MATHEMATICAL AND COMPUTER MODELING

УДК 519.688

СТЕПАН БІЛАН,
АНДРІЙ ДЕМАШ

ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ГЕНЕРАТОРА ПІДКЛЮЧІВ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

У статті розглядаються підходи та основні проблеми існуючих методів шифрування відеоінформації. Описаний метод шифрування відеоданих на основі клітинних автоматів, який дозволяє підвищити надійність захисту відеоінформації, збільшити довжину ключа шифрування, підвищити швидкодію засекречування зображення та спростити підготовку початкових установок блоку формування підключів. Описана програмно-апаратна реалізація генератора підключів для системи шифрування відеоінформації, в основу якої покладено вищезазначений метод. Даний генератор реалізований з використанням двох клітинних автоматів, що дозволяє формувати ключову гаму у неявному вигляді. Основний клітинний автомат здійснює передачу сигналу збудження від клітини до клітини, а додатковий клітинний автомат здійснює зміну станів усіх власних клітин згідно заданої функції та вибраної околиці. Гама залежить від початкової карти станів клітинних автоматів та початкових налаштувань траєкторії руху. Генератор реалізований на дешевих ПЛІС з високими показниками по швидкодії, що дозволяє зашифровувати відеоінформацію в реальному часі в процесі передачі її по каналах зв'язку.

Ключові слова: шифрування, відеоінформація, клітинний автомат, гама, ПЛІС.

Вступ. Технології обробки відеосигналу, поряд з бездротовими технологіями, розвиваються сьогодні найбільш високими темпами. Такі теми як оцифровування, поліпшення, стискання і передача відеоінформації, висвітлюються в технічній літературі регулярно та докладно. Разом з тим, надійний захист відеоінформації від несанкціонованого доступу – все ще екзотична тема навіть для спеціалізованих видань. Незважаючи на потребу в шифрувальній техніці самих різних споживачів: охоронних агентств, відео- і телекомпаній – ринок пристроїв захисту відеоінформації дотепер дуже вузький. Причини такого стану речей полягають, в основному, у технології застосування "стійкого крипто" до телевізійного сигналу стандартних форматів. Крім того, у зв'язку з появою мереж передачі даних високої пропускної здатності і розвитком мультимедійних технологій виникає проблема шифрування великих обсягів інформації [1, 2]. Одночасно з цим, при обміні чутливою до компрометації інформацією загальнодоступними каналами, у всій повноті проявляється необхідність захистити дані від несанкціонованого доступу, забезпечивши при цьому їх доступність та цілісність.

Постановка проблеми. На сьогодні існує багато методів і засобів шифрування відеоінформації, які представляють зображення у вигляді послідовності двійкових біт. При цьому послідовність розбивається на блоки, які в подальшому шифруються відомими методами. Однак, зображення представляються великими бітовими масивами, а довжина ключів при цьому обмежена, що потенційно може призвести до злому зашифрованої числової послідовності. Підвищити якість шифрування дозволяє використання спеціальної функції і додаткові способи, які на основі початкової ключової послідовності формують ключ. Крім того, постійна зміна ключової послідовності в часі знижує імовірність зламу алгоритму. Досягти постійної функціональної зміни ключової послідовності дозволяє використання клітинних автоматів (КА) [3, 4].

Аналіз існуючих методів та інструментів для шифрування відеоінформації. На даний час, для захисту візуальної інформації застосовуються ряд способів [5, 6], які полягають в перетвореннях зображення на основі унітарних математичних перетворень. Зображення піддається унітарному математичному перетворенню (перетворення Фур'є), а отримані коефіцієнти перетворення шифруються шляхом додавання маски – ключа, яка має випадкову фазову характеристику. Також відомі способи використовують оцифровування зображень, що спрощує реалізацію таких методів шифрування. Головними проблемами таких методів є слабкий захист інформації при розшифровуванні, оскільки шумові помилки знижують якість відновлення. Крім того, способи характеризуються низькою швидкодією при їх реалізації за рахунок використання трансформацій зображень. У розглянутих способах можливе визначення імовірних комбінацій шляхом послідовного перебору і розшифрування зображення. Проблемою є також використання перетворення Фур'є і додаткові перетворення оцифрованого зображення, а також використовуються додаткові перетворення і шифрування модуля і фази сигналів.

Найбільш близьким до способу реалізації генератора, є спосіб засекречування візуальної інформації [7]. Недоліком даного способу є низька надійність захисту інформації, яка обумовлена тим, що формування ключа здійснюється стаціонарними бітовими картами, які не дають функціональної зміни ключової бітової послідовності в часі, а також обмеження довжини періоду формування бітової послідовності при формуванні ключової гами.

В роботі [8] розглядаються можливі підходи до попереднього шифрування і до шифрування з стисненням. Основний акцент робиться на шифрування стислої інформації. При цьому, шифрування здійснюється відомими алгоритмами з відомими способами формування ключової гами.

Відомий також стрип – метод шифрування зображень [9, 10], який полягає в нарізуванні відеосигналу на смуги і формування послідовності сигналів з нарізаних бітових смуг. З цих смуг можуть бути сформовані матриці, які піддаються застосуванню матричних операторів. Матрична обробка використовується для боротьби з шумами і маскування зображення методом шифрування [11-13].

Ці методи вимагають удосконалення з точки зору представлення зображення і формування ключової послідовності, адаптованої до його розмірності.

Опис методу шифрування відеоданих на основі КА. В основу реалізації поставлені наступні задачі:

– підвищення надійності захисту відеоінформації за рахунок можливості зміни закону поблокового сканування та подання зображення множиною розрядних шарів, а також за рахунок власного формування підключів, коди яких залежать від реалізованого блоку формування підключів на основі клітинного автомату;

– збільшення довжини ключа шифрування, що дозволяє здійснювати потокове шифрування усього масиву бітової послідовності;

– підвищення швидкодії засекречування зображення шляхом шифрування за рахунок формування одного біту на виході клітинного автомату, що усуває потребу зчитування значення збудженої клітини разом з станами клітин її околиці;

– спрощення підготовки початкових установок блоку формування підключів за рахунок вільного використання станів клітинних автоматів без попереднього визначення форми траєкторії.

