УДК 681.324+519.68(045)

[1]**Н. В. Загородна**, канд.техн. наук,
[2]**С. А. Лупенко**, д-р. техн. наук,
[3]**А. М. Луцків**, канд.техн.наук

ОБҐРУНТУВАННЯ ВИБОРУ ДОСТУПНИХ ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ВИСОКОПРОДУКТИВНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ ДЛЯ ЗАДАЧ КРИПТОАНАЛІЗУ

Тернопільський національний технічний університет ім. І. Пулюя,
e-mail: [1]zagorodna.n@gmail.com, [2]l.andriy@gmail.com, [3]lupenko@ua.fm

Проананалізовано та обґрунтовано сучасні доступні програмно-апаратні засоби для криптоаналізу. Сформовано вимоги до високопродуктивної обчислювальної системи для криптоаналізу. Розроблено проект кластерної системи для крипто аналізу, виходячи з критеріїв гнучкості, доступності, функціональності та простоти розроблення.

Ключові слова: криптоаналіз, високопродуктивні обчислення, обчислювальні кластери, GPU.

Вступ і постановка завдання. Криптографічний захист каналів зв'язку тісно інтегрований в усі сфери життєдіяльності людини, починаючи від засобів захисту спеціального зв'язку силових структур і закінчуючи захистом з'єднань користувачів приватних сторінок мережі Інтернет.

Шифрування каналу зв'язку відбувається за допомогою симетричних шифрів сеансовими ключами, а шифрування сеансових ключів для передавання незахищеними каналами зв'язку здійснюється за допомогою асиметричних алгоритмів шифрування. Ускладненість використання асиметричних алгоритмів шифрування для шифрування каналу зв'язку зумовлюється більшою довжиною ключа порівняно із симетричними шифрами за такої ж криптостійкості, а також великою ресурсоємністю операцій шифрування. Тому особливу роль у шифруванні сучасних мереж передавання даних відіграють симетричні блокові шифри, зокрема UMTS/W-CDMA (A5/3-KASUMI), IEEE 802.16/WiMAX – AES, різні реалізації VPN-мереж: IPSec (3DES), L2TP/IPSec (3DES/AES), OpenVPN (AES).

Розроблення криптостійких алгоритмів безпосередньо пов'язано з розвитком іншої галузі криптології – криптоаналізом. Криптоаналіз є визначальним для розроблення нових та вдосконалення існуючих шифрів, аудиту інформаційної безпеки систем, які використовують шифрування.

Для криптоаналітика важливим є дослідження усіх компонент систем шифрування каналу зв'язку як на етапі обміну сеансовими ключами, так і на етапі шифрування сеансу. Тому актуальним є створення багатофункціональної, гнучкої за можливостями використання різних методів криптоаналізу для різних криптоалгоритмів, високошвидкісної апаратно-програмної системи, яка була б доступною за ціною та простою щодо реалізації конкретних криптоатак на системи шифрування.

У цій роботі обґрунтовано вибір програмно-апаратної системи для криптоаналізу, яка була б доступною для вищого технічного навчального закладу.

Вимоги до комп'ютерної системи криптоаналізу. Система криптоаналізу повинна давати змогу досліджувати криптостійкість алгоритмів шифрування, тобто стійкість до криптографічної атаки за певних фіксованих умов, і вимірюватися потрібною кількістю ресурсів для проведення криптоатаки. Ресурсами є такі величини [1]:

1. Кількість інформації, необхідна для здійснення успішної атаки: кількість пар відомих або вибраних текстів.

2. Час, необхідний для здійснення успішної атаки. Його визначають за кількістю тестових операцій шифрування атакуючим алгоритмом, виконання яких за дотримання інших необхідних умов дає змогу, наприклад, визначити ключ шифрування. Цей параметр визначає часову складність криптоалгоритму.

3. Ємність пам'яті, необхідна для проведення успішної атаки. Багато криптоатак не може бути реалізована на практиці у зв'язку з недостатньою ємністю оперативної та дискової пам'яті. Цей параметр визначає просторову складність криптоалгоритму.

