Міністерство освіти і науки України

Всеукраїнський конкурс студентських наукових робіт
«Комп’ютерна інженерія»

Наукова робота

Засоби захисту інформаційної безпеки банку

Шифр Панцир

2019 рік

ЗМІСТ

ВСТУП ……2

1 Дослідження властивостей інформаційних потоків обміну даних при встановленні з’єднання в мережах зв’язку …….....4

2 Реалізація алгоритму блоково-динамічного шифрування в системах «клієнт-банк» ……..……6

2.1 Модифікована модель реалізації блочного шифрування інформації з динамічним формуванням ключа в системах «клієнт-банк» при встановленні з’єднання ……6

2.2 Алгоритмічно-функціональне моделювання методу Blowfish на основі алгоритму блоково-динамічного шифрування в системах «клієнт-банк» ……..……9

2.3 Практична реалізація шифрування з динамічними змінами підключів в системі «клієнт-банк» ……....20

ВИСНОВКИ ……..…..26

ПЕРЕЛІК ПОСИЛАНЬ ……..…27

ВСТУП

Інформація – одне з найважливіших джерел процвітання будь-якої держави, банку чи фірми. Недарма кажуть: “Хто володіє інформацією, той володіє світом”. Будь-яке управлінське рішення базується і коштує тієї інформації, на основі якої воно прийняте.

Витік інформації може завдати серйозної шкоди банку, його економічному становищу та іміджу, часто дозволяючи конкурентам зайняти провідні позиції на ринку, а іноді призводить і до банкрутства.

Уже сьогодні потребують негайного вирішення такі проблеми:

- забезпечення безпеки обміну інформацією між відділами банків, що працюють в режимі єдиного кореспондентського рахунку в Національному банку України.

- безпеки інформації, що циркулює у відомчих мережах передачі даних. Уже існує відомча мережа передачі даних банку “Україна”;

- відсутності нормативно-правової бази, яка дає змогу вирішувати питання електронного грошового обігу – як між відділами банків, так і між банками і їхніми клієнтами (в системах “Клієнт–Банк”);

- відсутності єдиних стандартів галузі – як найпоширеніших алгоритмів, так і термінології;

- на сьогоднішній день ніякими засобами, крім досить слабких інструментів найпопулярніших мережевих операційних систем, не забезпечується безпека інформації;

Без комплексного вирішення цих та інших питань створити надійну систему електронних розрахунків і зробити доступ до неї простим і зручним для всіх її учасників є завданням недосяжним.

Найбільш вразливим місцем в системі «клієнт-банк» є пересилання документів між клієнтом і банком. Це породжує три типи проблем, пов’язаних з необхідністю:

- взаємного розпізнавання абонентів (проблема автентифікації при встановленні зв’язку);

- захист документів, які передаються каналами зв’язку (забезпечення цілісності та конфіденційності документів);

- захист самого процесу обміну документами (проблема доведення факту відправлення/доставки документа).

У банку в процесі обробки прийнятого ЕПД можуть виникнути такі проблеми:

- підтвердження цілісності та юридичної значимості прийнятого документа (ідентифікація та автентифікація відправника, а також автентифікація повідомлення);

- забезпечення захисту від несанкціонованої модифікації вже прийнятого ЕПД або від нав’язування хибної інформації зловмисником всередині відділення банку;

- захист цілісності використовуваних при обробці ЕПД в банку програмних засобів для блокування можливостей несанкціонованого доступу і модифікації інформації про стан рахунків клієнта;

Отже, для забезпечення надійності роботи системи «клієнт-банк» засоби захисту мають забезпечувати:

- ідентифікацію та автентифікацію клієнта-відправника ЕПД з однозначною авторизацією документа;

- автентифікацію ЕПД;

- автентифікацію програмного забезпечення, яке функціонує у клієнта в банку;

- автентифікацію абонентів у процесі встановлення зв’язку і передачі повідомлення;

- приховування смислового змісту повідомлення, що передається;

- захист сформованих ЕПД від несанкціонованого доступу як у клієнта, так і в банку;

- фіксацію фактів прийому (передачі) документів з веденням відповідних архівів і журнальних файлів.

Метою роботи є визначення принципів роботи і розробка апаратних засобів для шифрування інформації та збільшення криптостійкості блочних алгоритмів в системі «Клієнт-Банк» на основі введення динамічного ключа.

Об'єктом досліджень є криптографічний захист інформації при встановленні з’єднання від несанкціонованого користування.

Предметом досліджень засоби блочного шифрування інформації в системі «клієнт-банк».

Методи досліджень базуються на теорії криптографії, теорії алгебри логіки, теорії скінченних автоматів та комп'ютерному моделюванні.

1 Дослідження властивостей інформаційних потоків обміну даних при встановленні з’єднання в мережах зв’язку

Державна інформація представляє великий інтерес для кримінальних елементів. Сьогодні у керівництва більшості державних організацій немає сумнівів щодо необхідності серйозно піклуватися про інформаційну безпеку (у збереженні державних таємниць, забезпеченні безпеки електронних документів в системі «клієнт-банк»). Застосування сучасних інформаційних технологій в державних системах розширює можливості для різних зловживань, пов’язаних з використанням обчислювальної техніки (так званих «комп'ютерних злочинів»).

Щорічні втрати від злочинів в цій сфері складають в світі, за різними оцінками, від 170 млн. до 10 млрд. доларів США. За деякими даними, в промислово розвинених країнах середній збиток від одного комп'ютерного злочину (а значну частку таких злочинів складають зловживання в фінансовій сфері) близький до 450 тис. дол., а щорічні сумарні втрати в США і Західній Європі досягають 100 млрд. і 35 млрд. дол. США, відповідно. У останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов’язаних з комп'ютерною злочинністю і в Україні.

Актуальність проблеми захисту інформації пов’язана із зростанням можливостей обчислювальної техніки та введенням нових інформаційних технологій. Розвиток засобів, методів і форм автоматизації процесів обробки інформації і масове застосування персональних комп'ютерів роблять інформацію дуже уразливою.

Саме тому для протидії комп'ютерним злочинам або зменшення збитку від них необхідно грамотно вибирати заходи і засоби забезпечення захисту інформації від навмисного руйнування, крадіжки та несанкціонованого доступу.

Для захисту корпоративної мережі використовуються такі стандартні методи захисту, як шифрування даних, аутентифікація, забезпечення цілісності при передачі даних, конфіденціальність інформації, тобто ті засоби захисту, які передбачені операційною системою Windows 2007. В корпоративних мережах з використанням Active Directory або інших, як правило, використовуються довірчі відносини та метод шифрування даних з відкритим ключем.

Для забезпечення безпеки протоколу IP використовується механізм Керування безпекою IP (IP Security Management), який дозволяє призначати й застосовувати політику безпеки IP, що гарантує захищений обмін інформацією для всієї мережі. Механізм безпеки IP являє собою реалізацію протоколу безпеки IP (IP Security, IPSec), він приймає участь у захисті інформації при передачі тільки на транспортному рівні.

ISAKMP/Oakley – служба керування ключами, є локальним резидентним агентом, що отримує політику безпеки від агента політики.

IPSec дає системі можливість вибирати протоколи захисту, вирішувати, які

алгоритми використовувати та які криптографічні ключі підтримувати. Політика IPSec визначає ступінь довіри між елементами мережі.

Застосування політики закритості, в свою чергу, обмежить всі інші типи трафіку від адресатів, які не розуміють IPSec або не є частиною довіреної групи, і якщо клієнт не розуміє IPSec, то з'єднання буде неможливе.

Вимоги до забезпечення повної безпеки не завжди можуть бути повністю реалізовані. Завжди існує імовірність нападу, що зумовлює необхідність ретельного вивчення усіх можливих випадків такого розвитку подій.

Наведемо загальну блок-схему захисту корпоративної мережі в системі «клієнт-банк» (рис. 1).

На схемі зображено взаємодію служб і компонентів захисту інформації при передачі даних по мережі.

Все це свідчить про те, що механізм відкритих ключів не здатний повністю захистити корпоративну мережу системи «клієнт-банк» від зовнішнього втручання і для кращого захисту дуже секретної інформації треба віддавати перевагу передачі інформації, що зашифрована закритим ключем.

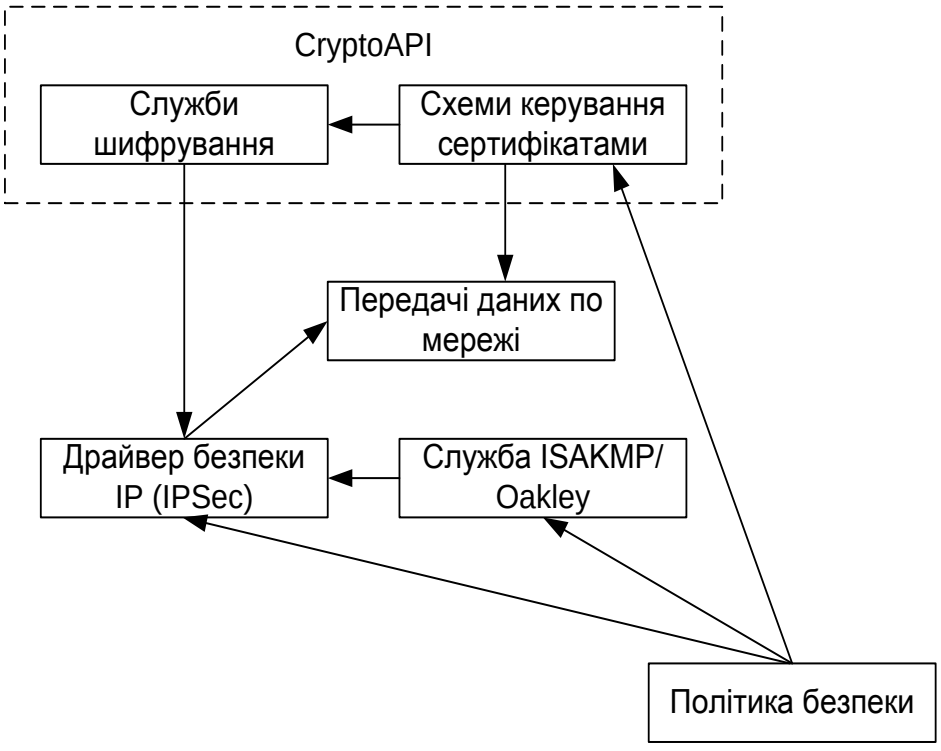

Рис. 1– Загальна блок-схема захисту корпоративної мережі в системі «клієнт-банк»

2 Реалізація алгоритму блоково-динамічного шифрування в системах «клієнт-банк»

2.1 Модифікована модель реалізації блочного шифрування інформації з динамічним формуванням ключа в системах «клієнт-банк» при встановленні з'єднання

Для передачі та прийому шифрованої інформації розроблено пристрій, блок-схему якого представлено на рис. 4.1.

