



УКРАЇНА

(19) UA

(11) 53617

(13) C2

(51) 7 H04L9/18

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(54) ПРИСТРІЙ КОДУВАННЯ

1

2

(21) 97073759

(22) 23 01 1996

(24) 17 02 2003

(86) PCT/DE96/00094, 23.01.1996

(31) 195 05 097 5

(32) 15 02 1995

(33) DE

(46) 17 02 2003, Бюл. № 2, 2003 р.

(72) Райнер Роберт, DE

(73) СІМЕНС АКЦІЕНГЕЗЕЛЬШАФТ, DE

(56) Патент EP №0384478 публ. 29 08 1990

(57) 1 Пристрій кодування з блоком кодування, який містить щонайменше один вхід даних та щонайменше один вихід даних, а також тактовий вхід, який через перший перемикач навантажений тактовим сигналом, вихідний реєстр, що містить один вхід даних і один вихід даних, а також тактовий вхід, який навантажений тактовим сигналом, причому вихід даних блока кодування з'єднаний з входом даних вихідного реєстра через другий перемикач, який відрізняється тим, що пристрій оснащений засобами для створення першого і другого проміжків часу, підключеними з можливістю керування першим перемикачем, або, відповідно, другим перемикачем, причому другий проміжок часу лежить усередині першого проміжку часу, а керований тактовим сигналом блок кодування підключений з можливістю створення з вхідних даних вихідних даних протягом першого проміжку часу, і передачі цих вихідних даних про-

тягом другого проміжку часу від блока кодування через другий перемикач у вихідний реєстр

2 Пристрій кодування за п. 1, який відрізняється тим, що засоби для створення першого і другого проміжків часу утворені регульованим лічильником, який забезпечений тактовим входом, що навантажений тактовим сигналом

3 Пристрій кодування за п. 1 або 2, який відрізняється тим, що вихідний реєстр виконаний у вигляді зсувного реєстра, другий перемикач є перемикачем із двома входами і одним виходом, а вихід даних вихідного реєстра з'єднаний з другим входом перемикача

4 Пристрій кодування за п. 3, який відрізняється тим, що зсувний реєстр розділений на множину частин зсувного реєстра, причому до кожної частини зсувного реєстра доданий, відповідно, перемикач, вихід якого з'єднаний з входом, і другий вхід якого з'єднаний з виходом блока зсувного реєстра, а перший вхід з'єднаний з виходом увімкнутого перед ним блока зсувного реєстра або блока кодування, причому кожен перемикач підлягає керуванню засобами створення проміжків часу

5 Пристрій кодування за будь-яким з пп. 1 - 4, який відрізняється тим, що блок кодування охоплений зворотним зв'язком з зсувним реєстром із доданим до нього нелінійним блоком виводу

6 Пристрій кодування за будь-яким з пп. 1 - 5, який відрізняється тим, що вихідний реєстр заблокований для передчасного зчитування

При передачі даних між двома блоками однієї системи, наприклад, між таким рухомих елементом, як мікросхема карта, і стаціонарним елементом, як пристрій зчитування, стає все більш важливим кодувати дані, які підлягають передачі, тому що знання переданих даних дає б зловмиснику можливість маніпулювати процесом, який керується цими даними. Процес кодування може відбуватися таким чином, що спочатку від одного з блоків передають до іншого блоку дані, що кодується там за допомогою пристрою кодування. Закодовані дані потім передають назад від блоку, що кодує, до блоку, що передає. У блоці, що передає,

закодовані дані знову декодують, причому при такому процесі можна застосовувати як симетричні так і несиметричні алгоритми, або кодувати, як у рухомому елементі, і порівнювати з прийнятим закодованим даним

Названий останнім спосіб хоча і не може використовуватися для передачі будь-якої інформації, тому що кінцевий приймач повинен вже знати інформацію, проте він може служити переважно для підтвердження вірогідності, тому що рухомий елемент, що кодує прийняте дані і передає його назад на стаціонарний елемент, повинен у такий спосіб доводити, що він має у своєму розпоряд-

