УДК 658.012.4:621 DOI
DOI https://doi.org/10.32782/IT/2024-4-24

Віталій ТУПКАЛО
доктор технічних наук, професор, професор кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
ORCID**:** *0000-0002-6594-530X*

Бібліографічний опис статті: Тупкало, В. (2024). Блоково-композиційний метод формування контрольних сигнатур функціонування цифрових систем на основі властивостей сигнатурного поля TSF[2^n,P^m(x)]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 206–214, doi: https://doi.org/10.32782/IT/2024-4-24

БЛОКОВО-КОМПОЗИЦІЙНИЙ МЕТОД ФОРМУВАННЯ КОНТРОЛЬНИХ СИГНАТУР ФУНКЦІОНУВАННЯ ЦИФРОВИХ СИСТЕМ НА ОСНОВІ ВЛАСТИВОСТЕЙ СИГНАТУРНОГО ПОЛЯ TSF[2^N,P^M(X)]

В контексті посилення актуальності проблеми забезпечення надійності функціонування різноманітних цифрових інформаційно-вимірювальних систем комплексів управління об'єктами критичної інфраструктури в умовах зовнішнього шкідливого впливу (кібератак), актуальною стає задача розробка цих комплексів управління із властивістю контролепридатності структурних вузлів (пристроїв) у реальному масштабі часу їх функціонування. При цьому визначальними умовами рішення задачі синтезу повинні бути дві: досягнення високої здатності апаратного функціонального контролю виявляти багатократні помилки у двійкових кодах при їх передачі, обробці та зберіганні та апаратна надлишковість функціонального контролю повинна бути мінімальною. Тому на базовому схемотехнічному рівні побудови цифрових систем виникає, в першу чергу, необхідність подальшого розвитку (нового етапу) схемотехніки мікросхем середнього та високого ступеня інтеграції.

Мета роботи. *На основі критичного аналізу ряду звісних методів функціонального апаратного контролю запропоновано схемотехнічний сигнатурно-функціональної підхід щодо створення нового покоління мікросхем середнього та високого ступеня інтеграції із вбудованими вузлами функціонального сигнатурного функціонального контролю, які б забезпечували високу достовірність контролю за мінімальної схемотехнічної (апаратної) надлишковості.*

Метод. *Рішення задачі синтезу ґрунтується на використанні математичного апарату авторської сигнатурної алгебри сигнатурного поля В. Тупкало TSF[2^n,P^m(x)].*

Наукова новизна. *Розроблено нове методичне рішення задачі синтезу формувачів контрольних сигнатур паралельного комбінаційного типу для багато розрядних операндів шляхом їх агрегації з окремих уніфікованих типових блоків малої розрядності. Доказана можливість двох способів такої агрегації при побудові формувачів сигнатур комбінаційного типу.*

Висновки. *Виходячи з двох запропонованих варіантів використання моделей паралельних формувачів сигнатур комбінаційного типу, можна запропонувати два можливих напрямків подальшого розвитку схемотехніки мікросхем середнього та високого ступеня інтеграції для побудови цифрових інформаційно-вимірювальних систем комплексів управління широкого призначення. По-перше, запропоновані моделі можуть бути реалізовані як окремі серії мікросхем вузлів сигнатурного контролю для побудова функціонально контролепридатних (самоконтролюючих у реальному часі функціонування) цифрових інформаційно-вимірювальних систем комплексів управління, по-друге – як функціональна інтегрована складова низки базових мікросхем схемотехніки цифрових систем. Подальшим напрямом розвитку теми статті є розробка методів схемотехніки сигнатурного функціонального контролю цифрових інформаційно-вимірювальних систем комплексів управління на основі множини сигнатурних полів В. Тупкало TSF[2^{kn},P^m(x)].*

Ключові слова: *функціональний сигнатурний контроль, методи контролю цифрових систем, функціональна контролепридатність, кіберстійкість.*

Vitaliy TUPKALO
Doctor of Technical Sciences, Professor, Professor at the Department of Cybersecurity, Information Technologies and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121
ORCID: *0000-0002-6594-530X*

To cite this article: Tupkalo, V. (2024). Blokovo-kompozytsiinyi metod formuvannia kontrolnykh syhnatur funktsionuvannia tsyfrovykh system na osnovi vlastyvostei syhnaturnoho polia TSF[2^n,P^m(x)] [Block-composition method for forming control signatures of the functioning of digital systems based on the properties of the signature field TSF[2^n,P^m(x)]]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 206–214, doi: https://doi.org/10.32782/IT/2024-4-24

BLOCK-COMPOSITION METHOD OF FORMING CONTROL SIGNATURES OF DIGITAL SYSTEMS OPERATION BASED ON THE PROPERTIES OF THE SIGNATURE FIELD TSF[2^N,P^M(X)]

In the context of increasing relevance of the problem of ensuring the reliability of the functioning of various digital information and measuring systems of control complexes by critical infrastructure objects in conditions of external harmful influence (for example, cyberattacks), the task of developing these control complexes with the property of controllability of structural units (devices) in the real time scale of their functioning becomes relevant. At the same time, the determining conditions for solving the synthesis problem should be two: achieving a high ability of hardware functional control to detect multiple errors in binary codes during their transmission, processing and storage, and hardware redundancy of functional control should be minimal. Therefore, at the basic circuit level of building digital systems, there is, first of all, the need for further development (a new stage) of the circuitry of microcircuits of medium and high integration.

