Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
https://www.nv.nltu.edu.ua
https://doi.org/10.36930/40320210
Article received 22.02.2022 p.
Article accepted 28.04.2022 p.
UDC 004.31

ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

@ Correspondence author
A. Ya. Davletova
a7davletova@gmail.com

А. Я. Давлетова
Західноукраїнський національний університет, м. Тернопіль, Україна

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК ЛОГІЧНОГО ЕЛЕМЕНТА "ПРОВІДНЕ І" ЯК ПРИШВИДШУВАЧА ОПЕРАЦІЙ ДОДАВАННЯ У ПРОЦЕСОРАХ ШИФРУВАННЯ ДАНИХ

Проаналізовано характеристики апаратної та часової складностей базових, двоходових, логічних елементів, що є основою для проектування складних цифрових пристроїв, компонентів обчислювальних засобів, спецпроцесорів аналого-цифрового та цифрового опрацювання сигналів. Встановлено, що найскладнішою мікроелектронною реалізацією характеризується логічний елемент "Виключне АБО", що відповідно зумовлює високу часову затримку виконання арифметико-логічних операцій. Запропоновано спрощення структури та мікроелектронної реалізації логічного елемента "Виключне АБО". Реалізовано логічний елемент "Провідне І" на трьох логічних елементах І-НЕ та АБО, що виконує функцію логічного елемента "Виключне АБО". Це забезпечує зменшення апаратної складності у 2-3 рази. Використання емітерно-зв'язаної логіки (ЕЗЛ) (англ. *Emitter Coupled Logic*, ECL) передбачає наявність транзисторів на виходах логічних елементів та дає змогу об'єднувати їх виходи без втрати функцій. Це сприяє підвищенню швидкодії спрацювання за 1 мікротакт, тобто у 3 рази, порівняно з класичною реалізацією логічного елемента "Виключне АБО". Використання логічного елемента "Провідне І", як компоненти однорозрядних суматорів, дасть змогу підвищити їх продуктивність. Запропоновано вдосконалення однорозрядних неповних та повних двійкових суматорів, на підставі оптимізованого логічного елемента "Провідне І". Подано розрахунки та побудовано графіки оцінок часової та апаратної складностей запропонованих схемотехнічних рішень суматорів. Наведені діаграми ілюструють підвищення швидкодії та спрощення структури поданих базових компонентів процесорів порівняно з відомими. Визначено широку сферу застосування розроблених пришвидшувачів: у системах захисту інформації, багаторозрядних комбінаційних та пірамідальних суматорах з пришвидшеними переносами, пристроїв сортування двійкових чисел, визначення Хемінгової віддалі між сигналами та багато інших. У задачах шифрування даних швидкодія спецпроцесора принципово залежить від швидкодії його компонентів, а заміна операцій множення багаторозрядних чисел операціями додавання, з використанням теоретико-числового базису (ТЧБ) Радемахера-Крестенсона, на етапах генерації ключів, шифрування та дешифрування дає змогу значно зменшити часову складність залежно від розрядності параметрів алгоритмів шифрування.

Ключові слова: логічний елемент; однорозрядний суматор; апаратна складність; швидкодія виконання операції; спецпроцесор.

Вступ / Introduction

Для представлення чисел у комп'ютерних системах найчастіше використовується двійкова система числення теоретико-числового базису (ТЧБ) Радемахера. Тому тривалість виконання арифметичних операцій у двійковій системі, загалом, залежить від суматорів, основних функціональних компонентів та, зокрема, внаслідок формування та розповсюдження наскрізних переносів. Перспективним напрямом вдосконалення алгоритмів захисту даних в комп'ютерних системах є реалізація розпаралелення потоків даних на підставі системи залишкових класів ТЧБ Крестенсона. Тому заміна операції множення багаторозрядних чисел операцією додавання у ТЧБ Радемахера-Крестенсона дає змогу зменшити обчислювальну складність та збільшити швидкодію процесорів шифрування даних.

У задачах шифрування даних швидкодія спецпроцесора принципово залежить від швидкодії його компонентів, а заміна операцій множення багаторозрядних чисел операціями додавання, з використанням ТЧБ Радемахера-Крестенсона, на етапах генерації ключів, шифрування та дешифрування дає змогу значно зменшити часову складність залежно від розрядності параметрів алгоритмів шифрування. Тому вдосконалення засобів обчислювальної техніки, які застосовуються у системах захисту даних, є актуальною науково-технічною задачею.

Постановка задачі та мети дослідження. Важливим компонентом арифметико-логічних пристроїв високопродуктивних процесорів є однорозрядні неповні та повні суматори. Аналіз наявних схемотехнічних рішень побудови таких суматорів [20] показує, що їх апаратна та часова складності змінюється відповідно у границях 3-12 елементи та 1-5 мікротактів. Відомі структури неповних і повних однорозрядних суматорів характеризуються великою апаратною складністю та низькою швидкодією. Ці недоліки за використання таких

Інформація про автора:
Давлетова Аліна Ярославівна, викладач, кафедра спеціалізованих комп'ютерних систем. **Email:** a7davletova@gmail.com; https://orcid.org/0000-0002-1192-2532

Цитування за ДСТУ: Давлетова А. Я. Дослідження характеристик логічного елемента "Провідне І" як пришвидшувача операцій додавання у процесорах шифрування даних. Науковий вісник НЛТУ України. 2022, т. 32, № 2. С. 61–67.
Citation APA: Davletova, A. Ya. (2022). Investigation of the characteristics of the logical element "Leading I" as an accelerator of addition operations in data encryption processors. *Scientific Bulletin of UNFU*, 32(2), 61–67. https://doi.org/10.36930/40320210

суматорів у багаторозрядних комбінаційних суматорах, наприклад у 1024-бітних процесорах шифрування даних, призводять до відповідної значної апаратної складності їх реалізації.

