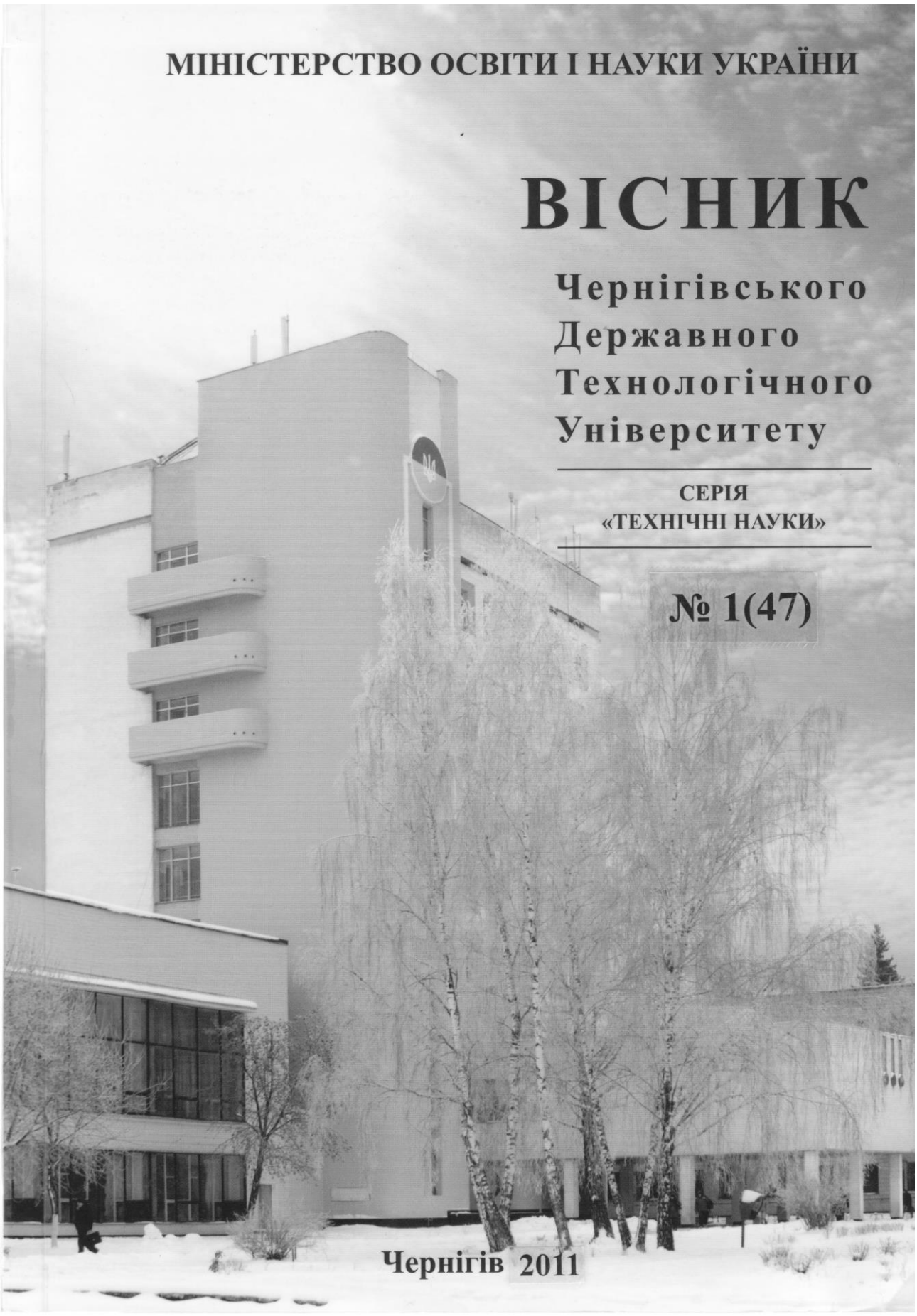
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

# ВІСНИК

## Чернігівського Державного Технологічного Університету

СЕРІЯ
«ТЕХНІЧНІ НАУКИ»

№ 1(47)



Чернігів 2011

УДК 004.274

**О.В. Цулун**, магістрант
**А.І. Роговенко**, ст. викладач
Чернігівський державний технологічний університет, м. Чернігів, Україна