Зображення, яке потрібно зашифрувати, оцифровують шляхом перетворення його у дискретну форму. Оцифровка нерастрового зображення здійснюється проектуванням його на матричну однорідну клітинну структуру. Кожна клітина має свою вхідну оптичну апертуру, від геометричної форми та розмірів котрої залежить рівень дискретизації зображення. Кожна клітина здійснює перетворення відповідного дискретного одиничного поля вхідного зображення у код, який кодує колір та інтенсивність світла, що формує даний одиничний дискрет зображення.

Таким чином, оцифроване зображення подається множиною кодів, які зберігаються у клітинах матричного клітинного однорідного середовища. Дане середовище також розбите на горизонтальні матричні шари, які складаються з відповідних розрядів усіх клітин. Наприклад, перший матричний шар (бітовий зріз) формується з перших розрядів кодів клітин.

За допомогою даного клітинного середовища аналогове зображення подається тривимірною структурою, яка формує його тривимірний код.

Для проведення його шифрування здійснюють послідовне сканування кожного матричного клітинного шару у заданій послідовності. Сканування здійснюється поблоково та кожний блок паралельно зчитується і подається у блок шифрування. Блок представляє собою задану групу біт, яка може бути подана стрічкою або іншою формою.

Отже, подання зображення на вхід блоку шифрування здійснюється у спотвореній формі. Така форма обумовлена заданим законом сканування, який належить до ключових даних. Реалізацію зазначеного підходу детально розглянуто в [14].

Для генерації підключів використовують спеціально розроблену структуру, яка реалізована на двох КА. Основний КА здійснює передачу сигналу збудження від клітини до клітини, а додатковий КА здійснює зміну станів усіх власних клітин згідно заданої функції та вибраної околиці. На рис. 1 представлена структура генератора.

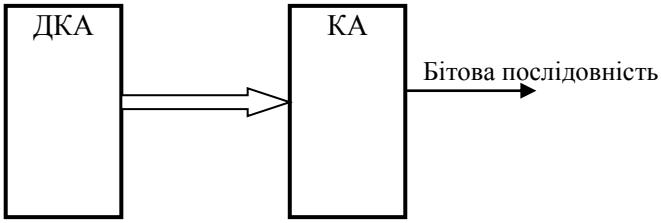

Рисунок 1 – Структура генератора

ДКА – додатковий клітинний автомат містить $n \times m = N$ клітин, кожна з яких електрично зв’язана входами і виходами з усіма клітинами, що належать її околиці за околицею Мура. Клітина ДКА представлена на рис. 2.

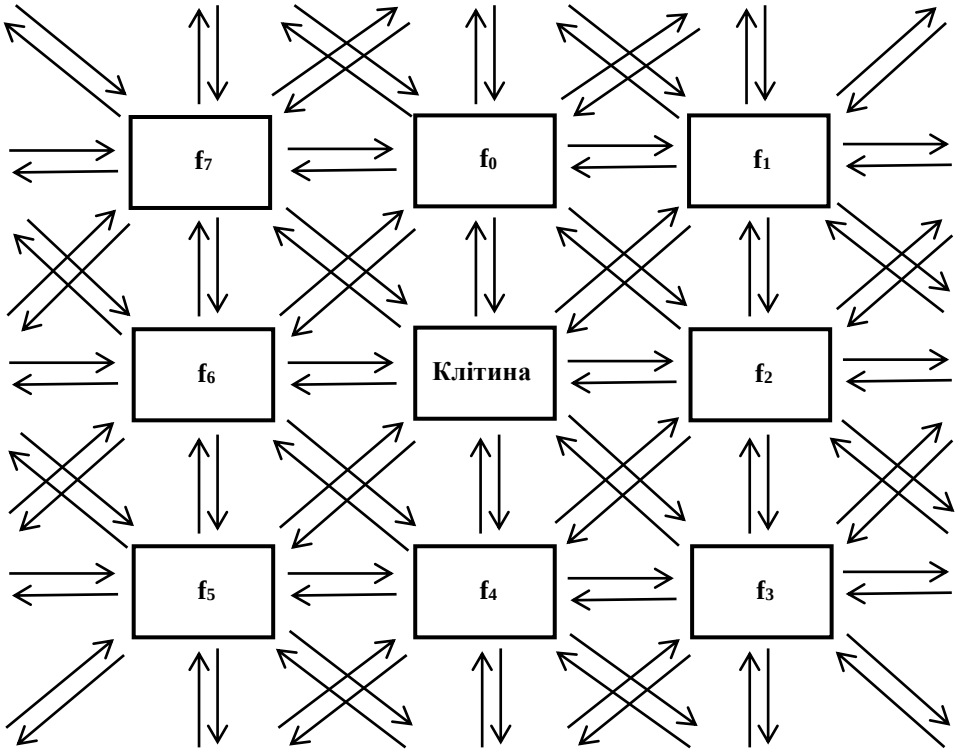

Рисунок 2 – Клітина ДКА

ДКА функціонує на кожному часовому такті так, що усі його клітини виконують операцію XOR над сигналами від клітин околиці і власним станом. Приклад роботи ДКА подано на рис. 3. На кожному такті клітина переходить у одиничний стан (або залишається в ньому), якщо кількість одиниць (сигнали надходять з виходів клітин околиці і з виходу власної клітини) на її інформаційних входах не парна і навпаки, клітина має стан логічного "0", якщо кількість одиниць – парна.