Purpose of the work. *Based on a critical analysis of a number of well-known methods of functional hardware control, a circuit-technical signature-functional approach is proposed to create a new generation of microcircuits of medium and high integration with built-in functional signature functional control nodes, which would provide high reliability of control with minimal circuit-technical (hardware) redundancy.*

Method. *The solution to the synthesis problem is based on the use of the mathematical apparatus of the author's signature algebra of the field V. Tupkalo TSF[2^n,P^m(x)].*

Scientific novelty. *A new methodological solution to the problem of synthesizing control signature generators of the parallel combinational type for multi-bit operands by aggregating them from separate unified typical blocks of small bit size has been developed.*

Conclusions. *Based on the two proposed options for using models of parallel combinational signature generators, it is possible to propose two possible directions for further development of circuit design of microcircuits of medium and high degree of integration for building digital information and measuring systems of control complexes of wide purpose. Firstly, the proposed models can be implemented as separate series of microcircuits of signature control nodes for building functionally controllable (self-controlled in real time functioning) digital information and measuring systems of control complexes, secondly – as a functional integrated component of a number of basic microcircuits of circuit design of digital systems. A further direction of development of the topic of the article is the development of circuit design methods of signature functional control of the digital information and measuring systems based on the set of signature fields V. Tupkalo TSF[2^{kn},P^m(x)].*

Key words: *functional signature control, digital systems control methods, functional controllability, cyber resilience.*

Аналіз останніх досліджень і публікацій. З аналізу стану сучасної бази мікросхем для побудови цифрових інформаційно-вимірювальних пристроїв та систем (Прищепа, Погребняк, 2006; Бондаренко, Бородін, Карнаушенко, 2020; Піддубний, Товкач, 2021) у контексті забезпечення їх ефективної контролепридатності при експлуатації можна зробити висновок, що існуючі серії мікросхем є тільки функціонально-орієнтованими для синтезу множини цифрових інформаційно-вимірювальних систем комплексів управління (ЦІВСКУ) за різним функціонально-цільовим призначенням. Тому в умовах можливого зовнішнього шкідливого впливу (наприклад, кібератак) на ЦІВСКУ актуальною стає проблема подальшого розвитку (нового етапу) схемотехніки мікросхем середнього та високого ступеня інтеграції. Одним з перспективних напрямів рішення цієї проблеми є розробка нового покоління серій мікросхем з вбудованими елементами функціонального контролю (ФК) щодо можливості на їх основі розробляти вузли апаратного ФК для об'єктно-орієнтованих цифрових пристроїв та систем. При цьому визначальними умовами рішення задачі синтезу повинні бути дві: досягнення високої здатності апаратного ФК виявляти багатократні помилки у двійкових кодах при їх передачі, обробці та зберіганні, а також апаратна надлишковість ФК повинна бути мінімальною. Тому, на нашу думку, є необхідність у проведенні обґрунтування та формування пропозиції щодо подальшого напряму розвитку системотехніки мікросхем середнього та високого ступеня інтеграції із вбудованими апаратними елементами функціонального контролю з можливістю на їх основі розробляти цифрові інформаційно-вимірювальні пристрої та системи комплексів

управління критичної інфраструктури з високою функціональною контролепридатністю у реальному часі функціонування.

Виклад основного матеріалу дослідження. В контексті визначеної проблеми забезпечення функціональної контролепридатності цифрових пристроїв та систем відомий ряд методів функціонального контролю, в яких формуються двійкові контрольні характеристики (сигнатури), а саме:

– контроль цифрових кодів на парність / непарність (контроль однократних помилок у блоках n-розрядних двійкових послідовностей шляхом сумування їх одиниць по модулю два) (Бондаренко, Глушко, Меньков, 2003);

– числовий (двійковий) контроль (Локазюк, 1996; Чегренець, Руденко, 2016);

– програмно-логічні методи контролю ходу виконання програм (Говорущенко, Гнатчук,2010; Романкевич, 2016);

– сигнатурний контроль виконання логічних та арифметичних операцій на основі апарату синтезу сигнатурної алгебри (Тупкало,2021; Тупкало, 2024).

Результат аналізу цих методів представлений в таблиці 1.

З аналізу даних Таблиці 1 можна зробити наступні висновки:

1) загальний принцип методів ФК – відстеження правильності виконання операційних дій

Таблиця 1

Аналіз відомих методів ФК, в яких формуються двійкові контрольні характеристики (сигнатури)

№	Метод	Сутність методу	Контрольна характеристика
1.	Контроль цифрових кодів на парність / непарність (Бондаренко, Глушко, Меньков, 2003)	Сумування по модулю два одиниць у старших n – розрядах поточних контрольованих двійкових послідовностей з подальшим порівнянням результату з еталонним значенням заздалегідь сформованого (n + 1)-го контрольного розряду.	Один додатковий розряд (1 або 0) для супроводу n- розрядних двійкових послідовностей. Недолік – можливість виявити тільки однократні помилки у блоках n-розрядних двійкових послідовностей.
2.	Числовий (двійковий) контроль (Локазюк, 1996; Чегренець, Руденко, 2016)	Здійснюється за допомогою контрольних k-розрядних кодів, що представляють собою остачу від ділення двійкових n-розрядних чисел на деякий модуль p (двійкове число) з подальшим порівнянням результату остачі з еталонним значенням заздалегідь сформованої k-розрядної остачі. (n + 1) – го контрольного розряду.	Двійковий k-розрядний код, який формується відповідним вузлом ділення (апаратна надлишковість). Величина модуля p, від якої залежить величина кратності виявлених операційних помилок, повинна бути по можливості невелика, з тим щоб код залишку від ділення на число p будь-яких чисел не вимагали великого обсягу обладнання для реалізації числового контролю.
3.	Програмно-логічні методи контролю ходу виконання програм (Говорущенко, Гнатчук,2010; Романкевич, 2016)	Кожній ділянці (фрагменту адресації кортежу команд) перед виконанням присвоюється свій m-розрядний код, який попередньо запам'ятовується. В кінці виконання кожної ділянки здійснюється контроль на «свій код». Якщо коди не співпадають, то це свідчить про збій правильного виконання ділянки.	Контрольний m- розрядний двійковий код, як остача (сигнатура) ділення поліному контрольованого n -розрядного коду (n > m) на незвідний примітивний поліном $P^m(x)$ ступеню m. При цьому вибір величини ступеню поліному m визначає досяжну кратність виявлення помилки контролю на «свій код». Формування сигнатур відбувається за допомогою m – розрядного регістру зсуву зі зворотними зв'язками відповідно поліному $P^m(x)$. Недолік – затримка у часі формування коду сигнатур контрольованого кортежу ходу виконання програм.
4.	Сигнатурний контроль виконання логічних та арифметичних операцій на основі апарату логічного синтезу сигнатурної алгебри (Тупкало, 2021; Тупкало, 2024)	*Базовою операцією сигнатурного контролю є логічне співвідношення сигнатур вхідних поточних операндів з сигнатурою кінцевого результату виконання певних цільових операцій.* Реалізація методу зводиться до побудови контрольного вузла комбінаційного типу шляхом відповідної комутації функціонально закінчених комбінаційних елементів з кінцевої множини (стандартного набору) [9].	Формування m – розрядних сигнатур, як остачі ділення поліному контрольованого n -розрядного коду числа (n > m) на незвідний примітивний поліном $P^m(x)$ ступеню m: $A(x) \equiv sigA(x) = A(x) \bmod P(x)$. Синтез формувача сигнатур (sig) відбувається вузлом комбінаційної логіки паралельного типу (Tupkalo, Cherepkov, 2023)