Виділяють поняття «*теоретична криптографічна стійкість*», яку визначає розробник і яка зазвичай є кількістю можливих варіантів значень ключа за методу повного перебору. Виокремлюють також поняття «*практична криптографічна стійкість*» алгоритму шифрування, яку визначають застосуванням відомих, більш ефективних, аніж повне перебирання, методів. До таких методів належать диференціальний та лінійний методи, метод «бумерангу», метод неможливих диференціалів, метод Дейвіса, метод «зустрічі посередині» та інші. Ці методи можна комбінувати між собою, а також з методами повного перебирання, чи його оптимізованими різновидами (атака за словником і «райдужні» таблиці). Ці методи дають змогу отримати ключ лише з деякою імовірністю, тому повторення криптографічної атаки з тими ж, або іншими вхідними повідомленнями, дозволяють підвищити ймовірність зламу. У цьому аспекті важливим є завдання оптимізації криптоатаки за часом її проведення шляхом розпаралелення обчислювальної задачі, а у випадку неможливості розпаралелення методу – можливість виконання того ж методу з різними вхідними даними. Тобто, якщо алгоритм містить рекурсивні залежності і немає можливості проведення декомпозиції, то його багатократне повторення з іншими діапазонами ключів та парами вхідних повідомлень дає змогу підвищити ймовірність зламу. Що стосується здатності розпаралелення, то можна вирізнити XSL-атаку (eXtended Sparse Linearization), яка зводиться до подання алгоритму шифрування як системи деяких алгебричних рівнянь. Так, алгоритм AES-128 може бути поданий у вигляді системи 8000 рівнянь з 1600 невідомими. Розв'язання таких рівнянь донедавна мало суто теоретичний характер. Однак коректна реалізація цього методу за допомогою високопродуктивних обчислювальних систем робить уразливими майже всі сучасні симетричні блокові шифри.

Під час проектування системи криптоаналізу згадані ресурси вказують на необхідні параметри системи криптоаналізу, а саме: на високу швидкодію процесора або процесорів та велику ємність оперативної пам'яті. Очевидно, що швидкість обміну між процесором або процесорами та пам'яттю має бути якомога більшою.

Характеристики часто вживаних симетричних блокових алгоритмів шифрування, зокрема щодо їх криптостійкості, наведено у таблиці.

Наведені методи криптоаналізу мають здатність до розпаралелення, що дає змогу підвищити їх ефективність за рахунок використання високопродуктивних обчислювальних систем.

Для реалізації систем криптоаналізу, як правило, використовують спеціалізовані апаратно-програмні комплекси, що в ряді випадків орієнтовані на розв'язання одного типу задач. Прикладом такої системи є розробка компанії IBM [2], яка орієнтована виключно на роботу з алгоритмом DES. З точки зору криптоаналітика більш прийнятною є та платформа, яка дає змогу змінювати методи криптоаналізу і має можливість модифікації. Очевидно, що така універсальність може бути забезпечена за допомогою програмного забезпечення (за винятком ПЛІС), запуск якого визначається розв'язуваними задачами.

Ще вагомими критеріями вибору програмної платформи є зручність розроблення для неї програмного забезпечення, наявність інструментальних засобів: утиліт та вихідного коду відповідних утиліт, а також криптографічних бібліотек з реалізованими криптографічними алгоритмами та протоколами.

Характеристики поширених алгоритмів шифрування

Назва алгоритму шифрування	Сфера застосування	Теоретична криптосійкість	Практична криптостійкість (кількість операцій)	Метод криптоаналізу	Право власності (номер патента)
A5/3, UEA1, UIA1 (KASUMI)	Мережі безпровідного зв'язку UMTS/W-CDMA	2^{128}	2^{32}	«Сендвіч-атака» [3]	Mitsubishi Electric Corporation US 7096369
AES-128	Мережі безпроводового зв'язку IEEE 802.16/WiMAX, Віртуальні приватні мережі на основі протоколів IPSec, L2TP/IPSec, OpenVPN, SSH, LTE	2^{128}	2^{100}	Лінійний, XSL-атака, атака на основі зв'язаних ключів	Стандарт, без патентних обмежень
AES-196		2^{196}	2^{176}		
AES-256		2^{256}	$2^{99.5}$		
3DES	Віртуальні приватні мережі на основі протоколів IPSec, L2TP/IPSec, OpenVPN, SSH, електронні платіжні системи (Europay, MasterCard, VISA та інші)	2^{168}	2^{84}	«Зустріч посередині»	Без патентних обмежень
DES		2^{56}	$2^{39} – 2^{41}$	Лінійний, диференціальний, атака Дейвіса	Стандарт, без патентних обмежень
CMEA	CDMA2000	2^{64}	$2^{24} – 2^{32}$	Атака на основі відомих відкритих текстів	U.S. Patent 5,159,634
TEA	Хеш-функція в Microsoft Xbox	2^{128}	2^{32}	Атака на основі зв'язаних ключів	Без патентних обмежень
IDEA	PGP	2^{128}	$2^{126.8}$	Поєднання диференціального і лінійного	MediaCrypt (US patent 5,214,703)
Safer+	Bluetooth (генерування ключів і аутентифікація)	2^{256}	2^{200}	«Зустріч посередині»	Без патентних обмежень

