають грід-, або метакластерні-системи [2–5].

Постановка проблеми

В Україні такою метакластерною системою є Український національний грід (УНГ). До переваг використання таких систем, зокрема УНГ, належать:

1. Можливість об'єднання результатів діяльності вчених-криптологів у межах одного віртуального дослідницького майданчика, яким є віртуальна організація.
2. Надання обчислювальних ресурсів тим науковцям, які ними не володіють.
3. При здійсненні досліджень у рамках державних програм використання обчислювальних ресурсів є безкоштовним.

Альтернативою грід-обчисленням можна розглядати технологію хмарних сервісів, які надають в оренду обчислювальні ресурси, наприклад, датацентри компанії Amazon Elastic Compute Cloud (Amazon EC2). Проте їх використання пов'язане з такими складностями:

- вхідні дані та результати обчислень зберігаються у віддаленому сховищі, що є неприйнятним при роботі з конфіденційними даними;
- вартість оренди обчислювальних хмарних сервісів є сьогодні невиправдано високою для академічних досліджень, зокрема тих, які здійснюються бюджетними організаціями.

На основі наведеного вище окреслимо актуальні в цій предметній області задачі:

- створення паралельних та векторних криптоаналітичних методів й розпаралелення та векторизація існуючих;
- розроблення паралельного, векторного та гібридного криптоаналітичного програмного забезпечення, яке орієнтоване на наявні в Україні кластерні та грід-системи;
- створення зручного інтерфейсу користувача для доступу до обчислювальних ресурсів та криптоаналітичного програмного забезпечення.

Аналіз останніх досліджень та публікацій

Отже, доступними високопродуктивними обчислювальними системами для вітчизняних вчених-криптоаналітиків є кластерні системи [1] та грід-мережі [2–5], однак стримувальними факторами їх використання є незручність безпосереднього використання інтерфейсу командного рядка, складність адміністрування та моніторингу відповідних обчислювальних систем. З метою усунення стримувальних факторів необхідно розробити зручний графічний інтерфейс та відповідні програмні криптоаналітичні модулі, які б спрощували роботу вченого-криптоаналітика. Водночас архітектура системи має бути масштабованою та розширюваною відповідно до задач.

Доцільним також є створення тематичної віртуальної організації для об’єднання вчених, які працюють у цій предметній області, а також створення віртуальної криптоаналітичної лабораторії для відповідної тематичної віртуальної організації. Прикладом створення такої системи у відповідній предметній області є віртуальна лабораторія молекулярної динаміки[5], яка об'єднує науковців віртуальної організації moldyngrid Українського національного гріду (УНГ). Під віртуальною криптоаналітичною лабораторією варто розуміти інформаційну систему, яка об’єднує такі складові:

- “бек-енд” — криптоаналітичне програмне забезпечення адаптоване до векторних, паралельних та гібридних обчислювальних засобів, які є елементами грід-мережі;
- сховище даних, яке містить результати експериментальних досліджень;
- “фронт-енд” — інтерфейс керування криптоаналітичним програмним забезпеченням, який дає змогу здійснювати представлення отриманих експериментальних результатів та виконувати необхідні в грід-системі операції засобами графічного веб-інтерфейсу.

Перевагами такого підходу є:

- створення власної бази даних (знань) у межах деякої віртуальної лабораторії (організації) в галузі криптоаналізу, що дає змогу оптимізувати час проведення експерименту шляхом усунення дублюючих експериментів та раціонального використання готових напрацювань;
- забезпечення користувача зручним інтерфейсом;
- забезпечення надійного та прозорого способу доступу до сховища даних;
- можливість використання зручного засобу моніторингу виконання завдань у ґрід-системі;
- об'єднання у віртуальній організації науковців, які не мають власних обчислювальних потужностей.

Формулювання цілі статті

Основним завданням є реалізація віртуальної криптоаналітичної лабораторії, яка є веб-сайтом, що забезпечує зручний веб-інтерфейс до криптографічних та криптоаналітичних грід-програм.

Зважаючи на відсутність грід-орієнтованого програмного забезпечення для дослідників у галузі криптоаналізу, актуальним та важливим науково-прикладним завданням є створення віртуальної криптоаналітичної грід-орієнтованої лабораторії CryptoGRID-TNTU, що об'єднує паралельне програмне забезпечення для криптоаналізу та зручний користувацький web-інтерфейс для керування та моніторингу досліджень у галузі криптології.

