УДК 003.26.09:004.032.24:519.852.67

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

МОНІТОРИНГ ТА КЕРУВАННЯ ОБЧИСЛЮВАЛЬНИМИ ПРОЦЕСАМИ У СУЧАСНИХ КЛАСТЕРНИХ СИСТЕМАХ ПІД ЧАС РОЗВ'ЯЗАННЯ ЗАДАЧ КРИПТОАНАЛІЗУ

Проаналізовано особливості сучасних високопродуктивних кластерних систем, наявні методи та засоби керування обчислювальними процесами в них стосовно задач криптоаналізу. Розглянуто підходи до моделювання роботи обчислювальних кластерів з метою оптимізації керування обчислювальними процесами на основі моніторингу стану вузлів та міжвузлових з'єднань. Проаналізовано ефективність використання кластерної системи для задач криптоаналізу та запропоновано шляхи до її підвищення.

Ключові слова: криптоаналіз, моніторинг, обчислювальні кластери, керування обчислювальними процесами, GPU.

In the article the characteristics of modern high-performance cluster systems and existing methods and tools to manage computing processes in them in terms of problems of cryptanalysis are analyzed. The approaches to modeling of computing clusters to optimize the management of computing processes on the basis of monitoring nodes are proposed. The efficiency of cluster system for problems of cryptanalysis and ways to improve it are suggested.

Key words: cryptanalysis, monitoring, computing clusters, management of computing processes, GPU.

Вступ. Загальна постановка проблеми

Швидкий розвиток високопродуктивних обчислювальних систем приводить до того, що ціла низка криптографічних алгоритмів, які вважались теоретично криптостійкими декілька років тому, сьогодні такими не є. Тому при розробці нових криптографічних алгоритмів необхідно оцінити їх криптостійкість, для чого потрібно враховувати потенційні можливості високопродуктивних обчислювальних систем і оцінювати їх швидкодію та продуктивність в аспекті криптоаналізу. Ефективна робота високопродуктивної системи опрацювання даних є неможливою без ефективного керування нею. Керування передбачає планування, пріоритезацію та розподіл обчислювальних задач у відповідній паралельній та розподіленій комп'ютерній системі (ПРКС). Паралельність передбачає розподіл виконання обчислювального процесу між двома (або більше) процесорами в межах одного фізичного або одного віртуального комп'ютера, які виконуються протягом тих самих часових інтервалів. Розподіленість передбачає розподіл виконання обчислювального процесу між двома (або більше) підпроцесами, причому підпроцеси можуть існувати на тому самому обчислювальному вузлі або найчастіше виконуються на різних комп'ютерах, що зв'язуються по мережі. Ці підпроцеси можна виконувати загалом у різні часові діапазони. У межах дослідження створена ПРКС, паралельність виконання обчислювальних процесів якої забезпечується багатоядерними графічними платами, які дають змогу паралельно виконувати кілька тисяч одночасних потоків, а розподіленість — шляхом використання кількох вузлів, обладнаних графічними платами.

Зв'язок висвітленої проблеми із важливими науковими та практичними завданнями

З урахуванням наведеного вище, важливою науково-практичною задачею є оцінювання швидкості виконання того чи іншого криптоаналітичного алгоритму для певного типу алгоритмів шифрування на певній ПРКС. Крім особливостей апаратного та програмного забезпечення,

факторами, які впливають на загальну швидкодію роботи обчислювальної системи, є використання тих чи інших алгоритмів роботи системи пакетного оброблення завдань. Система пакетноого оброблення завдань використовує певні алгоритми планування доступних ресурсів для обчислювальних задач. Ефективність даних алгоритмів може відрізнятись залежно від конкретної обчислювальної задачі. Тому важливим є прогнозування необхідного часу для виконання того чи іншого криптоаналітичного алгоритму на тій чи іншій ПРКС. Таке прогнозування можна здійснювати двома способами.

Перший спосіб — емпіричний, який полягає в створенні тестових наборів, які відображають певні спрощені елементи обчислювальних задач криптоаналізу з подальшим їх виконанням на ПРКС, яка є прототипом проектованої високопродуктивної системи. Після виконання відповідних тестових наборів та оцінювання продуктивності прототипу ПРКС результати екстраполюються на реальні криптоалгоритми та формулюються вимоги до продуктивності проектованої ПРКС.