цифрових пристроїв та систем, заснований на формуванні та порівнянні еталонних та поточних контрольних характеристик (сигнатур) операційних двійкових n- розрядних послідовностей (кодів);

2) в контексті визначеної вище проблема подальшого розвитку (нового етапу) схемотехніки мікросхем середнього та високого ступеня інтеграції з вбудованими елементами ФК в першу чергу слід звернути увагу на 3 і 4 методи ФК з точки зору принципової можливості забезпечення ефективної контролепридатності (кратність виявлення помилок у двійкових операційних кодах) цифрових пристроїв та систем, а саме: m- розрядна сигнатура формується, як остача ділення поліному контрольованого n-розрядного коду числа на обраний (твірний) незвідний примітивний поліном $P^m(x)$ ступеню m (n > m). При цьому в рамках сигнатурного поля Тупкало (Tupkalo signature field) TSF[2^n, $P^m(x)$] кратність виявлення помилок у двійкових кодах визначається звісним вибором (Тупкало, Черепков, 2024) величини цього ступеню при співвідношенні $n = (2^m – 1)$;

3) метод сигнатурного контролю 4 може одночасно задовольнити, як вимогу виявлення багатократних помилок у двійкових операційних кодах, так і вимогу мінімальної апаратної надлишковості контролюючого вузла, а саме: базовою операцією формування сигнатур є остачі ділення поліномів контрольованих n – розрядних кодів чисел (n > m) на незвідний примітивний поліном $P^m(x)$ ступеню m. При цьому синтез апаратної надлишковості ФК може звестися до побудови контрольного вузла шляхом відповідної комутації функціонально закінчених комбінаційних елементів з кінцевої множини (стандартного набору). Тому цей синтез запропоновано здійснювати на основі використання апарату логічного синтезу авторської сигнатурної алгебри поля TSF[2^n, $P^m(x)$] (зокрема, методики синтезу формувача сигнатур паралельного типу на основі використання сигнатурної утворюючої матриці незвідного примітивного полінома (Тупкало, Черепков,2023).

Згідно вищезазначеної мети дослідження пропонуються наступні визначення.

Визначення 1. Сигнатурний апаратний функціональний контроль – це вбудовані в структурні функціональні частини об’єктів контролю цифрових систем вузли сигнатурного контролю комбінаційного типу з необхідними вимогами до ефективності контролю.

Визначення 2. Сигнатурна функціональна контролепридатність ЦІВСКУ – це придатність системи до виявлення помилок у реальному масштабі часу при виконанні її цільових вимірювальних (обчислювальних) функцій $f_i \in F(X_{[L]})$ за допомогою певних вбудованих засобів сигнатурного функціонального контролю.

В контексті сутності визначення 2 модель сигнатурного функціонального контролю ЦІВСКУ представлена на рис. 1

Виходячи з вищезазначеного, сутність задачі синтезу визначимо так: нехай для заданого об’єкту функціонального контролю G доступними для контролю є тільки його входи та виходи. Треба визначити метод синтезу апаратної надлишковості комбінаційного типу згідно моделі рис. 1 при умові, щоб необхідна ефективність сигнатурного функціонального контролю (СФК) забезпечувалося би і при довільному співвідношенні k = L / n при обраному твірному незвідному примітивному поліномі $P^m(x)$ ступеню m. Тобто, не було б обмежень при реалізації СФК на величину розрядності L двійкових операндів об’єкту контроля.

З метою реалізації зазначеної задачі синтезу пропонується доказ наступної теореми (сигнатурна композиційна теорема Віталія Тупкало).

Теорема 1. Сигнатура L – розрядного двійкового числа U_L, що є послідовною конкатенацією з k окремих n- розрядних блокових частин U_{in} (i = 1,2, …) при обраному незвідному примітивному твірному поліномі сигнатур $P^m(x)$, дорівнює сумі за модулем два сигнатур його k окремих n- розрядних блокових частин U_{in} при умові, що L = kn, $n = (2^m – 1)$:

$$\text{sig } U_L = \text{sig } (U_{1n} \prec U_{2n} \prec \ldots \prec U_{kn}) =$$

$$= \text{sig } U_{1n} \oplus \text{sig } U_{2n} \oplus \ldots \oplus \text{sig } U_{kn}, \qquad (1)$$

де $\prec$ – операція конкатенації та «склеювання» окремих n-розрядних блокових частин Uin у порядку їхньої послідовності (відношення передування) від молодших до старших розрядів числа UL.

Доказ Теореми 1. Введемо наступне визначення.

Визначення 3. α-кратна сигнатура n-розрядного числа $\text{sig}^\alpha A_n$ – це сигнатура перетвореного числа виду $(A_n \prec W_{kn})$ – де W_{kn} – число нульової

kn – розрядності (k = 1,2, …).