# АРХІТЕКТУРА КРИПТОГРАФІЧНОГО АКСЕЛЕРАТОРА З МОЖЛИВІСТЮ ЗМІНИ КРИПТОГРАФІЧНОГО АЛГОРИТМУ

*Проведено огляд існуючих криптографічних акселераторів. Запропонована архітектура криптографічного акселератора, яка дозволяє змінювати апаратно реалізовані криптографічні алгоритми, інтегрувати акселератор в процесорні системи з різними системними магістралями і забезпечує скорочення часу виконання криптографічних операцій.*

## Постановка проблеми

На даний час із збільшенням обсягу конфіденційної інформації, що передається через всесвітні мережі, зростанням вимог до швидкості шифрування, ресурсоємності криптографічних алгоритмів і появою різних комп'ютерних систем, що виконують шифрування, підвищуються вимоги, що висуваються до криптографічного акселератору [1]. Актуальними є задачі прискорення виконання криптографічних операцій; отримання з мінімальними часовими і апаратними витратами криптографічного акселератора з певним набором реалізованих криптографічних алгоритмів та його інтеграції у процесорні системи з різними системними магістралями.

У статті наводиться постановка і рішення задачі скорочення часу виконання криптографічних операцій; інтеграції криптографічного акселератора у різні процесорні системи, а також зміни криптографічних алгоритмів без зміни архітектури самого акселератора.

У роботі наведено вирішення актуальних прикладних задач, що дають суттєвий економічний ефект: зменшення витрат часових ресурсів на виконання криптографічної задачі; мінімальні апаратні і часові витрати на інтеграцію криптографічного акселератора в потрібну процесорну систему, а також на зміну криптографічних алгоритмів, реалізованих криптографічним акселератором.

Пропонуються архітектурні рішення, що дозволяють інтегрувати криптографічний акселератор у системи з різними системними магістралями і реалізовувати необхідні криптографічні алгоритми з мінімальними апаратними і часовими витратами, а для скорочення часу виконання криптографічної задачі використовувати її паралельне виконання на рівні обчислювального блоку.

## Аналіз досліджень і основних публікацій

Проаналізувавши низку сучасних криптографічних пристроїв таких як Sun Crypto Accelerator 6000 [2], Broadcom BCM 5840 [3], Amphion Semiconductor CS5210-40 [4], Cryptonite [5], Cryptomaniac [6], HiFn 8200 Series Services Processor [7] можна зробити висновок що існуючі криптографічні акселератори не вирішують ряду поставлених завдань:

Завдання 1 – Прискорення виконання криптографічних задач шляхом паралельного виконання на рівні обчислювальних блоків.

Завдання 2 – Інтеграція криптографічного акселератора в різні процесорні системи.

Завдання 3 – Реалізація потрібного набору криптографічних алгоритмів.

Сучасні криптографічні акселератори не підтримують паралельне виконання криптографічних задач, або підтримують паралельне виконання на рівні кількох плат. Недоліком даного методу є значне використання ресурсів процесорної системи [2].

Існуючі рішення мають архітектурні особливості для прискорення виконання певного набору алгоритмів. При необхідності змінити алгоритми на інші потрібно змінювати всю архітектуру [3, 4, 5].

Криптографічні акселератори передбачають підключення лише до певних процесорних систем. Способи обміну даними з процесорними системами є неефективними, оскільки використовують значну частину часового ресурсу процесора [6, 7].

Наприклад, найбільш розповсюдженим є обмін через пам'ять криптографічного акселератору, який полягає у необхідності зовнішньої процесорної системи читати дані із своєї пам'яті та записувати дані у пам'ять криптографічного акселератору. Результат записується у пам'ять криптографічного акселератору, після чого зовнішня процесорна система повинна прочитати результат із пам'яті криптографічного акселератору. Недоліком даного способу обміну є затрата часових ресурсів зовнішньої процесорної системи на передачу криптографічної задачі акселератору та на отримання результату, затрата апаратних ресурсів на забезпечення криптографічного акселератору пам'ятю.

У роботі пропонується: прискорити виконання криптографічних задач і скоротити використання ресурсів процесорної системи за рахунок паралельного виконання задач на рівні обчислювальних блоків; забезпечити інтеграцію криптографічного акселератора в різні процесорні системи за рахунок змінюваного зовнішнього інтерфейсу і незмінного внутрішнього; забезпечити мінімальні витрати на отримання потрібного набору криптографічних алгоритмів за рахунок єдиного інтерфейсу підключення спеціалізованих обчислювачів до криптографічного акселератора.