Другий спосіб — теоретичний і ґрунтується на математичній моделі ПРКС і враховує її апаратні та програмні особливості та обчислювальну задачу. На основі моделювання стає можливим розробляти ефективні алгоритми роботи планувальників завдань відповідних систем.

На думку авторів, поєднуючи наведені способи, можливо отримати бажані результати, а саме: оцінити можливості тієї чи іншої ПРКС для певної криптоаналітичної задачі та оптимізувати роботу програмного забезпечення ПРКС.

Актуальність теми зумовлена необхідністю розробки високоефективних систем криптоаналізу для дослідження сучасних систем криптографічного захисту даних. У цій роботі досліджується питання керування роботою ПРКС та її моніторингу. Оскільки апаратні засоби ПРКС постійно оновлюються, стають доступнішими, а також з’являються нові досконаліші методи криптоаналізу, тому необхідно враховути ці фактори під час організації обчислень. Отже, необхідно здійснювати моніторинг ПРКС та коригування роботи планувальника обчислювальних задач шляхом вибору ефективних алгоритмів його роботи.

Також на актуальність дослідження вказує бурхливий розвиток протягом останніх кількох років ПРКС на базі графічних карт – технології GPGPU (General Purpose computation on Graphical Processor Unit — графічні процесори для виконання задач загального призначення) [1], що дає змогу істотно підвищити продуктивність мікропроцесорної системи кластерного вузла. Також варто зазначити, що GPU-процесори показують хорошу ефективність під час роботи з цілочисельними типами даних, які є основними в криптографічних алгоритмах. Водночас системи керування ресурсами та моніторингу ПРКС не завжди повною мірою підтримують цю технологію. Отже, шляхом дослідження та вибору ефективних алгоритмів планування, шляхом моделювання ПРКС на базі GPU можна оптимізувати їх роботу та оцінити їх продуктивність з погляду криптоаналізу.

Мета і задачі дослідження. Метою дослідження є аналіз наявних математичних моделей та засобів моделювання ПРКС, створення тестових криптоаналітичних наборів, що дасть змогу здійснити верифікацію математичної моделі та провести тестування ПРКС. Дослідження роботи системи керування обчислювальними завданнями ПРКС при виконанні тестових криптоаналітичних задач шляхом її моніторингу. З урахуванням наведених вище аргументів дослідження здійснюється на ПРКС, яка обладнана GPU-платами.

Аналіз останніх досліджень та публікацій

З метою оцінювання продуктивності обчислювальної системи, якою є GPU-кластер і яка використовує технології CUDA та MPI, можна використовувати тестові програми: Matrix Algebra on GPU and Multicore Architectures (MAGMA) [2], The Scalable HeterOgeneous Computing Benchmark Suite (SHOC) [3] та тест LINPACK (HPL) [4]. Ці тестові програми використовують різноманітні математичні конструкції, чисельне розв’язання яких, як правило, є ресурсоємним, наприклад, розв’язання систем лінійних алгебраїчних рівнянь. Такий підхід дає змогу оцінити орієнтовну швидкодію ПРКС, проте має певні відмінності порівняно з задачами криптоаналізу, зокрема передбачає використання чисел з плаваючою комою, а криптографічні й відповідно криптоаналітичні алгоритми базуються на використанні цілочисельної арифметики. У результаті чого певні GPU-

плати нижчого цінового сегменту, які мають потужні процесорні засоби, але не обладнані блоками для роботи з типами даних float та double показуватимуть погані результати на вищенаведених тестах і водночас буде спостерігатись приріст швидкодії в межах криптоаналітичних задач.

Тому доцільно тестування проводити на аналогічних тестах. Одним із найпростіших способів є використання програми John the Ripper password cracker відкритого проекту Openwall [5].

Виділення проблем

Визначальним фактором в аспекті створення високопродуктивних криптоаналітичних обчислювальних систем є зменшення їх вартості та їхня загальна доступність, що забезпечується шляхом використання доступного апаратного забезпечення, зокрема багатоядерних багатовузлових кластерних систем і графічних відеоадаптерів з потужними графічними процесорами та програмного забезпечення, яке має відкритий вихідний код, шляхом використання безкоштовних засобів програмування високопродуктивних обчислювальних систем.