Нагадаємо, логічний елемент – пристрій, призначений для оброблення інформації в цифровій формі (послідовності сигналів високого – '1' і низького – '0' рівнів у двійковій логіці, послідовність '0', '1' та '2' – в трійковій логіці, послідовності '0', '1', '2', '3', '4', '5', '6', '7', '8' та '9' – в десятковій логіці). Фізично логічні елементи можуть бути виконані механічними, електромеханічними (на електромагнітних реле), електронними (на діодах і транзисторах), пневматичними, гідравлічними, оптичними та ін. способами. Логічні операції (булева функція) своє теоретичне обґрунтування отримали в математичній логіці. Логічні операції з одним операндом називаються унарними, з двома – бінарними, з трьома – тернарними і т. д.

Удосконалення засобів обчислювальної техніки, зокрема пришвидшувачів обчислювальних операцій типу додавання, множення, піднесення до квадрата, модулярного експоненціювання дає змогу реалізувати складніші алгоритми опрацювання цифрових даних. Важливим напрямом вирішення цього класу задач є оптимізація системних характеристик пришвидшувачів виконання операції додавання, синтез схемотехнічних рішень двійкових суматорів із гранично мінімальними параметрами апаратної та часової складностей, що дасть змогу істотно покращити характеристики складних компонентів обчислювальних засобів як аналого-цифровий перетворювач, АЦП (англ. *Analog-to-digital converter*, ADC), арифметико-логічний пристрій, АЛП (англ. *Arithmetic Logic Unit*, ALU), багаторозрядних суматорів, квадраторів, швидкодіючих перемножувачів, проблемно-орієнтованих процесорів шифрування даних та ін.

Об'єкт дослідження – розроблення компонентів засобів обчислювальної техніки.

Предмет дослідження – методи вдосконалення елементарної бази цифрової обчислювальної техніки, які забезпечують можливість підвищення швидкодії, зменшення апаратної складності та спрощення задач цифрового опрацювання сигналів.

Мета роботи – дослідити характеристики логічного елемента "Виключне АБО" та "Провідне І" як пришвидшувача виконання операцій у процесорах шифрування даних, використання якого як компонента забезпечить оптимізацію системних характеристик обчислювальних засобів та дасть змогу підвищити їх продуктивність.

Для досягнення зазначеної мети потрібно визначити такі *основні завдання дослідження*: систематизувати базові компоненти пристроїв обчислювальної техніки; визначити перспективи покращення системних характеристик логічного елемента "Виключне АБО"; синтезувати структуру та системні характеристики логічного елемента "Провідне І"; схемотехнічно реалізувати структури однорозрядних двійкових суматорів покращеними системними характеристиками.

Матеріали та методи дослідження. В основу методів побудови універсальних і спеціалізованих процесорів покладено фундаментальні засади здійснення алгоритмів виконання обчислювальних арифметико-логічних та комунікаційних операцій. Фундаментальні основи теорії елементної бази, функціональних і структурних компонентів універсальних цифрових процесорів і спецпроцесорів викладено у роботах відомих учених і спеціалістів у галузі цифрової техніки та мікроелектроніки [3, 14, 17, 24, 25] О. В. Палагіна, В. К. Задіраки, В. П. Боюна, О. В. Дрозда, Я. М. Николайчука та ін.

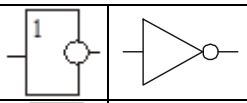
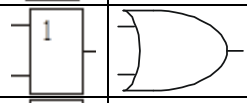
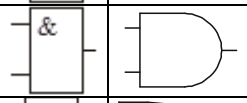
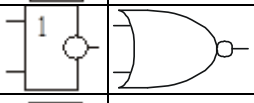
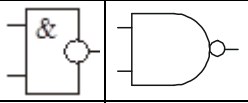
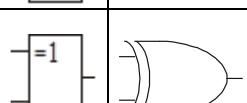
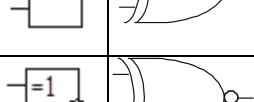
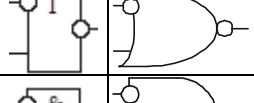
Аналіз останніх досліджень та публікацій. У роботі [15] наведено критерії ефективності методів і схемотехнічних рішень спецпроцесорів і застосування оцінок апаратної, часової та структурної складностей. Отримані результати в роботі [22] можуть бути покладені в основу побудови високопродуктивних спецпроцесорів генерації ключів асиметричних криптосистем. Наведені теоретичні основи [8] методів знаходження залишків багаторозрядних чисел Мерсена в ТЧБ Радемахера на підставі операції додавання, що дає змогу зменшити часову складність алгоритму пошуку. У роботі [19] описано методи та дослідження можливості збільшення швидкодії алгоритмів криптографічного захисту в ТЧБ Радемахера-Крестенсона на підставі математики арифметичних дій непозиційної системи числення залишків. Запропонований у роботі [23] метод виправлення пакетних помилок на підставі модульних кодів корекції на підставі модульних коригувальних кодів, що можуть бути реалізовані проблемно-орієнтованими спецпроцесорами шифрування даних. У роботі [4] описано принципи реалізації структур спецпроцесорів сортування даних, що містить схему порівняння на підставі суматора. У роботі [1] наведено фундаментальні основи цифрової електроніки та найновіші цифрові технології. У роботі [9] запропоновано способи оптимізації характеристик суматорів, що є компонентами спецпроцесорів шифрування даних.