Наприклад, для 7-ми розрядного числа A_7 = = 0111101 його двократною сигнатурою є його перше перетворення sig (0111101.0000000) = = sig^2(0111101), трикратною сигнатурою є друге перетворення sig (0111101.0000000.0000000) = = sig^3(0111101) і т.д.

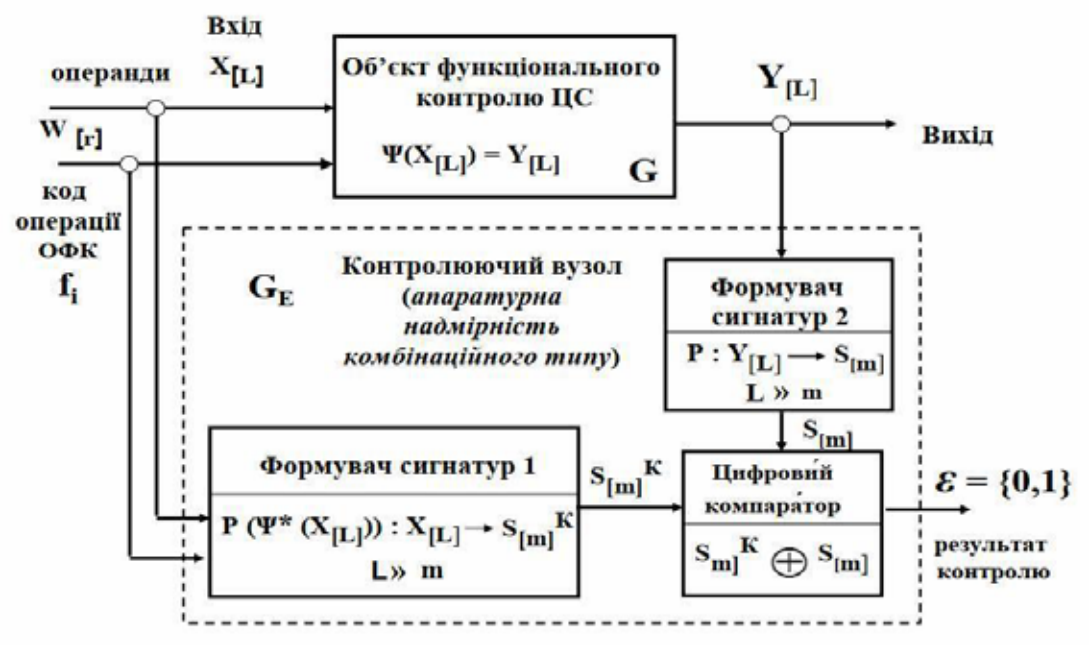


Рис. 1. Модель сигнатурного функціонального контролю (авторська модель)

G_E – вузол сигнатурного контролю, що складається з двох m-розрядних формувачів сигнатур (ФС); m-розрядного компаратора (КК) двох контрольних сигнатур; f_i – управлінські коди вибору виду контрольованих операцій з множини F.

Тоді, якщо двійкове kn-розрядне число U_L є результатом конкатенації з k окремих n- розрядних чисел

$$U_L = (U_{1n} \prec U_{2n} \prec \dots \prec U_{kn}), \qquad (2)$$

то на основі вище наведеного визначення, сигнатура результату конкатенації цих чисел є сумою за модулем два (в рамках розрядності L = kn) їх відповідних перетворень ($U_{in} \prec W_{in}$) у низці (послідовності) формування конкатенації. Тобто,

$$sig U_L = sig\, U_{1n} \oplus sig^2 U_{2n} \oplus sig^3 U_{3n} \oplus \dots \oplus sig^{(k-1)} U_{kn}, \qquad (3)$$

що і треба було доказати.

Перевіримо справедливість рівняння (3) по наступним вхідним даним:

для формування сигнатур використано регістр зсуву зі зворотними зв'язками за видом твірного поліному сигнатур $P^3(x) = x^3 + x + 1$; n = 7;

$$U_L = 0000111.0010101.1000110.$$

Згідно (3) маємо: $U_{17} = 1000110$; $U_{27} = 0010101$; $U_{37} = 0000111$.

Тоді при використанні Додатку А маємо:

$$sig\, U_L = (00001110010101100011 0)_{21} = \mathbf{110} =$$

$$= sig^3(0000111) \oplus sig^2(0010101) \oplus sig1000110 =$$

$$= sig\,(0000111.0000000.0000000) \oplus$$

$$sig\,(0010101.0000000) \oplus sig\,(1000110\,) =$$

$$= 101 \oplus 011 \oplus 000 = \mathbf{110}.$$

Ліва і права частина рівняння співпали.

Відносно рівнянню (3) слід зауважити, що оскільки операція формування m-розрядних сигнатур n-розрядних чисел на основі використання незвідного примітивного поліному $P^m(x)$ ступеню m при умові співвідношення $n = (2^m - 1)$ є лінійною (Тупкало, Черепков, 2024) і сигнатури створюють кільце сигнатурного поля $TSF[2^n, P^m(x)]$, то для рівняння (3) справедливим є застосування принципу суперпозиції за модулем два:

$$sig\, U_L = sig\,(U_{1n} \oplus U_{2n} \oplus \dots \oplus U_{kn}). \qquad (4)$$

Перевіримо справедливість рівняння (4) при попередніх вхідних даних і використовуємо таблицю поля $TSF[7, P^3(x)]$ у Додатку:

$$sig\, U_L = 110 =$$

$$= sig\,(1000110 \oplus 0010101 \oplus 0000111) =$$

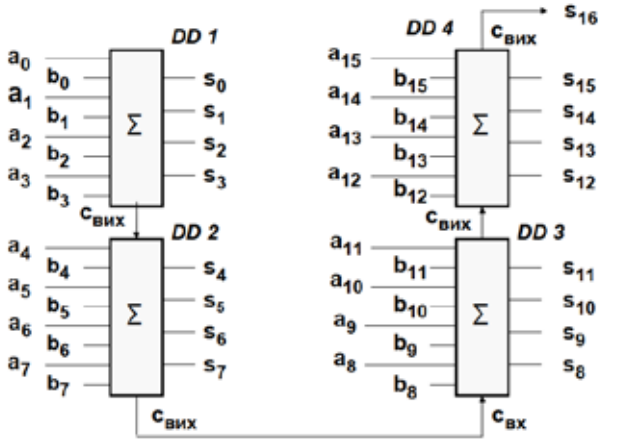
$$= sig\,(1010100) = \mathbf{110}.$$

Результати перевірок обох рівнянь (3) і (4) співпали.