(13) C2

(11) 53617

(19) UA

дженні правильний алгоритм кодування, або, відповідно, пристрій правильного кодування і може себе в такий спосіб посвідчити. Таким самим чином може відбуватися, природньо, і підтвердження автентичності стаціонарного елемента, або, відповідно, пристрою зчитування, тому що тільки тоді, коли обидва елементи розташовують тим же самим пристроєм кодування, або, відповідно, тим же самим алгоритмом кодування, закодоване в обох елементах дане при порівнянні дає в результаті позитивний збіг.

Для більшості алгоритмів кодування, у яких в приймачі знову декодують закодоване дане, необхідні складні обчислювальні блоки, що, звичайно, утворені мікропроцесором і спеціальним сопроцесором, і потребують значного часу обчислення. Значно простішими є псевдовипадкові генератори, з якими проте може здійснюватися тільки вищезазначений другий спосіб, тому що кодування вхідного даного такого псевдовипадкового генератору не може бути скасоване, й у таким чином в обох елементах системи може бути виконаний тільки процес кодування і порівняння один з одним результатів обох процесів кодування.

Вхідними даними для пристрою кодування звичайно стає дане, яке підлягає кодуванню, а також секретний код. Для підвищення надійності, проте, можуть залучатися також інші дані, зокрема, дані, що змінюються в часі, наприклад, вміст лічильника помилок. Усі ці вхідні дані переробляють за допомогою секретного алгоритму, який утримується в закодованих вихідних даних. Алгоритм при цьому може бути реалізований, як у прикладі зсувового регістру, апаратними засобами, наприклад, за рахунок логічного зв'язку множини наявних у зсувовому регістрі станів.

Оскільки дані в будь-якому випадку присутні у цифровій формі, для їхнього кодування необхідний тактовий сигнал, що синхронізує окремі процеси. З множини імпульсів тактового сигналу, що з'являються в процесі кодування, зловмисник міг би спробувати зробити висновки про вид процесу кодування.

За прототип винаходу, що пропонується, прийнято пристрій кодування з блоком кодування, що містить, щонайменше, один вхід даних та, щонайменше, один вихід даних, а також тактовий вхід, який через перший перемикач навантажено тактовим сигналом, із вихідним регістром, що містить один вхід даних і один вихід даних, а також тактовий вхід, що навантажено тактовим сигналом, причому вихід даних блоку кодування з'єднаний з входом даних вихідного регістру через другий перемикач (ЄП, А, 0 384 478, МКІ⁶ Н04L 9/18, 29 08 90 р.)

Недоліком відомого пристрою є недостатня надійність захисту даних, що підлягають передачі, від особи, зацікавленої в їх виявленні. Як правило, предметом зацікавленості є вид процесу кодування, тобто його тривалість, яка в зазначеному пристрої недостатньо захищена і може бути визначеною.

В основу винаходу поставлена задача створення умов для неможливості розпізнавання часу, необхідного для створення результатів кодування, в пристрої для кодування шляхом оснащення його

засобами для створення проміжків часу, які з допомогою відповідних ім перемикачів керують перетворенням вхідного сигналу у вихідний, що забезпечує почергове функціонування перемикачів, і в умовах, коли перемикач, керований більшим проміжком часу, закритий, забезпечує можливість створення вихідних даних блоком кодування, що не вписуються у вихідний регістр і не вносять вкладу в закодований банк даних при неперервному процесі струмоспоживання вихідним регістром, і тим самим дезінформує стороннього спостерігача щодо визначення тривалості безпосередньо процесу кодування.