Логічно також врахувати критерій зручності супроводу системи, який визначається документованістю, доступністю і відкритістю її компонент.

Таким чином, основними критеріями для обґрунтування вибору апаратно-програмних засобів системи криптоаналізу є: 1) швидкодія процесорів та доступна їм ємність пам'яті; 2) швидкість доступу та латентність при доступі до пам'яті (на одному вузлі та в системах з розподіленою пам'яттю); 3) універсальність системи; 4) зручність розроблення програмного забезпечення для криптоаналізу; 5) зручність супроводу системи; 6) вартість апаратних та програмних компонент системи.

Обґрунтуємо апаратно-програмний комплекс для реалізації методів криптоаналізу з урахуванням наведених критеріїв.

Огляд та обґрунтування апаратних засобів для криптоаналізу. Найпоширенішими високопродуктивними системами в світі є кластерні системи, обчислювальні вузли яких є SMP-системами (Symmetric Multiprocessing – системи із симетричним мультипроцесуванням), які ґрунтуються на багатоядерних і багатопроцесорних системах, що забезпечує високий ступінь паралелізму. Використовуючи процесори Intel з підтриманням технології

HyperThreading можна суттєво підвищити ефективність паралелізму (якщо немає потреби в синхронізації процесів та спільної роботи з кешем процесора). Проте, зважаючи на критерій цінової доступності, оптимальним є використання багатоядерних процесорів фірми AMD, зокрема Phenom, а не багатопроцесорних систем.

Важливе місце серед архітектур паралельних та розподілених комп'ютерних систем (ПРКС) відіграє MPP (Massive Parallel Processing), на якій базується сучасна технологія обчислень з використанням спеціалізованих графічних процесорів (GPU – Graphical Processor Unit) [4]. Особливістю цієї технології є її невисока вартість і відносна простота використання графічних процесорів для завдань загального призначення – general purpose graphical processor unit (GPGPU). Лідером зі створення спеціалізованих обчислювальних пристроїв на основі GPU є компанія nVidia з технологією CUDA. Обчислювальні можливості мають не лише спеціалізовані плати типу nVidia Tesla GPU Modules [5], а також звичайні відеокарти nVidia, які можуть бути використані як пристрої для обчислень. Попри те, що в найдешевші CUDA-сумісні відеокарти мають невелику ємнімть оперативної пам'яті і немає модулів для роботи з дійсними типами даних (чисел з плаваючою комою), однак для криптоаналізу вони цілком придатні, оскільки тут домінуючими є операції з цілочисловими типами даних та бітовими полями. Ці плати мають високошвидкісну шину обміну даними між ядрами графічних процесорів та вбудованою високошвидкісною пам'яттю.

Альтернативою технології GPGPU щодо швидкодії є використання програмованих логічних інтегральних схем (ПЛІС). Основною перевагою ПЛІС порівняно з GPGPU є висока швидкодія (у деяких випадках можна створювати системи криптоаналізу у режимі реального часу) опрацювання великих потоків даних. ПЛІС дає змогу змінити архітектуру обчислювальної системи залежно від обчислювальної задачі, чого не можна зробити за допомогою GPGPU. Проте робота з ПЛІС вимагає фахових знань у галузі електроніки, а не лише теорії криптографічних алгоритмів та навичок системного й прикладного програмування. Також варто зазначити, що засоби GPGPU є дешевшими, аніж аналогічні ПЛІС. З практичного погляду, якщо обчислювальна задача не передбачає апаратної реалізації у вигляді окремого пристрою і не критична до оброблення в режимі реального часу, то використання графічних процесорів буде суттєво дешевшим порівняно з ПЛІС-системами.