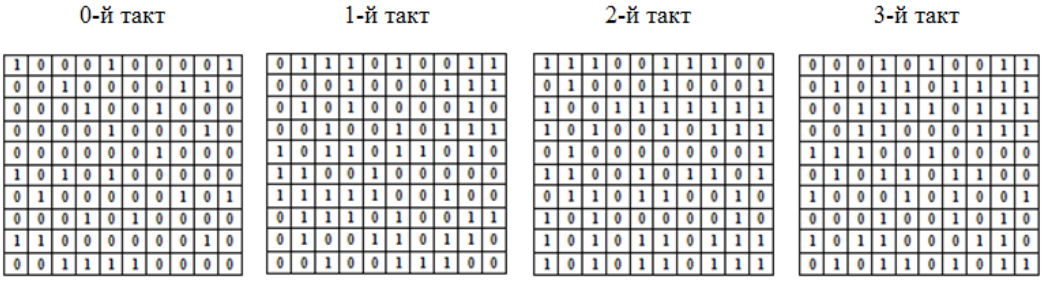

Рисунок 3 – Приклад роботи ДКА

Стан КА з кожним наступним тактовим сигналом може змінитись у одній клітині, яка на даний тактовий момент була збуджена. Також збуджена клітина переходить у стан спокою, а збудженою стає та клітина її околиці, якій переданий сигнал збудження. Приклад функціонування КА подано на рис. 4.

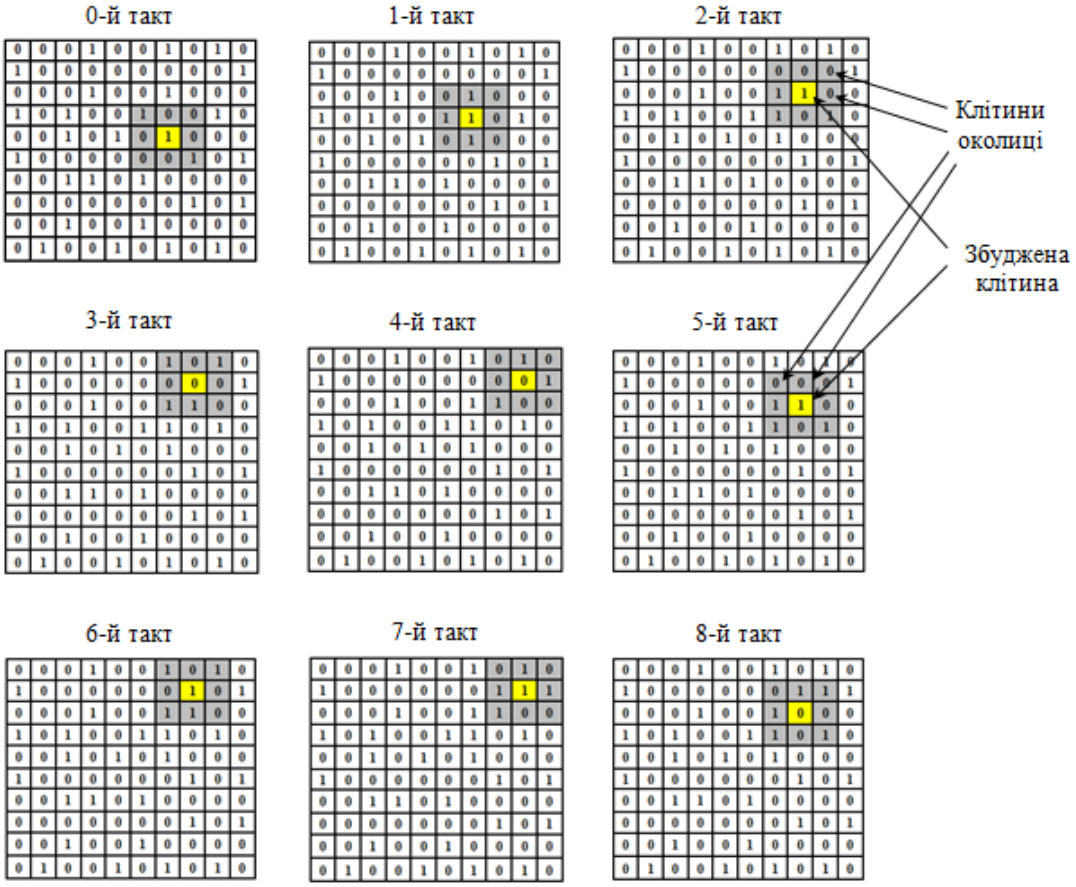

Рисунок 4 – Приклад функціонування КА

З кожним тактом клітина переміщується у полі КА згідно з заданою функцією. У даному випадку переміщення здійснюється шляхом аналізу перших трьох клітин околиці згідно кодування, поданого для околиці Мура на рис. 2. Тобто верхня сусідня клітина має нульовий індекс, права верхня сусідня клітина має індекс одиниці, права горизонтальна сусідня клітина має індекс двійки і т.д. за годинниковою стрілкою до сьомого індексу. Формування сигналів передачі збудження до клітин околиці здійснюється за табл. 1.

Таблиця 1 – Формування сигналів передачі збудження

X_2	X_1	X_0	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	1	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0
0	1	1	0	0	0	1	0	0	0	0
1	0	0	0	0	0	0	1	0	0	0
1	0	1	0	0	0	0	0	1	0	0
1	1	0	0	0	0	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1

Отже, на одному виході збудженої клітини формується одиничний сигнал до однієї із восьми клітин околиці. Інформаційний сигнал від клітини КА поступає на вихід тільки тоді, коли клітина знаходиться у збудженому стані.

Апаратна реалізація генератора. Для реалізації способу шифрування візуальної інформації на основі КА була обрана мікросхема FPGA Cyclone II (EP2C35F672C6) корпорації Altera, яка відноситься до сімейства недорогих ПЛІС початкового рівня. Основні характеристики мікросхеми наведено в [14].

На рис. 5 приведена функціональна схема генератора.