Приклад рішення задачі синтезу та пропозиції

Зауваження до теореми 1. Відносно обов'язковості умови L = nk Теореми 1 слід

звернути увагу на наступне. Якщо після конкатенації окремих двійкових чисел у моноблок U_L загальна кількість розрядів моноблока не дорівнює величині L = kn, то необхідно провести доповнення недостатньої кількості розрядів нульовими розрядами зі сторони старших розрядів моноблоку U_L. Пояснення цього зауваження зробимо на прикладі блок-схеми шістнадцяти розрядного арифметичного двійкового суматора, представленого на рис. 2.



DD 1 - DD4 – мікросхеми К561ИМ1 (аналог CD4008A)

Рис. 2. Блок-схема шістнадцяти розрядного арифметичного двійкового суматора

Приклад 1. Вхідні дані: A_{16} = 1 1 0 1 0 0 1 1 0 1 1 1 0 1 0 1;

B_{16} = 1 1 1 1 0 1 1 1 0 1 0 1 0 0 0 1;

$D_{17} = (A + B)_{17}$ = 1 1 1 0 0 1 0 1 0 1 1 0 0 0 1 1 0 ;

$P^3(x) = x^3 + x + 1$.

Тоді маємо: $n = 2^m - 1 = 2^3 - 1 = 7$; $L_n / n = 17 : 7 = 2$ і остача 3.

Цей результату в контексті вищевикладеного зауваження до теореми 1 відносно двох альтернативних рівнянь (1) і (4) дає підстави стверджувати, що побудова вузла сигнатурного контролю може мати два варіанти.

Варіант № 1. Реалізація вузла сигнатурного ФК ґрунтується на рівнянні (1). Тобто, для виконання умови теореми 1 щодо організації сигнатурного контролю операції складання двійкового 16- ти розрядного суматора рис. 2 за mod $P^3(x)$ необхідно мати вузол контролю, який складається з трьох 7-ми розрядних по входу і трьома виходами (коду сигнатур при m = 3) формувачів сигнатур комбінаційного паралельного типу. При цьому цей варіант враховує сутність вищезазначене зауваження до теореми 1. Графічне пояснення сутності формування коду нульового доповнення при вхідних даних прикладу 1 представлено на рис. 3. Таким чином, на входи старших розрядів третього формувача сигнатури блоку U_{3n} необхідно подати код нульового доповнення $Q^4 = q_3q_2q_1q_0$.

Згідно вхідних даних прикладу 1 доказ коректності визначення варіанту № 1 синтезу апаратної надлишковості ФК для 16- ти розрядного арифметичного двійкового суматора на основі рівняння (1) зводиться до наступної послідовності обчислень:

$$sigD_{17} = sig\ U_{17} = sig\ (11100101011000110)_{17} =$$

$$= sig(\mathbf{0000}111.0010101.1000110)_{21} =$$

$$= sig\ (0000111)_7 \oplus sig\ (0010101)_7$$

$$\oplus\ sig\ (1000110)_7.$$

Якщо для формування сигнатур було б використано регістр зсуву зі зворотними зв'язками за видом твірного поліному сигнатур $P^3(x) = x^3 + x + 1$ (див. Рис. 4,а), то на 17-му такті зсуву було б отримано результат:

$$sig\ (11100101011000110)_{17} = 110.$$

У нашому випадку для формування сигнатур паралельним способом використовується формувач сигнатур (7x3) поля TSF[7,$P^3(x)$]

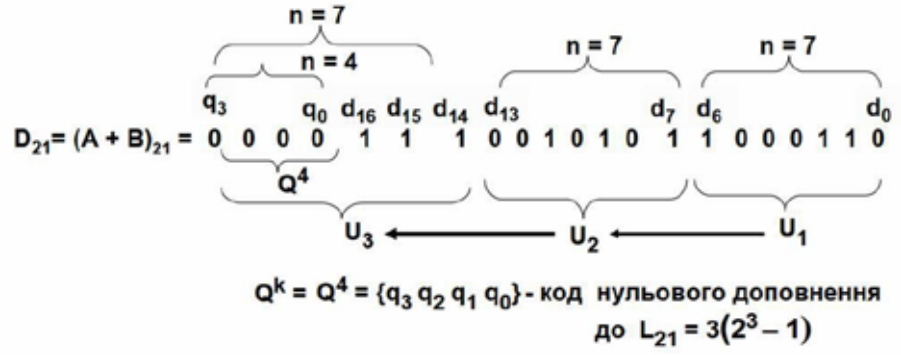


Рис. 3. Сутність формування коду нульового доповнення

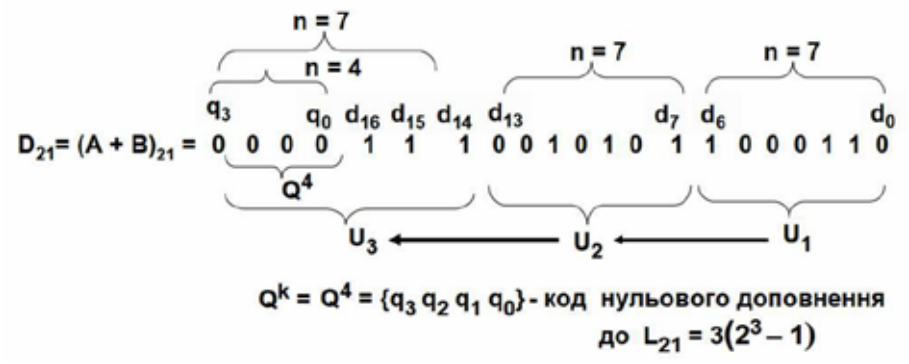


Рис. 4. Формування сигнатур:

а) у послідовний спосіб з використанням регістру зсуву зі зворотніми зв'язками;
б) у паралельний спосіб з використанням формувачів комбінаційного типу.

