# Дослідження криптостійкості алгоритму KASUMI на доступних високопродуктивних обчислювальних засобах

Ю.О. Кондрацький, С.А. Лупенко, А.М. Луцків

*Ternopil Ivan Pul`uj National Technical University, Ruska str., 56, Ternopil, Ukraine*

l.andriy@gmail.com

**Анотація.** *У роботі описано розробку системи криптоаналізу блокового симетричного алгоритму KASUMI. Для криптоаналізу використано відомий метод «сендвіч-атаки». У результаті аналізу даного криптоаналітичного методу запропоновані способи підвищення швидкості його виконання шляхом декомпозиції обчислювальної задачі та її розподілу між обчислювальними засобами. Програмне забезпечення орієнтоване на використання в обчислювальних системах зі спільною та розподіленою пам'яттю, зокрема на доступні високопродуктивні апаратно-програмні засоби, до яких належать кластерні та метакластерні (грід) системи.*

## Ключові слова

Криптоаналіз, «сендвіч-атака», обчислювальні кластери, KASUMI

## 1 Вступ

Симетричний блоковий алгоритм шифрування KASUMI має різні сфери застосування, зокрема використовується у мережах передачі даних стандартів UMTS, GSM, GPRS та інших. Загалом алгоритм KASUMI теоретично може використовуватись для безпосереднього шифрування даних, що передаються. У стандарті UMTS він використовується в алгоритмах забезпечення цілісності (UEA1) та конфіденційності (UIA1) [1].

Надійність криптоалгоритму визначається його криптостійкістю. Виділяють поняття теоретичної криптографічної стійкості, яка вказується розробниками шифру і, як правило, є кількістю можливих варіантів значень ключа при методі повного перебору. Також, виокремлюють поняття практична криптографічна стійкість алгоритму шифрування, яка визначається на основі застосування відомих, більш ефективних, аніж повний перебір методів. Теоретична криптостійкість KASUMI становить $2^{128}$, а практична визначається найефективнішою криптоаналітичною атакою, відомою на сьогодні - «Сендвіч-атака з пов'язаними ключами» [2]. Згідно з літературними джерелами даний метод носить теоретичний характер й бути реалізований відносно реальної системи передавання даних не може, оскільки передбачає наявність великої кількості вхідних даних. Варто також зазначити, що описані методи криптоаналізу досить часто носять теоретичний характер й оцінки їх складності, як і реалізовність, доцільно перевіряти на практиці, тому важливим є реалізувати створені криптоаналітичні методи на відповідних обчислювальних засобах.

## 2 Аналіз алгоритму «сендвіч-атаки з пов'язаними ключами»

Коротко розглянемо даний метод криптоаналізу з точки зору його декомпозиції. «Сендвіч-атака» належить до типу диференціальних атак. Вона базується на «бумеранг-атаці», що розглядає шифр як каскад з двох субшифрів. «Сендвіч-атака» розглядає алгоритм як каскад з трьох субшифрів.

У «сендвіч-атаці» здійснено поділ шифру на три субшифри, $E=E_1+M+E_0$. Припущення такі ж як і в «бумеранг-атаці»: нехай існує диференціал пов'язаних ключів $\alpha \rightarrow \beta$ для $E_0$ з різницею ключів $\Delta K_{ab}$ з ймовірністю p, і диференціал пов'язаних ключів $\gamma \rightarrow \delta$ для $E_1$ з різницею $\Delta K_{ac}$ з ймовірністю q. Алгоритм атаки є

таким же як і в базовій атаці (ігнорування центрального субшифру M). Проте, аналіз є детальнішим і потребує великої уваги при розгляді залежностей між різними розподілами.

Ключовою ідеєю «сендвіч-атаки» є перехід середини. В базовій «бумеранг-атаці», якщо пара ($P_a$, $P_b$) є правильною парою по відношенню до першого диференціалу, і обидві пари ($C_в$, $C_c$) і ($C_b$, $C_d$) є правильними парами по відношенню до другого диференціалу, то отримується наступна залежність:

$$(X_a \oplus X_b = \beta) \wedge (X_a \oplus X_c = \gamma) \wedge (X_b \oplus X_d = \gamma) ,$$