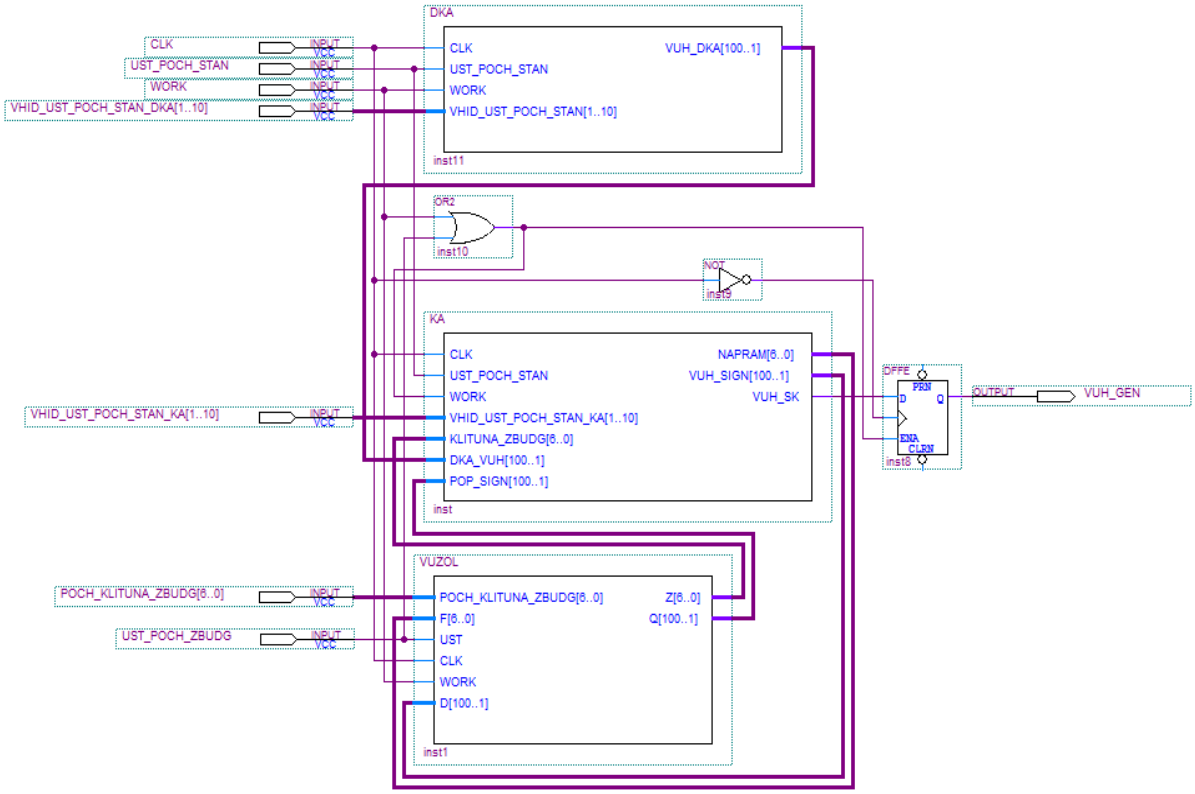

Рисунок 5 – Функціональна схема генератора

ДКА реалізований на D-тригерах із входом дозволу роботи ENA:

DD[100..1]:DFFE;

У початковий момент часу по передньому фронту сигналу синхронізації CLK за позитивним фронтом сигналу UST_POCH_STAN, а також за позитивним фронтом на вході дозволу роботи DD[].ENA=VCC, через вхід VHID_UST_POCH_STAN_DKA[1..10] до ДКА записуються початкові стани клітин, які можуть знаходитись у стані логічного “0” або “1” (див. рис. 3).

```
IF UST_POCH_STAN THEN
        DD[].ENA=VCC;
        DD[].D=(VHID_UST_POCH_STAN[1..10],DD[100..11]);
ELSE
        DD[].ENA=GND;
END IF;
```

За позитивним фронтом сигналу WORK з наступним тактовим сигналом CLK, а також за позитивним фронтом на вході дозволу роботи DD[].ENA=VCC, здійснюється аналіз околиці для кожної клітини ДКА та формується інформаційний сигнал до відповідної клітини КА.

DD[1]=(DD[1] XOR DD[91] XOR DD[92] XOR DD[2] XOR DD[12] XOR DD[11] XOR DD[20] XOR DD[10] XOR DD[100]);

DD[2]=(DD[2] XOR DD[92] XOR DD[93] XOR DD[3] XOR DD[13] XOR DD[12] XOR DD[11] XOR DD[1] XOR DD[91]);

. . .

DD[99]=(DD[99] XOR DD[89] XOR DD[90] XOR DD[100] XOR DD[10] XOR DD[9] XOR DD[8] XOR DD[98] XOR DD[88]);

DD[100]=(DD[100] XOR DD[90] XOR DD[81] XOR DD[91] XOR DD[1] XOR DD[10] XOR DD[9] XOR DD[99] XOR DD[89]);

Інформаційні сигнали до КА поступають через вихід VUH_DKA[]. Діаграма, яка описує роботу ДКА, представлена на рис. 6.