комбінаційного паралельного типу, який представлений на рис. 5. Тому, повертаючись до рівняння (3) і використовуючи таблицю В. Тупкало поля TSF[7,P³(x)] у Додатку А, отримуємо:

$$\text{sig}\,(0000111)_7 \oplus \text{sig}\,(0010101)_7 \oplus \text{sig}\,(1000110)_7 =$$
$$= 101 \oplus 011 \oplus 000 = 110,$$

тобто є повний збіг із попереднім отриманим результатом.

Технічна реалізація паралельного формувача сигнатур для 21-го розрядного моноблока U_{21} зводиться до побудови комбінаційного вузла 3(7x3) згортки трьох сигнатур від трьох 7-ми розрядних блоків 21-го розрядного моноблока U_{21} за модулем два пірамідального типу з числом функціональних ступеней згортки, рівного двом. При цьому на входи чотирьох старших розрядів формувача сигнатури третього блоку U_{3n} необхідно подати код нульового доповнення $Q^4 = q_3q_2q_1q_0$. При цьому час виконання операції формування 3-х розрядної сигнатури моноблока U_{21} становить вчетверенну величину затримки двовходового елемента сума за модулем два М2.

Варіант № 2. Реалізація вузла сигнатурного ФК грунтується на основі рівняння (4). Згідно вхідних даних прикладу 1 доказ коректності визначення варіанту № 2 синтезу апаратної надлишковості ФК для 16-ти розрядного арифметичного двійкового суматора на основі рівняння (4) зводиться до наступної послідовності обчислень з використанням таблиці поля TSF[7,P³(x)] у Додатку А, отримуємо:

$$\text{sig}_{[3]}A_{[7]} = \begin{cases} S_3 = a_7 \oplus a_5 \oplus a_4 \oplus a_3 \\ S_2 = a_6 \oplus a_4 \oplus a_3 \oplus a_2 \\ S_1 = a_5 \oplus a_3 \oplus a_2 \oplus a_1 \end{cases}$$

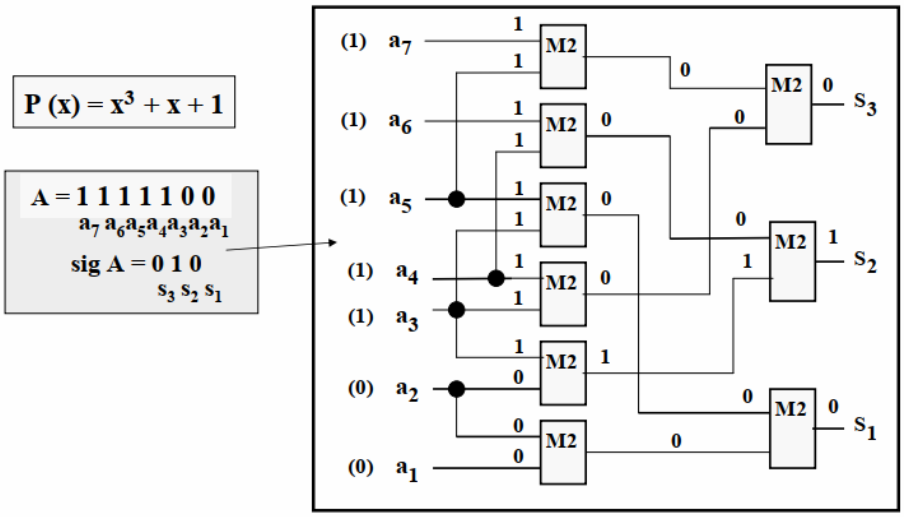


Рис. 5. Формувач сигнатур (7x3) поля TSF[7,P³(x)] комбінаторного паралельного типу (авторська модель)

$$\text{sig } U_{17} = \text{sig } (11100101011000110)_{17} =$$
$$= \text{sig } (0000111.0010101.1000110)_{21} = \mathbf{110} =$$
$$= \text{sig } (0000111 \oplus 0010101 \oplus 1000110) =$$
$$\text{sig } (1010100)_7 = 110, \qquad (4)$$

тобто є повний збіг із отриманим результатом варіанта № 1.

Технічна реалізація паралельного формувача сигнатур (7x3) комбінаційного типу за цим варіантом зводиться до побудови комбінаційного вузла згортки за модулем два трьох 7-ми розрядних блоків 21-го розрядного моноблока U_{21} з урахуванням нульове доповнення $Q^4 = q_3q_2q_1q_0$ блоку U_{3n} шляхом подачі на відповідні входи суматора сигнал логічної одиниці. З отриманої на першому функціональному ступені згортки за модулем два 7-ми розрядного результату W_7 формується контрольна 3-х розрядна сигнатура $sigW_7$, що дорівнює сигнатурі 21-го розрядного моноблока U_{21}. Таким чином, контрольний вузол пірамідального комбінаційного типу за варіантом № 2 має, як і варіант № 1, два функціональні ступеня згортки. При цьому час виконання операції формування сигнатури моноблока $(A+B)_{21}$ становить також вчетверенну величину затримки двовходового елемента згортки за модулем два М2. Вузол сигнатурного контролю за варіантом № 2 представлений на рис. 6.