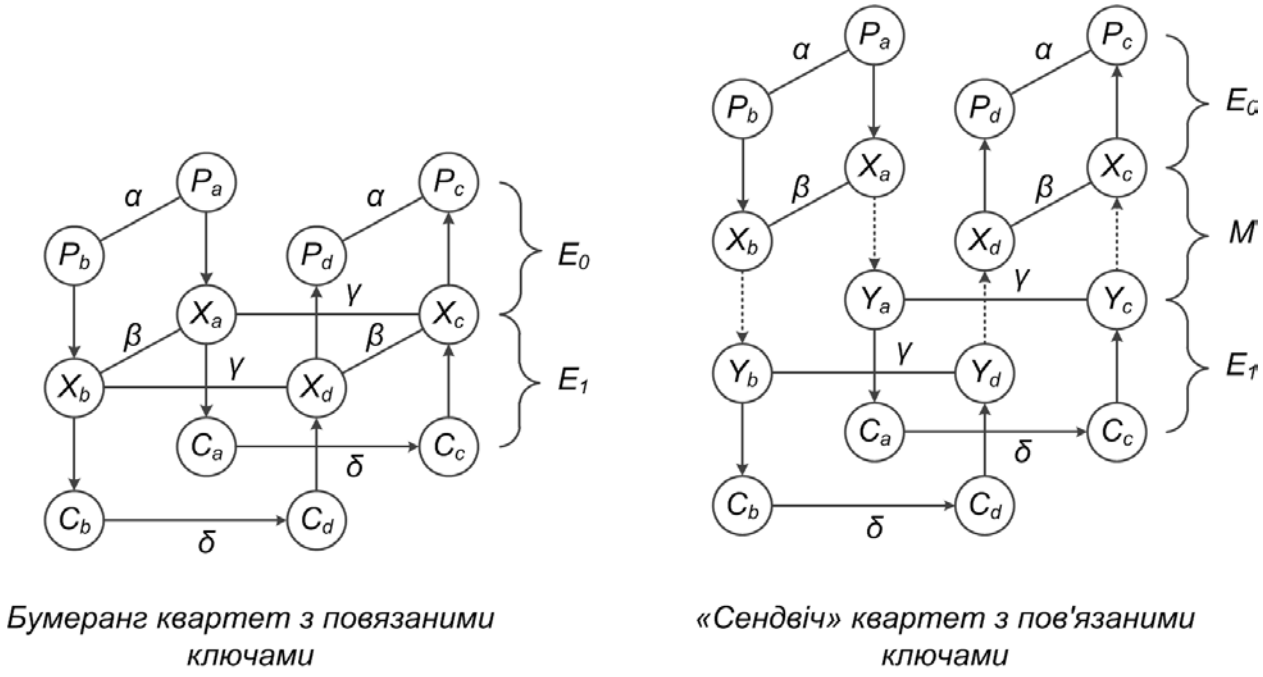
де $X_i$ – проміжне значення шифрування $P_i$.

Тоді

$$X_c \oplus X_d = (X_c \oplus X_a) \oplus (X_a \oplus X_b) \oplus (X_b \oplus X_d) = \beta \oplus \gamma \oplus \gamma = \beta ,$$

у результаті $P_c \oplus P_d = \alpha$ з ймовірністю p (рис. 1). У випадку «сендвіч-атаки», отримуємо:

$$(X_a \oplus X_b = \beta) \wedge (Y_a \oplus Y_c = \gamma ) \wedge (Y_b \oplus Y_d = \gamma) .$$




*Бумеранг квартет з повязаними ключами*

*«Сендвіч» квартет з пов'язаними ключами*

Рисунок 1 – Конструкції бумеранг та сендвіч квартетів

Розглянемо основні етапи алгоритму й виділимо найресурсоємніші ділянки алгоритму, які будуть в більшій мірі визначати необхідні потреби в часі та пам'яті. «Сендвіч-атака» з пов'язаними ключами на повний KASUMI складається з 4 етапів, як показано на рисунку 4.2.

Перший етап алгоритму представляє собою планування пов'язаних ключів, очевидно що дана процедура не потребує великих часових затрат, тобто її можна опустити при оцінці.

Другий етап – збір даних, тобто проводиться генерування вхідних даних та їх аналіз. Дані квартети отримуються шляхом проведення операцій шифрування та дешифрування з пов'язаними ключами. Часова складність в цьому випадку становить $2^{26}$, тобто $2^{25}$ – на знаходження $C_b$ з $C_a$, а також $2^{25}$ – на знаходження $C_d$ з $C_c$. Дані зберігаються в асоціативних структурах, типу хеш-таблиці, що дає змогу проводити в них швидкий пошук. Тому часом на проведення пошуку можемо знехтувати.

На третьому етапі проводиться аналіз квартетів, тобто використовуючи правильні квартети та припущені значення частини ключа, знаходимо інші частини вихідного ключа. Оскільки, правильні квартети мають одне і те ж значення, то часозатратність даної операції дуже мала.

На четвертому етапі проводиться повний перебір 32-х біт ключа і часова складність даної операції становить $2^{32}$.