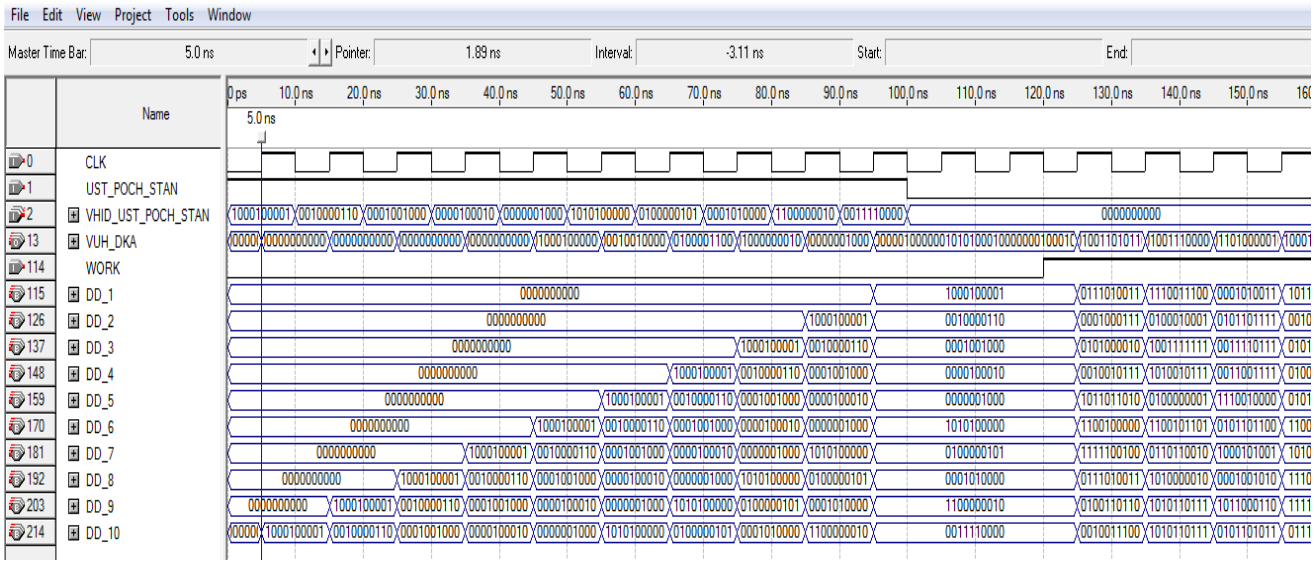

Рисунок 6 – Робота ДКА

Для реалізації функції розповсюдження збудження по КА реалізовано блок VUZOL (див. рис. 7).

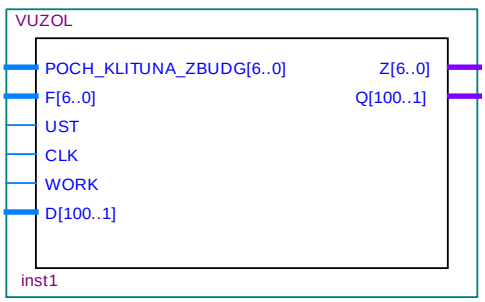

Рисунок 7 – Блок реалізації функції розповсюдження збудження

Блок VUZOL реалізує:

- вибір клітини з початковим збудженням;
- управління розповсюдженням збудження по КА;
- управління зміною станів клітин КА.

Робота блоку VUZOL здійснюється за висхідним сигналом синхронізації CLK. За позитивним фронтом сигналу UST клітина КА, визначена входом POCH_KLITUNA_ZBUDG[6..0], встановлюється у збуджений стан. Розповсюдження збудження здійснюється за позитивним фронтом сигналу WORK. Траєкторія збудження визначається виходом Z[6..0]. Крім того, до КА подається логічний стан збудженої клітини – “0” або ”1”. Нижче представлена реалізація блоку VUZOL, описана у AHDL-коді.

```
SUBDESIGN VUZOL
(POCH_KLITUNA_ZBUDG[6..0],F[6..0],UST,CLK,WORK,D[100..1]:INPUT;
Z[6..0],Q[100..1]:OUTPUT;)
VARIABLE
DD[6..0]:DFF;
FF[100..1]:DFF;
BEGIN
FF[].CLK=CLK;
DD[].CLK=!CLK;
Z[]=DD[];
IF UST THEN
DD[]=POCH_KLITUNA_ZBUDG[];
FF[]=D[];
Q[]=FF[];
ELSIF WORK THEN
DD[]=F[];
FF[]=D[];
Q[]=FF[];
ELSE
DD[]=DD[];
FF[]=FF[];
END IF;
END;
```

КА реалізований на D-тригерах із входом дозволу роботи ENA:

```
DD[100..1]:DFFE;
```

У початковий момент часу по передньому фронту сигналу синхронізації CLK за позитивним фронтом сигналу UST_POCH_STAN, а також за позитивним фронтом на вході дозволу роботи DD[].ENA=VCC, через вхід VHID_UST_POCH_STAN_KA[1..10] до КА записуються початкові стани клітин, які можуть знаходитись у стані логічного “0” або “1” (див. рис. 4).

```
IF UST_POCH_STAN THEN
DD[].ENA=VCC;
DD[].D=(VHID_UST_POCH_STAN_KA[1..10],DD[100..11]);
```

Крім того, одна з усіх клітин КА за позитивним фронтом сигналу WORK за даними від входу KLITUNA_ZBUDG[6..0] встановлюється у стан збудження. Тобто клітини КА можуть знаходитись у одному з двох інформаційних станів: логічний “0” або логічна “1”, а також у стані збудження або спокою. Формування траєкторії збудження та стан клітин КА відбувається по висхідному фронту сигналу синхронізації CLK.

```
CASE KLITUNA_ZBUDG[] IS
WHEN 1 =>
        CASE (DD[2],DD[92],DD[91]) IS
        WHEN (0,0,0) => NAPRAM[]=91;
        WHEN (0,0,1) => NAPRAM[]=92;
        WHEN (0,1,0) => NAPRAM[]=2;
        WHEN (0,1,1) => NAPRAM[]=12;
        WHEN (1,0,0) => NAPRAM[]=11;
        WHEN (1,0,1) => NAPRAM[]=20;
        WHEN (1,1,0) => NAPRAM[]=10;
        WHEN (1,1,1) => NAPRAM[]=100;
        END CASE;
DD[1]=(DKA_VUH[1] XOR POP_SIGN[1] XOR DD[91] XOR DD[92] XOR DD[2] XOR
DD[12] XOR DD[11] XOR DD[20] XOR DD[10] XOR DD[100]);
        DD[1].ENA=VCC;
        VUH_SK=DD[1];
        VUH_SIGN[1]=DD[1];
                                                    . . .
WHEN 100 =>
        CASE (DD[91],DD[81],DD[90]) IS
        WHEN (0,0,0) => NAPRAM[]=90;
        WHEN (0,0,1) => NAPRAM[]=81;
        WHEN (0,1,0) => NAPRAM[]=91;
        WHEN (0,1,1) => NAPRAM[]=1;
        WHEN (1,0,0) => NAPRAM[]=10;
        WHEN (1,0,1) => NAPRAM[]=9;
        WHEN (1,1,0) => NAPRAM[]=99;
        WHEN (1,1,1) => NAPRAM[]=89;
        END CASE;
        DD[100]=(DKA_VUH[100] XOR POP_SIGN[100]  XOR DD[90]  XOR DD[81]
XOR DD[91]  XOR DD[1]  XOR DD[10]  XOR DD[9]  XOR DD[99]  XOR DD[89] );
        DD[100].ENA=VCC;
        VUH_SK=DD[100];
        VUH_SIGN[100]=DD[100];
WHEN OTHERS => DD[].ENA=GND;
END CASE;
```

На вихід VUH_SK КА поступає тільки логічний стан тої клітини, яка знаходиться у збудженому стані.