Поставлена задача досягається за рахунок того, що в пристрій кодування з блоком кодування, що містить, щонайменше, один вхід даних та, щонайменше, один вихід даних, а також тактовий вхід, який через перший перемикач навантажено тактовим сигналом, із вихідним регістром, що містить один вхід даних і один вихід даних, а також тактовий вхід, що навантажено тактовим сигналом, причому вихід даних блоку кодування з'єднаний з входом даних вихідного регістру через другий перемикач, згідно винаходу, оснащено засобами для створення першого і другого проміжків часу, підключених з можливістю управління першим перемикачем, або, відповідно, другим перемикачем, причому другий проміжок часу лежить усередині першого проміжку часу, а керований тактом тактового сигналу блок кодування підключений з можливістю створення з вхідних даних вихідні дані під час першого проміжку часу, і передачі цих вихідних даних під час другого проміжку часу від блоку кодування через другий перемикач у вихідний регістр, при цьому засоби для створення першого і другого проміжків часу утворені регульованим лічильником, який забезпечений тактовим входом, що навантажено тактовим сигналом.

Крім того, вихідний регістр виконано у вигляді зсувового регістру, другий перемикач є перемикачем із двома входами і одним виходом, а вихід даних вихідного регістра з'єднаний з другим входом перемикача, причому цей зсувовий регістр розділений на множину частин зсувового регістра, причому кожній частині зсувового регістра додано у відповідність перемикач, вихід якого з'єднаний з входом, і другий вхід якого з'єднаний з виходом блоку зсувового регістра, а перший вхід з'єднаний з виходом увімкненого перед ним блоку зсувового регістру або блоку кодування, причому кожен перемикач підлягає управлінню засобами створення проміжків часу.

Блок кодування запропонованого пристрою є охопленим зворотним зв'язком з зсувовим регістром з доданням йому нелінійним блоком виводу, а вихідний регістр заблокований для передчасного зчитування.

Винахід пояснюється нижче на прикладі виконання за допомогою фігур. При цьому на фігурах показано:

Фігура 1 - блок-схема спеціального пристрою кодування, що відповідає винаходу.

Фігура 2 - варіант виконання частини пристрою кодування, що відповідає винаходу.

Фігура 1 показує пристрій кодування, що відповідає винаходу, який містить у центральний час-

тині блок кодування VE. До цього блоку кодування VE підводять входні дані E. Ці входні дані E підводять у наведеному прикладі послідовно і складаються, вони, наприклад, з входного даного, яке повинно бути закодоване, секретного коду, а також інших даних, головним чином даних, які змінюються у часі, як, наприклад, актуальний стан лічильника помилок. Звичайно, було б також можливим підводити ці дані паралельно і логічно зв'язувати їх якимось чином. У наведеному прикладі блок кодування VE утворений зсувовим регістром SR, якому підпорядковано блок зворотнього зв'язку RK. Цей блок зворотнього зв'язку RK зв'язує відповідні логічні стани всередині зсувового регістру SR і підводить результат цього зв'язку назад до входу зсувового регістру SR, де він зв'язується з входними даними E, наприклад, підсумовується з ними. Зсувовому регістру SR далі поставлений у відповідність блок виводу AK, що нелінійно зв'язує певні стани зсувового регістру SR і підводить результат цього зв'язку, що може бути, наприклад, множенням, до перемикаючого елемента, SE, який управляється цим сигналом від AK. Через цей перемикаючий елемент SE вихідні дані зсувового регістру SR підводять до виходу блока кодування VE як вихідні дані A.

Зсувовий регістр SR у такий спосіб створює в залежності від входних даних E та від апаратної реалізації блоку зворотнього зв'язку RK безперервну послідовність бітів даних, з яких тільки деякі в залежності від блоку виводу AK підводяться до виходу блока кодування VE як вихідні дані A.