Проведений аналіз показує, що арифметична операція додавання є базовою для алгоритмів опрацювання сигналів та обчислень у системах захисту інформації. Ця операція та компоненти, які її реалізують, є вагомим компонентом, який істотно впливає на продуктивність, апаратну та структурну складності спеціалізованих процесорів шифрування даних. Тому вдосконалення базових елементів, суматорів двійкової системи числення є важливою задачею для оптимізації їх системних характеристик та досягнення максимальної швидкодії.

Результати дослідження та їх обговорення / Research results and their discussion

1. Класи та системні характеристики логічних елементів, які є елементарними одиницями структур обчислювальних засобів. Базовими елементами сучасних обчислювальних засобів, мікропроцесорів, мікроконтролерів та спецпроцесорів, які реалізуються на підставі вбудованих кристалів та програмовано логічних інтегральних схем, ПЛІС (англ. *Programmable Logic Device*, PLD) і застосовуються та широкомасштабно тиражуються у програмно-апаратних комплексах, системах автоматичного управління та захисту даних, є логічні вентилі, логічні елементи та однорозрядні неповні та повні двійкові суматори. У табл. 1 наведено умовні позначення та системні характеристики апаратної (A) та часової (τ) складностей базових, двовходових, логічних елементів, які реалізуються засобами мікроелектроніки, що випускаються відомими фірмами Altera, Integrated Device Manufacturers, Xilinx і Lattice, та ін.

Табл. 1. Графічні позначення логічних елементів і їх системні характеристики / Graphical notation of logical elements and their system characteristics

№	Назва операції	Назва елемента	Умовне графічне позначення	*A*	τ
1	Інверсія	НЕ, NOT		1	1
2	Диз'юнкція	АБО, OR		1	1
3	Кон'юнкція	І, AND		1	1
4	Заперечення диз'юнкції	АБО-НЕ, NOR (NOT OR)		2	2
5	Заперечення кон'юнкції	І-НЕ, NAND (NOT AND)		2	2
6	Еквівалентність	Виключне АБО (сума по модулю 2), XOR (EXCLUSIVE OR)		5	3
7	Заперечення еквівалентності	Виключне АБО-НЕ, XNOR (EXCLUSIVE NOT OR)		5	3
8	Імплікація	ЯКЩО, ТО		3	3
9	Заборона	ЗАБОРОНА		3	3

На діаграмі (рис. 1,*a*) показано характеристики апаратної та часової складностей наведених у табл. 1 логічних елементів (1-9 номер логічного елементу).

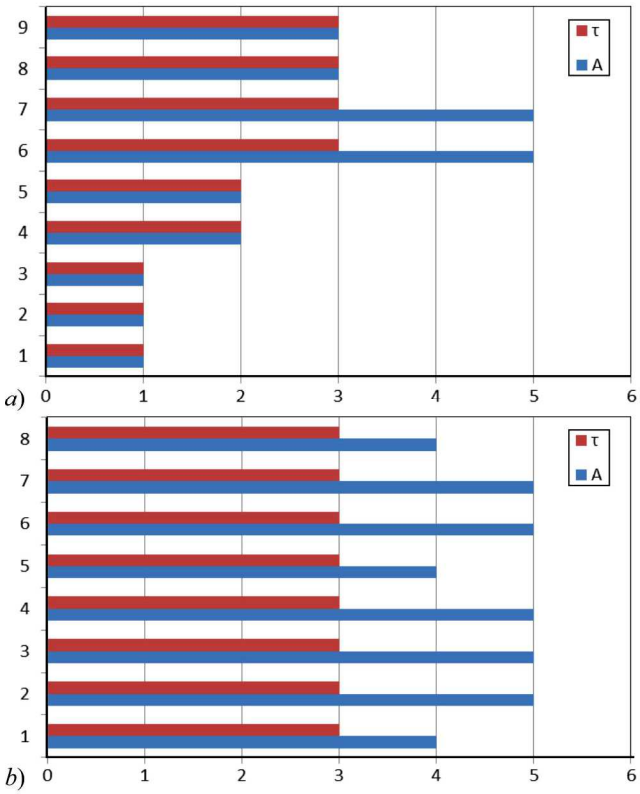
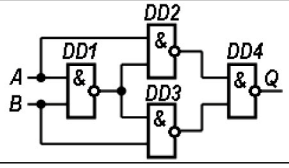
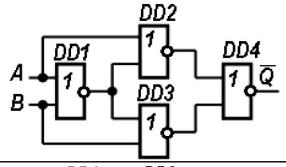
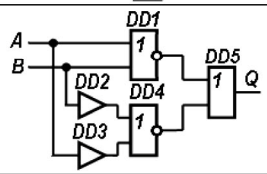
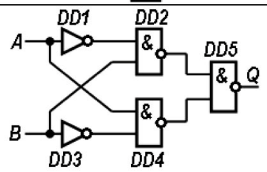
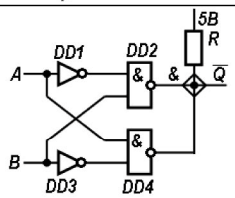
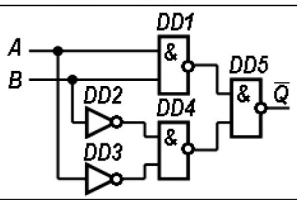
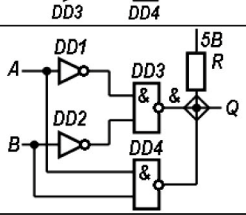
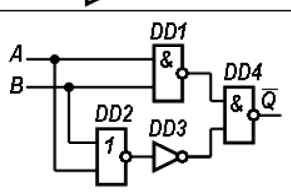