Для вирівнювання фронту сигналу VUH_SK від КА застосовано D-тригер із входом дозволу роботи ENA, який працює по низхідному сигналу CLK. На вхід дозволу роботи ENA подається сигнал UST_POCH_ZBUDG або WORK. Нижче представлені діаграми роботи генератора (див. рис. 8 і 9). Основні характеристики реалізації наведені в табл. 2.

Таблиця 2 – Характеристики роботи генератора

Параметр	Характеристики швидкодії
Номінальна тактова частота	71,75 МГц
Номінальна швидкодія	9,69 Гбіт/с
Максимальна тактова частота	420 МГц
Максимальна швидкодія	56,7 Гбіт/с
Використання ресурсів FPGA	
Загальна кількість логічних елементів	2215 / 33 216 (7%)
Комбінаційних без тригера	308
Тригерів з комбінаційною частиною	1907

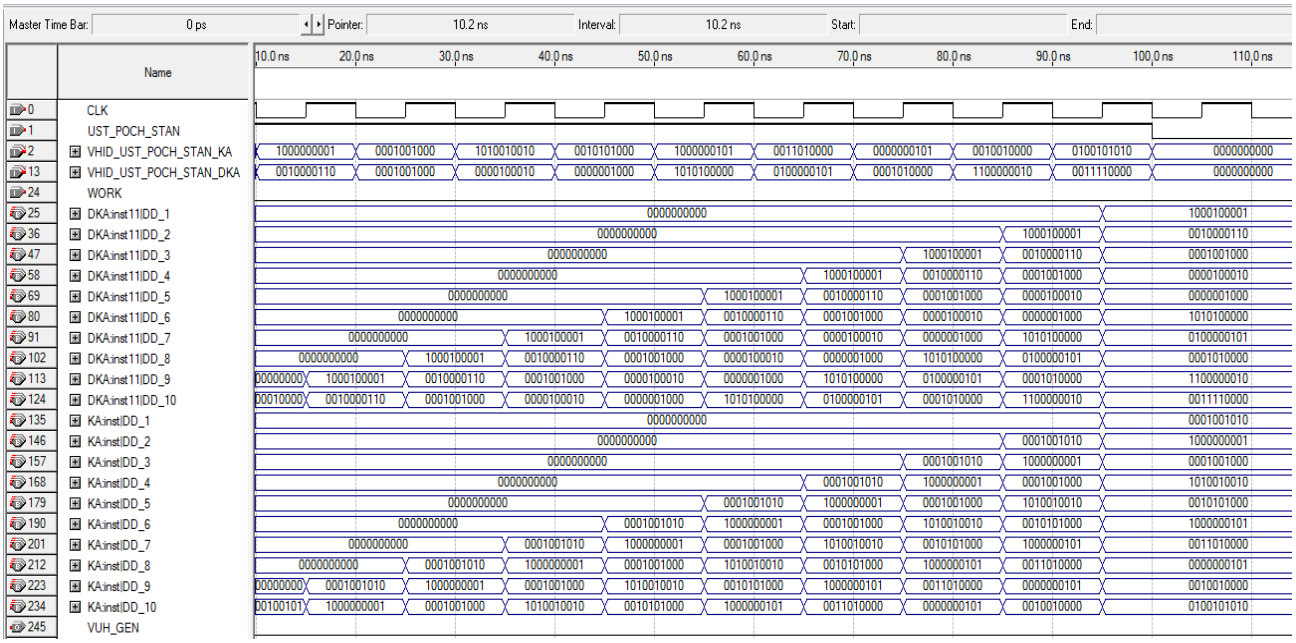

Рисунок 8 – Запис початкових станів клітин КА та ДКА

Рисунок 9 – Робота генератора

Висновки. Оскільки зображення подається великим масивом даних, який кодується бітовою послідовністю великої довжини, використання ключа шифрування обмеженої довжини послаблює стійкість шифру відеоінформації. Найбільш ефективне шифрування відеоданих дає використання ключа, довжина якого відповідає довжині бітової послідовності, що кодує відеозображення. Ключ задається не як готова бітова послідовність, а як коди операцій, які виконуються генератором. Ключова послідовність формується згідно заданої організації КА та ДКА. Довжина ключової гами може бути збільшена шляхом збільшення розмірності КА, а також вдалого вибору локальної функції переходів. Псевдовипадковість формування ключової гами підвищує надійність захисту та стійкість до зламу. Достатньо знати початкові установки КА та ДКА, щоб сформувати бітову ключову гаму з великим періодом повтору. За рахунок трьохмірного кодування зображень та використання технологій клітинних автоматів підвищується швидкодія шифрування у порівнянні з прототипом, оскільки усувається потреба зчитування станів

околиці основного КА. Апаратна реалізація на ПЛІС доводить високу ефективність використання даного підходу щодо захисту цифрових відеоданих. Отримані апаратні характеристики системи значно підвищують надійність функціонування, а також зменшують залежність від необхідності застосування додаткових програмних та апаратних засобів перетворення відеоданих.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] А. Володин, В. Митько, и Е. Спинко, “Шифрование видеосигнала – практикум разработчика”. [Электронный ресурс]. Доступно: http://www.chipinfo.ru/literature/chipnews/200103/2.html. Дата обращения: Сент. 10, 2016.

[2] Г. Басалова, “Шифрование, помехоустойчивое кодирование и сжатие информации”. [Электронный ресурс]. Доступно: http://www.intuit.ru/studies/courses/691/547/lecture/12397. Дата обращения: Сент. 10, 2016.

[3] S. Wolfram, “Cellular automata”, in *Cellular Automata and Complexity*. [Online]. Available: http://www.stephenwolfram.com/publications/cellular-automata-complexity/pdfs/cellular-automata.pdf. Accessed on: Sept. 10, 2016.