Тому, в контексті досліджуваної проблеми, важливими є керування та моніторинг роботи обчислювальної системи. З цією метою використовується програмне забезпечення для керування обчислювальною системою – система пакетної обробки завдань (portable batch system PBS), яка здійснює розподіл обчислювальних ресурсів та запуск завдань залежно від наявності доступних ресурсів й система моніторингу, яка дає змогу аналізувати ефективність завантаженості ПРКС.

Основним завданням проектування високопродуктивних криптоаналітичних обчислювальних систем є оптимальний вибір апаратного та правильне налаштування або модифікація програмного забезпечення з метою підвищення швидкодії при виконанні криптоаналітичних задач.

Формулювання мети

З метою створення ПРКС, що орієнтовані на виконання задач криптоаналізу, доцільно здійснювати моделювання таких обчислювальних систем з урахуванням наведених вище факторів. А математична модель повинна відображати апаратно-програмну складову та криптоаналітичний алгоритм.

Зокрема програмний засіб [5] орієнтований на методи повного перебору, а відповідно дає змогу оцінювати роботу ПРКС лише при оцінюванні теоретичної криптографічної стійкості, яка визначається перебором ключів з усієї множини можливих. До того ж ця система орієнтована на роботу з хеш-функціями.

Для апробації моделі ПРКС для задач криптоаналізу, а також тестування створеної кластерної системи, орієнтованої на розв’язання задачі криптоаналізу доцільно створити низку тестових наборів – програм тестування обчислювального GPU-кластера.

Одним із шляхів формування тестових наборів GPU-кластерів є тестування на основі тестів [2,3,4]. Проте варто зазначити, що ці тести належать до синтетичних і з метою апробації криптоаналітичних методів і адекватності для їх розв’язання спроектованої і сконфігурованої ПРКС автори пропонують створити тестові набори, які

1) включають такі криптоаналітичні методи: диференціального, лінійного та алгебраїчного криптоаналізу, метод повного перебору, тести на визначення простоти чисел (для дослідження асиметричних систем шифрування);

2) містять типові компоненти та структури даних алгоритмів шифрування та їх криптоаналітичного дослідження, зокрема: S- та P-блоків для блокових шифрів, регістрів зсуву зі зворотними зв’язками (LSFR).

Аналіз отриманих наукових результатів

Розглянемо загальні підходи до розв’язання задачі криптоаналізу в ПРКС. Оскільки криптостійкість переважної більшості сучасних криптографічних алгоритмів базується на високій просторовій (вимоги до обсягу пам’яті) та часовій (вимоги до швидкості роботи та кількості процесорних пристроїв) складностях криптоаналітичних методів, це зумовлює їх високу ресурсоємність. Як показує практика [1, 5, 6] для успішної реалізації відповідних криптоаналітичних методів доцільним є використання спеціалізованих високопродуктивних систем. Зокрема, це паралельні та розподілені комп’ютерні системи на базі технологій GPGPU (General Purposes

Graphical Processor Unit — графічних процесорів для розв'язання задач загального призначення), FPGA (Field-programmable gate array — програмованих користувачем вентильних матриць), DSP (Digital Signal Processor – цифрових сигнальних процесорів) та інших. З погляду функціональних можливостей апаратного забезпечення в задачах криптоаналізу варто виділити технології GPGPU та FGPA, що обґрунтовується наступними міркуваннями.

GPGPU базується на використанні графічних процесорів GPU (Graphical Processor Unit), які показують високу ефективність у задачах з цілочисельною арифметикою, мають високий ступінь паралелелізму, швидку оперативну пам'ять та високошвидкісні внутрішні шини обміну даними. Водночас у криптографічних алгоритмах домінуючими є операції з цілочисельними типами даних та бітовими полями з великою кількістю однотипних блоків. І очевидно, що високу ефективність ця архітектура може показати при криптоаналізі блокових шифрів.

FPGA є реконфігурованою архітектурою і дає змогу створювати апаратні функціональні блоки, що орієнтовані на реалізацію конкретних криптоаналітичних алгоритмів. Варто зазначити, що ця технологія дає змогу створювати будь-яку архітектуру ПРКС: MIMD чи SIMD, тобто формувати аналоги багатоядерних чи векторних обчислювальних систем. Очевидно, що векторні обчислювальні пристрої можуть показати високу ефективність у задачах криптоаналізу потокових шифрів, які як правило базуються на регістрах зсуву зі зворотним зв'язком.