**Формування цілі статті**

Метою є дослідження можливості зміни апаратно реалізованих криптографічних алгоритмів акселератора, а також його інтеграції в різні процесорні системи та скорочення часу виконання криптографічних операцій.

**Виклад основного матеріалу дослідження**

Проведені дослідження для виявлення залежності кількості тактів на виконання криптографічної задачі від кількості банків буферів і обчислювальних блоків. Дослідження являли собою моделювання роботи криптографічного акселератора, що виконує шифрування блоку інформації 4048 байтів алгоритмом 3DES, при різній кількості обчислювальних блоків та банків буферів. Дослідження проводилися за допомогою пакету MATLAB, інструментів Simulink і Stateflow. Результати досліджень представлені на рисунку 1.

На данному рисунку результат I – кількість тактів на виконання шифрування при одному блоці 3DES з одним банком буферів. Результат II – кількість тактів на виконання шифрування при двох блоках 3DES з одним банком буферів. Результат III – кількість тактів на виконання шифрування при одному блоці 3DES з двома банками буферів. Результат IV – кількість тактів на виконання шифрування при двох блоках 3DES з двома банками буферів.

Виходячи з результатів досліджень, можна зробити висновок, що збільшення кількості обчислювальних блоків до двох призводить до зменшення числа тактів на виконання шифрування на 46 %.

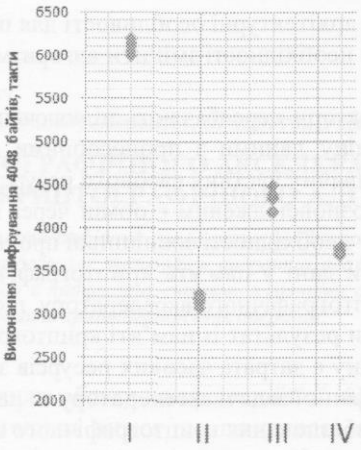



*Рис. 1. Залежність кількості тактів на виконання криптографічної задачі від кількості банків буферів і обчислювальних блоків*

При одному обчислювальному блоці криптографічного алгоритму і двох банках буферів досягається зменшення числа тактів на виконання шифрування на 25 %, що пояснюється відсутністю очікування обчислювальним блоком надходження даних.

При двох обчислювальних блоках і двох банках буферів зменшення числа тактів на виконання шифрування становить 38 %. Збільшення швидкодії виявляється менше, ніж при двох обчислювальних блоках і одному банку вхідних і вихідних буферів. Це пояснюється тим, що при збільшенні числа обчислювальних блоків і банків буферів дані не встигають поступити в буфери своєчасно і обчислювальні блоки чекають їх надходження.

Звідси можна зробити висновок, що для виконання алгоритмів, які не можуть виконуватися паралельно, краще збільшити кількість банків буферів. Для алгоритмів, що можуть виконуватися паралельно, краще збільшити кількість обчислювальних блоків, при цьому кількість буферів збільшувати не варто.

Архітектура криптографічного акселератора представлена на рисунку 2.

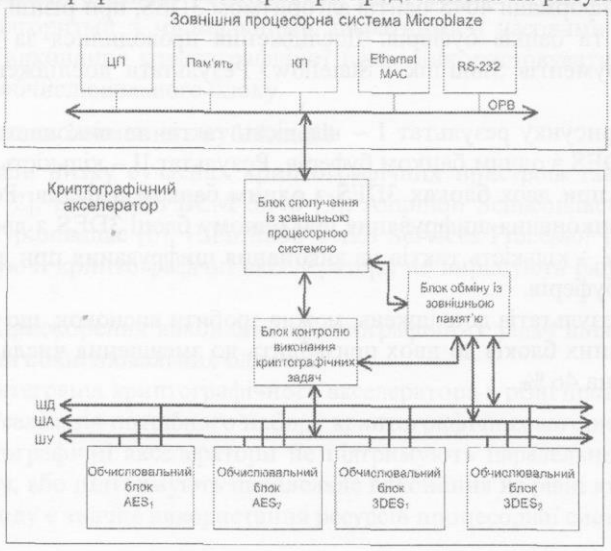



*Рис. 2. Архітектура криптографічного акселератора*

Прискорення виконання криптографічних задач може бути досягнуто в результаті їх паралельного виконання на рівні обчислювальних блоків і паралельного виконання однієї задачі кількома обчислювальними блоками.