Рис. 1. Характеристики апаратної та часової складностей: *a*) логічних елементів; *b*) логічного елемента "Виключне АБО" / Characteristics of hardware and time complexity: *a*) of logical elements; *b*) of the logical element "Exclusive OR"

Серед названих логічних елементів найскладнішу мікроелектронну реалізацію має логічні елементи "Виключне АБО" та "Виключне АБО-НЕ". Вони характеризуються у 3-4 рази більшою апаратною складністю відносно інших логічних елементів. Класичну реалізацію таких елементів [2] наведено в табл. 2, де їх реалізацію здійсннено за допомогою таких логічних елементів, як І, АБО, НІ.

Табл. 2. Класична реалізація логічних елементів "Виключне АБО" / Classic implementation of logical elements "Exclusive OR"

№ п/п	Реалізація	*A*	τ	№ п/п	Реалізація	*A*	τ
1		4	3	5		4	3
2		5	3	6		5	3
3		5	3	7		5	3
4		5	3	8		4	3

Логічний елемент, що реалізує функцію "Виключне АБО", широко застосовується у цифрових функціональних пристроях комбінаційного типу, тому їх характеристики взаємозалежні. На діаграмі (рис. 1,*b*) показано характеристики апаратної та часової складностей наведених у табл. 2 елементів.

Аналіз діаграм (див. рис. 1,*b*) показує, що логічний елемент "Виключне АБО" характеризується високою апаратною складністю, оскільки він містить 4-5 логічних елементів, з яких 3 з'єднані послідовно і затримка сигналів становить не менше 3 мікротактів та приводить до зниження швидкодії та зростання апаратної складності одноразрядних двійкових суматорів.

Приклади масового застосування логічного елемента "Виключне АБО" у структурах багаторозрядних суматорів [10] кореляційних і спектральних [18] спецпроцесорів, спецпроцесорів визначення функцій Хеммінгового простору у задачах прийняття рішень [11], швидкодіючих багаторозрядних аналого-цифрових перетворювачів [21], а також багаторозрядних процесорів шифрування даних [12] визначають перспективу покращення системних характеристик логічного елемента "Виключне АБО". При цьому істотно спрощується проектування утиліт на кристалах ПЛІС. Зменшується у 3-4 рази число задіяних вентилів, а також знижуються характеристики тепловиділення кристалів.

2. Синтез структури та системні характеристики логічного елемента "Провідне І". Використання логічних елементів, реалізованих на мікроелектронній технології емітерно-зв'язаної логіки (ЕЗЛ), передбачає наявність транзисторів на виходах логічних елементів І-НЕ та АБО, що дає змогу об'єднувати їх виходи без втрати функцій [15].

Запропоноване спрощення мікроелектронної реалізації логічного елемента "Виключне АБО" на логічних елементах І-НЕ та АБО, виходи яких об'єднані і реалізують логічний елемент "Провідне І", наведено на рис. 2. Число компонентів реалізованого логічного елемента становить 2*v* (вентилі), а тривалість затримки сигналів – 1 *t* (мікротакт).

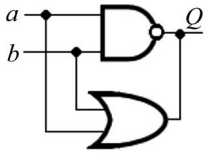


Рис. 2. Мікроелектронна реалізація логічного елемента "Провідне І" / Microelectronic implementation of the logical element "Leading I"

Запропонований логічний елемент "Провідне І", що реалізує функцію "Виключне АБО", порівняно з відомими мікроелектронними реалізаціями, характеризується зменшенням кількості логічних елементів до двох, тобто у 2-3 рази меншою апаратною складністю та підвищенням швидкодії спрацювання за 1 мікротакт, тобто у 3 рази порівняно з класичною реалізацією. Застосування такого елемента можливе як компоненти одноразрядного напівсуматора (рис. 3), який реалізований за допомогою 3 логічних І-НЕ, АБО та І, два з яких утворюють елемент "Провідне І". Таке рішення дає змогу отримати швидкодіючий одноразрядний напівсуматор з часовою затримкою сигналів на виходах суми та переносу в 1 мікротакт та зменшеною апаратною складністю до трьох логічних елементів.