Як правило, системи на базі GPU або FPGA об'єднуються в спеціалізовані обчислювальні мережі, формуючи кластерні або MPP-системи.

Ефективне використання апаратних засобів ПРКС забезпечується застосуванням спеціалізованого системного програмного забезпечення: засобів розробки (компіляторів та бібліотек), операційних систем та утиліт. Серед спеціалізованого системного програмного забезпечення особливу роль при моніторингу та керуванні спеціалізованими ПРКС відіграють: системи керування обчислювальними завданнями ПРКС, які забезпечують пріоритетність виконання завдань та рівномірність завантаженості елементів обчислювальної системи, а також засоби моніторингу роботи ПРКС, які дають змогу проводити аналіз статистики використання компонент ПРКС (процесорних пристроїв, пам'яті, комунікаційної підсистеми, системи зберігання даних) при здійсненні тих чи інших обчислювальних задач.

Ефективне керування запуском обчислювальних процесів у ПРКС, яке базується на моніторингу роботи компонент обчислювальної системи дає змогу оптимізувати виконання завдань криптоаналізу.

Типи криптоаналітичних методів залежать від типів криптографічних алгоритмів та їх параметрів. Важливою є модифікація існуючих алгоритмів криптоаналізу для реалізації їх у ПРКС з метою покращення їх характеристик, таких як: ступеня паралелізму, середнього ступеня паралелізму, прискорення та ефективності паралельного алгоритму, а також ступеня векторизації при використанні векторних процесорів.

Розглянемо основні етапи здійснення криптоаналізу в ПРКС.

1. Здійснюється аналіз криптографічного алгоритму, наявних вхідних даних та відомих методів криптоаналізу. На даному етапі необхідно дослідити можливість розпаралелення цих методів, якщо вони не паралельні та оцінити ефективність їх розпаралелення. Якщо вони паралельні — оцінити їх ефективність, прискорення та ступінь паралелізму. Якщо ж методи криптоаналізу відсутні або неефективні — необхідно розробити власні методи. На основі запропонованих методів розробляється паралельний алгоритм та оцінюються його параметри. Проектування паралельного алгоритму здійснюється з урахуванням можливості його масштабування.

2. Проводиться аналіз можливих апаратних та програмних засобів для реалізації та виконання криптоаналітичного алгоритму з точки зору їх оптимальності для даного типу задачі.

3. Обраний криптоаналітичний алгоритм реалізується на відповідному апаратно-програмному комплексі шляхом розробки програмного забезпечення, або й апаратних компонент. Цей етап передбачає налагодження та тестування системи.

Варто зазначити, що на першому етапі, за умови розроблення нового криптоаналітичного алгоритму важливим фактором є правильна декомпозиція обчислювальної задачі. Декомпозиція

задачі буде визначатися наявними вхідними даними та типом алгоритму: якщо алгоритм не може бути розпаралеленим, однак є багатоітераційним, то очевидно, що буде використано декомпозицію по даних, якщо ж алгоритм складається з окремих слабкопов'язних блоків, то очевидно, що буде здійснено функціональну декомпозицію.

Варто зазначити, що перший етап є тісно пов'язаний з другим етапом, оскільки орієнтований на деяку програмно-апаратну платформу і визначає тип паралелізму, який планується використати: крупнозернистий, середньозернистий чи дрібнозернистий. Цей фактор буде визначальним для ефективності розпаралелення обчислювальної задачі. Так, якщо розглядати програмно-апаратні компоненти ПРКС, то можна умовно виділити два класи: зі змінною архітектурою і з незмінною архітектурою. До першого класу належать системи на базі FPGA-контролерів, до другого — системи, архітектури яких чітко сформовані виробниками на етапі проектування, а певна їх модифікація можлива шляхом великокомпонентного формування обчислювальних мереж різних топологій. Системи, які належать до першого класу можна адаптувати до різних типів паралелізму: крупнозернистого, середньозернистого і дрібнозернистого, а в другому класі при реалізації криптоаналітичних алгоритмів необхідно дрібнозернистий паралелізм чітко пов'язувати з типовими обчислювальними пристроями або їх складовими, якими можуть виступати спеціалізовані процесори або їх ядра (що особливо актуально в GPU), а крупнозернистий паралелізм — з обчислювальними вузлами, процесорними/графічними платами або й з окремими підмережами.