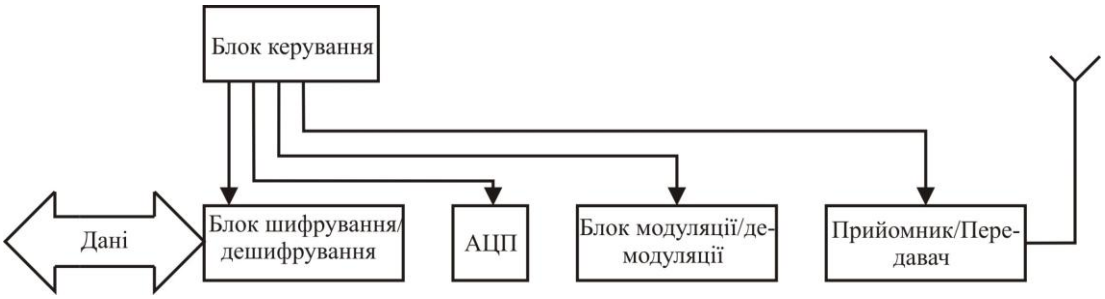

Рис. 2.1 – Пристрій передачі та прийому шифрованої інформації

Розроблений пристрій передачі та прийому шифрованої інформації складається з блоку керування, який керує усім процесом та забезпечує синхронізацію всіх пристроїв. Дані приймаються блоком Прийомник/передавач і після попередньої обробки та підсилення сигналу він передається у блок Модуляції/демодуляції, де сигнал демодулюється і готується для перетворення у цифровий вигляд. Після перетворення в цифровий вигляд у АЦП дані надходять до блоку шифрування/дешифрування, де вони дешифруються і готові до подальшого використання.

Для блоку шифрування дані повинні надходити послідовно по 64 біти, а на виході ми отримаємо потік розшифрованої інформації.

Шифрування здійснюється за алгоритмом, блок-схему якого наведено нижче (рис. 2.2), дешифрування (рис. 2.3), структурна схема (рис. 2.4).

Пристрій, функціонує наступним чином (рис. 2.4). По 32-бітних шинах даних X1 і X2 надходять дані, які шифруються. За допомогою елемента, що побітно додає за модулем 2, здійснюється побітне додавання сигналів X1 і ключів P1, та відповідний результат зберігається в пам'яті. З виходу вхідного елемента XOR сигнали по 8 біт надходять на входи $Рг_1$–$Рг_4$, які формують значення комірки, що стала активною після подання сигналів на адресний вхід. Ці значення із $Рг_1$–$Рг_4$ подаються на вхід АЛП, який виконує над даними відповідні операції і на виході якого буде утворюватись результат у 32-бітному вигляді. Кожний біт результату подається на 32-бітний елемент XOR, який побітно додає за модулем 2 з 32-бітами числа X2.

Рис. 2.2 – Схема шифрування

Рис. 2.3 – Схема дешифрування

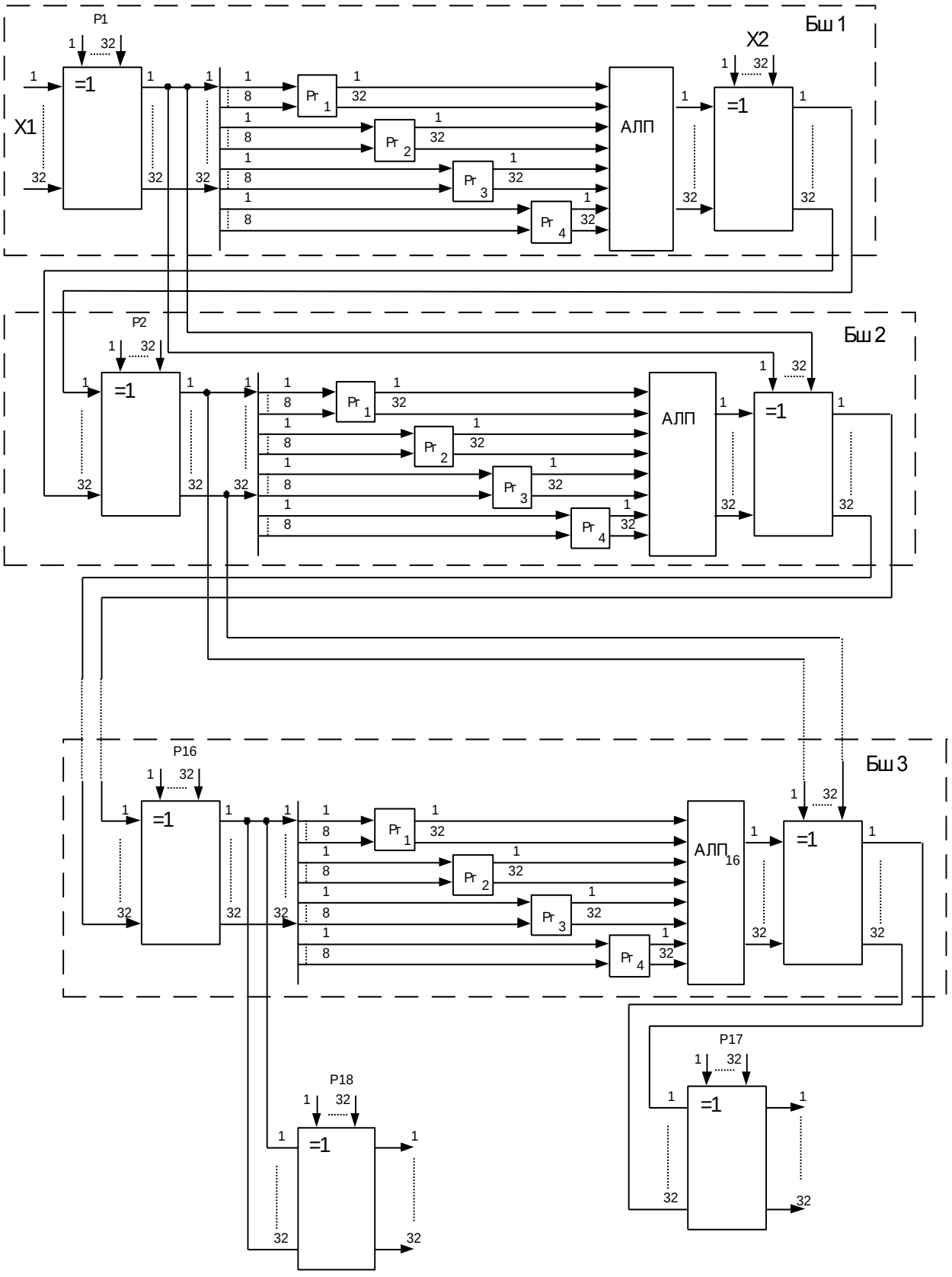

Рис. 2.4 – Структурна схема блоку шифрування

Результат побітного додавання за модулем 2 подається на вхід наступного 32-бітного елемента XOR, а на інший вхід подається значення P2. З результатом

відбуваються ті ж операції, що були описані вище, і після цього на перший вхід 32-бітного елемента XOR подається результат обчислень, а на інший вхід подається сигнал з виходу першого елемента XOR попереднього циклу. Після останнього 16 циклу на виходах першого і останнього 32-бітного елемента XOR отримаємо результуючі сигнали, які подаються на входи 32- бітних елементів XOR, з додатковим побітним додаванням за модулем 2 з значеннями P17 і P18. Після цих операцій на виходах 32-бітних XOR елементів отримаємо результат у вигляді двох 32-бітних чисел.

Пристрій дає можливість шифрувати та розшифровувати цифрові дані, які подаються на вхід, використовуючи розроблений блоково-динамічний метод шифрування. Моделювання його в середовищі Active-HDL дозволяє реалізувати його на сучасних ПЛІС.

2.2 Алгоритмічно-функціональне моделювання методу Blowfish на основі блоково-динамічного шифрування в системах «клієнт-банк»

Програмна реалізація блокового шифрування текстових повідомлень, не дає можливості суттєво підвищити швидкодію шифрування та стійкість криптоалгоритму. Альтернативою програмній реалізації алгоритму виступає його технічна реалізація, особливо перспективним напрямком є застосування сучасних ПЛІС, які набувають широкого використання в різних галузях. На даному етапі у виготовленні ПЛІС та програмного забезпечення для них бере участь ціла низка фірм, таких як Xilinx, Altera, Actel тощо.

Для моделювання і проектування електронних схем на базі ПЛІС використовуються різні прикладні програми з цілою низкою спеціалізованих мов програмування.