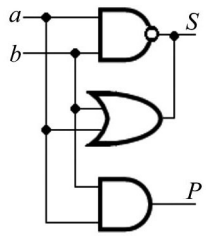


Рис. 3. Структура одноразрядного двійкового напівсуматора / The structure of a single-bit binary half-adder

Запропонований напівсуматор працює так. При подачі на входи напівсуматора логічних значень $a = 0$ та $b = 0$ на виході логічного елемента І-НЕ формується сигнал "1" одночасно на виході логічного елемента АБО формується "0", що відповідає сигналу $S = 0$. При цьому на виході переносу логічного елемента І формується сигнал "0". При подачі на вхід напівсуматора логічних значень $a = 1$ та $b = 1$ на виході логічного елемента І-НЕ формується сигнал "0" одночасно на виході логічного елемента АБО формується "1", що відповідає сигналу $S = 0$. При цьому на виході переносу логічного елемента І формується сигнал "1". При подачі на входи напівсуматора логічних значень $a = 1$ та $b = 0$ або $a = 0$ та $b = 1$ на виході логічного елемента І-НЕ формується сигнал "1" одночасно на виході логічного елемента АБО формується "1", що відповідає сигналу $S = 1$. При цьому на виході переносу логічного елемента І формується сигнал "0".

3. Синтез структур одноразрядних двійкових суматорів на підставі логічного елемента "Провідне І". Класична структура повного одноразрядного суматора (рис. 4) [1] з прямими входами та виходами містить 2 послідовно з'єднані логічні елементи "Виключне АБО", які складаються з 4-5 логічних елементів І, АБО, НЕ, логічних елементів І та АБО.

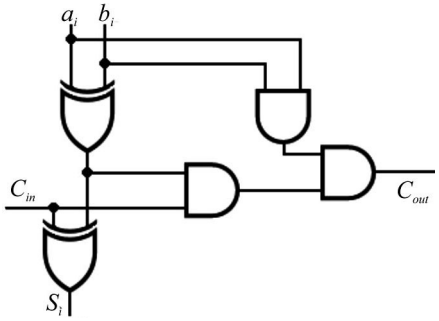


Рис. 4. Класична реалізація повного одноразрядного двійкового суматора / Classic implementation of a full single-bit binary adder

Апаратна складність таких суматорів становить $A = 11 - 13v$, залежно від реалізації логічного елемента "Виключне АБО". Також вони мають низьку швидкодію, оскільки містять два послідовно з'єднані логічні елементи "Виключне АБО", що приводить до затримки сигналів $\tau_{Si} = 6\upsilon$ та $\tau_{Cout} = 2 \vee 5\upsilon$.

Для реалізації вдосконаленого повного одноразрядного двійкового суматора (рис. 5) успішно можна використати запропонований логічний елемент "Провідне І".

Системні характеристики цього суматора такі: апаратна складність $A = 7v$, часова затримка сигналів після виходу суми $\tau_{Si} = 2\upsilon$ та після виходу переносу $\tau_{Cout} = 2\upsilon$. На підставі структури одноразрядного неповного суматора (див. рис. 3), де застосований логічний

елемент "Провідне І", запропоновано схемотехнічну реалізацію структури повного однорозрядного суматора (рис. 6) [16].

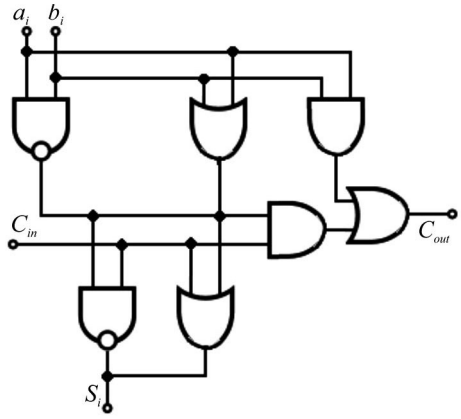


Рис. 5. Повний однорозрядний суматор з прямими входами та виходами / Full single-bit adder with direct inputs and outputs

Структура цього суматора відрізняється від відомих наявністю інверсних входів $\overline{C_{in}}$ та інверсних виходів $\overline{C_{out}}$, що дає змогу забезпечити мінімальну затримку сигналів наскрізних переносів $\tau_{Cout} = 1\upsilon$, сигналу суми $\tau_{Si} = 2\upsilon$, характеризується зменшеною апаратною складністю $A = 8\nu$ порівняно з класичною реалізацією.