На етапі тестування та налагодження доцільно здійснювати криптоаналіз спрощених шифрів: зі зменшеною кількістю раундів, меншими довжинами ключів, меншими таблицями заміщень-перестановок або меншою довжиною регістрів зсуву для потокових шифрів. Налагодження і тестування програмного забезпечення у ПРКС для задачі криптоаналізу здійснюється за допомогою системи керування обчислювальними завданнями з постійним моніторингом обчислювального процесу з метою виявлення можливих помилок та оцінювання характеристик криптоаналітичного програмного забезпечення.

Отже, ефективність криптоаналізу визначається характеристиками паралельного криптоаналітичного алгоритму, а також інтегральними показниками роботи апаратних та програмних компонент ПРКС.

За своєю суттю система керування обчислювальними завданнями ПРКС — це система масового обслуговування користувачів обчислювальної системи, яка має затримки і здійснює буферизацію нових задач, які очікують виконання. В основі роботи систем керування обчислювальними завданнями лежать алгоритми розподілу, планування та пріоритезації обчислювальних задач. Ефективність роботи цих алгоритмів є визначальною для тривалості виконання завдань та ефективності розподілу ресурсів, зокрема, при використанні ПРКС з великою кількістю обчислювальних вузлів.

Для керуванням ресурсами та чергами завдань кластерів використовуються PBS-системи, найпоширенішими відкритими з яких є такі:

1. TORQUE RESOURCE MANAGER [7] є відкритим менеджером ресурсів і джерелом забезпечення контролю над пакетною обробкою завдань і розподілених обчислювальних вузлів. Як правило він використовується разом із системою керування завданнями – MAUI CLUSTER SCHEDULER, який є відкритим програмним продуктом з можливістю підтримки різноманітних політик планування, пріоритетів і інших функціональних можливостей.

2. SLURM [8] є менеджером ресурсів із відкритим вихідним кодом, розроблений для Linux-кластерів різних масштабів. До його основних переваг належать висока масштабовність (забезпечення роботи гетерогенних кластерів до 65536 вузлів з сотнями тисяч процесорів), підтримка до 120000 завдань, доступність вихідного коду (ліцензія GNU General Public License), стійкість до збоїв системи, наявність механізму плагінів для підтримки різних систем, наявність різноманітних механізмів аутентифікації, можливість використання різноманітних планувальників завдань тощо.

Перевагою відкритого програмного забезпечення є доступ до вихідного коду PBS, що дає змогу реалізувати ефективніші алгоритми керування обчислювальними процесами, а це є особливо актуально при використанні нестандартних вузькоспеціалізованих апаратних засобів. У ході

експлуатації ПРКС та його програмного забезпечення необхідно здійснювати постійний моніторинг та оцінювання статистичних характеристик використання компонент системи, як інтегральних, так і за кожною окремою підсистемою ПРКС, зокрема:

- завантаженість процесора: загальна, окремою програмою, користувачами, простою процесора при очікуванні надходження нових даних тощо;
- використання пам'яті: кеш-пам'яті, буферів пам'яті, віртуальної пам'яті, розподіленої пам'яті тощо;
- проходження вхідного та вихідного мережевого трафіку переданого різними мережевими інтерфейсами по різних протоколах;
- характеристики спеціалізованих обчислювальних пристроїв, наприклад, при використанні GPU (рис. 1).

Для моніторингу відповідних кластерних систем, як правило, використовується відкритий програмний продукт GANGLIA [9], який є масштабованою розподіленою системою моніторингу ПРКС, таких як кластери й мережі. Вона є ієрархічною, орієнтованою на об'єднання кластерів. Ця система використовує такі технології, як XML для представлення даних, XDR для компактної портативної передачі даних і утиліти RRDtool для зберігання даних і візуалізації. Вона використовує ретельно спроектовані структури даних і алгоритми, щоб досягти дуже низьких накладних витрат і високого паралелізму. Реалізація технології є надійною, портованою під різні операційні системи та архітектури процесорів, і використовується на тисячах кластерів по всьому світу. Перевагою даної системи є відкритість програмного коду, а також зручний програмний інтерфейс (API), який дає змогу створювати додаткові модулі на мовах C та Python. Наприклад, для моніторингу роботи GPU-кластера було реалізовано відповідний модуль [10], результати роботи якого зображені на рис. 1.