Отже, загальна часова складність буде дорівнювати $2^{26} + 2^{32}$. Оскільки, $2^{26}$ значно менше, ніж $2^{32}$, то можна сказати, що часова складність алгоритму криптоаналізу дорівнює $2^{32}$.

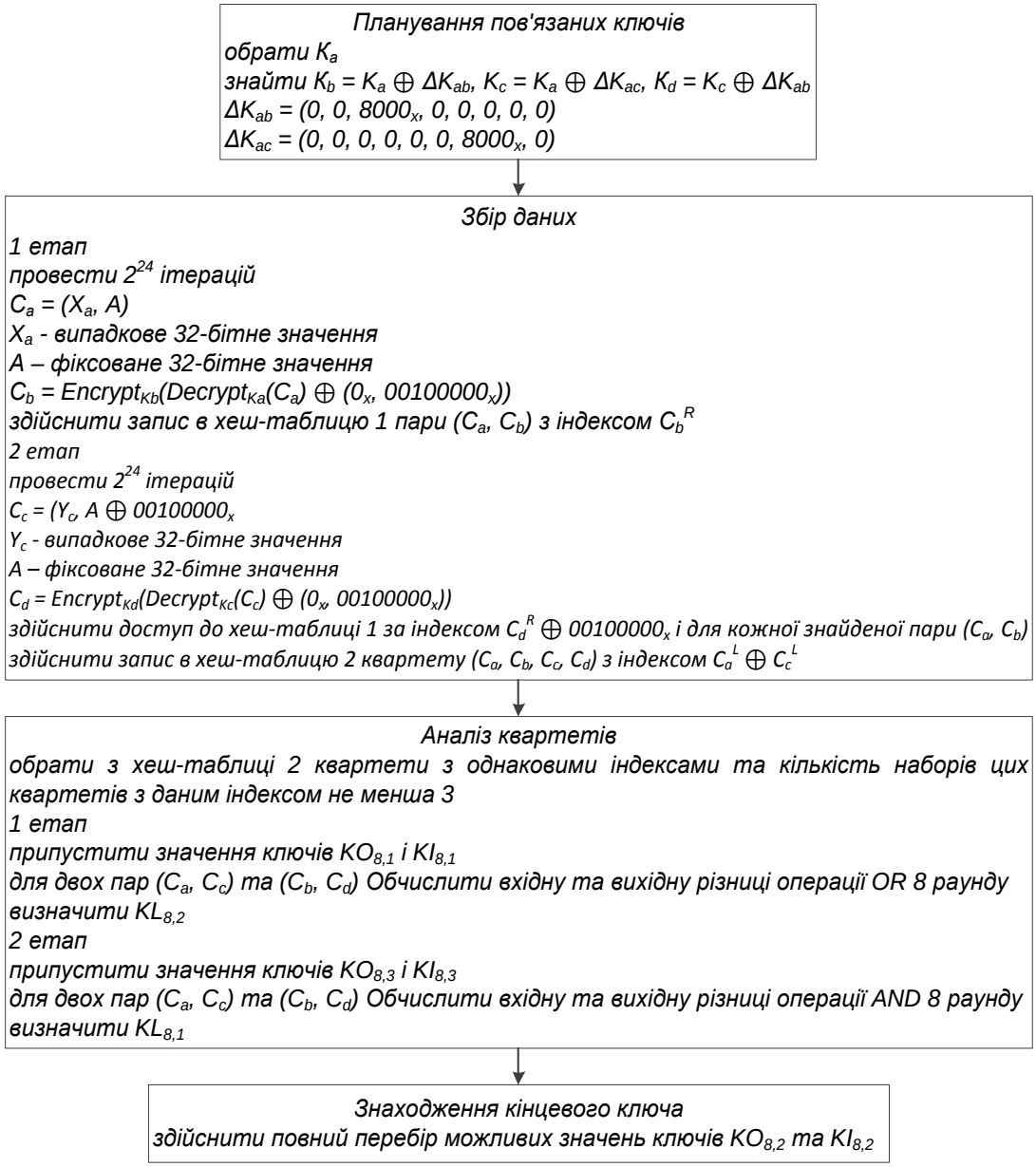



Рисунок 2 – Схема криптоаналітичної атаки

При оцінюванні вимог до пам’яті слід врахувати пам'ять для вихідних даних та пам'ять для оперування ними. Очевидно, що визначальним буде значення об’єму пам'яті для вихідних даних, тобто складність даних – $2^{26}$. Необхідний об’єм пам’яті буде складати $2^{30}$ байт, тобто $2^{26}$ пар відкритих текстів/шифротекстів, де кожна пара займає 16 байт.