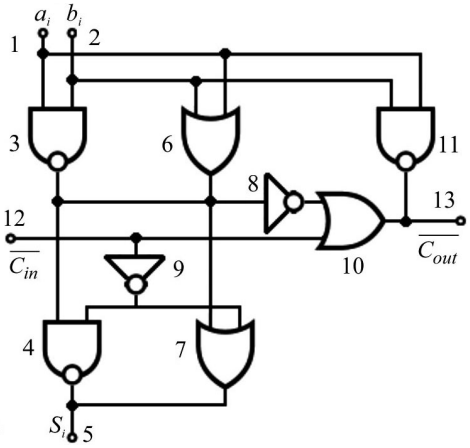


Рис. 6. Повний однорозрядний суматор з інверсними входами та виходами / Full single-bit adder with inverse inputs and outputs

Запропонований повний однорозрядний суматор працює так. При подачі на входи a_i та b_i логічних значень "0" або "1" на монтажно з'єднаному виході першого логічного елемента І-НЕ та першого логічного елемента АБО зі затримкою на 1 мікротакт формується логічний сигнал, який відповідає модульній сумі $a_i \oplus b_i$, який надходить на перші входи другого логічного елемента І-НЕ, другого логічного елемента АБО та першого логічного елемента НЕ. При появі на інверсному вході переносу $\overline{C_{in}}$ логічного значення "0" або "1", який інвертується у прямий сигнал переносу на виході другого логічного елемента НЕ, на виході суми пристрою формується логічне значення S_i, яке відповідає прямому виходу суми повного однорозрядного суматора. Інверсні сигнали, які формуються на виході першого логічного елемента НЕ та входу переносу $\overline{C_{in}}$ на виході третього логічного елемента АБО, згідно з правилом Де-Морана булевої алгебри $\overline{S} \vee \overline{C_{in}} = \overline{S \wedge S_{in}}$ формують сигнал інверсії їх кон'юнкції, який на виході монтажного з'єднання з третім логічним елементом І-НЕ, реалізує функцію логічного елемента "Виключаюче АБО" та формує інверсне логічне значення біта переносу $\overline{C_{out}}$ на його виході, який є другим виходом однорозрядного суматора.

На рис. 7 наведено діаграму апаратної та часової складностей розглянутих повних однорозрядних двійкових двійкових суматорів.

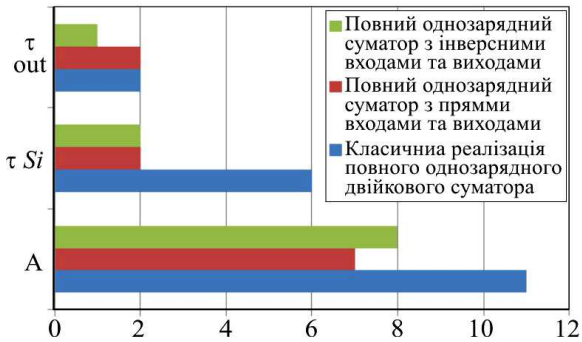


Рис. 7. Характеристики апаратної та часової складностей повних однорозрядних двійкових суматорів / Characteristics of hardware and time complexity of complete single-bit binary adders

З рис. 7 видно, що запропонована реалізація характеризується підвищеною у 3-4 рази швидкодією формування переносів у старші розряди порівняно з суматорами при класичній реалізації, що дає змогу відповідно у 2 рази підвищити швидкодію багаторозрядних двійкових суматорів паралельного типу при його використанні як однорозрядного компонента.

Обговорення результатів дослідження. Внаслідок проведених досліджень структур і системних характеристик логічних елементів синтезовано елемент "Провідне І", використання якого, як базового, для реалізації однорозрядних неповного та повного суматорів дає змогу оптимізувати їх системні характеристики. Вирішення складної задачі зменшення часової складності наскрізних переносів однорозрядних суматорів, реалізовано шляхом створення суматора з інверсними переносами. Застосування його як компоненти багаторозрядних двійкових суматорів, структури яких містять велику кількість послідовно з'єднаних однорозрядних суматорів, що забезпечує максимальну швидкодію, за рахунок затримки сигналів наскрізних переносів на 1 мікротакт, та, відповідно, підвищення швидкості цифрового опрацювання даних в процесорах шифрування даних.

Отже, внаслідок проведеного дослідження отримано такі *основні результати*: досліджено характеристики логічного елемента "Виключне АБО" та "Провідне І" як пришвидшувача виконання операцій у процесорах шифрування даних, використання якого як компоненти забезпечує оптимізацію системних характеристик обчислювальних засобів та дає змогу підвищити їх продуктивність.

Наукова новизна отриманих результатів дослідження – розроблено логічний елемент "Провідне І", що реалізує функцію логічного елемента "Виключне АБО", із зменшеним числом елементів та тривалістю затримки сигналів. Удосконалено структури компонентів обчислювальних засобів шляхом застосування логічного елемента "Провідне І", що дало змогу досягти оптимізації характеристик їх апаратної та часової складностей.

Практична значущість результатів дослідження – запропоновані схемотехнічні рішення удосконалених одноразрядних неповного та повних суматорів, на підставі логічного елемента "Провідне І" як пришвидшувача виконання операцій додавання, можуть бути використані у структурах складніших обчислювальних пристроїв, зокрема багаторозрядних суматорів, перемножувачів, процесорів шифрування даних, що дасть змогу забезпечити істотне зниження їх часової, апаратної та структурної складностей.