Однією з найбільш популярних мов моделювання електронних схем для ПЛІС є VHDL і Verilog, які дають можливість подати схемотехнічне рішення з досконалим часовим аналізом. Тому подання блоково-динамічного алгоритму шифрування даних технічною реалізацією на базі ПЛІС у вигляді VHDL моделі є доцільним з точки зору його схемотехнічно-часового аналізу.

Пристрій шифрування даних повинен шифрувати дані 32-448-бітним ключем, удосконаленим методом Blowfish.

Для створення апарату шифрування використовується технологія FPGA і середовище розробки Active-HDL. Для реалізації пристрою було створено кілька окремих блоків, які з’єднані шинами даних.

Модель пристрою складається з наступних основних блоків (рис 4.5)

sbox0_init – sbox3_init – ПЗУ, в якому знаходяться початкові значення S-блоків;

parray_init – ПЗУ, в якому знаходяться початкові значення P-блоків; crypt – блок шифрування дешифрування даних; F – арифметично-логічний блок; keychun-ker – блок для виділення 448-бітного ключа на чотири частини; parray_control – блок для роботи з P-блоками; sboxes_control – блок для роботи з S-блоками.

Дані, які будуть піддаватись шифруванню надходять через блок KCHUNK, який заповнює повний 448-бітний ключ ключем, що надійшов на вхід. Якщо вхідний ключ 448-бітний, то цей блок просто передає його до блоку PARR. Блок виконує шифрування ключа за допомогою блоку crypt, і зберігає результати в буфері parray. Для створення S-блоків використовується блок SBCTRL, який здійснює ініціалізацію S-блоків шифрування та вибірку необ-хідних значень за адресами S-блоків. Для зберігання початкових даних S-блоків служать блоки SB0_INIT-SB3_INIT, а для збереження робочих S-блоків – SB0-SB3. Блок шифрування CRY використовує блок підстановки u_F, який, використовуючи значення S-блоків, обчислює функцію: ((sbox0_data + sbox1_data) xor sbox2_data) + sbox3_data.

Для визначення стану кожної операції використовуються сигнали повідомлення про завершення певної операції, певного блоку: parray_crypt_go, crypt_done, init_parray, sub_parray, sub_parray_done, init_sboxes, sub_sboxes, sub_sboxes_done, sboxes_crypt_go, sboxes_crypt_go.

На рис. 4.5 подана структурно-функціональна схема пристрою для шифрування даних, отримана у середовищі Active-HDL.

Пристрій для шифрування може працювати в двох режимах: режимі шифрування та режимі дешифрування, для задання якого використовується вхід encrypt, 1 – шифрування, 0 – дешифрування. Але при створенні ключа при шифруванні чи дешифруванні потрібно обов’язково вказати режим шифрування для зашифрування блоків P і S.

Блок crypt виконує функції шифруваня або дешифрування даних. Для збереження поточних службових даних використовуються регістри: count_up, count_reset, xL, xR, xL_next, xR_next.

Робота блоку crypt подана таблицею 2.1

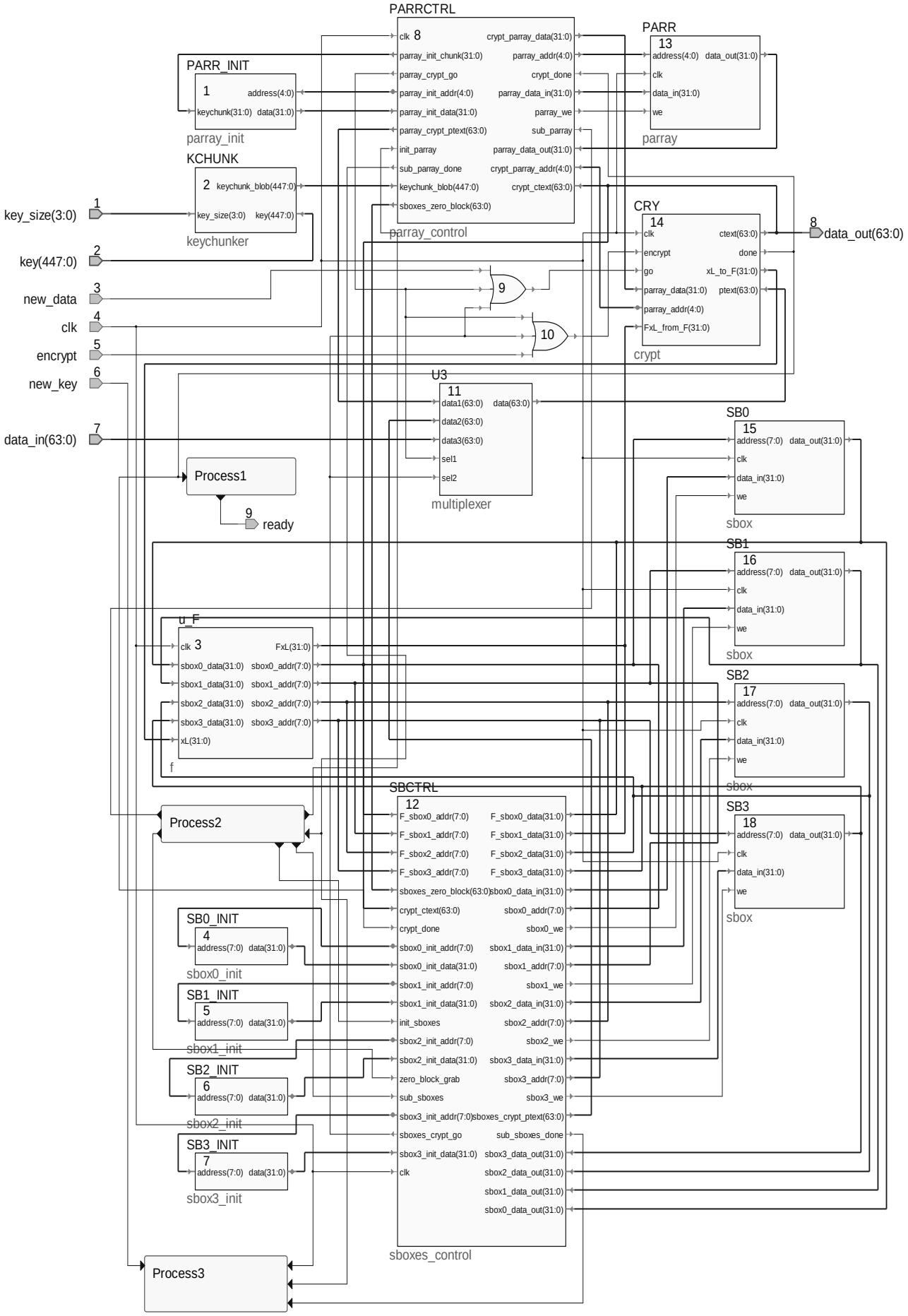

Рис.2.5 – Структурно-функціональна схема пристрою шифрування даних

Таблиця 2.1– Робота блоку crypt

Стан	Умова	Перехід	Виходи при виконанні умови	Виходи при не виконанні умови
IDLE	go = 0	IDLE	done = 1	done = 0
START	1	CRUNCH1	done = 0	-
CRUNCH1	1	CRUNCH2	done = 0	-
CRUNCH2	NO (count_up=1 AND parray_addr=16)OR NOT(count_up=0 AND parray_addr = 1)	CRUNCH1	done = 0	done = 0
FINAL1	1	FINAL2	done = 0	-
FINAL2	1	IDLE	done = 0	done = 0

Блок-схема роботи блоку шифрування подана на рис. 2.6.

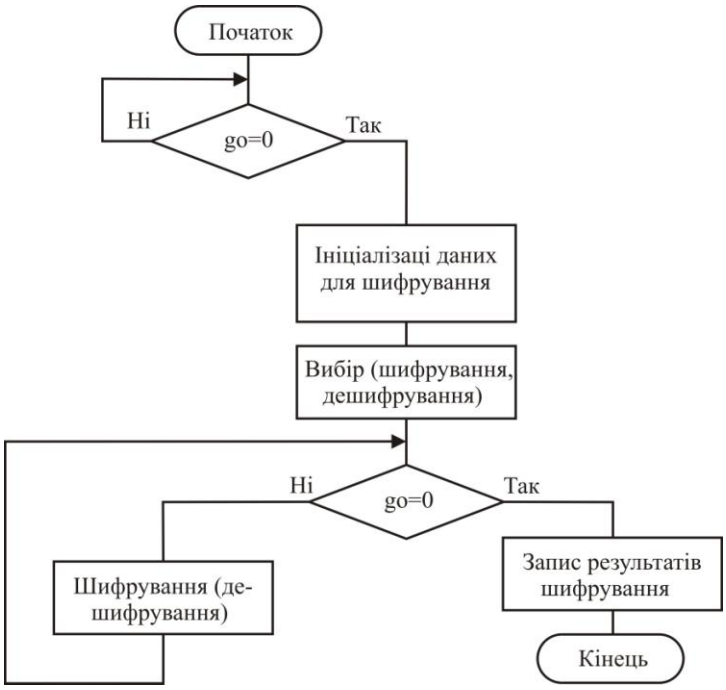

Рис. 2.6 – Блок-схема роботи блоку шифрування

Діаграму роботи пристрою керування ітераційного операційного пристрою CRIPT_STATES подано на рис. 2.7.