Результати моніторингу можуть бути використані як вхідні дані при моделюванні ПРКС.

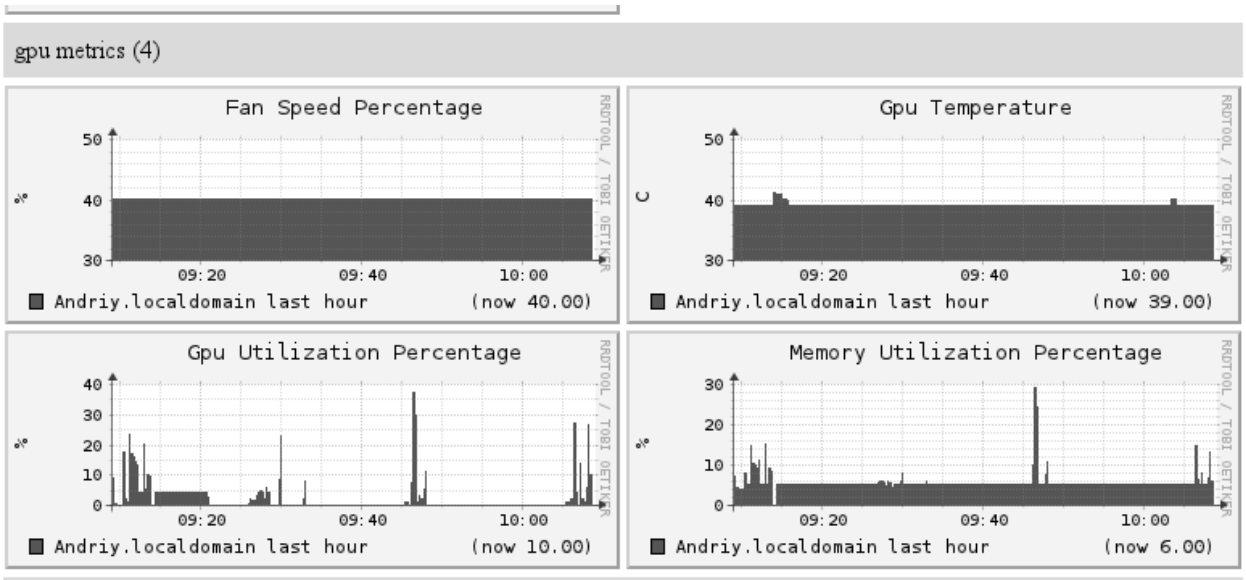

Рис. 9. Результати моніторингу GPU-плати nVidia GTX 465

Під час експлуатації обчислювальної системи необхідно оцінювати:

- продуктивність;
- надійність;
- точність опрацювання даних (послідовність, коректність результатів).

Оцінювання продуктивності системи дає змогу визначити орієнтовний час проведення обчислень. Оскільки обчислювальна система складається з деякої множини обчислювальних засобів (процесорів, спеціалізованих плат, обчислювальних вузлів тощо) з різною продуктивністю та з різними

параметрами доступу до мереж передачі даних, то керуючий вузол при формуванні та постановці на виконання обчислювальної задачі, може певним чином оптимізувати її запуск та подальше виконання, тобто, по-суті, здійснюватиме деяку оптимізацію обчислювальної системи під розв'язувану задачу.

Оцінити продуктивність ПРКС можна шляхом її математичного та імітаційного моделювання. Математична модель системи криптоаналізу на базі ПРКС повинна враховувати: наявну множину обчислювальних вузлів, множину комутаторів, множину направлених мережевих зв'язків між ними, пропускну здатність кожного мережевого з'єднання, кількість обчислювальних пристроїв (ядер), об'єми оперативної та дискової пам'яті.