Висновок / Conclusions

Запропонована структура логічного елемента "Провідне І", що реалізує функцію "Виключне АБО", забезпечує зменшення його апаратної складності у 2-3 рази та підвищує швидкодію спрацювання у 3 рази порівняно з класичною реалізацією. Синтез на підставі цього елемента структур одноразрядних напів- та повних двійкових суматорів забезпечує досягнення їх мінімаксних критеріїв апаратної та часової складностей. Використання вдосконалених суматорів, як базових компонентів для багаторозрядних процесорів, які реалізують арифметично-логічні операції у базисі Радемахера-Крестенсона, дають змогу шифрувати багаторозрядні масиви даних у режимі реального часу, зменшити обчислювальну складність, підвищують продуктивність та регулярність архітектури багаторозрядних процесорів шифрування даних.

References

1. Anand, A. Kumar. (2016). *Fundamentals of Digital Circuits*. PHI Learning; 4th edition. 1503.
2. Davletova, A. Ya. (2019). Research of system characteristics of accelerators of arithmetic and logic operations. *Proceedings of the International Scientific and Practical Conference "Information Technology and Computer Modeling", 214–217.* Retrieved from: https://www.itcm.comp-sc.if.ua/2019/zbirnyk2019.pdf
3. Drozd, O. V., & Kharchenko, V. S. (2012). *Working diagnostics of secure information and measurement systems*. National Aerospace University. H. E. Zhukovsky "KhAI", 614.
4. Gryga, V., Nykolaychuk, Y., Nyckolaychuk, L., Vozna, N., & Klym, H. (2019). Structuring of Algorithms for Data Sorting and New Principles of Their Parallelization. *9th International Conference on Advanced Computer Information Technologies* (*ACIT*), 205–208. https://doi.org/10.1109/ACITT.2019.8779864
5. Grytsyuk, M. Yu., & Hrytsiuk, Yu. I. (2018). Nature and Sustainable Development of Tourism in the Carpathian Region Ukraine. *Scientific Bulletin of UNFU*, 28(2), 99–110. https://doi.org/10.15421/40280219
6. Havrysh, V. I., & Hrytsiuk, Yu. I. (2021). Analysis of temperature regimes in heat-sensitive layered elements of digital devices caused by internal heating. *Scientific Bulletin of UNFU, 31(*5), 108–112. https://doi.org/10.36930/40310518
7. Hrytsiuk, Yu., Grytsyuk, P., Dyak, T., & Hrynyk, H. (2019). Software Development Risk Modeling. IEEE 2019 14th *International Scientific and Technical Conference on Computer Sciences and Information Technologies* (CSIT 2019), (Vol. 2, pp. 134–137), 17–20 September, Lviv, Ukraine. Lviv: Lviv Polytechnic National University, 206 p. https://doi.org/10.1109/stc-csit.2019.8929778
8. Ivasiev, S., Kasyanchuk, M., Yakymenko, I., Gomotiuk, O., Shylinska, I., & Bilovus, L. (2020). Algorithmic Support for Rabin Cryptosystem Implementation Based on Addition. *10th International Conference on Advanced Computer Information Technologies* (*ACIT*). *779–782.* https://doi.org/10.1109/ACITT.2019.8779899
9. Krulikovskyi, B., Vozna, N., Kimak, V., & Davletova, A. (2016). The Method to Optimize Structural, Hardware and Time Complexities Characteristics Multi-Bit Adders of Special Processors for Data Encryption. *Modern Problem of Radio Engineeriong, Telecommunikations and Computer Science: proceedings of the XIII th International Conference TSET'2016,* February 23–26, 2016, 455–459. https://doi.org/10.1109/TCSET.2016.7452087
10. Krulikovskyi, B., Vozna, N., Kimak, V., & Davletova, A. (2016). The Method to Optimize Structural, Hardware and Time Complexities Characteristics Multi-Bit Adders of Special Processors for Data Encryption. *Modern Problem of Radio Engineeriong, Telecommunikations and Computer Science: proceedings of the XIII th International Conference* TSET'2016, 455–459. https://doi.org/10.1109/TCSET.2016.7452087
11. Krulikovskyi, B. B., Davletova, A. Ya., & Ivasiev, S. V. (2016). Method and special processors for determining the functions of the Hamming space in decision-making problems. *Proceedings of the VIII International School-Seminar "Decision Theory",* 152–153.
12. Krulikovskyi, B. B., Davletova, A. Ya., & Kimak, V. L. (2014). System characteristics of components of multi-bit data encryption processors. *Information problems of computer systems, law, energy, economics, modeling and management.* ISCM2014, 105–107.
13. Leshkevych, I. F., & Grytsiuk, Yu. I. (2017). The Problems of Definition and Analysis of Software Requirements. *Scientific Bulletin of UNFU, 27*(4), 148–158. https://doi.org/10.15421/40270433
14. Malinovsky, B. N., Boyun, V. P., & Kozlov, L. G. (1989). *Introduction to cybernetics. Parallel structures and methods.* Scientific thought, 272.
15. Nykolaichuk, Ya. (2017). *Specialized computer technology in computer science.* Monograph. Ternopil: "Beskydy", 919.
16. Nykolaichuk, Ya. M., Gryga, V. M., Vozna, N. Ya., & Davletova, A. Ya. (2018). Patent №124563 Ukraine IPC (2018.01) G06F 7/00 Full single-digit adder. № u 2017 11720; stated 30/11/2017; Bull. № 7.
17. Palagin, A. V., Boyun, V. P., & Yakovlev, Y. S. (2017). Problems of creating computer systems using nanoelement base. *Control systems and machines, 5,* 3–15. https://doi.org/10.15407/usim.2017.05.003
18. Pikh, V. Ya., Voronych, A. R., Nykolaichuk, Ya. M. (2015). High-performance special processors of correlation, spectral and entropic signal processing. *Proceedings of the International Scientific School-Seminar "Computational Optimization Issues",* 49–50.
19. Vozna, N. Y., Nykolaychuk, Y. M., & Volynskyi, O. I. (2019). Algorithms for Solving Problems of Cryptographic Protection of Color Image Pixels in the Rademacher's Basis and Residue Number Systems. *Cybernetics and Systems Analysis 55*(3), *474–487.* https://doi.org/10.1007/s10559-019-00155-2
20. Vozna, N. Ya., Davletova, A. Ya., & Nikolaychuk, Ya. M. (2019). *Methods of improving the structures of high-speed single-bit and multi-bit binary adders*. Bulletin of the National University "Lviv Polytechnic" "Computer Systems and Networks". Vol. 1, no. 1, 35–52. https://doi.org/10.23939/csn2019.01.035
21. Vozna, N. Ya., Krulikovskyi, B. B., Nykolaichuk, Ya. M., Gryga, V. M., & Pikh, V. Ya. (2018). Analog-to-digital converter. Patent № 116176 Ukraine IPC H03M 1/38 (2006.01). Published on February 12, 2018, Bulletin no. 3.
22. Yakymenko, I., Kasianchuk, M., Ivasiev, S., Shevchuk, R., Batko, Y., & Vasylkiv, V. (2020). Method for Determining Prime and Relatively Prime Numbers of 2 n+k Type Based on the Periodicity Property. *10th International Conference on Advanced Computer Information Technologies* (*ACIT*), Deggendorf, Germany. 751–754. https://doi.org/10.1109/ACIT49673.2020.9208812
23. Yatskiv, V., Tsavolyk, T., & Yatskiv, N. (2018). Burst error-correcting codes based on modular correcting codes.14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET). 1110–1113. https://doi.org/10.1109/TCSET.2018.8336388
24. Zadiraka, V. K., & Oleksyuk, O. S. (2003). *Computer arithmetic of multi-digit numbers: Scientific publication*. Kyiv, 264. [In Ukrainian].
25. Zadiraka, V., & Nykolaichuk, Ya. (2014). *Methods of Effective Protection of Information Flows*. Ternopil: Terno-graf, 308.