Використання графічних процесорів порівняно з центральними процесорами дає змогу суттєво збільшити продуктивність системи криптоаналізу завдяки більшій кількості одночасно виконуваних потоків (для повного завантаження сучасного багатоядерного центрального процесора достатньо 10 – 20 потоків, а графічного – кілька тисяч). Тому вибір відносно недорогих багатоядерних процесорів AMD Phenom цілком виправданий і під час розроблення системи криптоаналізу основний акцент варто робити на використання графічних процесорів.

Для організації кластерної системи з розподіленою пам'яттю ключовим є комунікаційний інтерфейс, зокрема його характеристики латентності та пікової пропускної здатності. За цими критеріями лідером є технологія InfiniBand, однак її вартість досить висока. Для мінімізації затрат на побудову кластерної системи можна використовувати комунікаційне обладнання на основні технології Gigabit Ethernet. На базі цього стандарту можна створити обчислювальну та сервісну мережі.

Перспективним видається використання ґрід-технологій для криптоаналізу, тобто створення метакластерних систем. Для таких цілей потенційно може бути використана вітчизняна система «Український академічний ґрід», однак висока латентність комунікаційних каналів, неоднорідність програмного забезпечення, непрогнозованість виконання завдань в окремо взятих кластерних системах вказують на малу ефективність та значну складність її використання на нинішньому етапі її розвитку. У цьому контексті видається виправданим та доцільним створення приватних ґрід-мереж для завдань такого класу.

На думку авторів, для організації високопродуктивної ПРКС доцільно використовувати кластерну технологію із SMP-вузлами, які обладнані багатоядерними процесорами AMD Phenom II X4 955 та CUDA-сумісними відеокартами nVidia GTX 465 з комунікаційним інтерфейсом Gigabit Ethernet. Під час створення програмного забезпечення для ПРКС, у зв'язку з високою латентністю технології Gigabit Ethernet, необхідно мінімізувати міжвузлові обміни даними на рівні алгоритмів та програмної реалізації (передача «запакованих» даних у MPI), а розрахунки виконувати на обчислювальних ядрах GPU. Така конфігурація буде досить продуктивною та недорогою за рахунок використання процесорів AMD Phenom, відеокарт nVidia GTX 465, які реалізують сучасну архітектуру Fermi (Compute capability: 2.0), та середовища обміну даними Gigabit Ethernet. Використання такої конфігурації апаратного забезпечення уможливить доступність, достатню продуктивність, гнучкість та зручність проведення процедур криптоаналізу. Єдиним вузьким місцем цієї системи є комунікаційний інтерфейс, який для зменшення латентності і за наявності матеріальних ресурсів рекомендується замінити на InfiniBand.

Іншим фактором, що визначає гнучкість та доступність такої системи, є використання вільного відкритого програмного забезпечення [6]: прикладного та системного, а також засобів його розроблення.

Огляд та обґрунтування програмних засобів для криптоаналізу. Для організації роботи ПРКС необхідно встановлювати таку операційну систему, яка б підтримувала обґрунтоване вище апаратне забезпечення і давала змогу виконувати ресурсоємні завдання криптоаналізу на базі паралельних і розподілених технологій. Підтримка апаратного забезпечення передбачає ефективну роботу з процесором (процесорами/ядрами) і пам'яттю, системною платою, мережевими адаптерами, спеціалізованими CUDA-сумісними відеокартами. Цим критеріям цілком відповідає ядро операційної системи Linux, яка використовується на 95 % суперкомп'ютерів світу [7]. Крім критерію надійності роботи, варто враховувати критерій вартості, що є особливо важливим у сучасних умовах дефіциту бюджету державних технічних закладів. Зважаючи на те, що в комерційних операційних системах вартість ліцензії визначається кількістю процесорів/ядер і ємністю пам'яті ПРКС, доцільно використовувати ядро операційної системи Linux, яке відкрите і безкоштовне, а драйвери до CUDA-сумісних відеокарт є закритими комерційними, однак також безкоштовними.