Для зручності роботи криптоаналітиків доцільно об'єднати в межах криптоаналітичного грід-орієнтованого програмного комплексу (віртуальної криптоаналітичної лабораторії) різноманітні

криптографічні та криптоаналітичні засоби, які вже є реалізовані, зокрема під відкритими ліцензіями, а також розробляти власні програмні компоненти для формування бази досліджуваних алгоритмів шифрування та методів криптоаналізу. Це можна забезпечити двома шляхами:

- орієнтуватися на конкретні реалізації криптографічних алгоритмів з використанням відповідних криптоаналітичних методів, а також з оптимізацією цих методів під конкретне паралельне, векторне чи розподілене обчислювальне середовище;
- розробляти універсальні криптоаналітичні засоби, у яких були б реалізовані криптоаналітичні методи, які дослідник мав би змогу використовувати для різних досліджуваних алгоритмів.

Очевидно, що перший метод є простішим з погляду реалізації, проте другий метод дає змогу досліджувати нові криптографічні алгоритми, а також розробляти нові криптоаналітичні методи на основі поєднання існуючих. Тому доцільно при побудові програмної системи криптоаналізу використовувати обидва підходи, а саме здійснювати дослідження симетричних систем шифрування та хеш-функцій, а з метою апробації програмної системи використовувати добре відомі криптоаналітичні методи та криптографічні алгоритми. На рис. 1 зображено алгоритми шифрування та криптоаналітичні методи, які досліджуються у межах робіт у науково-дослідній лабораторії моделювання, математичного та програмного забезпечення інформаційних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя і є компонентами проектованої програмної системи.