Пропонується використовувати алгоритм контролю виконання задач, який буде опитувати стан кожного з обчислювальних блоків і на підставі отриманої інформації приймати рішення з яким з них взаємодіяти в даний момент і які операції виконувати.

Особливістю обчислювального блоку є контролер, який, виконуючи операції взаємодії з криптографічним акселератором, забезпечує незалежність обчислювачів від особливостей криптографічного акселератора і дозволяє зосередити архітектуру обчислювача на виконання алгоритму з найбільшим швидкодією.

Для забезпечення мінімальних витрат на отримання потрібного набору криптографічних алгоритмів використовуються обчислювальні блоки, що мають єдиний інтерфейс роботи з іншими блоками криптографічного акселератору.

Структура обчислювального блоку представлена на рисунку 3.

Скорочення використання ресурсів процесорної системи та прискорення обміну даними досягається використанням пам'яті зовнішньої процесорної системи для обміну даними та передачею команд у пам'ять криптографічного акселератора. Для запобігання конкуренції на шині використовуються двопортова пам'ять. Передача команд, обмін службовою інформацією відбувається через міст сполучення з шиною зовнішньої процесорної системи.

Структура взаємодії з зовнішньої процесорної системою представлена на рисунку 4.

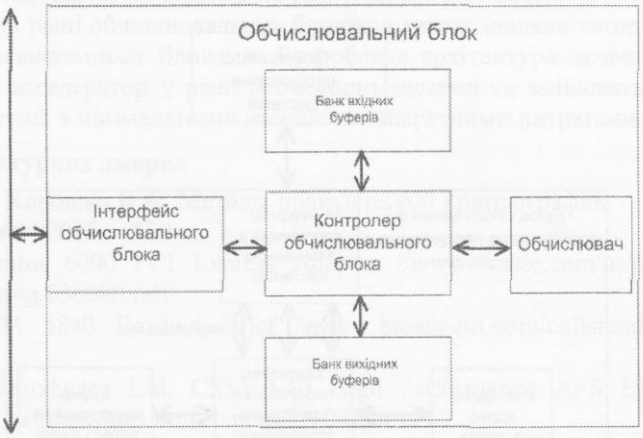



*Рис. 3. Структура обчислювального блоку*

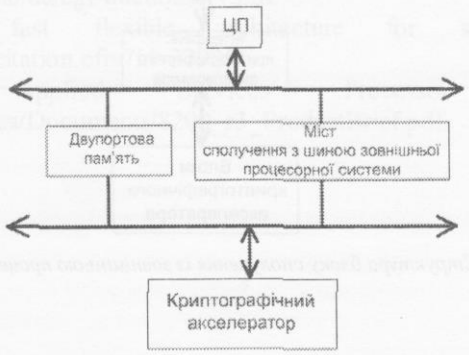



*Рис. 4. Структура взаємодії з зовнішньої процесорної системою*

Інтеграція криптографічного акселератора в різні процесорні системи реалізується шляхом заміни блоку сполучення із зовнішнім процесорної системою.

Структура блоку сполучення із зовнішньою процесорною системою представлена на рисунку 5.

Даний блок буде мати змінний зовнішній інтерфейс і незмінний внутрішній, а також забезпечуватиме перетворення адреса і даних, використовуваних у процесорній системі. Таким чином, для інтеграції в іншу процесорну систему достатньо змінити лише цей блок, зміни ніяк не відіб'ються на архітектурі інших блоків.

Для перевірки пропонованих рішень був реалізований криптографічний акселератор на мові VHDL. Була створена бібліотека обчислювальних блоків і блоків сполучення для інтеграції у софт процесори Microblaze і LEON3.