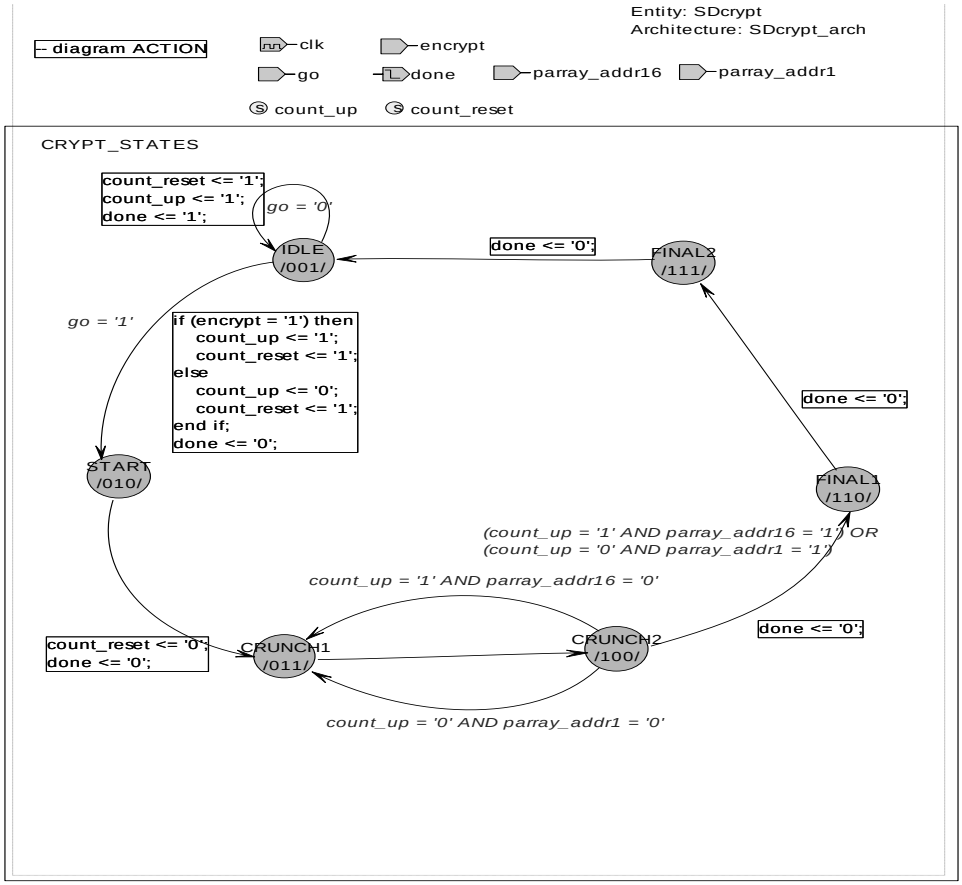

Рис. 2.7 – Діаграма роботи пристрою керування ітераційного операційного пристрою CRIPT_STATES.

Блок f – це арифметично-логічний блок, який виконує функції обчислення логічно-арифметичної функції із значень підстановки, які зчитуються із двомірних регістрів (S0-S3). Для збереження поточних службових даних використовуються регістри: a, b, c, d, в яких зберігаються адреси комірок, двомірних регістрів S0-S3. Блок функціонує в такий спосіб.

Блок keychunker створює 448-бітний ключ із ключа, що передається на вхід. На вхід може передаватись ключ різної довжини від 32 біт до 448, тому даний блок перетворює кожний ключ у 448-бітний. Для перетворення використовується двомірний регістр keychunk типу array (0 to 13) of unsigned (31 downto 0), у якому будуть формуватися значення, по 32 біти, які потім передаються на вихід.

Блок parray – це двомірний регістр, у якому зберігаються дані ключа P. Кожне значення, що зберігається по певній адресі, – 32-бітне число.

Блок sbox – це двомірний регістр, у якому зберігаються дані S-блоків. Кожне значення, що зберігається по певній адресі, – 32-бітне число.

Блок parray_control контролює всі операції з підключами P.

Для збереження поточних службових даних використовуються регістри: zero_block – 64-розрядний регістр, keychunk – двомірний регістр для зберігання частин ключа P.

Робота блоку parray_control подана в табл. 2.2.

Таблиця 2.2 – Робота блоку parray_control

Блок-схема роботи блоку керування ключем подана на рис. 2.8.

Стан	Умова	Перехід	Виходи при виконанні умови	Виходи при не виконанні умови
PASS	1	INIT	-	-
INIT	parray_init_addr = 17 AND init_parray = 0	PASS	parray_crypt_go =0sub_parray_done=1 parray_we = 0	parray_crypt_go =0parray_we = 1
SUB	NOT(crypt_done=1 AND just_started=0)	SUB	parray_crypt_go =0	parray_crypt_go= 0
SUB_WRITE1	1	SUB_WRITE2	parray_we=1	parray_crypt_go= 0
SUB_WRITE2	NOT(parray_init_addr = 17)	SUB	parray_crypt_go =1 parray_we=1	parray_crypt_go= 0parray_we=1

Діаграма роботи пристрою керування ітераційного операційного пристрою роботи з P-блоками подана на рис. 2.9.

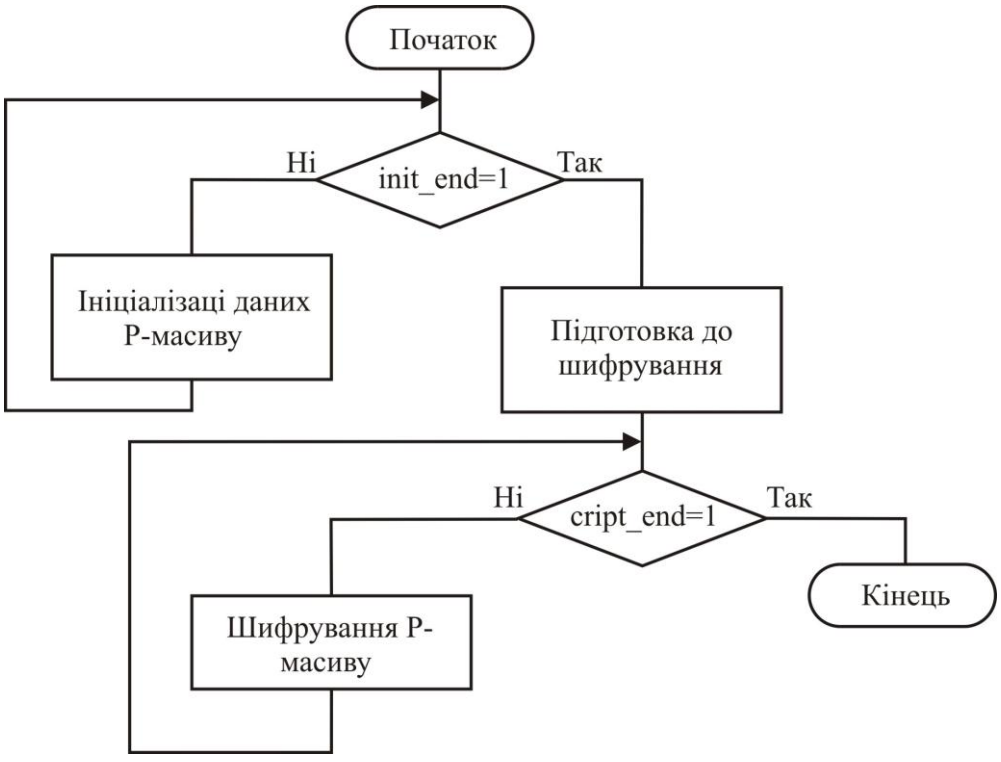

Рис. 2.8 – Блок-схема роботи блоку керування ключем

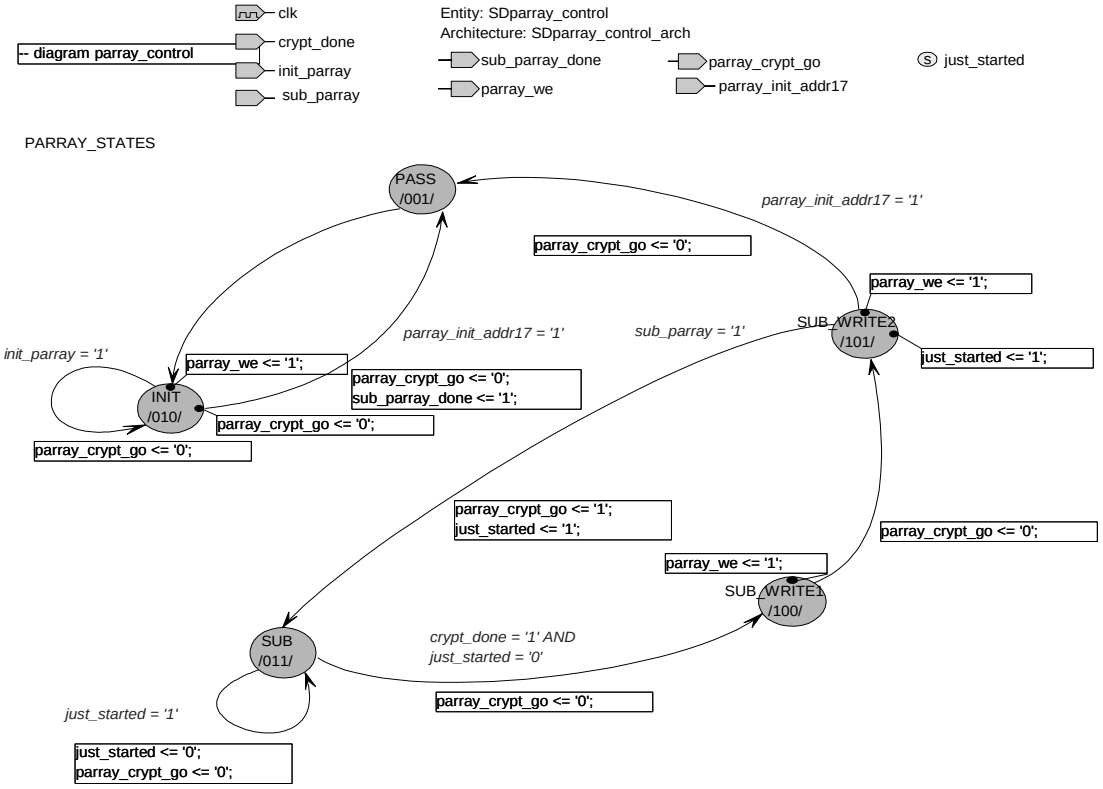

Рис. 2.9 – Діаграма роботи пристрою керування ітераційного операційного пристрою роботи з P-блоками

Parray_init подає з себе ПЗП, у якому зберігаються початкові дані ключа P. Кожне значення, що зберігається по певній 5-бітній адресі – 32-бітне число.