Проаналізуймо необхідні програмні компоненти для створення і запуску спеціалізованого програмного забезпечення для реалізації криптоаналітичних методів у ПРКС. Оскільки основні типи даних у алгоритмах шифрування – цілочислові (шістнадцяткові, двійкові або символьні), то операції над ними (бітовий зсув, додавання і множення за модулем 2, виключне АБО) можуть бути реалізовані як асемблерні вставки в програмах, написаних мовою програмування С, яка до того ж підтримується більшістю наведених нижче бібліотек. До засобів розроблення належать: компілятор мови С – відкритий і безкоштовний компілятор GCC [8]; набір засобів розроблення проекту GNU: ld (лінкувальник), as (асемблер), ar (компресор виконуваних файлів), gprof (профайлер), gdb (відлагоджувач); засобів дослідження роботи коду: strace, valgrind, а також відкрита стандартна бібліотека мови С – glibc.

Для застосування можливостей багатоядерних процесорів і ефективного розпаралелення програм на SMP-системах доцільно використовувати технологію OpenMP [9], яка реалізована у відкритій бібліотеці GOMP. Ключовою особливістю технології OpenMP є можливість відносно нескладної модифікації С-коду вже існуючих програм для їх розпаралелювання.

Для застосування можливостей CUDA-сумісних відеокарт необхідно використати програмне забезпечення технології CUDA: драйвер CUDA-сумісної відеокарти, набір засобів розроблення – CUDA Toolkit та відповідні спеціалізовані бібліотеки. Можна також створити програмне забезпечення з підтриманням стандарту OpenCL (Open Computing Language) –

фреймворку для створення паралельних комп'ютерних програм з орієнтацією на спеціалізовані графічні та центральні процесори, які не є CUDA-сумісними.

Для взаємодії розподілених програм доцільно використовувати технологію MPI [10], зокрема її реалізацію OpenMPI – безкоштовний відкритий програмний продукт, який повністю підтримує специфікації MPI-2.

За допомогою наведених засобів можна створювати програмне забезпечення, поєднуючи технології CUDA та MPI: частини обчислювальної задачі виконуються на окремих вузлах з картами nVidia GTX 465, а обмін даними між підпрограмами відбувається передаванням повідомлень засобами MPI.

Крім засобів розроблення паралельних та розподілених програм, потрібні також спеціалізовані бібліотеки, які містять деякі набори вже реалізованих алгоритмів шифрування та базових криптографічних примітивів (режими шифрування ECB, CBC, OFB, PCBC, CBC, методи стиснення (LZO), перевірки контрольних сум (CRC32)), а саме, це бібліотека OpenSSL, набір API-функцій Linux ядра та численні утиліти, які використовуються для аудиту безпеки інформаційних систем. Вибір бібліотек OpenSSL та API-функцій ядра Linux зумовлюється великою кількістю підтримуваних криптографічних алгоритмів та протоколів, ефективністю їх роботи, кількістю застосувань, безкоштовністю та доступністю вихідного коду, що корисно при розробленні та дослідженні роботи криптоалгоритмів.