Ці вихідні дані A підводять до першого входу перемикача S2, вихід якого з'єднаний з входом вихідного регістру AR. Вихід цього вихідного регістру AR утворює, по-перше, вихід пристрою кодування, а, по-друге, підведений назад до другого входу перемикача S2. Вихідний регістр може при цьому бути послідовним регістром, як наприклад, зсувовий регістр, або також паралельним регістром, у якому відбувається запис мультиплексором. У цьому вихідному регістрі AR вихідні дані A проміжно запам'ятовуються і можуть бути зчитані тільки після закінчення процесу кодування. Щоб забезпечити синхронність блоку кодування VE і вихідного регістра AR, до обох елементів пристрою кодування згідно з винаходом підводять тактовий сигнал C1. До блоку кодування VE тактовий сигнал C1 підводять проте через перемикач S1. Обидва перемикачі S1 та S2 управляються, відповідно, сигналом, що походить від засобів для створення сигналів St1, St2, які тривають певний відрізок часу. При цьому перемикач S1 управляється сигналом St2, що триває проміжок часу t1. Перемикач S2 управляється сигналом St2, котрий триває проміжок часу t2, котрий знаходиться всередині проміжку часу t1. Засіб Z може бути виготовлений переважно з лічильником, який після досягнення визначених проміжків часу t1, t2 видає відповідно сигнали St1, St2 для приведення в дію перемикачів S1, S2. З цією метою до лічильника засобу Z підводять також тактовий сигнал C1.

Пристрій кодування працює таким чином.

При включенні перемикач S1 замкнений, а перемикач S2 знаходиться в такому стані, що вихід блоку кодування VE з'єднано з входом вихідного

регістру AR. Одночасно з тактовим сигналом C1 блок кодування VE починає створювати вихідні дані A, що записуються у вихідний регістр AR через перемикач S2. Після закінчення проміжку часу t2 сигнал St2 змінює свій стан так, що перемикач S2 перемикається і вихід вихідного регістру AR через перемикач S2 з'єднується з його входом. Перемикач S1 залишається і далі закритим, тому що проміжок часу t1 є більшим, ніж проміжок часу t2. Блок кодування VE створює таким чином і далі вихідні дані A, які, однак, більше не вписуються у вихідний регістр AR і тим самим не вносять вкладу у закодоване слово даних. Замість цього дані у вихідному регістрі AR зрушуються по колу. Після закінчення проміжку часу t1 стан сигналу St1 змінюється так, що перемикач S1 відкривається і блок кодування VE більше не одержує тактового сигналу, і таким чином більше не може створювати вихідні дані A.

Спостерігач цього процесу кодування може ззовні тільки вимірювати споживання струму напівпровідниковою мікросхемою, яка містить у собі пристрій кодування, і звідси робити висновки про тривалість процесу кодування. Оскільки тактовий сигнал C1 підводиться до пристрою кодування довше, ніж триває власне процес кодування і споживання вихідного регістру також не припиняється, оскільки також до нього підводять і далі тактові сигнали і, таким чином, дані зрушуються по колу, визначення тривалості дійсного процесу кодування є неможливим.

Значення проміжків часу t1 і t2 можуть запам'ятовуватися у незагубленому при відключенні живлення накопичувачі, що може також утримуватися поряд з пристроєм кодування в напівпровідниковій мікросхемі, ці значення, відповідно, завантажуються до початку процесу кодування в лічильник Z. Поряд із підведеним до блоку кодування VE секретним кодом вони являють собою секретні дані пристрою кодування і за допомогою відповідних заходів безпеки не повинні бути доступними ззовні.

Було б також можливим підводити до лічильника Z третій проміжок часу, причому проміжок часу t2 починає збігати тільки після третього проміжку часу після початку першого проміжку часу t1.