Для зчитування даних з ПЗП на вхід address подається адреса числа від 0 до 17 і через вихід data буде видаватись число, над яким проводяться операції XOR із 32-бітним числом, що подане на вхід keychunk.

Блок sbox0_init як ПЗП зберігає початкові дані масиву S1. Кожне значення, що зберігається по 8-бітній адресі, це 32-бітне число. Для одержання на виході data числа, яке зберігається у ПЗП, необхідно на вхід address подати 8-бітну адресу.

ПЗП – це блок sbox1_init, у якому зберігаються початкові дані масиву S2. Кожне значення, що зберігається по 8-бітній адресі, це також 32-бітне число. Для одержання на виході data числа, яке зберігається у ПЗП, необхідно на адресний вхід address подати 8-бітну адресу.

У блоці sbox2_init зберігаються початкові дані масиву S3 у вигляді чисел довжиною 32 біти кожне. Для одержання на виході data числа, яке зберігається у ПЗП, необхідно на вхід address подати 8-бітну адресу.

Блок sbox2_init зберігає початкові дані масиву S4 з числами довжиною 32 біти. Для одержання на виході data числа, яке зберігається, необхідно на вхід address подати 8-бітну адресу.

Блок sboxes_control – це блок який контролює всі операції з S-таблицями.

Для збереження поточних службових даних використовуються регістри: zero_block – 64-розрядний регістр, sboxes_counter – 9-розрядний регістр для зберігання числа підрахунку операцій.

Робота блоку sboxes_control подана таблицею 4.3. Блок-схема роботи блоку керування S-блоками подана на рис. 4.10. Діаграма переходів роботи пристрою керування ітераційного операційного пристрою роботи з S-блоками подана на рис. 2.11.

Таблиця 2.3 – Робота блоку sboxes_control

Стан	Умова	Перехід	Виходи при виконанні умови	Виходи при не виконанні умови
PASS	1	INIT	sboxes_crypt_go=0	-
INIT	sbox0_init_addr = 255	PASS	sboxes_crypt_go=0	sboxes_crypt_go=1
SUB	crypt_done=0	SUB	sboxes_crypt_go=0	sboxes_crypt_go=0
SUB_WRITE1	1	SUB_WRITE2	sboxes_crypt_go=0	-
SUB_WRITE2	NOT(sboxes_counter = 511)	SUB	sboxes_crypt_go=1	sboxes_crypt_go=0

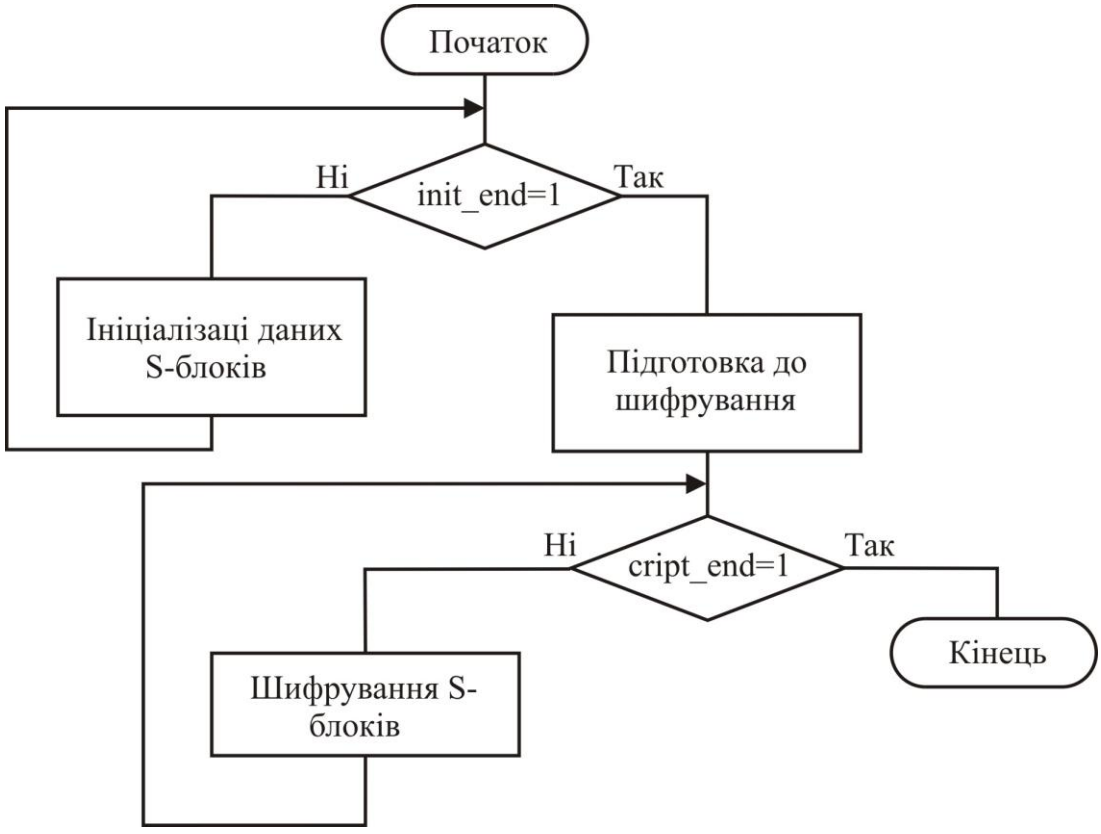

Рис. 2.10 – Блок-схема роботи блоку керування S-блоками

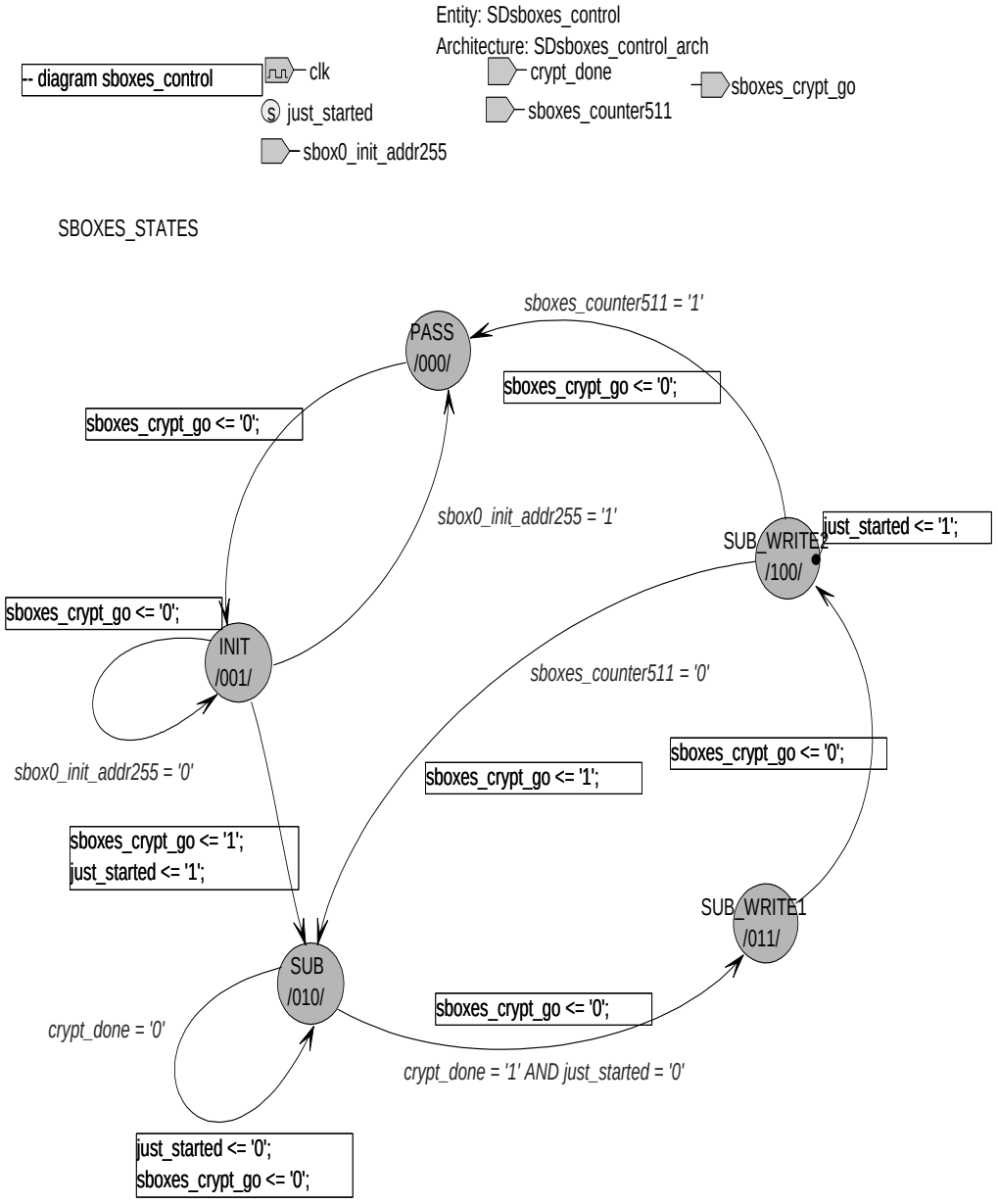

Рис. 2.11 Діаграма роботи пристрою керування ітераційного операційного пристрою роботи з S-блоками

Блок blowfish – це головний блок, який контролює всі процеси створення ключа, шифрування та дешифрування.

