

Реалізація алгоритмів кодування/декодування інформації на базі FPGA

УДК 512.624.95 (045)

Володимир Опанасенко¹, Станіслав Зав'ялов²,
Олександр Софіюк³^{1,3}Інститут кібернетики ім. В.М. Глушкова НАН України, ²ООО «Радіонікс»,
¹opanasenko@incub.kiev.ua, ²radionix13@gmail.com, ³otsof@yandex.ua

Сьогодні, у зв'язку з інтенсивним розвитком систем захисту інформації, актуальною стає задача технічної модернізації існуючих пристроїв, які реалізують прийом та передавання кодової інформації, за допомогою сучасної елементної бази – FPGA (Field Programmable Gate Array – програмовні користувачем вентильні матриці). FPGA знаходять усе більше широке застосування в світі для створення сучасних систем управління, передавання інформації, цифрової обробки сигналів, підтримки телекомунікацій та інших.

Метою даної роботи є підвищення ефективності розробки пристроїв кодування/декодування інформації за рахунок їхньої апаратної реалізації на базі FPGA, що забезпечує додатковий захист інформації у каналах передавання.

Виконано апаратну реалізацію на базі кристалів FPGA серії Spartan6 (6SLX4CSG225-3):

- генераторів псевдовипадкових слів (ПВС) які використовують принцип реконфігуровності, що забезпечує можливість модернізації їх алгоритмів та динамічну зміну внутрішньої структури (реконфігурацію) у процесі функціонування;

- пристроїв формування послідовностей фазово-кодової модуляції (ФКМ) та послідовностей, які кодовано кодами Баркера. Довжина послідовностей є змінною (змінюється командою центрального процесора залежно від виконуваної задачі). Допускається формування до 10-ти послідовностей ФКМ різної довжини та до 10-ти значень кодів Баркера для заданої довжини. 7-ми розрядним кодом Баркера можна кодувати до 8-ми значень посилки управління.

За допомогою САПР ISE 14.02 Foundation шляхом описання мовою VHDL на базі кристалу серії Spartan6 (6SLX4CSG225-3) виконано проектування і реалізація: трьох типів генераторів ПВС за різними алгоритмами; пристроїв формування послідовностей ФКМ та послідовностей, які кодовано кодами Баркера.

Наявність вбудованих блоків DSP в структурі сучасних кристалів FPGA дозволяє ефективну апаратну реалізацію кодування/декодування інформації за рахунок реалізації основних операцій множення із накопиченням на вентильному рівні.

Отримані характеристики часових та апаратних витрат реалізації генераторів ПВС за трьома алгоритмами наведено у табл. 1, а для реалізації пристроїв формування послідовностей ФКМ та послідовностей, які кодовано кодами Баркера, наведено в Табл. 2.

Таблиця 1
Оцінки апаратних і часових витрат при реалізації генераторів ПВС

Алгоритм	T _{CLK} , нс	DSP		Кількість Tg			Кількість LUTs		
		Викор.	Дост.	Викор.	Дост.	%	Викор.	Дост.	%
Алгоритм 1	5,773	1	8	103	4800	2	108	2400	4
Алгоритм 2	10,750	2	8	103	4800	2	92	2400	3
Алгоритм 3	6,224	2	8	87	4800	1	45	2400	1

Таблиця 2
Оцінки апаратних і часових витрат при реалізації пристроїв формування послідовностей

Формування послідовностей	T _{CLK} , нс	Кількість регістрів			Кількість LUTs		
		Викор.	Доступно	%	Викор.	Доступно	%
ФКМ	4,5083	395	11440	3	1539	5720	26
кодами Баркера	4,963	403	11440	3	488	5720	8

Результати моделювання з використанням системи моделювання ModelSim SE 10.1c (часова діаграма) одного із запропонованих генераторів ПВС для відповідного алгоритму наведено на рис. 1.

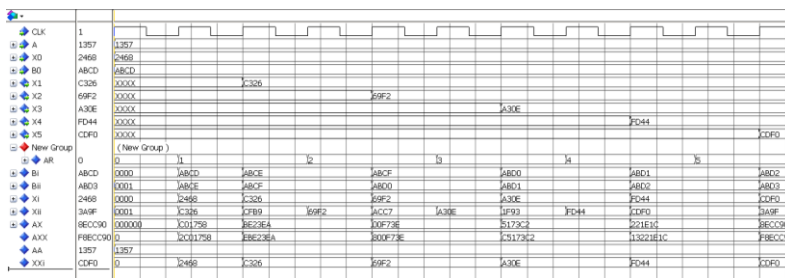


Рис. 1. Часова діаграма роботи генератора ПВС

Результати моделювання пристроїв формування послідовностей наведено на рис. 2, 3 відповідно.



Рис. 2. Часова діаграма формування послідовностей ФКМ

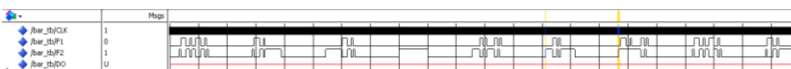


Рис. 3. Часова діаграма формування послідовностей кодів Баркера