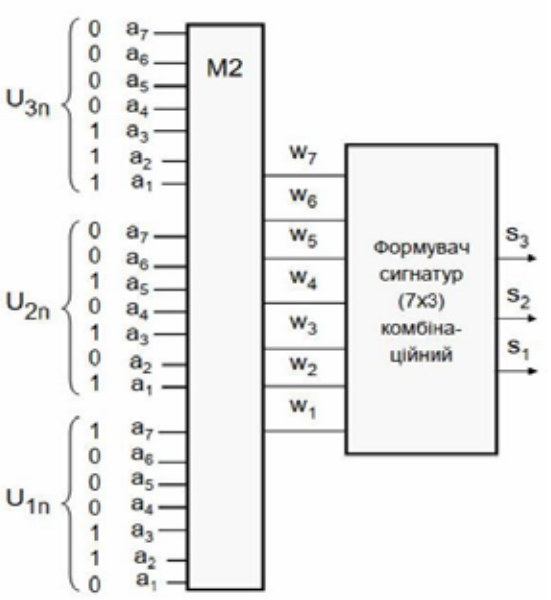


Рис. 6. Вузол сигнатурного контролю за варіантом № 2

Виходячи з вищезазначеного в контексті теореми 1 слід зауважити, що поле $TSF[2^n,P^m(x)]$ при співвідношенні $n = (2^m – 1)$ є окремим випадком сімейства полів В. Тупкало (Tupkalo Signature Field) $TSF[2^{kn}, P^m(x)]$. При варіації змінних поля n, m, k в загальному сенсі $TSF[2^{kn}, P^m(x)]$ – це множина (сімейство) сигнатурних полів В. Тупкало, кожне з яких є скінченими. Згідно даного твердження пропонується наступне визначення.

Визначення 3. Сигнатурне поле В. Тупкало (Tupkalo Signature Field) TSF $[2^{kn}, P^m(x)]$ є кінцевим полем (множиною) сюрективного відображення двох взаємно пов'язаних підможин: підмножини $L = kn$ – розрядних ($k = 1,2,\ldots$) двійкових чисел U_L та підмножини значень (класів) m – розрядних сигнатур $sigU_L(x) = U_L(x) \bmod P^m(x)$ при умові $L > m$, $n = (2^m – 1)$; $P^m(x)$ – незвідний примітивний поліном поля (породжувальний поліном m – розрядних сигнатур поля).

ЛІТЕРАТУРА:

1. Прищепа М. М., Погребняк В. П. Мікроелектроніка. У 3-х частинах. Ч. 2. Елементи мікросхемотехніки: Навч. посіб / М. М. Прищепа. Київ: Вища школа, 2006. 503 с.

2. Бондаренко І. М., Бородін О. В., Карнаушенко В. П. Сучасна компонентна база електронних систем: навч. посібник для студентів ЗВО. Харків: ХНУРЕ, 2020. 268 с.

3. Піддубний В. О., Товкач І. О. Елементна база радіоелектронної апаратури: В 4 ч. Ч. 4. Основи мікроелектроніки: навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка». Київ :КПІ ім. Ігоря Сікорського, 2021. 98 с.

4. Бондаренко І. М., Глушко А. П., Меньков О. М. Коди та кодування. Навч. посібник. Харків. ХІ ВПС, 2003. 116 с.

5. Локазюк В. М. Контроль і діагностування обчислювальних пристроїв та систем: Навч. посібник для вузів. Хмельницький: ТУП, 1996. 175 с.

6. Чегренець В. М., Руденко Н. В. Комп'ютер та комп'ютерна арифметика. Київ: Державний Університет Телекомунікацій, Навчально-науковий Інститут Телекомунікацій та Інформатизації, 2016. 120 с

7. Говорущенко Т. О., Гнатчук Є. Г. Особливості відмовостійких комп'ютерних систем з програмованою логікою як об'єктів діагностування. *Вісник Хмельницького національного університету*. № 5, 2010. С. 222–226.

8. Авраменко А. С., Авраменко В. С., Косенюк Г. В. Тестування програмного забезпечення. Навчальний посібник. Черкаси: ЧНУ імені Богдана Хмельницького, 2017. 284 с.

9. Тупкало В. М. Розробка моделей кіберстійких інформаційних систем управління на основі використання математичного апарату сигнатурної алгебри. V Міжнарод. наук.-практ. конф. «Управління якістю в освіті та промисловості: досвід, проблеми та перспективи», 20-21 травня 2021 р. зб. тез доп. Львів: ЛА «Піраміда», 2021. С. 186–187.

10. Тупкало В. М. Розробка моделей кіберстійких інформаційних систем управління на основі використання математичного апарату сигнатурної алгебри: авторське свідоцтво № 131020; заяв. 31.10.2024; опубл. 29.11.2024, Бюл. № 84.

11. Tupkalo V., Cherepkov S. Systems engineering of cybersecured digital and information measuring systems based on the signature Boolean-polynomial algebra synthesis apparatus. *Measurements infrastructure*. № 5. 2023. pp.1–14.

12. Tupkalo V., Cherepkov S. Signature functional control of digital automatic device register operations. *Measurements infrastructure*. № 7. 2024. pp.1–13.

REFERENCES:

1. Pryshchepa, M. M., Pogrebnyak, V. P. (2006). Mikroelektronika [Microelectronics]. In 3 parts. Part 2. Elements of microcircuitry: Textbook / M. M. Pryshchepa. Kyiv: Higher School.

2. Bondarenko, I. M., Borodin, O. V., Karnaushenko, V. P. (2020). Suchasna komponentna baza elektronnykh system [Modern component base of electronic systems]: textbook for students of higher educational institutions. Kharkiv: KhNURE.

3. Piddubny, V. O., Tovkach, I. O. (2021). Elementna baza radioelektronnoi aparatury: V 4 ch. Ch. 4. Osnovy mikroelektroniky [Elemental base of radioelectronic equipment: In 4 parts. Part 4. Fundamentals of microelectronics]: teaching aids for students of specialty 172 «Telecommunications and radio engineering». Kyiv: Igor Sikorsky Kyiv Polytechnic Institute.

4. Bondarenko, I. M., Glushko, A. P., Menkov, O. M. (2003). Kody ta koduvannia [Codes and coding]. Textbook. Kharkiv. XI Air Force.

5. Lokaziuk, V. M. (1996). Kontrol i diahnostuvannia obchysliuvalnykh prystroiv ta system: Navch. posibnyk dlia vuziv [Control and diagnostics of computing devices and systems: Textbook for universities]. Khmelnytsky. 175 p.