Робота блоку blowfish подана в таблиці 4.4. Діаграма переходів роботи пристрою керування ітераційного операційного пристрою шифрування подана на рис. 2.12.

Таблиця 2.4 – Робота блоку blowfish

Стан	Умова	Перехід
S_NORMAL	new_key=0	S_NORMAL
S_INIT_START	1	S_INIT
S_INIT	sub_sboxes_done=0	S_INIT
S_SUB_PARRAY_START	1	S_SUB_PARRAY
S_SUB_PARRAY	sub_parray_done=0	S_SUB_PARRAY
S_SUB_SBOXES_START	1	S_SUB_SBOXES
S_SUB_SBOXES	sub_sboxes_done=0	S_SUB_SBOXES

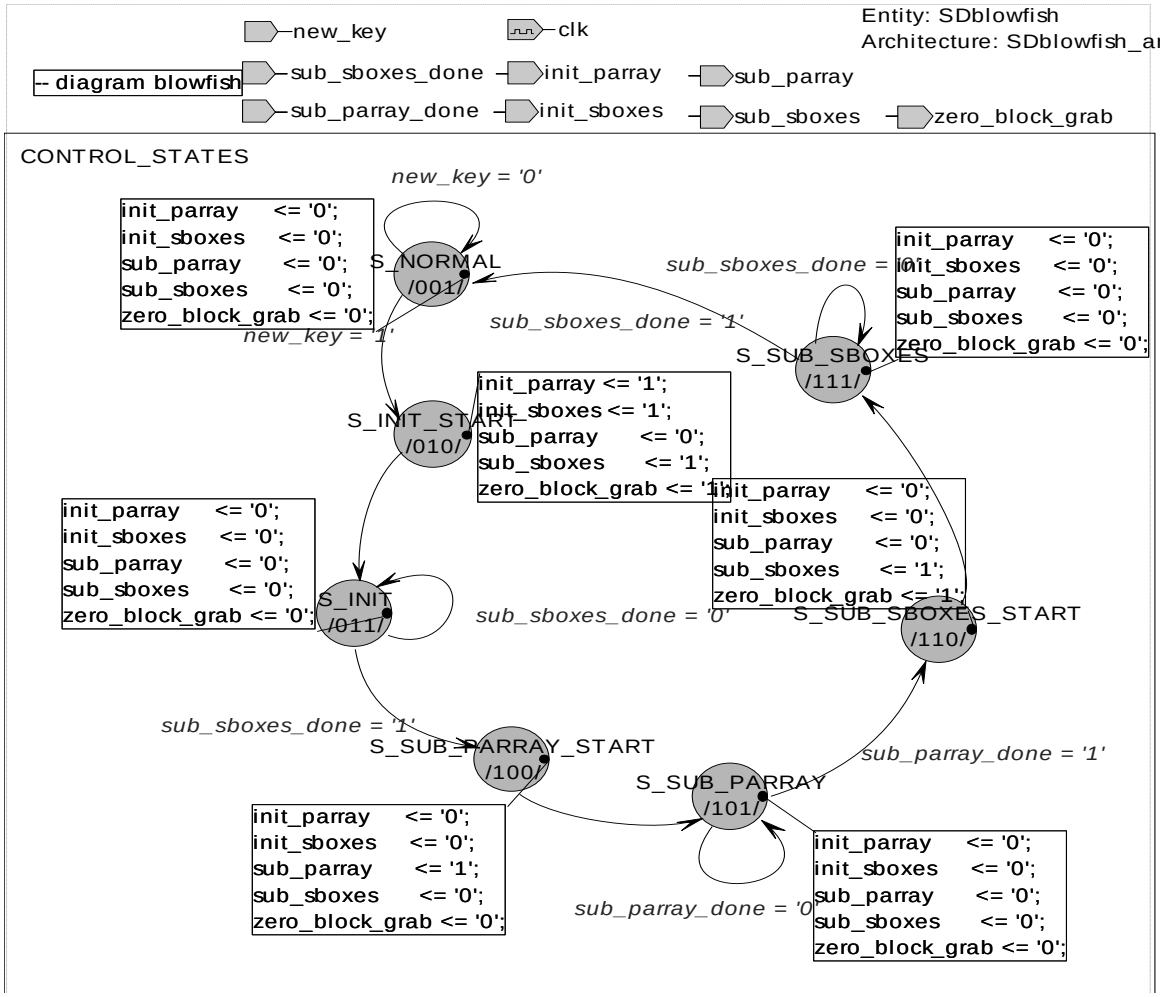

Рис. 2.12 – Діаграма роботи пристрою керування ітераційного операційного пристрою шифрування

Для більш детального опису схеми проведемо поетапний часовий аналіз на конкретному прикладі. Визначимо початкові дані.

Ключ шифрування:

f8446ff1e038ca17035f4ba1b12b6ba35b52fc0177c80eac7a501ab9e01b32c2d92f2f36aa38f52a0142eb790da98b26b155e1c348dcdb91

Дані для шифрування: 1234567890123456

На рис. 2.13 подано у часовому процесі надходження вхідних даних.

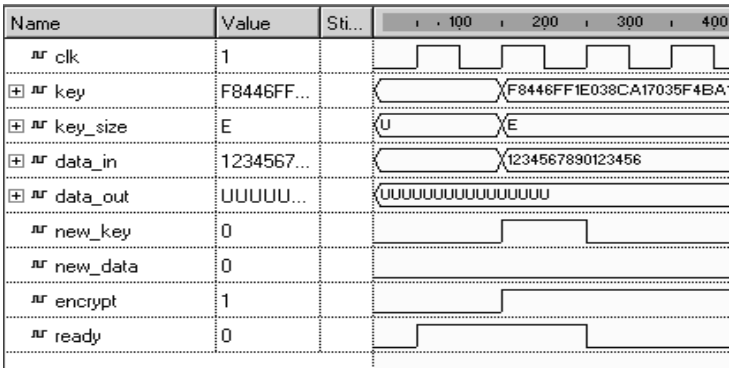

Рис. 2.13 – Часовий процес надходження вхідних даних

Закінчення режиму шифрування визначається наявністю на виході ready логічної одиниці. При цьому на виході data_out буде результат шифрування.

На рис. 2.14 подано часовий процес результату шифрування даних.

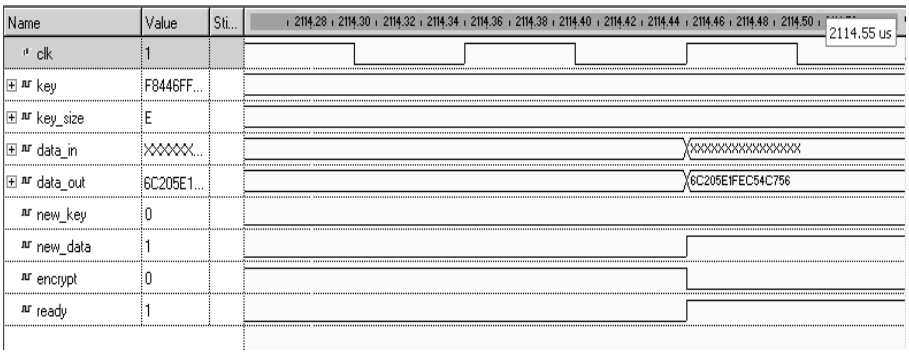

Рис. 2.14 – Часовий процес результату шифрування даних

Після шифрування отримані такі дані: 6C205E1FEC54C756

VHDL-моделювання блоково-динамічного шифрування показало процес шифрування повідомлень, а також дало можливість показати ефективність застосування ПЛІС для підвищення швидкодії реалізації запропонованого методу.

2.3 Практична реалізація швидкодіючого шифрування з динамічними змінами підключів в системах «клієнт-банк»

Практична реалізація блоково-динамічного шифрування розглядалася на прикладі шифрування конкретного повідомлення.

Перший крок шифрування полягає у створенні ключа

key = 123, keysize = 3

$key2_1$ = 3245345792

$key2_2$ = 29681548

Ініціалізуємо масив S константними числами.