Залежність кількості тактів на шифрування блоку даних 4048 байтів 3DES алгоритмом від кількості обчислювальних блоків представлена на рисунку 6. На даному рисунку результат I – кількість тактів на виконання шифрування при одному блоці 3DES, результат II – кількість тактів на виконання шифрування при двох блоках 3DES, результат III – кількість тактів на виконання шифрування при трьох блоках 3DES. Виходячи з графіка, можна зробити висновок, що кількість тактів, необхідних на виконання шифрування блоку даних зменшилася на 46 % при двох обчислювальних блоках і на 59 % при трьох обчислювальних блоках.

Результати, отримані в процесі налагодження криптографічного акселератора на згаданих процесорах, підтверджують ефективність вищеописаних рішень.

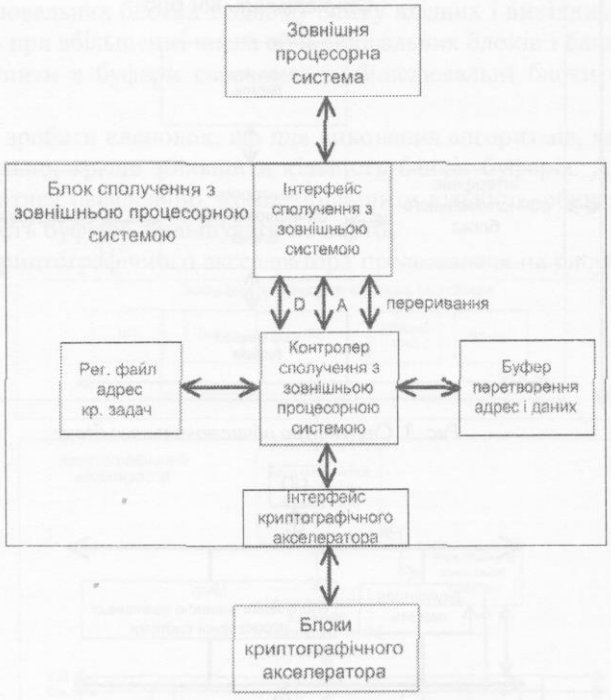



*Рис. 5. Структура блоку сполучення із зовнішньою процесорною системою*

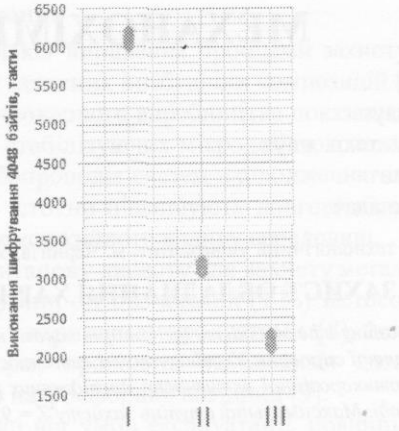



*Рис. 6. Залежність кількості тактів на шифрування блоку даних 4048 байтів 3DES алгоритмом від кількості обчислювальних блоків*

**Висновки**

Проведений огляд архітектурних особливостей існуючих криптографічних акселераторів, виявлено їх суттєві недоліки. Показана актуальність поставлених задач і запропоновані їх рішення. Запропонована архітектура криптографічного акселератора дозволяє зменшити число тактів на виконання криптографічної задачі за рахунок паралельного виконання на рівні обчислювальних блоків, а також завдяки алгоритму розподілу задач між обчислювальними блоками. Розроблена архітектура дозволяє інтегрувати криптографічний акселератор у різні процесорні системи та змінювати набір криптографічних алгоритмів з мінімальними часовими і апаратними витратами.

**Список літературних джерел**

1. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К.: ООО Полиграф-Консалдинг, 2005. – 500 с.
2. Crypto Accelerator 6000 PCI Express Adapter //www.oracle.com/us/products/servers-storage/networking/036080.pdf.
3. Broadcom BCM 5840 Product Brief //www.broadcom.com/collateral/pb/1250-PB11-R.pdf.
4. Amphion Semiconductor Ltd. CS5210-40 High Performance AES Encryption Cores //www.chipfind.net/datasheet/conexant/cs521040.htm.
5. Cryptonite. A Programmable Crypto Processor Architecture For High-Bandwidth Applications //www.deposit.d-nb.de/cgi-bin/dokserv.pdf.
6. Cryptomaniac: A fast flexible architecture for secure communication //www.portal.acm.org/citation.cfm?id=379256.
7. 8200 Series Applied Services Processor Product Brief //www.cn.exar.com/Files/Documents/8200_r3_ProductBrief.pdf.