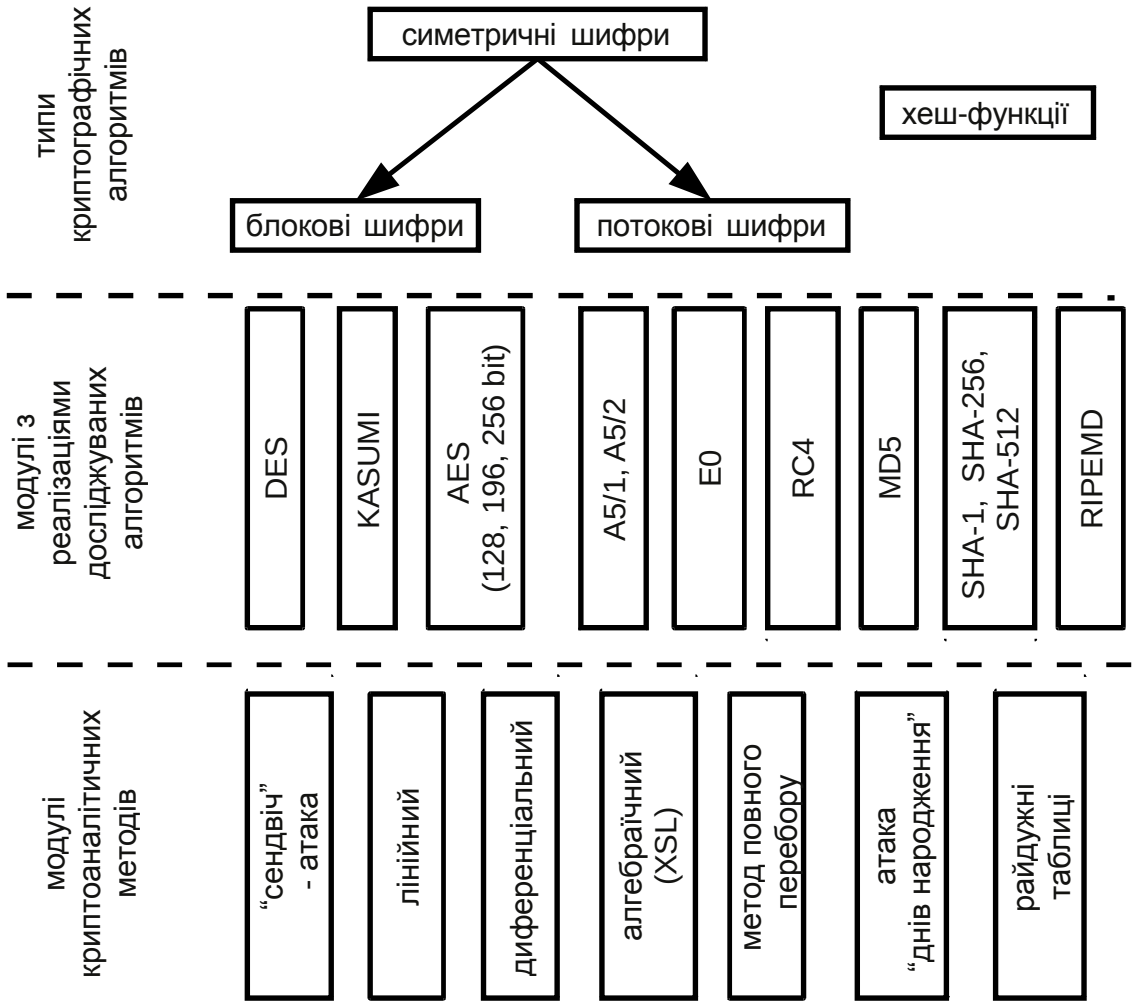

Рис. 1. Компоненти віртуальної криптоаналітичної лабораторії (проект)

При проектуванні віртуальної криптоаналітичної грід-орієнтованої лабораторії необхідно забезпечити:

- зручний інтерфейс користувача для моніторингу та керування виконанням задач;
- зручний спосіб доступу до експериментальних даних (зашифрованих повідомлень, результатів попередніх експериментів);
- зручний спосіб кооперації членів віртуальної організації;
- наявність бази знань попередніх криптоаналітичних експериментів;
- можливість подальшого розширення і додавання модулів.

Забезпечити ці вимоги необхідно, розробляючи власне програмне забезпечення та враховуючи при цьому специфіку використовуваного системного програмного забезпечення, зокрема проміжного програмного забезпечення NorduGrid ARC. Ключовою вимогою до роботи програмного комплексу є захищеність роботи системи, яка полягає у надійних механізмах аутентифікації користувачів та використанні захищених каналів зв'язку. У цьому аспекті виправданим є використання вже наявних розробок: з погляду як програмного забезпечення, так і з методології побудови віртуальних лабораторій грід-мереж.

Для реалізації поставленої задачі доцільно використовувати готові напрацювання у галузі криптоаналізу, криптографії та паралельних систем опрацювання даних. Очевидно, що системне програмне забезпечення для організації грід-сайту повинно відповідати вимогам Національного операційного центру грід-ресурсів, а розробляючи основні модулі доцільно, використовуючи технології MPI, OpenMP та один з варіантів технології GPGPU й відповідно мов програмування C/C++. У цьому випадку зручно використовувати криптографічні бібліотеки openssl, gnutls та низку інших, оскільки вони є добре апробованими й розповсюджуються за відкритими ліцензіями. Доцільно також використовувати технологію JAVA, оскільки вона забезпечує достатньо великий набір криптографічних бібліотек, має засоби паралельного та розподіленого програмування і є кросплатформовою. Доцільно використати готові криптоаналітичні компоненти та утиліти, а саме для методу повного перебору: john, oclhashcat та аналогічні їм. На особливу увагу заслуговує використання засобів алгебраїчного криптоаналізу як достатньо сучасного й ефективного методу криптоаналізу. При використанні програмних компонент доцільно використовувати відкрите програмне забезпечення, а власноручно створене також поширювати за відкритими ліцензіями.

Отже, основними завданнями є:

- розроблення грід-орієнтованого програмного забезпечення для розв'язання задач криптоаналізу;
- створення віртуальної криптоаналітичної лабораторії (веб-сайту CryptoGRID-TNTU) для забезпечення зручного інтерфейсу до грід-орієнтованого ПЗ, з інтеграцією у неї криптоаналітичного грід-орієнтованого програмного забезпечення.