[4] M. Bruno, and P. Sole, “Pseudo-random Sequences Generated by Cellular Automata”, in *Proc. International conference on ralations, orders and graphs. Interaction with computer scince*, Mandia, Tunisia, May 2008. [Online]. Available: https://arxiv.org/abs/0807.3865. Accessed on: Sept. 10, 2016.

[5] С.В. Валов, А.Я. Ольховский, О.А. Павлов, Ю.Ф. Пахомов, и В.Г. Стародубцев, “Устройство кодирования и декодирования речевых сигналов”, *Патент Российской Федерации № 2050698*, Дек. 20, 1995.

[6] Ю.Б. Рицар, М.П. Козловський, М.В. Шовгенюк, С.В. Волошиновський, та З.Д. Грицьків, “Спосіб засекречування візуальної інформації”, *Патент України № 22285*, Черв. 15, 2001.

[7] В.В. Мохор, С.М. Білан, А.А. Демаш, “Спосіб засекречування візуальної інформації”, *Патент України* № 99465, Черв. 10, 2015.

[8] А.В. Яковенко, В.В. Ларин, и Р.В. Тарнополов, “Подходы для защиты видеоинформации на основе устранения избыточности в инфокоммуникациях”, *Сучасна спеціальна техніка*, № 2 (37), с. 82-89, 2014.

[9] И.Л. Ерош, А.М. Сергеев, и Г.П. Филатов, “О защите цифровых изображений при передаче по каналам связи”, *Информационные управляющие системы*, № 5, с. 20-22, 2007.

[10] Л.А. Мироновский, и В.А. Слаев, *Стрип-метод преобразования изображений и сигналов*. Санкт-Петербург, Россия: Политехника, СПб., 2006.

[11] L. Tang, “Methods for encrypting and decrypting MPEG video data efficiently”, in *Proc. of the fourth ACM international conference on Multimedia*, Boston, USA, 1996, pp. 219-229. doi: 10.1145/244130.244209.

[12] H. Cheng, and X. Li, “On the Application of image Decomposition to Image Compression and Encryption”, in *Proc. of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, Essen, Germany, 1996, pp. 116-127. doi: 10.1007/978-0-387-35083-7_11.

[13] T. Kunkelmann, and U. Horn, “Partial Video Encryption based on Scalable Coding”, in *Proc. 5th International Workshop on Systems, Signals and Image Processing*, Zagreb, Croatia, 1998, pp. 215 – 218.

[14] S. Bilan, and A. Demash, “High performance encryption tools of visual information based on cellular automata”, *Information Technology and Security*, vol. 4. iss. 1 (6), pp. 62-75, January-June 2016.

Стаття надійшла до редакції 24.09.2016.

REFERENCES

[1] A. Volodin, V. Mitko, and E. Spinko, "Video signal encryption – developer workshop". [Online]. Available: http://www.chipinfo.ru/literature/chipnews/200103/_2.html. Accessed on: Sept. 10, 2016.

[2] G. Basalova, "Encryption, noise-immune encoding and information compression". [Online]. Available: http://www.intuit.ru/studies/courses/691/547/lecture/_12397. Accessed on: Sept. 10, 2016.

[3] S. Wolfram, "Cellular automata", in *Cellular Automata and Complexity*. [Online]. Available: http://www.stephenwolfram.com/publications/cellular-automata-complexity/pdfs/cellular-automata.pdf. Accessed on: Sept. 10, 2016.

[4] M. Bruno, and P. Sole, "Pseudo-random Sequences Generated by Cellular Automata", in *Proc. International conference on ralations, orders and graphs. Interaction with computer scince*, Mandia, Tunisia, May 2008. [Online]. Available: https://arxiv.org/abs/0807.3865. Accessed on: Sept. 10, 2016.

[5] S.V. Valov, A.Ia. Olkhovskii, O.A. Pavlov, Iu.F. Pakhomov, and V.G. Starodubtsev, "Speech signals encoding and decoding device", *RU Patent Appl.* 2050698, Dec. 20, 1995.

[6] Yu.B. Rytsar, M.P. Kozlovskyi, M.V. Shovheniuk, S.V. Voloshynovskyi, and Z.D. Hrytskiv, "The method of visual information securing", *UA Patent Appl.* 22285, June 15, 2001.

[7] V.V. Mokhor, S.M. Bilan, and A.A. Demash, "The method of securing visual information", *UA Patent Appl.* 99465, June. 10, 2015.

[8] A.V. Iakovenko, V.V. Larin, and R.V. Tarnopolov, "Approaches for protection vydeoynformatsyy based on Elimination of redundancy in ynfokommunykatsyyah", *Modern special equipment*, no. 2 (37), pp. 82-89, 2014.

[9] I.L. Erosh, A.M. Sergeev, and G.P. Filatov, "Protection of images during transfer via communication channels", *Information and Control Systems*, no. 5, pp. 20-22, 2007.

[10] L.A. Mironovskii, and V.A. Slaev, *Strip method of images and signals transformation*. Saint Petersburg, Russia: Politekhnika, SPb, 2006.

[11] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently", in *Proc. of the fourth ACM international conference on Multimedia*, Boston, USA, 1996, pp. 219-229. doi: 10.1145/244130.244209.

[12] H. Cheng, and X. Li, "On the Application of image Decomposition to Image Compression and Encryption", in *Proc. of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, Essen, Germany, 1996, pp. 116-127. doi: 10.1007/978-0-387-35083-7_11.

[13] T. Kunkelmann, and U. Horn, "Partial Video Encryption based on Scalable Coding", in *Proc. 5th International Workshop on Systems, Signals and Image Processing*, Zagreb, Croatia, 1998, pp. 215 – 218.

[14] S. Bilan, and A. Demash, "High performance encryption tools of visual information based on cellular automata", *Information Technology and Security*, vol. 4. iss. 1 (6), pp. 62-75, January-June 2016.