В циклі ініціалізуємо P-масив за алгоритмом, поданим на рис 4.15

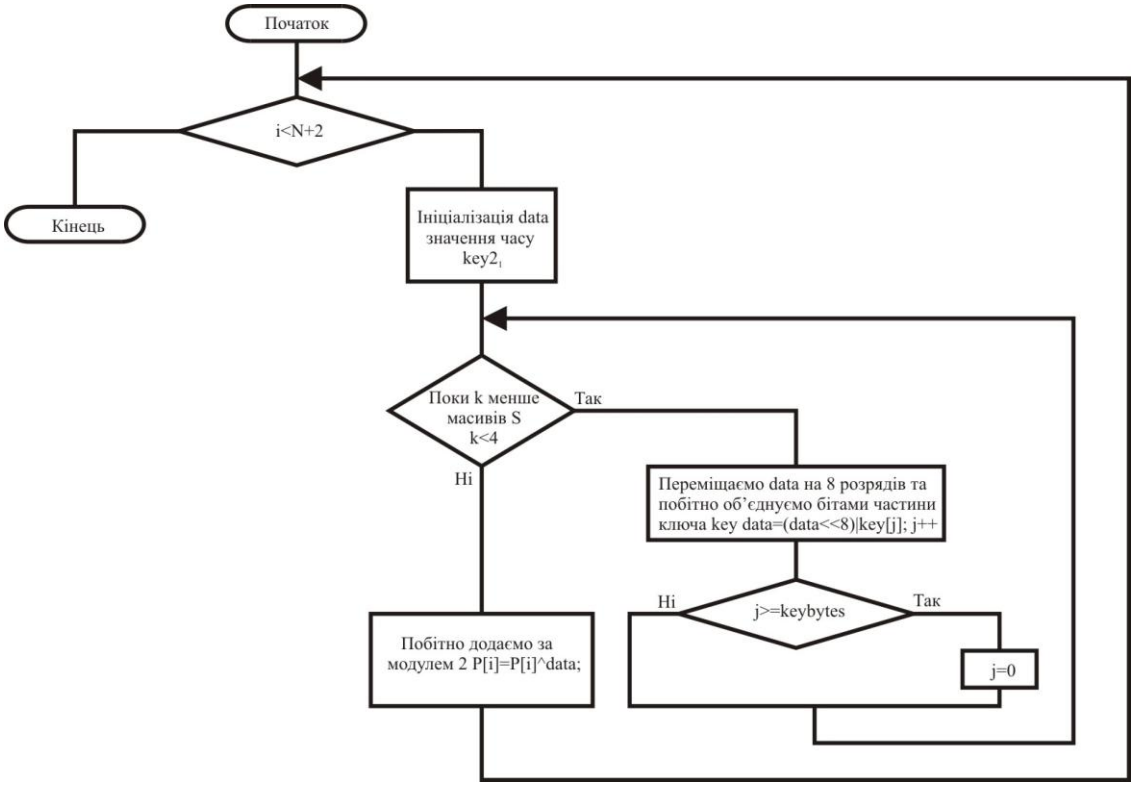

Рис. 2.15 – Схема ініціалізації P-масива

Після 18 ітерацій масив P має значення: (таблиця 2.5)

Таблиця 2.5 – Масив P

I	P_i	I	P_i
0	825373489	9	825373489
1	842215730	10	842215730
2	858862131	11	858862131
3	825373489	12	825373489
4	842215730	13	842215730
5	858862131	14	858862131
6	825373489	15	825373489
7	842215730	16	842215730
8	858862131	17	858862131

Формуємо ключ P шляхом його шифрування (рис. 2.16).

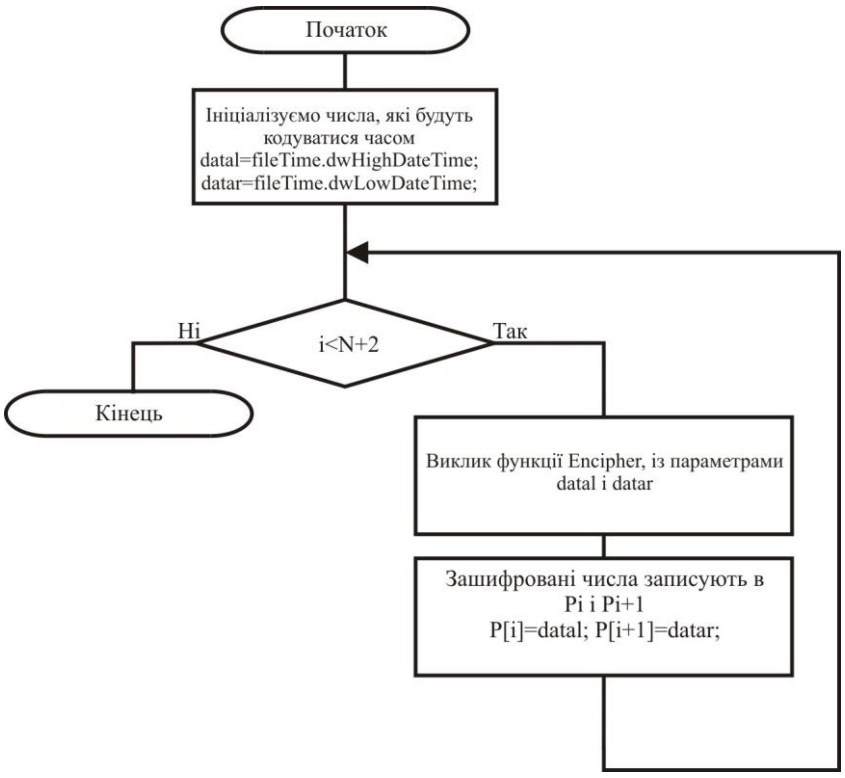

Рис. 2.16 – Схема формування ключа P

Функція шифрування реалізується алгоритмом, поданим на рис. 2.17, а функція підстановки за алгоритмом 2.18. Ключі P_{16} = 1378648790 і P_{17} = 3763196346 використаємо для шифрування S-блоків згідно алгоритму (рис. 2.19). Отриманий ключ P подаємо (табл. 2.6).

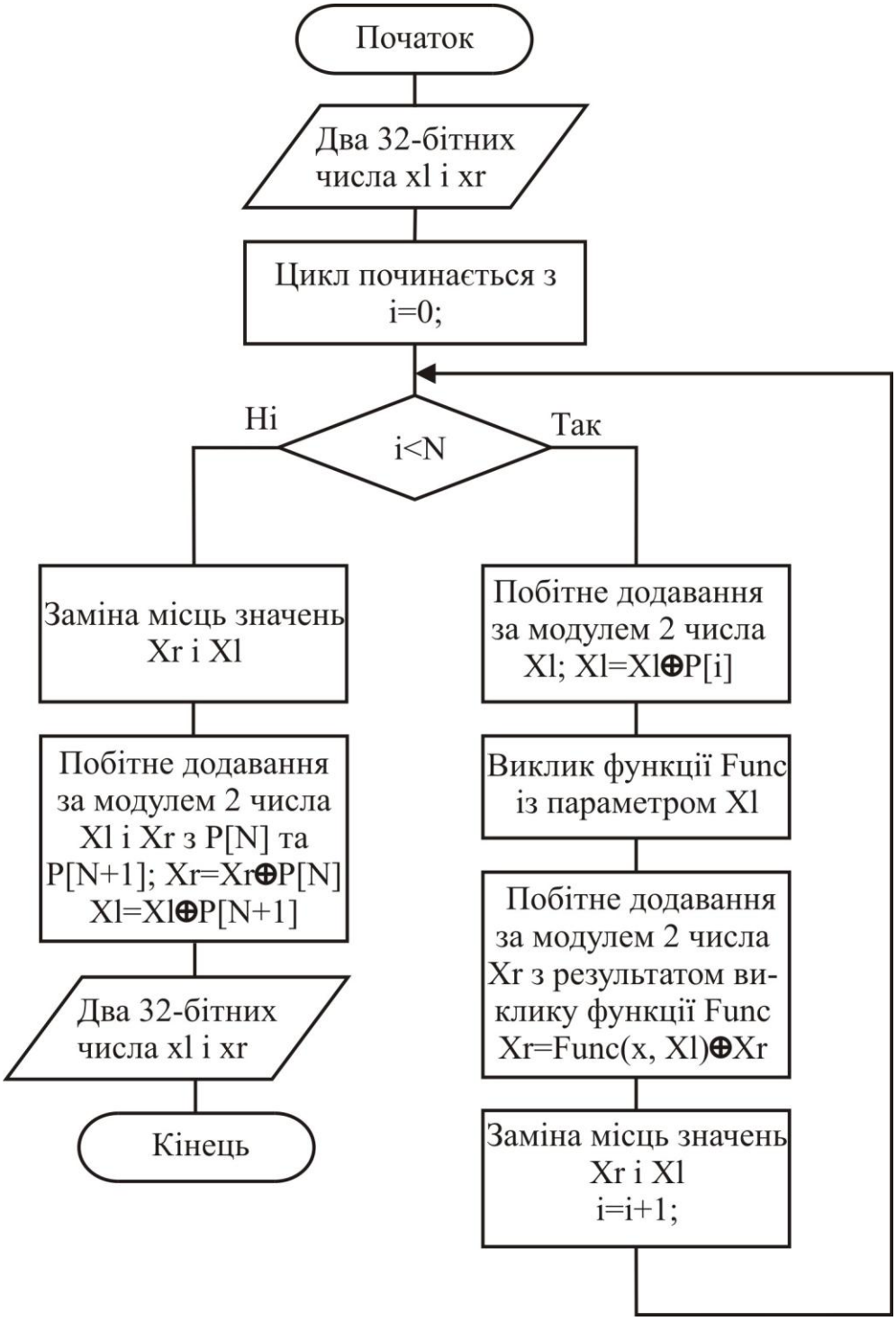

Рис. 2.17 – Схема функції шифрування

Рис. 2.18 – Схема функції підстановки

Таблиця 2.6 Отриманий ключ P

i	P_i	i	P_i
0	4165234673	9	2855859498
1	3761818135	10	211628703
2	56576929	11	229215014
3	2972412835	12	2975195587
4	1532165121	13	1222433681
5	2009599660	14	3647362257
6	2052070073	15	3888116358
7	3759878850	16	1378648790
8	3643748150	17	3763196346