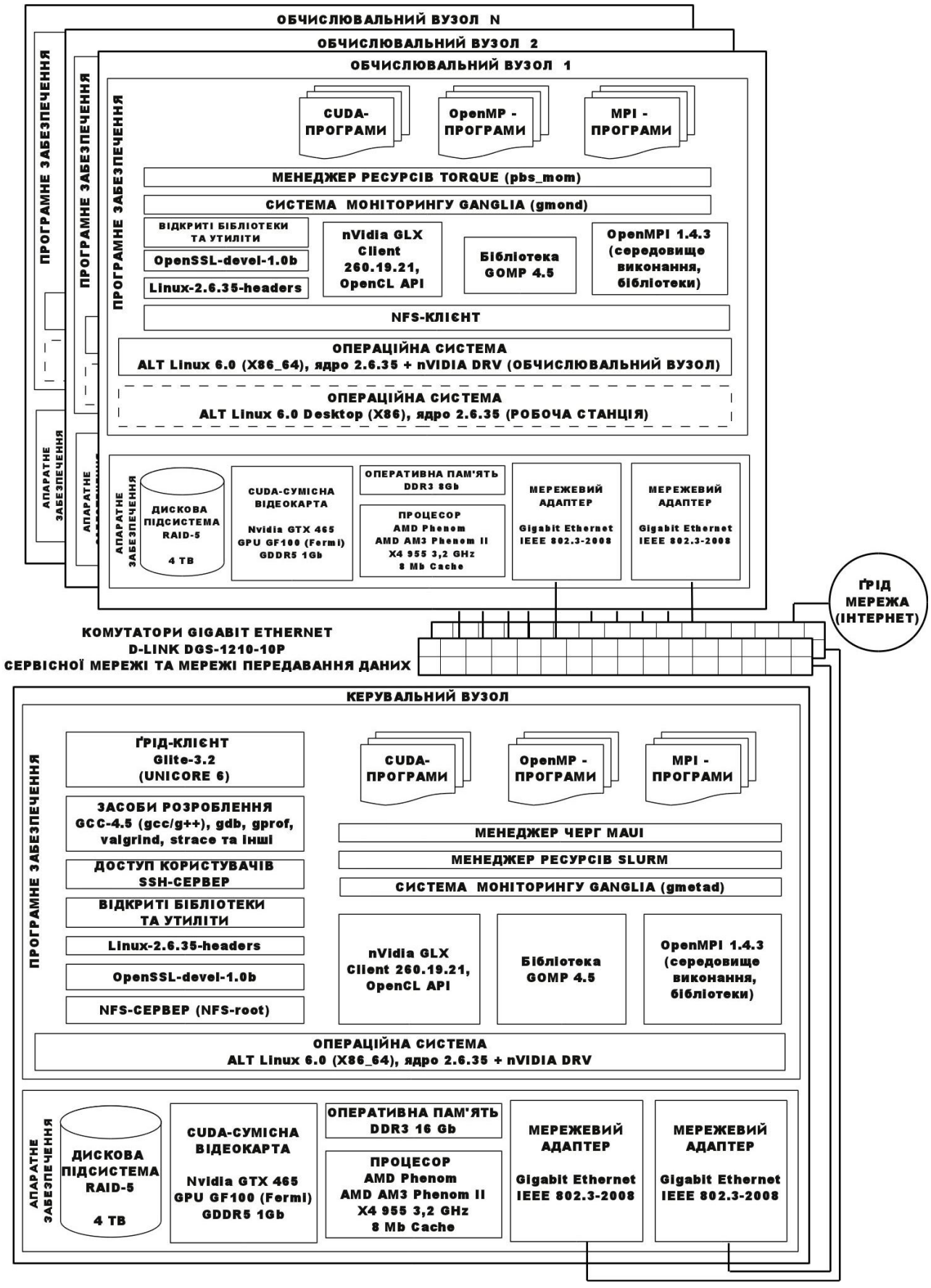
Для забезпечення критерію зручності розроблення системи криптоаналізу доцільно використати низку утиліт та бібліотек як компоненти системи криптоаналізу, оскільки вони розповсюджуються під відкритою ліцензією і мають відкритий вихідний код. До таких утиліт належать: john (реалізує атаку повного перебору на хеш-функції shadow-файлів, має підтримку OpenMP та CUDA); hydra (реалізує атаку повного перебирання на більшості сервісів віддаленого доступу), а також tcpdump, ngrep, sslscan, ssldump та інші утиліти, зокрема ті, які входять у дистрибутив BackTrack 4 [11]. Не всі з наведених утиліт паралельні, проте їх вихідний код відкритий, тому їх можна модифікувати та оптимізувати для описаних вище апаратних засобів.

Запропоновані засоби розроблення та утиліти дають змогу сформувати комплекс програм для автоматизованого криптоаналізу даних, що передаються мережами зв'язку і, таким чином, здійснювати аудит безпеки каналів зв'язку і тестування надійності криптоалгоритмів. Зокрема, розробляючи системи криптоаналізу зашифрованих даних, що передаються VPN-мережею, розробник концентрує увагу на коректній декомпозиції та розпаралеленні методу криптоаналізу, а процес перехоплення і аналізу мережевих пакетів вже реалізовано у згаданих бібліотеках та утилітах.