A. Ya. Davletova
West Ukrainian Nationally University, Ternopil, Ukraine

INVESTIGATION OF THE CHARACTERISTICS OF THE LOGICAL ELEMENT "LEADING I" AS AN ACCELERATOR OF ADDITION OPERATIONS IN DATA ENCRYPTION PROCESSORS

The analysis of the classical construction of components of computer tools, specialized problem-oriented processors has shown that the most important task of optimizing their system characteristics is to achieve maximum speed and reduce hardware complexity. Since the basis for the design of complex digital devices is the basic logical elements, the research of their system characteristics is conducted in this work. As a result, the greatest hardware complexity is determined to be the logical element "Exclusive OR". It is implemented on the basis of a combination scheme of five logical elements. This causes a high time delay in performing arithmetic and logic operations. In order to simplify the structure and microelectronic implementation of the logic element "Exclusive OR", the logic element "Leading I" is proposed. Its implementation is possible through the use of logic elements implemented by microelectronic technology ECL. A simplified structure of a single-bit half-adder due to the use of the logical element "Leading I" as a component is proposed. This reduces the hardware complexity of the half-adder to 3 elements. The obtained high-speed single-bit adder with time delay of signals at the outputs of the sum and transfer 1 *v*. The circuit solution of the structure of a single-bit binary adder based on the logical element "Leading I" is proposed in the work. The system characteristics of this adder are 2-3 times better compared to the classic implementation. Based on the high-speed single-bit half-adder, the structure of the full single-bit adder is synthesized, which is characterized by increased 3-4 times the speed of formation of transfers to higher digits in comparison with adders in the classical implementation. This allows, respectively, increasing twice the performance of multi-bit binary adders of the parallel type when used as a single-bit component. In the work, calculations and the diagram of comparison of system characteristics of the considered full single-bit binary adders are resulted. The synthesis of structures of single-bit semi- and full binary adders on the basis of the element "Leading I" ensures the achievement of their min/max criteria of hardware and time complexity. Therefore, their use as components of multi-bit processors such as information security systems will significantly increase their performance and reduce hardware complexity. Methodological and circuit solutions for the synthesis of high-speed single-bit adders and full adders with optimized characteristics are presented, which is the basis for building a structure of complex high-performance special processors for data processing in the TNB of Rademacher.

Keywords: logical element; single-bit adder; hardware complexity; speed of operation; special processor.