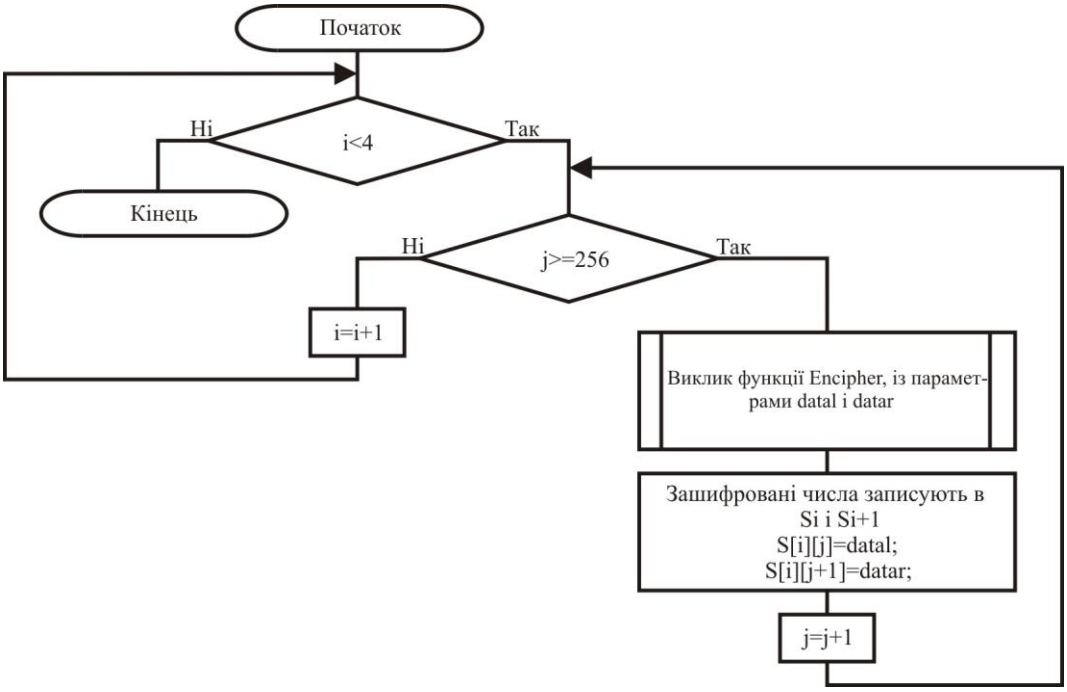

Рис. 2.19 – Схема шифрування S-блоків

У функцію шифрування передаються два 32-бітних числа, обираються спочатку перше і останнє, поступово направляючись до середини.

1, 2, 3, 4,…20, 21, 22…38, 39, 40, 41

Якщо залишається одне число, то воно кодується разом з наступним елементом масиву після нього. Так, у наведеному прикладі, 21 буде кодуватися з 41. При обраній операції ці числа будуть кодуватися першими. Це дає можливість кодувати як парну кількість подвійних слів, так і непарну.

Процес кодування двох 32-бітних чисел X_L і X_R складається з таких етапів:

1. Наступні операції виконуються у циклі 16 раз.

1.1. $X_L = X_L \oplus X_R$ – числа додаються за модулем 2

1.2. X_R = Func(X_L) $\oplus X_R$ – число X_R додається за модулем 2 з F(X_L), де F(X_L) – це функція, яка виконує наступні дії:

1.2.1 Розділяємо X_L на чотири 8-бітних частини: *a, b, c, d*, що здійснюється зсувом цього числа праворуч на 8 біт.

1.2.2 Функція обчислюється як $((S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus S_{3,c}) + S_{4,d} \bmod 2^{32}$.

1.3. Переставляємо X_L та X_R

2. Переставляємо X_L та X_R

3. $X_R = X_R \oplus P_{17}$ – числа додаються за модулем 2 з елементом ключа P_{17}

4. $X_R = X_R \oplus P_{18}$ – число додається за модулем 2 з елементом ключа P_{18}

Ми отримали закодоване повідомлення.

Результат в 32-бітних числах:

Таблиця 2.7 – Вихідна зашифрована інформація

i	Зашифровані дані
0	1427316382
1	3983571191
2	404923365

Висновки

Використання запропонованої моделі динамічної зміни підключів дозволило розробити пристрій блоково-динамічного шифрування в системі «клієнт-банк», який підвищує ефективність функціонування сучасних блочних шифрів. Він також дає можливість проводити процеси шифрування та дешифрування інформації заздалегідь підготовленими секретними даними, що готуються в доповняльних блоках. Застосування пристрою дозволило підвищити ступінь захисту в системі «клієнт-банк».

Розроблено пристрій для передачі та прийому шифрованої інформації на основі моделі алгоритму блоково-динамічно шифрування в системі «клієнт-банк». Пристрій дає можливість шифрувати та розшифровувати цифрові дані, які подаються на вхід, використовуючи розроблений блоково-динамічний метод шифрування. Моделювання його в середовищі Active-HDL дозволяє реалізувати його на сучасних ПЛІС.

Технічно реалізовано пристрій шифрування даних на основі алгоритму блоково-динамічно шифрування в системі «клієнт-банк» на базі ПЛІС у вигляді VHDL-моделі. Для реалізації пристрою було створено кілька окремих блоків, які з’єднані шинами даних. VHDL-моделювання блоково-динамічного шифрування показало процес шифрування повідомлень, а також дало можливість показати ефективність застосування ПЛІС для підвищення швидкодії реалізації запропонованого методу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Грушо А. А. Теоретические основы защиты информации / Грушо А. А., Тимонина Е. Е. – М.: Издательство Агентства "Яхтсмен", 1996. – 192 с.

2. Biham E. Differential Cryptanalysis of the Data Encryption Standard / Biham E., Shamir A. – Springer: Verlag, 1993. – 385 p.

3. Гундарь К. Ю. Основы современной криптографии / Гундарь К. Ю., Гончаров В. В., Серов Р. Е. – М.: ЮНИТИ, 2001. – 312 с.

4. Варфоломеев А. А. Криптосистемы. Основные свойства и методы анализа стой кости: Учебное пособие / Варфоломеев А. А., Жуков А. Е., Пудовкина М. А. – М.: ПАИМС, 2000. – 272 с.

5. Блочные криптосистемы. Основные свойства и методы анализа стойкости: Учебное пособие / Варфоломеев А. А., Жуков А. Е., Мельников А. Б., Устюжанин Д.Д. – М.: МИФИ, 1998. – 198 с.

6. Поляков А. К. Моделирование ЭВМ на языке VHDL / Поляков А. К. – М.: МЭИ, 1994. – 107 с.

7. Ben Cohen. VHDL Coding Styles and Methodologies / Ben Cohen – Boston: Kluwer Academic Publisher, 1995. – 314 pp.

8. Грушвицкий Р. И. Проектирование систем на микросхемах программируемой логики / Грушвицкий Р. И., Мурсаев А. Х., Угрюмов Е. П. – Спб.: БХВ – Петербург, 2002. – 608 с.

9. Стешенко В. Б. Синтез логических схем с использованием языка VHDL. Военная наука и техника / Стешенко В. Б. – 2003. – № 2. – С.78-84.

10. Поляков А. К. Языки VHDL и VERILOG в проектировании цифровой аппаратуры / Поляков А. К. – М.: СОЛОН-Пресс, 2003. – 320 с.

11. Дж. Ф. Уэйкерли. Проектирование цифровых устройств / Дж. Ф. Уэйкерли. – М.: Постмаркет, 2002. – 554 с.

12. Білан С. М. Алгоритмічно-функціональне VHDL – моделювання та технічна реалізація блоково-динамічного шифрування на ПЛІС. Матеріали першої міжнародної науково-технічної конференції „Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2005)” / Білан С. М. , Шварц І. М. – Вінниця, 2005. – с. 26-30.

13. Колесник В. Д. Курс теории информации / Колесник В. Д., Полтырев Г. Ш. – М.: Наука, 1982. – 456 с.

14. Лагутин В.С. Утечка и защита информации в телефонных каналах / Лагутин В.С., Петраков А.В. – М.: Энергоатомиздат, 1996. – 304с.

Анотація
Наукова робота - Шифр Панцир

Об’єм роботи складає 28 сторінок. Робота містить 20 рисунків та 7 таблиць, 14 бібліографічних джерел.

Інформація – одне з найважливіших джерел процвітання будь-якої держави, банку чи фірми. Недарма кажуть: “Хто володіє інформацією, той володіє світом”. Будь-яке управлінське рішення базується і коштує тієї інформації, на основі якої воно прийняте.

Витік інформації може завдати серйозної шкоди банку, його економічному становищу та іміджу, часто дозволяючи конкурентам зайняти провідні позиції на ринку, а іноді призводить і до банкрутства.

Без комплексного вирішення питань захистустворити надійну систему електронних розрахунків і зробити доступ до неї простим і зручним для всіх її учасників є завданням недосяжним.

Найбільш вразливим місцем в системі «клієнт-банк» є пересилання документів між клієнтом і банком. Це породжує три типи проблем, пов’язаних з необхідністю:

- взаємного розпізнавання абонентів (проблема автентифікації при встановленні зв’язку);

- захист документів, які передаються каналами зв’язку (забезпечення цілісності та конфіденційності документів);

- захист самого процесу обміну документами (проблема доведення факту відправлення/доставки документа).

У банку в процесі обробки прийнятого ЕПД можуть виникнути такі проблеми:

- підтвердження цілісності та юридичної значимості прийнятого документа (ідентифікація та автентифікація відправника, а також автентифікація повідомлення);

- забезпечення захисту від несанкціонованої модифікації вже прийнятого ЕПД або від нав’язування хибної інформації зловмисником всередині відділення банку;

- захист цілісності використовуваних при обробці ЕПД в банку програмних засобів для блокування можливостей несанкціонованого доступу і модифікації інформації про стан рахунків клієнта;

Метою роботи є визначення принципів роботи і розробка апаратних засобів для шифрування інформації та збільшення криптостійкості блочних алгоритмів в системі «Клієнт-Банк» на основі введення динамічного ключа.

Об'єктом досліджень є криптографічний захист інформації при встановленні з’єднання від несанкціонованого користування.

Предметом досліджень засоби блочного шифрування інформації в системі «клієнт-банк».

Методи досліджень базуються на теорії криптографії, теорії алгебри логіки, теорії скінченних автоматів та комп'ютерному моделюванні.