Для вирішення цих завдань необхідно розв'язати низку задач:

1. Вибрати програмно-апаратні засоби для роботи ґрід-системи.
2. Захистити роботу ґрід-системи.
3. Забезпечити узгодженість роботи окремих кластерних систем при роботі над єдиною задачею (синхронізація підпрограм).
4. Створити спеціалізовані системи зберігання даних, які б містили проміжні та остаточні результати експериментів.
5. Здійснити порівняльний аналіз математичного та програмного криптоаналітичного забезпечення.
6. Розробити алгоритми та методи декомпозиції обчислювальної задачі для ґрід-середовища з урахуванням затримок комунікаційних каналів та проблем синхронного виконання розподілених програм.
7. Створити ґрід-орієнтоване програмне забезпечення для здійснення криптоаналізу.
8. Створити спеціалізоване програмне забезпечення для роботи з обчислювальною системою віртуальної організації, яка б забезпечувала доступ до сховища даних, містила базові криптоаналітичні конструкції та забезпечувала колективну роботу фахівців.

Виклад основного матеріалу

На основі наведених вище вимог до грід-орієнтованої програмної системи, з урахуванням криптоаналітичних компонент (модулів) було розроблено загальну архітектуру грід-орієнтованої програмної системи [5]. Загальна архітектура інформаційної системи "користувач-віртуальна криптоаналітична лабораторія-грід" виглядатиме, як це показано на рис. 2.

Криптоаналітичний грід-портал об'єднує криптоаналітичні модулі, кількість яких можна нарощувати відповідно до потреб задач криптоаналізу. Грід-портал, посуті, є веб-сайтом з можливістю авторизованого входу для користувачів віртуальної криптоаналітичної лабораторії. Водночас цілком можливим є запуск окремих модулів типовим способом, тобто через командний інтерфейс проміжного програмного забезпечення грід. Варто зазначити, що кожна підсистема може бути розширена іншими програмними компонентами, а також можливим є додавання нових методів. Кожен криптоаналітичний модуль має свою внутрішню архітектуру, яка залежить від використовуваного методу й відповідно математичного, алгоритмічного й/або програмного забезпечення. Коротко зупинимось на цих модулях.

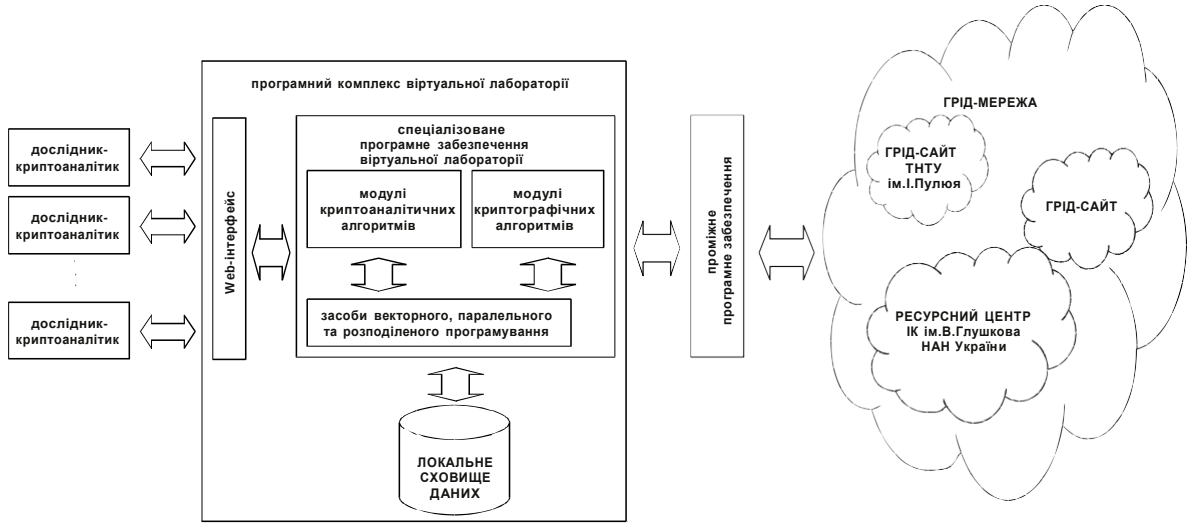

Рис. 2. Загальна архітектура інформаційної системи "користувач-віртуальна криптоаналітична лабораторія-грід"

Сьогодні автори проекту працюють над алгебраїчним методом та методом "сендвіч-атаки", які є модулями створюваної системи. Також система містить метод повного перебору та його різновиди, оскільки він є найпростішим, відносно просто розпаралелюється і його зручно використовувати для тестування створюваної системи.