6. Chegrenets, V. M., Rudenko, N. V. (2016). Kompiuter ta kompiuterna aryfmetyka [Computer and computer arithmetic]. Kyiv: State University of Telecommunications, Educational and Scientific Institute of Telecommunications and Informatization. 120 p.

7. Govorushchenko, T. O., Gnatchuk, E. G. (2010). Osoblyvosti vidmovostiikykh kompiuternykh system z prohramovanoiu lohikoiu yak obiektiv diahnostuvannia [Features of fault-tolerant computer systems with programmable logic as objects of diagnostics]. *Bulletin of Khmelnytsky National University*. № 5, P. 222–226

8. Avramenko, A. S., Avramenko, V. S., Kosenyuk, G. V. (2017). Testuvannia prohramnoho zabezpechennia [Software testing.] Textbook. Cherkasy: Bohdan Khmelnytskyi National University. 284 p.

9. Tupkalo, V. M. (2021). Rozrobka modelei kiberstiikykh informatsiinykh system upravlinnia na osnovi vykorystannia matematychnoho aparatu syhnaturnoi alhebry [Development of models of cyber-resistant information management systems based on the use of the mathematical apparatus of signature algebra]. V International Scientific and Practical Conference «Quality Management in Education and Industry: Experience, Problems and Prospects». P. 186–187.

10. Tupkalo, V. M. (2024). Rozrobka modelei kiberstiikykh informatsiinykh system upravlinnia na osnovi vykorystannia matematychnoho aparatu syhnaturnoi alhebry [Development of models of cyber-resistant information management systems based on the use of the mathematical apparatus of signature algebra]: author's certificate No. 131020; application. 10/31/2024; publ. 11/29/2024, Bull. No. 84.

11. Tupkalo, V., Cherepkov, S. (2023). Systems engineering of cybersecured digital and information measuring systems based on the signature Boolean-polynomial algebra synthesis apparatus. *Measurements infrastructure*. № 5. pp.1–14.

12. Tupkalo, V., Cherepkov, S. (2024). Signature functional control of digital automatic device register operations. *Measurements infrastructure*. № 7. pp.1–13.

Додаток А. Сигнатурне поле TSF[7, $P^3(x)$], $P^3(x) = x^3 + x + 1$
(Tupkalo, Cherepkov, 2023**)**

Addition A. Signature field TSF[7, $P^3(x)$], $P^3(x) = x^3 + x + 1$
(Tupkalo, Cherepkov, 2023**)**

№	A	sigA	№	A	sigA	№	A	sigA	№	A	sigA	№	A	sigA
1	*0000000*	*000*	31	0011110	111	61	0111100	110	91	1011010	100	121	1111000	101
2	0000001	001	32	0011111	110	62	0111101	111	92	1011011	101	122	1111001	100
3	0000010	011	33	0100000	010	63	0111110	101	93	*1011100*	*000*	123	1111010	110
4	0000011	010	34	0100001	011	64	0111111	100	94	1011101	001	124	1111011	111
5	0000100	111	35	0100010	001	65	1000000	100	95	1011110	011	125	1111100	010
6	0000101	110	36	*0100011*	*000*	66	1000001	101	96	1011111	010	126	1111101	011
7	0000110	100	37	0100100	101	67	1000010	111	97	1100000	110	127	1111110	001
8	0000111	101	38	0100101	100	68	1000011	110	98	1100001	111	128	*1111111*	*000*
9	0001000	110	39	0100110	110	69	1000100	011	99	1100010	101	*Ідеал поля TSF(7,3) при $P(x)=x^3+x+1$*		
10	0001001	111	40	0100111	111	70	1000101	010	100	1100011	100			
11	0001010	101	41	0101000	100	71	*1000110*	*000*	101	1100100	001			
12	0001011	100	42	0101001	101	72	1000111	001	102	*1100101*	*000*			
13	0001100	001	43	0101010	111	73	1001000	010	103	1100110	010	1	*0000000*	*000*
14	*0001101*	*000*	44	0101011	110	74	1001001	011	104	1100111	011	14	*0001101*	*000*
15	0001110	010	45	0101100	011	75	1001010	001	105	*1101000*	*000*	24	*0010111*	*000*
16	0001111	011	46	0101101	010	76	*1001011*	*000*	106	1101001	001	27	*0011010*	*000*
17	0010000	101	47	*0101110*	*000*	77	1001100	101	107	1101010	011	36	*0100011*	*000*
18	0010001	100	48	0101111	001	78	1001101	100	108	1101011	010	47	*0101110*	*000*
19	0010010	110	49	0110000	111	79	1001110	110	109	1101100	111	53	*0110100*	*000*
20	0010011	111	50	0110001	110	80	1001111	111	110	1101101	110	58	*0111001*	*000*
21	0010100	010	51	0110010	100	81	1010000	010	111	1101110	100	71	*1000110*	*000*
22	0010101	011	52	0110011	101	82	*1010001*	*000*	112	1101111	101	76	*1001011*	*000*
23	0010110	001	53	*0110100*	*000*	83	1010010	010	113	1110000	011	82	*1010001*	*000*
24	*0010111*	*000*	54	0110101	001	84	1010011	011	114	1110001	010	93	*1011100*	*000*
25	0011000	011	55	0110110	011	85	1010100	110	115	1110010	000	102	*1100101*	*000*
26	0011001	010	56	0110111	010	86	1010101	111	116	1110011	001	105	*1101000*	*000*
27	*0011010*	*000*	57	0111000	001	87	1010110	101	117	1110100	100	115	*1110010*	*000*
28	0011011	001	58	*0111001*	*000*	88	1010111	100	118	1110101	101	128	*1111111*	*000*
29	0011100	100	59	0111010	010	89	1011000	111	119	1110110	111	модель Тупкало В.М.		
30	0011101	101	60	0111011	011	90	1011001	110	120	1110111	110			