Для продуктивної роботи кластера необхідна низка системних утиліт для керування ресурсами кожного окремо взятого вузла і кластера загалом, зокрема, таких утиліт, як система пакетного оброблення завдань, яка включає менеджер ресурсів та черг завдань і засоби моніторингу роботи.

У створюваній системі (див. рисунок) доцільно використовувати систему пакетного оброблення завдань – SLURM та менеджер черг maui, оскільки вони добре масштабуються і відносно просто інтегруються з GPU-картами. Для моніторингу роботи кластерної системи доцільно використовувати систему веб-моніторингу Ganglia. Ganglia дає змогу переглядати завантаженість кластерної системи в режимі реального часу та статистику за певні проміжки часу за різними показниками: завантаженістю пам'яті, процесора, мережі.

Для організації ґрід-систем є велика кількість відкритого і безкоштовного проміжного програмного забезпечення (middleware): gLite, UNICORE, ARC, Globus та ін. Виконувати розподілений криптоаналіз можна в ґрід-мережі, для чого треба задіяти територіально розподілені кластери. Однак проводити моніторинг і керувати завданнями, їх координувати на розподілених кластерних системах, які використовують як засоби обчислення графічні процесори, досить складно з огляду на наведені вище аргументи.



Архітектура обчислювального кластера для криптоаналізу

Для розроблення системи криптоаналізу ключовим є питання комплексного технічного супроводу налаштованої системи, яке зводиться до наявності якісної документації, можливості поновлення пакетної бази і технічного підтримання. Для цих цілей необхідно вибрати дистрибутив, до якого б входили всі згадані програмні компоненти. На думку авторів, таким дистрибутивом є ALTLinux [12]. До того ж цей дистрибутив добре себе зарекомендував під час реалізації міждержавного російсько-білоруського проекту «СКИФ-ГРИД» і встановлений (ALT Linux Skif 4.1) на найпотужнішому на теренах СНД кластері «СКИФ Т-60» (станом на 2008 р.).

ALTLinux має великий репозитарій пакетів програм з підтриманням архітектур ×86, ×86_64 та ARM, систему керування пакетами – APT з форматом встановлюваних файлів RPM. У межах дистрибутиву розроблено унікальну за своїми можливостями систему безпечного компонування пакетів – hasher. Особлива увага приділяється захищеності операційної системи та надійності окремих її компонент.

Для тестування GPU-кластерів, які використовують технології CUDA та MPI на етапах встановлення та конфігурування, доцільно використовувати тестові програми: Matrix Algebra on GPU and Multicore Architectures (MAGMA) [13] і The Scalable HeterOgeneous Computing Benchmark Suite (SHOC) [14].

Таким чином, обґрунтоване програмне забезпечення кластерної системи є безкоштовним, відкритим і розповсюджується під ліцензіями BSD та GPL [6], крім засобів для CUDA-розробки [15].

Архітектура кластерної системи. На рисунку показано архітектуру обчислювального кластера для криптоаналізу. Працює ця система в двох режимах: 1) режимі мережі робочих станцій – завантаження відбувається з локального жорсткого диска, використовується операційна система ALTLinux Desktop 6.0 з комплектом програмного забезпечення, необхідним для здійснення навчального процесу, в навчальний час; 2) режимі кластера – завантаження відбувається по локальній мережі з nfsroot-сервера з використанням технології PXE у вихідні дні, неробочий час та під час виконання спеціалізованих лабораторних робіт.

Орієнтована швидкодія спроектованої системи визначається швидкістю CUDA-сумісної плати для різних типів операцій: з дійсними числами одинарної та подвійної точності – 847.169 Gflop/s та 106.849 Gflop/s відповідно, цілочислових операцій для 32-бітних та 24-бітних чисел: 426.211 Giop/s та 425.911 Giop/s відповідно, а також з параметрами взаємозв'язків між вузлами кластера. Пікова пропускна здатність мережі Gigabit Ethernet становить 125 Мбайт/с, а латентність – близько 150 с. Проте для реальних задач цей параметр може бути й меншим залежно від типу і кількості комунікаційного обміну між вузлами. Коефіцієнт прискорення з урахуванням ефекту розпаралелювання задачі залежить від характеру міжпроцесної взаємодії.