# 3 Програмна реалізації криптоаналітичної системи

Описаний алгоритм криптоаналізу реалізовано з використанням технології MPI та OpenMP, тобто орієнтовано на використання у системах з розподіленою пам’яттю (кластер з багатоядерними обчислювальними вузлами) [4]. Критеріями при виборі технології програмування були доступність обчислювальних засобів та універсальність технології програмування, що дає змогу використовувати створене алгоритмічне та програмне забезпечення на звичайних Beowulf-кластерах.

Проведені експерименти показали зниження часозатрат для здійснення криптоаналізу. Згідно проведених тестувань, при використанні технології OpenMP та типового набору вхідних даних, ідентифікація правильних квартетів відбувається з ймовірністю 0,76, при використанні MPI та збільшенні набору вхідних даних — 0,94. Виконання обчислювальної задачі показало, що середній час здійснення криптоаналізу алгоритму KASUMI методом «сендвіч-атаки» (пошук квартету) становить приблизно 30-40хв для одного тестового набору вхідних

даних (кожний набір вхідних даних опрацьовується SMP-системою, яка є вузлом кластера). Кластер загалом опрацьовує близько 100 наборів вхідних даних.
Таким чином дане програмне забезпечення є орієнтованим на кластерні системи й ефективно може бути застосоване в мета-кластерних системах (грід). Також, на думку авторів, більшої ефективності можна досягти шляхом використання технології GPGPU. Особливістю даної технології є її невисока вартість і відносна простота розробки. На сьогодні створенням спеціалізованих обчислювальних пристроїв на основі GPU займається низка компаній, зокрема nVidia, яка розробила технологію CUDA. Варто зазначити, що обчислювальні можливості мають не лише спеціалізовані плати, типу nVidia Tesla GPU Modules, а також звичайні відеокарти nVidia, які можуть бути використані як пристрої для обчислень. Хоча, у найдешевших CUDA-сумісних відеокартах є невеликий об'єм оперативної пам'яті і модулі для роботи з дійсними типами даних (числа з плаваючою комою) відсутні, проте для задач криптоаналізу вони цілком придатні, оскільки в цих задачах домінуючими є операції з цілочисельними типами даних та бітовими полями. Також дані плати мають високошвидкісну шину обміну даними між ядрами графічних процесорів та вбудованою високошвидкісною пам'яттю.
Альтернативою технології GPGPU з точки зору швидкодії є використання програмованих логічних інтегральних схем (ПЛІС) [5]. Основною перевагою ПЛІС у порівнянні з GPGPU є висока швидкодія при опрацюванні великих потоків даних. ПЛІС дає змогу змінити архітектуру обчислювальної системи в залежності від обчислювальної задачі, а в GPGPU цього зробити неможливо. 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 практичної точки зору, якщо обчислювальна задача не передбачає апаратної реалізації у вигляді окремого пристрою і не критична до обробки в режимі реального часу, то використання графічних процесорів буде суттєво дешевшим у порівнянні з ПЛІС-системами. Таким чином, на даний час авторами здійснюється оптимізація криптоаналітичного програмного забезпечення для його використання на GPGPU-системах — технологія nVidia CUDA.

# 4 Висновки та перспективи подальших досліджень

Реалізоване паралельне програмне забезпечення жодним чином не компрометує системи передавання даних на основі стандарту UMTS, проте дає змогу досліджувати надійність низки її криптографічних компонент, які забезпечують цілісність та конфіденційність даних, що передаються шляхом використання алгоритму шифрування KASUMI. У роботі показано, що розпаралелення обчислювальної задачі криптоаналізу дає змогу підвищити її ефективність — зменшити час здійснення криптоаналізу, а також підвищити його достовірність.
При створенні сучасних криптоаналітичних систем доцільним також є проведення порівняльного аналізу різних програмно-апаратних засобів паралельних та розподілених комп'ютерних систем з метою визначення найбільш ефективних на різних етапах криптоаналітичної атаки. Такий аналіз дасть змогу розробляти ефективніші криптоаналітичні алгоритми для інших симетричних блокових шифрів.

# Перелік посилань

[1] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".
[2] Dunkelman O. A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony / Orr Dunkelman, Nathan Keller, Adi Shamir // Weizmann Institute of Science 10 January 2010 [Електронний ресурс]. – Режим доступу: URL: http://eprint.iacr.org/2010/013.pdf — Назва з екрану.
[3] Encrypt the given plain text with the given key using the KASUMI block cipher [Електронний ресурс]. – Режим доступу:URL: http://people.rit.edu/aar3301/Kasumi.java – Назва з екрану.
[4] 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). - К.: НАУ, 2011. - с.42-50.
[5] Мельник А. О. Персональні суперкомп’ютери: архітектура, проектування, застосування. Монографія./ А. О. Мельник, В. А. Мельник // Львів: Видавництво Львівської політехніки, 2013. 516 с.