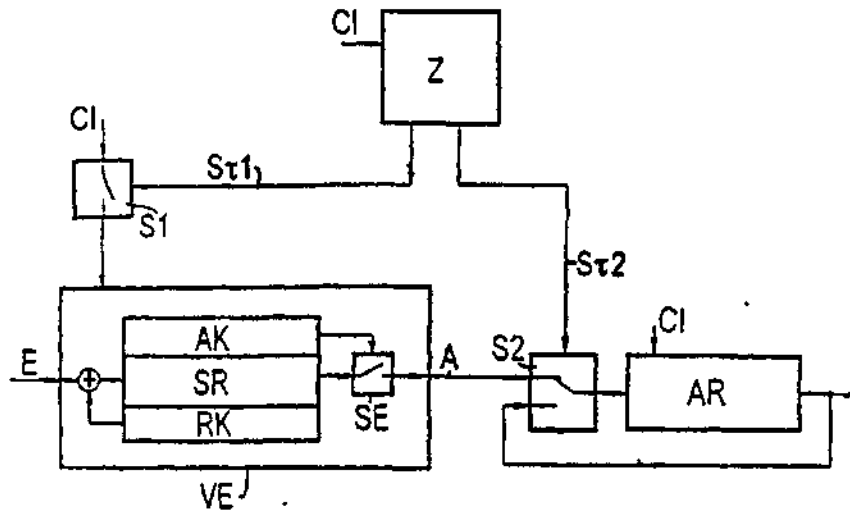
На фігурі 2 наведена альтернатива до поданого на фігурі 1 вихідного регістру AR у з'єднанні з перемикачем S2. Вихідний регістр AR при цьому розділений на множини частин AR1, ARn, яким поставлено у відповідність по перемикачу U1, Un. При цьому вихідні дані A блоку кодування VE підводять до першого входу першого перемикача U1, причому вихід цього першого перемикача U1 з'єднаний з виходом першої частини вихідного регістру AR1. Вихід першої частини вихідного регістру AR1 з'єднаний по-перше, з першим входом другого перемикача U2 і, по-друге, з другим входом першого перемикача U1. Однаковим чином з'єднані інші перемикачі U2, Un і частини вихідного регістру AR2, ARn. Вихід частини вихідного регістру ARn утворює вихід усього вихідного регістру.

До кожного з перемикачів U1, Un підведений другий сигнал St2, що триває другий проміжок часу t2. Крім того, до кожного з вихідних регістрів

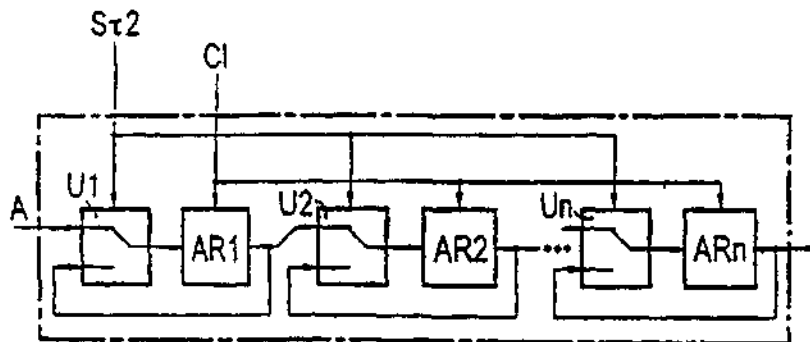
AR1 ARn підведений тактовий сигнал C1. При цьому варіанті вихідного регістру зміст цього вихідного регістру зрушується не через увесь регістр, а тільки через окремі частини. У екстремальному випадку мова може йти тільки про один єдиний біт, так що послідовність закодованого вихідного даного, що стоїть у вихідному регістрі, більше не змінюється також після закінчення другого проміжку часу t2.

Вихідний регістр AR повинен бути виконаний у

наведених на фігурах 1 та 2 випадках у вигляді зсувних регістрів, проте це виконання вихідних регістрів не є обов'язковим для реалізації задуму, що лежить у підґрунті винаходу. Основною умовою є тільки те, що споживання струму вихідного регістру також після закінчення другого проміжку часу t2 не змінювалось, так що спостерігач ззовні не зможе розпізнати, з якого часу у вихідний регістр більше не записуються ніякі дані.



Фіг.1



Фіг.2