СТЕПАН БЕЛАН,
АНДРЕЙ ДЕМАШ

ПРОГРАММНО-АППАРАТНАЯ РЕАЛИЗАЦИЯ ГЕНЕРАТОРА ПОДКЛЮЧЕЙ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

В статье рассматриваются подходы и основные проблемы существующих методов шифрования видеоинформации. Описан метод шифрования видеоданных на основе клеточных автоматов, который позволяет повысить надежность защиты видеоинформации, увеличить длину ключа шифрования, повысить быстродействие засекречивания изображения и упростить подготовку исходных параметров блока формирования

подключей. Описана программно-аппаратная реализация генератора подключей для системы шифрования видеоинформации, в основу которой положен вышеупомянутый метод. Данный генератор реализован с использованием двух клеточных автоматов, что позволяет формировать ключевую гамму в неявном виде. Основной клеточный автомат осуществляет передачу сигнала возбуждения от клетки к клетке, а дополнительный клеточный автомат осуществляет смену состояний всех своих клеток согласно заданной функции и выбранной окрестности. Гамма зависит от начальной карты состояний клеточных автоматов и начальных настроек траектории движения. Генератор реализован на дешевых ПЛИС с высокими показателями по производительности, что позволяет зашифровывать видеоинформацию в реальном времени в процессе передачи ее по каналам связи.

Ключевые слова: шифрование, видеоинформация, клеточный автомат, гамма, ПЛИС.

STEPAN BILAN,
ANDRII DEMASH

HARDWARE-SOFTWARE REALISATION OF THE GENERATOR OF SUBKEY BASED ON THE CELLULAR AUTOMATA

This article describes approaches and the basic problems of existing methods of encryption methods – low reliability of information protection and low speed of their implementation. Is described the method of encryption of videodata based on cellular automata, which allows to raise reliability of protection of a videoinformation, to increase length of a key of encryption, to raise speed of encryption images and to simplify preparation of initial parameters for the subkeys formation block. According to aforementioned method, the image that you want to encrypt, digitizes and submit to the encryption block in distorted form. This form is due to the law given scan, which belongs to the key data. The encryption block uses subkeys, which generate by special structure, implemented on two cellular automata. The main cellular automata transmits excitation signal from cell to cell and additional cellular automata carries alteration of all its cells under a given function and selected neighborhood. Is described software and hardware implementation of subkeys generator for video encryption system, which is based on the aforementioned method. This generator is implemented using two cellular automata, which allows you to create key gamma in implicit form. The additional cellular automata operate at every cycle time so that all its cells perform XOR operation on signals from the cell neighborhood and its own state. The state of the main cellular automaton with each successive clock signal can change in a single cell, which at the time clock was excited. Also excited cell goes dormant and cell neighborhood, which passed excitation signal, becomes excited. Information signal from cell of cellular automata goes to output only when the cell is in an excited state. Gamma depends on the initial map state of cellular automata and initial settings of trajectory. The generator is implemented on low-cost FPGA with high performance, which allow encrypting videoinformation in real time in the transmission of the communication channels.

Keywords: encryption, video, cellular automata, Field-Programmable Gate Array.

Степан Миколайович Білан, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: bstepan@ukr.net.

Андрій Андрійович Демаш, заступник начальника науково-дослідного відділу, Державний науково-дослідний інститут спеціального зв'язку та захисту інформації, Київ, Україна.

E-mail: irlandec_lup@ukr.net.

Степан Николаевич Белан, кандидат технических наук, доцент, доцент кафедри кибербезопасности и использования автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Андрей Андреевич Демаш, заместитель начальника научно-исследовательского отдела, Государственный научно-исследовательский институт специальной связи и защиты информации, Киев, Украина.

Stepan Bilan, candidate of technical sciences, associate professor, associate professor of cybersecurity and application of information systems and technologies academic department, Institute of special communications and information protection National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Andrii Demash, deputy head of research division, State research institute for special telecommunication and information protection, Kyiv, Ukraine.

УДК 004.032.2:512.624

ШОЛОГОН ОЛЬГА,
ШОЛОГОН ЮЛІЯ

ЗМЕНШЕННЯ ЗАГАЛЬНОЇ КІЛЬКОСТІ ЛОГІЧНИХ ЕЛЕМЕНТІВ У КЛАСИЧНОМУ ДВОКРОКОВОМУ ПОМНОЖУВАЧІ ЗАСОБАМИ VIVADO HLS

В Україні практично всі реалізації захисту інформації є програмними, основним недоліком яких, є недостатня стійкість до зламу, тому для збільшення надійності реалізації захисту інформації виникає необхідність у створенні апаратних засобів для виконання операцій над елементами скінченних полів. Однією з можливостей є реалізація на програмованих логічних інтегральних схемах. Як правило, помножувачі в полях Галуа $GF(p^m)$ будуються за допомогою засобів мови VHDL. Основним недоліком такого підходу є значні часові та апаратні затрати. В даній статті, запропоновано будувати помножувач у полях Галуа $GF(p^m)$ за допомогою середовища Vivado HLS. В роботі розглянуто метод оптимізаціїї при якому використовувались типи з визначеною точністю. В результаті досліджень, було доведено ефективність використання середовища Vivado HLS у порівнянні із засобами VHDL. Кількість найпростіших логічних елементів було зменшено у 3 рази, а також кількість тригерів із динамічним і потенційним управлінням скоротились вдвічі. Використання даного методу дає можливість розробляти помножувачі у полях Галуа $GF(p^m)$ з великим порядком.

Ключові слова: захист інформації, поля Галуа $GF(p^m)$, Vivado HLS, VHDL, класичний двокроковий алгоритм, типи з визначеною точністю

Постановка проблеми. Розробка вбудованих комп'ютерних систем нерозривно пов'язана з розвитком елементної бази, на якій виконується реалізація програми. Від ефективності використання апаратних засобів залежить швидкість реалізації алгоритмів та їх ефективність [1]. Переважно для програмування складних вбудованих систем використовуються програмовані логічні інтегральні схеми (ПЛІС) [2]. У зв'язку з цим виникає необхідність у розробці механізмів для забезпечення безпеки ПЛІС [3]. Це можна досягти шляхом виконання операцій над елементами скінченних полів [4].