Висновки. Сформовано вимоги для високопродуктивного апаратно-програмного комплексу для розв'язання задач криптоаналізу в паралельних та розподілених середовищах. Здійснено вибір і обґрунтування доступних для вищого технічного навчального закладу програмно-апаратних засобів криптоаналізу, які характеризуються гнучкістю, доступністю за ціною, функціональністю та гнучкістю у процесі реалізації різних методів та різних шифрів і достатні для задач криптоаналізу. Сформовано проект ПРКС для задач криптоаналізу, проведено оцінювання його швидкодії.

Список літератури

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – СПб.: Триумф, 2002. – 816 с.
2. *Guneysu T.* Cryptanalysis with COPACOBANA / T. Guneysu, T. Kasper, M. Novotn, C. Paar, A. Puppy // IEEE TRANSACTIONS ON COMPUTERS. – 2008. – P. 1498 –1513.

3. *Dunkelm O. A* Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony / O. Dunkelm, N. Keller, A. Shamir. [Електронний ресурс]. – Режим доступу: URL: http://eprint.iacr.org/2010/013 – Назва з екрана.
4. *Боресков А. В.* Основы работы с технологией CUDA./ А. В. Боресков, А. А. Харламов. – СПб.: ДМК Пресс, 2010. – 230 с.
5. *High* Performance Computing – Supercomputing with Tesla GPUs [Електронний ресурс]. – Режим доступу: URL: http://www.nvidia.com/object/tesla_computing_solutions.html – Назва з екрана.
6. *Бойко І.* Відкрите програмне забезпечення для розробки інформаційних систем: порівняльний аналіз і перспективи розвитку в Україні / І. Бойко, С. Лупенко, А. Луцків // Комп'ютинг. – Тернопіль: Терноп. акад. народного господарства. – 2005. – Т. 4, вип. 1. – С. 99 – 106.
7. *TOP500* SuperComputer Sites [Електронний ресурс]. – Режим доступу: URL: http://www.top500.org/ – Назва з екрана.
8. *Гриффитс А.* GCC. Настольная книга пользователей, программистов и системных администраторов: пер. с англ. – М.: 000 «ТИД «ДС», 2004. – 624 с.
9. *Антонов А. С.* Параллельное программирование с использованием технологии OpenMP: учеб. пособие. – М.: Изд-во МГУ, 2009. – 77с.
10. *Антонов А. С.* Параллельное программирование с использованием технологии MPI: учеб. пособие. – М.: Изд.-во МГУ, 2004. – 71с.
11. *Back*Track Linux – Penetration Testing Distribution [Електронний ресурс]. – Режим доступу: URL: http://www.backtrack-linux.org/ — Назва з екрана.
12. *ALT* Linux Team [Електронний ресурс]. – Режим доступу: URL: http://www.altlinux.org/ – Назва з екрана.
13. *Matrix* Algebra on GPU and Multicore Architectures [Електронний ресурс]. – Режим доступу: URL: http://icl.cs.utk.edu/magma/index.html – Назва з екрана.
14. *Scalable* HeterOgeneous Computing (SHOC) Benchmark Suite [Електронний ресурс]. – Режим доступу: URL: http://ft.ornl.gov/doku/shoc/start – Назва з екрана.
15. *CUDA* Zone [Електронний ресурс]. – Режим доступу: URL: http://www.nvidia.com/object/cuda_home_new.html – Назва з екрана.

Н. В. Загородна, С. А. Лупенко, А. М. Луцкив

Обоснования выбора доступных программно-аппаратных средств высокопроизводительных вычислительных систем для задач криптоанализа

Проанализированы и обоснованы современные доступные программно-аппаратные средства криптоанализа. Сформированы требования к высокопроизводительной вычислительной системе для криптоанализа. Разработан проект кластерной системы для криптоанализа исходя из критериев гибкости, доступности, функциональности и простоты разработки.

N. V. Zagorodna, S. A. Lupenko, A. M. Lutskiv

Substantiation to choose low cost software and hardware components for highperformance compute system for cryptanalysis tasks

The article deals with the analysis and substantiation of modern low cost hardware and software tools for cryptanalysis. Requirements for high-performance computing systems for cryptanalysis are formed. The design of cluster system for cryptanalysis based on the criteria of flexibility, availability, functionality and ease of development is developed.