Програмне забезпечення підсистеми, що реалізує метод "сендвіч-атаки" на алгоритм Kasumi, оснований на методі *"сендвіч-атаки" із пов'язаними ключами* на 8-раундовий KASUMI, з часовою складністю 2^{32} [6]. Цей програмний модуль реалізовано мовою C++ з використанням технологій OpenMP та MPI, тобто орієнтовано на використання в системах зі спільною та розподіленою пам'яттю (кластерні, та грід-системи).

Програмне забезпечення підсистеми, що реалізує метод алгебраїчного криптоаналізу [7] складається з двох компонент: першої для дослідження потокових та другої для дослідження блокових шифрів.

Потокові шифри (Grain, Trivium, Bivium, HiTag2 та Crypto-1) досліджують за допомогою системи програм cryptominisat (автор програми Mate Soos) [8] — це програма SAT-обчислювач (система розв'язання рівнянь у кон'юнктивній нормальній формі) з великим набором функціональних можливостей і є найшвидшою сьогодні системою. Зараз розробники модифікують цю програму для розподілених обчислень. Сьогодні паралельності виконання програми можна досягти декомпозицією обчислювальної задачі за вхідними даними.

Програмне забезпечення підсистеми, що реалізує метод повного перебору, основується на використанні утиліти з відкритим вихідним кодом John the Ripper (з набором jumbo-розширень), яка призначена для відновлення паролів за їхніми хеш-функціями. Водночас ця підсистема може бути відносно просто розширена за допомогою інших програм: oclHashcat, hydra, hashkill, Ophcrack та інших.

Висновки

Обґрунтовано та розроблено грід-орієнтоване математичне та програмне забезпечення, що реалізує метод "сендвіч-атаки" на алгоритм Kasumi, алгебраїчний криптоаналіз та метод повного перебору. Спроектовано та розроблено прототип веб-інтерфейсу до криптоаналітичної грід-орієнтованої програмної системи CryptoGRID-TNTU (http://www.nalabs.org.ua) з інтеграцією основних криптоаналітичних підсистем.

1. Загородна Н. В. Обґрунтування вибору доступних програмно-апаратних засобів високопродуктивних обчислювальних систем для задач криптоаналізу / Н. В. Загородна, С. А. Лупенко, А. М. Луцків // Електроніка та системи управління. – 2011. – №1(27). – С. 42–50. 2. Загородна Н. В. Особливості створення GRID-систем на основі GPU-вузлів для розв'язання задач криптоаналізу / Н. В. Загородна, С. А. Лупенко, А. М. Луцків // Вісник національного університету "Львівська політехніка" "Інформаційні системи та мережі". – 2011. – № 699. – С. 302–320. 3. Загородна Н. В. Реалізація сучасних криптоаналітичних методів у обчислювальному грід-середовищі на основі кластерних архітектур / Н. В. Загородна, С. А. Лупенко, А. М. Луцків // Електроніка та системи управління. – 2011. – № 3(29). – С. 5–15. 4. Перевозчикова О.Л. Тульчинский В.Г. Ресурсные центры УНГ / Робоча нарада "Український Національний Грід – 2010" [Електронний ресурс]. – Режим доступу: URL:http://grid.nas.gov.ua/images/ stories/NANU/General/UNG-10-Talks/tulchinsky.pdf – Назва з екрану. 5. Лупенко С. Криптоаналітична віртуальна лабораторія у грід-середовищі / С. Лупенко, А. Луцків // Праці міжнародної конференції "Кластерні обчислення", Київ, 12 червня-14 червня 2012. – Київ, 2012. – С. 40–43. 6. Кондрацький Ю. Практичні аспекти здійснення криптоаналізу методом "сендвіч атаки з пов'язаними ключами" алгоритму KASUMI / Ю. Кондрацький, А. Луцків //Актуальні задачі сучасних технологій: збірник тез доповідей міжнародної науково-технічної конференції молодих учених та студентів, 19–20 грудн. 2012р., м. Тернопіль – Тернопіль,: Видавництво ТНТУ ім. Івана Пулюя, 2012. – с. 199–200. 7. Courtois N. How Fast can be Algebraic Attacks on Block Ciphers? [Електронний ресурс]. – Режим доступу: URL: http://eprint.iacr.org/2006/168.pdf – Назва з екрану. 8. Mate Soos – CryptoMiniSat2 [Електронний ресурс]. – Режим доступу: URL: http://www.msoos.org/cryptominisat2/ – Назва з екрану.