Математична модель системи криптоаналізу на базі ПРКС повинна давати відомості про обчислювальну потужність кожного обчислювального ядра, загальну обчислювальну потужність обчислювальної системи, динамічні параметри кожного обчислювального вузла в певний момент часу. З метою оптимізації роботи планувальника завдань необхідно також передбачити модель його роботи.

Наведеним критеріям відповідає модель, запропонована у [11]:

$$G_T = (P, K, E, b, c, m, d, s), \tag{1}$$

де $P = \{p_1, p_2, ..., p_n\}$ – множина обчислювальних вузлів; $K = \{k_1, k_2, ..., k_z\}$ – множина комутаторів, E – множина спрямованих мережевих зв'язків між ними; $b : E \to Z_+ \cup \{0\}$ – відображення, що характеризує пропускну здатність кожного мережевого зв'язку (байт/с); $c, m, d : P \to Z_+$ визначають для кожного обчислювального вузла p_i, відповідно, кількість його обчислювальних ядер $c(p_i) = C_i$, обсяги оперативної $m(p_i) = M_i$ (кбайт) і дискової пам'яті $d(p_i) = D_i$ (кбайт); $s : P \to R_+$ для вузла p_i задає відносну продуктивність $s(p_i) = S_i$ кожного його обчислювального ядра, яка визначає, у скільки разів ядра цього вузла працюють швидше від обчислювальних ядер найнепродуктивнішого вузла кластера; p_0 – виділений вузол, на якому працює його керуюча система, не входить у множину P, але пов'язаний з усіма обчислювальними вузлами кластера з допомогою мережі керування; C_i, M_i, D_i і S_i – статичні параметри i-го вузла обчислювального кластера. До динамічних характеристик належать $u_i(t), m_i(t), d_i(t)$, які відповідно визначають завантаженість його обчислювальних ядер, обсяг доступної оперативної і дискової пам'яті в момент часу $t \in [0; +\infty)$.

Ця модель орієнтована на багатоядерні кластерні SMP-системи, проте може бути застосована для GPU кластерів з деякою модифікацією, зокрема шляхом урахування наступних особливостей GPGPU-систем у наведеній моделі наявності пам'яті та обчислювальних ядер хост-системи та GPU-плати. А також шляхом аналізу виконання обчислювального алгоритму ПСКЗ (PBS). Моделювання роботи ПСКЗ можна здійснювати за допомогою програмного продукту [12].

У таблиці наведено кількісні результати часу здійснення криптоаналізу методом повного перебору хеш-функцій (кількість можливих варіантів за секунду) за допомогою [5]. Хоча формування тестових наборів авторами ще здійснюється, проте вони вже дають змогу формувати загальні висновки про швидкодію тієї чи іншої системи, а також оцінити можливості тієї чи іншої технології в аспекті її використання до задачі криптоаналізу. У таблиці наведено результати дослідження ПРКС на базі технологій GPGPU: OpenCL та nVidia CUDA (драйвер nVidia 285.05.09).

Результати тестування ПРКС методом повного перебору

Пристрій	Технологія програмування	Назва досліджуваного алгоритму			
		MD5 (portable), операцій/с	MD5, операцій/с	SHA256, операцій/с	SHA512, операцій/с
GeForce 9600 GT	CUDA	79318	-	991	480
	OpenCL	68670	28614	-	-
GeForce GTX 465	CUDA	378000	368435	5415	2805
	OpenCL	306586	298411	-	-

Отже, отримавши результати тестування обчислювальної системи та знаючи теоретичну і практичну криптографічну стійкість, можемо оцінити час здійснення криптоаналізу певного алгоритму.

Висновки і перспективи подальших наукових розвідок

Розглянуто підходи до моделювання роботи обчислювальних кластерів у задачах криптоаналізу, що дасть змогу в подальшому оптимізувати роботу планувальника завдань ПРКС, здійснювати оцінювання часозатрат криптоаналізу в відповідній системі, оцінювати необхідні апаратні ресурси для розв'язання задачі криптоаналізу. А також наведені підходи до моделювання дають змогу спростити проектування високопродуктивних обчислювальних систем у залежності від завантаженості обчислювальних вузлів та стану мереж передачі даних.

У подальшому планується вдосконалення математичної моделі (1) з урахуванням особливостей GPU-, FPGA- та DSP-вузлів та забезпечення можливостей оцінювання теоретичної продуктивності ПРКС необхідної для розв'язання певних криптоаналітичних алгоритмів.

А в теоретичному напрямку здійснюється:

- інтегрування існуючого програмного забезпечення для моніторингу та керування ПРКС з апаратним: взаємозв'язок SLURM, GANGLIA з GPU-, FPGA- та DSP-кластером;
- проводиться розробка програмного забезпечення для моделювання роботи ПРКС на основі створеної моделі.

Перспективним є дослідження різних реалізацій апаратних та програмних засобів у рамках технології GPGPU, зокрема апаратного забезпечення відеоакселераторів AMD (ATI) та відповідно APP SDK, а також програмних засобів OpenCL. Іншим перспективним напрямком є моделювання обчислювальних процесів та обчислювальних систем на базі грід-мереж [13].

На цьому етапі дослідження авторами здійснюється розробка тестових криптоаналітичних наборів, які дають змогу здійснювати криптоаналіз не лише методом повного перебору, а й іншими методами, зокрема лінійним, диференціальним та алгебраїчним [6].

1. Загородна Н. В., Лупенко С. А. Луцків А. М. Обґрунтування вибору доступних програмно-апаратних засобів високопродуктивних обчислювальних систем для задач криптоаналізу. // Електроніка та системи управління. 2011. № 1(27). – К.: НАУ, 2011. – С.42–50. 2. Matrix Algebra on GPU and Multicore Architectures [Електронний ресурс]. – Режим доступу: URL: http://icl.cs.utk.edu/magma/index.html — Назва з екрану. 3. Scalable HeterOgeneous Computing (SHOC) Benchmark Suite [Електронний ресурс]. – Режим доступу: URL: http://ft.ornl.gov/doku/shoc/start – Назва з екрана. 4. CUDA Accelerated Linpack On Clusters [Електронний ресурс]. – Режим доступу: URL: http://www.nvidia.com/content/GTC-2010/pdfs/2057_GTC2010.pdf – Назва з екрана. 5. John the Ripper password cracker [Електронний ресурс]. – Режим доступу: URL: http://www.openwall.com/john/ — Назва з екрана. 6. Загородна Н. В., Лупенко С. А. Луцків А. М. Сучасні алгебраїчні криптоаналітичні методи систем захисту мереж передачі даних // Матеріали першої науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя "Інформаційні моделі, системи та технології". – Тернопіль: ТНТУ, 2011. – 37 с. 7. TORQUE Resource Manager [Електронний ресурс]. – Режим доступу: URL: http://www.clusterresources.com/products/torque-resource-manager.php — Назва з екрану. 8. SLURM: A Highly Scalable Resource Manager [Електронний ресурс]. – Режим доступу: URL: https://computing.llnl.gov/linux/slurm/slurm.html — Назва з екрану. 9. Ganglia Monitoring System [Електронний ресурс]. – Режим доступу: URL: http://ganglia.sourceforge.net/ — Назва з екрана. 10. Monitoring nVidia GPU metrics with Ganglia [Електронний ресурс]. – Режим доступу: URL: http://agaoglu.tumblr.com/post/3074180322/monitoring-nvidia-gpu-metrics-with-ganglia — Назва з екрана. 11. Полежаев П.Н. Планирование задач для вычислительного кластера с учетом сети и многопроцессорности узлов // Параллельные вычислительные технологии (ПаВТ'2011): труды международной научной конференции (Москва, 28 марта – 1 апреля 2011 г.) [Электронный ресурс] – Челябинск: Издательский центр ЮУрГУ, 2011. – 730 с. – URL: http://omega.sp.susu.ac.ru/books/conference/PaVT2011. 12. Slurm Simulator – Barcelona Supercomputing Center [Електронний ресурс]. – Режим доступу: URL: http://www.bsc.es/plantillaA.php?cat_id=705 — Назва з екрана. 13. Загородна Н. В., Лупенко С. А. Луцків А. М. Особливості створення GRID-систем на основі GPU-вузлів для розв'язання задач криптоаналізу // Вісник Нац. ун-ту "Львівська політехніка". Інформаційні системи та мережі . №699. – Львів: Вид-во Львівської політехніки, 2011. – С. 302–320.